F-Secure Anti-Virus Client Security

Guide de l'administrateur

« F-Secure » et le symbole du triangle sont des marques déposées de F-Secure Corporation, et les noms des produits F-Secure ainsi que les symboles et logos sont des marques déposées ou des marques de commerce de F-Secure Corporation. Tous les noms de produits mentionnés dans la présente documentation sont des marques commerciales ou des marques déposées de leurs sociétés respectives. F-Secure Corporation dénie tout intérêt propriétaire vis-à-vis des marques et noms de sociétés tierces. F-Secure Corporation ne pourra être tenue pour responsable des erreurs ou omissions afférentes à cette documentation, quand bien même cette société s'efforce de vérifier l'exactitude des informations contenues dans ses publications. F-Secure Corporation se réserve le droit de modifier sans préavis les informations contenues dans ce document.

Sauf mention contraire, les sociétés, noms et données utilisés dans les exemples sont fictifs. Aucune partie de ce document ne peut être reproduite ou transmise à quelque fin ou par quelque moyen que ce soit, électronique ou mécanique, sans l'autorisation expresse et écrite de F-Secure Corporation.

Ce produit peut être couvert par un ou plusieurs brevets F-Secure, dont les suivants :

GB2353372 GB2366691 GB2366692 GB2366693 GB2367933 GB2368233 GB2374260

Copyright © 2004 F-Secure Corporation. Tous droits réservés.

12000060-5C18

Sommaire

A PROPOS DE CE GUIDE

Présentation

Ce manuel décrit la configuration et les opérations que vous pouvez effectuer avec l'interface utilisateur du mode antivirus de F-Secure Policy Manager et fournit les informations dont vous avez besoin pour commencer l'administration centralisée d'applications F-Secure Anti-Virus Client Security.

Le Guide de l'administrateur de F-Secure Anti-Virus Client Security contient les chapitres suivants.

Chapitre 1. *Introduction*. Décrit les composants de base de F-Secure Anti-Virus Client Security et les principales fonctions de F-Secure Policy Manager.

Chapitre 2. *Installation de F-Secure Policy Manager*. Instructions d'installation de F-Secure Policy Manager Server et de la console.

Chapitre 3. *Introduction à l'interface utilisateur du mode antivirus de F-Secure Policy Manager*. Décrit les composants de l'interface utilisateur du mode antivirus de F-Secure Policy Manager.

Chapitre 4. *Configuration du réseau géré*. Explique comment planifier et créer le réseau administré de manière centralisée.

Chapitre 5. *Configuration de la protection contre les virus et les logiciels espions*. Explique comment configurer les mises à jour de définitions de virus, l'analyse en temps réel et l'analyse du courrier électronique.

Chapitre 6. *Configuration de la protection Internet*. Explique comment configurer les niveaux et règles de sécurité, le contrôle des applications et le système de détection des intrusions (IDS).

Chapitre 7. *Comment vérifier que l'environnement est protégé*. Fournit une liste de contrôle concernant la surveillance du domaine et la façon de d'assurer que le réseau est protégé.

Chapitre 8. *Mise à jour du logiciel*. Contient des instructions sur la mise à niveau du logiciel avec F-Secure Policy Manager.

Chapitre 9. *Opérations sur les hôtes locaux*. Fournit des informations sur les tâches d'administration telles que la planification locale d'une analyse et la collecte d'informations à partir des fichiers journaux locaux.

Chapitre 10. *Informations sur les virus*. Explique où obtenir des informations supplémentaires sur les virus et comment envoyer un échantillon de virus à F-Secure.

Chapitre 11. *Configuration de la prise en charge de Cisco NAC*. Décrit l'installation et la configuration d'un support NAC (Network Access Control) Cisco.

Chapitre 12. *Fonctions avancées : Protection contre les virus et les logiciels espions*. Couvre les fonctions avancées de protection antivirus, telles que l'analyse planifiée, l'utilisation du proxy antivirus et la gestion basée sur SNMP.

Chapitre 13. *Fonctions avancées : Protection Internet*. Couvre les fonctions de protection Internet avancées, telles que la vérification des ports et de l'IP avec le contrôle des applications, l'ajout de nouveaux services et le dépannage des problèmes de connexion.

Annexe A. *Modification de PRODSETT.INI*. Contient des informations concernant la modification de PRODSETT.INI, fichier qui indique au programme d'installation les modules logiciels à installer sur les postes de travail.

Annexe B. *Messages d'alerte et d'erreur de l'analyse du courrier électronique*. Décrit les messages d'alerte et d'erreur que l'analyse du courrier électronique peut générer.

Glossaire — Définition des termes

Support technique — Web Club et contacts pour obtenir de l'aide.

A propos de F-Secure Corporation — Présentation de la société et de ses produits.

Documentation complémentaire

F-Secure Policy Manager Aide en ligne

L'aide en ligne de F-Secure Policy Manager contient des informations sur les interfaces utilisateur tant en mode antivirus qu'en mode avancé. L'aide en ligne est accessible à partir du menu *Aide* en sélectionnant*Sommaire de l'aide* ou en appuyant sur F1.

Des informations concernant l'interface utilisateur du mode antivirus de F-Secure Policy Manager sont accessibles sous Administration de *F-Secure Anti-Virus Client Security Administration* dans l'arborescence de navigation.

Des informations concernant l'interface utilisateur du mode avancé de F-Secure Policy Manager sont accessibles sous F-Secure Policy Manager dans l'arborescence de navigation.

F-Secure Anti-Virus Client Security Aide en ligne

L'interface utilisateur locale de F-Secure Anti-Virus Client Security s'accompagne d'une aide en ligne contextuelle. Cette aide en ligne est accessible à partir de l'interface utilisateur principale et des boîtes de dialogue avancées en cliquant sur le bouton **Aide** ou en appuyant sur F1.

L'aide en ligne s'ouvre toujours sur une page contenant des informations sur votre emplacement actuel dans l'interface utilisateur de F-Secure Anti-Virus Client Security. Le volet de gauche de l'aide en ligne permet de parcourir rapidement l'aide au travers de l'arborescence et d'accéder à une fonction de recherche.

F-Secure Policy Manager Guide de l'administrateur

Pour plus d'informations sur l'administration d'autres produits logiciels F-Secure avec F-Secure Policy Manager, reportez-vous au Guide de l'administrateur de F-Secure Policy Manager. Ce dernier contient des informations sur l'interface utilisateur en mode avancé et explique comment configurer et gérer d'autres produits F-Secure. Il propose également des informations sur F-Secure Management Agent, F-Secure Policy Manager Web Reporting et F-Secure Anti-Virus Proxy.

Guide de l'administrateur de F-Secure Policy Manager Reporting Option

Le Guide de l'administrateur de F-Secure Policy Manager Reporting Option explique comment générer des rapports indiquant, par exemple, les taux d'infection ou les mises à jour des définitions de virus dans le domaine géré. Il décrit aussi les modèles disponibles pour les types de rapports les plus couramment utilisés et explique comment personnaliser les rapports.

Conventions utilisées dans les guides F-Secure

Cette section décrit les symboles, polices et termes utilisés dans ce manuel.

Symboles

WARNING: The warning symbol indicates a situation with a risk of irreversible destruction to data.

IMPORTANT: *An exclamation mark provides important information that you need to consider.*

REFERENCE - A book refers you to related information on the topic available in another document.

NOTE - A note provides additional information that you should consider.

TIP - A tip provides information that can help you perform a task more quickly or easily.

⇒ An arrow indicates a one-step procedure.

Fonts

Arial bold (blue) is used to refer to menu names and commands, to buttons and other items in a dialog box.

Arial Italics (blue) is used to refer to other chapters in the manual, book titles, and titles of other manuals.

Arial Italics (black) is used for file and folder names, for figure and table captions, and for directory tree names.

`Courier New` is used for messages on your computer screen.

Courier New bold is used for information that you must type.

SMALL CAPS (BLACK) is used for a key or key combination on your keyboard.

Arial underlined (blue) is used for user interface links.

Times New Roman regular is used for window and dialog box names.

PDF Document

This manual is provided in PDF (Portable Document Format). The PDF document can be used for online viewing and printing using Adobe® Acrobat® Reader. When printing the manual, please print the entire manual, including the copyright and disclaimer statements.

For More Information

Visit F-Secure at http://www.f-secure.com for documentation, training courses, downloads, and service and support contacts.

In our constant attempts to improve our documentation, we would welcome your feedback. If you have any questions, comments, or suggestions about this or any other F-Secure document, please contact us at documentation@f-secure.com.

1 INTRODUCTION

1.1 Présentation

Cette section décrit les principaux composants de F-Secure Client Security et de F-Secure Policy Manager et fournit une introduction à la gestion basée sur les stratégies.

1.2 F-Secure Client Security Composants et fonctions

F-Secure Client Security est utilisé pour protéger l'ordinateur des virus, des vers, des logiciels espions, des rootkits et autres antiprogrammes, ainsi que contre tout accès non autorisé à partir du réseau. F-Secure Client Security est composé de la protection antivirus, de la protection Internet et de la gestion des applications. Lors de l'installation de F-Secure Client Security, vous pouvez sélectionner les composants à installer.

1.2.1 Protection antivirus et antispyware

La protection antivirus et antispyware inclut plusieurs méthodes d'analyse : Analyse en temps réel, analyse du courrier électronique, analyse du trafic Web, recherche de rootkits et analyse manuelle. Il inclut également le contrôle du système, des mises à jour automatiques, l'Agent de mise à jour automatique F-Secure et le service d'informations sur les virus.

Analyse en temps réel

La fonction d'analyse en temps réel offre une protection continue contre les virus et logiciels espions lorsque les fichiers sont ouverts, copiés, déplacés, renommés ou téléchargés à partir d'Internet.

L'analyse en temps réel fonctionne de manière transparente en tâche de fond. Elle recherche la présence éventuelle de virus lorsque vous accédez à des fichiers stockés sur disque dur, sur disquettes ou sur lecteurs réseau. Si vous tentez d'accéder à un fichier infecté, l'analyse en temps réel interrompt automatiquement l'exécution du virus. En fonction de la stratégie de sécurité définie, le virus est supprimé du fichier ou un message d'avertissement s'affiche. Pour plus d'informations, reportez-vous à la section “*Configuration de l'analyse en temps réel*”, *166*.

Analyse du courrier électronique

L'analyse du courrier électronique peut être utilisée pour analyser les messages électroniques entrants et sortants et leurs pièces jointes. Elle empêche les virus de pénétrer sur le réseau de l'entreprise et vous empêche d'envoyer par mégarde des pièces jointes infectées. L'analyse du courrier électronique peut être configurée pour éliminer les pièces jointes infectées des messages entrants. Lorsqu'elle a détecté une infection dans un message sortant, elle peut bloquer le trafic sortant jusqu'à ce que le problème soit résolu. Pour plus d'informations, reportez-vous à la section “*Configuration de l'analyse du courrier électronique*”, *175*.

Analyse du trafic Web (HTTP)

L'analyse du trafic Web protège les ordinateurs contre les virus incorporés dans le trafic HTTP. Elle analyse les fichiers HTML, les fichiers images, les applications téléchargées et les fichiers exécutables, et supprime les virus automatiquement. Pour plus d'informations, reportez-vous à la section “*Configuration de l'analyse du trafic Web (HTTP)*”, *180*.

Recherche de rootkits

Si vous souhaitez vous assurer qu’il n’existe aucun fichier, aucun processus, aucune application ni aucun lecteur cachés sur votre ordinateur, vous avez la possibilité d’analyser manuellement le système à la recherche de rootkits. Pour plus d'informations, reportez-vous à la section “*Configuration de la recherche de rootkits*”, *173*.

Analyse manuelle

Vous pouvez utiliser l'analyse manuelle, par exemple après avoir installé F-Secure Client Security, si vous craignez qu'un virus ou un logiciel espion soit présent sur l'ordinateur ou si un virus a été détecté dans le réseau local. Vous pouvez choisir d'analyser tous les fichiers ou uniquement un certain type. Vous pouvez également décider de ce qu'il faut faire du fichier infecté ; l'Assistant de nettoyage vous guidera dans ce processus. Vous pouvez aussi utiliser la fonction **Analyse planifiée** pour analyser automatiquement et régulièrement votre ordinateur, par exemple toutes les semaines ou 1 ou 2 fois par mois.

Contrôle du système

Le contrôle du système est un nouveau système de prévention des intrusions fondé sur un hôte qui analyse le comportement des fichiers et des programmes. Il offre une couche supplémentaire de protection en bloquant les virus, vers et autres codes malveillants qui essaient d'effectuer des actions dangereuses sur votre ordinateur. Pour plus d'informations, reportez-vous à la section "*Configuration du contrôle du système*", *172*..

Mises à jour automatiques

La fonction Mises à jour automatiques assure la mise à jour permanente des définitions de virus et de logiciels espions. Les mises à jour de définitions de virus sont signées par F-Secure Anti-Virus Research Team. Cette signature est basée sur un cryptage solide et le paquet ne peut pas être modifié en cours de chemin.

Si les virus sont complexes, les mises à jour de définitions de virus comprennent des outils d'éradication prenant la forme de fichiers exécutables. L'intégrité du code exécutable fourni étant très importante, les moteurs d'analyse F-Secure vérifient que tout le code de mise à jour est signé par F-Secure Anti-Virus Research. Si cette intégrité est compromise, le code n'est pas exécuté. Pour plus d'informations, reportez-vous à la section "*Configuration des mises à jour automatiques*", *162*.

Agent de mise à jour automatique F-Secure

Grâce à l'Agent de mise à jour automatique F-Secure, vous pouvez recevoir des mises à jour de définitions de virus ainsi que des informations sans interrompre votre travail pour attendre le téléchargement complet des fichiers depuis le Web. Agent de mise à jour automatique F-Secure télécharge automatiquement les fichiers en tâche de fond en utilisant une bande passante non utilisée par d'autres applications Internet, ce qui vous permet d'être toujours sûr de bénéficier des dernières mises à jour sans avoir à les rechercher sur le Web.

Si l'Agent de mise à jour automatique F-Secure est connecté en permanence à Internet, il reçoit automatiquement les mises à jour de définitions de virus après leur publication par F-Secure.

Lorsque Agent de mise à jour automatique F-Secure démarre, il se connecte au serveur de mise à jour F-Secure. L'agent interroge régulièrement le serveur pour savoir si de nouvelles données sont disponibles. L'agent télécharge uniquement les parties de définitions de virus qui ont changé depuis le dernier téléchargement. Si le transfert est interrompu pour une raison quelconque, la session suivante démarre à partir de l'endroit où la session précédente s'est arrêtée. Pour plus d'informations, reportez-vous à la section “*Configuration des mises à jour automatiques*”, *162*.

Informations sur les virus

F-Secure Virus News vous avertit instantanément des événements majeurs qui se produisent dans le monde en matière de sécurité. Le service F-Secure Virus News est fourni avec Agent de mise à jour automatique F-Secure. Pour plus d'informations, reportez-vous à l'aide en ligne de F-Secure Client Security.

1.2.2 Protection Internet

La protection Internet comprend les modules Pare-feu, Contrôle des applications et Système de détection des intrusions (IDS). Ensemble, ces composants peuvent être utilisés pour protéger votre ordinateur contre les tentatives de connexion non autorisées, les attaques internes et le vol d'informations, les applications malveillantes et d'autres applications indésirables telles que les logiciels d'égal à égal. La protection des stations de travail et des portables avec la protection Internet F-Secure Client Security protège également l'ensemble du réseau local, car les ordinateurs individuels ne peuvent pas être utilisés comme porte d'accès au réseau.

La protection Internet offre différents niveaux de sécurité possibles selon les besoins des utilisateurs, de leur mobilité, de la stratégie de sécurité de l'entreprise et de l'expérience des utilisateurs.

Pare-feu

Le pare-feu fait partie intégrante de la protection Internet. Lorsque la protection Internet est installée sur votre ordinateur, vous bénéficiez d'une protection par pare-feu, même quand vous n'êtes pas connecté au réseau local (par exemple, chez vous, lorsque vous vous connectez à Internet via un fournisseur d'accès).

En règle générale, un pare-feu autorise ou refuse le trafic en fonction des adresses locales ou distantes, des protocoles et des services utilisés et de l'état actuel des connexions existantes. Il est également possible d'émettre une alerte chaque fois qu'une règle est appelée ou que des datagrammes interdits sont reçus, ce qui permet de visualiser plus facilement le type de trafic circulant sur le système. Pour plus d'informations, reportez-vous à la section “*Configuration des niveaux et règles de sécurité de la protection Internet*”, *204*.

Contrôle des applications

Le contrôle des applications peut servir à empêcher les applications non autorisées d'accéder au réseau. En outre, le contrôle de lancement des applications et le contrôle de manipulation des applications protègent les ordinateurs contre les applications malveillantes qui tentent de lancer ou d'utiliser d'autres applications sur l'ordinateur.

Le contrôle des applications offre à l'administrateur la possibilité de contrôler l'utilisation du réseau et d'empêcher l'emploi d'applications qui sont contraires à la stratégie de sécurité de l'entreprise. Ces mécanismes permettent de faciliter la prévention de la plupart des attaques présentées ci-dessus tout en renforçant les stratégies de sécurité mises en place. Vous pouvez configurer différentes règles pour différentes applications : les applications qui sont considérées comme fiables peuvent bénéficier d'un accès libre ; les autres applications peuvent se voir refuser l'accès ou c'est à l'utilisateur de décider si l'application peut établir une connexion. Pour plus d'informations, reportez-vous à la section “*Configuration du contrôle des applications*”, *216*.

Système de prévention des intrusions

Le système de prévention des intrusions (IDS) peut être utilisé pour détecter des schémas suspects dans le trafic réseau. Il peut aussi être utilisé pour surveiller les virus qui tentent de s'attaquer aux ordinateurs du réseau local. IDS enregistre les tentatives de connexion systématiques effectuées depuis l'extérieur, qui sont souvent un signe que quelqu'un tente de trouver des ports ouverts sur l'hôte. Le système de détection des intrusions bloque les paquets malveillants visant ce type de port sur l'hôte. Pour plus d'informations, reportez-vous à la section “*Configuration de la prévention des intrusions*”, *226*.

1.2.3 Gestion des applications

Agent SNMP

F-Secure SNMP Agent est un agent d'extension SNMP Windows NT, chargé et déchargé avec l'agent principal. Cet agent offre un sous-ensemble des fonctionnalités de Policy Manager et sert essentiellement à des fins d'alerte et de surveillance de statistiques.

F-Secure Management Agent

F-Secure 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 F-Secure Policy Manager, et effectue des installations basées sur la stratégie.

Prise en charge NAC (Network Admission Control) Cisco

F-Secure Corporation 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. Pour plus d'informations, reportez-vous à la section “*Configuration de la prise en charge de Cisco NAC*”, *267*.

1.3 Introduction à F-Secure Policy Manager

Cette section présente une brève introduction à F-Secure Policy Manager. Pour plus d'informations, reportez-vous au Guide de l'administrateur de F-Secure Policy Manager.

F-Secure Policy Manager offre un mode évolutif de gestion de la sécurité de nombreuses applications sur différents systèmes d'exploitation, à partir d'un emplacement centralisé. Utilisez ce produit pour mettre à jour les logiciels de sécurité, gérer les configurations et gérer le personnel de l'entreprise même s'il est important et itinérant.

F-Secure Policy Manager peut être utilisé pour :

- 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.

1.3.1 Principaux composants de F-Secure Policy Manager

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

F-Secure 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 F-Secure Policy Manager Console, puis distribuées aux stations de travail

par F-Secure Policy Manager Server. Cette console permet d'installer les produits F-Secure à distance sur d'autres postes de travail sans aucune intervention de l'utilisateur final.

F-Secure Policy Manager Console inclut deux interfaces utilisateur :

- l'interface utilisateur en **mode-antivirus** optimisée pour l'administration de F-Secure Client Security et de F-Secure Anti-Virus pour stations de travail. Ce manuel décrit l'interface en mode antivirus.
- L'interface utilisateur en **mode avancé** qui peut être utilisée pour gérer d'autres produits F-Secure. L'interface utilisateur en mode avancé est décrite dans le Guide de l'administrateur de Policy Manager.

F-Secure 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 F-Secure Policy Manager Server et les hôtes administrés s'établit via le protocole standard HTTP, qui assure un fonctionnement optimal aussi bien sur les réseaux locaux (LAN) que sur les réseaux étendus (WAN).

F-Secure Policy Manager Web Reporting est un système de rapports graphiques d'entreprise basé sur le Web et inclus dans F-Secure 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. Pour plus d'informations, reportez-vous au Guide de l'administrateur de F-Secure Policy Manager.

F-Secure Policy Manager Reporting Option est un composant en option de F-Secure Policy Managerqui, avec un répertoire de communication existant (CommDir) dans F-Secure Policy Manager Server, collecte des données d'alertes, d'états et de propriétés à partir du domaine de sécurité administré ou du ou des hôtes sélectionnés. Pour plus d'informations, reportez-vous au Guide de l'administrateur de F-Secure Policy Manager Reporting Option.

Serveur et agent de mise à jour F-Secure Policy Manager sont utilisés pour la mise à jour des définitions de virus et logiciels espions sur les hôtes administrés. Agent de mise à jour automatique F-Secure permet aux utilisateurs de recevoir des mises à jour des bases de données de définitions de virus et d'autres informations sans interrompre leur travail pour attendre le téléchargement complet des fichiers depuis le Web. Il télécharge les fichiers automatiquement en tâche de fond en utilisant la bande passante non utilisée par les autres applications Internet.

F-Secure Management Agent applique 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.

L'**Assistant de certificat VPN+** est une application qui permet de créer des certificats pour F-Secure VPN+.

1.3.2 Fonctions de F-Secure Policy Manager

Distribution des logiciels

- Installation de 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.

Configuration et gestion par stratégies

- Configuration centralisée des stratégies de sécurité. Les stratégies sont distribuées à partir de F-Secure Policy Manager Server sur la station de travail de l'utilisateur. L'intégrité des stratégies est assurée par l'utilisation de signatures numériques.

Gestion des événements

- Rapports à l'Observateur d'événements (journaux locaux et distants), agent SNMP, 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.

1.4 Terminologie de base

Hôte

Dans ce document, ce terme se réfère à un ordinateur qui est géré de manière centralisée avec F-Secure 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.

Le flux d'informations entre F-Secure Policy Manager Console et les hôtes est assuré par le transfert de fichiers de stratégie.

Pour plus d'informations, reportez-vous au Guide de l'administrateur de F-Secure Policy Manager.

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 F-Secure 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.

2 INSTALLATION DE F-SECURE POLICY MANAGER

2.1 Présentation

Ce chapitre couvre les sujets suivants :

- La configuration requise de F-Secure Policy Manager Server et de F-Secure Policy Manager Console.
- Les instructions d'installation de F-Secure Policy Manager Console et Server sur le même ordinateur. L'installation de F-Secure Policy Manager Console et Server s'effectue à partir du CD F-Secure.

  Pour plus d'informations sur d'autres scénarios d'installation, ainsi que sur des problèmes de sécurité de serveur, reportez-vous aux chapitres *Installation de F-Secure Policy Manager Console* et *Installation de* F-Secure Policy Manager Server dans le Guide de l'administrateur de F-Secure Policy Manager.

Le programme d'installation de F-Secure Policy Manager installe également F-Secure Policy Manager Web Reporting, composant utilisé pour créer des rapports graphiques au format HTML sur l'état du domaine géré. Pour plus d'informations sur le composant Web Reporting, reportez-vous au chapitre « Web Reporting » dans le Guide de l'administrateur de F-Secure Policy Manager.

2.2 Configuration requise

2.2.1 F-Secure Policy Manager Server

Pour installer F-Secure Policy Manager Server, votre système doit être doté de la configuration minimale suivante :

Système d'exploitation :	Microsoft Windows 2000 Server (SP 3 ou version ultérieure) ; Windows 2000 Advanced Server (SP 3 ou version ultérieure) ; Windows Server 2003, Edition Standard ou Edition Web ; Windows 2003 Small Business Server.
Processeur :	Processeur Intel Pentium III 450 MHz ou plus rapide. La gestion de plus de 5 000 hôtes ou l'utilisation du composant Web Reporting requiert un processeur Intel Pentium III 1 GHz ou plus rapide.

Mémoire :	256 Mo de RAM. Lorsque le composant Web Reporting est activé, 512 Mo de RAM.
Espace disque :	Espace disque : 200 Mo d'espace disponible sur le disque dur (500 Mo ou plus 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 malaisé 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 exige un réseau 100 Mbits.

2.2.2 F-Secure Policy Manager Console

Pour installer F-Secure Policy Manager Console, votre système doit être doté de la configuration minimale suivante :

Système d'exploitation :	Microsoft Windows 2000 Professional (SP3 ou version ultérieure) ; Windows 2000 Server (SP3 ou version ultérieure) ; Windows 2000 Advanced Server (SP3 ou version ultérieure) Windows XP Professionnel (SP2 ou version ultérieure) ; Windows Server 2003, Edition Standard ou Edition Web ; Windows 2003 Small Business Server.
Processeur :	Processeur Intel Pentium III 450 MHz ou plus rapide. La gestion de plus de 5 000 hôtes exige un processeur Pentium III 750 MHz ou plus rapide.
Mémoire :	256 Mo de RAM. La gestion de plus de 5 000 hôtes exige 512 Mo de mémoire.
Espace disque :	100 Mo d'espace disponible sur le disque dur.
Affichage :	Ecran 256 couleurs minimum d'une résolution de 1 024 x 768 (recommandé : couleurs 32 bits et résolution de 1 280 x 960 ou supérieure).
Réseau :	Interface de réseau Ethernet ou l'équivalent. Il est conseillé d'utiliser un réseau à 10 Mbits entre la console et le serveur. La gestion de plus de 5 000 hôtes requiert une connexion 100 Mbits entre la console et le serveur.

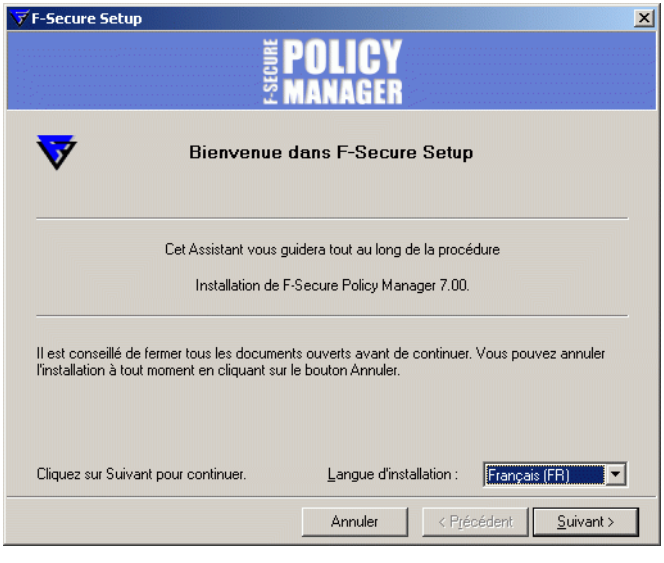
2.3 Procédure d'installation

Etape 1.

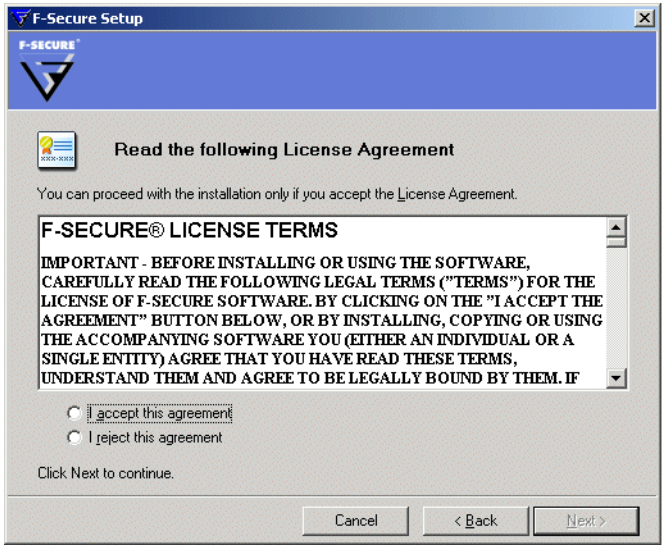
1. Introduisez le CD-ROM F-Secure dans le lecteur adéquat.
2. Sélectionnez *Professionnel*. Cliquez sur **Suivant** pour continuer.
3. Sélectionnez *F-Secure Policy Manager* dans le menu *Installation ou mise à jour du logiciel de gestion*.

Etape 2.

Prenez connaissance du contenu de l'écran d'accueil, puis suivez les instructions relatives à l'installation. Sélectionnez ensuite la langue d'installation dans le menu déroulant. Cliquez sur **Suivant** pour continuer.

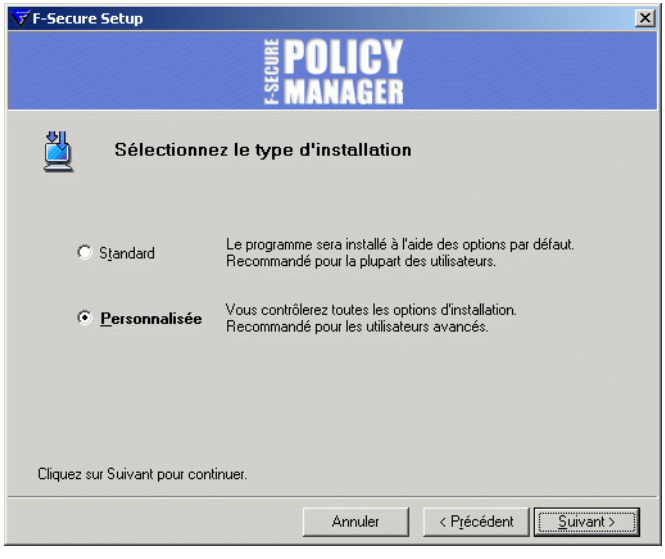


Etape 3. Prenez connaissance du contrat de licence. Si vous êtes d'accord, cliquez sur *J'accepte le contrat*. Cliquez sur **Suivant** pour continuer.



Etape 4. Sélectionnez le type d'installation :

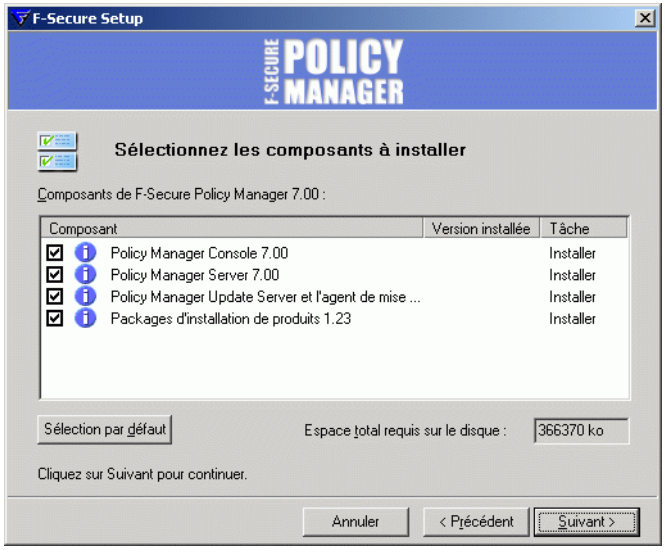
- *Traditionnel* - Le programme d'installation installe le produit avec les options par défaut :
  - F-Secure Policy Manager Server, F-Secure Policy Manager Console, le serveur et l'agent de mise à jour de F-Secure Policy Manager sont installés sur le même ordinateur.
  - Les ports par défaut sont utilisés pour les modules F-Secure Policy Manager Server.
  - Seul F-Secure Policy Manager Console installé sur le même ordinateur est autorisé à accéder F-Secure Policy Manager Server.
  - L'accès aux rapports Web est également autorisé depuis les autres ordinateurs.
- *Personnalisé* - C'est l'option par défaut (recommandée) qui vous permet de spécifier, par exemple, le répertoire d'installation et les ports pour les modules F-Secure Policy Manager Server. Certaines boîtes de dialogue d'installation ne s'affichent que lorsque Personnalisé est sélectionné.
- *Réinstaller* - Cette option réinstalle tous les composants existants et restaure les paramètres manquants. Cette boîte de dialogue s'affiche uniquement en présence d'une installation précédente de F-Secure Policy Manager sur l'ordinateur.


F-Secure Setup
F-SECURE POLICY MANAGER
Sélectionnez le type d'installation
Standard
Le programme sera installé à l'aide des options par défaut.
Recommandé pour la plupart des utilisateurs.
Personnalisée
Vous contrôlerez toutes les options d'installation.
Recommandé pour les utilisateurs avancés.
Cliquez sur Suivant pour continuer.
Annuler
< Précédent
Suivant >

Etape 5. Sélectionnez les composants suivants à installer :

- F-Secure Policy Manager Console
- F-Secure Policy Manager Server
- Serveur et agent de mise à jour de F-Secure Policy Manager
- Fichiers d'installation F-Secure

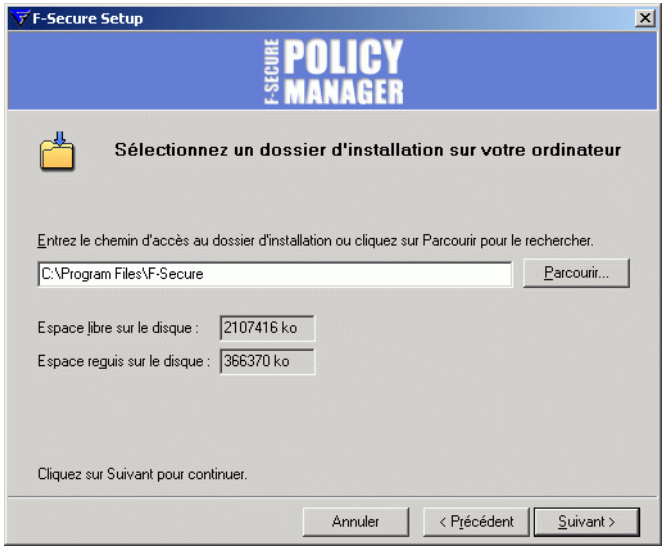
Cliquez sur **Suivant** pour continuer.



Etape 6. Choisissez le dossier de destination.

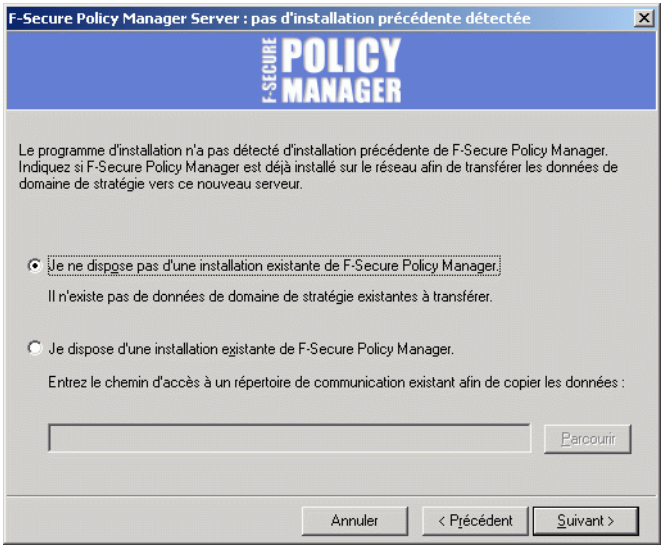
Nous vous recommandons d'utiliser le répertoire d'installation par défaut. Utilisez la fonction **Parcourir** pour installer F-Secure Policy Manager dans un autre répertoire.

Cliquez sur **Suivant** pour continuer.



Etape 7. Le programme d'installation demande confirmation en présence de l'installation précédente de F-Secure Policy Manager.

Cette boîte de dialogue s'affiche uniquement si l'installation n'a pas détecté une installation précédente de F-Secure Policy Manager Server sur l'ordinateur.



1. Si ***Oui***, sélectionnez *J'ai une installation existante de F-Secure Policy Manager*. Saisissez le chemin du répertoire de communication du programme F-Secure Policy Manager installé. Le contenu de ce répertoire est copié sous le *<répertoire d'installation du serveur>\ répertoire de communication (répertoire commdir\ sous le répertoire d'installation de* F-Secure Policy Manager Server *5)*, et ce répertoire sera utilisé par F-Secure Policy Manager Server comme référentiel. Vous pouvez utiliser le répertoire commdir précédent comme sauvegarde, où vous pouvez le supprimer une fois que vous avez vérifié que F-Secure Policy Manager Server 5 est correctement installé.
2. Si ***Non***, sélectionnez*Je n'ai pas d'installation existante de F-Secure Policy Manager*.

Cette option n'exige pas la présence d'un répertoire de communication antérieur. Un répertoire de communication vide sera créé à l'emplacement par défaut (dans le répertoire d'installation de *<F-Secure Policy Manager 5>\commdir*).

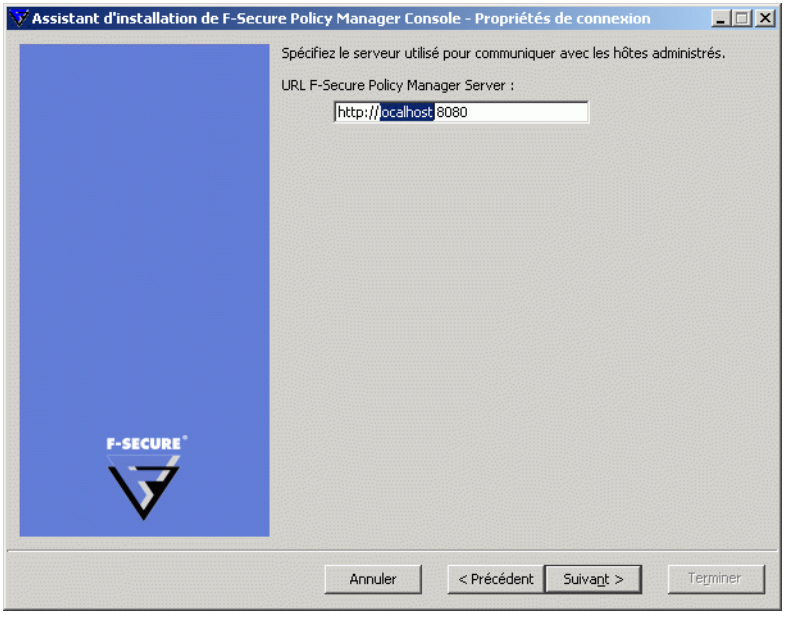
Cliquez sur **Suivant** pour continuer.

Etape 8.

Indiquez si vous souhaitez conserver les paramètres existants ou les modifier.

Cette boîte de dialogue s'affiche uniquement si une installation précédente de F-Secure 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 le fichier de configuration de F-Secure Policy Manager Server (*HTTPD.conf*). 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 le fichier *HTTPD.conf* et restaure les valeurs par défaut des paramètres.



Cliquez sur **Suivant** pour continuer.

Etape 9. Sélectionnez les modules de F-Secure 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 F-Secure Policy Manager Console. Le port HTTP par défaut est 8080.

> *Si vous voulez modifier le port de communication par défaut, vous devez également modifier le paramètre Numéro de port HTTP dans F-Secure Policy Manager Console.*

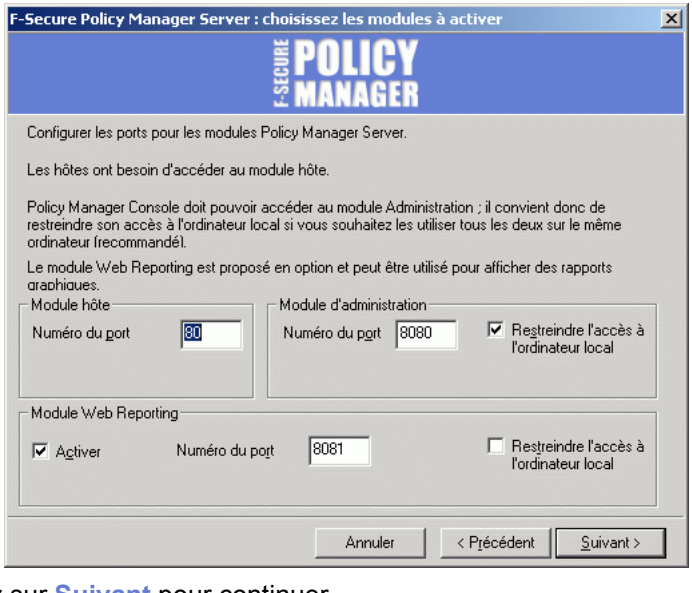
Par défaut, l'accès au module Administration est restreint à l'ordinateur local. C'est le mode d'utilisation du produit le plus sécurisé.

En cas de connexion via un réseau, il est conseillé d'envisager de sécuriser la communication à l'aide de F-Secure SSH ou de F-Secure VPN+.

Pour les environnements nécessitant une sécurité maximale, reportez-vous à la section *Installation de F-Secure Policy Manager dans des environnements à haute sécurité* dans le Guide de l'administrateur de *F-Secure Policy Manager*.

- Le module Web Reporting est utilisé pour la communication avec F-Secure Policy Manager Web Reporting. Indiquez si vous souhaitez l'activer. Web Reporting se connecte au module d'administration via un socket local pour rechercher les données du serveur. Le port par défaut est 8081.

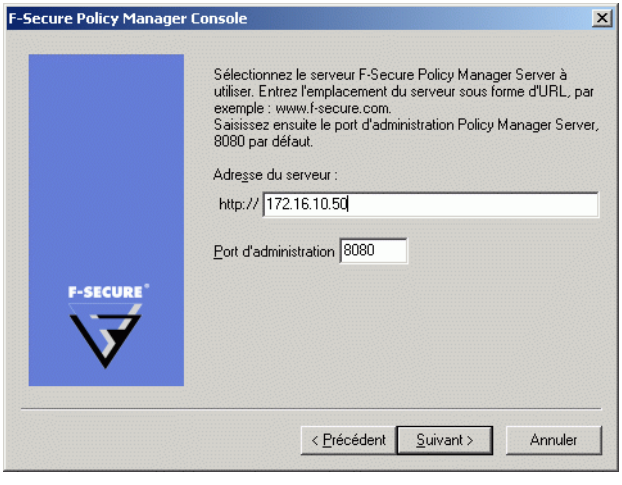
  Par défaut, l'accès aux rapports Web est également autorisé depuis les autres ordinateurs. Si vous souhaitez uniquement un accès depuis cet ordinateur, sélectionnez *Restreindre l'accès à l'ordinateur local*.



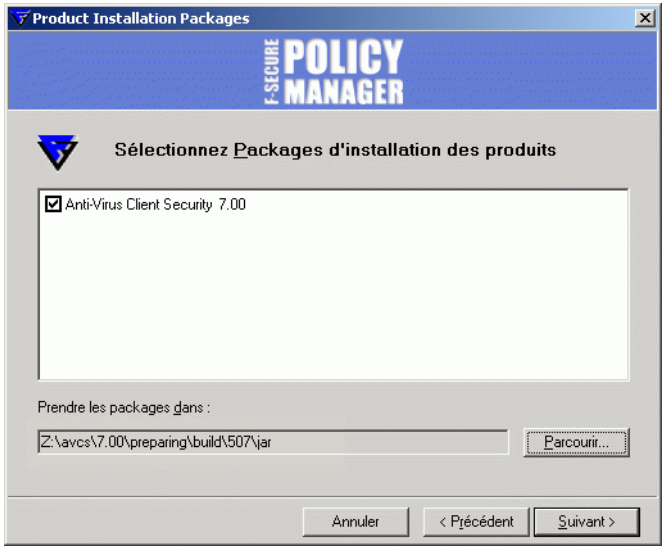
Cliquez sur **Suivant** pour continuer.

