F-Secure Policy Manager

Guide de l'administrateur

 12000013-5C18

Sommaire

A PROPOS DE CE GUIDE

Présentation

F-Secure Policy Manager fournit des outils pour administrer les produits logiciels F-Secure suivants :

- F-Secure Client Security
- F-Secure Internet Gatekeeper pour Windows
- F-Secure Anti-Virus pour
  - les stations de travail Windows
  - les serveurs Windows
  - les serveurs Citrix
  - Microsoft Exchange
  - MIMEsweeper
- F-Secure Linux Security
- F-Secure Linux Client Security
- F-Secure Linux Server Security
- F-Secure Policy Manager Proxy.

Organisation du guide

Le Guide de l'administrateur de F-Secure Policy Manager contient les chapitres suivants.

Chapitre 1. *Introduction à F-Secure Policy Manager Console.* Décrit l'architecture et les composants de la gestion basée sur les stratégies.

Chapitre 2. *Configuration requise.* Définit la configuration logicielle et matérielle requise pour F-Secure Policy Manager Console et F-Secure Policy Manager Server.

Chapitre 3. *Installation de F-Secure Policy Manager Server.* Couvre l'installation de F-Secure Policy Manager Server sur le serveur.

Chapitre 4. *Installation de F-Secure Policy Manager Console.* Couvre l'installation des applications F-Secure Policy Manager Console sur la station de travail de l'administrateur.

Chapitre 5. *Utilisation de F-Secure Policy Manager Console*. Donne une présentation globale du logiciel et décrit les procédures d'installation et d'ouverture de session, les options de menu et les tâches de base.

Chapitre 6. *Maintenance de F-Secure Policy Manager Server.* Décrit les procédures de sauvegarde et les routines de restauration.

Chapitre 7. *Mise à jour des bases de données de définition de virus.* Décrit les différents modes de mise à jour des bases de données de définitions de virus.

Chapitre 8. *F-Secure Policy Manager sous Linux.* Décrit les procédures d'installation et d'administration F-Secure Policy Manager sous Linux.

Chapitre 9. *Web Reporting*. Décrit comment utiliser F-Secure Policy Manager Web Reporting, un nouveau système de rapports graphiques d’entreprise basé sur le Web inclus dans F-Secure Policy Manager Server.

Chapitre 10. *F-Secure Policy Manager Proxy.* Contient une brève introduction à Proxy F-Secure Policy Manager.

Chapitre 11. *Dépannage*. Contient des informations de dépannage et des questions fréquentes.

Annexe A. *Prise en charge de SNMP*. Contient des informations sur la prise en charge de SNMP.

Annexe B. *Codes d'erreur d'llaunchr*. Contient la liste des codes d'erreur d'llaunchr.

Annexe C. *Codes d'erreur de l'installation distante avec FSII*. Décrit les codes d'erreur les plus courants et les messages qui apparaissent durant l'opération Autodécouvrir hôtes Windows.

Annexe D. *Notation NSC pour les masques de réseau*. Définit la notation NSC pour masques de réseau et fournit des informations à ce sujet.

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.

Conventions utilisées dans les guides F-Secure

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

Symboles

AVERTISSEMENT : Le symbole d'avertissement signale un risque de destruction irréversible des données.

IMPORTANT : *Le point d'exclamation signale des informations importantes à prendre en compte.*

REFERENCE : l'image d'un livre renvoie à un autre document contenant des informations sur le même sujet.

REMARQUE : une remarque donne des informations complémentaires à prendre en compte.

CONSEIL : un conseil donne des informations qui vous permettront de réaliser une tâche avec plus de facilité ou de rapidité.

⇒ Une flèche signale une procédure composée d'une seule étape.

Polices

La police **Arial Gras (bleu)** est utilisée pour les noms et les options de menus, les boutons et autres éléments des boîtes de dialogue.

La police *Arial Italique (bleu)* est utilisée pour les références aux autres chapitres de ce manuel ainsi que les titres de livres ou d'autres manuels.

La police *Arial Italique (noir)* est utilisée pour les noms de fichiers et de dossiers, les titres des figures et des tableaux et les noms des arborescences.

La police `Courier New` est utilisée pour les messages affichés à l'écran.

La police **`Courier New Gras`** est utilisée pour les informations que vous devez taper.

Les **PETITES MAJUSCULES (NOIR)** sont utilisées pour les touches du clavier ou combinaisons de touches.

La police Arial Souligné (bleu) est utilisée pour les liens sur l'interface utilisateur.

La police Times New Roman Normal est utilisée pour les noms de fenêtres et de boîtes de dialogue.

Document PDF

Ce manuel est fourni au format PDF (Portable Document Format). Il peut être visualisé en ligne ou imprimé avec Adobe® Acrobat® Reader. Si vous imprimez le manuel, imprimez-le en entier, y compris les mentions de copyright et de disclaimer.

Pour plus d'informations

Rendez-vous sur le site de F-Secure à l'adresse suivante : http://www.f-secure.com . Vous y trouverez notre documentation, des formations, des fichiers à télécharger et des informations de contact pour les services et le support technique.

Nous nous efforçons constamment d'améliorer notre documentation et vos commentaires sont les bienvenus. Pour toute question, commentaire ou suggestion concernant ce document ou tout autre document F-Secure, veuillez nous contacter à l'adresse suivante : documentation@f-secure.com.

1 Introduction à F-Secure Policy Manager Console

1.1 Présentation

F-Secure Policy Manager offre une manière modulable de gérer la sécurité de plusieurs 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, surveiller la conformité de l'entreprise et gérer le personnel même s'il est nombreux et itinérant. F-Secure Policy Manager offre une infrastructure étroitement intégrée pour la définition des stratégies de sécurité, la diffusion des stratégies et l'installation d'applications sur des systèmes locaux et distants ainsi que le contrôle des activités de tous les systèmes de l'entreprise afin de vous assurer de leur conformité avec les stratégies de l'entreprise et un contrôle centralisé.

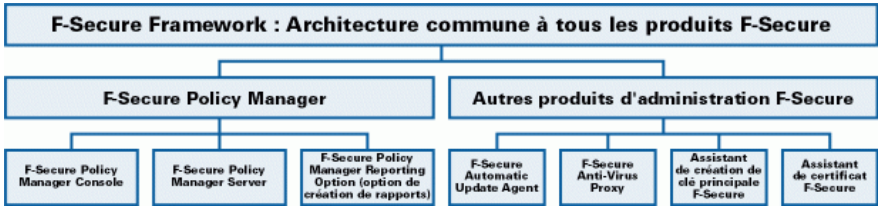


Figure 1-1 Architecture de gestion de F-Secure

L'agent de mise à jour automatique F-Secure peut être installé en tant que partie intégrante de F-Secure Policy Manager Server.

La puissance de F-Secure Policy Manager repose sur l'architecture d'administration F-Secure, qui offre une grande évolutivité pour un personnel réparti géographiquement et itinérant. F-Secure Policy Manager se compose de F-Secure Policy Manager Console et de F-Secure Policy Manager Server. Ils sont parfaitement intégrés avec les agents F-Secure Management Agent qui gèrent toutes les fonctions d'administration sur les hôtes locaux.

Principaux composants de F-Secure Policy Manager

F-Secure Policy Manager Console fournit une console d'administration centralisée pour assurer la sécurité des hôtes administrés sur le 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. F-Secure Policy Manager Console est une application basée sur Java exécutable sur différentes plates-formes. Elle permet notamment d'installer F-Secure Management Agent à distance sur d'autres postes de travail sans utiliser de scripts de connexion locaux, sans redémarrer l'ordinateur et sans aucune intervention de l'utilisateur final.

F-Secure Policy Manager Server stocke les stratégies et les logiciels diffusés par l'administrateur ainsi que les informations d'état et les alertes envoyées par les hôtes administrés. Utilisé comme extension d'un serveur Web Apache, il s'agit d'un composant évolutif. 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 Web de création de rapports graphiques à l'échelle de l'entreprise 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.