Etape 10. Spécifiez l'adresse de F-Secure Policy Manager Server, ainsi que le numéro du port d'administration. Cliquez sur **Suivant** pour continuer.

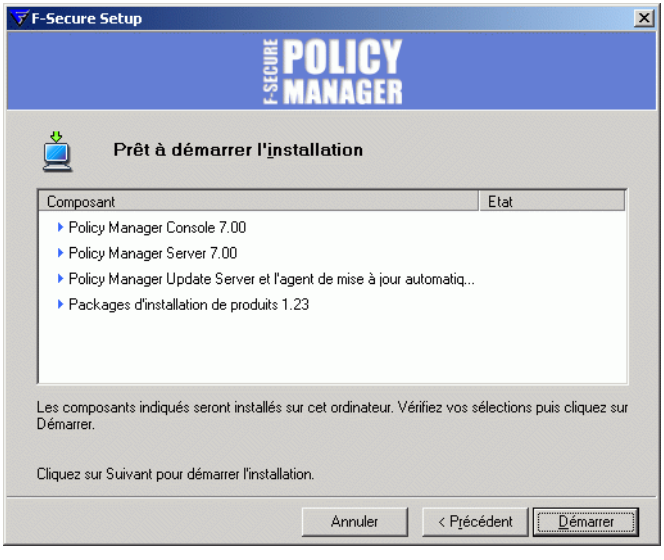
Selon la méthode d'installation choisie, cette fenêtre n'est pas toujours affichée.



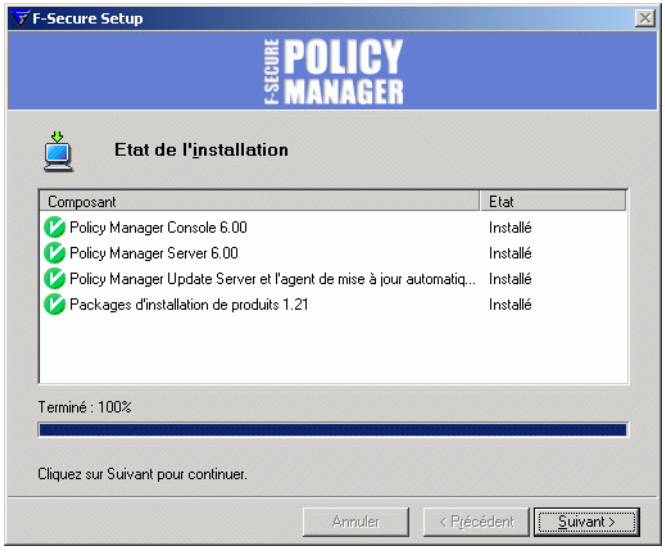
Etape 11. Sélectionnez le ou les packages d'installation de produits dans la liste des packages disponibles (si vous avez activé l'option Packages d'installation F-Secure à l'*Etape 5.* , 30). Cliquez sur **Suivant**.



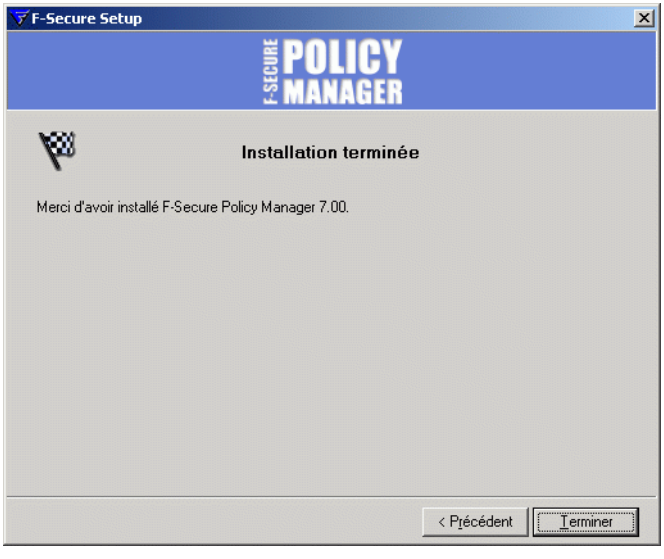
Etape 12. Examinez les modifications que le programme d'installation va apporter. Cliquez sur **Démarrer** pour lancer le service.



Etape 13. Lorsque le programme d'installation est terminé, il affiche tous les composants dont l'installation a abouti.



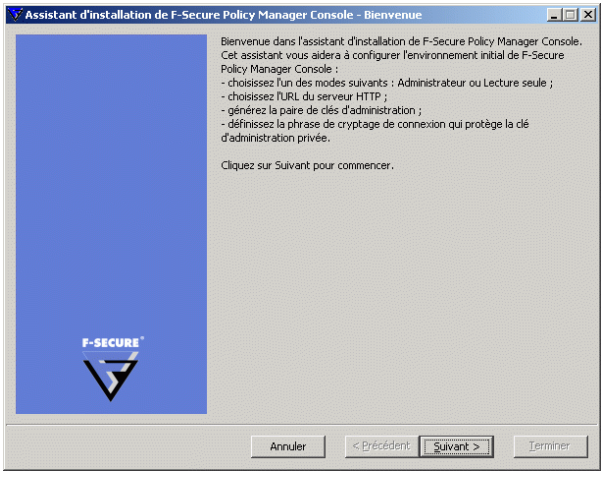
Etape 14. Cliquez sur **Terminer** pour terminer l'installation de F-Secure Policy Manager Server. Vous devez ensuite exécuter F-Secure Policy Manager Console pour la première fois.



Etape 15. Il est important d'exécuter F-Secure Policy Manager Console après l'installation, certaines propriétés de connexion étant collectées lors de son démarrage initial.

Le raccourci se trouve sous *Démarrer→Programmes→F-Secure Policy Manager Console→F-Secure Policy Manager Console*. Lorsque l'application F-Secure 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.

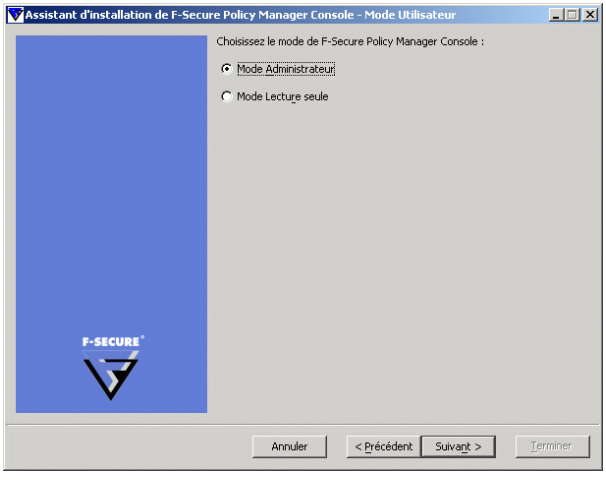
La première page de l'Assistant d'installation de F-Secure Policy Manager Console résume le processus d'installation. Cliquez sur **Suivant** pour continuer.



Etape 16. 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*. Si ces clés n'existent pas, elles seront créées plus tard dans le processus d'installation.

Cliquez sur **Suivant** pour continuer.

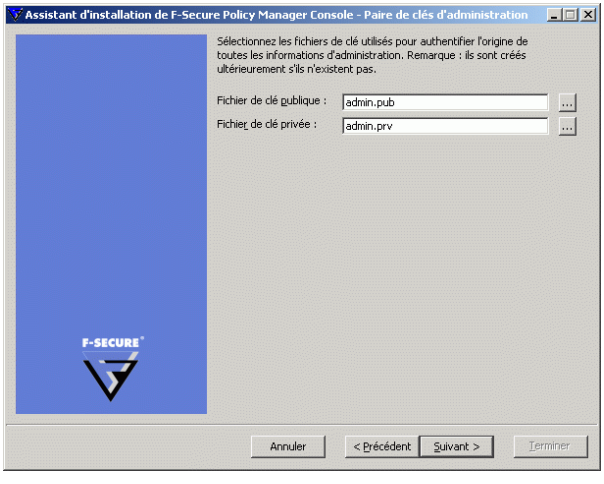


Etape 17. Entrez le chemin d'accès au répertoire où vous souhaitez stocker les fichiers de clé privée et de clé publique de l'administrateur. Par défaut, les fichiers de clé sont enregistrés dans le répertoire d'installation de F-Secure Policy Manager Console.

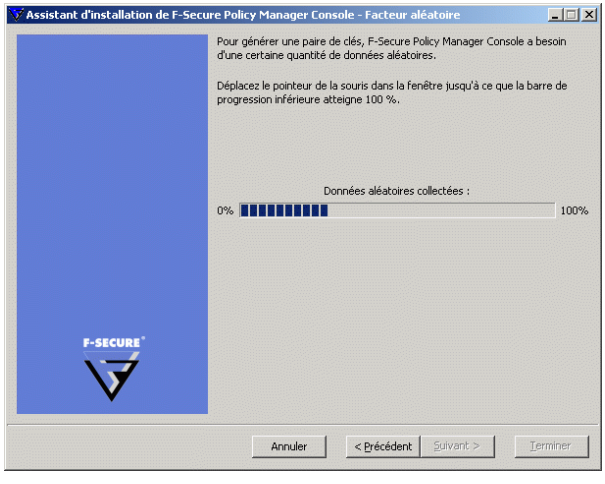
Program Files\F-Secure\Administrator.

Cliquez sur **Suivant** pour continuer.

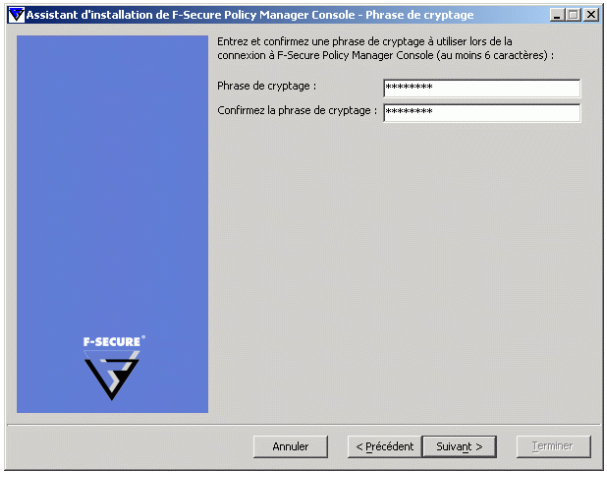
Si la paire de clés n'existe pas encore, elle sera créée plus tard dans le processus de configuration.



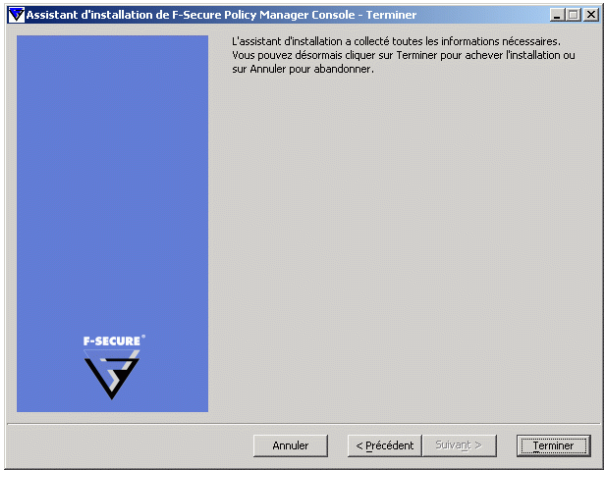
Etape 18. Déplacez votre curseur dans la fenêtre afin d'initialiser le facteur aléatoire utilisé par le générateur du jeu de clés d'administration. L'utilisation des déplacements de la souris assure que le facteur de l'algorithme de génération de jeu de clés est suffisamment aléatoire. Lorsque l'indicateur d'avancement atteint 100 %, la boîte de dialogue *Phrase de cryptage* s'affiche automatiquement.



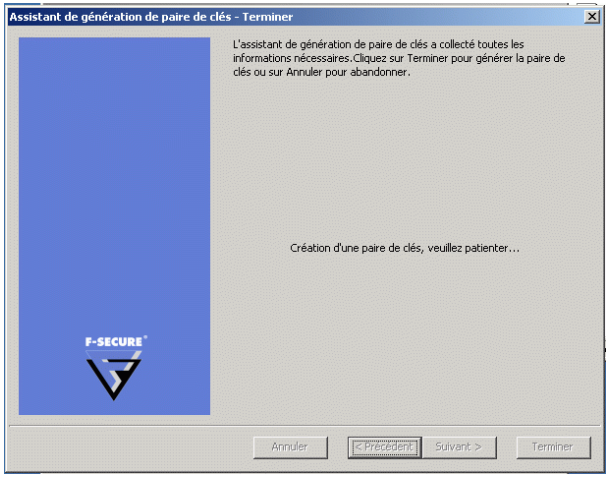
Etape 19. Entrez une phrase de cryptage qui protège votre clé privée d'administration. Confirmez cette phrase dans la zone *Confirmer la phrase de cryptage*. Cliquez sur **Suivant**..



Etape 20. Cliquez sur **Terminer** pour terminer le processus de configuration.

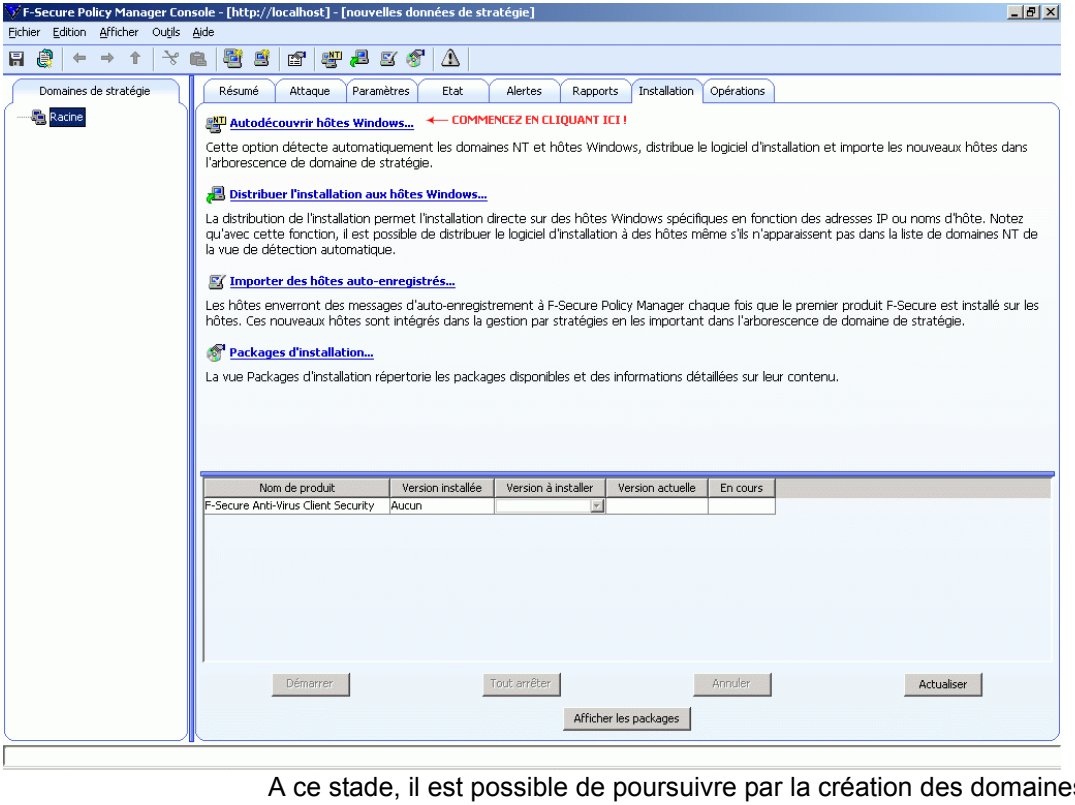


F-Secure Policy Manager Console génère la paire de clés de gestion.



Pour plus d'informations sur la sauvegarde de la clé admin.pub, reportez-vous au chapitre Maintenance de F-Secure Policy Manager Server *dans le Guide de l'administrateur de F-Secure Policy Manager.*

Etape 21. Après la génération de la paire de clés, F-Secure Policy Manager Console démarre.



A ce stade, il est possible de poursuivre par la création des domaines de stratégie et l'installation des hôtes. Pour plus d'informations, reportez-vous aux sections “*Création de la structure du domaine*”, *127* et “*Ajout d'hôtes*”, *129*.

Si vous décidez de quitter F-Secure Policy Manager Console, puis souhaitez vous reconnecter ultérieurement, reportez-vous à la section “*Première connexion*”, *123*.

Si vous souhaitez vous familiariser avec l'interface utilisateur de F-Secure Policy Manager Console, reportez-vous à la section “*Introduction à l'interface utilisateur du mode antivirus de F-Secure Policy Manager*”, *49*.

Modification du chemin d'accès au navigateur Web

F-Secure Policy Manager Console obtient le chemin d'accès au navigateur Web par défaut pendant l'installation. Si vous voulez modifier ce chemin d'accès, ouvrez le menu *Outils* et choisissez l'option *Préférences*.

Cliquez sur l'onglet *Emplacements* et entrez le nouveau chemin d'accès au fichier.

2.4 Désinstallation F-Secure Policy Manager

Pour désinstaller F-Secure Policy Manager Console et Server (ou d'autres composants de F-Secure Policy Manager), procédez comme suit :

1. Cliquez sur le menu *Démarrer* de Windows et accédez au *Panneau de configuration*. Cliquez sur *Ajout/Suppression de programmes*.
2. Choisissez le composant à désinstaller (F-Secure Policy Manager Console ou Server), puis cliquez sur le bouton **Ajouter/Supprimer**.
3. La boîte de dialogue *Désinstallation de F-Secure* s'affiche. Cliquez sur **Démarrer** pour démarrer la désinstallation.
4. Au terme de la désinstallation, cliquez sur **Fermer**.
5. Recommencez les étapes 2 à 4, si vous souhaitez désinstaller d'autres composants de F-Secure Policy Manager.
6. Une fois que vous avez désinstallé les composants, quittez *Ajout/Suppression de programmes*.
7. Il est recommandé de réamorcer l'ordinateur après la désinstallation. Le redémarrage est nécessaire pour nettoyer les fichiers restant sur l'ordinateur après la désinstallation et avant les installations subséquentes des mêmes produits F-Secure.

3 Introduction à l'interface utilisateur du mode antivirus de F-Secure Policy Manager

3.1 Présentation

Cette section présente l'interface utilisateur du Mode antivirus de F-Secure Policy Manager. Elle décrit également certaines fonctions génériques et certains éléments visuels utilisés dans l'interface utilisateur pour indiquer comment fonctionne la transmission des paramètres par héritage.

F-Secure Policy Manager inclut également une autre interface utilisateur, l'interface utilisateur en mode avancé. Elle permet de gérer des produits autres que F-Secure Client Security et F-Secure Anti-Virus 5.40. Elle est également utilisée lorsque vous devez modifier les paramètres avancés de F-Secure Client Security. Vous pouvez basculer entre les deux modes en sélectionnant Mode avancé ou Mode antivirus dans le menu Affichage. Pour plus d'informations sur l'interface utilisateur en mode avancé, reportez-vous au Guide de l'administrateur de F-Secure Policy Manager.

Les principaux composants de l'interface utilisateur en mode antivirus de F-Secure Policy Manager sont les suivants :

- L'onglet *Domaines de stratégie*, qui affiche la structure des domaines de stratégie gérés.
- Les onglets de gestion : *Résumé*, *Attaque* , *Paramètres* , *Etat*, *Alertes*, *Rapports*, *Installation* et *Opérations* qui peuvent être utilisés pour configurer et surveiller F-Secure Client Security installé sur les hôtes ainsi que pour effectuer des opérations.
- *Affichage des messages*, 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.

3.2 Onglet Domaines de stratégie

Dans l'onglet *Domaines de stratégie*, vous pouvez effectuer les opérations suivantes :

- Ajouter un nouveau domaine de stratégie en cliquant sur l'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 un domaine ou un hôte sélectionné, vous pouvez accéder à ces options dans 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*.

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.

3.3 Onglets de gestion

Cette section décrit les onglets de gestion (*Résumé*, *Attaque*, *Paramètres*, *Etat*, *Alertes*, *Rapports*, *Installation* et *Opérations*), ainsi que les différentes pages de chacun de ces onglets.

3.3.1 Onglet Résumé

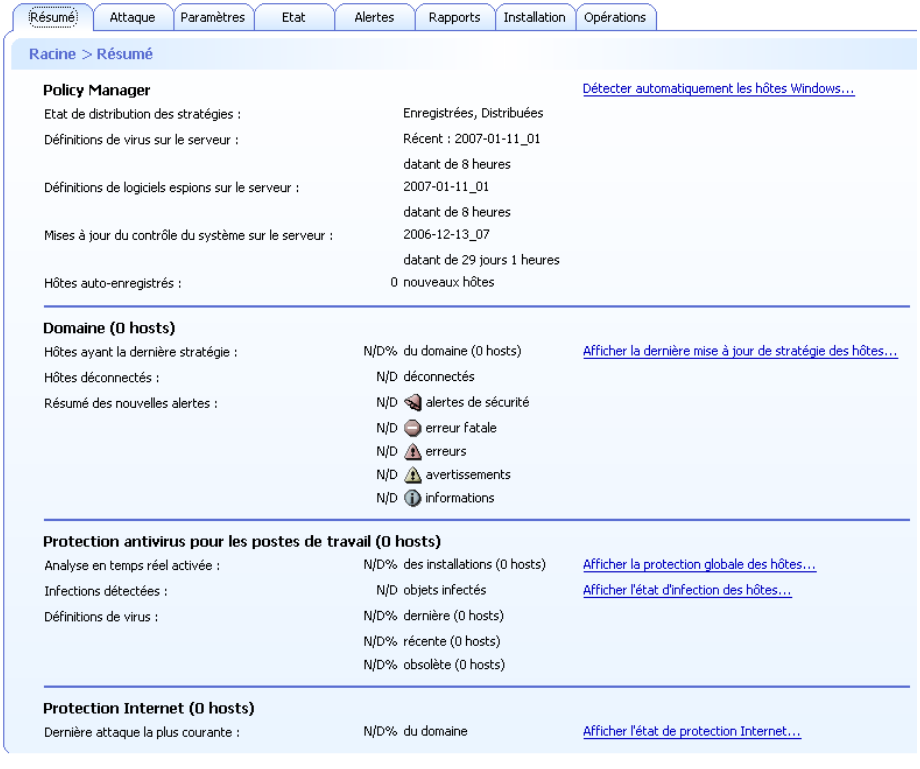


Figure 3-1 Onglet Résumé

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

Pour plus d'informations sur l'utilisation de l'onglet *Résumé* pour vérifier rapidement la protection du domaine, reportez-vous à la section “*Comment vérifier que l'environnement est protégé*”, *231*.

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 les postes de travail,* et *Protection Internet.*
- Lorsqu'un hôte est sélectionné, les sections sont : *Policy Manager*, *Hôte*, *Protection antivirus* et *Protection Internet*.

Ces sections sont décrites en détail ci-dessous.

Onglet Résumé lorsqu'un domaine est sélectionné

Lorsqu'un domaine est sélectionné dans l'onglet *Domaines de stratégie*, les informations suivantes s'affichent dans l'onglet *Résumé* :

Policy Manager

Figure 3-2 Informations associées à Policy Manager sur l'onglet Résumé

Dans la section *Policy Manager*, vous pouvez :

- Voir l'état actuel de distribution des stratégies sous *Etat de la distribution des stratégies* (*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 du contrôle du système 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

Figure 3-3 Informations associées aux domaines sur l'onglet Résumé

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 dernière mise à jour de stratégie 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 :

	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

Figure 3-4 Informations associées à la protection antivirus sur l'onglet Résumé

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 l'analyse en temps réel est activée. 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.

Si F-Secure Anti-Virus 5.40 est installé sur certains hôtes, la version des définitions de virus de ces hôtes est marquée « unknown » (inconnue).

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

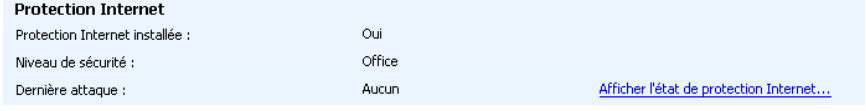


Figure 3-5 Informations associées à la protection Internet sur l'onglet Résumé

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 quel pourcentage du domaine a été 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

Figure 3-6 Informations associées aux hôtes sur l'onglet Résumé

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 d'hôte* s'affichent.
- 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 décrites dans la section "*Protection antivirus pour postes de travail*", *56*, la section *Protection antivirus pour postes de travail* affiche également le numéro de version des définitions de virus.

Protection Internet

Outre les informations décrites sous "*Protection Internet*", *57*, la section *Protection Internet* affiche également le niveau de sécurité de la protection Internet actuellement sélectionné sur l'hôte.

3.3.2 Onglet Attaque

La section Informations de sécurité affiche des informations sur la sécurité de F-Secure. Les informations de sécurité concernent généralement l'apparition de nouveaux virus, et elles indiquent la version des définitions de virus requise sur les hôtes pour assurer une protection efficace contre ce nouveau virus. Il peut également s'agir d'informations plus génériques concernant diverses menaces à la sécurité.

La section Informations de sécurité indique combien de vos hôtes sont protégés, et précise si la protection est disponible sur Policy Manager Server. Si la protection n'est actuellement pas disponible, Policy Manager Server la télécharge automatiquement à partir de F-Secure dès qu'il est disponible.

Les informations de sécurité indiquent le niveau d'alerte de la menace à la sécurité :

Niveau	Description
1	Alerte du niveau le plus élevé. Épidémie mondiale d'un nouveau virus dangereux.
2	Nouveau virus provoquant d'importantes infections. Pourrait être local, associé à une région spécifique.
3	Nouvelle technique ou nouvelle plate-forme de virus trouvée. Pas nécessairement susceptible d'être rencontrée
[pas de numéro]	Il n'y a actuellement pas d'alerte pour ce virus.

La section *Dernières informations détaillées sur la sécurité*, présente des informations détaillées sur les virus sélectionnés. Vous pouvez même obtenir plus de détails avec votre navigateur Web en cliquant sur le lien proposé.

Le tableau dans la section *Dernières informations détaillées sur la sécurité* répertorie tous les hôtes dans le domaine actuellement sélectionné. Pour chaque hôte, les informations suivantes sont fournies :

- La colonne *Protégé* indique si l'hôte est protégé contre le virus auquel il est fait référence dans les informations actuellement sélectionnées.
- La colonne *Déconnecté* indique si l'hôte est actuellement connecté ou déconnecté.
- Les zones *Version des définitions de virus*, *Définitions de virus mises à jour* et *Dernière connexion au serveur* présentent d'autres informations relatives aux mises à jour automatiques.
- *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 F-Secure Policy Manager.

Notez que certaines colonnes peuvent être masquées. Pour afficher des colonnes masquées, cliquez avec le bouton droit sur un en-tête de colonne.

Si un hôte est déconnecté, il est probablement hors tension. Si de tels les hôtes sont affichés comme étant non protégés, vous pouvez probablement ne pas en tenir compte puisqu'ils mettront automatiquement à jour les définitions de virus et de logiciels espions dès leur remise sous tension.

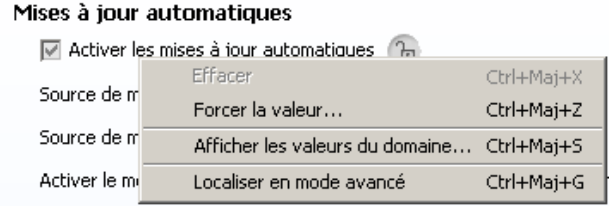
Delta de mise à jour indique l'état de fonctionnement des mises à jour automatiques de l'hôte lorsque ce dernier a envoyé des statistiques à F-Secure Policy Manager Server pour la dernière fois. Si vous avez un hôte affiché comme étant non protégé, mais affiche une faible valeur dans la colonne Delta de mise à jour, l'hôte est probablement ok et peut être ignoré.

3.3.3 Onglet Paramètres

L'onglet Paramètres contient 12 pages servant à configurer les composants de F-Secure Client Security. Elles sont décrites brièvement ci-dessous. Vous trouverez plus de détails sur les valeurs que vous pouvez sélectionner sur chaque page ainsi que des exemples pratiques de configuration aux sections "*Configuration de la protection contre les virus et les logiciels espions*", *159* et "*Configuration de la protection Internet*", *199*.

Pour plus d'informations sur les symboles de verrouillage et autres éléments affichés sur toutes les pages *Paramètres*, voir "*Transmission des paramètres par héritage*", *116*.

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	L'option *Forcer la valeur* n'est disponible que si un domaine de stratégie est sélectionné. Vous pouvez forcer le paramètre du domaine actuel à être également actif dans tous les sous-domaines et sur tous les 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

L'option *Afficher les valeurs du domaine* n'est disponible que si un domaine de stratégie est sélectionné. Elle permet d'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 valeurs 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

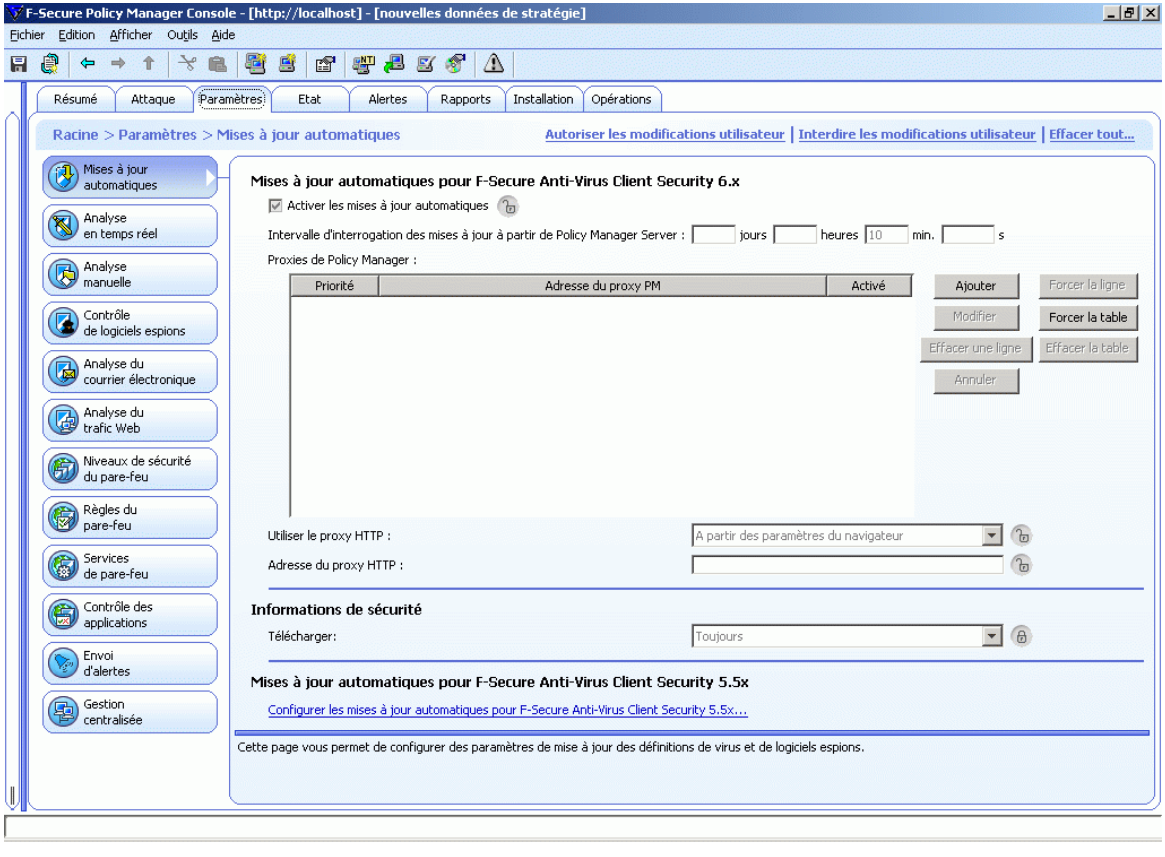


Figure 3-7 Paramètres > Onglet Mises à jour automatiques

Mises à jour automatiques pour F-Secure Client Security 6.x et ultérieur

Dans la section *Mises à jour automatiques pour F-Secure Client Security 6.x et ultérieur* 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 F-Secure Policy Manager Server.
- Voir une liste de serveurs proxy Policy Manager. 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.

Pour des exemples de configuration et plus d'informations, reportez-vous à la section “*Configuration des mises à jour automatiques*”, *162*.

Mises à jour automatiques pour F-Secure Client Security 5.5x

Si vous cliquez sur le lien **Configurer les mises à jour automatiques pour F-Secure Client Security 5.5x**, une page s'ouvre et affiche les paramètres de mises à jour automatiques pour les hôtes exécutant F-Secure Client Security 5.x.

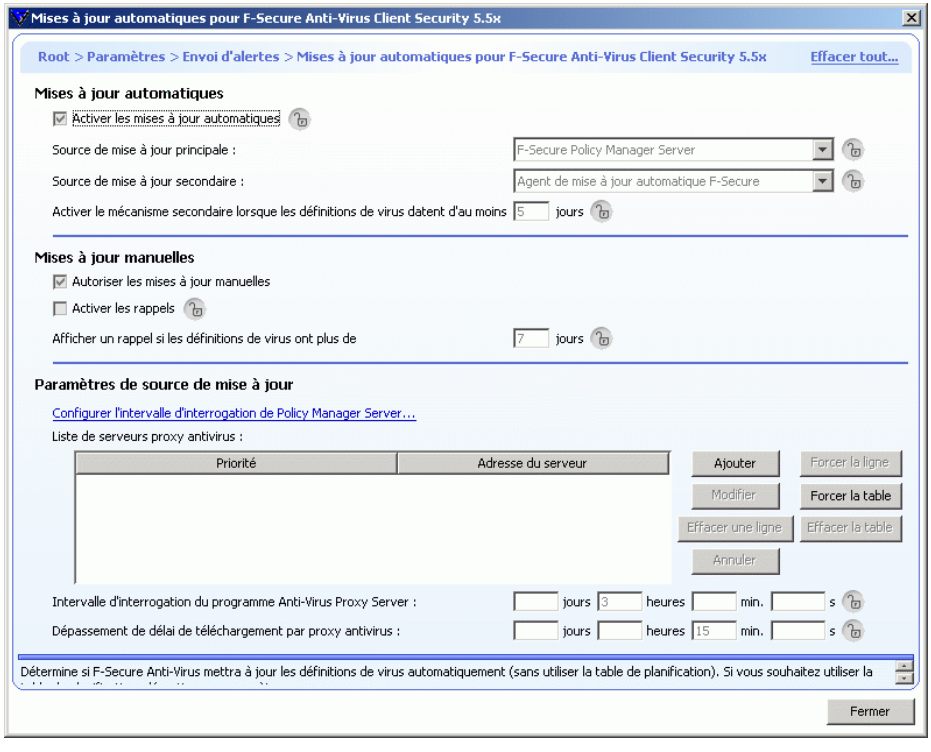


*Figure 3-8 Page Paramètres > Mises à jour automatiques > Mises à jour automatiques F-Secure Client Security 5.*x

Mises à jour automatiques

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

- Activer ou désactiver les mises à jour automatiques.
- Sélectionner les sources de mise à jour principale et secondaire à utiliser.
- Définir le nombre de jours après lesquels l'utilisation de la source de mise à jour secondaire est activée.

Mises à jour manuelles

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

- Choisir d'autoriser ou non les mises à jour manuelles.
- Indiquer si un rappel est affiché sur l'écran des utilisateurs lorsque leurs définitions de virus deviennent vieilles et déterminer à partir de quel âge les définitions de virus déclenchent ces rappels.

Paramètres de source de mise à jour

Dans la section *Paramètres de source de mise à jour*, vous pouvez :

- Cliquer sur **Configurer l'intervalle d'interrogation de Policy Manager Server** pour accéder à la page *Gestion centralisée*, où vous pouvez configurer l'intervalle d'interrogation.
- Voir une liste des serveurs de proxy antivirus. Vous pouvez également ajouter de nouveaux serveurs à la liste, supprimer des serveurs de la liste et modifier leurs adresses et priorités.
- Voir l'intervalle d'interrogation du serveur proxy antivirus actuellement défini. La valeur par défaut (3 heures) convient pour la plupart des environnements.
- Voir le délai de téléchargement par proxy antivirus actuellement défini. La valeur par défaut (15 minutes) convient pour la plupart des environnements.
- Pour voir des exemples de configuration et d'autres informations, reportez-vous à la section *Configuration des mises à jour de définition de virus* dans le Guide de l'administrateur de *F-Secure Client Security 5.60*.

Analyse en temps réel

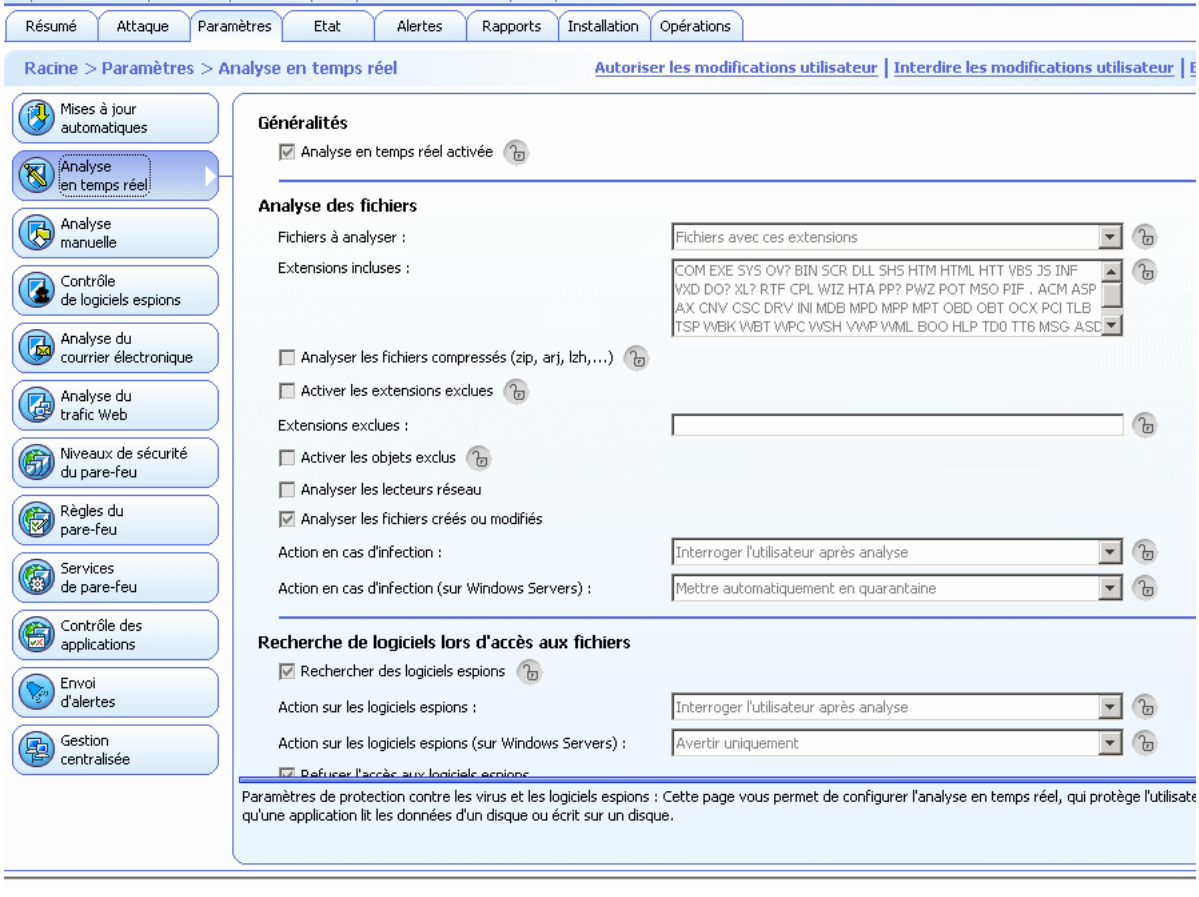


Figure 3-9 Page Paramètres > Analyse en temps réel

Généralités

Dans la section *Généralités*, vous pouvez activer ou désactiver l'analyse en temps réel.

Analyse des fichiers

Dans la section *Fichiers à analyser*, vous pouvez :

- Sélectionner quels fichiers seront analysés et définir les extensions incluses.
- Sélectionner si l'analyse en temps réel est exécutée également à l'intérieur des fichiers compressés.
- 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.
- Sélectionner si les fichiers sont analysés lorsqu'ils sont créés ou modifiés.
- Définir l'action à effectuer lorsqu'un fichier infecté est détecté.

Pour des exemples de configuration, une explication des options *Action en cas d'infection* et d'autres informations, reportez-vous à la section “*Configuration de l'analyse en temps réel*”, *166*

Recherche de logiciels espions lors d'accès aux fichiers

Dans la section *Recherche de logiciels espions lors d'accès aux fichiers*, vous pouvez :

- Activer ou désactiver l'analyse en temps réel pour logiciels espions.
- Sélectionner l'action à effectuer en cas de découverte d'un logiciel espion.
- Refuser ou autoriser l'accès à un logiciel espion.
- Sélectionner si les alertes de détection de logiciels espions sont présentées aux utilisateurs.
- Accéder à d'autres options de recherche de logiciels espions en cliquant sur le lien **Configurer d'autres options de recherche de logiciels espions en mode avancé**.

Pour des exemples de configuration, une explication des options *Action sur les logiciels espions* et d'autres informations, reportez-vous à la section “*Configuration de la recherche de logiciels espions*”*, 183*

Contrôle du système

Dans la section Contrôle du système, vous pouvez :

- Activer ou désactiver le contrôle du système.
- Sélectionner l’action à effectuer lorsqu’une tentative de modification du système est détectée.
- Sélectionner si ActiveX est interdit d’exécution sur les hôtes administrés.

Pour un exemple de configuration, une explication des options *Action sur les tentatives de modification du système* et d'autres informations, reportez-vous à la section “*Configuration du contrôle du système*”*, 172*

Analyse du secteur d'amorçage

Dans la section *Analyse du secteur d'amorçage*, vous pouvez :

- Activer ou désactiver l'analyse en temps réel pour les secteurs d'amorçage des disquettes.
- Sélectionner si les secteurs d'amorçage sont analysés au démarrage.
- Sélectionner l'action à effectuer lorsqu'une infection est détectée.

Dans la liste déroulante *Action en cas d'infection*, vous pouvez sélectionner l'action que devra exécuter F-Secure Client Security lors de la détection d'un secteur d’amorçage infecté.

Sélectionnez l'une des actions suivantes :

Action	Définition
Interroger l'utilisateur après analyse	Démarre l'Assistant de nettoyage F-Secure lorsqu'un secteur d'amorçage infecté est détecté sur une disquette.
Nettoyer automatiquement	Nettoie automatiquement le secteur d'amorçage lorsqu'un virus est détecté.
Avertir uniquement	Indique qu'un virus a été détecté et vous empêche d'accéder à l'objet infecté. Cette option se contente de vous signaler la présence du virus. Elle n'entreprend aucune action à son encontre.

Analyse manuelle

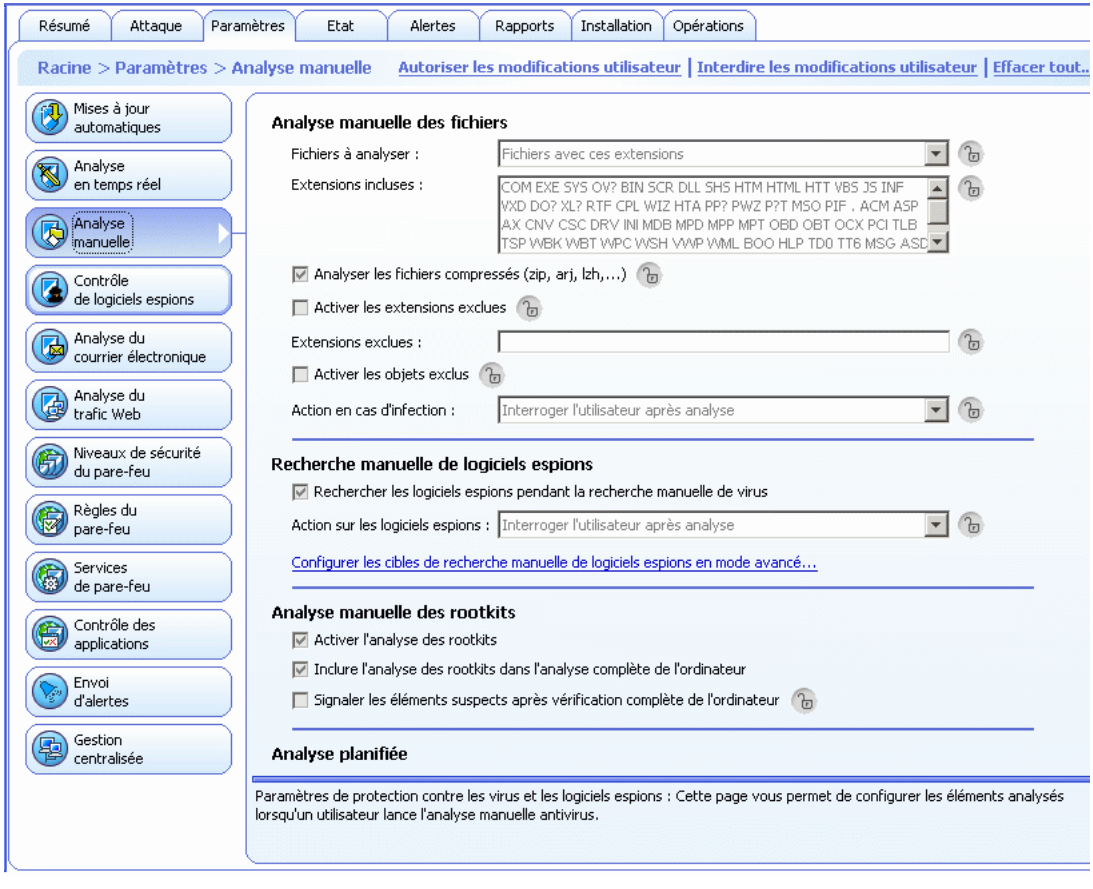


Figure 3-10 Paramètres > Analyse manuelle

Analyse manuelle de fichiers

La section *Analyse manuelle des fichiers* offre les options suivantes pour la sélection des éléments à analyser :

- *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.

- *Analyser les fichiers compressés*

  Cochez cette case pour analyser les fichiers compressés, tels que les fichiers 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.

- *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*. (Voir aussi “*Traitement des extensions de fichiers*”, *169*.)

- *Activer les objets exclus*

  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 F-Secure Client Security lors de la détection d'un fichier infecté.

Sélectionnez l'une des actions suivantes :

Action	Définition
Interroger l'utilisateur après analyse	Lance l'Assistant de nettoyage F-Secure 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 l'objet infecté par le virus. Cette option est donc déconseillée.
Avertir 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.

Recherche manuelle de logiciels espions

Dans la section *Recherche manuelle de logiciels espions*, vous pouvez :

- Activer ou désactiver la recherche manuelle de logiciels espions pendant une analyse antivirus.
- Sélectionner l'action à effectuer en cas de découverte d'un logiciel espion.
- Accéder aux paramètres de cibles de recherche manuelle de logiciels espions en cliquant sur le lien **Configurer les cibles de recherche manuelle de logiciels espions en mode avancé**.

Pour des exemples de configuration, une explication des options Action sur les logiciels espions et d'autres informations, reportez-vous à la section "*Configuration de la recherche de logiciels espions*", *183*

Analyse des rootkits

Dans la section *Analyse des rootkits*, vous pouvez :

- Activer ou désactiver l'analyse des 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.

Pour des exemples de configuration et plus d'informations, reportez-vous à la section "*Configuration de la recherche de rootkits*"*, 173*.

Analyse planifiée

Le lien **Configurer la recherche planifiée en mode avancé** donne accès à l'interface utilisateur en mode avancé de F-Secure Policy Manager Console, où la recherche planifiée peut être configurée. Pour plus d'informations, reportez-vous à la section "*Configuration d'une analyse planifiée*"*, 274*.

Analyse manuelle du secteur d'amorçage

Dans la section *Analyse manuelle du secteur d'amorçage*, 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

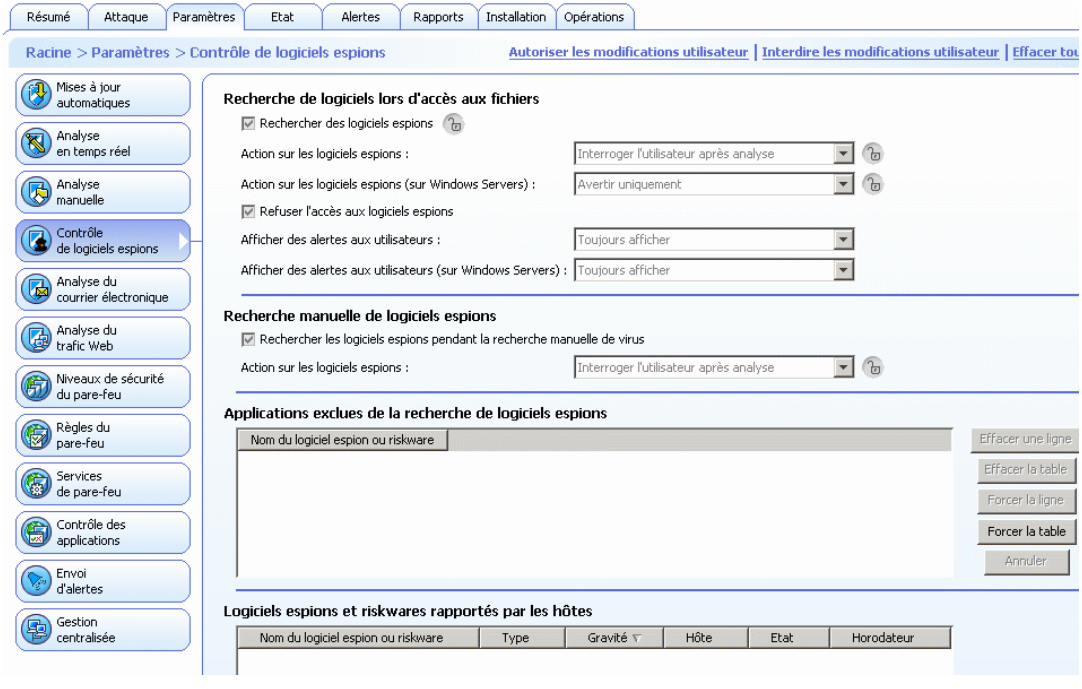


Figure 3-11 Paramètres > Contrôle des logiciels espions

Recherche de logiciels espions lors d'accès aux fichiers

Cette section contient les mêmes paramètres de recherche de logiciels espions que la section *Recherche de logiciels lors d'accès aux fichiers* dans la page *Paramètres > Analyse en temps réel*. Pour plus d'informations, reportez-vous à la section "*Recherche de logiciels espions lors d'accès aux fichiers*", *69*.

Recherche manuelle de logiciels espions

Cette section contient les mêmes paramètres de recherche de logiciels espions que la section *Recherche manuelle de logiciels espions* de la page *Paramètres > Recherche manuelle*. Pour plus d'informations, reportez-vous à la section "*Recherche manuelle de logiciels espions*", *74*.

Applications exclues de la recherche manuelle

La table *Applications exclues de la recherche de logiciels espions* affiche la liste des logiciels espions et des riskwares dont les administrateurs ont autorisé l'exécution sur les hôtes.

Logiciels espions et riskwares rapportés par les hôtes

La table *Logiciel espion et riskware signalés par les hôtes* 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 (le *score TAC*, reportez-vous au Glossaire) 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.

Le paramètre **Modifier la recherche de logiciels espions pour mettre automatiquement en quarantaine tous les nouveaux logiciels espions** modifie les paramètres de recherche de logiciels espions en temps réel et manuelle de façon que tous les logiciels espions qui ne sont pas explicitement autorisés par l'administrateur sont interdits d'exécution.

Pour plus d'informations sur la recherche de logiciels espions et pour des exemples de configuration, reportez-vous à la section “*Configuration de la recherche de logiciels espions*”, *183*.

Analyse du courrier électronique

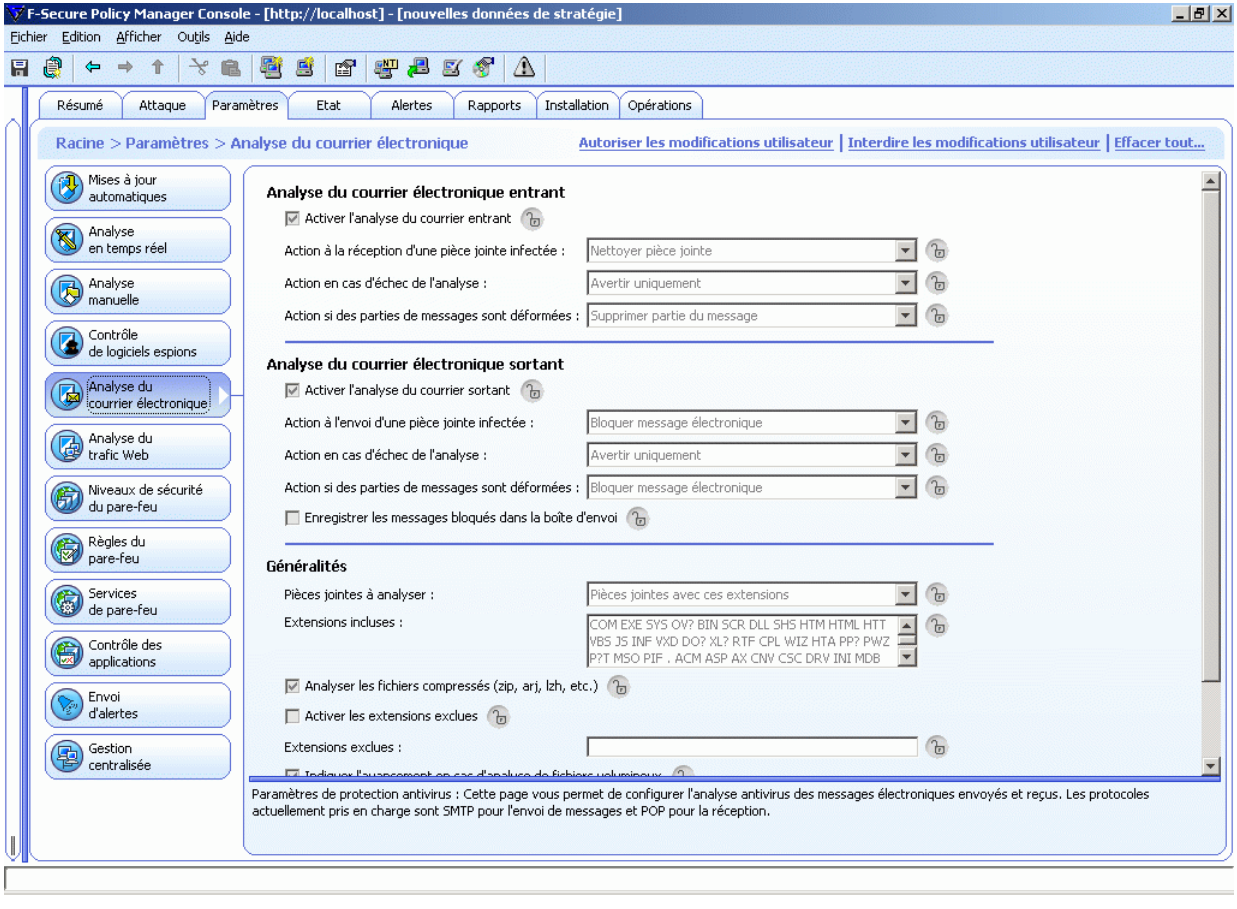


Figure 3-12 Page Paramètres > Analyse du courrier électronique

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 la section *Analyse du courrier électronique entrant*, vous pouvez :

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

Analyse du courrier électronique sortant

Dans la section *Analyse du courrier électronique sortant*, vous pouvez :

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

Généralités

Dans la section *Généralités*, vous pouvez :

- Sélectionner si toutes les pièces jointes sont analysées ou seulement certaines. Vous pouvez également ajouter de nouvelles extensions à la liste *Extensions incluses*.
- Sélectionner si l'analyse du courrier électronique porte également sur les pièces jointes compressées.
- Sélectionner si certaines extensions seront exclues de l'analyse et définir lesquelles.
- 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.

Pour des exemples de configuration et plus d'informations, reportez-vous à la section “*Configuration de l'analyse du courrier électronique*”, *175*.

Analyse du trafic Web

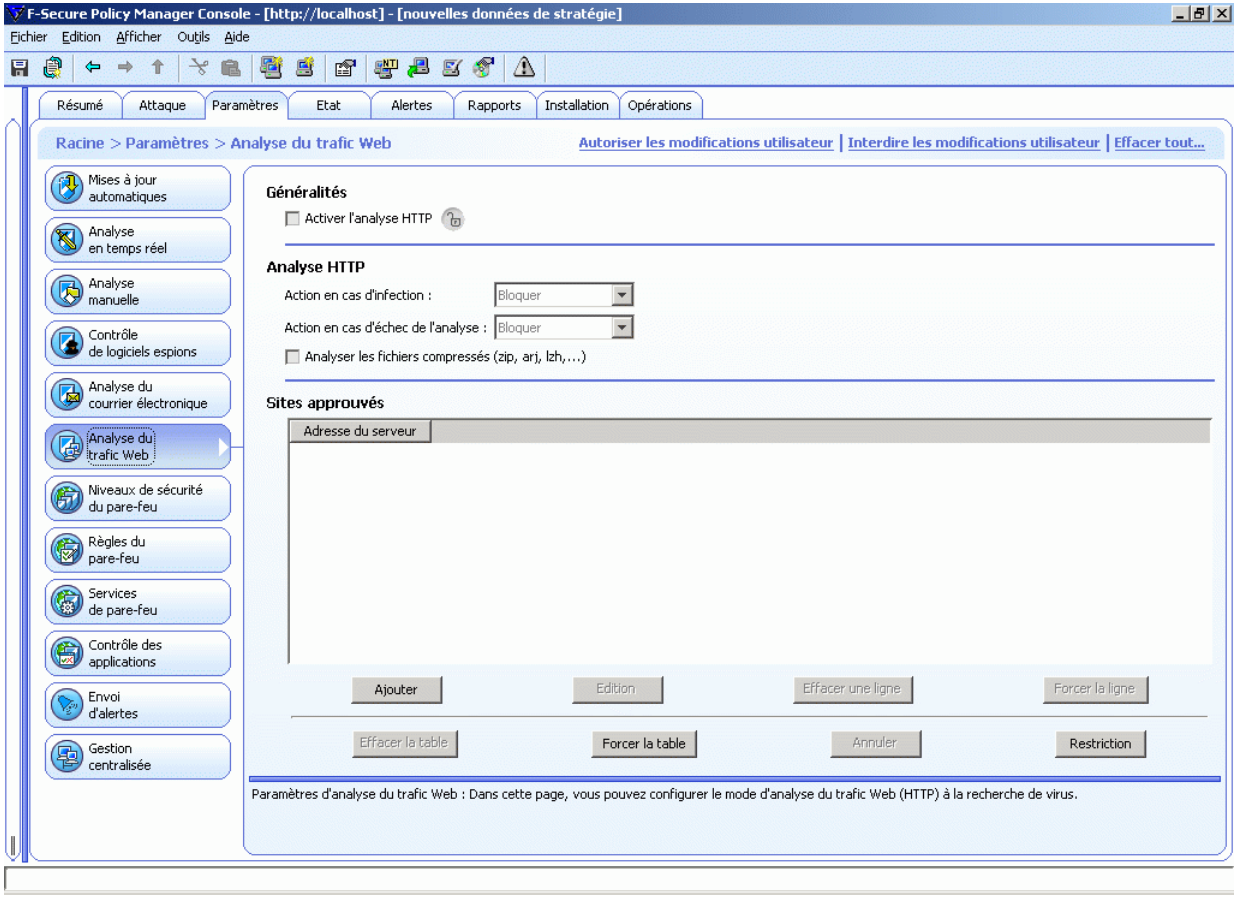


Figure 3-13 Paramètres > Analyse du trafic Web

Généralités

Dans la section *Généralités*, vous pouvez activer ou désactiver l'analyse 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

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

Pour plus d'informations sur l'analyse du trafic Web et pour des exemples de configuration pratique, reportez-vous à la section “*Configuration de l'analyse du trafic Web (HTTP)*”, *180*.

Niveaux de sécurité du pare-feu

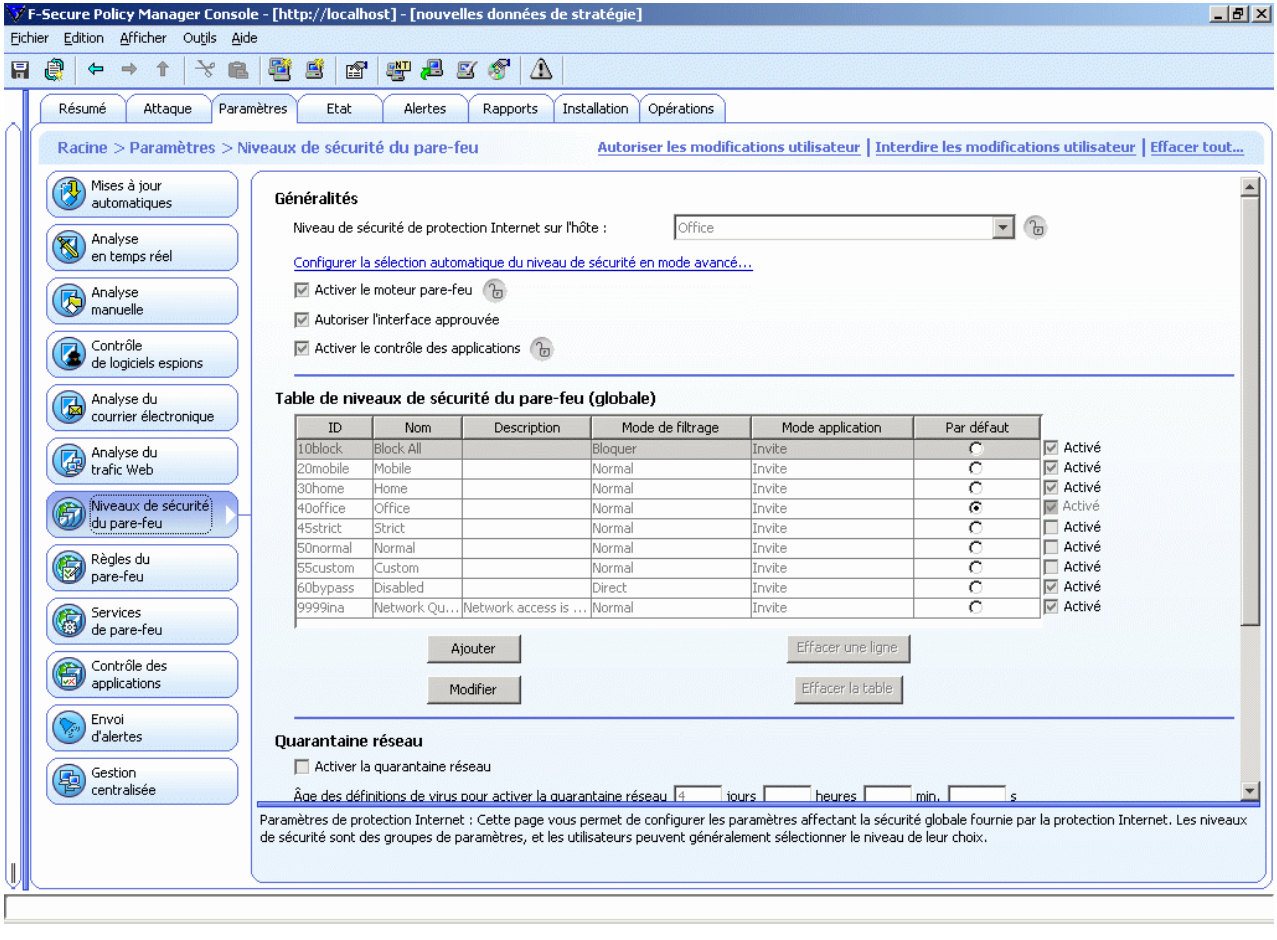


Figure 3-14 Paramètres > Niveaux de sécurité du pare-feu

Généralités

Dans la section *Généralités*, vous pouvez :

- Sélectionner le niveau de sécurité de la protection Internet au niveau de l'hôte. Pour plus d'informations, reportez-vous à la section "*Niveaux de sécurité globale de pare-feu*", *201*.
- 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. Pour plus d'informations, reportez-vous à la section "*Configuration de la sélection automatique du niveau de sécurité*", *282*.
- 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*. Pour plus d'informations, reportez-vous à la section "*Configuration des niveaux et règles de sécurité de la protection Internet*", *204*.
- Activer l'utilisation de l'interface approuvée. Pour plus d'informations, reportez-vous à la section "*Interface approuvée*", *281*.
- Activer la fonction de contrôle des applications. Pour plus d'informations, reportez-vous à la section "*Configuration du contrôle des applications*", *216*.

Quarantaine réseau

Dans la section *Quarantaine réseau*, vous pouvez :

- Activer 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.

Pour plus d'informations et pour voir un exemple de configuration, reportez-vous à la section "*Configuration de la quarantaine réseau*", *210*.

Prévention des intrusions

Dans la section *Prévention des intrusions*, vous pouvez :

- Activer et désactiver la détection des intrusions.
- Sélectionner l'action en cas de paquet malveillant. Les options sont :
- *Consigner et supprimer* et *Consigner sans supprimer*.
- Définir la gravité d'alerte centralisée.
- Définir le niveau d'alerte et de performances.

Pour des exemples de configuration et plus d'informations, reportez-vous à la section “*Configuration de la prévention des intrusions*”*, 226*.

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

La table des niveaux de sécurité du pare-feu 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.

Pour plus d’informations, reportez-vous à la section “*Niveaux de sécurité globale de pare-feu*”*, 201*.

Règles de pare-feu

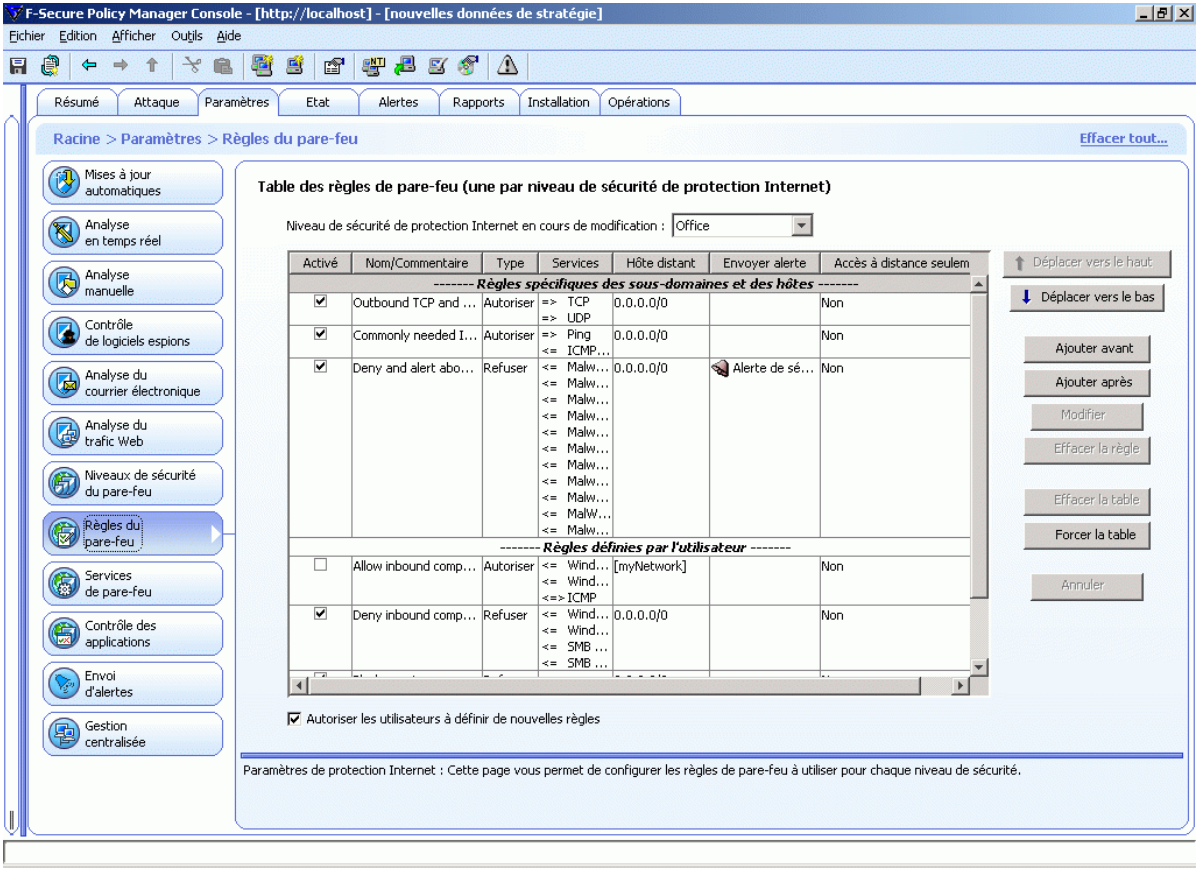


Figure 3-15 Paramètres > Règles de pare-feu

Table des règles de pare-feu

La page *Règles de pare-feu* contient la *table des règles de pare-feu* qui répertorie les règles définies pour différents niveaux de sécurité. Vous pouvez sélectionner le niveau de sécurité de la protection Internet 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 la table.

Lorsque le pare-feu de la protection Internet F-Secure est utilisé, les règles de firewall sont vérifiées dans l'ordre où elles s'affichent dans la table, de haut en bas. Pour les niveaux de sécurité avec mode de filtrage « normal »(voir la page *Niveaux de sécurité de firewall* dans l'onglet *Paramètres*), 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 finals 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 :

- Si la règle est 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.
- Si l'envoi d'une alerte est activé.
- Si la règle s'applique uniquement lorsqu'une liaison d'accès à distance est utilisée.

Lorsque l'option *Autoriser les utilisateurs à définir des nouvelles règles* est sélectionnée, les utilisateurs peuvent créer de nouvelles règles.

Spécifier un nouvel emplacement modifie l'emplacement des règles définies par l'utilisateur dans la *table des règles de pare-feu*.

En outre, le contrôle des applications sur l'hôte crée automatiquement des règles 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 avec état 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.

Pour plus d'informations sur la création et la modification de règles de pare-feu, reportez-vous aux sections “*Configuration des niveaux et règles de sécurité de la protection Internet*”, *204* et “*Configuration des alertes de règle de la protection Internet*”, *212*.

Services de pare-feu

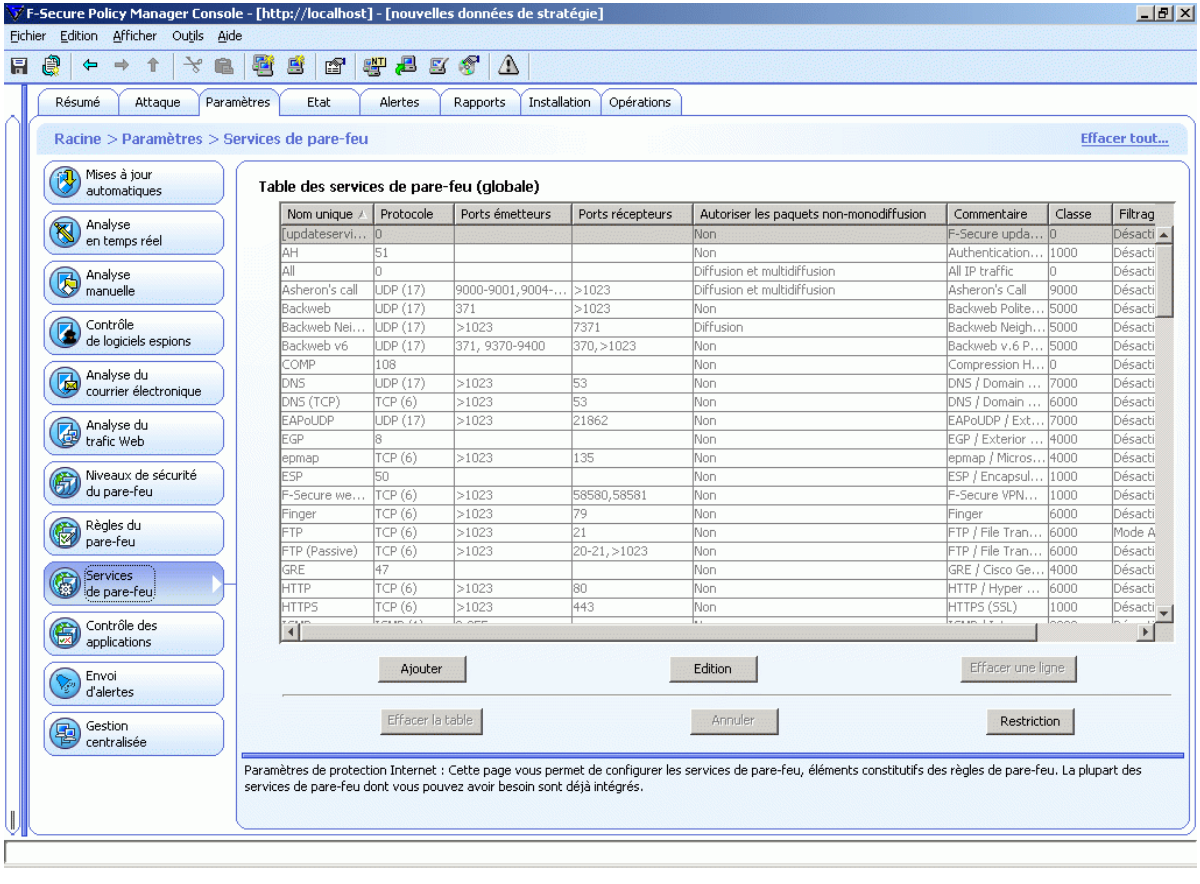


Figure 3-16 Paramètres > Services de pare-feu

Un service (abréviation de service de réseau) correspond à un service disponible sur le réseau, par exemple, le partage de fichier, 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)

La *table des services de pare-feu* affiche une liste de services définis pour le pare-feu. Il est également possible de créer ou de permettre aux utilisateurs finals de créer de nouveaux services pour le pare-feu. Pour plus d'informations sur l'ajout et la modification de services de pare-feu, reportez-vous à la section “*Ajout de nouveaux services*”, *291*.

Vous pouvez également empêcher les utilisateurs d'ajouter de nouveaux services en cochant la case *Taille fixe* sous la table. Lorsque cette restriction est activée, les utilisateurs finals ne peuvent ni ajouter ni supprimer de lignes dans les tables.

Contrôle des applications

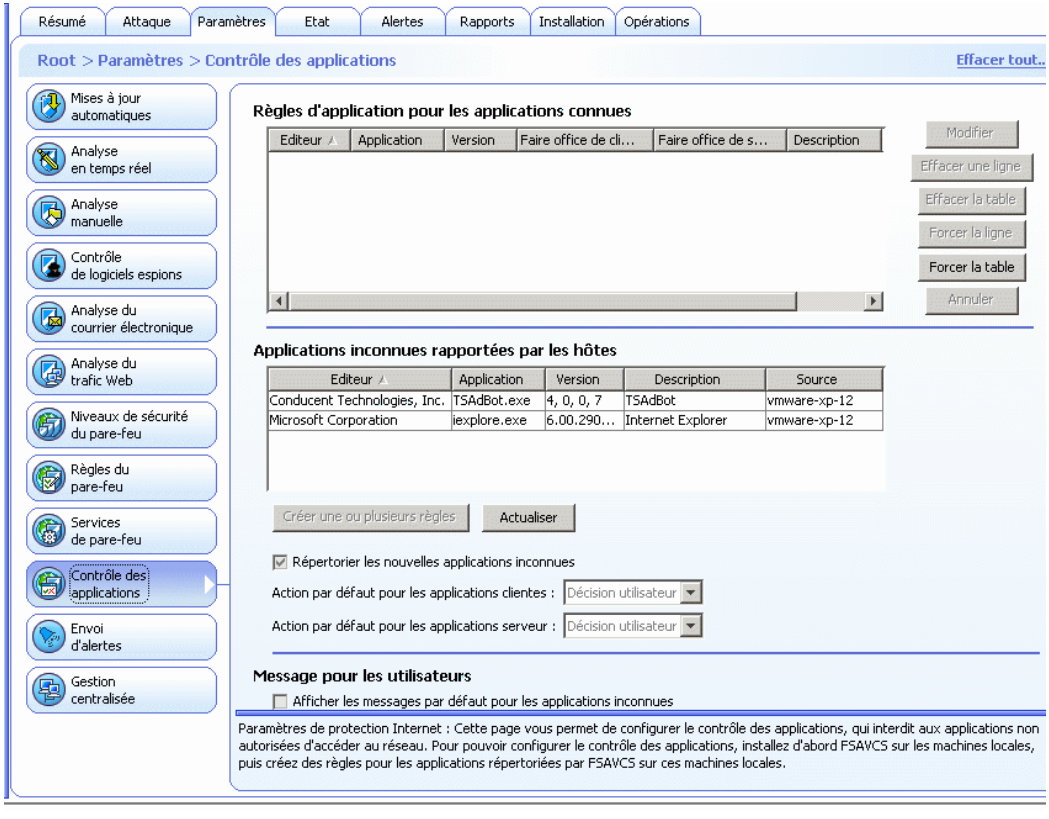


Figure 3-17 Paramètres > Contrôle des applications

Règles d'application pour les applications connues

La page *Contrôle des applications* 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

La liste *Applications rapportées par les hôtes* répertorie les applications que les hôtes ont signalées et pour lesquelles il n'existe pas encore de règles.

Sur cette page, vous pouvez également :

- 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*.

Message pour les utilisateurs

La section *Message pour les utilisateurs* contient les options suivantes :

- L'option *Afficher les messages par défaut pour les applications inconnues* permet aux utilisateurs de voir les messages par défaut en cas de tentatives de connexion par des applications inconnues.
- 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.

Pour plus d'informations sur la configuration et l'utilisation du Contrôle des applications ainsi que pour des exemples de configuration, reportez-vous à la section “*Configuration du contrôle des applications*”, *216*.

Envoi d'alertes

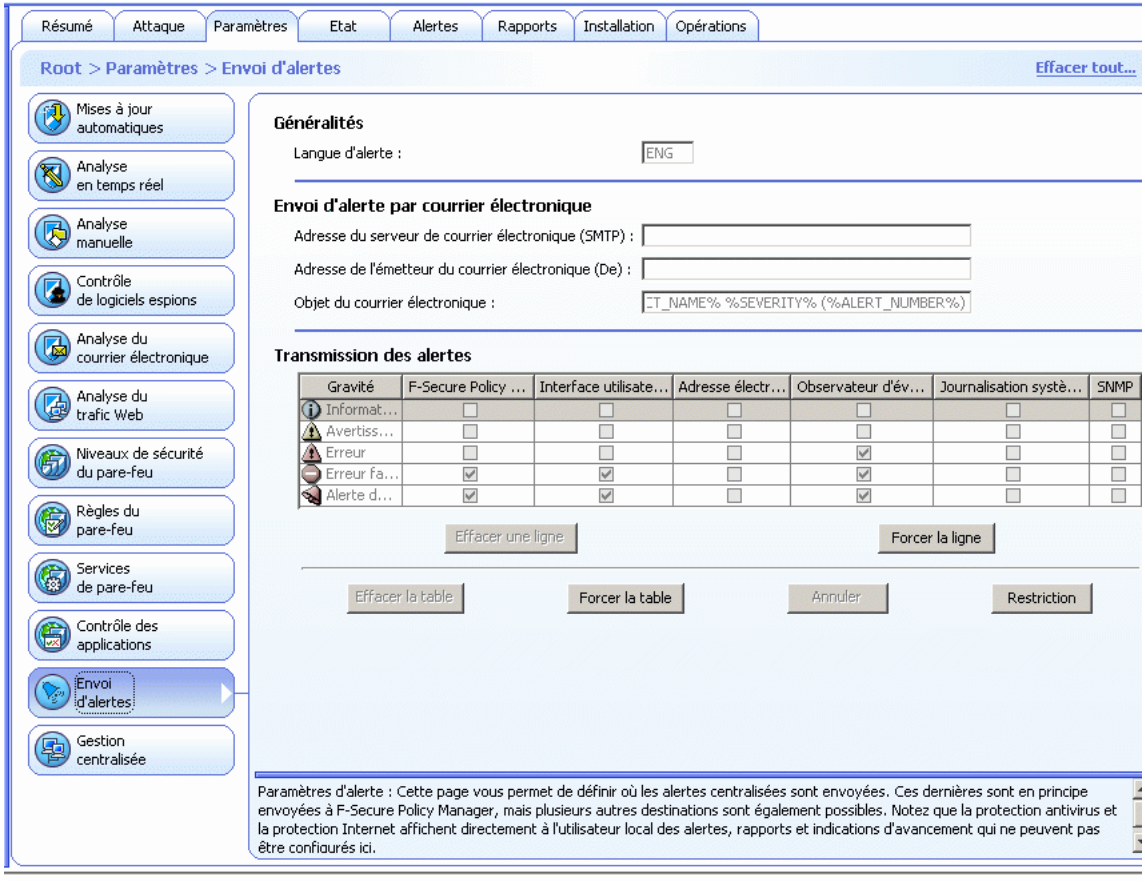


Figure 3-18 Paramètres > Envois d'alerte

Généralités

Dans la section *Généralités*, vous pouvez :

- Sélectionner la langue de l'alerte.

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.

Pour des informations sur la configuration de l'envoi d'alertes, reportez-vous à la section “*Envoi d'alertes par courrier électronique*”, *93*.

Transmission des alertes

La table *Transmission des alertes* permet de configurer la destination des alertes d'une certaine gravité.

Pour des exemples de configuration de transmission d'alertes antivirus, reportez-vous à la section “*Configuration d'envoi d'alertes de F-Secure Client Security*”, *194* .

Pour des exemples de configuration de la transmission d'alertes de protection Internet, reportez-vous aux sections “*Configuration des alertes de règle de la protection Internet*”, *212* et “*Utilisation d'alertes pour vérifier le fonctionnement de la protection Internet*”, *225*.

Gestion centralisée

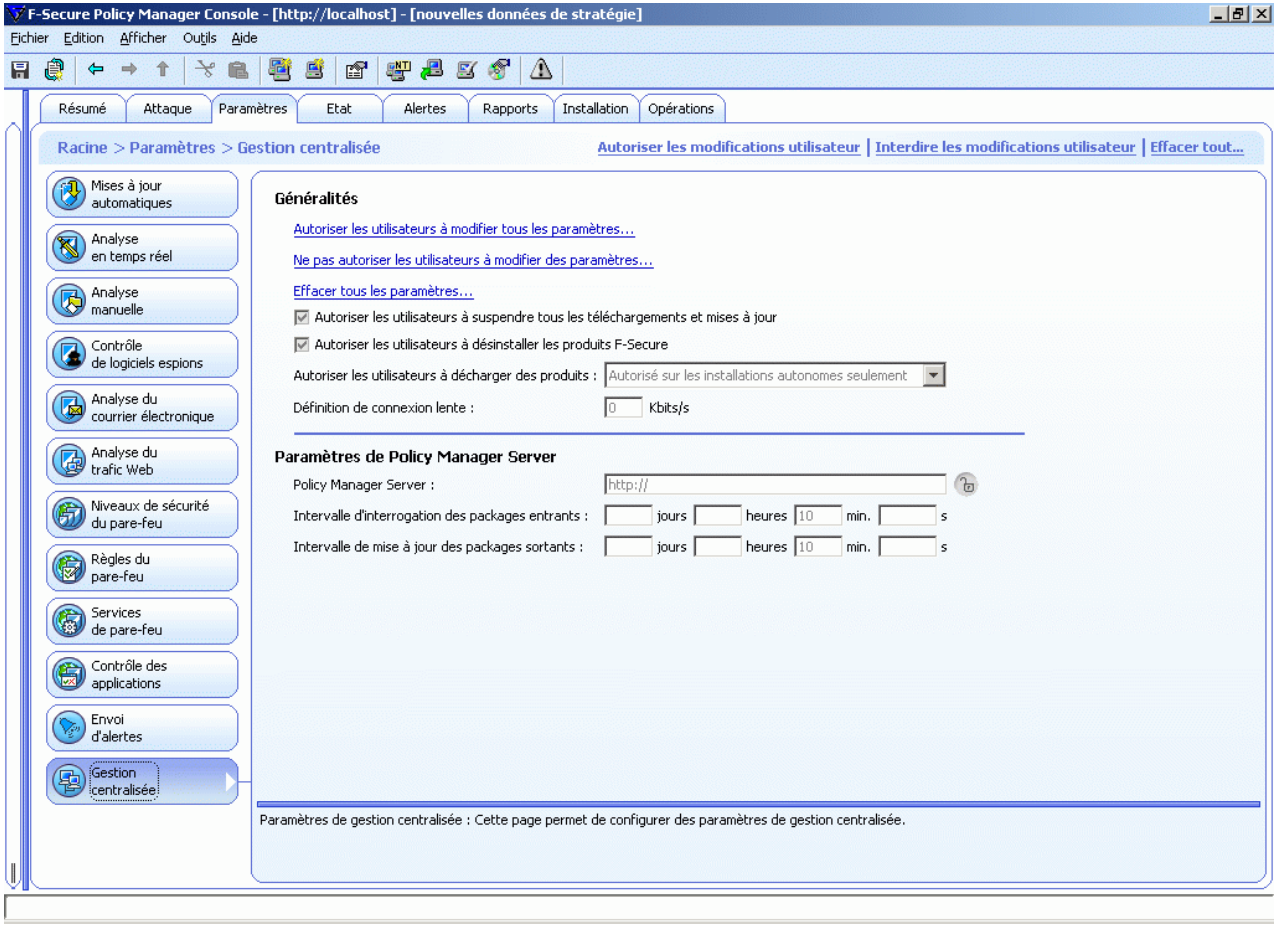


Figure 3-19 Settings > Gestion centralisée

Généralités

La section *Généralités* contient les options suivantes :

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

Cette option détermine comme non finals tous les paramètres des interfaces utilisateur antivirus et avancée de F-Secure Policy Manager, 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 finals tous les paramètres des interfaces utilisateur antivirus et avancée de F-Secure Policy Manager, ce qui signifie que les utilisateurs ne sont pas autorisés à modifier tous les paramètres. Pour plus d'informations sur les paramètres finals, reportez-vous à la section "*Transmission des paramètres par héritage*", *116*.