F-Secure Policy Manager Reporting Option est un programme de ligne de commande autonome qui, via un répertoire de communication (CommDir) existant dans F-Secure Policy Manager Server, collecte les données d'alerte, d'état et de propriété du domaine de sécurité géré ou de l'hôte de votre choix. F-Secure Policy Manager Reporting Option permet à l'utilisateur de générer des rapports relatifs aux données figurant dans le répertoire de communication de Secure Policy Manager Server à l'aide de modèles XSL (semblables à des requêtes prédéfinies). Ces rapports peuvent ensuite être exportés sous forme de fichiers HTML, XML, CSV ou TXT.

Le serveur et l'agent de mise à jour de **F-Secure Policy Manager** servent à mettre à jour les définitions de virus et de logiciels espions sur les hôtes administrés. L'agent de mise à jour automatique F -Secure permet aux utilisateurs d'obtenir des mises à jour automatiques ainsi que des informations sans avoir à interrompre leur travail pour télécharger les fichiers à partir d'Internet. L'agent de mise à jour automatique F-Secure télécharge automatiquement les fichiers en tâche de fond en utilisant la bande passante inutilisée par d'autres applications Internet. Ainsi, l'utilisateur est sûr de disposer des mises à jour les plus récentes et ce, sans avoir à effectuer de recherches sur Internet. 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 dans les deux heures qui suivent leur publication par F-Secure.

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

1.2 Ordre d'installation

Pour installer F-Secure Policy Manager, procédez dans l'ordre indiqué ci-dessous, sauf si vous installez F-Secure Policy Manager Server et F-Secure Policy Manager Console sur le même ordinateur. Dans ce dernier cas, le programme d'installation installe tous les composants au cours de la même opération.

1. F-Secure Policy Manager Server, puis agent et serveur de mise à jour F-Secure Policy Manager,
2. F-Secure Policy Manager Console,
3. Applications du point administré.

1.3 Fonctionnalités

Distribution des logiciels

- Première installation dans un domaine NT à l'aide du système d'installation de F-Secure.
- Mise à jour des fichiers exécutables et des fichiers de données, dont les bases de données de F-Secure Anti-Virus.
- Prise en charge des mises à jour par stratégies. Les stratégies contraignent F-Secure Management Agent à effectuer les mises à jour sur un hôte. Les stratégies et les logiciels sont signés, ce qui permet d'authentifier et d'assurer la sécurité des processus complets de mise à jour.
- Les mises à jour peuvent s'effectuer de différentes manières :
- à partir du CD-ROM de F-Secure ;
- sur le poste client à partir du site Web de F-Secure. Ces mises à jour peuvent être automatiquement « distribuées » par l'agent de sauvegarde automatique F-Secure ou « récupérées » à la demande sur le site Web de F-Secure.
- F-Secure Policy Manager Console peut être utilisé pour exporter des packages d'installation préconfigurés, qu'il est également possible de transmettre à l'aide d'un logiciel tiers, tel que SMS, ou des outils similaires.

Configuration et gestion par stratégies

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

Gestion des événements

- Transmission de rapports à l'Observateur d'événements (journaux locaux et distants), à l'agent SNMP, à la messagerie électronique, aux fichiers de rapport, etc. via l'interface API de F-Secure Management.
- Redirection d'événements par stratégies.
- Statistiques relatives aux 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 Gestion par stratégies

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. La gestion par stratégies met en œuvre de nombreuses fonctions :

- contrôle et suivi à distance du comportement des produits,
- analyse des statistiques générées par les produits et par F-Secure Management Agent,
- lancement à distance d'opérations prédéfinies,
- transmission à l'administrateur système des alertes et des notifications émises par les produits.

L'échange d'informations entre F-Secure Policy Manager Console et les hôtes s'effectue via le transfert des fichiers de stratégie. Il existe trois types de fichiers de stratégie :

- fichiers de stratégie par défaut (*.dpf*),
- fichiers de stratégie de base (*.bpf*),
- fichiers de stratégie incrémentielle (*.ipf*).

La configuration courante d'un produit inclut ces trois types de fichiers.

Fichiers de stratégie par défaut

Le fichier de stratégie par défaut contient les paramètres par défaut d'un produit qui sont appliqués lors de l'installation. Les stratégies par défaut sont utilisées uniquement sur l'hôte. La valeur d'une variable est extraite du fichier de stratégie par défaut lorsque ni le fichier de stratégie de base ni le fichier de stratégie incrémentielle ne contiennent d'entrée correspondante. Chaque produit possède son propre fichier de stratégie par défaut. Les nouvelles éditions des logiciels intègrent également les nouvelles versions du fichier de stratégie par défaut.

Fichiers de stratégie de base

Les fichiers de stratégie de base contiennent les restrictions et les paramètres administratifs de toutes les variables pour tous les produits F-Secure installés sur un hôte donné (grâce à la définition de stratégies au niveau du domaine, un groupe d'hôtes peut partager le même fichier). Le fichier de stratégie de base est signé par F-Secure Policy Manager Console, ce qui permet de le protéger contre toute modification lorsqu'il est diffusé sur le réseau et stocké dans le système de fichiers d'un hôte. Ces fichiers sont envoyés à F-Secure Policy Manager Server à partir de F-Secure Policy Manager Console. L'hôte récupère à intervalles réguliers les nouvelles stratégies créées par F-Secure Policy Manager Console.

Fichiers de stratégie incrémentielle

Les fichiers de stratégie incrémentielle permettent de stocker les modifications apportées localement à la stratégie de base. Seules sont autorisées les modifications comprises dans les limites définies dans la stratégie de base. Les fichiers de stratégie incrémentielle sont ainsi envoyés à F-Secure Policy Manager Console à intervalles réguliers afin que l'administrateur puisse visualiser les paramètres et les statistiques en cours.

1.4.1 Base d'informations de gestion

La base d'informations de gestion (MIB) est une structure hiérarchique de données de gestion utilisée par le système SNMP (Simple Network Management Protocol). Dans F-Secure Policy Manager, elle permet de définir le contenu des fichiers de stratégie. Chaque variable est associée à un identificateur unique (OID, ID d'objet) et à une valeur accessible à partir de l'interface API Stratégie. Outre les définitions de la base d'informations de gestion (MIB) du système SNMP, la base d'informations de gestion de F-Secure inclut plusieurs extensions nécessaires à une gestion complète par stratégies.

Les catégories suivantes sont définies dans la base d'informations de gestion (MIB) d'un produit :

Paramètres	Cette catégorie permet de gérer la station de travail de la même manière qu'un système SNMP. Les produits gérés fonctionnent dans les limites spécifiées ici.
Statistiques	Cette catégorie fournit à F-Secure Policy Manager Console les statistiques relatives au produit.
Opérations	Deux variables de stratégie gèrent les opérations : (1) une variable pour transmettre à l'hôte l'identificateur de l'opération et (2) une variable pour informer F-Secure Policy Manager Console des opérations exécutées. La seconde variable est transmise à l'aide des statistiques habituelles ; elle accuse réception de toutes les opérations antérieures simultanément. Un éditeur personnalisé destiné à l'édition des opérations est associé à la sous-arborescence et masque les deux variables.
Privé	Les bases d'informations de gestion peuvent également contenir des variables que le produit stocke en vue d'un usage interne entre les sessions. Cela lui évite de recourir à des services externes, tels que les fichiers du Registre de Windows.
Interruptions	Les interruptions sont des messages (notamment des alertes et des événements) envoyés à la console locale, au fichier journal, au processus d'administration à distance, etc. La plupart des produits F-Secure intègrent les types d'interruptions suivants :
	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 irrécupérable survenue sur l'hôte.

Alerte de sécurité. Incident lié à la sécurité survenu sur l'hôte.