- Effacer tous les paramètres

  Cette option rétablit les paramètres par défaut pour tous les composants de F-Secure 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 les logiciels 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, il faut soit sélectionner cette option, soit arrêter d'abord le service F-Secure 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 (zéro) signifie que toutes les connexions sont considérées comme rapides.

Paramètres de Policy Manager Server

- *Policy Manager Server*

  Adresse URL du serveur F-Secure Policy Manager Server.

- *Intervalle de récupération des packages entrants*

  Définit la fréquence à laquelle l'hôte essaie de récupérer les packages entrants depuis le serveur 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 au serveur 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.

3.3.4 Onglet Etat

Les différentes pages de l'onglet *Etat* affichent des informations détaillées sur l'état de certains composants d'applications F-Secure 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.

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

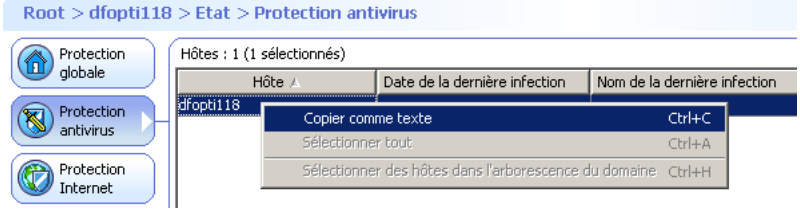


Figure 3-20 Le menu contextuel que vous pouvez ouvrir en cliquant avec le bouton droit sur une ligne

En cliquant avec le bouton droit sur une ligne des pages 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.
- L'option *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

Figure 3-21 Page Etat > Protection globale

La page *Protection globale* affiche une synthèse de l'état de protection de chaque hôte :

- 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-Secure Gateway (GW)
- Version des définitions de virus sur les produits F-Secure 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 des définitions de courrier indésirable sur des produits F-Secure Gateway (GW)
- Version des définitions de courrier indésirable sur les produits F-Secure Gateway
- 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.

- Delta de mise à jour, qui 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 F-Secure Policy Manager.

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

Protection antivirus

Figure 3-22 Page Etat > 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

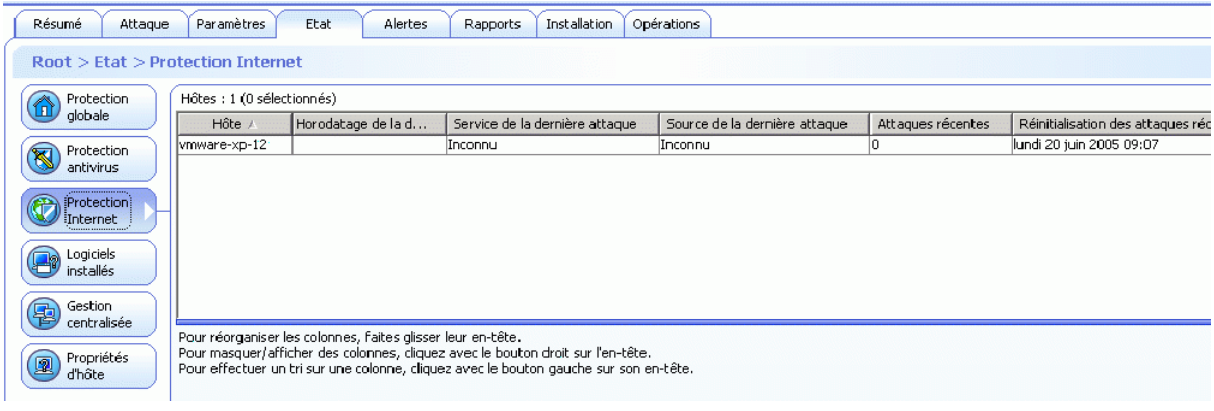


Figure 3-23 Page Etat > Protection Internet

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

Figure 3-24 Etat > Logiciels installés

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

- La version du logiciel F-Secure Client Security (ainsi que le numéro de révision et d'éventuels correctifs)
- 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 l'agent de mise à jour automatique est installé
- Si le contrôle du système est installé
- Version de Policy Manager Proxy

Gestion centralisée

Figure 3-25 Etat > Gestion centralisée

La page *Gestion centralisée* affiche une synthèse des informations liées 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 F-Secure 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 d'hôte

Figure 3-26

Figure 3-27 Etat > Propriétés d'hôte

La page *Propriétés d'hôte* affiche les informations suivantes pour 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.

3.3.5 Onglet Alertes

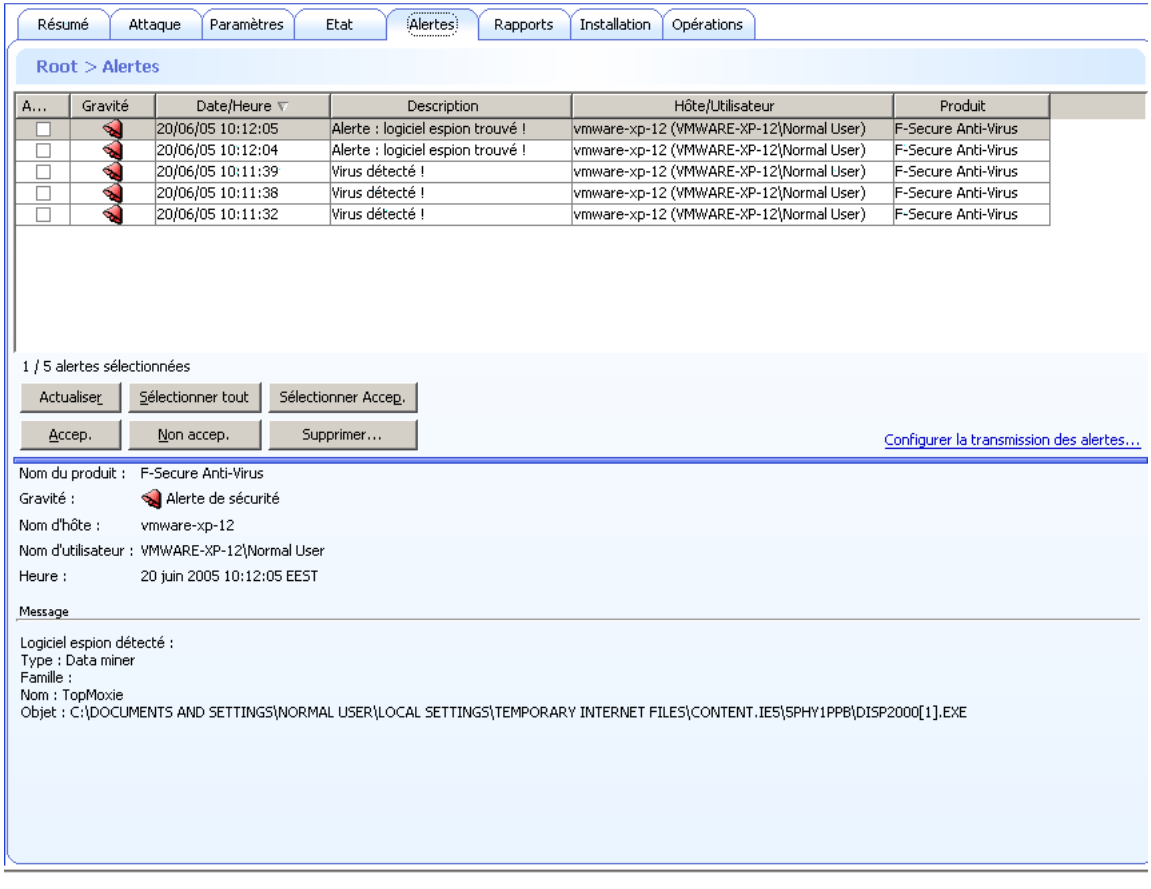


Figure 3-28 Onglet Alertes

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 :

- gravité (pour plus d'informations, reportez-vous à la section "*Affichage des alertes*", *235*).
- date et heure
- description
- hôte et l'utilisateur
- 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 émetteur, etc. Des alertes d'analyse de F-Secure Client Security peuvent également avoir un rapport attaché. 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 à la page *Alertes*, où vous pouvez configurer la transmission d'alertes. Pour un exemple de configuration, reportez-vous à la section "*Configuration d'envoi d'alertes de F-Secure Client Security*", *194*.

Pour plus d'informations sur l'utilisation des alertes pour la surveillance des virus et attaques, reportez-vous à la section "*Affichage des alertes*", *235*.

3.3.6 Onglet Rapports

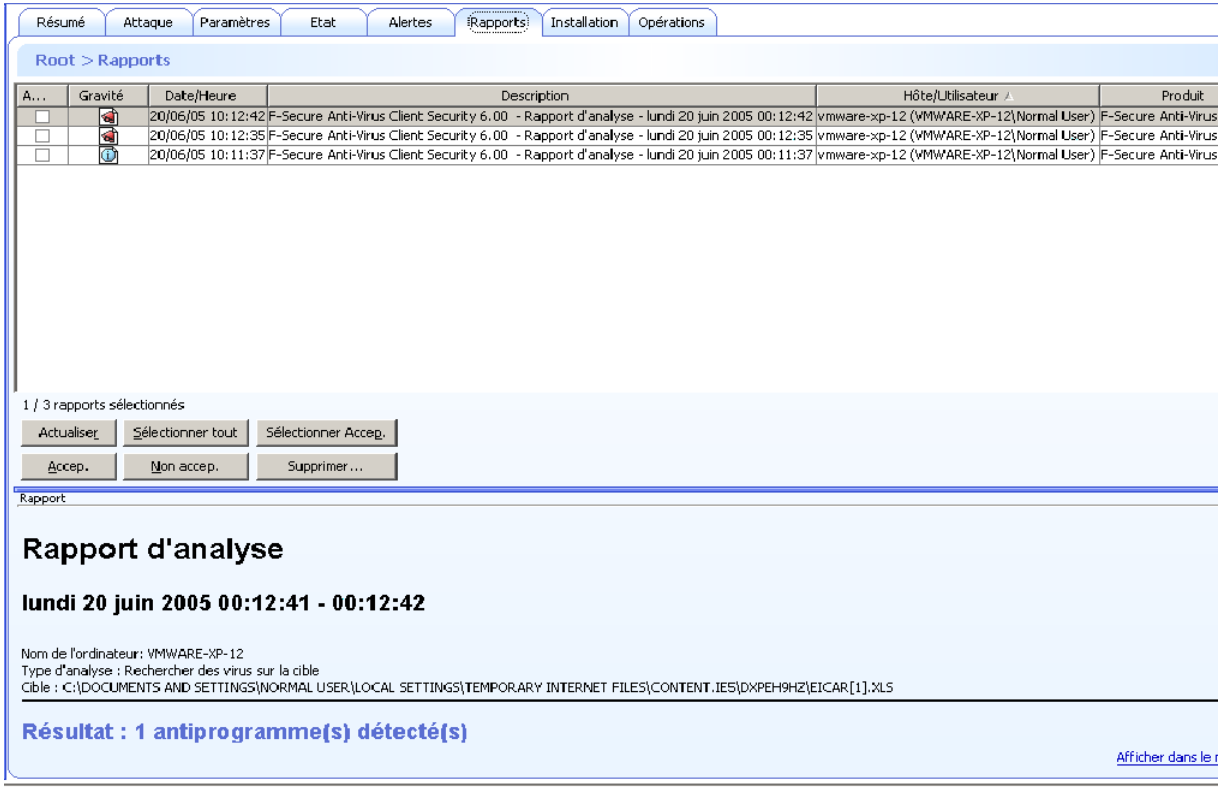


Figure 3-29 Onglet Rapports

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 pour chaque rapport :

- gravité
- date et heure
- description
- hôte et l'utilisateur
- 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.

Pour plus d'informations sur l'utilisation des alertes pour la surveillance, reportez-vous à la section “*Visualisation des rapports d'analyse*”, *234*.

3.3.7 Onglet Installation

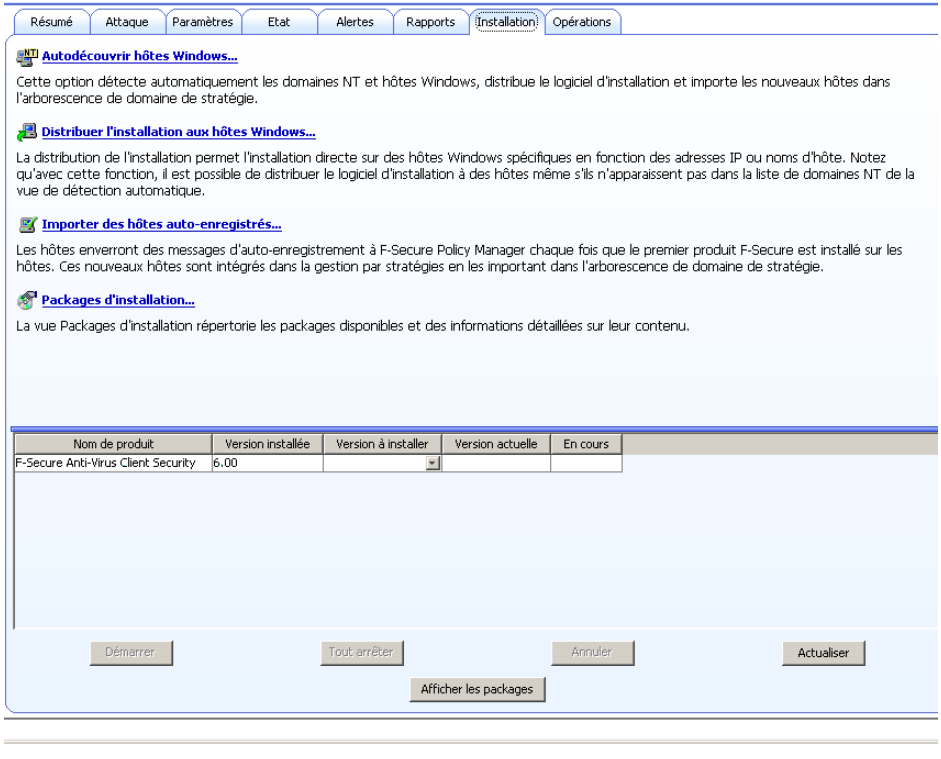


Figure 3-30 Onglet Installation

L'onglet *Installation* est le premier qui s'ouvre lorsque 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-enregistrés...	Les hôtes envoient des messages d'enregistrement automatique à F-Secure 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.

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. Pour plus d'informations, reportez-vous aux notes de publication.

3.3.8 Onglet Opérations

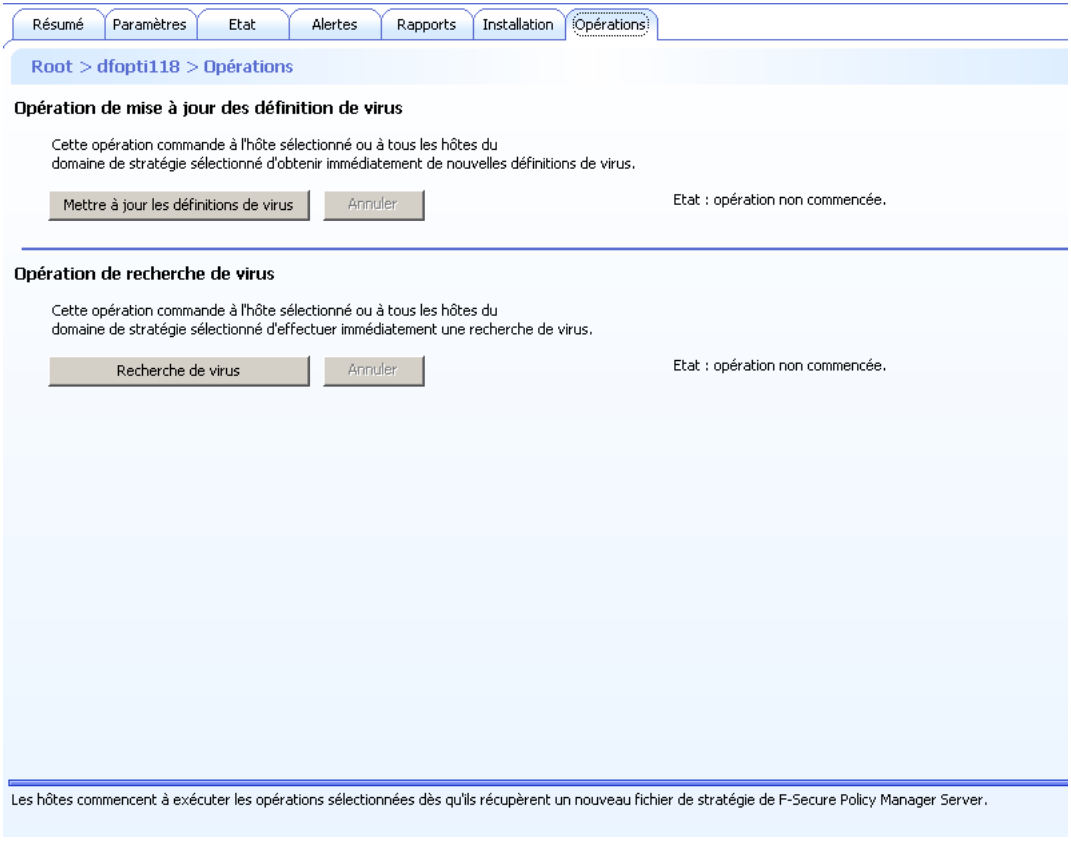


Figure 3-31 Onglet Opérations

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. Pour plus d'informations, reportez-vous à la section “*Que faire en cas d'apparition d'un nouveau virus ?*”, *264*.

3.4 Barre d'outils

La barre d'outils contient des boutons pour les tâches de F-Secure Policy Manager Console les plus courantes.

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.

Met à jour la base de données de définitions de virus.

Affiche toutes les alertes. L'icône est mise en surbrillance s'il existe de nouvelles alertes. Lorsque vous démarrez F-Secure Policy Manager Console, l'icône est toujours mise en surbrillance.

3.5 Commandes des menus

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 les stratégies	Distribue les fichiers de stratégie.
	Exporter le fichier de stratégie de l'hôte	Exporte les fichiers de stratégie.
	Quitter	Quitte F-Secure 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-enregistrement.
	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	Barre d'outils	Affiche la barre d'outils.
	Barre d'état	Affiche la barre d'état.
	Info-bulles	Affiche les descriptions des boutons sur lesquels vous placez le pointeur de la souris.
	Editeurs de restriction intégrés	Bascule entre l'éditeur de restriction intégré et la boîte de dialogue des restrictions.
	Ouvrir pour les nouveaux messages	Affiche ou masque le volet Messages en bas de l'écran.
	Domaine/Hôte précédent	Accède au domaine ou à l'hôte précédent dans l'historique de sélection de l'arborescence.
	Domaine/Hôte suivant	Accède au domaine ou à l'hôte suivant dans l'historique de sélection de l'arborescence.
	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 décrite dans le présent manuel.
	Actualiser <Elément>	Permet d'actualiser manuellement l'affichage du rapport, de l'état ou de l'alerte. L'option de menu change selon la page sélectionnée.
	Actualiser tout	Permet d'actualiser manuellement toutes les données affectées par l'interface, soit : la stratégie, l'état, les alertes, les rapports, les packages d'installation et les 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 F-Secure 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.
	Mettre à jour les définitions de virus sur le serveur	Importe les définitions de virus sur le serveur à partir d'un fichier zip.
	Préférences	Définit les propriétés locales de F-Secure Policy Manager Console. Ces propriétés concernent uniquement l'installation locale de F-Secure Policy Manager Console.
Aide	Sommaire	Affiche l'index de l'aide.

Web Club	Ouvre votre navigateur Web et établit une connexion au Web Club de F-Secure Policy Manager.
Contacts	Affiche les coordonnées des contacts de la société F-Secure.
À propos de F-Secure Policy Manager Console	Affiche les informations de version.

3.6 Transmission des paramètres par héritage

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 F-Secure 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 finals, ce qui signifie que les utilisateurs ne sont pas autorisés à les modifier. Le type *Final* impose toujours la stratégie : la variable de stratégie remplace toute valeur de l'hôte local et l'utilisateur final ne peut pas modifier cette valeur tant que la restriction est de type *Final*. Si les paramètres n'ont pas été définis comme finals, les utilisateurs sont autorisés à les modifier.

3.6.1 Affichage de l'héritage de 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	
		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. Si le symbole 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. Si le symbole 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.
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.

3.6.2 Verrouillage et déverrouillage simultanés de tous 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.

Pour plus d'informations sur le verrouillage et le déverrouillage de tous les paramètres dans l'interface utilisateur de F-Secure Policy Manager, voir aussi les sections "*Gestion centralisée*", *94* et "*Interdiction de modification des paramètres par les utilisateurs*", *193*.

Pour plus d'informations sur la transmission de valeurs forcées à des sous-domaines et la visualisation des valeurs actuelles, reportez-vous à la section "*Menu contextuel des pages Paramètres*", *61*.

3.6.3 Héritage des paramètres dans les tables

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.

4 CONFIGURATION DU RÉSEAU GÉRÉ

4.1 Présentation

Ce chapitre indique comment planifier le réseau géré et précise les meilleures approches de déploiement de F-Secure Client Security dans différents types d'environnements.

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

- Dans un domaine Windows, vous pouvez utiliser les fonctions *Autodécouvrir* et *Auto-enregistrement* 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 F-Secure 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 finals ayant des besoins de sécurité similaires et de regrouper les ordinateurs portables et portatifs dans leurs propres sous-domaines. 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.

Ces aspects seront traités dans la section “*Création de la structure du domaine*”, *127*.

4.2 Première connexion

Cette section explique comment se connecter à F-Secure Policy Manager Console et comment configurer les propriétés de connexion et les préférences de communication.

4.2.1 Ouverture de session

Lorsque vous démarrez F-Secure Policy Manager Console, la boîte de dialogue suivante s'ouvre. Cliquez sur **Options** pour développer la boîte de dialogue et afficher davantage d'options.

Figure 4-1 F-Secure Policy Manager Console Boîte de dialogue d'ouverture de session

Vous pouvez utiliser la boîte de dialogue pour sélectionner des connexions définies. Chaque connexion a des préférences spécifiques, ce qui simplifie la gestion de plusieurs serveurs avec une seule instance de F-Secure Policy Manager Console.

Après la sélection de la connexion, entrez la phrase de cryptage de F-Secure 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 également 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.

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

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

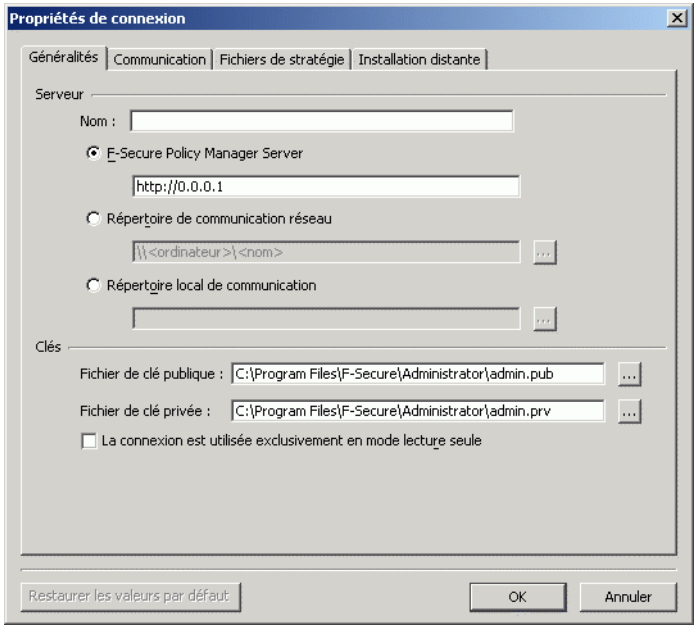


Figure 4-2 La boîte de dialogue Propriétés de connexion

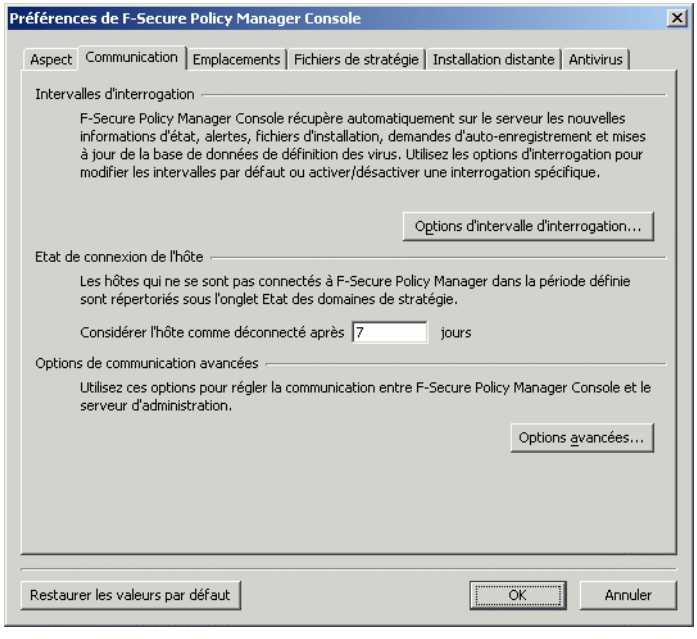
Le champ *Nom* permet de définir le nom que portera la connexion dans le champ *Connexion :* de la boîte de dialogue d'ouverture de session. Si le champ *Nom* reste vide, l'URL ou le chemin d'accès s'affiche.

Les chemins des fichiers de clé publique et privée indiquent le jeu de clés d'administration à utiliser pour l'environnement en question. Si les fichiers de clés spécifiés n'existent pas, F-Secure Policy Manager Console génère une nouvelle paire de clés.

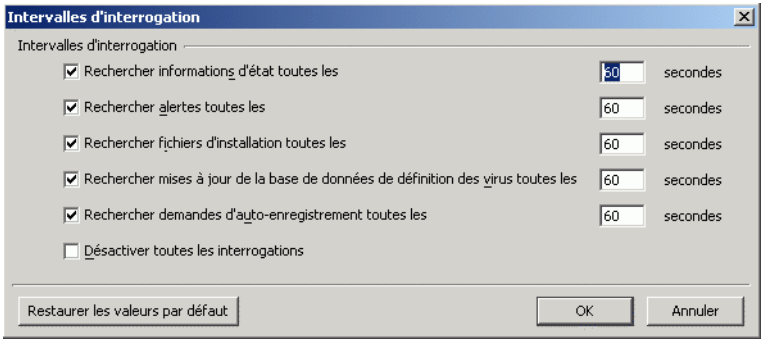
Vérification des préférences de communication

Cliquez sur l'onglet *Communication* pour personnaliser les paramètres de communication.

1. Pour modifier les intervalles d'interrogation, cliquez sur **Options d'intervalle d'interrogation**. Dans la plupart des cas, vous pouvez accepter les valeurs par défaut.
2. *Etat de connexion de l'hôte* contrôle quand les hôtes sont considérés comme déconnectés de F-Secure Policy Manager. Tous les hôtes qui n'ont pas contacté F-Secure Policy Manager Server dans l'intervalle défini sont considérés comme déconnectés. Ces hôtes déconnectés sont signalés par une icône de notification dans l'arborescence et sont placés dans la liste Hôtes déconnectés de l'onglet Synthèse.
3. Notez qu'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, les ordinateurs portables ne pourront peut-être pas accéder quotidiennement au serveur, mais, dans la plupart des cas, cette situation est normale.



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



4.3 Création de la structure du domaine

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.

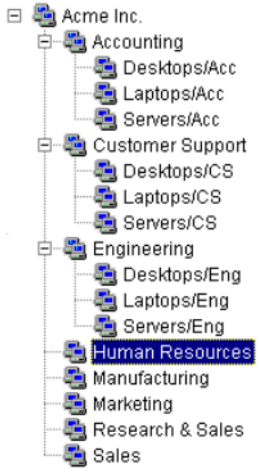


Figure 4-3 Exemple de structure de domaines de stratégie

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

On peut également créer les différents bureaux nationaux en tant que sous-domaines.

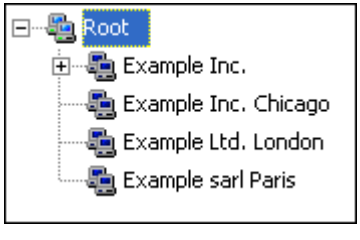


Figure 4-4 Exemple de structure de domaines de stratégie : bureaux nationaux en tant que sous-domaines

On peut également grouper les hôtes en sous-domaines en fonction de la version de F-Secure Client Security installée. Vous pouvez, par exemple, grouper les hôtes qui ont installé F-Secure Client Security 6.x dans un sous-domaine et les hôtes qui ont installé F-Secure Client Security 7.x dans un autre domaine.

4.3.1 Ajout de domaines et sous-domaines de stratégie

1. Dans le menu *Edition*, choisissez *Nouveau domaine de stratégie* (après avoir sélectionné un domaine parent), ou cliquez sur  dans la barre d'outils. Ou encore, vous pouvez appuyer sur les touches CTRL et INSER. Le nouveau domaine de stratégie est un sous-domaine du domaine parent sélectionné.
2. Vous êtes alors invité à entrer le nom de la stratégie de domaine. Une icône représentant le domaine est créée sous l'onglet *Domaines de stratégie*.
3. De la même façon, vous pouvez créer les sous-domaines : sélectionnez le domaine créé, cliquez sur  dans la barre d'outils et entrez un nom pour le nouveau sous-domaine.

4.4 Ajout d'hôtes

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

- Importez les hôtes directement à partir de votre domaine Windows, puis installez F-Secure Client Security sur ceux-ci à distance.
- Importez des hôtes par auto-enregistrement après que F-Secure Client Security y a été installé localement.

4.4.1 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 en sélectionnant la commande ‘Autodécouvrir hôtes Windows’ sous l'onglet *Installation* de F-Secure Policy Manager Console. Notez que cela installe également F-Secure Client Security sur les hôtes importés. Pour importer des hôtes à partir d'un domaine Windows, sélectionnez le domaine cible, puis la commande ‘Autodécouvrir hôtes Windows du menu *Edition*. Cette commande ouvre la fenêtre Autodécouvrir hôtes Windows. Sélectionnez les hôtes où vous souhaitez installer le logiciel et cliquez sur **Installer**.

4.4.2 Hôtes auto-enregistrés

Dans les domaines Linux et dans les domaines où F-Secure Client Security a été localement installé sur des hôtes, la méthode la plus pratique pour importer des hôtes dans F-Secure Policy Manager Console consiste à utiliser la fonction d'auto-enregistrement. Vous procédez à cette opération uniquement après l'installation de F-Secure Client Security sur les hôtes et après que ces derniers ont envoyé une demande d'auto-enregistrement. F-Secure Client Security devra être installé à partir d'un CD-ROM, à partir d'un script de connexion ou par une autre méthode. Pour importer des hôtes auto-enregistrés, cliquez sur  ou choisissez la commande *Importer des hôtes auto-enregistrés* du menu *Edition* ou de la vue Installation. Une fois l'opération terminée, l'hôte est ajouté à l'arborescence du domaine. Vous pouvez importer les hôtes auto-enregistrés dans différents domaines en fonction d'autres critères, comme l'adresse IP ou DNS des hôtes. Pour plus d'informations, reportez-vous à la section “*Règles d'importation pour l'auto-enregistrement*”, *132*.

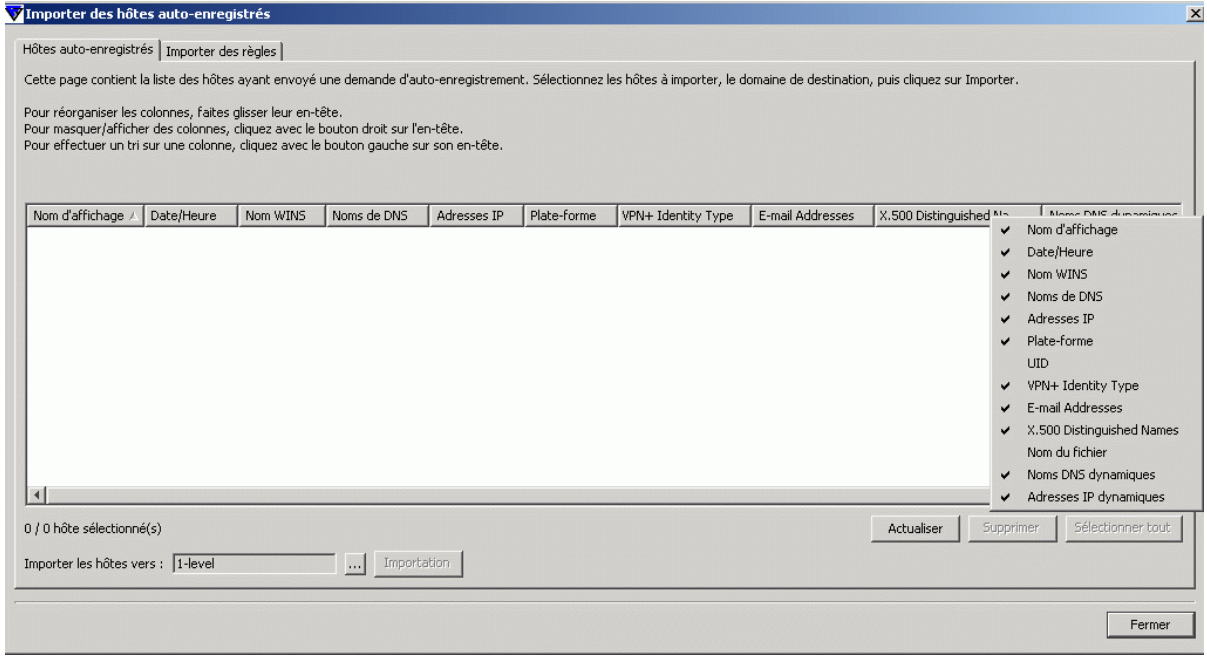


Figure 4-5 Boîte de dialogue Importer des hôtes auto-enregistrés > onglet Hôtes auto-enregistrés

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 (voir l'étape 6 de la section *Utilisation du package JAR d'installation distante personnalisé*). 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'endroit approprié, ainsi que modifier la largeur de chaque colonne. Le menu contextuel du tableau (accessible par un clic du bouton droit de la souris dans la barre d'en-tête du tableau) permet de choisir les propriétés d'auto-enregistrement affichées dans le tableau.

Règles d'importation pour l'auto-enregistrement

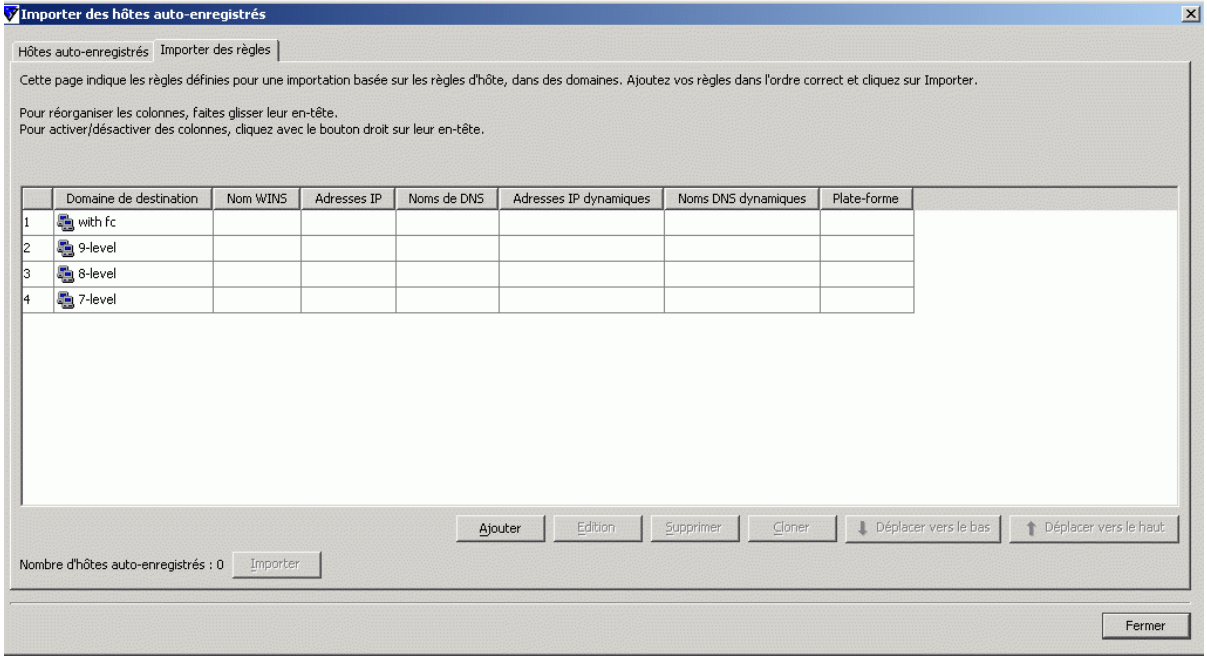


Figure 4-6 Boîte de dialogue Importer des hôtes auto-enregistrés > onglet Importer des règles

Vous pouvez définir les règles d'importation des hôtes auto-enregistrés sous l'onglet *Importer des règles* de la fenêtre *Importer des hôtes auto-enregistrés automatiquement*. Vous pouvez utiliser les éléments suivants comme critères d'importation dans les règles :

- *Nom WINS*, *Nom DNS*, *Nom DNS dynamique*, *Propriétés personnalisées*
  - Ils prennent en charge le caractère générique * (astérisque), qui peut remplacer n'importe quel nombre de caractères. Par exemple : *test_hôte** ou **.exemple.com*.
  - La casse n'est pas respectée.
- *Adresse IP*, *Adresse IP dynamique*
  - L'adresse IP exacte est prise en charge lors de la correspondance (par exemple, *192.1.2.3*) ainsi que le sous-domaine IP (par exemple, *10.15.0.0/16*).

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 des colonnes visibles sont utilisées comme critères de correspondance lors de l'importation des hôtes dans le domaine de stratégie. Les autres valeurs, à savoir celles des colonnes masquées, ne sont pas prises en compte.

Vous avez également la possibilité d'ajouter des propriétés personnalisées en tant que critères pour l'importation des hôtes. Vous pouvez par exemple utiliser des propriétés personnalisées pour créer des fichiers d'installation distincts destinés à des unités d'exploitation différentes qui doivent être regroupées dans des domaines de stratégie spécifiques de ces unités. Dans ce cas, vous pouvez utiliser le nom de l'unité comme propriété personnalisée, puis créer des règles d'importation qui font appel à ces noms d'unité comme critères 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 propriété personnalisée, procédez comme suit :

1. Cliquez avec le bouton droit sur un en-tête de colonne et sélectionnez *Ajouter une propriété personnalisée*. La boîte de dialogue *Nouvelle propriété personnalisée* s'ouvre.
2. Nommez la propriété personnalisée, par exemple en utilisant le nom de l'unité. Cliquez ensuite sur **OK**.
3. La nouvelle propriété personnalisée apparaît désormais dans la table et vous pouvez l'employer comme critère d'importation dans les nouvelles règles d'importation que vous créez pour l'auto-enregistrement.

Pour créer une règle d'importation pour l'auto-enregistrement, procédez comme suit :

4. Cliquez sur le bouton **Ajouter** de l'onglet *Importer des règles*. La boîte de dialogue *Sélectionner le domaine de stratégie de destination pour la règle* contenant les domaines et sous-domaines existants s'affiche.
5. Sélectionnez le domaine pour lequel vous créez la règle et cliquez sur **OK**.
6. Vous pouvez maintenant définir les critères d'importation. Sélectionnez la ligne que vous venez de créer, cliquez dans la cellule à renseigner, puis cliquez sur **Modifier**. Entrez la valeur dans la cellule.

Lors de l'importation des hôtes auto-enregistrés, les règles sont vérifiées en commençant par celle du haut, et la première règle qui correspond est appliquée. Pour changer l'ordre de ces règles, cliquez sur **Déplacer vers le bas** ou sur**Déplacer vers le haut**.

Si vous voulez créer plusieurs règles pour un domaine, utilisez l'option **Cloner**. Commencez par créer une règle pour le domaine. Sélectionnez ensuite la ligne et cliquez sur **Cloner**. Vous pouvez maintenant modifier les critères sur la nouvelle ligne dupliquée.

Lorsque vous voulez débuter l'importation, sélectionnez l'onglet Hôtes auto-enregistrés et cliquez sur Importer. Les règles que vous avez définies sont validées avant le début de l'importation. Une fois l'importation des hôtes terminée, une boîte de dialogue s'affiche. Elle répertorie le nombre d'hôtes importés avec succès et le nombre d'échecs.

Notez qu'un groupe de conditions vide est toujours considéré comme répondant aux critères.

Création manuelle d'hôtes

Pour créer manuellement un hôte, sélectionnez un domaine de stratégie et choisissez *Nouvel hôte* dans le menu *Edition* ou cliquez sur le bouton **Ajouter un hôte**. Vous pouvez également appuyer sur la touche INSER. Cette opération est utile dans les cas suivants :

Apprentissage et test – Vous pouvez essayer un sous-ensemble des fonctions de F-Secure Policy Manager Console sans installer de logiciel en complément de F-Secure Policy Manager Console. Par exemple, vous pouvez créer des domaines et hôtes tests, et essayer des fonctions d'héritage de stratégie.

Définition anticipée de stratégie : vous pouvez définir et générer à l'avance une stratégie pour un hôte avant d'installer le logiciel sur cet hôte.

4.4.3 F-SecureInstallations à distance

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 NT, et l'utilisateur peut sélectionner les hôtes de destination dans une liste. La fonction *Distribuer l'installation aux hôtes Windows* 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. Vous devez disposer de droits d'administrateur pour utiliser ces méthodes d'installation.

Avant d'installer les hôtes

Avant de démarrer l'installation de F-Secure Client Security sur les hôtes, vous devez vérifier l'absence d'applications antivirus ou pare-feu en conflit pouvant y être installées.