2 CONFIGURATION REQUISE

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 :* Microsoft Windows 2000 Server (SP4 ou version ultérieure) Windows 2003 Server (32 et 64 bits) Windows 2008 Server (32 et 64 bits) *Linux :* Red Hat Enterprise Linux 3, 4 et 5 openSUSE Linux 10.3 SUSE Linux Enterprise Server 9 et 10 SUSE Linux Enterprise Desktop 10 Debian GNU Linux Etch 4.0 Ubuntu 8.04 Hardy
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 l'utilisation d'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 requis :	Espace disque requis : 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 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 :* Microsoft Windows 2000 Professionnel (SP4 ou version ultérieure) Windows XP Professionnel (SP2 ou version ultérieure) Windows Vista (32 et 64 bits) Windows 2000 Server SP4 Windows 2003 Server (32 et 64 bits). Windows 2008 Server (32 et 64 bits). *Linux :* Red Hat Enterprise Linux 3, 4 et 5 openSUSE Linux 10.3 SUSE Linux Enterprise Server 9 et 10 SUSE Linux Enterprise Desktop 10 Debian GNU Linux Etch 4.0 Ubuntu 8.04 Hardy
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 RAM.

Espace disque requis :	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 à 100 Mbits entre la console et le serveur.

3 INSTALLATION DE F-SECURE POLICY MANAGER SERVER

3.1 Présentation

Vous trouverez ci-dessous des instructions avancées pour l'installation de F-Secure Policy Manager Server sur un ordinateur dédié uniquement au serveur. F-Secure Policy Manager Server peut également être installé sur le même ordinateur que F-Secure Policy Manager Console.

F-Secure Policy Manager Server est le lien entre F-Secure Policy Manager Console et les hôtes administrés. Il sert au stockage des stratégies et des fichiers logiciels distribués par l'administrateur, ainsi que des informations d'état et des alertes envoyées par les hôtes administrés.

La communication entre F-Secure Policy Manager Server et d'autres composants peut être établie via le protocole standard HTTP, qui assure un fonctionnement optimal aussi bien sur les réseaux locaux (LAN) que sur les réseaux longue distance.

Les informations stockées par F-Secure Policy Manager Server incluent les fichiers suivants :

- la structure du domaine de stratégie,
- les données de stratégie, c'est-à-dire les informations de stratégie réelles liées à chaque domaine de stratégie ou à chaque hôte,
- les fichiers de stratégie de base créés à partir des données de stratégie,
- les informations d'état, notamment les fichiers de stratégie incrémentielle, les alertes et les rapports,
- les demandes d'auto-enregistrement envoyées par les hôtes,
- les certificats de l'hôte,
- les informations de sécurité reçues de F-Secure,
- les packages d'installation des produits et de mise à jour des bases de données de définitions de virus.
- Le composant Web Reporting stocke des données de tendances statistiques et historiques sur les hôtes.

3.2 Problèmes de sécurité

F-Secure Policy Manager Server emploie la technologie de serveur Web Apache. Bien que nous mettions tout en œuvre pour fournir une technologie sûre et à jour, il est conseillé de consulter régulièrement les sites suivants afin d'obtenir des informations sur la technologie Apache et sa sécurité.

Les informations les plus récentes sur les problèmes de sécurité relatifs aux systèmes d'exploitation et au serveur Web Apache sont disponibles sur le site Web de CERT : http://www.cert.org.

Vous trouverez un document fournissant des conseils sur la manière de sécuriser l'installation du serveur Web Apache à l'adresse http://www.apache.org/docs/misc/security_tips.html., ainsi qu'une liste répertoriant les points vulnérables à l'adresse http://www.apacheweek.com/features/security-13.

Les notes de publication contiennent des informations importantes relatives à l'installation et à la sécurité. Lisez ces notes attentivement !

3.2.1 Installation de F-Secure Policy Manager dans des environnements à haute sécurité

F-Secure Policy Manager est essentiellement destiné à la gestion de produits F-Secure Anti-Virus dans des réseaux d'entreprise internes. F-Secure ne recommande pas d'employer F-Secure Policy Manager sur des réseaux publics tels qu'Internet.

IMPORTANT : *Lors de l'installation de F-Secure Policy Manager dans des environnements à haute sécurité, il convient de s'assurer que le port Administration (par défaut le port 8080) et le port Hôte (par défaut le port 80) ne sont pas visibles sur Internet.*

Fonctions de sécurité intégrées à F-Secure Policy Manager

F-Secure Policy Manager possède des fonctions de sécurité intégrées qui garantissent la détection de toute modification de la structure du domaine de stratégie et des données de stratégie. Plus important encore, elles interdisent le déploiement de modifications non autorisées sur les hôtes administrés. Ces deux fonctions reposent sur une paire de clés d'administration qui n'est accessible qu'aux administrateurs. Dans la plupart des cas, ces fonctions, reposant sur de puissantes signatures numériques, fourniront l'équilibre idéal entre facilité d'utilisation et sécurité à la plupart des installations antivirus. Par contre, les fonctions suivantes peuvent exiger une configuration supplémentaire dans des environnements à haute sécurité :

1. Par défaut, tous les utilisateurs peuvent accéder en lecture seule à Policy Manager Server, mais ils peuvent uniquement consulter les données d'administration. Cette méthode permet de partager aisément les informations avec les utilisateurs ne disposant pas de droits d'administration complets. Plusieurs utilisateurs peuvent ouvrir simultanément une session en lecture seule, afin de surveiller l'état du système sans perturber les autres administrateurs ou les hôtes administrés.
2. Pour faciliter la migration vers de nouvelles clés d'administration, il est possible de signer de nouveau la structure du domaine de stratégie et les données de stratégie à l'aide d'une nouvelle clé ou d'une clé existante. Si cette opération est effectuée accidentellement, ou volontairement par un utilisateur non autorisé, l'utilisateur autorisé remarquera la modification lorsqu'il tentera d'ouvrir une nouvelle session dans F-Secure Policy Manager. Dans le pire des cas, l'utilisateur autorisé devra restaurer des sauvegardes afin d'éliminer les éventuelles modifications apportées par l'utilisateur non autorisé. Dans tous les cas, les modifications de la structure du domaine de stratégie et des données de stratégie seront détectées, et il est impossible de distribuer ces modifications aux hôtes administrés sans la paire de clés d'origine.

Ces deux fonctions peuvent s'avérer indésirables dans un environnement à haute sécurité, où il doit même être interdit de visualiser les données d'administration. Les mesures suivantes peuvent être prises pour accroître le niveau de sécurité du système :

Différents scénarios d'installation possibles pour les environnements à haute sécurité :

1. F-Secure Policy Manager Server et F-Secure Policy Manager Console seront installés sur le même ordinateur et l'accès à F-Secure Policy Manager Server sera limité à l'hôte local uniquement. Après cela, seule la personne ayant un accès physique à l'hôte local peut utiliser F-Secure Policy Manager Console.

   Lorsque l'accès à F-Secure Policy Manager Server est limité à l'hôte local au cours de l'installation (voir l'*Etape 8.* , 37), le programme d'installation de F-Secure modifie le paramètre `#FSMSA listen` du fichier *httpd.conf* comme suit :

   ```
   #FSMSA listen
       Listen 127.0.0.1:8080 <- Autoriser les connexions
       uniquement de l'hôte local au port PMC 8080
   ```

2. L'accès à F-Secure Policy Manager Server sera limité uniquement aux adresses IP définies séparément via la modification du fichier *httpd.conf*.

Si l'accès au port 8080 était limité à l'hôte local au cours de l'installation, vous devez maintenant ouvrir le port et définir la liste des adresses IP autorisées (reportez-vous au paramètre Listen 8080 de l'exemple ci-dessous).

Voici un exemple de section du fichier httpd.conf modifiée :

```
#FSMSA listen
Listen 8080 <- s'assurer que les connexions ne sont pas
limitées à l'hôte local


#FSMSA port
<VirtualHost _default_:8080>
    <Location /fsmsa/fsmsa.dll>
     Order Deny,Allow
     Deny from all <- D'abord tout refuser
     Allow from 127.0.0.1 <- Ensuite, autoriser l'accès au
serveur depuis l'ordinateur local
     Allow from 10.128.129.2 <- Autoriser l'accès depuis
l'ordinateur serveur
    Allow from 10.128.129.209 <- Autoriser l'accès depuis le
poste de travail administrateur
     SetHandler fsmsa-handler
    </Location>
</VirtualHost>
```

Ensuite, seule la personne ayant accès aux ordinateurs ayant les adresses IP définies peut utiliser F-Secure Policy Manager Console.

3. S'il est vraiment indispensable d'utiliser F-Secure Policy Manager via un réseau public (comme Internet), il est recommandé de crypter la connexion entre F-Secure Policy Manager Server et F-Secure Policy Manager Console à l'aide d'un produit de type VPN ou SSH.

F-Secure Policy Manager Console et F-Secure Policy Manager Server peuvent également être installés sur le même ordinateur, avec un accès illimité à l'hôte local. Un accès administrateur à distance à F-Secure Policy Manager Console peut être prévu à l'aide d'un produit de connexion de bureau à distance sécurisé.

Installation de F-Secure Policy Manager Web Reporting dans des environnements à haute sécurité

F-Secure Policy Manager Web Reporting a été conçu pour être utiliser dans des réseaux d'entreprise internes en vue de générer, par exemple, des rapports graphiques de l'état de la protection contre les virus et des alertes de F-Secure Client Security. F-Secure ne recommande pas d'employer F-Secure Policy Manager Web Reporting sur des réseaux publics tels qu'Internet.

Différents scénarios d'installation possibles pour les environnements à haute sécurité :

1. L'accès aux rapports Web est limité à l'hôte local au cours de l'installation. Après cela, seule la personne ayant un accès physique à l'hôte local peut utiliser F-Secure Policy Manager Web Reporting.

   Lorsque l'accès à F-Secure Policy Manager Web Reporting est limité à l'hôte local au cours de l'installation (voir l' , 38), le programme d'installation de F-Secure modifie le paramètre `#Web Reporting listen` du fichier *httpd.conf* comme suit :

   ```
   #Web Reporting listen
   Listen 127.0.0.1:8081 <- Autoriser les connexions au port
   8081 de Web Reporting uniquement depuis l'hôte local
   ```

2. L'accès à F-Secure Policy Manager Web Reporting sera limité uniquement aux adresses IP définies séparément via la modification du fichier *httpd.conf* (voir ci-dessous).

Si l'accès au port 8081 était limité à l'hôte local au cours de l'installation, vous devez maintenant ouvrir le port et définir la liste des adresses IP autorisées (reportez-vous au paramètre Listen 8081 de l'exemple ci-dessous).

Voici un exemple de section du fichier *httpd.conf* modifiée. Dans cet exemple, l'accès est autorisé à partir de l'hôte local et d'une adresse IP définie séparément :

```
#Web Reporting listen
Listen 8081

# Web Reporting port:
<VirtualHost _default_:8081>
    JkMount /* ajp13
   ErrorDocument 500 "Policy Manager Web Reporting could not
be contacted by
the Policy Manager Server.
  <Location / >
    Order Deny,Allow
    Deny from all <- D'abord tout refuser
    Allow from 127.0.0.1 <- Ensuite, autoriser l'accès à Web
Reporting depuis l'ordinateur local
    Allow from 10.128.129.209 <- Autoriser l'accès depuis le
poste de travail administrateur
  </Location>
</VirtualHost>
```

Ensuite, seule la personne ayant accès à l'hôte local ou à l'ordinateur ayant les adresses IP définies peut utiliser F-Secure Policy Manager Web Reporting.

3.3 Procédure d'installation

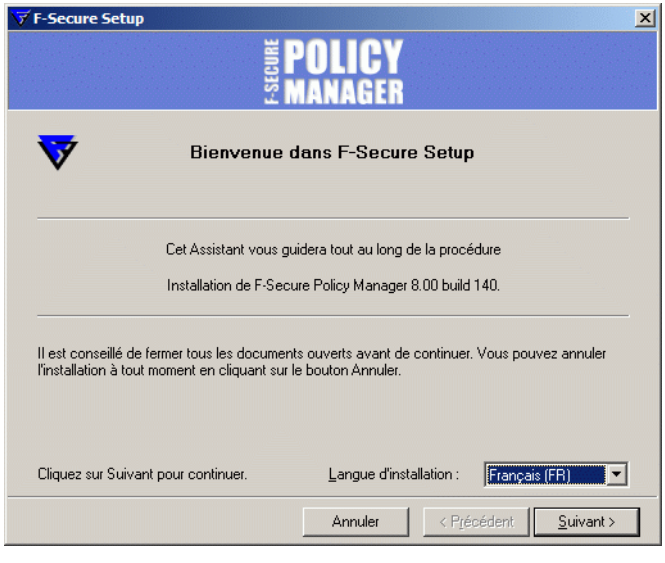
Pour installer F-Secure Policy Manager Server, vous devez disposer d'un accès physique au serveur.

Etape 1.

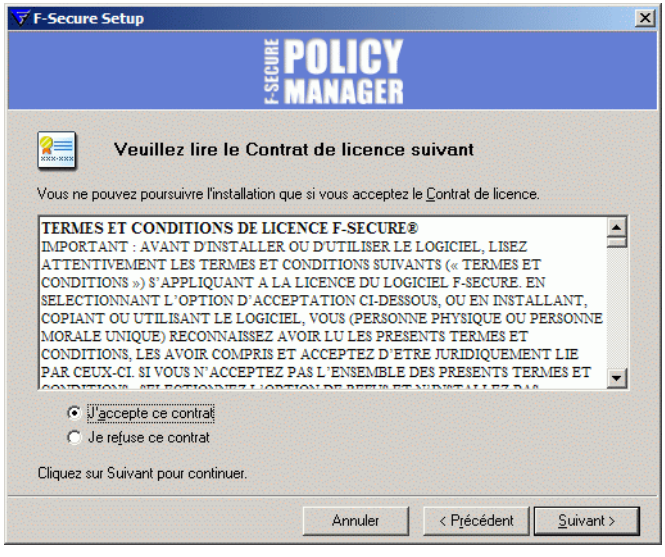
1. Introduisez le CD-ROM F-Secure dans le lecteur adéquat.
2. Sélectionnez *Professionnel*. Cliquez sur **Suivant** pour continuer.
3. Accédez au menu *Installation ou mise à jour de logiciels administrés*, puis choisissez F-Secure Policy Manager.

Etape 2.

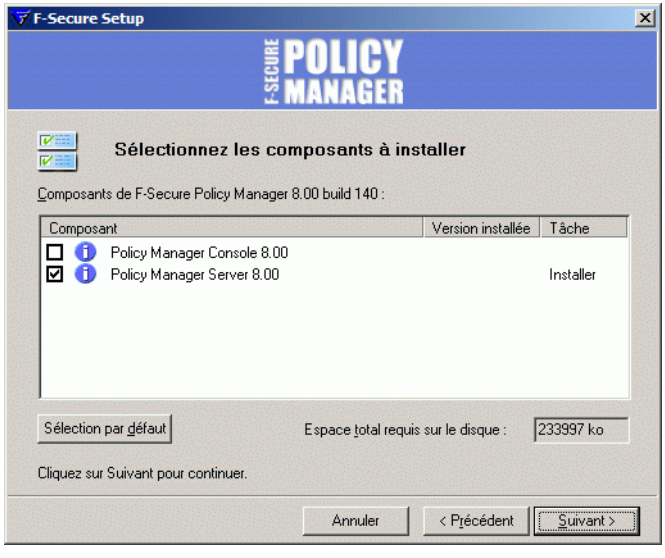
L'installation démarre. Prenez connaissance du contenu de l'écran d'accueil, puis suivez les instructions relatives à l'installation. Sélectionnez la langue d'installation dans le menu déroulant. Cliquez sur **Suivant** pour continuer.