F-Secure Setup reconnaît et supprime automatiquement les programmes antivirus suivants :

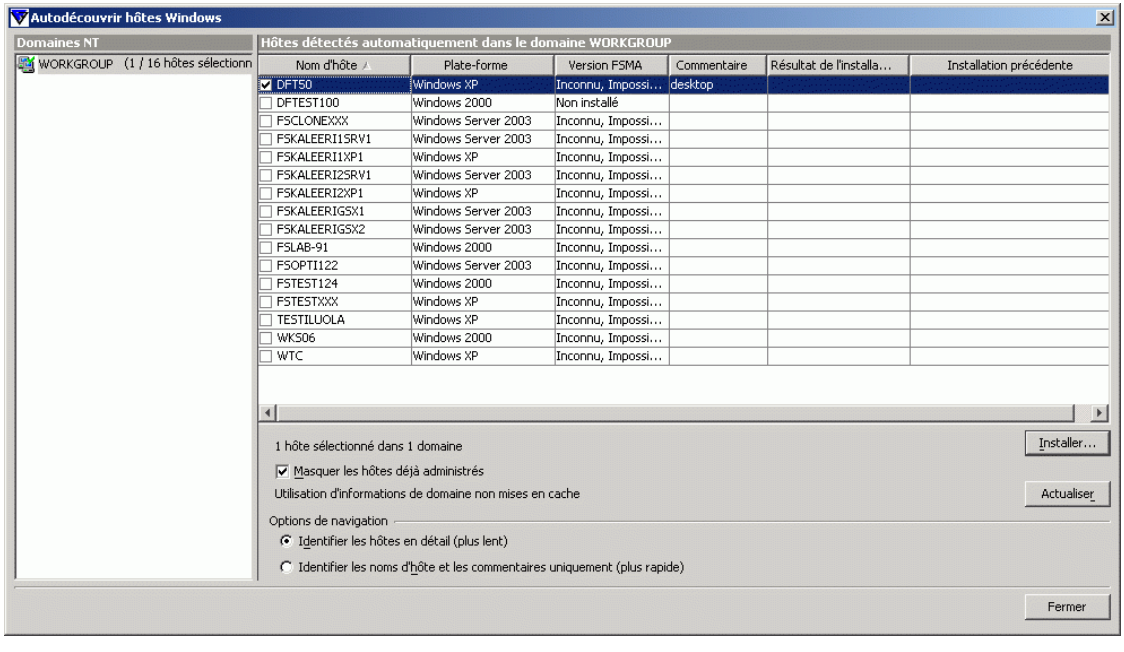
- AVG Anti-Virus 7.0, version 7.322
- AVG Anti-Virus 7.1, version 7.1.362
- AVIRA Desktop, version 1.0.0.22
- CA eTrust Antivirus 2005, version 7.1.192
- CA eTrust EZ Antivirus 2005, version 6.1.7
- CA eTrust EZ AntiVirus 2005, version 7.0.5.3
- CA EZ Trust Firewall
- Cisco VPN Client Firewall (ZoneAlarm firewall service)
- Dr Solomon's VirusScan, versions 4.50 et 4.51
- H+BEDV AntiVir Personal Edition 6.19.11.63
- Kaspersky Anti-Spam Personal, version 1.1
- McAfee Internet Security 5.02.6 et 5.00.5
- McAfee Internet Security Suite 2004, version 6.0 (composant pare-feu)
- McAfee Internet Security Suite 2004, version 6.0 (composant VirusScan)
- McAfee Personal Firewall Express, version 4.5
- McAfee VirusScan 4.05 NT
- McAfee VirusScan Enterprise 7.0
- McAfee VirusScan Enterprise 7.1
- McAfee VirusScan Home Edition 7.0.2.6000
- McAfee VirusScan Professional Edition 7.0
- McAfee VirusScan Professional/Personal Edition 7.02.6000
- Microsoft AntiSpyware, beta 1.0 version
- NAI ePolicy Orchestrator Agent 2000, version 2.0.0.376
- NAI ePolicy Orchestrator Agent 3000, versions 3.1.1.184 et 3.5.0.412
- Norman Virus Control, version 5.8
- Norman Virus Control 5.50 avec pare-feu
- Norman Virus Control, version 5.5

- Panda AdminSecure, version 3.02
- Panda AdminSecure, version 3.06.10
- Panda ClientShield Corporate, version 2.00
- Panda ClientShield Corporate, version 3.01.10.0000
- Panda FileSecure Version 6.07
- Panda Network Agent Version 3.02
- Sophos Anti-Virus 3.82 et 3.77
- Sourcenext 2006 version 9.0.0001 (Japonais)
- Symantec AntiVirus Corporate Edition version 10.0.0.359
- Symantec AntiVirus Corporate Edition version 10.0.1.1000
- Symantec AntiVirus Corporate Edition version 8.0.0.374
- Symantec AntiVirus Corporate Edition version 9.0.0.338 (= Symantec Client Security 2.0)
- Symantec AntiVirus Corporate Edition version 9.0.2.1000
- Symantec AntiVirus Corporate Edition version 9.0.3.1000
- Symantec Live Update 1.7 (pour Symantec AntiVirus Corporate Edition)
- Symantec Live Update 1.8 (pour Symantec AntiVirus Corporate Edition)
- Symantec Live Update 2.0.39.0 (pour Symantec AntiVirus Corporate Edition)
- Symantec Live Update 2.6.18.0 (pour Symantec AntiVirus Corporate Edition)
- Symantec Norton AntiVirus Corporate Edition 7.6.0.0000
- Trend Micro Internet Security 2004, version 11.10.1299
- Trend Micro Officescan Corporate Edition, version 5.5
- Trend Micro Officescan, version 5.02 (seulement pour une installation sur Windows 2000)
- Trend Micro PC-cillin 2003, version 10.01
- Trend Micro Virus Buster 2004 (Japonais)
- Trend Micro Virus Buster 2005 (Japonais)
- Trend Micro VirusBuster 2006, version 14.0 (Japonais)

Autodécouvrir hôtes Windows

Pour effectuer l'installation :

1. Sélectionnez le domaine de stratégie des hôtes sur lesquels vous allez installer F-Secure Client Security.
2. Ouvrez le menu *Edition* et choisissez la commande *Découverte automatique des hôtes Windows*. Vous pouvez aussi cliquer sur le bouton  .



3. Dans la liste des domaines NT, sélectionnez l'un des domaines puis 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 de découverte automatique suivantes :

Masquer les hôtes déjà administrés

Cochez la case *Masquer les hôtes déjà administrés* 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 F-Secure 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. Pour cocher les cases correspondantes, appuyez sur la BARRE D'ESPACEMENT.

   Vous pouvez sélectionner plusieurs hôtes en maintenant la touche MAJ enfoncée et en effectuant l'une des actions 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 NT sélectionné.
   - *Désactiver tout* : désactive les cases à cocher de tous les hôtes du domaine NT sélectionné.

   Cliquez sur **Installer** pour continuer.

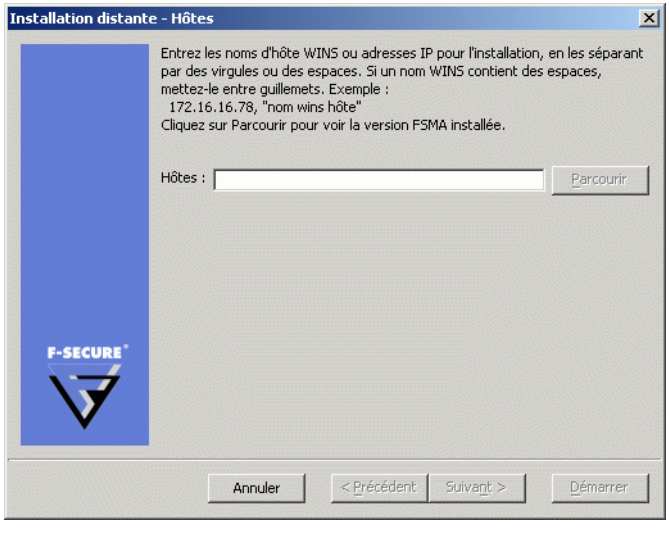
5. Une fois les hôtes de destination sélectionnés, passez à la section "*Installation distante après sélection de l'hôte de destination*", *141*, où vous trouverez des instructions sur l'installation à distance des applications sur les hôtes.

Distribuer l'installation aux hôtes Windows

Pour effectuer l'installation :

1. Sélectionnez le domaine de stratégie des hôtes sur lesquels vous allez installer F-Secure Client Security.
2. Ouvrez le menu *Edition* et choisissez la commande *Distribuer l'installation aux hôtes Windows*. 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** afin de connaître la version de F-Secure Management Agent sur les hôtes.

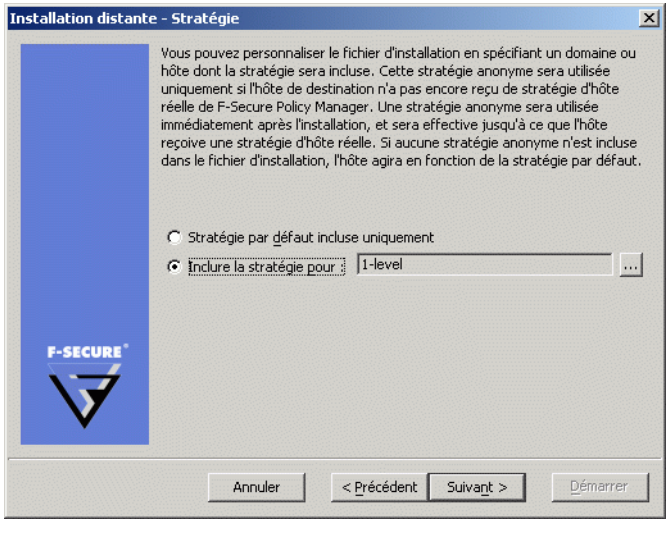


4. Une fois les hôtes de destination sélectionnés, passez à la section “*Installation distante après sélection de l'hôte de destination*”, *141*, où vous trouverez des instructions sur l'installation à distance des applications sur les hôtes.

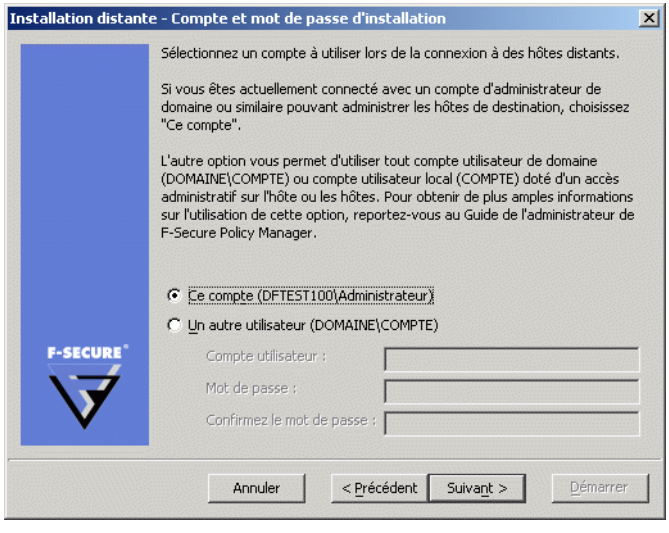
Installation distante après sélection de l'hôte de destination

Pour exécuter à distance des packages d'installation après avoir sélectionné les hôtes de destination :

1. Sélectionnez le package d'installation, puis cliquez sur **Suivant** pour continuer.
2. Sélectionnez les produits à installer. Vous pouvez forcer la réinstallation s’il existe déjà des applications portant le même numéro de version. Cliquez sur **Suivant** pour continuer.
3. Acceptez la stratégie par défaut ou choisissez la stratégie d’hôte ou de domaine à employer comme stratégie anonyme. Cliquez sur **Suivant** pour continuer.



4. Choisissez le compte d'utilisateur et le mot de passe pour l'installation distante.



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.

Sélectionnez soit **Ce compte** (le compte actuel), soit **Un autre utilisateur**.

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

a. Vous êtes déjà connecté en tant qu'administrateur de domaine.
b. 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.

Si vous employez 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.

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, fermez les connexions actives avant de démarrer l'installation distante.

5. Prenez connaissance de la synthèse de l'installation. 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.

6. F-Secure Policy Manager installe F-Secure Management Agent et les produits sélectionnés sur les hôtes. Durant ce processus, la ligne *Etat* affiche l'avancement de la procédure. Vous pouvez à tout moment cliquer sur le bouton **Annuler** pour interrompre l'installation.

   Lorsque la mention *terminé* s'affiche dans la ligne *Etat*, l'opération est terminée. Vous pouvez sélectionner le domaine dans lequel inclure les nouveaux hôtes à l'aide des paramètres d'*importation*. Cliquez sur **Terminer**. F-Secure Policy Manager Console place les nouveaux hôtes dans le domaine sélectionné à l'étape 1, 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'auto-enregistrement et les hôtes peuvent être importés de cette façon.

7. Après quelques minutes, le volet Affichage produit (volet de droite) affiche la liste des produits installés. Pour consulter cette liste, cliquez sur l'onglet *Installation* du volet Propriétés, ou sélectionnez le domaine supérieur du volet*Domaine de stratégie*.

4.4.4 Installation par stratégies

Des fichiers de stratégie de base sont utilisés pour démarrer des installations sur les hôtes où F-Secure Management Agent est déjà installé. F-Secure Policy Manager Console crée un package d'installation spécifique d'une opération, qu'il stocke sur F-Secure 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.

F-Secure Management Agent sur les hôtes récupère les nouvelles stratégies à partir de F-Secure Policy Manager Server et découvre la tâche d'installation. F-Secure Management Agent récupère le package d'installation spécifié dans les paramètres de la tâche à partir du serveur et démarre le programme d'installation.

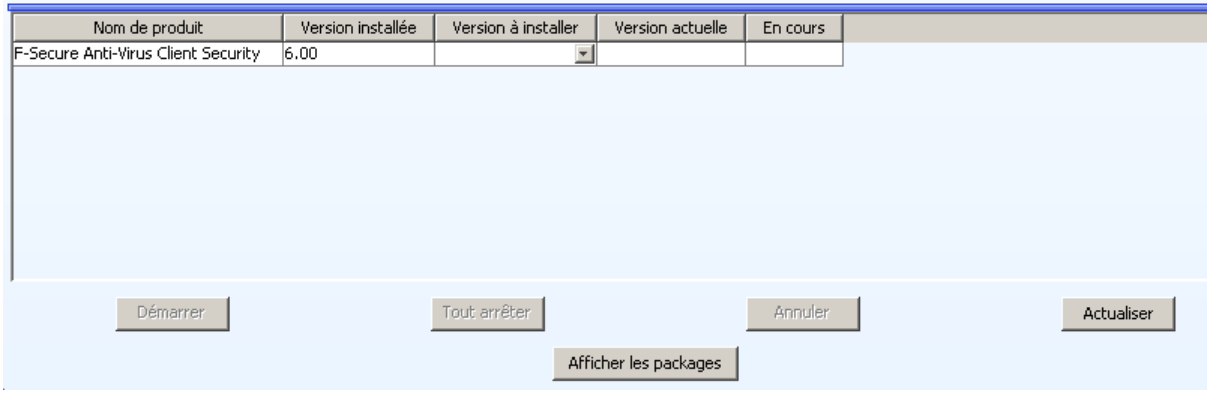
Au terme de l'installation, F-Secure Management Agent envoie le résultat de l'opération au serveur, dans un fichier de stratégie incrémentiel. F-Secure Policy Manager Console découvre les nouvelles informations d'état et affiche les résultats.

La désinstallation s'effectue à l'aide des mêmes mécanismes de remise.

Utilisation de l'éditeur d'installation

L'éditeur d'installation doit être utilisé sur les hôtes sur lesquels F-Secure Management Agent installed. Pour accéder à cet éditeur, cliquez sur l'onglet Stratégie du volet Propriétés, puis sélectionnez le nœud racine (l'arborescence secondaire F-Secure). Alternativement, vous pouvez cliquer sur l'onglet *Installer* du volet Propriétés. L'Editeur d'installation s'affiche dans le volet *Affichage produit*.

Dans l'Editeur d'installation, l'administrateur sélectionne les produits à installer sur l'hôte ou le domaine de stratégie actuellement sélectionné.



L'éditeur 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 — Avancement de l'installation. Cette zone affiche des informations différentes pour les hôtes et pour les domaines.

Lorsqu'un hôte est sélectionné, la zone *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 de la zone En cours pour afficher des informations d'état détaillées.
Terminé	L'installation ou la désinstallation est achevée. Ce message disparaît lorsque vous fermez l'éditeur d'installation.
(Zone vide)	Aucune opération n'est en cours. La zone *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 ont 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 zone *Version installée* affiche le numéro de version des produits actuellement installés.

Lorsque tous les numéros de version requis sont sélectionnés, cliquez sur **Démarrer**. L'éditeur d'installation démarre alors l'Assistant d'installation, qui invite l'utilisateur à configurer les paramètres de

l'installation. L'éditeur d'installation prépare ensuite un package personnalisé de distribution de l'installation pour chaque opération d'installation. Le nouveau package est enregistré sur F-Secure Policy Manager Server.

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

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 hôtes* dans la boîte de dialogue de confirmation.

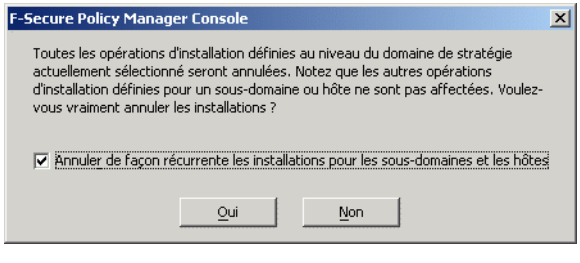


Figure 4-7 Boîte de dialogue de confirmation d'annulation d'installation

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. Le bouton **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'éditeur 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.

F-Secure Management Agent

Lors de l’installation de F-Secure Management Agent, aucune information sur les statistiques indiquant que la désinstallation a réussi n’est envoyée car F-Secure Management Agent a été supprimé et ne peut pas envoyer d’informations.

Si vous désinstallez par exemple F-Secure Anti-Virus et F-Secure Management Agent :

1. Désinstaller F-Secure Anti-Virus
2. Attendez que F-Secure Policy Manager Console signale le succès ou l'échec de la désinstallation.
3. Si F-Secure Anti-Virus a été désinstallé avec succès, désinstallez F-Secure Management Agent.

4. Si la désinstallation de F-Secure Management Agent a échoué, F-Secure 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 F-Secure Management Agent contenant la mention “en cours…”.

4.4.5 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.

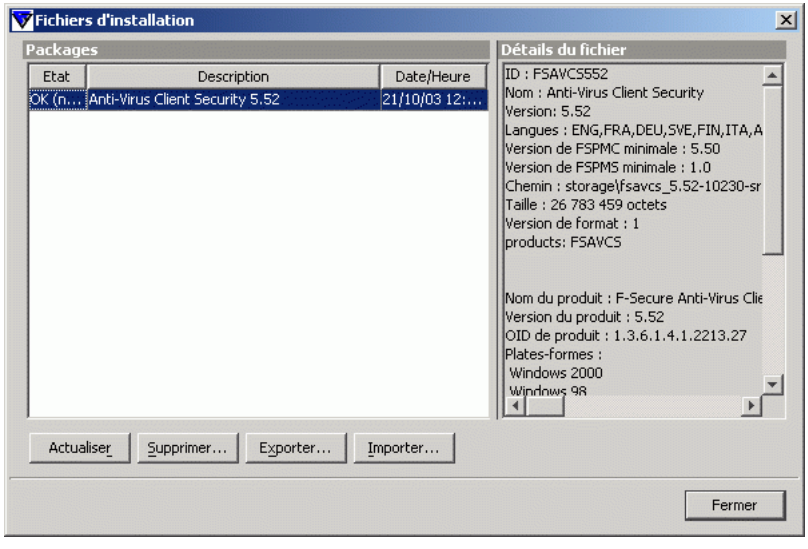
La procédure d'exportation dans les deux formats est la même (voir ci-dessous). Vous pouvez sélectionner le format de fichier pour le package personnalisé dans la boîte de dialogue *Exporter le package d'installation* (voir l'étape 4, ci-dessous).

Script de connexion sur les plates-formes Windows

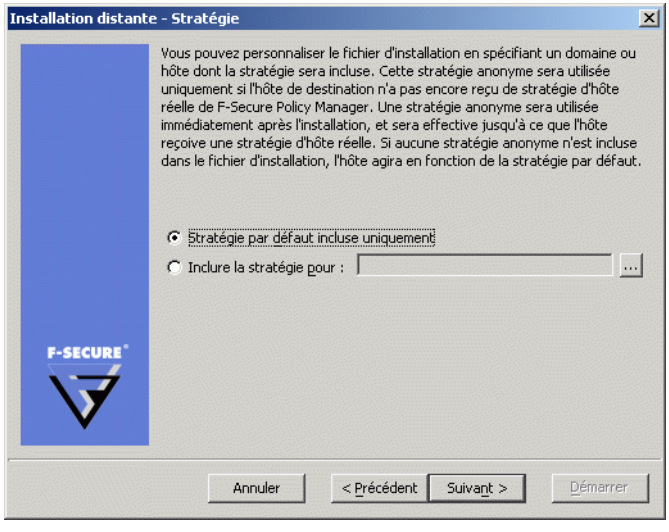
Il existe trois méthodes : utilisation d'un package JAR d'installation à distance personnalisé, utilisation d'un package MSI personnalisé ou utilisation de l'approche non-JAR.

Utilisation du package JAR d'installation distante personnalisé

1. Exécutez F-Secure Policy Manager Console.
2. Choisissez *Packages d'installation* dans le menu *Outils*. La boîte de dialogue *Packages d'installation* s'affiche.

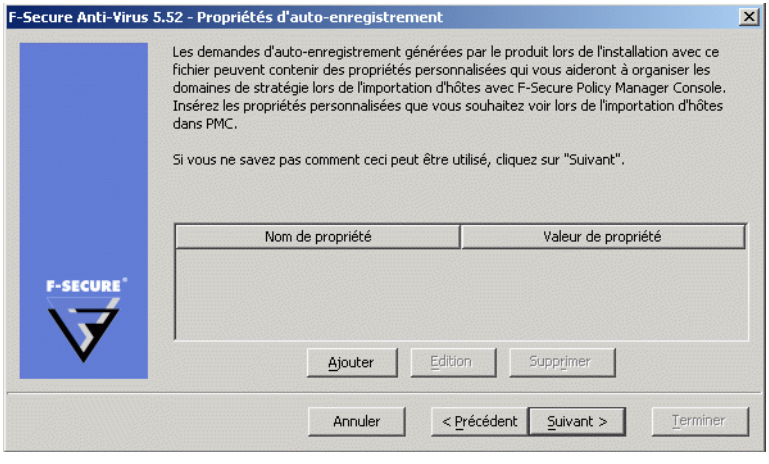


3. Sélectionnez le package d'installation contenant les produits à installer, puis cliquez sur **Exporter**.
4. Spécifiez le format de fichier, *JAR* ou *MSI*, et l'emplacement où vous souhaitez enregistrer le package d'installation personnalisé. Cliquez sur **Exporter**.
5. Sélectionnez les produits à installer (F-Secure Management Agent sera installé par défaut). Cliquez sur **Suivant** pour continuer.
6. Acceptez la stratégie par défaut ou choisissez la stratégie d'hôte ou de domaine à employer comme stratégie anonyme. Cliquez sur **Suivant** pour continuer.



7. Une page récapitulative présente les options choisies pour l'installation. Prenez-en connaissance, puis cliquez sur **Démarrer** pour accéder à l'Assistant d'installation.
8. F-Secure Policy Manager Console affiche l'Assistant d'installation distante qui collecte toutes les informations d'installation nécessaires pour les produits sélectionnés.
   a. Lisez l'écran d'accueil de l'Assistant d'installation distante.
   b. Entrez le code du produit que vous allez installer.
   c. Sélectionnez les composants à installer.
   d. Entrez la langue du produit que vous allez installer.
   e. 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.
   f. Entrez l'adresse de F-Secure Policy Manager Server.
   g. Vous pouvez inclure autant de propriétés d'auto-enregistrement personnalisées que vous le voulez dans le fichier d'installation. Un hôte ajoute ces propriétés personnalisées au message d'auto-enregistrement qu'il envoie à F-Secure Policy Manager après l'installation locale. Ces 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.

h. Sélectionnez l'action à exécuter si un logiciel entrant en conflit est détecté lors de l'installation. Il est conseillé de sélectionner l'option *Désinstaller les produits conflictuels*.

i. Si vous avez sélectionné 'Prise en charge Cisco NAC' à installer à l'étape précédente, la boîte de dialogue *Sélection d'un certificat de serveur Cisco AAA* s'affiche. Entrez le chemin d'accès au certificat de serveur Cisco AAA.

j. Si un redémarrage s'impose après l'installation sur des ordinateurs, précisez la façon dont il doit avoir lieu.

9. Lorsque vous atteignez la dernière page de l'assistant, cliquez sur **Terminer** pour continuer.

10. 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 le répertoire*...\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 F-Secure Management Agent est déjà installé.

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

Fourniture du nom d'utilisateur et du mot de passe pour une installation par script de connexion

Lorsque vous effectuez une installation sur Windows2000 (ou version plus récente), vous pouvez également utiliser les paramètres suivants :

`/user:domaine\nom_utilisateur` (variante : `/user:nom_utilisateur`) — Spécifie le compte utilisateur et le nom de domaine. Le nom de domaine est facultatif.

`/password:secret` (variante : `/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, Ilaunchr démarre le programme d'installation.

Exemple de la commande :

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

Sans utilisation du fichier JAR

1. Copiez les fichiers d'installation appropriés dans un répertoire d'installation (les fichiers d'installation se trouvent dans le répertoire *software*\<*application*>\ du CD-ROM, par exemple les fichiers de F-Secure Client Security 6.0 se trouvent dans le répertoire *software**fsavcs*\.
2. Copiez le fichier *admin.pub* dans le répertoire d'installation indiqué ci-dessus.

3. Modifiez le fichier *prodsett.ini*. Ce fichier indique au programme d'installation les modules à installer, ainsi que le répertoire dans lequel ceux-ci doivent être installés (répertoire de destination) sur les postes de travail. Pour plus d'informations sur la modification du fichier *Prodsett.ini*, voir "*Modification de PRODSETT.INI*", *301*.
4. Ajoutez la ligne suivante au script d'ouverture de session :

   `setup.exe\silent /checkFSMA`

   Si le paramètre `/checkFSMA` n'est pas utilisé, l'installation s'exécute chaque fois que *runsetup.exe* est exécuté.

4.5 Installation locale

Cette section comporte la configuration requise pour F-Secure Client Security ainsi que des informations sur la fourniture d'une copie du fichier de clé *Admin.pub* sur les stations de travail.

4.5.1 Configuration système requise pour l'installation locale

Pour installer F-Secure Client Security, votre système doit être doté de la configuration minimale suivante :

Processeur :	Intel Pentium III 600 Mhz ou supérieur (1 Ghz ou supérieur recommandé)
Système d'exploitation :	Microsoft Windows 2000 Professionnel, SP 4 Microsoft Windows XP Édition familiale/ Professionnel (SP 2 requis pour un bon fonctionnement)
Mémoire :	256 Mo de RAM (512 Mo recommandé)
Espace disque requis :	150 Mo (200 Mo recommandé)

4.5.2 Instructions d’installation

Les instructions d'installation de F-Secure Client Security se trouvent dans le *Guide de mise en route de F-Secure Client Security* .

Fourniture d'une copie du fichier de clé Admin.pub aux postes de travail

Lorsque vous configurez les postes 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 les produits F-Secure sur les stations de travail à distance à l'aide de F-Secure 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 clé *Admin.pub* sur les stations 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 à l'aide de produits F-Secure administrés à distance. Par défaut, F-Secure Policy Manager Console place la clé publique dans la racine du répertoire de communication.
- Le répertoire où sont stockés les fichiers de clé publique et clé privée de l'administrateur a été défini lors de l'installation. Pour plus d'informations, reportez-vous à la section *Etape 17.* , 43.

Pour plus d'informations sur la sauvegarde de la clé *admin.pub*, reportez-vous au chapitre Maintenance de F-Secure Policy Manager Server dans le *Guide de l'administrateur F-Secure Policy Manager*.

4.6 Installation sur un hôte infecté

Si l'hôte sur lequel vous allez installer F-Secure 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. En effet, l'outil d'installation llaunchr.exe ne peut pas fonctionner sur un ordinateur infecté par Klez.

Vous pouvez télécharger l'outil Klez à partir de l'adresse

ftp://ftp.europe.f-secure.com/anti-virus/tools/kleztool.zip

Le fichier 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.

4.7 Comment vérifier que les connexions de gestion fonctionnent

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

5 CONFIGURATION DE LA PROTECTION CONTRE LES VIRUS ET LES LOGICIELS ESPIONS

5.1 Présentation : Objectif de l'utilisation de la protection contre les virus et les logiciels espions

La protection contre les virus et les logiciels espions dans F-Secure Client Security est composée de mises à jour automatiques, d'analyse manuelle, d'analyse programmée, d'analyse en temps réel, de recherche de logiciels espions, de contrôle du système, de recherche de rootkits, d'analyse du courrier électronique, d'analyse du trafic Web, de la gestion des apparitions de nouveaux virus et du service Informations sur les virus. Ce chapitre contient des instructions générales de configuration et quelques exemples de configuration pour chacun de ces services (sauf les informations sur les virus et l'analyse manuelle, lesquelles sont présentées dans la section "*Analyse manuelle*", *72*), ainsi que des instructions concernant la configuration de la transmission d'alertes et le test de la protection antivirus.

L'analyse planifiée est une fonction avancée décrite dans les sections "*Ajout d'une analyse planifiée à partir d'un hôte local*", *247* et "*Configuration d'une analyse planifiée*", *274*.

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 contre les virus et 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 signalés.
- La pièce jointe infectée (dans une analyse du courrier électronique) est nettoyée, supprimée ou bloquée.

Ces actions sont décrites dans les sections "*Paramètres de configuration de l'analyse en temps réel*", *166* et "*Paramètres de configuration de l'analyse du courrier électronique*", *175*.

5.2 Configuration des mises à jour automatiques

Cette section explique les différents paramètres de configuration disponibles pour les mises à jour automatiques dans F-Secure 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.

F-Secure Client Security 5.5x utilise différents paramètres de mises à jour automatiques, auxquels vous pouvez accéder en cliquant sur le lien **Configurer les mises à jour automatiques pour F-Secure Client Security 5.5x**.

5.2.1 Fonctionnement des mises à jour automatiques

L'agent de mise à jour automatique installé avec F-Secure Client Security tente de télécharger les mises à jour automatiques à partir des sources de mises à jour configurées dans l'ordre suivant :

a. Si des proxies Policy Manager sont utilisés dans le réseau de l'entreprise, le client tente de se connecter à F-Secure Policy Manager Server par l'intermédiaire de chaque proxy Policy Manager à tour de rôle.
b. 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 F-Secure Policy Manager Server.
c. Ensuite, le client tente de télécharger les mises à jour directement depuis F-Secure Policy Manager Server.
d. Si des proxies Policy Manager sont utilisés dans le réseau de l'entreprise, le client tente de se connecter au serveur de mise à jour F-Secure par l'intermédiaire de chaque proxy Policy Manager à tour de rôle.
e. 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.
f. Le client tente ensuite de télécharger les mises à jour directement depuis le serveur de mise à jour de F-Secure.

5.2.2 Paramètres de configuration des mises à jour automatiques

Dans la page *Mises à jour automatiques* de l'onglet *Paramètres*, vous pouvez spécifier si vous souhaitez que F-Secure 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*.

Policy Manager Proxy est une liste de serveurs Proxy F-Secure Policy Manager disponibles. L'agent de mise à jour automatique installé avec F-Secure 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*.

5.2.3 Configuration des mises à jour automatique 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 le Policy Manager Server. La configuration s'effectue comme suit :

1. Sélectionnez *Racine* sous 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 souhaitez empêcher les utilisateurs de changer ces paramètres, cliquez sur le symbole de cadenas en regard des paramètres.
7. Cliquez sur  pour enregistrer les données de stratégie.

8. Cliquez sur  pour diffuser la stratégie.

5.2.4 Configuration de Policy Manager Proxy

Proxy F-Secure Policy Manager est un nouveau produit, qu'il ne faut pas confondre avec F-Secure Anti-Virus Proxy. Pour plus d'informations sur Proxy F-Secure Policy Manager, reportez-vous au Guide de l'administrateur de Proxy F-Secure Policy Manager.

Si chaque bureau d'une entreprise a son propre proxy Policy Manager, il est souvent judicieux de configurer les portables que l'utilisateur emporte d'un bureau à l'autre pour qu'ils utilisent un proxy Policy Manager comme source de mise à jour principale. 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 leurs propres serveurs proxy Policy Manager et que tous seront inclus dans la liste des serveurs proxy Policy Manager.

1. Sélectionnez le sous-domaine dans lequel utiliser le Policy Manager 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. La section *Proxies de Policy Manager* contient une liste des serveurs proxy disponibles. Cliquez sur **Ajouter** pour ajouter de nouveaux serveurs à la liste. La fenêtre *Propriétés du serveur Proxy F-Secure Policy Manager* .
5. Entrez un numéro de priorité dans la zone de texte *Priorité* de Policy Manager Proxy. Ces numéros sont utilisés pour définir l'ordre dans lequel les hôtes tentent de se connecter aux proxies Policy Manager. Utilisez, par exemple, 10 pour le proxy Policy Manager situé dans le bureau où l'hôte se trouve normalement et 20, 30 etc. pour les autres proxies.
6. Saisissez l'URL du Proxy F-Secure Policy Manager dans la zone de texte *Adresse du serveur*. Cliquez ensuite sur **OK**.

7. Répétez les étapes 5 et 6 pour ajouter les autres serveurs à la liste.
8. Une fois tous les proxies Policy Manager 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 les données de stratégie.
11. Cliquez sur  pour diffuser la stratégie.

Les utilisateurs finals peuvent également ajouter des proxies Policy Manager 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. Les proxies Policy Manager ajoutés par les utilisateurs finals sont tentés avant ceux ajoutés par l'administrateur

5.3 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.

5.3.1 Paramètres de configuration de l'analyse en temps réel

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

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.

- *Analyser les fichiers compressés*

  Cochez cette case pour analyser les fichiers compressés, tels que les fichiers ZIP, ARJ, LZH, RAR, CAB, TAR, BZ2, GZ, JAR et TGZ. L'analyse de fichiers compressés volumineux sollicite fortement les ressources système et risque donc de ralentir le système. Par conséquent, cette option s'accorde mal avec la protection en temps réel.

- *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 F-Secure Client Security 6.0, 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 lecture ou exécution. Lorsqu'un fichier est ouvert en écriture ou qu'un nouveau fichier est créé, si ce paramètre est activé, le fichier est analysé lors de sa fermeture.

Dans la liste déroulante *Action en cas d'infection*, vous pouvez sélectionner l'action que devra exécuter F-Secure Client Security lors de la détection d'un fichier infecté. Sélectionnez l'une des actions suivantes :

Action	Définition
Interroger l'utilisateur après analyse	Lance l'Assistant de nettoyage F-Secure 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.
Avertir 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.

Action	Définition
Mettre automatiquement en quarantaine	Place automatiquement le fichier infecté en quarantaine.

Traitement des extensions de fichiers

F-Secure 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 F-Secure 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.

Recherche de logiciels espions en temps réel

Pour plus d'informations sur la configuration de la recherche de logiciels espions et pour des exemples cette configuration, reportez-vous à la section “*Configuration de la recherche de logiciels espions*”, *183*.

5.3.2 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* sous l'onglet *Domaines de stratégie*.
2. Accédez à l'onglet *Paramètres* et sélectionnez la page *Analyse en temps réel*.
3. Cochez la case *Analyse en temps réel activée*.
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. Pour plus d'informations sur les autres paramètres d'analyse en temps réel, reportez-vous à la section “*Paramètres de configuration de l'analyse en temps réel*”, *166*.
7. Cliquez sur  pour enregistrer les données de stratégie.
8. Cliquez sur  pour diffuser la stratégie.

5.3.3 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* sous l'onglet *Domaines de stratégie*.
2. Accédez à l'onglet *Paramètres* et sélectionnez la page *Analyse en temps réel*.
3. Cochez la case *Analyse en temps réel activée*.
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. Pour plus d'informations sur les autres paramètres d'analyse en temps réel, reportez-vous à la section “*Configuration de l'analyse en temps réel*”, *166*.

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 les données de stratégie.
9. Cliquez sur  pour diffuser la stratégie.

5.3.4 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* sous 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. Ajoutez 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 les données de stratégie.
7. Cliquez sur  pour diffuser la stratégie.

5.4 Configuration du contrôle du système

Le contrôle du système F-Secure est un nouveau système de prévention des intrusions fondé sur un hôte 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 le contrôle du système est activé, vous pouvez configurer le contrôle des applications de façon à ce qu'il demande aux utilisateurs l'action à effectuer lorsque le contrôle du système n'approuve pas une application.

5.4.1 Paramètres de configuration du contrôle du système

Pour activer le contrôle du système, cochez la case *Activer le contrôle du système*.

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	Le contrôle du système demande aux utilisateurs s'ils souhaitent autoriser ou bloquer les actions surveillées, même lorsque l'application est identifiée comme sûre.

Action	Définition
Demander en cas de doute	Le contrôle du système demande aux utilisateurs s'ils souhaitent autoriser ou bloquer les actions surveillées uniquement si le contrôle du système ne peut pas identifier l'application comme sûre ou non sûre (option par défaut).
Automatique : Ne pas demander	Le contrôle du système bloque les applications non sûres et autorise automatiquement les applications sûres sans poser aucune question à l'utilisateur.

Pour activer la protection ActiveX, cochez la case *Interdire l'exécution de tous les ActiveX*. La protection ActiveX interdit aux navigateurs Web d'exécuter des applications Web ActiveX. Certains sites Web peuvent utiliser ActiveX pour installer des logiciels indésirables sur les ordinateurs. Toutefois, certaines pages Web ne peuvent pas être affichées sans contrôle ActiveX.

La protection ActiveX peut être activée uniquement lorsque le contrôle du système est activé.

5.5 Configuration de la recherche de rootkits

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.

5.5.1 Paramètres de configuration de la recherche de rootkits

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 la Policy Manager Console.

Sélectionnez *Afficher 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.

5.5.2 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* sous 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 *Afficher 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**. Vous devez distribuer la stratégie pour lancer l'opération.

7. Cliquez sur  pour enregistrer les données de stratégie.
8. Cliquez sur  pour diffuser la stratégie.
9. Une fois la recherche terminée sur les hôtes locaux, vous pouvez afficher les rapports d'analyse de l'onglet *Rapports* afin de voir si des rootkits ont été détectés.

5.6 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 mail local. Tous les fichiers envoyés sont traités par l'analyse en temps réel.

5.6.1 Paramètres de configuration de l'analyse du courrier électronique

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

Pour activer l'analyse des messages électroniques sortants et des pièces jointes (trafic SMTP), cochez la case *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 pièce jointe* supprime la pièce jointe.
   - *Avertir uniquement* ignore la pièce jointe mais la 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 message 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 la pièce jointe mais la 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 finals, cochez la case *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 options suivantes sont disponibles pour la sélection des éléments à analyser :

- *Toutes les pièces jointes*

  Toutes les pièces jointes sont analysées, quelle que soit leur extension.

- *Pièces jointes avec ces extensions :*

  Seules les pièces jointes portant les extensions définies sont analysées. 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.

- *Analyser les fichiers compressés*

  Cochez cette case pour analyser les pièces jointes compressées, tels que les fichiers ZIP, ARJ, LZH, RAR, CAB, TAR, BZ2, GZ, JAR et TGZ. L'analyse de pièces jointes compressées volumineuses sollicite de nombreuses ressources système et risque donc de ralentir le système.

- *Activer les extensions exclues*

  Vous pouvez spécifier les pièces jointes à ne pas analyser en entrant les extensions de fichier appropriées dans le champ *Extensions exclues*. Reportez-vous également à la section “*Traitement des extensions de fichiers*”, *169*.

Si vous souhaitez qu'une boîte de dialogue s'affiche lorsque des fichiers volumineux sont analysés, cochez la case *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, cochez la case *Afficher le rapport si des infections sont détectées*.

Pour plus d'informations sur les messages d'alerte virale et d'erreur d'analyse qui peuvent s'afficher sur l'écran des utilisateurs finals lorsque l'analyse du courrier électronique est activée, reportez-vous à la section "*Messages d'alerte et d'erreur de l'analyse du courrier électronique*", *321*

5.6.2 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.

Etape 1.

1. Sélectionnez *Racine* sous l'onglet *Domaines de stratégie*.
2. Accédez à l'onglet *Paramètres* et sélectionnez la page *Analyse du courrier électronique*.

Etape 2. Configuration de l'analyse du courrier électronique entrant

1. Sélectionnez *Activer l'analyse du courrier entrant*.
2. Sélectionnez l'action à exécuter dans la liste déroulante *Action à la réception d'une pièce jointe infectée*. Pour obtenir des explications sur les différentes actions, reportez-vous à la section "*Paramètres de configuration de l'analyse du courrier électronique*", *175*.
3. Sélectionnez l'action à exécuter dans la liste déroulante *Action en cas d'échec de l'analyse*.
4. Sélectionnez l'action à exécuter dans la liste déroulante *Action si des parties de messages sont déformées*.

Etape 3. Configuration de l'analyse du courrier électronique sortant

1. Sélectionnez *Activer l'analyse du courrier sortant*.
2. Sélectionnez l'action à exécuter dans la liste déroulante *Action à la réception d'une pièce jointe infectée*.
3. Sélectionnez l'action à exécuter dans la liste déroulante *Action en cas d'échec de l'analyse*.
4. Sélectionnez l'action à exécuter dans la liste déroulante *Action si des parties de messages sont déformées*.

Etape 4. Vérification des paramètres généraux

Vérifiez que les autres paramètres de cette page conviennent pour votre système et modifiez-les au besoin. Pour plus d'informations sur les autres paramètres d'analyse e-mail, reportez-vous à la section "*Configuration de l'analyse du courrier électronique*", *175*.

Etape 5.

1. Cliquez sur  pour enregistrer les données de stratégie.
2. Cliquez sur  pour diffuser la stratégie.

5.7 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.

5.7.1 Paramètres de configuration de l'analyse HTTP

Pour activer l'analyse HTTP, cochez la case *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 options 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 options disponibles sont les suivantes :

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

Cochez la case *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 serveurs approuvés dans la table Sites HTTP approuvés. Le contenu des sites approuvés ne sera pas analysé à la recherche de virus.

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

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

1. Sélectionnez *Racine* sous 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. Vérifiez 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 les données de stratégie.
8. Cliquez sur  pour diffuser la stratégie.

5.7.3 Exclusion d'un site Web de l'analyse HTTP

Vous pouvez exclure un site 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.

Etape 1.

1. Sélectionnez *Racine* sous l'onglet *Domaines de stratégie*.
2. Accédez à l'onglet *Paramètres* et sélectionnez la page *Analyse du trafic Web*.

Etape 2. Exclusion d'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 manière suivante :

1. Cliquez sur le bouton **Ajouter** sous la table *Sites approuvés* . Vous créez ainsi une nouvelle ligne dans la table.
2. Cliquez sur la ligne que vous venez de créer afin qu'elle devienne active et tapez *http://*.example.com/**

   Vous excluez ainsi tous les sous-domaines.
3. Cliquez sur le bouton **Ajouter** sous la table *Sites approuvés* . Vous créez ainsi une ligne dans la table.
4. Cliquez sur la ligne que vous venez de créer afin qu'elle devienne active et tapez http://example.com/*

   Vous excluez ainsi le domaine de second niveau.

Etape 3. Exclusion d'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 :

1. Cliquez sur le bouton **Ajouter** sous la table *Sites approuvés* . Vous créez ainsi une nouvelle ligne dans la table.
2. Cliquez sur la ligne que vous venez de créer afin qu'elle devienne active, et tapez *http://www.example2.com/news/**

Etape 4.

1. Cliquez sur  pour enregistrer les données de stratégie.
2. Cliquez sur  pour diffuser la stratégie.

5.8 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 de F-Secure 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.

5.8.1 Paramètres de contrôle des logiciels espions

Recherche de logiciels lors d'accès aux fichiers

Pour activer la recherche de logiciels espions en temps réel, cochez la case *Rechercher des logiciels espions*.

Dans la liste déroulante *Action en cas d'infection*, vous pouvez sélectionner l'action à prendre si du logiciel espion est détecté. Sélectionnez l'une des actions suivantes :

Action	Définition
Avertir uniquement	Le logiciel espion est uniquement signalé, aucune action n'est effectuée.
Interroger l'utilisateur après analyse	L'utilisateur est invité à indiquer ce qu'il souhaite faire avec le logiciel espion.
	Une remarque au sujet de l'option Interroger l'utilisateur après analyse : *Si Afficher des alertes aux utilisateurs a la valeur Afficher en mode autonome seulement, et si l'hôte fait l'objet d'une gestion centralisée, le logiciel espion est uniquement signalé à l'administrateur. L'utilisateur n'est pas interrogé sur le logiciel espion.*
Supprimer automatiquement	Le logiciel espion est supprimé automatiquement.
Mettre en quarantaine automatiquement	Le logiciel espion est mis en quarantaine.
	Il est déconseillé de supprimer ou de mettre en quarantaine les logiciels espions automatiquement. Reportez-vous à la section "Remarque à propos du nettoyage des logiciels espions et des riskwares", 183.

Pour empêcher les utilisateurs d'accéder à du logiciel espion mis en quarantaine, cochez la case *Refuser l'accès aux logiciels espions*. Notez que l'accès aux logiciels espions détectés est interdit par défaut.

Dans *Afficher des alertes aux utilisateurs*, vous pouvez choisir si les dialogues de détection des logiciels espions trouvés sont affichés aux utilisateurs. Les options sont :

- *Afficher en mode autonome seulement* - Dans les environnements gérés de manière centralisée, les dialogues de détection des logiciels espions détectés par l'analyse en temps réel ne sont pas présentés.
- *Toujours afficher*- Les dialogues de détection des logiciels espions détectés par l'analyse en temps réel sont toujours présentés à l'utilisateur.

Le lien **Configurer d'autres options de recherche de logiciels espions en mode avancé** donne accès à l'interface utilisateur en mode avancé de F-Secure Policy Manager Console, où d'autres options de recherche de logiciels espions peuvent être configurées.

Recherche manuelle de logiciels espions

Pour activer la recherche manuelle de logiciels espions, cochez la case Rechercher les logiciels espions pendant la recherche manuelle de virus.

Dans la liste déroulante *Action en cas d'infection*, vous pouvez sélectionner l'action à prendre si du logiciel espion est détecté. Sélectionnez l'une des actions suivantes :

Action	Définition
Avertir uniquement	Le logiciel espion est uniquement signalé, aucune action n'est effectuée.
Interroger l'utilisateur après analyse	L'utilisateur est invité à indiquer ce qu'il souhaite faire avec le logiciel espion.
Supprimer automatiquement	Le logiciel espion est supprimé automatiquement.
Mettre en quarantaine automatiquement	Le logiciel espion est mis en quarantaine.

Le paramètre Afficher des alertes aux utilisateurs sur la page Analyse en temps réel n'a pas d'effet sur la recherche manuelle de logiciels espions.

Le lien **Configurer les cibles de recherche manuelle de logiciels espions en mode avancé** vous donne accès à l'interface utilisateur en mode avancé de F-Secure Policy Manager Console, où vous pouvez configurer les cibles de recherche manuelle de logiciels espions.

Applications exclues de la recherche manuelle

Cette table affiche les logiciels espions et riskwares qui ont été autorisés par l'administrateur.

Logiciels espions et riskwares rapportés par les hôtes

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.
Etat du logiciel espion	Affiche l'état actuel de l'élément de logiciel espion. Les états sont les suivants : *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.

Logiciels espions et riskwares rapportés par les hôtes	
	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.

Traitement par défaut du logiciel espion

Si le paramètre *Modifier la recherche de logiciels espions pour mettre automatiquement en quarantaine tous les nouveaux logiciels espions* est sélectionné, tous les nouveaux logiciels espions qui ne sont pas explicitement autorisés par l'administrateur sont automatiquement mis en quarantaine. Cela s'applique à la recherche manuelle et en temps réel de logiciels espions. Cela change les paramètres suivants :

- Dans la section *Recherche de logiciels lors d'accès aux fichiers*, le paramètre *Action sur les logiciels espions* prend la valeur *Supprimer automatiquement et mettre en quarantaine*.
- Dans la section *Recherche manuelle de logiciels espions*, le paramètre *Action sur les logiciels espions* devient *Supprimer automatiquement et mettre en quarantaine*.
- Dans la page *Contrôle des logiciels espions*, le paramètre *Refuser l'accès aux logiciels espions* est activé.

*Cliquez sur le lien **Modifier la recherche de logiciels espions pour mettre automatiquement en quarantaine tous les nouveaux logiciels espions** lorsque vous êtes certain que l'interdiction des logiciels espions n'aura pas d'incidence sur les applications ordinaires et illégitimes dans votre entreprise.*

5.8.2 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 logiciels de dialogue en direct (IRC) ou de transfert des 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*.

Etape 1. Création d'un domaine de test et activation de la recherche de logiciels espions

1. Créez un environnement de test avec quelques ordinateurs où tournent les programmes normalement utilisés dans votre entreprise.
2. Importez ces hôtes dans le domaine géré de manière centralisée.
3. Accédez à l'onglet *Paramètres* et sélectionnez la page *Analyse en temps réel*. Activez la recherche de logiciels espions sur les hôtes en sélectionnant *Rechercher des logiciels espions* dans la section *Recherche de logiciels lors d'accès aux fichiers*.

Vous pouvez également lancer une recherche manuelle de logiciels espions sur les hôtes.

4. Cliquez sur  pour enregistrer les données de stratégie.
5. Cliquez sur  pour diffuser la stratégie.

Etape 2. Vérifiez les logiciels espions et riskwares trouvés

1. 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*. Vérifiez la liste des logiciels espions et riskwares signalés. Si des applications sont nécessaires dans votre entreprise, sélectionnez-les dans le tableau et cliquez sur **Autoriser l'application**.
2. Une boîte de dialogue vous invitant à confirmer l'action s'ouvre. 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**.
3. L'application sélectionnée sera placée dans le tableau *Applications exclues de la recherche de logiciels espions*.

Etape 3. Modification de la configuration de la recherche de logiciels espions pour prévoir une mise en quarantaine automatique

Configurez les paramètres *Traitement par défaut des logiciels espions* :

1. 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 l'option *Permettre aux utilisateurs d'autoriser les logiciels espions* a la valeur to *Non autorisé*.
2. Configurez la recherche de logiciels espions de manière à prévoir la mise en quarantaine automatique de tous les logiciels espions détectés en cliquant sur le lien **Modifier la recherche de logiciels espions pour mettre automatiquement en quarantaine tous les nouveaux logiciels espions**. Cliquez sur **Oui** dans la boîte de dialogue de confirmation.

3. Vérifiez que les paramètres de recherche de logiciels espions en temps réel sont valides pour le domaine géré. Ils se trouvent dans la section *Recherche de logiciels lors d'accès aux fichiers*.
4. Vérifiez que les paramètres de recherche manuelle de logiciels espions sont valides pour le domaine géré. Ils se trouvent dans la section *Recherche manuelle de logiciels espions*.

Etape 4. Distribution de la stratégie

Distribuez une stratégie incluant les paramètres de traitement des logiciels espions dans l'ensemble du domaine :

1. Cliquez sur  pour enregistrer les données de stratégie.
2. Cliquez sur  pour diffuser la stratégie.

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

Dans cet exemple, une recherche de logiciels espions est lancée dans l'ensemble du domaine. Cette intervention nettoie partiellement la table *Logiciels espions et riskwares signalés par les hôtes*.

1. Sélectionnez *Racine* sous l'onglet *Domaines de stratégie*.
2. Accédez à l'onglet *Paramètres* et sélectionnez la page *Analyse manuelle*.
3. Dans la section *Recherche manuelle de logiciels espions* , sélectionnez *Rechercher les logiciels espions pendant la recherche manuelle de virus*.
4. Comme la tâche d'analyse manuelle inclut également la recherche manuelle de virus, vérifiez les paramètres dans la section *Recherche manuelle de virus*, est modifiez-les si nécessaire.
5. Accédez à l'onglet *Opérations* et cliquez sur le bouton **Recherche de virus et de logiciels espions**. Vous devez distribuer la stratégie pour lancer l'opération.
6. Cliquez sur  pour enregistrer les données de stratégie.

7. Cliquez sur  pour diffuser la stratégie.

5.8.4 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 ou de riskwares.
2. Accédez à l'onglet *Paramètres* et sélectionnez la page *Contrôle des tels logiciels espions*.
3. Sélectionnez le composant de logiciel espion dont vous souhaitez autoriser l'utilisation dans la table *Logiciels espions et riskwares signalés par les hôtes*, puis cliquez sur **Autoriser l'application**.
4. Une boîte de dialogue vous invitant à confirmer l'action s'ouvre. 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**.
5. L'application sélectionnée sera placée dans le tableau *Applications exclues de la recherche de logiciels espions*.
6. Cliquez sur  pour enregistrer les données de stratégie.
7. Cliquez sur  pour diffuser la stratégie.

5.9 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 finals. 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 une des pages de l'onglet *Paramètres*, vous pouvez définir tous les paramètres comme finals 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 finals 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 marque également comme finals les paramètres du mode avancé.

5.9.1 Marquage de tous les paramètres de protection antivirus comme finals

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

1. Sélectionnez *Racine* sous l'onglet *Domaines de stratégie*.
2. Accédez à l'onglet *Paramètres* et sélectionnez la page *Gestion centralisée*.
3. Sélectionnez l'onglet *Paramètres* et sélectionnez la page *Mises à jour de définitions de virus*.

4. Vérifiez que tous les paramètres de cette page sont corrects. Cliquez sur Interdire les modifications utilisateur. Tous les paramètres de cette page sont maintenant marqués comme finals.
5. Sélectionnez la page *Analyse en temps réel*.
6. Vérifiez que tous les paramètres de cette page sont corrects. Cliquez ensuite sur Interdire les modifications utilisateur.
7. Sélectionnez la page *Analyse manuelle*.
8. Vérifiez que tous les paramètres de cette page sont corrects. Cliquez ensuite sur Interdire les modifications utilisateur.
9. Sélectionnez la page *Analyse du courrier électronique*.
10. Vérifiez que tous les paramètres de cette page sont corrects. Cliquez ensuite sur Interdire les modifications utilisateur.
11. Cliquez sur  pour enregistrer les données de stratégie.
12. Cliquez sur  pour diffuser la stratégie.

5.10 Configuration d'envoi d'alertes de F-Secure Client Security

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

5.10.1 Configuration de F-Secure Client Security pour prévoir l'envoi d'alertes de virus à une adresse électronique

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

Etape 1.

1. Sélectionnez *Racine* sous l'onglet *Domaines de stratégie*.
2. Accédez à l'onglet *Paramètres* et sélectionnez la page *Envoi d'alertes*.

Etape 2. 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 :

1. Entrez l'adresse du serveur SMTP dans le champ *Adresse du serveur de courrier électronique (SMTP)*.

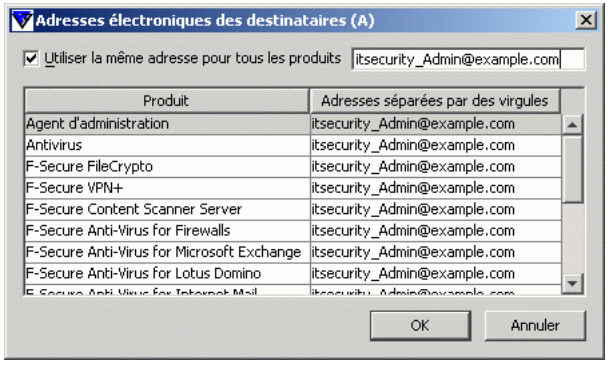
   Utilisez le format suivant :

   <hôte>[:<port>] où « hôte » est le nom DNS ou l'adresse IP du serveur SMTP et « port » le numéro de port du serveur SMTP.
2. Entrez l'adresse de l'expéditeur pour les messages d'alerte par courrier électronique dans le champ *Adresse de l'émetteur du courrier électronique (De) :* .
3. 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.

Etape 3. Configuration de la transmission des alertes par courrier électronique

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

1. Cochez la case *Adresse électronique* sur la ligne *Alerte de sécurité*. La boîte de dialogue *Adresses électroniques des destinataires (A)* s'ouvre.



2. Cochez la case *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. Une fois terminé, cliquez sur **OK**.
3. Cliquez sur pour enregistrer les données de stratégie.
4. Cliquez sur pour diffuser la stratégie.

5.10.2 Désactivation des fenêtres indépendantes d'alerte de F-Secure Client Security

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

1. Sélectionnez *Racine* sous l'onglet *Domaines de stratégie*.
2. Accédez à l'onglet *Paramètres* et sélectionnez la page *Envoi d'alertes*.
3. Désactivez les cases à cocher pour tous les produits dans la colonne *Interface utilisateur locale*.

4. Cliquez sur  pour enregistrer les données de stratégie.
5. Cliquez sur  pour diffuser la stratégie.

5.11 Surveillance des virus sur le 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 le lien 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.

5.12 Test de la protection antivirus

Pour tester le bon fonctionnement de F-Secure Client Security, vous pouvez utiliser un fichier de test spécial qui est détecté par F-Secure 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 utiliser le fichier EICAR pour tester votre analyse du 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 F-Secure 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.

6 CONFIGURATION DE LA PROTECTION INTERNET

6.1 Présentation : Objectif de l'utilisation de la protection Internet

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. Elle 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. Pour obtenir des explications détaillées sur les différents niveaux de sécurité, reportez-vous à la section “*Niveaux de sécurité globale de pare-feu*”, *201*.

6.1.1 Niveaux de sécurité globale de pare-feu

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

Quarantaine réseau	Si la fonction Quarantaine réseau est activée, ce niveau de sécurité est automatiquement sélectionné lorsque les critères de quarantaine réseau sur l'hôte sont remplis. Pour plus d'informations, reportez-vous à la section "*Configuration de la quarantaine réseau*", *210*. Ce niveau de sécurité permet le téléchargement de mises à jour automatiques et des connexions à F-Secure 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.
Normal	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.

6.1.2 Principes d'élaboration des niveaux de sécurité

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 la table *Niveaux de sécurité du pare-feu*. Les règles dans la table *Niveaux de sécurité du pare-feu* sont lues 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. Cela réduit les risques en matière de sécurité. 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.

6.2 Configuration des niveaux et règles de sécurité de la protection Internet

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 la structure du domaine créée au chapitre 4, ce qui signifie que, 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.*

6.2.1 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. Sélectionnez l'onglet *Paramètres* et sélectionnez la fenêtre *Niveaux de sécurité du pare-feu*. Le niveau de sécurité par défaut actuellement inclus dans la stratégie apparaît dans la liste déroulante *Niveau de sécurité de protection Internet sur l'hôte*.

3. Sélectionnez le niveau de sécurité *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 les données de stratégie.
6. Cliquez sur  pour diffuser 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*.

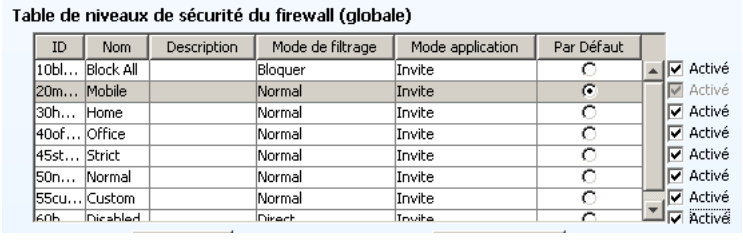
Si le niveau de sécurité sélectionné ne peut pas être utilisé pour une raison quelconque, celui par défaut est utilisé à la place. Le niveau de sécurité par défaut actuel est indiqué dans la table Niveaux de sécurité globale de la page Niveaux de sécurité du pare-feu.

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

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.* dans 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*.



4. Policy Manager vous invite à confirmer le changement de niveau de sécurité pour tous les hôtes gérés. Cliquez sur **OK**.
5. Cliquez sur pour enregistrer les données de stratégie.
6. Cliquez sur pour diffuser la stratégie.

6.2.3 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. La procédure est la suivante :

Etape 1. Création d'un niveau de sécurité

1. Sélectionnez *Racine* sous l'onglet *Domaines de stratégie*.
2. Accédez à l'onglet *Paramètres* et sélectionnez la page *Niveaux de sécurité du pare-feu*.
3. Cliquez sur **Ajouter** pour ajouter un nouveau 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* . Cliquez sur **Terminer**.
5. Cliquez sur  pour enregistrer les données de stratégie.
6. Cliquez sur  pour diffuser la stratégie.

Etape 2. Création de règles pour le nouveau niveau de sécurité

Les options disponibles dans l'Assistant Règle utilisé dans cette étape sont expliquées plus en détail dans la section "Ajout d'une nouvelle règle de la protection Internet avec alerte", 212

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* que vous venez de créer. 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 *Assistant Règles de pare-feu* s'ouvre.
4. Dans la fenêtre *Type de règle*, sélectionnez *Autoriser*.
5. Dans la fenêtre *Hôtes distants*, sélectionnez *Tout hôte distant* pour appliquer la règle à toutes les connexions Internet.
6. Dans la fenêtre *Services*, sélectionnez :
   - *HTTP* dans la colonne *Service* pour appliquer la règle au trafic HTTP ;
   - => dans la colonne *Direction* pour appliquer la règle aux connexions sortantes uniquement.
7. Dans la fenêtre *Paramètres avancés*, vous pouvez accepter les valeurs par défaut.

8. Vérifiez la nouvelle règle dans la fenêtre *Résumé*. Vous pouvez également ajouter un commentaire décrivant la règle, par exemple "*Autorisation du trafic HTTP sortant pour la navigation.*". Cliquez sur **Terminer**.
9. Cliquez sur **Ajouter après** pour ajouter en fin de liste une règle interdisant tout autre trafic dans les deux sens.
10. Dans la fenêtre *Type de règle*, sélectionnez *Refuser*.
11. Dans la fenêtre *Hôtes distants*, sélectionnez *Tout hôte distant* pour appliquer la règle à toutes les connexions.
12. Dans la fenêtre *Services*, sélectionnez :
    - *Tout le trafic* dans la colonne *Service* pour appliquer la règle à tout le trafic ;
    - *Les deux* dans la colonne *Direction* pour appliquer la règle aux connexions entrantes et sortantes.
13. Dans la fenêtre *Paramètres avancés*, vous pouvez accepter les valeurs par défaut.
14. Vérifiez la nouvelle règle dans la fenêtre *Résumé*. Vous pouvez également ajouter un commentaire décrivant la règle. Par exemple, "Refuser le reste". Cliquez sur **Terminer**.

Etape 3. Mise en application du 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 *Racine* avant de l'activer à un niveau inférieur de la hiérarchie des domaines de stratégie. La procédure est la suivante :

1. Sélectionnez *Racine* sous 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 table *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 les données de stratégie.
8. Cliquez sur  pour diffuser la stratégie.

6.3 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. Leurs droits d'accès normaux 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 (reportez-vous à la section “*Réglage de la quarantaine réseau*”, *211*).

6.3.1 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 de désactiver la quarantaine réseau.
- Spécifiez 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.

6.3.2 Activation de la quarantaine réseau à l'échelle du domaine

Pour activer la quarantaine réseau dans l'ensemble du domaine, procédez comme suit :

1. Sélectionnez Racine sous 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 l'*Age des définitions de virus pour activer 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 les données de stratégie.
7. Cliquez sur  pour diffuser la stratégie.

6.3.3 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.

6.4 Configuration des alertes de règle de la protection Internet

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.

6.4.1 Ajout d'une nouvelle règle de la protection Internet avec alerte

Dans cet exemple, une règle *Refuser* avec alerte est créée pour le trafic ICMP sortant pour un sous-domaine particulier. Lorsque quelqu'un tente d'envoyer une commande ping à l'ordinateur, une alerte est émise. À 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.

Etape 1.

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. La fenêtre *Assistant Règles de pare-feu* s'ouvre.

Etape 2. Type de règle

Sélectionnez *Refuser* pour refuser les connexions ICMP entrantes.

Etape 3. Spécification des hôtes concernés

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 le champ de texte situé 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*.

Etape 4. Choix du service refusé et de 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*.

Etape 5. Définition des options avancées

1. Précisez si la règle s'applique uniquement lorsqu'une liaison à distance est ouverte en activant ou en désactivant la case à cocher.
2. Sélectionnez le type d'alerte dans la liste déroulante *Envoyer une alerte*. Pour cette règle, sélectionnez *Alerte de sécurité*.
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 locale de F-Secure Client Security.
5. Vous pouvez accepter les valeurs par défaut pour le reste des champs de cette fenêtre.

Etape 6. Vérification et acceptation de 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.

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*.

Etape 7. Configuration de la transmission des alertes

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. Au besoin, cochez la case *Alerte de sécurité* dans la colonne *Policy Manager Console*.

Pour plus d'informations sur la configuration de la transmission des alertes, reportez-vous au Guide de l'administrateur de F-Secure Policy Manager.

Etape 8. Mise en application de la nouvelle règle

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* dans 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 les données de stratégie.
5. Cliquez sur  pour diffuser la stratégie.

Etape 9. Test de la règle créée

Vous pouvez tester la règle que vous venez de créer en envoyant une commande ping à l'un des hôtes gérés 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 :

1. Sélectionnez le sous-domaine pour lequel vous avez créé la règle dans l'onglet *Domaines de stratégie*.
2. Activez l'onglet *Résumé* et vérifiez si de nouvelles alertes de sécurité sont affichées pour le domaine.
3. 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.

6.5 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 (pour une définition de ce terme et d'autres, consultez le "*Glossaire*"*, 327*) 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 finals utilisent réellement.

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

De quelle façon le contrôle des applications et le contrôle du système fonctionnent-ils 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 du contrôle du système 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* actuellement définie.
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 le contrôle du système* est activé, le contrôle des applications vérifie à partir du contrôle du système que la connexion sortante est autorisée. Si le contrôle du système identifie maintenant l'application, l'utilisateur final n'est pas invité à choisir et la connexion sortante est autorisée.
4. Si le contrôle du système n'a pas identifié l'application, l'utilisateur est invité à choisir si la connexion est autorisée ou refusée.

6.5.1 Paramètres de configuration du contrôle des applications

La page Contrôle des applications contient les informations suivantes :

Règles d'application pour les applications connues	
Application	Affiche le nom du fichier exécutable.
Faire office de client (sortant)	Les actions possibles sont les suivantes : Refuser, Autoriser, Décision utilisateur. Pour obtenir des explications, voir plus bas.
Faire office de serveur (entrant)	Les actions possibles sont les suivantes : Refuser, Autoriser, Décision utilisateur. Pour obtenir des explications, voir plus bas.
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 (voir ci-dessus), 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*. Vous avez le choix entre les actions suivantes :

Action	
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 finals décider du choix à faire lors des invites de connexion sortante, vous pouvez réduire le nombre de fenêtres indépendantes qu'ils voient en sélectionnant le paramètre *Ne pas inviter pour les applications que le contrôle du système 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 finals de n'installer que les plug-ins approuvés.

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

Etape 1. Création d'une liste d'applications connues

1. Créez un environnement de test avec, par exemple, deux ordinateurs où tournent les programmes normalement utilisés dans votre entreprise.
2. Importez ces hôtes dans le domaine géré de manière centralisée.
3. 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 rapportées par les hôtes*.
4. Définissez les règles d'autorisation pour ces applications. Pour plus d'informations, reportez-vous à la section “*Création d'une règle pour une application inconnue au niveau racine*”, *221*.
5. 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.

Etape 2. Configuration des paramètres de base du contrôle des applications

Configurez ensuite les paramètres de base qui seront utilisés lors de l'exécution du contrôle des applications.

1. 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.
2. 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.
3. Spécifiez que les nouvelles applications doivent être signalées à l'administrateur en cochant la case *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.

4. 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*.

Etape 3. Vérification et mise en application des paramètres

Le contrôle des applications peut être activé pour l'ensemble du domaine comme suit :

1. Sélectionnez *Racine* sous l'onglet *Domaines de stratégie*.
2. Sélectionnez la page *Niveaux de sécurité du pare-feu* dans l'onglet *Paramètres* et assurez-vous que la case *Activer le contrôle des applications* est cochée.
3. Cliquez sur  pour enregistrer les données de stratégie.
4. Cliquez sur  pour diffuser la stratégie.

6.5.3 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*.

Etape 1. Sélection des applications sur lesquelles porte la règle

1. Accédez à l'onglet *Paramètres* et sélectionnez la page *Contrôle des applications*.
2. Sélectionnez Internet Explorer 4.01 dans la table *Applications inconnues rapportées par les hôtes*.
3. Cliquez sur **Créer une ou plusieurs règles** pour lancer l'Assistant de règle de contrôle des applications.

Etape 2. Sélection du type de règle d'application

1. Sélectionnez *Refuser* comme action à exécuter lorsque l'application fait office de client et tente d'établir une connexion sortante.
2. Sélectionnez *Refuser* comme action à exécuter lorsque l'application fait office de serveur et tente d'établir une connexion entrante.

Etape 3. Sélection du message affiché aux utilisateurs

1. Indiquez si un message est affiché aux utilisateurs en cas de tentative de connexion. Les options sont : *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....
2. 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*”.

Etape 4. Sélection de la cible de la règle

1. 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*.
2. 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.

Etape 5. Mise en application de la nouvelle règle

1. Cliquez sur  pour enregistrer les données de stratégie.
2. Cliquez sur  pour diffuser la stratégie.

6.5.4 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*.

Etape 1. Sélection de la règle à modifier

1. Accédez à l'onglet *Paramètres* et sélectionnez la page *Contrôle des applications*.
2. Sélectionnez la règle à modifier dans la table *Règles d'application pour les applications connues*.
3. Cliquez sur **Modifier** pour lancer l'Assistant Règles de contrôle des applications.

Etape 2. Modification du type de règle d'application

1. 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)*.
2. Sélectionnez l'action à exécuter lorsque l'application fait office de serveur et tente d'établir une connexion entrante.

Etape 3. Sélection du message affiché aux utilisateurs

Indiquez si un message est affiché aux utilisateurs en cas de tentative de connexion.

Etape 4. Sélection de la nouvelle cible de la règle

1. Sélectionnez le domaine ou l'hôte sur lequel porte la règle. Dans ce cas, 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.
2. 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.

Etape 5. Mise en application de la nouvelle règle

1. Cliquez sur  pour enregistrer les données de stratégie.
2. Cliquez sur  pour diffuser la stratégie.

6.5.5 Désactivation des fenêtres contextuelles de contrôle des applications

Si vous souhaitez que le contrôle des applications soit entièrement transparent vis-à-vis des utilisateurs finals, vous devez désactiver toutes les fenêtres contextuelles. La procédure est la suivante :

1. Sélectionnez *Racine* sous 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. Une fois ces modifications effectuées, enregistrez les données de stratégie et distribuez la stratégie de manière à mettre en application la nouvelle configuration.

6.6 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 Règle de pare-feu démarre.

4. Dans la fenêtre *Type de règle*, sélectionnez *Autoriser*.
5. Dans la fenêtre *Hôtes distants*, sélectionnez *Tout hôte distant*.
6. Dans la fenêtre *Services*, sélectionnez *Ping* dans la liste déroulante *Service* et *Les deux* dans la liste déroulante *Directions*.
7. Dans la fenêtre *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. Dans la fenêtre *Résumé*, vous pouvez vérifier que la règle est correcte et entrer un commentaire décrivant la règle.
9. Cliquez sur  pour enregistrer les données de stratégie.
10. Cliquez sur  pour diffuser la stratégie.
11. 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*.

6.7 Configuration de la prévention des intrusions

La prévention des intrusions surveille le trafic entrant et tente de détecter d'éventuelles tentatives d'intrusion. Il 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 de détection des intrusions crée une alerte et exécute l'action prévue lors de sa configuration.

6.7.1 Paramètres de configuration de la prévention des intrusions

Les paramètres de configuration 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 détection 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

- Options disponibles :
  - *Consigner et supprimer le paquet* signifie que le paquet est consigné dans le journal d'alertes avec ses données d'en-tête (adresses IP, ports et protocole) et n'est pas autorisé à franchir le composant de détection des intrusions.
  - *Consigner sans supprimer le paquet*signifie que le paquet est consigné dans le journal d'alertes avec ses données d'en-tête (adresses IP, ports et protocole), mais est autorisé à franchir le composant de détection des intrusions.

Gravité de l'alerte

- Options disponibles : *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 IDS 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 F-Secure Client Security, 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.

6.7.2 Configuration d'IDS pour les ordinateurs de bureau et les portables

Dans cet exemple, l'IDS 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.

Etape 1. Configuration d'IDS pour les ordinateurs de bureau

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*.
3. Cochez la case *Activer la détection des intrusions*.
4. Sélectionnez *Consigner sans supprimer le paquet* dans la liste déroulante *Action en cas de paquet dangereux* .
5. Sélectionnez *Avertissement* dans la liste déroulante *Gravité de l'alerte* .
6. Sélectionnez *25%* dans la liste déroulante *Sensibilité de la détection* .

Etape 2. Configuration d'IDS pour les portables

1. Sélectionnez le sous-domaine *Laptops/Eng.* dans l'onglet *Domaines de stratégie*.
2. Accédez à l'onglet *Paramètres* et sélectionnez la page *Niveaux de sécurité du pare-feu*.
3. Cochez la case *Activer la détection des intrusions*.
4. Sélectionnez *Consigner sans supprimer le paquet* dans la liste déroulante *Action en cas de paquet dangereux* .

5. Sélectionnez *Avertissement* dans la liste déroulante *Gravité de l'alerte* .
6. Sélectionnez *100%* dans la liste déroulante *Niveau d'alerte et de performances* .

Etape 3. Mise en application de la détection des intrusions

1. Cliquez sur  pour enregistrer les données de stratégie.
2. Cliquez sur  pour diffuser la stratégie.

7 COMMENT VÉRIFIER QUE L'ENVIRONNEMENT EST PROTÉGÉ

7.1 Présentation

Cette section contient une liste de vérifications à effectuer pour vous assurer que l'environnement est protégé.

7.2 Vérification de l'état de protection dans l'onglet Attaque

L'onglet *Attaque* fournit une nouvelle méthode pour contrôler si tous les hôtes dans le domaine géré sont protégés contre les attaques de virus. L'onglet Attaque constitue un emplacement centralisé où vous pouvez voir les dernières informations sur les virus F-Secure et vérifier le pourcentage des hôtes qui sont déjà protégés.

1. Sélectionnez *Racine* sous l'onglet *Domaines de stratégie*.
2. Accédez à l'onglet *Attaque*. Il affiche une liste d'éléments de F-Secure Virus News, et indique combien d'hôtes sont protégés contre chaque virus. Lorsque vous sélectionnez un élément d'informations, des informations détaillées sur ce virus s'affichent.
3. Dans la section *Dernières informations détaillées sur la sécurité*, vous trouverez des informations sur chaque hôte dans le domaine sélectionné. Vous pouvez également voir si l'hôte est actuellement déconnecté et à quand remonte sa dernière connexion au serveur.

7.3 Comment vérifier que tous les hôtes utilisent la dernière stratégie

1. Sélectionnez *Racine* sous l'onglet *Domaines de stratégie*.
2. Cliquez sur 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'affichent.

4. Dans la page *Gestion centralisée*, vous pouvez voir les hôtes qui n'ont pas la stratégie la plus récente. Vous pouvez également prendre connaissance des raisons pouvant expliquer cette situation : par exemple, l'hôte est déconnecté ou a subi une erreur fatale.

7.4 Comment vérifier que le serveur utilise les définitions de virus les plus récentes

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

7.5 Comment vérifier que les hôtes ont les définitions de virus les plus récentes

1. Sélectionnez *Racine* sous 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 :
   a. Vous pouvez sélectionner l'onglet *Etat* et consulter 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 le bouton **Mettre à jour les définitions de virus**. Cette commande enjoint aux hôtes sélectionnés d'aller chercher immédiatement de nouvelles définitions de virus.
   b. Vous pouvez également cliquer sur le lien *Mettre à jour les définitions de virus*. L'onglet *Opérations* s'affiche. Sous 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.

7.6 Comment vérifier qu'aucun hôte n'est déconnecté

1. Sélectionnez *Racine* sous 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'affichent.
4. Vérifiez les hôtes qui sont déconnectés et les raisons pouvant expliquer cette situation.

Vous pouvez définir la période au terme de laquelle un hôte est considéré comme déconnecté. Dans le menu Outils, sélectionnez Préférences. Sélectionnez ensuite l'onglet Communications dans la fenêtre Préférences. La section Connexion de l'hôte contient la durée définie.

7.7 Visualisation des rapports d'analyse

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

1. Sélectionnez les hôtes sous l'onglet *Domaines de stratégie*.
2. Cliquez sur l'onglet *Rapports*.
3. Les données d'analyse des hôtes sélectionnés s'affichent dans la table *Rapports*.
4. 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.

Pour des instructions sur l'affichage du dernier rapport d'analyse localement sur un hôte, reportez-vous à la section “*Affichage du rapport d'analyse le plus récent sur un hôte local*”, *247*.

7.8 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 dont vous avez déjà analysé les causes.

Lorsqu'une alerte est reçue, le bouton ⚠ s'allume. Pour afficher les alertes, cliquez sur ⚠. Vous pouvez également cliquer sur Afficher le résumé des alertes... sous l'onglet *Résumé*. L'onglet *Alertes* s'affiche. 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, ce bouton **Accep.** s'affiche en 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	Produit F-Secure à l'origine de 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.

Vous pouvez utiliser le bouton **Accep.** pour marquer les alertes que vous avez vues et que vous prévoyez de résoudre.

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.

7.9 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 :

- **F-Secure Policy Manager Web Reporting**, outil Web avec lequel vous pouvez générer une large variété de rapports graphiques à partir d'informations d'alertes et d'état de F-Secure Anti-Virus Client Security. Pour plus d'informations, reportez-vous au chapitre *Web Reporting* du Guide de l'administrateur de *F-Secure Policy Manager*.
- **F-Secure Policy Manager Reporting Option**, outil conçu pour surveiller le réseau géré. Il peut être installé sur tout poste de travail. Il contient des modèles prédéfinis pour la création de différents types de rapports. Pour plus d'informations, reportez-vous au Guide de l'administrateur de *F-Secure Policy Manager Reporting Option*.

7.10 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 comme suit :

1. Sélectionnez *Racine* sous 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*. En cas d'attaque, vous pouvez accéder à des informations plus détaillées en cliquant sur **Afficher l'état de protection Internet...**. Vous accédez alors à l'onglet *Etat* et à la page *Protection Internet*, où vous pouvez voir des informations détaillées sur les dernières attaques sur les différents hôtes.

8 MISE À JOUR DU LOGICIEL

8.1 Présentation

Vous pouvez effectuer une mise à jour à distance du logiciel F-Secure Anti-Virus 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.

Il est également possible de mettre à niveau F-Secure Anti-Virus Client Security en utilisant toute autre procédure d'installation expliquée dans "Ajout d'hôtes", 129.

8.1 Utilisation de l'éditeur d'installation

L'éditeur d'installation ne peut être utilisé que sur les hôtes équipés de F-Secure Management Agent.

1. Pour accéder à cet éditeur, cliquez sur l'onglet *Installation*. Les modules d'installation disponibles sont énumérés dans l'éditeur d'installation, dans la partie inférieure de cet onglet.
2. Vous pouvez sélectionner les produits et versions de produits à installer sur l'hôte ou le domaine de stratégie sélectionné en cliquant sur la flèche vers le bas dans la colonne *Version à installer* .

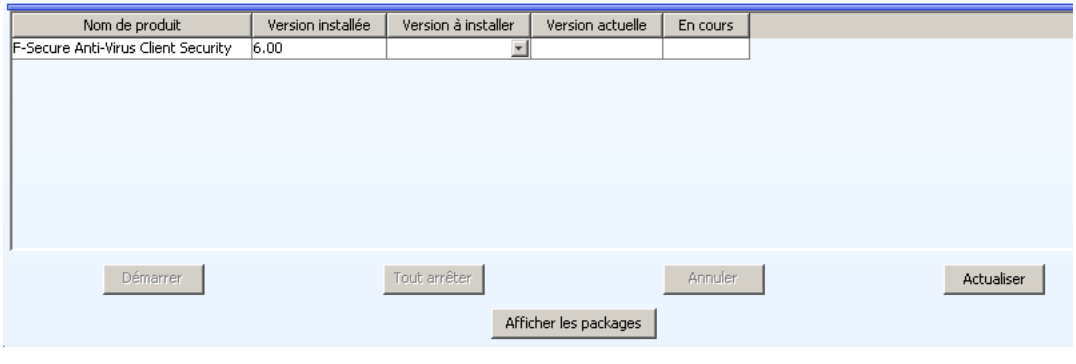


Figure 8-1 Editeur d'installation

L'éditeur 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	Avancement de l'installation. Cette zone affiche des informations différentes pour les hôtes et pour les domaines.

Lorsqu'un hôte est sélectionné, la zone *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.
Echec	L'installation ou la désinstallation a 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. Ce message disparaît lorsque vous fermez l'éditeur d'installation.

(Zone vide)	Aucune opération n'est en cours. La zone *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 ont 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 zone *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'éditeur d'installation démarre alors l'Assistant d'installation, qui invite l'utilisateur à configurer les paramètres de l'installation. L'éditeur d'installation prépare ensuite un package personnalisé de distribution de l'installation pour chaque opération d'installation. Le nouveau package est enregistré sur F-Secure Policy Manager Server.

   *Le bouton **Démarrer** permet de démarrer les opérations d'installation sélectionnées dans la zone Version à installer. Si vous fermez l'éditeur 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 hôtes* dans la boîte de dialogue de confirmation.

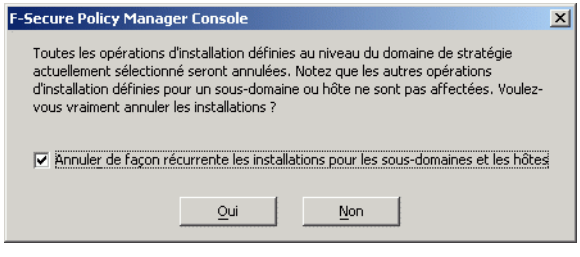


Figure 8-2 Boîte de dialogue de confirmation d'annulation d'installation

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. Le bouton **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'éditeur d'installation.

9 OPÉRATIONS SUR LES HÔTES LOCAUX

9.1 Présentation

Ce chapitre explique comment effectuer certaines opérations et résoudre des problèmes localement sur les hôtes. Ces opérations sont utiles lorsque vous soupçonnez la présence d'un virus sur un hôte local ou devez effectuer localement certaines tâches administratives.

9.2 Recherche manuelle de virus de fichier

Si vous pensez qu'un hôte est affecté par un virus ou si vous souhaitez vous assurer qu'un virus a bien été éradiqué d'un hôte, vous pouvez démarrer manuellement une recherche de virus sur l'ordinateur. Pour analyser manuellement des fichiers, procédez comme suit :

1. Sélectionnez la page *Protection contre les virus et les logiciels espions*.
2. Cliquez sur Analyser mon ordinateur.
3. Dans le menu contextuel qui s'affiche, sélectionnez *Rechercher des virus sur tous les disques durs*.
4. L'*Assistant Analyse* apparaît. Il montre l'avancement et les statistiques de l'analyse. Cliquez sur **Arrêter** pour interrompre l'analyse à tout moment.
5. A la fin de l'analyse, un rapport est généré. Cliquez sur **Afficher le rapport** pour visualiser le rapport dans votre navigateur Web.

Lorsque vous effectuez une analyse, F-Secure Anti-Virus Client Security utilise les paramètres d'analyse manuelle associés au niveau de protection antivirus actuel.

Vous pouvez aussi consulter le rapport d'analyse dans la liste qui apparaît sous l'onglet Rapports de Policy Manager.

9.3 Affichage du rapport d'analyse le plus récent sur un hôte local

Sous l'onglet *Protection contre les virus et les logiciels espions* de l'interface utilisateur d'Anti-Virus Client Security, vous pouvez voir l'état du rapport d'analyse. Si un rapport non lu est en attente, l'état suivant s'affiche : *Nouveau rapport disponible*. Vous pouvez accéder au rapport en cliquant sur Afficher....

Si vous avez lu le dernier rapport, l'état affiché est *Aucun nouveau rapport*.

9.4 Ajout d'une analyse planifiée à partir d'un hôte local

Une analyse planifiée est requise pour assurer l'intégrité de l'hôte. Un hôte n'est exempt des virus connus qu'après une analyse complète. Cette analyse doit être effectuée périodiquement.

Vous pouvez ajouter une analyse planifiée à partir de l'interface utilisateur locale afin d'exécuter une analyse quotidienne, hebdomadaire ou mensuelle. La procédure est la suivante :

1. Accédez à la page *Protection contre les virus et les logiciels espions* et cliquez sur Paramètres avancés....
2. Dans la page *Paramètres de protection antivirus avancés*, sélectionnez *Protection contre les virus et les logiciels espions→Analyse planifiée*.
3. Vous pouvez configurer F-Secure Anti-Virus Client Security pour analyser votre ordinateur à des moments spécifiques en cochant la case *Activer l'analyse planifiée*.

4. Pour définir la planification de l'analyse, sélectionnez *Quotidienne*, *Hebdomadaire* ou *Mensuelle* sous *Analyse effectuée*.
   - Sélectionnez *Quotidienne* pour effectuer l'analyse tous les jours à l'heure programmée. Les jours de la semaine qui figurent à droite sont tous sélectionnés et grisés.
   - Sélectionnez *Hebdomadaire* pour effectuer l'analyse toutes les semaines, au jour et à l'heure programmés. Vous pouvez sélectionner, à droite, autant de jours de la semaine que souhaité. L'analyse sera réalisée chaque jour sélectionné.
   - Sélectionnez *Mensuelle* pour effectuer l'analyse tous les mois, à la date et à l'heure programmées. Vous pouvez sélectionner jusqu'à trois jours par mois durant lesquels l'analyse est exécutée.
5. Sélectionnez l'heure de démarrage de l'analyse dans la liste déroulante *Heure de démarrage*. Si vous souhaitez ne démarrer l'analyse que lorsque l'ordinateur n'est pas utilisé, cochez la case *Si l'ordinateur est inutilisé pendant*, puis sélectionnez la durée d'inactivité dans la liste déroulante.

Pour savoir comment configurer l'analyse planifiée à partir de l'interface utilisateur avancée de Policy Manager, reportez-vous à la section “*Configuration d'une analyse planifiée*”, *274*.

9.5 Consignation et emplacement des fichiers journaux sur les hôtes locaux

A partir de l'interface utilisateur locale de F-Secure Anti-Virus Client Security, vous pouvez accéder à plusieurs fichiers journaux qui fournissent des données sur le trafic du réseau.

9.5.1 LogFile.log

LogFile.log contient toutes les alertes que F-Secure Anti-Virus Client Security a généré depuis son installation. Le fichier est associé à une taille maximale qu'il ne peut pas dépasser. La maintenance du fichier journal *Logfile.log* est assurée par F-Secure Management Agent. Ce fichier est utilisé par tous les hôtes exécutant F-Secure Management Agent.

Le fichier journal *Logfile.log* se trouve dans le répertoire *%Program Files%/F-Secure/Common* et peut être ouvert dans un éditeur de texte quelconque, tel que le Bloc-notes de Windows.

Vous pouvez également accéder au fichier *LogFile.log* à partir de l'interface utilisateur locale :

1. Accédez à la page *Paramètres avancés* et sélectionnez *Généralités →Gestion centralisée*.
2. Cliquez sur **Afficher le fichier journal**.