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



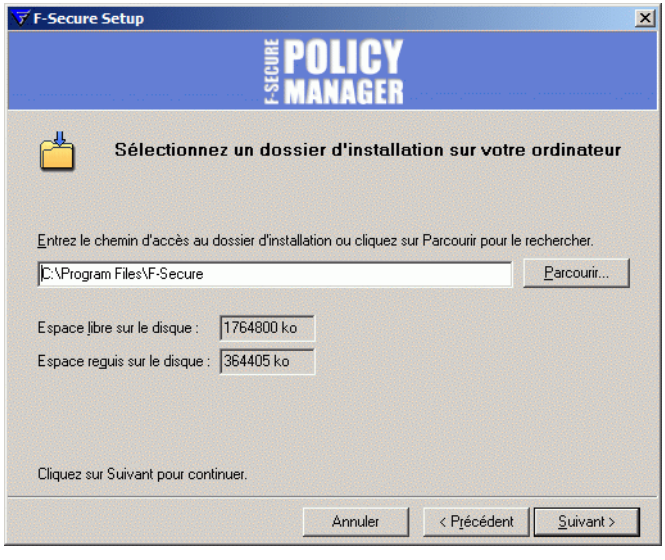
Etape 4. Si vous effectuez l'installation sur un ordinateur où rien n'a été installé auparavant, sélectionnez F-Secure Policy Manager Server. Cliquez sur **Suivant** pour continuer.



Etape 5. Choisissez le dossier de destination. Cliquez sur **Suivant**.

Nous vous recommandons d'utiliser le répertoire d'installation par défaut. Si vous souhaitez installer F-Secure Policy Manager Server dans un répertoire différent, utilisez la fonction **Parcourir**.

AVERTISSEMENT : Si F-Secure Management Agent est installé sur le même ordinateur, vous ne devez pas modifier le répertoire d'installation de F-Secure Policy Manager Server

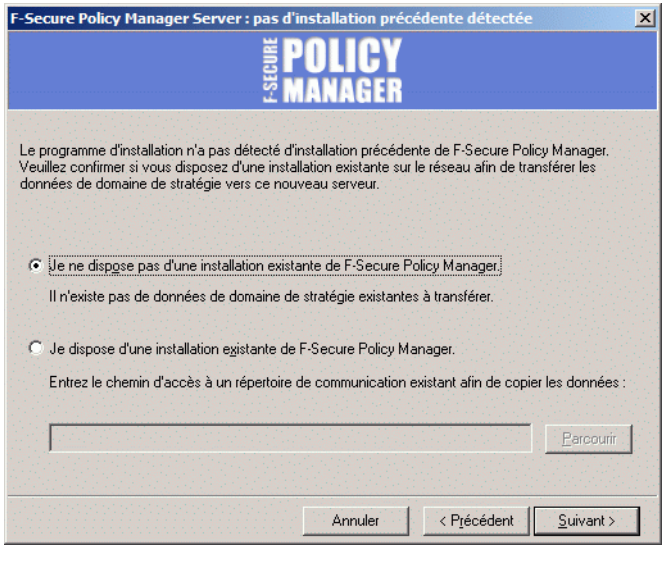


Etape 6. Le programme d'installation demande confirmation en présence de l'installation précédente de F-Secure Policy Manager.

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)*, 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 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*).

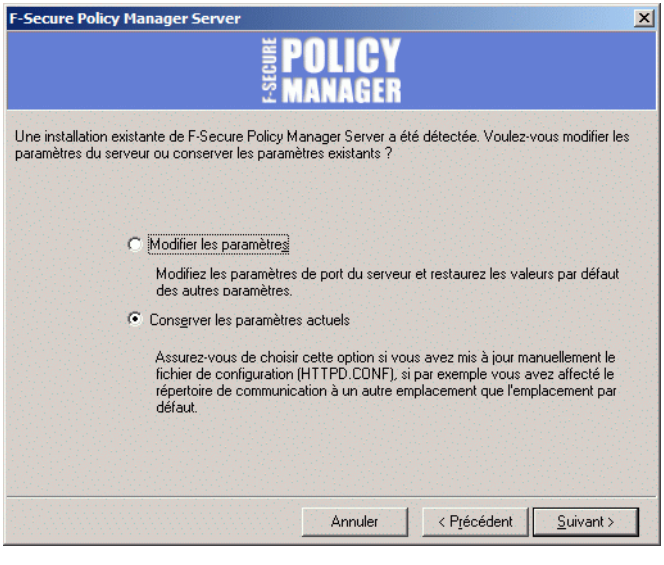
Cliquez sur **Suivant** pour continuer.



Etape 7. 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.



Etape 8. 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.

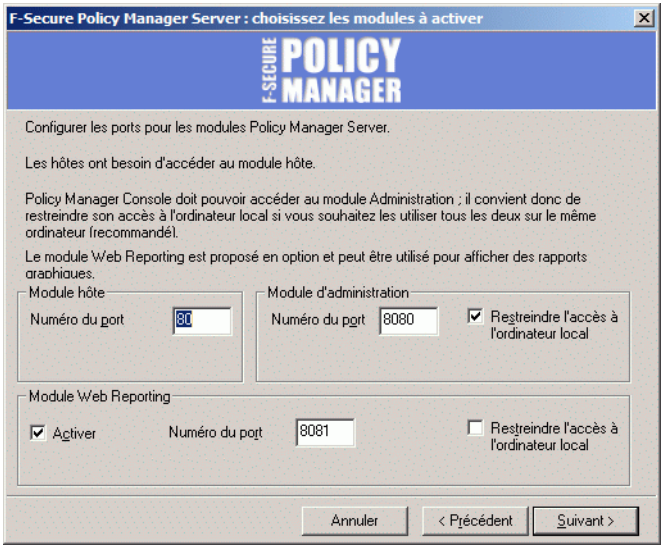
  Par défaut, l'accès au module Administration est restreint à l'ordinateur local. C'est le mode d'utilisation du produit le plus sécurisé.

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

  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 deF-Secure Policy Manager*.

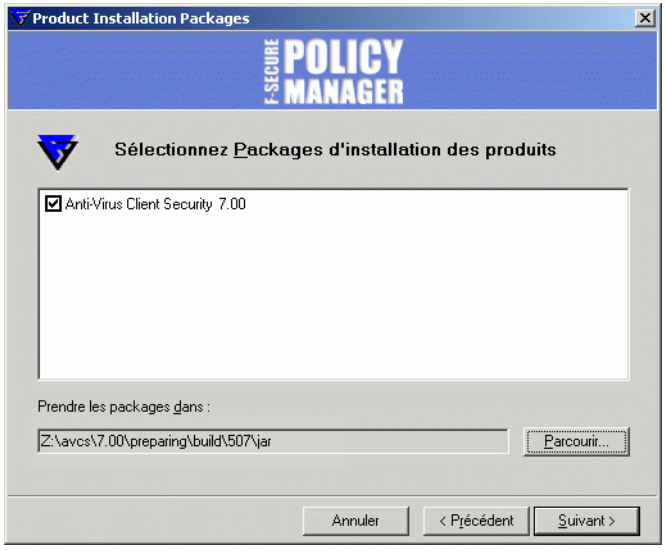
- Le module Web Reporting est utilisé pour la communication avec F-Secure Policy Manager Web Reporting. Indiquez si vous souhaitez l'activer. Web Reporting se connecte au module d'administration via un socket local pour rechercher les données du serveur. Le port par défaut est 8081.

  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*.

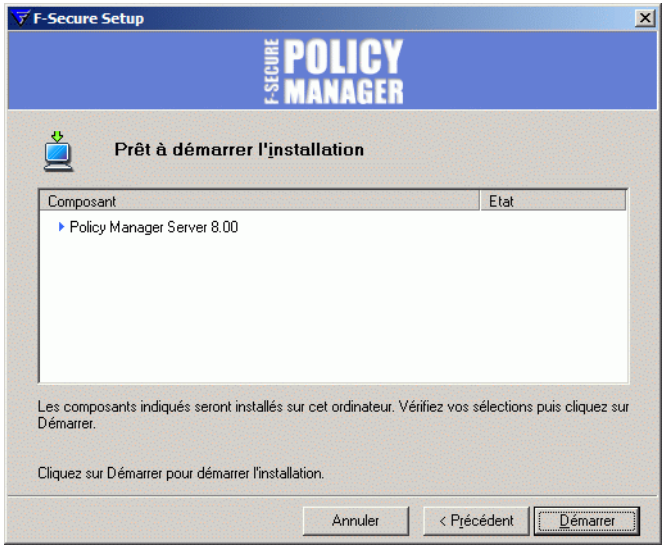


Cliquez sur **Suivant** pour continuer.

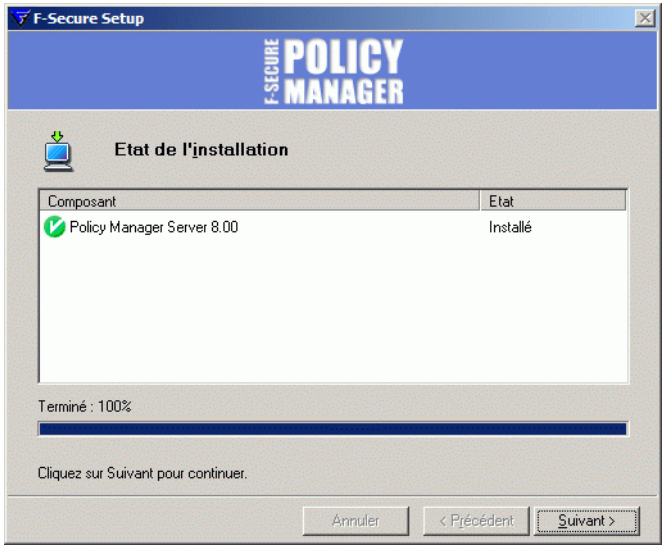
Etape 9. Sélectionnez le ou les fichiers d'installation de produits dans la liste des fichiers disponibles (si vous avez activé l'option Packages d'installation F-Secure à l'étape 4 de la page 17). Cliquez sur **Suivant**.



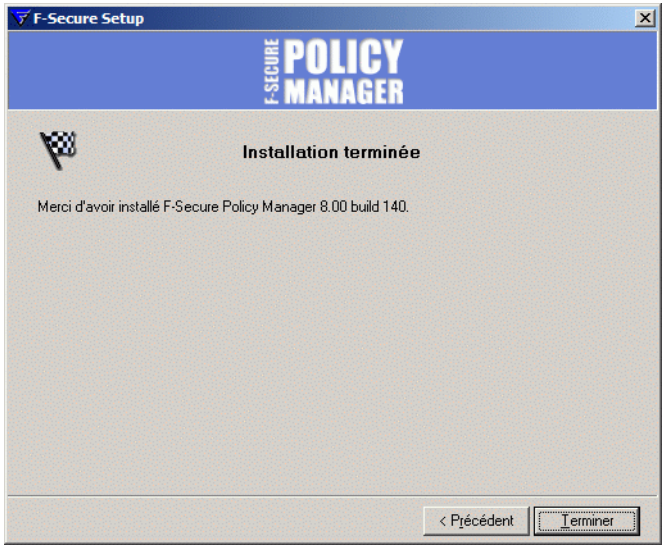
Etape 10. Le programme d'installation présente la liste des composants qui seront installés. Cliquez sur **Suivant**.



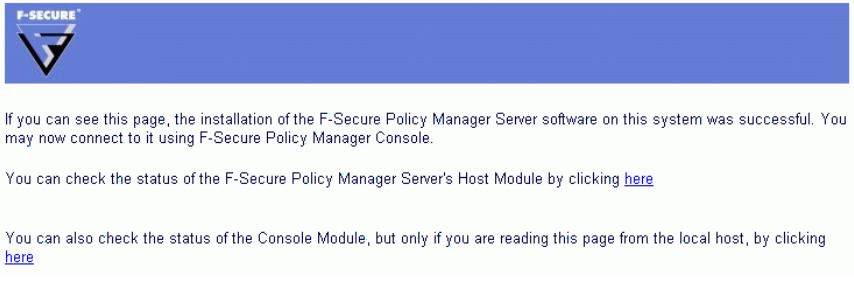
Etape 11. Lorsque le programme d'installation est terminé, il affiche tous les composants dont l'installation a abouti.



Etape 12. F-Secure Policy Manager Server est désormais installé. Redémarrez l'ordinateur si un message vous invite à le faire. Cliquez sur **Terminer** pour terminer l'installation.



Etape 13. Pour déterminer si l'installation a réussi, ouvrez un navigateur Web sur l'ordinateur où F-Secure Policy Manager Server a été installé, tapez *http://localhost:80* (si vous avez utilisé le numéro de port par défaut pendant l'installation), puis appuyez sur la touche ENTRÉE. Si l'installation du serveur a réussi, la page suivante s'affiche.



F-Secure Policy Manager Server commence à servir des hôtes uniquement après que F-Secure Policy Manager Server a initialisé la structure du répertoire de communication, ce qui s'effectue automatiquement lors de la première exécution de F-Secure Policy Manager Console.

Etape 14. L'assistant d'installation crée le groupe d'utilisateurs `FSPM users`. L'utilisateur qui avait ouvert une session et qui a procédé à l'installation est automatiquement ajouté à ce groupe. Pour autoriser un autre utilisateur à exécuter F-Secure Policy Manager, vous devez l'ajouter manuellement au groupe d'utilisateurs `FSPM users`.

3.4 Configuration de F-Secure Policy Manager Server

Le répertoire *conf* dans le répertoire d'installation de Policy Manager Server contient un fichier *httpd.conf*. Ce fichier contient les informations de configuration de F-Secure Policy Manager Server.

Après avoir modifié la configuration, vous devez arrêter F-Secure Policy Manager Server et le redémarrer pour que les modifications entrent en vigueur.

Les paramètres de F-Secure Policy Manager Web Reporting pouvant être configurés dans httpd.conf sont expliqués dans la section "Maintenance de Web Reporting", 183

3.4.1 Modification du chemin d'accès au répertoire de communication

Si le lecteur réseau sur lequel le répertoire de communication se trouve devient saturé, vous pouvez changer son emplacement en suivant les instructions ci-dessous.

1. Choisissez un nouveau chemin réseau sur un lecteur offrant plus d'espace. Créez le chemin et vérifiez que l'utilisateur *fsms_<nom Wins de l'ordinateur>* bénéficie de droits d'accès *Contrôle total* sur tous les répertoires du chemin.
2. Arrêtez le service F-Secure Policy Manager Server.
3. Copiez toute la structure de répertoires de l'ancien chemin commdir vers le nouveau chemin.
4. Changez la valeur des paramètres `CommDir` et `CommDir2` dans httpd.conf. La configuration par défaut contient les valeurs suivantes :

   ```
   CommDir "C:\Program Files\F-Secure\Management Server 5\CommDir"
   ```

   ```
   CommDir2 "C:\Program Files\F-Secure\Management Server 5\CommDir"
   ```

Si vous voulez remplacer l'emplacement du répertoire de communication par `E:\CommDir`, modifiez les paramètres en conséquence :

```
CommDir "E:\CommDir"
CommDir2 "E:\CommDir"
```

5. Démarrez le service F-Secure Policy Manager Server.
6. Vérifiez que tout fonctionne encore correctement.
7. Supprimez les anciens fichiers commdir.

3.4.2 Changement des ports où le serveur attend des demandes

Deux paramètres définissent les ports des deux modules WebServer qui constituent F-Secure Policy Manager Server : `Listen` et `<VirtualHost>`. Par défaut, le module d'administration de F-Secure Policy Manager Server (le composant qui traite les demandes provenant de Policy Manager Console) surveille le port 8080. Le module hôte de F-Secure Policy Manager Server (le composant qui traite les demandes des postes de travail) surveille pour sa part le port 80. Vous avez toutefois la possibilité d'en définir d'autres si ces valeurs par défaut ne vous conviennent pas.

Si vous voulez changer le port surveillé par le module d'administration de F-Secure Policy Manager Server, ajoutez une entrée `Listen` au fichier de configuration, en précisant le nouveau port (par exemple `Listen 8888`), puis supprimez le paramètre `Listen` qui définit le port par défaut surveillé par ce module : `Listen 8080`.

Lorsque vous ajoutez une nouvelle entrée Listen, veillez à supprimer l'entrée obsolète. Sinon, le serveur utilisera inutilement des ressources système, comme un port réseau.