9.5.2 Consignation de paquets

Le journal de paquets rassemble des informations complètes sur le trafic réseau. Il est, cependant, désactivé par défaut. Si vous soupçonnez une activité malveillante, vous pouvez activer ce journal afin de surveiller le trafic réseau. La procédure est la suivante :

1. Cliquez sur Paramètres avancés.
2. Dans la page *Paramètres de protection Internet avancés*, sélectionnez *Protection Internet* > *Consignation.*
3. Cliquez sur **Démarrer la consignation**

   Sur cette page, vous pouvez également définir :

   - La durée de la consignation (en secondes)
   - La taille maximale du fichier journal.

   La consignation est automatiquement interrompue après l'expiration de la période définie, si le fichier journal a atteint sa taille maximale, ou encore si vous cliquez sur **Arrêter la consignation**. Les journaux de paquets sont répartis sur 10 fichiers différents. Par conséquent,

vous pouvez consulter les journaux précédents tandis que le nouveau est généré. Le format du journal est binaire et compatible avec le format tcpdump. Il peut être lu avec la visionneuse de journal de paquets fournie par F-Secure ou avec une application courante de consignation des paquets telle que Ethereal.

4. Pour visualiser le fichier *packetlog*, cliquez deux fois dessus dans la fenêtre.

Le journal de paquets consigne tous les types de trafic réseau (informations relatives à l'acheminement, résolution de l'adresse matérielle, etc.), y compris les protocoles requis par votre réseau local. Ce trafic n'est généralement pas très utile et n'apparaît pas par défaut dans la visionneuse de journal de paquets intégrée. Pour l'afficher, il suffit de désélectionner la case *Filtrer non IP*.

Il est possible de désactiver la consignation de paquets à partir de Policy Manager Console.

Les particuliers peuvent se servir de la consignation de paquets pour recueillir des preuves de tentatives d'intrusion.

Le répertoire de consignation

Le répertoire de consignation est défini lors de l'installation de l'application. Vous pouvez en changer en cliquant sur **Parcourir**.

Journal des actions

Le journal des actions recueille continuellement des données sur les actions du pare-feu. Il s'agit d'un fichier texte normal d'une taille maximale de 10 Mo. Vous pouvez l'ouvrir avec n'importe quel éditeur de texte acceptant des fichiers volumineux. Vous pouvez effacer et supprimer ce fichier à tout moment. Vous pouvez donc facilement recommencer dans un nouveau fichier si le fichier initial devient trop volumineux. Il est possible d'afficher le journal des actions en cliquant sur le bouton **Afficher le journal des actions** de la page *Consignation*.

Le journal des actions utilise le format unix standard syslog.

Exemples pratiques de lecture du journal des actions :

Changement de stratégie de pare-feu, par exemple changement de niveau de sécurité :

07/16/03 15:48:01,success,general,daemon,Policy file has been reloaded.

Ouverture d'une connexion locale, entrante ou sortante :

1	2	3	4	5	6	7	8	9	10
07/16/03	16:54:41	info	appl control	C:\WINNT\system32\services.exe	allow	send	17	10.128.128.14	137

Les champs sont les suivants :

1. Date
2. Heure
3. Type
4. Raison interne
5. Nom de l'application
6. Action du contrôle des applications
7. Action réseau
8. Protocole
9. IP distante
10. Port distant

Connexion de réception

Si l'application a ouvert une connexion d'écoute (LISTEN), elle agit comme un serveur et les ordinateurs distants peuvent se connecter au port dédié à cette connexion. Le journal des actions enregistre également ces connexions.

1	2	3	4	5	6	7	8	9	10
07/15/03	16:48:00	info	appl control	unknown	allow	receive	17	10.128.129.146	138

Les champs sont les suivants :

1. Date
2. Heure
3. Type
4. Raison interne
5. Nom de l'application
6. Action du contrôle des applications
7. Action réseau
8. Protocole
9. IP distante
10. Port distant

Entrée de règle dynamique

Si une application ouvre une connexion d'écoute que l'utilisateur autorise, les règles statiques du pare-feu peuvent empêcher cette connexion. C'est pourquoi une règle dynamique est utilisée pour autoriser cette connexion sortante, juste pour la durée de la connexion et pour cette application uniquement.

1	2	3	4	5	6	7	8	9	10	11	12
07/15/03	16:47:59	info	dynamic rule	added	0.0.0.0	255.255.255.0	0	65535	371	371	allow
07/15/32	16:48:23	info	dynamic rule	removed	0.0.0.0	255.255.255.0	0	65535	371	371	allow

Les champs sont les suivants :

1. Date
2. Heure
3. Type d'alerte
4. Type de règle
5. Action effectuée
6. IP de la plage d'IP distantes
7. Masque de réseau de la plage d'IP distantes
8. Début de la plage de ports
9. Fin de la plage de ports
10. Port local source
11. Port local de destination
12. Action de la règle (autoriser/refuser)

9.5.3 Autres fichiers journaux

Journal système local

Vous pouvez également accéder au journal système local en cliquant sur le bouton **Ouvrir l'Observateur d'événements** de la page *Paramètres avancés de la gestion centralisée*.

9.6 Connexion à F-Secure Policy Manager et importation d'un fichier de stratégie manuellement

Si vous devez initialiser une connexion de l'hôte local à F-Secure Policy Manager Server, procédez comme suit :

1. Accédez à la page *Gestion centralisée*, où vous pouvez voir la date et l'heure de la dernière connexion à Policy Manager Server.
2. Cliquez sur Vérifier maintenant pour établir 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 F-Secure Policy Manager Console avant de l'importer. La procédure est la suivante :

Etape 1. Dans F-Secure Policy Manager Console

1. Sélectionnez l'hôte sous l'onglet *Domaines de stratégie*.
2. Cliquez avec le bouton droit sur l'hôte sélectionné et choisissez *Exporter le fichier de stratégie de l'hôte* dans le menu contextuel qui apparaît.
3. Enregistrez le fichier de stratégie de l'hôte sur un support de transfert de votre choix, par exemple une disquette.

Etape 2. Dans l'interface utilisateur locale de F-Secure Anti-Virus Client Security

1. Cliquez sur Importer manuellement la stratégie....
2. 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 F-Secure Policy Manager si l'hôte géré a été déconnecté en raison d'une stratégie mal configurée.

9.7 Suspension des téléchargements et mises à jour

Cette option est configurée depuis F-Secure Policy Manager Console. Elle est utile pour les hôtes qui utilisent parfois une ligne 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 sous l'onglet *Domaines de stratégie*.
2. Accédez à l'onglet *Paramètres* et sélectionnez la page *Gestion centralisée*.
3. Cochez la case *Autoriser les utilisateurs à suspendre tous les téléchargements et mises à jour*.
4. Cliquez sur  pour enregistrer les données de stratégie.
5. Cliquez sur  pour distribuer la stratégie.

9.8 Autoriser les utilisateurs à décharger les produits F-Secure

Cette option est configurée depuis F-Secure 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.

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 sous l'onglet *Domaines de stratégie*.
2. Accédez à l'onglet *Paramètres* et sélectionnez la page *Gestion centralisée*.
3. Sélectionnez l'une des options du menu déroulant *Autoriser l'utilisateur à décharger des produits*.

4. Cliquez sur  pour enregistrer les données de stratégie.
5. Cliquez sur  pour distribuer la stratégie.

10 INFORMATIONS SUR LES VIRUS

10.1 Informations sur les virus sur les pages Web de F-Secure

F-Secure Corporation met continuellement à jour une base de données complète d'informations sur les virus informatiques qui apporte des renseignements sur les divers symptômes de nombreux virus. Cette base de données est disponible sur Internet à l'adresse : http://www.f-secure.com/virus-info/.

10.2 Menaces les plus récentes

De nouvelles menaces pour la sécurité apparaissent quotidiennement. Par exemple, sept à dix nouveaux virus sont découverts chaque jour, dont certains sont capables de se diffuser mondialement en quelques heures. Lorsque des menaces potentielles sont découvertes, comme l'apparition de virus ou des attaques de type refus de service, le temps est un facteur primordial. Plus tôt vous serez averti des nouveaux virus et attaques de type déni de service, mieux vous pourrez protéger votre réseau. La liste des menaces les plus récentes est disponible sur le site du Centre d'informations sur la sécurité F-Secure : http://www.europe.f-secure.com/virus-info/virus-news/

Les menaces les plus récentes sont également annoncées sur votre bureau par le biais de F-Secure Anti-Virus Client Security sous la forme d'informations F-Secure.

10.2.1 F-Secure Radar

F-Secure Radar fournit des notifications instantanées sur les événements sérieux liés à la sécurité de par le monde via divers supports. F-Secure Radar diffuse des informations sur les attaques virales, attaques DOS (déni de service) et autres alertes de sécurité critiques à un large éventail d'équipements dont les téléphones mobiles, PDA et téléavertisseurs. Vous pouvez donc recevoir ces messages où que vous soyez. F-Secure Radar est un service disponible sous la forme d'un abonnement personnel d'un an.

Pour plus d'informations, reportez-vous à http://www.europe.f-secure.com/products/radar/.

10.3 Virus susceptibles d'être rencontrés

La « Wildlist » est une liste coopérative établie par 73 professionnels des informations sur les virus. Elle énumère les virus susceptibles d'être rencontrés. Ces rapports sont basés sur des incidents liés aux virus où un échantillon a été reçu et identifié par les participants. Les rumeurs et rapports non vérifiés en sont exclus. F-Secure Corporation est un membre actif de la Wildlist Organization.

La « Wildlist » est disponible sur Internet à l'adresse : http://www.europe.f-secure.com/virus-info/wild.shtml.

10.4 Comment envoyer un échantillon de virus à F-Secure

Cette section est destinée aux utilisateurs expérimentés.

Cette section comporte les rubriques suivantes relatives à l'envoi d'un échantillon de virus à F-Secure VirusLab :

- Comment préparer un échantillon de virus ?
- Quels fichiers envoyer ?
- Où envoyer un échantillon de virus ?
- Dans quelle langue envoyer les questions et descriptions de virus ?
- Quels sont les temps de réponse ?

Les instructions qui suivent décrivent dans les grandes lignes l'envoi d'un échantillon de virus à samples@f-secure.com. Pour obtenir des instructions plus détaillées, consultez :

http://www.europe.f-secure.com/support/technical/general/samples.shtml

10.4.1 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 du logiciel WinZip à l'adresse http://www.winzip.com/ . Un utilitaire InfoZIP gratuit est également disponible 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. Si vous envoyez plusieurs fichiers d'archivage (par exemple en raison de limitations du serveur), envoyez-les dans des messages séparés ou ajoutez un numéro d'ordre aux différents fichiers, par exemple :

sample_part1.zip
sample_part2.zip
...
sample_part18.zip

Votre serveur de messagerie ou fournisseur d'accès peut avoir un analyseur de courrier électronique (un programme antivirus qui vérifie l'absence de virus dans les messages entrants et sortants). Vos échantillons de virus risquent dès lors d'être supprimés avant de nous parvenir. Envoyez les échantillons dans un fichier d'archivage ZIP protégé par mot de passe. Vous pouvez envoyer le mot de passe de ce fichier dans le même message ou dans un message séparé.

10.4.2 Quels fichiers envoyer ?

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. 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 applications (par exemple Tristate), envoyez un échantillon de chaque type de fichier.

2. Virus infectant des fichiers exécutables

   Essayez de trouver différents fichiers infectés sur votre système. Généralement, 3 à 5 échantillons différents suffisent. Si possible, ajoutez des copies saines des mêmes fichiers (à partir 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

3. Virus du secteur d'amorçage

   Créez une image DCF ou TeleDisk de la disquette infectée. Essayez d'abord d'obtenir une disquette infectée de 1,44 Mo (remarque : certains virus n'infectent pas ce type de disquette). N'utilisez ni la compression ni l'option d'enregistrement rapide, car cela risquerait de laisser de côté certaines zones importantes du corps du virus. Notez que l'enregistrement rapide est activé par défaut. Vous pouvez télécharger l'utilitaire Teledisk à partir de notre site ftp :

   ftp://ftp.f-secure.com/misc/dos-util/teled215.zip

   Vous pouvez également envoyer une disquette infectée par courrier postal à nos bureaux finlandais :

   F-Secure Corporation
   Anti-Virus Research
   Tammasaarenkatu 7
   PL 24
   00180, Helsinki
   Finlande

Emballez correctement la disquette pour éviter qu'elle ne s'abîme en route. Notez que nous ne renvoyons pas les disquettes.

Si l'infection touche un disque dur, employez l'utilitaire GetMBR pour collecter des échantillons du secteur d'amorçage. Placez l'utilitaire GetMBR sur une disquette système saine, démarrez l'ordinateur infecté à partir de cette disquette et exécutez GetMBR. Envoyez le fichier MBR.DAT généré, après l'avoir placé dans un fichier d'archivage ZIP, à samples@f-secure.com. GetMBR peut être téléchargé depuis notre site ftp :

http://www.f-secure.com/download-purchase/tools.shtml

4. 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.

5. Une fausse alarme d'un de nos produits antivirus

   Si vous recevez un avis de détection raté ou incorrect, ou une fausse alarme F-Secure Anti-Virus Client Security, essayez de nous envoyer :

   - le fichier en question
   - le numéro de version de F-Secure Anti-Virus 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 façon de reproduire le problème
   - le rapport d'analyse de F-Secure Anti-Virus Client Security.

6. Une infection ou une fausse alarme sur un CD-ROM

   Si une infection ou une fausse alarme est relative à un CD-ROM, vous pouvez envoyer ce dernier à nos bureaux finlandais. Veuillez inclure une description du problème, ainsi qu'un rapport F-Secure Anti-Virus Client Security imprimé, si possible. Nous renverrons le CD-ROM s'il n'est pas infecté.

7. Message électronique suspect

Si vous avez un message électronique suspect ou un canular, essayez de l'enregistrer dans un fichier, puis de l'envoyer à samples@f-secure.com sous la forme d'une archive ZIP. Si vous ne pouvez pas enregistrer un message électronique suspect sur un disque dur, vous pouvez toujours le transmettre à samples@f-secure.com.

8. 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 :

   - 3 à 5 fichiers exécutables fréquemment utilisés
   - 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 Regedit inclus dans toutes les versions de Windows)
   - le contenu du dossier *\Menu Démarrer\Programmes\Démarrage*

10.4.3 Où envoyer l'échantillon de virus ?

Envoyez tous vos échantillons de virus, chevaux de Troie, portes dérobées, vers et fausses alarmes à :

samples@f-secure.com

N'envoyez l'échantillon à aucune adresse électronique personnelle chez F-Secure Corporation ; vos messages seraient éliminés par notre analyseur de courrier électronique. Envoyez vos exemples de canulars et vos questions relatives aux virus également à samples@f-secure.com

Si l'échantillon de virus est trop volumineux pour être envoyé par courrier électronique, vous pouvez le télécharger (sous la forme d'un fichier d'archivage ZIP) sur notre site ftp :

ftp://ftp.europe.f-secure.com/incoming

Envoyez un message à samples@f-secure.com avec le nom de l'archive téléchargée ainsi qu'une description de l'échantillon de virus.

10.4.4 Dans quelle langue ?

Envoyez toutes les descriptions de virus, problèmes et questions, si possible en anglais.

10.4.5 Temps de réponse

Notre temps de réponse habituel est de 24 à 48 heures. Les cas complexes peuvent être plus longs à étudier. Si vous n'obtenez pas de réponse de notre part dans la semaine, renvoyez votre message à samples@f-secure.com.

10.5 Que faire en cas d'apparition d'un nouveau virus ?

Cette section contient une 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 dernière version de F-Secure Anti-Virus Client Security et les dernières mises à jour de définition de virus. Si l'infection est identifiée avec précision, passez à l'étape 3. Si l'infection est identifiée comme *possible new virus* (nouveau virus possible), *could be an image of a boot sector virus* (pourrait être une image d'un virus de secteur d'amorçage) etc., envoyez un échantillon accompagné du rapport d'analyse F-Secure Anti-Virus Client Security à F-Secure Anti-Virus Research Team (samples@f-secure.com) selon les instructions données à l'adresse :

   http://www.europe.f-secure.com/support/technical/general/samples.shtml

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 aide au nettoyage, contactez l'assistance (Anti-Virus-Support@f-secure.com) ou si l'assistance ne peut pas aider, envoyez un message à F-Secure Anti-Virus Research Team (samples@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 d'en localiser un échantillon et envoyez celui-ci à F-Secure Anti-Virus Research Team (samples@f-secure.com) selon les instructions données à l'adresse :

   http://www.europe.f-secure.com/support/technical/general/samples.shtml

   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 l'analyse de l'antiprogramme par F-Secure Anti-Virus Research Team et suivez attentivement les instructions de nettoyage 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 F-Secure Anti-Virus Client Security et les dernières mises à jour des définitions de virus pour vous assurer qu'il ne reste aucun fichier infecté.

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 firewalls fonctionnent correctement sur les serveurs. Maintenez toujours à jour les installations de F-Secure Anti-Virus Client Security avec les toutes dernières bases de données de définitions de virus. Il est recommandé de mettre à jour F-Secure Anti-Virus Client Security deux fois par jour, lorsque de nouvelles mises à jour sont proposées par F-Secure Anti-Virus Research Team.

10. Avertissez vos partenaires de l'infection et recommandez-leur d'analyser leurs ordinateurs avec F-Secure Anti-Virus Client Security et les définitions de virus les plus récentes pour s'assurer qu'aucune infection n'a quitté l'enceinte de votre réseau.

11 Configuration de la prise en charge de Cisco NAC

11.1 Introduction

F-Secure Corporation 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 pour F-Secure Client Security comporte une option pour installer la prise en charge Cisco NAC. Lorsque vous sélectionnez cette option, le plug-in de FF-Secure NAC et le CTA sont installés. En outre, le serveur ACS doit être configuré pour surveiller les attributs de sécurité liés aux produits F-Secure.

Seule la version 1.0 du programme Cisco NAC est prise en charge.

11.2 Installation de la prise en charge de Cisco NAC

La prise en charge de Cisco NAC peut être installée sur les hôtes localement et à distance.

Installations locales

1. Lors de l'installation de F-Secure Client Security localement, sélectionnez *Prise en charge Cisco NAC* dans la boîte de dialogue *Composants à installer*.
2. Utilisez un outil Cisco, *ctaCert.exe,* pour installer un certificat pour l'agent CTA (Cisco Trust Agent).

Pour plus d'informations sur l'outil ctsCert, reportez-vous au document Cisco Trust Agent Administrator Guide.

Installations à distance

1. Lors de l'installation de F-Secure Client Security à distance, sélectionnez *Prise en charge Cisco NAC* dans la boîte de dialogue *Composants à installer*.
2. Ensuite, dans l'assistant Installation distante, la boîte de dialogue *Sélection d'un certificat de serveur Cisco AAA* s'affiche. Entrez le chemin d'accès au certificat de serveur Cisco AAA.

Pour plus d'informations, reportez-vous à la documentation de Cisco NAC.

11.2.1 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. Pour cela, utilisez l'outil *CSUtil* sur le serveur Cisco Secure ACS. Utilisez la commande suivante :

```
CSUtil.exe -addAVP fsnacpva.def
```

Le fichier *fsnacpva.def* se trouve sur le CD du produit F-Secure.

Pour plus d'informations sur CSUtil, reportez-vous à la documentation de Cisco ACS.

11.3 Attributs à utiliser pour un jeton de posture d'application

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 le lien **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 le lien **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 F-Secure Client Security suivants dans les règles des jetons de posture d'application :

Attributs de validation de posture pour anti-virus

Attribute-name	Type	Exemple
Software-Name	chaîne	F-Secure Anti-Virus
Software-Version	version	7.0.0.0
Dat-Date	date	[la date de la base de données]
Protection-Enabled	entier non signé	1= activé, 0= désactivé

Attributs de validation de posture pour pare-feu

Attribute-name	Type	Exemple
Software-Name	chaîne	F-SecureProtection Internet
Software-Version	version	7.0.0.0
Protection-Enabled	entier non signé	1= activé, 0= désactivé

12 Fonctions avancées : Protection contre les virus et les logiciels espions

12.1 Présentation

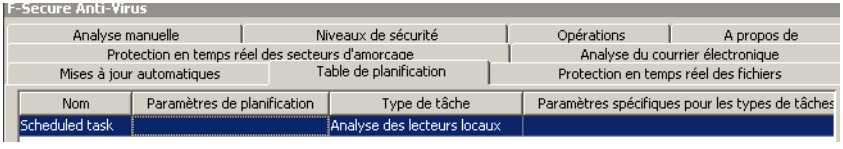
Cette section contient des instructions relatives à certaines tâches d'administration avancées de la protection antivirus, telles que la configuration d'une analyse planifiée à partir de l'interface utilisateur en mode avancé et la configuration du proxy Anti-Virus.

12.2 Configuration d'une analyse planifiée

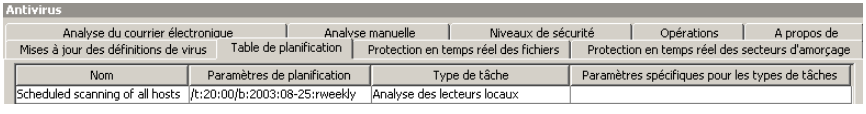
Une tâche d'analyse planifiée peut être ajoutée à partir de l'interface utilisateur en mode avancé de Policy Manager. Dans cet exemple, une tâche d'analyse planifiée est ajoutée à une stratégie pour l'ensemble du domaine de stratégie. L'analyse doit être effectuée chaque semaine, le lundi à 20h00, à partir du 25 août 2003.

1. Ouvrez le menu *Affichage* et sélectionnez l'option *Mode avancé*. L'interface utilisateur en mode avancé s'ouvre.
2. Sélectionnez *Racine* dans le volet *Domaines de stratégie*.
3. Sélectionnez l'onglet *Stratégie* dans le volet du milieu *Propriétés*.
4. Dans l'onglet *Stratégie*, sélectionnez :

   F-Secure/F-Secure Antivirus
5. Dans le volet de droite *Affichage produit*, sélectionnez la page *Table de planification*.
6. Les tâches planifiées actuellement définies s'affichent dans la section *Table de planification*. Vous pouvez maintenant ajouter une analyse planifiée comme nouvelle tâche.
7. Cliquez sur **Ajouter**. Une nouvelle ligne est ajoutée à la *table de planification*.
8. Cliquez sur la cellule *Nom* de la ligne que vous venez de créer, puis cliquez sur *Modifier*. 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.’*.

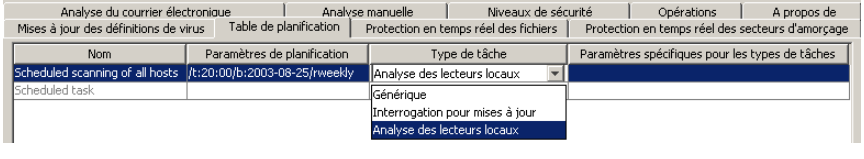


9. Cliquez ensuite sur la cellule *Paramètres de planification* et cliquez sur **Modifier**. Vous pouvez maintenant entrer les paramètres de l'analyse planifiée. Pour planifier une analyse chaque semaine, le lundi à 20h00, à partir du 25 août 2003, les paramètres sont les suivants : *"/t20:00 /b2003-08-25 /rweekly"*



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). Pour configurer des jours ouvrables et des jours spécifiques, reportez-vous à "Exécution d'analyses planifiées pour des jours ouvrables et des jours spécifiques", 276.

10. Sélectionnez le type de tâche en cliquant sur la cellule *Type de tâche*, puis en cliquant sur **Modifier**. Dans la liste déroulante qui s'ouvre, sélectionnez *Analyse des lecteurs locaux*.



11. La tâche d'analyse est maintenant prête pour la distribution.

12. Cliquez sur pour enregistrer les données de stratégie.

13. Cliquez sur pour diffuser la stratégie.

Pour savoir comment configurer l'analyse planifiée sur un hôte local à partir de l'interface utilisateur locale, reportez-vous à la section "*Ajout d'une analyse planifiée à partir d'un hôte local*", *247*.

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 mensueelle, 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 - /s3'.
  Par exemple, '*/t18:00 /rmonthly /s5 /s20'* signifie que l'analyse est exécutée le 5 et le 20 de chaque mois, à 18 heures.

Les analyses planifiées hebdomadaires sont automatiquement exécutées chaque lundi. Les analyses planifiées mensuelles sont automatiquement exécutées le premier jour de chaque mois.

12.3 Configuration de Policy Manager Proxy

Proxy F-Secure Policy Manager offre une solution aux problèmes de bande passante dans les installations distribuées de F-Secure Client Security ou F-Secure Anti-Virus pour stations de travail en réduisant de façon significative la charge des réseaux ayant des connexions lentes. Il met en mémoire cache les mises à jour récupérées à partir du serveur de mise à jour F-Secure central ou du F-Secure Policy Manager Server de l'entreprise.

Proxy F-Secure Policy Manager se trouve sur le même réseau distant que les hôtes qui l'emploient comme point de distribution des bases de données. Il doit y avoir un Proxy F-Secure Policy Manager dans chaque réseau derrière des lignes de réseau lentes.

Les hôtes exécutant F-Secure Client Security ou F-Secure Anti-Virus pour stations de travail récupèrent les mises à jour de définitions de virus via Proxy F-Secure Policy Manager. Proxy F-Secure Policy Manager contacte F-Secure Policy Manager Server et le serveur de distribution de F-Secure lorsque c'est nécessaire.

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 Proxy F-Secure Policy Manager dans le même réseau local, la connexion du réseau entre les postes de travail gérés et F-Secure Policy Manager Server présente une charge substantiellement plus légère.

Pour plus d'informations sur l'installation et la configuration du proxy Policy Manager, reportez-vous au Guide de l'administrateur Proxy F-Secure Policy Manager.

12.4 Configuration des mises à jour automatiques sur les hôtes à partir du proxy antivirus

La liste de proxies Policy Manager par le biais desquels les hôtes récupèrent les mises à jour peut être configurée dans l'onglet *Paramètres* de Policy Manager. Cette opération est décrite dans la section "*Configuration de Policy Manager Proxy*"*, 165*. Cependant, 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 modifier les adresses à partir desquelles le F-Secure Client Security local 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 le proxy à la liste.
4. Entrez le nom du premier Policy Manager Proxy dans le champ. Cliquez ensuite sur **OK**.
5. Répétez cette opération pour chaque proxy que vous souhaitez 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 que vous avez ajouté tous les the proxies, cliquez sur **OK**.

12.5 Configuration d'un hôte pour la gestion SNMP

L'extension d'administration SNMP de F-Secure SNMP est un agent d'extension SNMP Windows NT, chargé et déchargé avec l'agent principal. Le service SNMP est lancé normalement au démarrage de Windows de façon à ce que l'agent d'extension soit toujours chargé.

L'agent principal de Windows NT héberge les extensions et transmet les requêtes à F-Secure Management Agent, à son tour responsable de leur renvoi à la console d'administration dont elles sont issues. L’extension d'administration SNMP de F-Secure peut être chargée même si aucun module n’est chargé, ce qui lui permet de surveiller les activités de F-Secure Management Agent indépendamment des autres modules de F-Secure Management Agent.

Pour plus d'informations sur l'installation de F-Secure Management Agent avec Support SNMP et sur la configuration de l'agent SNMP Master, consultez le chapitre relatif au support SNMP dans le Guide de l'administrateur de F-Secure Policy Manager.

13 Fonctions avancées : Protection Internet

13.1 Présentation

Cette section couvre certaines fonctions avancées de la protection Internet. Elle contient également certaines informations de dépannage.

13.2 Gestion à distance des propriétés de la protection Internet

Cette section décrit la gestion à distance des propriétés de la protection Internet.

13.2.1 Consignation de paquets

La consignation de paquets est un outil de débogage très utile pour découvrir ce qui se passe sur le réseau local. C'est également 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 de paquets.

1. Ouvrez le menu *Affichage* et sélectionnez l'option *Mode avancé*. L'interface utilisateur en mode avancé s'ouvre.
2. Sélectionnez *Racine* dans le volet *Domaines de stratégie*.
3. Sélectionnez l'onglet *Stratégie* dans le volet du milieu *Propriétés*.
4. Dans l'onglet *Stratégie*, sélectionnez :

   \Protection Internet de F-Secure
5. Sélectionnez l'onglet *Consignation* dans le volet de droite *Affichage produit*.

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. Pour désactiver complètement la consignation, assurez-vous qu'elle est définie sur *Désactivé* et cochez la case *Final*. Distribuez la stratégie pour appliquer la modification.

Pour annuler cette modification par la suite, désactivez la case *Final* et distribuez la nouvelle stratégie.

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.

13.2.2 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. Ouvrez le menu *Affichage* et sélectionnez l'option *Mode avancé*. L'interface utilisateur en mode avancé s'ouvre.
2. Sélectionnez le sous-domaine où vous souhaitez activer l'interface approuvée dans le volet *Domaines de stratégie*.
3. Sélectionnez l'onglet *Stratégie* dans le volet du milieu *Propriétés*.
4. Dans l'onglet *Stratégie*, sélectionnez le chemin suivant :

   \Protection Internet de F-Secure\Paramètres\Moteur pare-feu\Autoriser interface approuvée

Sélectionnez *Activé* pour activer l'interface approuvée pour le sous-domaine actuellement sélectionné. Cela permet aux utilisateurs finals du sous-domaine de configurer une interface réseau comme interface approuvée. Enregistrez et distribuez la stratégie pour appliquer la modification.

13.2.3 Filtrage de 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 *Paramètres de 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. Cet état est contrôlé par la variable :

1. Ouvrez le menu *Affichage* et sélectionnez l'option *Mode avancé*. L'interface utilisateur en mode avancé s'ouvre.
2. Sélectionnez *Racine* dans le volet *Domaines de stratégie*.
3. Sélectionnez l'onglet *Stratégie* dans le volet du milieu *Propriétés*.
4. Dans l'onglet *Stratégie*, sélectionnez le chemin suivant :

   \Protection Internet de F-Secure\Paramètres\Moteur pare-feu\Moteur pare-feu

Pour faire en sorte que le filtrage des paquets soit toujours activé, définissez cette variable sur *Oui* et cochez la case *Final*. N'oubliez pas de distribuer la stratégie pour appliquer la modification.

13.3 Configuration de la sélection automatique du niveau de sécurité

Dans cet exemple, 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 ces informations sont nécessaires pour définir les critères de sélection automatique du niveau de sécurité.

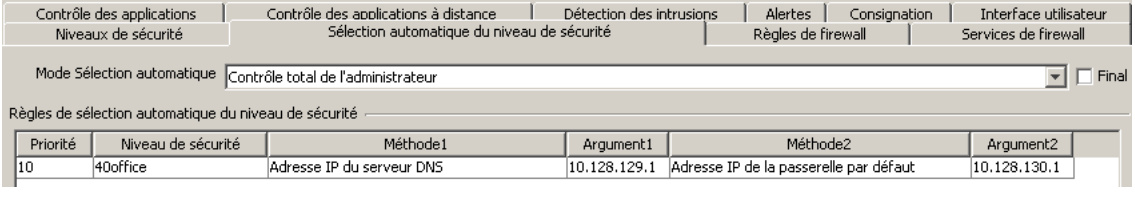
Vous pouvez identifier ces adresses en émettant une commande ipconfig -all à l'invite de commande.

1. Ouvrez le menu *Affichage* et sélectionnez l'option *Mode avancé*. L'interface utilisateur en mode avancé s'ouvre.
2. Sélectionnez le sous-domaine dans le volet *Domaines de stratégie*.
3. Sélectionnez l'onglet *Stratégie* dans le volet du milieu *Propriétés*.
4. Dans l'onglet *Stratégie*, sélectionnez le chemin suivant :

   \F-Secure\Protection Internet de F-Secure
5. Dans le volet de droite *Affichage produit*, sélectionnez la page *Sélection automatique du niveau de sécurité*.
6. Vérifiez 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*.
7. Cliquez sur **Ajouter** pour ajouter le premier niveau de sécurité, en l'occurrence *Bureau*.

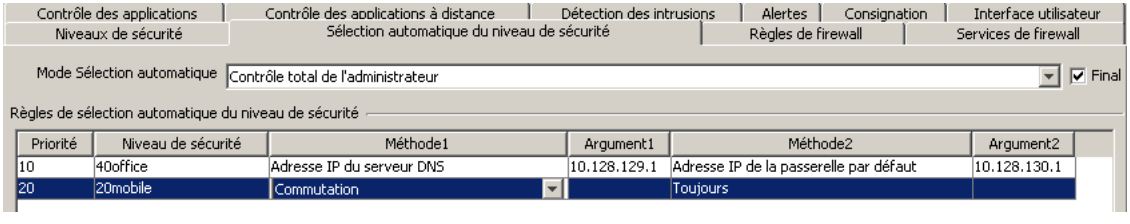
8. Pour entrer des données dans une cellule, sélectionnez la cellule et cliquez sur **Modifier**. Pour le niveau de sécurité *Bureau*, vous devez ajouter les données suivantes :
   - *Priorité :* les règles sont contrôlées dans l'ordre défini par les numéros de priorité, en commençant par le plus petit numéro.
   - Niveau de sécurité : entrez l'ID (composé du numéro et du nom) du niveau de sécurité, par exemple : *40bureau*.
   - *Méthode 1* : sélectionnez *Adresse IP du serveur DNS* dans la liste déroulante.
   - *Argument 1* : entrez l'adresse IP de votre serveur DNS local, par exemple : *10.128.129.1.*
   - *Méthode 2* : sélectionnez *Adresse IP de la passerelle par défaut* dans la liste déroulante.
   - *Argument 2* : entrez l'adresse IP de la passerelle par défaut. Par exemple : *10.128.130.1.*

   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.



9. Le premier niveau de sécurité est maintenant prêt. Cliquez sur **Ajouter** pour ajouter le deuxième niveau de sécurité, en l'occurrence *Mobile*.

10. Pour entrer des données dans une cellule, sélectionnez la cellule et cliquez sur **Modifier**. Pour le niveau de sécurité *Mobile*, vous devez ajouter les données suivantes :
    - *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, par exemple : 20*mobile*.
    - *Méthode 1* : sélectionnez *Accès à distance* dans la liste déroulante.
    - *Argument 1* : ce champ peut rester vide.
    - *Méthode 2* : sélectionnez *Toujours* dans la liste déroulante.
    - *Argument 2* : ce champ peut rester vide.



11. La configuration est maintenant prête.
12. Cliquez sur pour enregistrer les données de stratégie.
13. Cliquez sur pour distribuer la stratégie.

13.4 Dépannage de problèmes de connexion

S'il y a des problèmes de connexion, 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. Vérifiez que le problème ne provient pas du câble réseau.
2. Vérifiez qu'Ethernet est actif et fonctionne correctement.

3. Vérifiez que l'adresse DHCP est correcte. Pour ce faire, entrez la commande

   ipconfig

   à l'invite de commande.
4. 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

   à l'invite de commande. Ensuite, envoyez un ping à la passerelle par défaut pour voir si elle répond.
5. Si la navigation Internet normale ne fonctionne pas, vous pouvez essayer d'envoyer un ping à un serveur DNS.
6. Exécutez *nslookup* pour vous assurer que le service DNS fonctionne.
7. 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.
8. Ensuite, vérifiez si quelque chose a changé dans le domaine géré : une nouvelle stratégie est-elle utilisée et cette stratégie contient-elle des paramètres susceptibles de causer ces problèmes ?
9. Vérifiez dans les règles de pare-feu que les connexions HTTP sortantes sont autorisées.
10. 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.
11. 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.

13.5 Utilisation de la vérification de l'adresse IP et des ports avec le contrôle des applications

La vérification de l'adresse IP et des ports ne peut être utilisée qu'à partir de l'interface utilisateur locale.

Dans l'interface utilisateur de F-Secure Anti-Virus Client Security la page *Protection Internet* affiche le nombre d'applications Autorisées/refusées. Si vous souhaitez des informations plus détaillées sur les adresses autorisées et refusées ou si vous souhaitez configurer la vérification de l'adresse IP et des ports, procédez comme suit :

1. Cliquez sur Configurer... pour accéder à la page des paramètres avancés *Protection Internet*> *Contrôle des applications*.
2. Sélectionnez une application dans la liste et cliquez sur **Détails** pour consulter les adresses et ports autorisés et refusés.

La fenêtre *Propriétés de l'application* affiche les propriétés de l'application. Vous pouvez faire en sorte que l'application soit autorisée ou non à se connecter au réseau ou à accepter les connexions à votre ordinateur. La fenêtre *Propriétés de l'application* affiche les informations suivantes :

Informations sur l'application :	
Nom du fichier	Affiche le chemin et le nom du fichier exécutable. Vérifiez que ces informations se rapportent à la bonne application.
	Vous pouvez modifier le chemin de l'exécutable en cliquant sur **Parcourir**.
Description	Affiche la description interne du programme exécutable, généralement le nom de l'application. Vous pouvez également modifier cette description.
Informations sur la version	Affiche la description interne relative à la version du programme exécutable.

Le volet *Connexions connues* affiche toutes les listes d'autorisations et de refus. Vous pouvez modifier les listes d'autorisations et de refus en accédant à la liste à modifier. Ces listes apparaissent dans le volet de droite.

Adresses	Sortantes		Autorisées	Répertorie toutes les adresses IP sortantes auxquelles l'application est autorisée à se connecter.
Adresses	Sortantes		Refusées	Répertorie toutes les adresses IP sortantes auxquelles l'application n'est pas autorisée à se connecter.
Ports	Sortantes	TCP	Autorisées	Répertorie tous les numéros de ports TCP sortants auxquels l'application est autorisée à se connecter.
Ports	Sortants	TCP	Refusés	Répertorie tous les numéros de ports TCP sortants auxquels l'application n'est pas autorisée à se connecter.
Ports	Sortants	UDP	Autorisés	Répertorie tous les numéros de ports UDP sortants auxquels l'application est autorisée à se connecter.
Ports	Sortants	UDP	Refusé	Répertorie tous les numéros de ports UDP sortants auxquels l'application n'est pas autorisée à se connecter.
Ports	Entrants	TCP	Autorisés	Répertorie tous les numéros de ports TCP entrants auxquels l'application est autorisée à se connecter.

Ports	Entrants	TCP	Refusés	Répertorie tous les numéros de ports TCP entrants auxquels l'application n'est pas autorisée à se connecter.
Ports	Entrants	UDP	Autorisés	Répertorie tous les numéros de ports UDP entrants auxquels l'application est autorisée à se connecter.
Ports	Entrants	UDP	Refusés	Répertorie tous les numéros de ports UDP entrants auxquels l'application n'est pas autorisée à se connecter.

Cliquez avec le bouton droit de la souris sur l'entrée appropriée dans le volet de droite pour la modifier. Vous pouvez déplacer une entrée de la liste Autorisées vers la liste Refusées, ou inversement, supprimer une entrée ou résoudre l'adresse IP pour rechercher son nom DNS.

Vous pouvez déterminer ce qui se passe lorsque l'application essaie de se connecter au réseau, les sélections *Action sur une tentative de connexion inconnue* étant définies pour le *Client (sortant)*. Vous avez le choix entre les actions suivantes :

Sélections de l'action sur une tentative de connexion inconnue	
Vérifier	
Application uniquement	Vérifiez uniquement si l'application correspond à celle pour laquelle vous avez autorisé la connexion sortante à l'origine. Si c'est le cas, la connexion est autorisée. Sinon, l'action sélectionnée est exécutée.
Application et IP	Vérifiez que l'application correspond à celle pour laquelle vous avez autorisé la connexion sortante à l'origine et que la connexion à l'adresse IP demandée est autorisée. Si ces deux conditions sont remplies, la connexion est autorisée. Sinon, l'action sélectionnée est exécutée. Si *Action* a été configurée sur *Refuser*, l'adresse IP est ajoutée à la liste *Refusées*. Si *Action* a été configurée sur *Autoriser*, l'adresse IP est ajoutée à la liste *Autorisées*.

Sélections de l'action sur une tentative de connexion inconnue	
Application et port	Vérifiez que l'application correspond à celle pour laquelle vous avez autorisé la connexion sortante à l'origine et que la connexion au port demandé est autorisée. Si ces deux conditions sont remplies, la connexion est autorisée. Sinon, l'action sélectionnée est exécutée. Si *Action* a été configurée sur *Refuser*, le numéro de port est ajouté à la liste *Refusées*. Si *Action* a été configurée sur *Autoriser*, le numéro de port est ajouté à la liste *Autorisées*.
Action	
Refuser	Refuse la connexion au réseau à moins que les conditions de vérification ne soient remplies ou que l'adresse IP et le numéro de port figurent dans la liste *Autorisées*.
Autoriser	Autorise la connexion au réseau à moins que l'adresse IP distante ou le numéro de port figure dans la liste *Refusées*.
Invite	Invite à préciser l'action à entreprendre chaque fois que l'application se connecte au réseau, à moins que l'adresse distante ou le port réseau ne figure dans la liste Refusées ou *Autorisées*. Les adresses IP et les numéros de port de protocole sont regroupés dans les listes Autorisées et Refusées en fonction des paramètres de vérification.

Autorisation de certaines connexions et refus de toutes les autres :

Si vous souhaitez autoriser les connexions à certaines adresses IP ou certains ports et refuser toutes les autres connexions, procédez comme suit :

1. Assurez-vous que la liste Autorisées contient toutes les adresses IP ou numéros de ports où vous souhaitez autoriser les connexions.
2. Réglez *Action* sur *Refuser* et *Vérification* sur *Aucune vérification*.

Refus de certaines connexions et autorisation de toutes les autres :

Si vous souhaitez refuser les connexions à certaines adresses IP ou certains ports et autoriser toutes les autres connexions, procédez comme suit :

1. Vérifiez que toutes les adresses IP ou tous les numéros de port de protocole auxquels vous souhaitez refuser les connexions figurent dans la liste Refusées.
2. Réglez *Action* sur *Autoriser* et *Vérification* sur *Aucune vérification*.

13.6 Ajout de nouveaux services

Un service (abréviation de service de réseau) correspond à un service disponible sur le réseau, par exemple, le partage de fichier, 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.

13.6.1 Création d'un nouveau service Internet basé sur le port HTTP par défaut

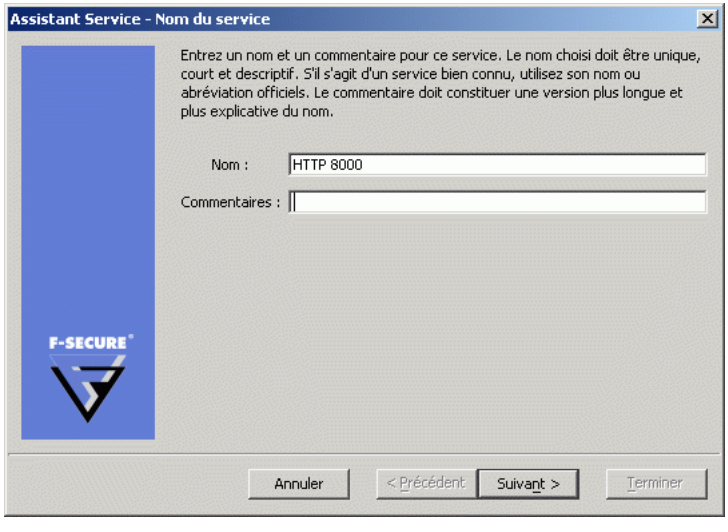
Dans cet exemple, on suppose qu'un serveur Web tourne sur un ordinateur et qu'il est configuré pour utiliser un port Web non standard. En règle générale, un serveur Web utiliserait le port TCP/IP 80, mais dans ce cas précis, il a été configuré de manière à utiliser le port 8000. Pour autoriser les connexions entre ce serveur et les postes de travail, vous allez devoir créer un service. Le service HTTP standard ne fonctionne pas ici parce que nous n'utilisons plus le port HTTP standard. Ce nouveau service est « *Port HTTP 8000* »et il est basé sur le service « *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 **Ajouter** pour démarrer l'Assistant des services de pare-feu.