Après l'ajout du paramètre `Listen`, F-Secure Policy Manager Server sait qu'il doit surveiller le nouveau port (8888 dans notre exemple). Vous devez toutefois le configurer de manière à associer le module d'administration de F-Secure Policy Manager Server à ce nouveau port.

Pour ce faire, vous devez modifier le paramètre <VirtualHost>, qui est associé au module d'administration deF-Secure Policy Manager Server. La configuration par défaut de ce paramètre est la suivante :

```
#FSMSA port
<VirtualHost _default_:8080>
<Location /fsmsa/fsmsa.dll>
 SetHandler fsmsa-handler
</Location>
</VirtualHost>
```

Pour associer le module au nouveau port, modifiez l'instruction comme suit :

```
#New FSMSA port
<VirtualHost _default_:8888>
<Location /fsmsa/fsmsa.dll>
 SetHandler fsmsa-handler
</Location>
</VirtualHost>
```

AVERTISSEMENT : Si certaines de vos stations de travail sont déjà configurées pour accéder à F-Secure Policy Manager Server (via le module hôte de F-Secure Policy Manager Server), vous ne devez pas modifier le port hôte de F-Secure Policy Manager Server via lequel les agents communiquent, puisque vous risquez d'être dans un état où les stations de travail ne pourront pas contacter le serveur

3.4.3 Paramètres de configuration de F-Secure Policy Manager Server

Cette section présente et explique toutes les entrées figurant dans le fichier de configuration de F-Secure Policy Manager Server ainsi que leur mode d'utilisation.

ServerRoot : ce paramètre définit le répertoire dans lequel le serveur est installé. Les chemins d'accès à d'autres fichiers de configuration sont pris en compte par rapport à ce répertoire.

Timeout : ce paramètre définit la période pendant laquelle le serveur attend avant de fermer une connexion réseau lorsqu'elle ne connaît plus aucun trafic entrant ou sortant.

LoadModule : ce paramètre définit le nom symbolique du module à lire et le chemin d'accès à la bibliothèque contenant les valeurs binaires du module.

Exemple : `LoadModule fsmsh_module "C:\serverroot\modules\fsmsh.dll"`

Listen : ce paramètre définit le port que le serveur doit surveiller. Ainsi, la configuration par défaut d'un serveur Web est la suivante : `Listen 80`. Vous pouvez restreindre l'origine des connexions reçues. Par exemple, `Listen 127.0.0.1:80` autorise les connexions au port 80 uniquement à partir de l'ordinateur sur lequel tourne le serveur (localhost).

Vous pouvez configurer F-Secure Policy Manager Server de manière à surveiller d'autres ports, en modifiant ce paramètre et le paramètre `<VirtualHost>` qui lui est associé, et qui est également abordé dans cette section. Pour plus d'informations, reportez-vous à la section “*Changement des ports où le serveur attend des demandes*”, *45*.

DocumentRoot : ce paramètre doit contenir un chemin d'accès absolu. Il définit le répertoire auquel tous les utilisateurs pourront accéder ; n'employez donc pas un chemin d'accès à un répertoire contenant des données confidentielles. Par défaut, F-Secure Policy Manager Server attribue un répertoire dans le répertoire d'installation de F-Secure Policy Manager Server, `htdocs\`. C'est ce répertoire qui contient la « page d’accueil » du serveur. Si vous le modifiez, cette page ne sera plus affichée.

<Directory "c:\un_chemin_d'accès">: : ce paramètre définit le type de paramètres de sécurité qui seront associés au répertoire indiqué dans le chemin d'accès.

ErrorLog : ce paramètre définit le nom du fichier dans lequel le serveur consignera les erreurs qu'il rencontre. Si le chemin d'accès au fichier ne commence pas par une barre oblique (/), il est considéré comme étant

relatif à ServerRoot. S'il commence par une barre droite (|), il est considéré comme une commande qui lance le traitement du journal d'erreurs. Cette fonction est utilisée pour l'appel de l'utilitaire **rotatelogs** (voir l'entrée **rotatelogs** de cette section), qui permet d'effectuer une rotation des fichiers journaux au lieu d'écrire dans un fichier toujours plus volumineux.

<VirtualHost _default_:port> : ce paramètre définit un ensemble de paramètres qui ne s'appliqueront qu'à un hôte virtuel (VirtualHost). Un hôte virtuel est un serveur virtuel, c'est-à-dire un serveur différent exécuté dans le même processus que d'autres serveurs. F-Secure Policy Manager Server ; par exemple, possède deux hôtes virtuels : un qui s'exécute dans le port 80 (module hôte deF-Secure Policy Manager Server) et un autre s'exécutant dans le port 8080 (FSMSA ou module d'administration).

Voici la configuration par défaut pour F-Secure Policy Manager Server :

```
# FSMSH port
<VirtualHost _default_:80>
<Location /fsms/fsmsh.dll>
SetHandler fsmsh-handler
</Location>
<Location /commdir>
SetHandler fsmsh-handler
</Location>
</VirtualHost>

#FSMSA port
<VirtualHost _default_:8080>
<Location /fsmsa/fsmsa.dll>
SetHandler fsmsa-handler
</Location>
</VirtualHost>
```

Commdir et **Commdir2 :** ces paramètres définissent le chemin d'accès au répertoire de communication ou au référentiel. Il s'agit du répertoire dans lequel F-Secure Policy Manager Server stocke toutes les données de gestion qu'il reçoit de Policy Manager Console et de F-Secure Management Agent. Vous pouvez modifier l'emplacement du répertoire de communication via ces paramètres, mais vous devez vous assurer que le compte à partir duquel le serveur est exécuté *(fsms_<nom wins de l'ordinateur>)* possède bien des droits complets sur ce répertoire.

```
Commdir "C:\Program Files\F-Secure\Policy Manager
Server\CommDir"
Commdir2 "C:\Program Files\F-Secure\Policy Manager
Server\CommDir"
```

CustomLog : cette entrée permet de consigner les demandes au serveur. Le premier paramètre est un fichier (dans lequel les demandes doivent être consignées) ou une barre verticale (|) suivie d'un programme qui recevra les informations de journal comme source d'entrée standard. Cette fonction est utilisée pour l'appel de l'utilitaire **rotatelogs** (voir l'entrée **rotatelogs** de cette section), qui permet d'effectuer une rotation des fichiers journaux au lieu d'écrire dans un fichier toujours plus volumineux.

Le second paramètre détermine ce qui est écrit dans le fichier journal. Il est défini par un paramètre **LogFormat** précédent.

Vous trouverez ci-dessous un exemple d'entrée dans le fichier *access.log* :

```
10.128.131.224 - - [18/Apr/2002:14:06:36 +0300]
/fsmsa/
fsmsa.dll?FSMSCommand=ReadPackage&Type=27&SessionID=248 HTTP/
1.1"
200 5299 0 - 0 - "FSA/5.10.2211 1.3.1_02 Windows2000/5.0 x86"
mod_gzip: DECHUNK:DECLINED:TOO_SMALL CR:0pct.
```

`10.128.131.224 - - [18/Apr/2002:14:06:36 +0300]` indique la date et l'heure d'envoi de la demande au serveur et l'hôte à l'origine de la demande (identifié par son adresse IP).

Le composant *fxnext* indique quel module la commande a envoyé à */fsmsa/fsmsa.dll*. Ce module *(fsmsa.dll)* est le module Admin. *fsmsh.dll* serait le module Hôte.

La commande et les paramètres viennent ensuite : `FSMSCommand=ReadPackage&Type=27&SessionID=248`. Dans le cas présent, l'hôte a demandé un objet de type 27 (un seul).

La version HTTP employée est également indiquée (`HTTP/1.1`).

La version HTTP est immédiatement suivie de six nombres :

1. Code de réponse HTTP : Dans cet exemple, `200` est utilisé, ce qui signifie OK selon la norme HTTP. Il existe d'autres codes, décrits dans la norme HTTP, que vous pouvez obtenir à l'adresse suivante : http://www.w3.org.
2. Octets transférés à partir du serveur : dans notre exemple, 5 299 octets ont été transférés.
3. Durée (en secondes) nécessaire au serveur pour servir la demande.
4. Etat de la connexion à la fin de la réponse.