Etape 1. Nom du service

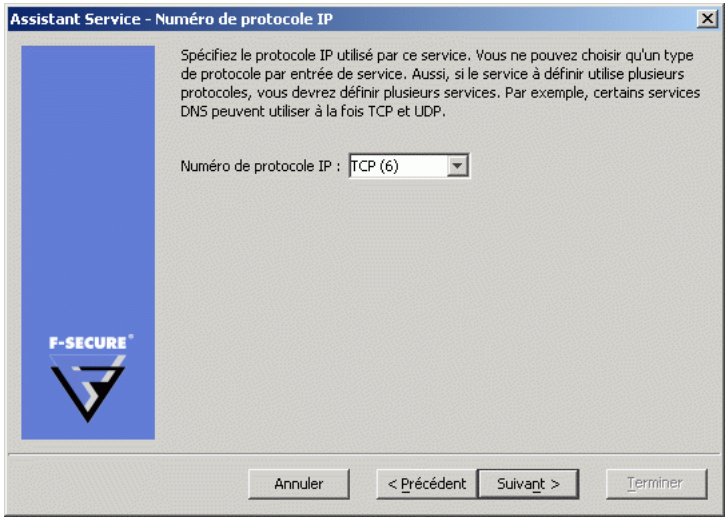
1. Renseignez le champ *Nom du service* en attribuant un nom unique au service. Deux services ne peuvent pas porter le même nom. Par exemple, Port HTTP 8000.
2. Entrez un commentaire décrivant le service dans le champ *Commentaire sur le service*. Le commentaire s'affichera dans la *Table des services de pare-feu*.



Etape 2. Numéro de protocole IP

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 à la table 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	Internet Control Message Protocol
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

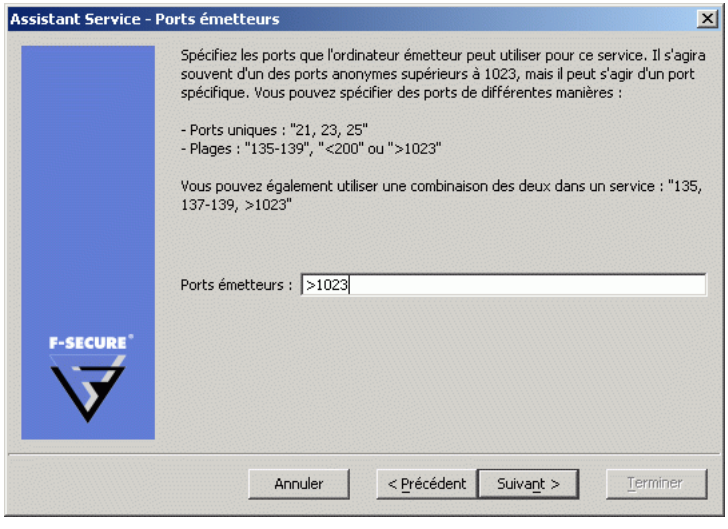
GRE	47	Cisco Generic Routing Encapsulation (GRE) Tunnel
ESP	50	Encapsulation Security Payload protocol
AH	51	Authentication Header protocol
PIM	103	Protocol Independent Multicast
COMP	108	Compression Header protocol
RAW	255	Raw IP packets

Etape 3. 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 ou inférieurs à *port*
- « *port* », uniquement le *port*
- « *minport-maxport* », *minport* et *maxport* plus tous les ports entre *minport* et *maxport*. Notez qu'il n'y a pas d'espace de part et d'autre du tiret.

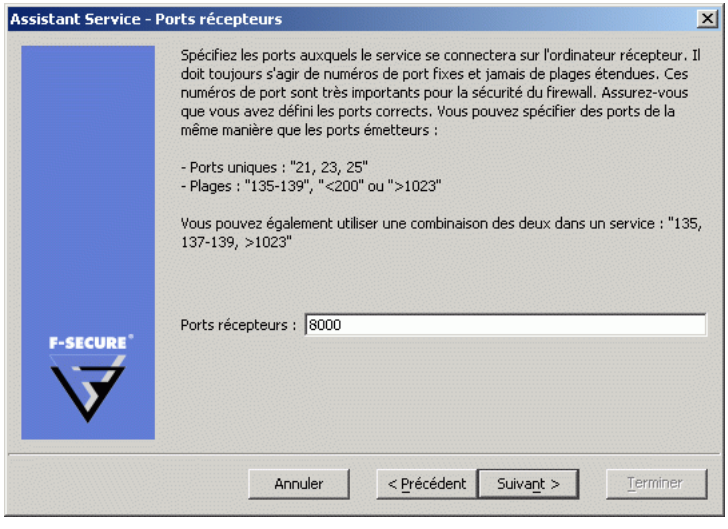
Vous pouvez définir des combinaisons de ces éléments, séparées par des virgules. Par exemple, les ports 10, 11, 12, 100, 101, 200 et supérieurs à 1023 peuvent être définis sous la forme « 10-12, 100-101, 200, >1023 ».



Dans cet exemple, définissez le port émetteur comme *>1023*.

Etape 4. Ports récepteurs

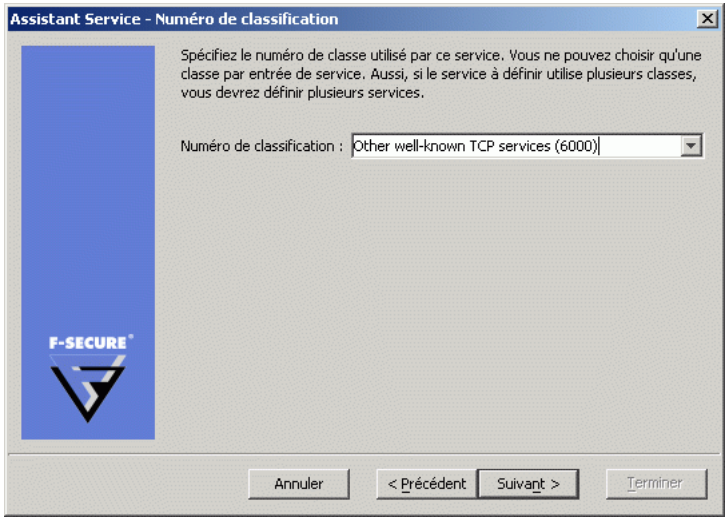
Si votre service utilise le protocole TCP ou UDP, vous devez définir les ports récepteurs couverts par le service.



Dans cet exemple, définissez le port récepteur comme *8000*.

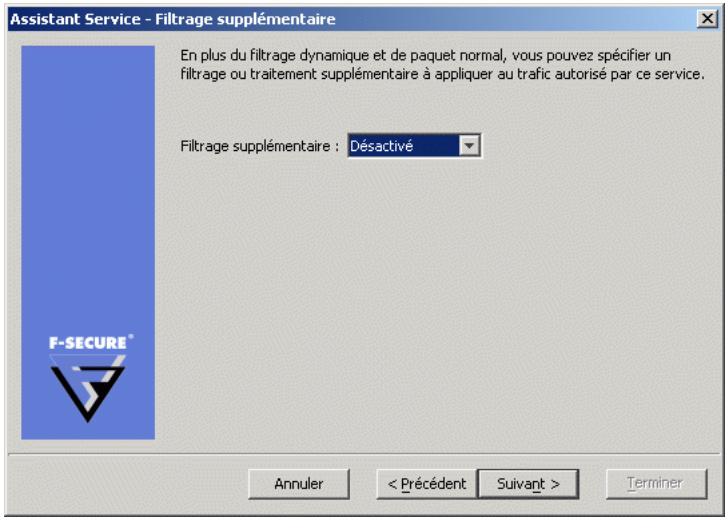
Etape 5. Numéro de classification

Sélectionnez un numéro de classification pour ce service dans la liste déroulante. Vous pouvez accepter la valeur par défaut.



Etape 6. Filtrage supplémentaire

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.

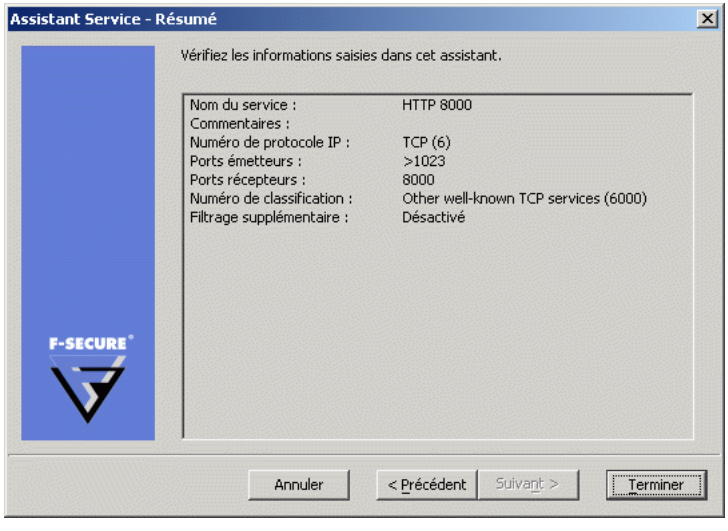


Dans cet exemple, vous pouvez accepter la valeur par défaut, qui est *Désactivé*.

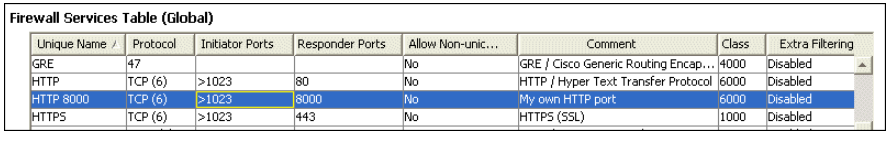
Lorsque le service utilise le protocole TCP et que la fonction Contrôle des applications n'est pas activée, vous pouvez sélectionner Mode FTP actif dans le menu déroulant Filtrage supplémentaire. Le mode FTP actif exige un traitement spécial de la part du pare-feu, car les informations concernant le port à ouvrir pour la connexion sont incluses dans les données transférées.

Etape 7. Vérification et acceptation de la règle

1. Vous pouvez maintenant vérifier la règle. Si vous devez apporter un changement quelconque à la règle, cliquez sur **Précédent** dans la règle.



2. Cliquez sur **Terminer** pour fermer l'Assistant Règle. La règle que vous venez de créer est maintenant affichée dans le *Table des règles de pare-feu*.



Etape 8. 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 firewall HTTP 8000 dans le niveau de sécurité de la protection Internet actuellement utilisé. Pour de plus amples informations sur la procédure à suivre, reportez-vous à la section "*Ajout d'une nouvelle règle de la protection Internet avec alerte*", *212*. Dans ce cas, vous pouvez

sélectionner le nouveau service dans la fenêtre *Assistant Règle - Service* et vous ne devez définir aucune alerte dans la fenêtre *Assistant Règle - Options avancées*.

A ANNEXE : Modification de PRODSETT.INI

A.1 Présentation

Le fichier *Prodsett.ini* indique au programme d'installation les modules à installer, ainsi que leur emplacement d'installation (répertoires de destination) sur les postes de travail. Cette annexe présente la liste des paramètres pouvant être modifiés dans *prodsett.ini*.

AVERTISSEMENT : ne modifiez pas de paramètres de prodsett.ini qui ne sont pas inclus dans cette annexe.

Dépendance entre les paramètres RequestInstallMode et InstallMode :
Les paramètres RequestInstallMode ont préséance sur la sélection des composants dont InstallMode=0.

A.2 Paramètres configurables dans Prodsett.ini

Vous pouvez modifier les paramètres suivants dans le fichier *prodsett.ini*.

[F-Secure common]	Paramètres communs
CD-Key=XXXX-XXXX-XXXX-XXXX-XXXX	Entrez la clé de CD 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.

[F-Secure common]	Paramètres communs
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.

[F-Secure common]	**Paramètres communs**
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. 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 : lorsque 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. *Remarque : cette option exécute un « redémarrage normal » de l'hôte et donc, dans certains cas, l'utilisateur peut retarder le redémarrage et même l'empêcher complètement.* (valeur par défaut) 3 = Ne pas redémarrer l'ordinateur après l'installation.

[FSMAINST.DLL]	Paramètres de F-Secure 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 ni InstallMode.
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 !

[FSMAINST.DLL]	Paramètres de F-Secure Management Agent
UseOnlyUID=	0 = F-Secure Management Agent utilise uniquement toutes les identités disponibles (nom DNS, adresse IP, nom WINS, Identité unique) pour s'identifier la première fois auprès du F-Secure Policy Manager Server. 1 = F-Secure Management Agent utilise uniquement son Identité unique pour s'identifier auprès du F-Secure 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 ni InstallMode.
[PMSUINST.DLL]	**Paramètres pour la prise en charge de F-Secure 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 ni InstallMode.
FsmsServerUrl=http://fsmsserver	URL vers le F-Secure Policy Manager Server.
FsmsExtensionUri=/fsms/fsmsh.dll	Ne modifiez pas ce paramètre.

[PMSUINST.DLL]	Paramètres pour la prise en charge de F-Secure Policy Manager
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 ni InstallMode.

[FSAVINST.DLL]	Paramètres pour F-Secure Client Security - Protection antivirus
RequestInstallMode=1	0 = Installer ce composant tel que défini dans le paramètre InstallMode. 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.
DeleteOldDirectory=0	0 = Si F-Secure Anti-Virus 4.x est installé sur l'ordinateur, F-Secure Anti-Virus 5.x ne sera pas installé et l'installation sera abandonnée. Ce paramètre s'applique en mode d'installation silencieuse uniquement (valeur par défaut). 1 = Si F-Secure Anti-Virus 4.x est installé sur l'ordinateur, F-Secure Anti-Virus 5.x sera installé et F-Secure Anti-Virus 4.x sera désinstallé. Le répertoire d'installation de F-Secure Anti-Virus 4.x et tous les fichiers (y compris dans tous les sous-répertoires) seront supprimés. Ce paramètre s'applique en mode d'installation silencieuse uniquement.
InstallService_F-Secure AVP=1	0 = Ne pas installer AVP (NT4, Win2000, WinXP). 1 = Installer (valeur par défaut).
InstallService_F-Secure Libra=1	0 = Ne pas installer Libra (NT4, Win2000, WinXP). 1 = Installer (valeur par défaut).
InstallService_F-Secure Orion=1	0 = Ne pas installer Orion (NT4, Win2000, WinXP). 1 = Installer (valeur par défaut).

[FSAVINST.DLL]	Paramètres pour F-Secure Client Security - Protection antivirus
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 paramètres RequestInstallMode ni InstallMode.

[FSSGSUP.DLL]	Paramètres du module de détection et d'élimination des conflits
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 ni InstallMode.
SidegradeAction=0	0 = Supprimer automatiquement tous les conflits détectés. (valeur par défaut) 1 = Annuler l'installation si un logiciel faisant conflit est installé.

[MEHINST.DLL]	Paramètres pour la prise en charge de SNMP
RequestInstallMode=1	0 = Installer ce composant tel que défini dans le paramètre InstallMode. 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.

[ES_Setup.DLL]	Paramètres d'installation de l'analyse de courrier électronique
RequestInstallMode=1	0 = Installer ce composant tel que défini dans le paramètre InstallMode. 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.

[FWESINST.DLL]	Paramètres pour le composant interne commun FWES.
RequestInstallMode=1	0 = Installer ce composant tel que défini dans le paramètre InstallMode. 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 F-Secure Client Security - Protection Internet
RequestInstallMode=1	0 = Installer ce composant tel que défini dans le paramètre InstallMode. 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.
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 de F-Secure Automatic Update Agent
RequestInstallMode=1	0 = Installer ce composant tel que défini dans le paramètre InstallMode. 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 pour F-Secure Client Security - Analyseur de réseau
RequestInstallMode=1	0 = Installer ce composant tel que défini dans le paramètre InstallMode. 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.

[FSPSINST.DLL]	Paramètres pour F-Secure Client Security - Analyseur de réseau
DisableScanningForApps= Wget.exe,mplayer.exe	Désactiver l'analyse réseau pour certains exécutables. C'est une liste de noms d'exécutables sans chemin d'accès, séparée par des virgules. 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 pour la prise en charge de NAC Cisco
RequestInstallMode=1	0 = Installer ce composant tel que défini dans le paramètre InstallMode. 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.

B ANNEXE : Messages d'alerte et d'erreur de l'analyse du courrier électronique

B.1 Présentation

Cette section fournit une liste des messages d'alerte et d'erreur que l'analyse du courrier électronique.

Echec de la session d'analyse du courrier électronique : erreur système

ID du message : 602

Message : « La connexion au serveur <nom du serveur> a été terminée par la fonction d'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

ID du message : 603

Message : « 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

ID du message : 604

Message : « 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

ID du message : 610

Message : « Echec de l'initialisation de la fonction d'analyse du courrier électronique, motif : <pour obtenir la raison, voir ci-dessus> »

Alerte : virus dans une pièce jointe

ID du message : 620-623

Définition : Lorsqu'un virus est trouvé, il est traité en fonction de la configuration avancée de F-Secure Anti-Virus Client Security. Les options de traitement des virus sont : Avertir uniquement, nettoyer ou éliminer.

Possibilités d'actions effectuées :

- L'infection a uniquement été signalée.
- La pièce jointe a été nettoyée.
- La pièce jointe a été supprimée.
- Le message électronique infecté a été bloqué.

Message :

```
Alerte : virus trouvé dans le courrier électronique.
Infection : <Nom du virus>
Pièce jointe : <Partie du message, fichier joint qui était
infecté>
Action : <Action effectuée>
Message <ID du message>
  De : <En-tête de message : adresse enregistrée de
l'expéditeur>
  A : <En-tête de message : adresse enregistrée du
destinataire>
  Objet : <En-tête de message : Objet enregistré du message>
```

Alerte : courrier électronique déformé

ID du message : 630-633

Définition : Lorsqu'un message déformé est trouvé, il est traité en fonction de la configuration avancée de F-Secure Anti-Virus Client Security. Les options de traitement des messages déformés sont : La partie déformée du message a uniquement été signalée, La partie déformée du message a été supprimée, Le message électronique déformé a été bloqué.

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.

Message :

```
Alerte : courrier électronique déformé.
Description : <description de la déformation.>
Partie du message : <partie du message déformée>
Action : <Action effectuée>
Message <ID du message>
  De : <En-tête de message : adresse enregistrée de
l'expéditeur>
  A : <En-tête de message : adresse enregistrée du
destinataire>
  objet : <En-tête de message : Objet enregistré du message>
```

Echec de l'analyse d'une pièce jointe à un message électronique

ID du message : 640-643

Définition : Lorsqu'une analyse échoue, le message est traité en fonction de la configuration définie dans la configuration avancée. Les options de traitement d'un message qui ne peut être correctement analysé sont : L'échec de l'analyse a uniquement été signalé, La pièce jointe a été supprimée, Le message a été bloqué.

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.

Message :

Echec de l'analyse d'une pièce jointe à un message électronique

Motif : <Description de l'échec de l'analyse.>

Pièce jointe : <Pièce jointe à l'origine de l'échec>

Action : <Action effectuée>

Message <ID du message>

De : <En-tête de message : adresse enregistrée de l'expéditeur>

A : <En-tête de message : adresse enregistrée du destinataire>

objet : <En-tête de message : Objet enregistré du message >

GLOSSAIRE

ActiveX

ActiveX est un ensemble de technologies de Microsoft activant le contenu interactif pour le World Wide Web. Etant donné que les paramètres de sécurité d'ActiveX dans Internet Explorer permettent d'autoriser les pages Web à installer automatiquement les commandes d'ActiveX en arrière-plan, ils peuvent représenter une menace de sécurité importante. Les commandes d'ActiveX peuvent accéder aux fichiers contenus sur votre disque dur.

logiciel publicitaire

Un logiciel publicitaire est un logiciel espion regroupant des informations personnelles et les envoyant à un publicitaire afin d'afficher des fenêtres publicitaires lorsque vous naviguez sur Internet. Un logiciel publicitaire suit généralement votre comportement de navigation sur le Web et l'envoie à des tiers sans votre autorisation ou sans que vous ne le sachiez.

Alerte

Message généré par un produit F-Secure en cas de problème avec un programme ou une opération. Des alertes sont également générées lorsqu'un virus est détecté. L'administrateur et l'utilisateur peuvent définir les alertes à générer soit en définissant des règles de firewall soit en activant ou en désactivant des alertes spécifiques. L'acceptation ou le refus d'un paquet réseau spécifique, des paquets comportant des indicateurs incorrects, des fragments trop petits ou une fragmentation incorrecte constituent également des événements générateurs d'alertes.

Application

Programme logiciel écrit pour un usage spécifique. Généralement, les applications sont démarrées manuellement.

Contrôle des applications

Le contrôle des applications est une fonction de protection Internet de F-Secure qui vérifie automatiquement si une application est autorisée à se connecter à Internet à partir de votre ordinateur en contrôlant si l'application figure dans la liste des logiciels sûrs (pré-approuvés) et des logiciels malveillants connus (chevaux de Troie, etc.).

Authentification

Acte de vérification de l'identité de quelqu'un.

Autorisation

Droit d'exécuter une action sur un objet. Il s'agit également de l'acte de prouver ce droit.

Porte dérobée

Application ou extension malveillante qui ouvre une possibilité pour un utilisateur distant d'accéder à l'ordinateur attaqué. Il s'agit très souvent d'une application qui ouvre un ou plusieurs ports d'écoute et attend des connexions de l'extérieur, mais il existe des variantes de ce schéma. Nombre de virus, chevaux de Troie et vers installent des portes dérobées pour perpétrer leurs méfaits.

Bit

Plus petite unité de taille de mémoire ; ces unités sont regroupées en ensembles appelés octets organisés en schéma séquentiel pour exprimer du texte, des nombres ou d'autres informations détaillées reconnaissables par l'unité centrale de l'ordinateur.

Trafic de diffusion

Le trafic de diffusion provient d'un ordinateur spécifique et est envoyé à l'ensemble d'un réseau ou d'un sous-réseau. Ce trafic utilise généralement les mécanismes de diffusion du réseau local (p. ex. Ethernet) et n'est pas transféré entre réseaux.

Détournement du navigateur

Une application qui tente de contrôler votre page de démarrage Web ou d'autres sites Web susceptibles d'être consultés, est appelée un programme tentant de détourner votre navigateur. Le programme tentant de détourner votre navigateur essaie de vous amener à consulter un site Web pour influer le trafic en vue d'augmenter les revenus liés à la publicité.

Octet

Ensemble de bits représentant un seul caractère. Un octet comprend 8 bits.

Certificat

Voir Clé publique.

Client

Programme utilisé pour communiquer avec un programme serveur installé sur un autre ordinateur et en obtenir des données.

Connexion

Raccourci pour « connexion réseau ». Ce terme désigne soit la connexion entre l'ordinateur et le réseau, soit des connexions individuelles établies avec des hôtes distants à partir de l'ordinateur local ou à partir d'hôtes distants avec l'ordinateur local. Pour TCP, ce terme équivaut à « connexion TCP » ; pour les autres protocoles TCP/IP, il désigne tous les datagrammes appartenant à la même session de communication.

Corrompu

Relatif à des données modifiées ou altérées sans l'autorisation ou l'accord de l'utilisateur.

Analyse de données

L'analyse de données est un programme pouvant collecter des informations personnelles sur votre navigation et utilisation des sites Web, notamment des données regroupées à partir de formulaires renseignés et soumis pour différents sites Web. L'analyse de données est généralement exécutée sans que vous le sachiez.

DoS (refus de service)

Tentative explicite de pirates informatiques d'empêcher les utilisateurs légitimes d'accéder à un service en interrompant les connexions, en « inondant » un réseau ou en empêchant un individu d'accéder au réseau.

Assistant de nettoyage

Une boîte de dialogue de l'interface utilisateur qui guide l'utilisateur dans le nettoyage de virus. Cet assistant apparaît sur l'interface utilisateur locale lorsqu'un virus est détecté.

Nom de domaine

Nom unique qui identifie un site Internet (par exemple, F-Secure.com).

DNS (système de nom de domaine)

DNS est la façon dont les noms de domaines Internet sont localisés et convertis en adresses IP (Internet Protocol). Un nom de domaine est un « pointeur » facile à retenir et menant à une adresse Internet. Par exemple, l'adresse Internet www.un.domaine.org est un nom DNS.

Analyse du courrier électronique

Analyse et nettoyage des messages électroniques afin d'éliminer les virus et le contenu malveillants dans la pile réseau d'un hôte. Il vise à éviter que des virus et tout autre contenu malveillant infecte le client de messagerie électronique de l'hôte.

Observateur d'événements

Module qui tient à jour des fichiers journaux sur les événements de programme, sécurité et système de votre ordinateur. Vous pouvez utiliser l'observateur d'événements pour visualiser et gérer les journaux d'événements, collecter des informations sur les problèmes de matériel et de logiciel, ainsi que pour surveiller les événements de sécurité Windows.

Extension

Raccourci pour : extension de fichier. L'extension de fichier est le suffixe ajouté à un nom de fichier pour indiquer le type du fichier. Par exemple, l'extension EXE indique que le fichier est exécutable.

Fausse alerte

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

Pare-feu

Combinaison de matériel et de logiciels qui fractionne un réseau en deux zones ou plus pour des raisons de sécurité.

FTP

Méthode très répandue de transfert de fichiers entre deux sites Internet.

Heuristique

Méthode exploratoire de résolution de problèmes utilisant des techniques d'auto-apprentissage.

Application cachée

Les applications cachées ne sont pas visibles, le processus de l’application et le fichier sont tous deux cachés pour les utilisateurs. Il est possible d’un rootkit masque l’application dans le gestionnaire des tâches Windows.

Lecteur caché

Les lecteurs cachés ne sont pas visibles pour les utilisateurs.

Fichier caché

Les fichiers cachés ne sont pas visibles pour les utilisateurs. Il est possible qu’un rootkit masque le fichier de la liste de fichiers classique.

Processus caché

Les processus cachés ne sont pas visibles pour les utilisateurs. Il est possible d’un rootkit masque le processus dans le gestionnaire des tâches Windows.

Hôte

Tout ordinateur en réseau qui met des services à disposition des autres ordinateurs du réseau.

HTTP

Protocole utilisé entre un navigateur Web et un serveur afin de demander un document et d'en transférer le contenu. Cette spécification est utilisée et développée par le World Wide Web Consortium.

Système de détection des intrusions (IDS)

Composant de protection Internet qui analyse le trafic réseau entrant à la recherche de certains modèles indiquant qu'une attaque du réseau est en cours.

IMAP

Internet Mail Application Protocol. Protocole semblable à POP, si ce n'est que les messages électroniques sont généralement traités sur le serveur au lieu d'être téléchargés sur le poste de travail.

IP

Internet Protocol. Protocole d'adressage des paquets TCP. Lorsque des données sont envoyées avec TCP, IP est utilisé pour étiqueter le paquet avec les adresses de l'expéditeur et du destinataire.

Adresse IP

Adresse utilisée par le protocole IP (Internet Protocol). Adresse réseau unique composée de 4 chaînes numériques séparées par des points. Cette structure est modifiée dans l'IPv6.

IPSec (protocole de sécurité IP)

(IETF) Protocole conçu afin d'obtenir une protection cryptographique de qualité compatible avec l'IPv4 et l'IPv6. Les services de protection offerts sont le contrôle de l'accès, l'intégrité en cas de rupture de connexion, l'authentification de l'origine des données, un service interdisant la relecture, la confidentialité (cryptage) et la confidentialité limitée du trafic. Ces services sont proposés au niveau de la couche IP, offrant ainsi une protection pour IP et/ou les protocoles des couches supérieures.

FAI

Fournisseur d'accès à l'Internet. Organisme qui permet d'accéder à Internet d'une façon ou d'une autre.

JAR

Java ARchive. Format de fichier permettant de regrouper de nombreux fichiers afin d'en créer un seul.

Mode noyau

Partie du système d'exploitation Windows dans laquelle, entre autres, les applications en mode utilisateur et les services emploient une API pour interagir avec le matériel de l'ordinateur. Le mode noyau contient également une interface avec le mode utilisateur et un système de synchronisation de ses services et de coordination de toutes les fonctions d'E/S. La mémoire du mode noyau est protégée contre tout accès par le mode utilisateur.

LAN

(Local Area Network, ou réseau local) Réseau d'ordinateurs limité à un site, généralement l'immeuble ou l'étage d'un immeuble. Un protocole de réseau simple est parfois utilisé.

En-tête incorrect

En-tête de message électronique incorrect. Il s'agit généralement d'un codage non standard du format MIME. La déformation est causée par un ver, une personne malveillante ou une erreur dans le client qui envoie le message. Un nombre en rapide croissance de vers utilise des messages déformés pour se répandre.

Antiprogramme

Programmes ou fichiers développés dans le but de nuire. Cela comprend les virus informatiques, les vers et les chevaux de Troie.

Mbit

Mégabit.

MIB

(Terminologie SNMP) Base des informations d'administration. Vous trouverez des informations détaillées sur les MIB dans les documents RFC1155-SMI, RFC1212-CMIB et RFC1213-MIB2.

MIME

Multipurpose Internet Mail Extension, un système standard d'identification du type de données contenu dans un fichier d'après son extension. MIME est un protocole Internet qui permet d'envoyer des fichiers binaires via l'Internet sous la forme de pièces jointes à des messages électroniques. Ces fichiers comprennent : graphiques, photos, son et vidéo ainsi que des documents texte formatés.

Trafic multidiffusion

Le trafic multidiffusion provient d'un hôte spécifique (généralement un serveur) et est destiné à un groupe de multidiffusion. Dans IP (Internet Protocol), les groupes correctement configurés utilisent les adresses de réseau multidiffusion (comprises entre 224.0.0.0 et 239.255.255.255) définies pour IP. La gestion des membres du groupe et le transfert du trafic multidiffusion sur les commutateurs et routeurs sont assurés par IGMP (Internet Group Management Protocol).

Masque de réseau

Cet élément décrit comment l'adresse IP est divisée entre la partie réseau et la partie hôte.

Réseau

Plusieurs ordinateurs connectés entre eux afin de partager des ressources. Plusieurs réseaux connectés entre eux constituent un interréseau.

Paquet

Unité de données acheminée entre une origine et une destination sur Internet. Lorsqu'un fichier (p. ex. un message électronique) est envoyé d'un endroit à un autre sur Internet, il est fractionné en paquets d'une taille appropriée pour assurer un routage efficace. Une fois tous les paquets parvenus à destination, ils sont assemblés pour reconstituer le fichier d'origine.

Consignation de paquets

La consignation de paquets est un outil servant à analyser le trafic réseau, collecter des traces de comportement illicite, etc. Elle consiste à copier dans un fichier la charge et les en-têtes de tout le trafic réseau vu par un ordinateur, afin de le consulter ultérieurement. La protection Internet enregistre les paquets dans le format tcpdump, qui est lisible par la plupart des outils d'analyse de réseau.

Ping

Envoi de paquets ICMP et attente de paquets en réponse afin de vérifier les connexions vers un ou plusieurs ordinateurs distants.

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.

Gestion par stratégies

Contrôle des opérations et configuration d'un système à l'aide de stratégies.

POP

Post Office Protocol. Mode le plus courant de récupération des messages électroniques d'un serveur de messagerie vers les postes de travail des utilisateurs par des clients de messagerie tels qu'Eudora, Netscape Messenger ou Pegasus.

Clé privée

Zone confidentielle de la clé dans un système de clé publique. Elle ne peut être utilisée que par son propriétaire. Clé utilisée pour décrypter des messages et créer des signatures numériques.

Niveau de protection

Niveaux de protection préconfigurés définissant votre niveau de sécurité. Ils sont automatiquement mis à jour pour garantir votre protection contre les formes les plus récentes de programmes malveillants et d'attaques via Internet.

Protocole

Raccourci de « protocole réseau » ; spécification formelle, détaillée d'un format de communication. Le protocole sert à permettre à tous les participants d'une communication de décoder et comprendre la communication. Dans ce document, le terme réfère le plus souvent à TCP/IP (Transmission Control Protocol/Internet Protocol) et à ses sous-protocoles.

Clé publique

Partie de la clé largement diffusée (et non maintenue sécurisée) dans un système de clé publique. Cette clé est utilisée pour le cryptage (non pour le décryptage) ou la vérification des signatures. La clé publique contient également d'autres informations sur l'objet, l'émetteur, la durée de vie, etc.

Quarantaine

Les éléments mis en quarantaine sont isolés de sorte qu'ils ne représentent plus une menace pour votre ordinateur.

La quarantaine contient toutes les applications détectées pendant l'analyse et mises en quarantaine. Vous pouvez mettre de nouvelles applications en quarantaine lorsque la Protection antivirus et antispyware les détecte.

Facteur aléatoire

Valeur de facteur utilisée pour initialiser le générateur de nombres aléatoires, mise à jour chaque fois qu'une application F-Secure est fermée.

Riskware

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 d'un ordinateur vers l'autre via Internet. Si vous avez installé ce programme de manière explicite, les risques sont moindres. Si le riskware est installé à votre insu, il est fort probable qu'il s'agisse d'une intention malveillante et il doit être supprimé. La différence entre un riskware et un antiprogramme (« malware ») est que l'antiprogramme a été conçu en particulier pour endommager votre ordinateur.

Rootkit

Les rootkits servent typiquement à masquer les logiciels malveillants des utilisateurs, des outils systèmes et des scanneurs antivirus. Tous les rootkits ne sont pas dangereux en soi mais ils sont souvent utilisés pour masquer des virus, des vers, des chevaux de Troie et des logiciels espions.

Serveur

Ordinateur ou composant logiciel qui fournit un type de service spécifique au logiciel client.

Service

Un service (abréviation de service de réseau) correspond à un service disponible sur le réseau, par exemple, le partage de fichier, 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.

SMTP

Simple Mail Transfer Protocol. Protocole TCP utilisé pour transmettre du courrier électronique entre les ordinateurs des utilisateurs finals et les serveurs de messagerie.

SNMP

Protocole de gestion de réseaux simples (Simple Network Management Protocol). Protocole TCP/IP standard pour le contrôle et la configuration des paramètres réseau et compteurs de répéteurs, ponts, routeurs et autres périphériques connectés à un réseau LAN (réseau local d'entreprise) ou WAN (réseau étendu). Dans F-Secure Policy Manager, il sert à envoyer et contrôler des alertes et statistiques.

Logiciel espion

Un logiciel espion est un logiciel pistant les informations utilisateur et les communiquant sans que vous le sachiez à des tiers via Internet. Généralement, un logiciel espion collecte des informations sur votre comportement de navigation à des fins de publicité, mais il peut également transférer des informations ou fichiers personnels de votre ordinateur, surveillez vos séquences de frappe au clavier ou modifier la configuration de votre navigateur Web. Les applications de logiciels espions peuvent être installées sur votre ordinateur sans votre autorisation et à votre insu, lors de l'installation d'un autre logiciel.

Sous-réseau

Section d'un réseau. Les ordinateurs situés dans le même sous-réseau sont généralement proches les uns des autres physiquement et ont des adresses IP qui commencent par les deux ou trois mêmes chiffres.

Journal des événements système

Service qui enregistre les événements dans les journaux du système, de la sécurité et des Application. Les événements F-Secure Client Security sont enregistrés dans des journaux Application.

Résultat TAC

Le résultat TAC détermine la probabilité qu'une application soit un antiprogramme, 1 étant la plus faible et 10 étant la plus forte. Le produit ne vous signale pas les objets dont le résultat est inférieur à 2.

TCP/IP

(Transmission Control Protocol/Internet Protocol, ou protocole de contrôle de transmission/protocole Internet) Ensemble de protocoles définissant Internet. Initialement conçues pour le système d'exploitation UNIX, des versions de TCP/IP sont désormais disponibles pour la plupart des systèmes d'exploitation. Pour accéder à Internet, votre ordinateur doit disposer du protocole TCP/IP.

Fichier texte

Tout fichier créé par un utilisateur et dont le contenu est destiné à être interprété comme une séquence d'une ligne ou plus composée de caractères imprimables ASCII ou latins.

Cookie de suivi

Les cookies de suivi pistent votre comportement de navigation Web. Ils peuvent collecter des informations sur les pages et publicités que vous avez vues ou sur toute autre activité lors de la navigation. Différents sites Web peuvent partager des cookies de suivi et chaque site Web ayant le même cookie de suivi peut y lire et écrire de nouvelles informations.

Cheval de Troie

Un cheval de Troie est généralement un programme exécutant des actions destructives ou dangereuses. Les actions destructives peuvent aller de l'effacement ou de la modification du contenu de fichiers sur un disque dur à une destruction complète des données.

Un cheval de Troie indirect est un outil d'accès distant permettant à un pirate de contrôler complètement le système infecté. Il peut envoyer, recevoir et exécuter des fichiers, voire écouter et voir le résultat sur votre ordinateur s'il dispose d'un microphone ou d'une Webcam.

Trafic monodiffusion

Trafic entre un ordinateur spécifique et un autre ordinateur spécifique.

URL

(Localisateur uniforme de ressources) Méthode standard d'identification de l'adresse d'une ressource Internet.

Mode Utilisateur

Zone protégée d'un système d'exploitation où les applications utilisateur sont exécutées et qui fait appel au mode Noyau afin d'activer les fonctions du système d'exploitation.

Virus

Programme qui se répand en se reproduisant.

Définitions de virus

Utilisées pour détecter des virus. Chaque fois qu'un nouveau virus est trouvé, la base de données doit être mise à jour afin que la protection antivirus puisse le détecter.

VPN

Réseau privé virtuel. Réseau privé sécurisé qui utilise le réseau Internet public existant.

WAN

(Wide Area Network, ou réseau étendu) Réseau ou interréseau qui couvre une zone plus vaste que celle d'un immeuble ou d'un campus.

Ver

Programme capable de se répliquer par l'insertion de copies dans les ordinateurs reliés en réseau.

Support technique

Présentation

Le support technique est disponible depuis le site Web de F-Secure. Vous pouvez y accéder depuis les applications F-Secure ou avec un navigateur Web.

Web Club

Le Web Club F-Secure propose une assistance aux utilisateurs des produits F-Secure. Pour y accéder, choisissez la commande Web Club du menu Aide de l'application F-Secure. A la première utilisation de cette option, entrez le chemin d'accès et le nom de votre navigateur Web ainsi que votre pays de résidence.

Pour vous connecter directement au Web Club depuis votre navigateur Web, entrez l'adresse suivante :

http://www.f-secure.com/webclub/

Descriptions de virus sur le Web

F-Secure Corporation met régulièrement à jour une base de données complète d'informations sur les virus informatiques sur son site Web. Vous pouvez consulter cette base de données d'informations sur les virus à partir du site :

http://www.f-secure.com/virus-info/.

Support technique avancé

Pour obtenir un support technique avancé, contactez le centre d'assistance technique de F-Secure à l'adresse http://support.f-secure.com/ ou contactez directement votre revendeur local F-Secure.

Pour obtenir l'assistance technique de base, veuillez contacter votre revendeur F-Secure.

Veuillez inclure les informations suivantes avec votre demande :

1. Nom et numéro de version de votre logiciel F-Secure (y compris le numéro de révision).
2. Nom et numéro de version de votre système d'exploitation (y compris le numéro de révision).
3. Description détaillée du problème, y compris tout message d'erreur affiché par le programme, ainsi que tout détail susceptible de nous aider à reproduire le problème.

Lorsque vous contactez F-Secure par téléphone, procédez comme suit afin que nous puissions vous aider plus efficacement et gagner du temps :

- Tenez-vous à proximité de votre ordinateur afin de pouvoir suivre les instructions fournies par le technicien ou apprêtez-vous à noter les instructions.
- Mettez l'ordinateur sous tension et, si possible, dans l'état où il se trouvait lorsque le problème est survenu. Vous devriez pouvoir reproduire le problème sur l'ordinateur avec un minimum d'efforts.

Après l'installation du logiciel F-Secure, vous trouverez peut-être un fichier ReadMe dans le dossier F-Secure (menu Démarrer→Programmes de Windows). Ce fichier contient les informations les plus récentes au sujet du produit.

Formation technique aux produits F-Secure

F-Secure fournit à ses distributeurs, revendeurs et clients une assistance, des documents et des informations techniques qui leur permettent d'utiliser correctement les produits et services de sécurité F-Secure. Des formations peuvent également être fournies pas les partenaires de formation certifiés de F-Secure. Ces outils et l'expérience de nos partenaires leur permettent de se distinguer de la concurrence en offrant une solution exclusive et puissante de sécurité en entreprise, tout en obtenant des niveaux de satisfaction de la clientèle élevés et en accroissant leur part de marché et leurs bénéfices.

Programme de formation

Pour plus d'informations sur les formations que nous proposons, accédez à notre page Web consacrée aux formations techniques aux produits F-Secure, à l'adresse suivante :

http://www.f-secure.com/products/training/

Les formations se donnent dans des locaux modernes et dotés de tous les équipements requis. Toutes nos formations comprennent une partie théorique et des exercices pratiques. Un examen de certification est organisé au terme de chaque formation. Pour plus d'informations sur les cours et les horaires, contactez votre bureau F-Secure local ou votre partenaire de formation certifié F-Secure.

Contacts

Questions générales : Training@f-secure.com

Inscription : Training-Registration@f-secure.com

Commentaires : Training-Feedback@f-secure.com

A propos de F-Secure Corporation

F-SecureCorporation est l'entreprise de l'industrie antivirus et de la prévention des intrusions affichant la plus forte croissance avec plus de 50 % de progression du chiffre d'affaires en 2004. Fondée en 1988, la société F-Secureest cotée sur le marché boursier d'Helsinki (Helsinki Stock Exchange) depuis 1999. Son siège social se trouve à Helsinki (Finlande) et nous possédons des filiales aux Etats-Unis, en France, en Allemagne, en Suède, au Royaume-Uni et au Japon. F-Secureest soutenue par un réseau de partenariats mondial intégrant des revendeurs et distributeurs à valeur ajoutée répartis dans plus de 50 pays. La protection proposée par F-Secureest aussi disponible par l'intermédiaire des FAI les plus importants, comme Wanadoo (Nordnet Securitoo), Deutsche Telekom et Charter Communications ou les principaux fabricants de téléphones mobiles, comme Nokia. Les toutes dernières informations sur les menaces de virus sont accessibles sur le Weblog de l'équipe de recherche antivirus F-Secure à l'adresse http://www.f-secure.com/weblog/.

Services pour les particuliers et les entreprises

Les services et le logiciel de F-Secureprotègent les particuliers et les entreprises contre les virus informatiques et les autres menaces qui surviennent par le biais d'Internet ou des réseaux de téléphonie mobile. Nos produits, qui ont été récompensés, incluent des antivirus et des pare-feu pour ordinateur de bureau, tous dotés de solutions de prévention des intrusions, d'antispam et d'antispyware. Notre atout majeur est la rapidité de nos réponses dès que de nouvelles menaces se présentent. Les entreprises bénéficient de la gestion centralisée de nos solutions et de la parfaite

intégration des solutions pour stations de travail et serveurs. Nos partenaires privilégiés proposent des services de sécurité aux entreprises qui ne disposent pas en interne de compétences en matière de sécurité.

Pour en savoir plus sur nos produits et nos services, visitez notre site Web à l'adresse http://www.f-secure.com/products/.