   X = connexion annulée avant la fin de la réponse.

   + = la connexion peut rester active après l'envoi de la réponse.

   - = la connexion sera fermée après l'envoi de la réponse.
5. Code d'erreur du module d'administration F-Secure Policy Manager Server (0 en cas de réussite).
6. Octets transférés au serveur ("-" équivaut à zéro).

La chaîne suivante identifie le client `"FSA/5.10.2211 1.3.1_02 Windows2000/5.0 x86"`. Dans le cas présent, notez que le serveur a été contacté par FSA 5.10 build 2211.

Les informations qui suivent concernent la compression des données : `mod_gzip: DECHUNK:DECLINED:TOO_SMALL`.
Dans le cas présent, les données n'ont pas été compressées, car elles étaient de taille trop réduite.

Enfin, le taux de compression est indiqué (0% dans cet exemple) : `CR:0pct`.

Rotatelogs : Il s'agit d'un petit programme utilisé pour pivoter les fichiers journaux produit par F-Secure Policy Manager Server. Ce programme permet de définir la durée pendant laquelle un fichier journal est conservé (8 jours par défaut) et à quel moment la rotation doit être effectuée. A ce moment, *access.log* est renommé *access.log.1* et un nouveau fichier *access.log* est créé afin de consigner les nouvelles demandes.

Exemple :

```
CustomLog '|""C:\Program Files\F-Secure\Policy Manager Server
5\bin\rotatelogs"
"C:\Program Files\F-Secure\Policy Manager Server
5\logs\access.log" 8 86400"' common"
```

Dans cet exemple, le paramètre CustomLog détermine que l'utilitaire rotatelogs doit ouvrir le fichier *access.log* et employer 8 fichiers (8 fichiers d'archivage plus le fichier actif) qui subissent une rotation quotidienne (86 400 secondes = 24 heures). En pratique, cela signifie que les fichiers de la dernière semaine plus un jour sont conservés, et qu'un autre fichier est utilisé pour stocker les accès pendant la journée actuelle.

<ifModule mod_gzip.c> : ce paramètre est une nouveauté de F-Secure Policy Manager Server. Il permet de compresser toutes les données transférées entre la console et le serveur. Ce paramètre marque le début des paramètres de compression, qui se terminent juste avant le paramètre </ifModule>. Pour plus d'informations sur ces paramètres, reportez-vous au fichier httpld.sample, situé dans le même répertoire que le fichier de configuration de F-Secure Policy Manager Server (<répertoire d'installation fspms>\conf).

mod_gzip_on Yes : ce paramètre est l'un des paramètres de compression ; il active ou désactive la prise en charge de la compression dans F-Secure Policy Manager Server. La compression est désactivée si le paramètre est remplacé par mod_gzip_on No.

FastPolicyDistribution On : ce paramètre permet d'activer l'équilibre entre performances et compatibilité descendante maximale. Lorsqu'il est activé, il permet à F-Secure Policy Manager Server de distribuer les stratégies d'une manière qui accélère considérablement le processus (de 30 à 100 fois en fonction du nombre d'hôtes). Ce paramètre doit être désactivé si d'autres composants accèdent en même temps au répertoire de communication (par exemple, F-Secure Management Agent).

RetryFileOperation 10 : ce paramètre indique au serveur combien de fois il doit retenter une opération infructueuse sur un fichier (avec un intervalle d'une seconde entre les tentatives) avant d'abandonner.

CommdirCacheSize 10 : la valeur numérique de ce paramètre indique au serveur quel pourcentage de la mémoire il doit utiliser pour stocker les fichiers en mémoire avant de les servir. Le serveur peut ainsi servir plus rapidement les fichiers, car il ne doit pas les lire en permanence à partir du disque. Si vous utilisez la valeur par défaut (10), le serveur emploie 10 % de la mémoire disponible pour cette mise en cache. Par exemple, sur un ordinateur doté de 512 Mo de RAM, 51,2 Mo seront employés pour la mise en cache.

3.5 Désinstallation de F-Secure Policy Manager Server

Pour désinstaller F-Secure Policy Manager 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 F-Secure Policy Manager Server (ou le composant à désinstaller), puis cliquez sur le bouton **Ajouter/Supprimer**.
3. La boîte de dialogue *F-Secure Désinstallation* s'affiche. Cliquez sur **Démarrer** pour démarrer la désinstallation.
4. Au terme de la désinstallation, cliquez sur **Fermer**.
5. Cliquez sur **OK** pour fermer la boîte de dialogue *Ajout/Suppression de programmes*.

4 Installation de F-Secure Policy Manager Console

4.1 Présentation

F-Secure Policy Manager Console peut fonctionner en deux modes :

- Mode administrateur - vous pouvez utiliser F-Secure Policy Manager Console avec toutes ces fonctionnalités.
- Mode Lecture seule : permet de visualiser les informations de F-Secure Policy Manager Console, mais pas d'accomplir des tâches administratives. Ce mode peut par exemple être utile pour les agents d'un service d'assistance.

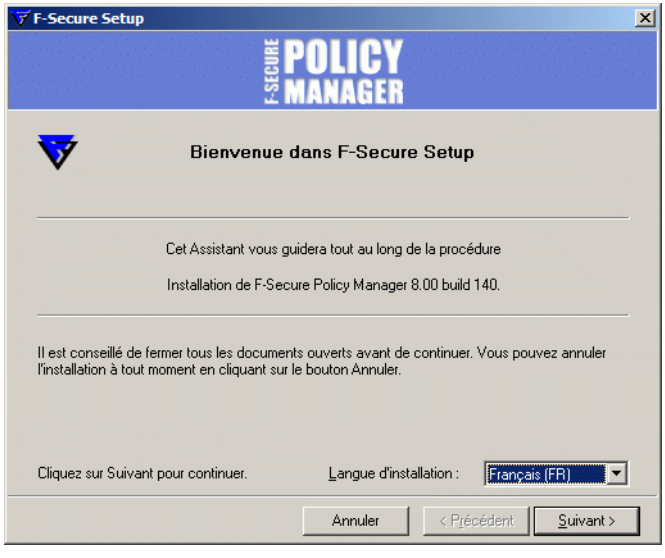
Les connexions en mode Administrateur et Lecture seule peuvent s'effectuer à l'aide de la même installation de la console. Les sections suivantes expliquent comment exécuter le programme d'installation de F-Secure Policy Manager Console à partir du CD-ROM F-Secure, ainsi que la manière de choisir le mode de fonctionnement initial lors de la première exécution de la console. L'installation à partir du CD-ROM est identique pour les deux modes. Il est toujours possible d'ajouter de nouvelles connexions en modes Administrateur et Lecture seule après le démarrage initial.

4.2 Procédure d'installation

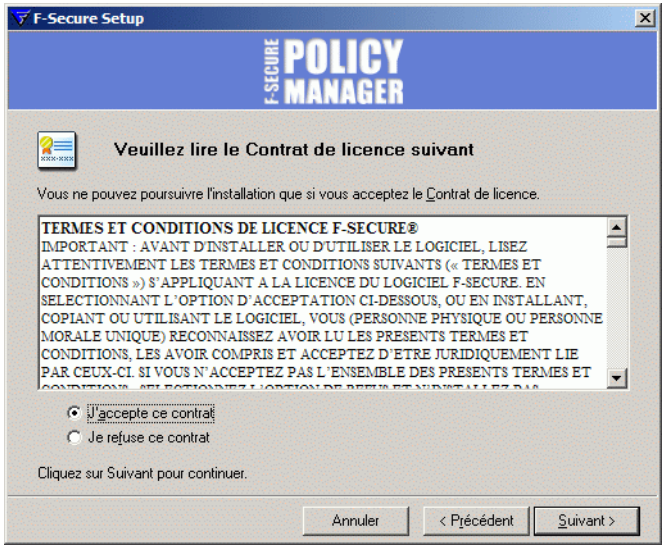
Etape 1.

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*.

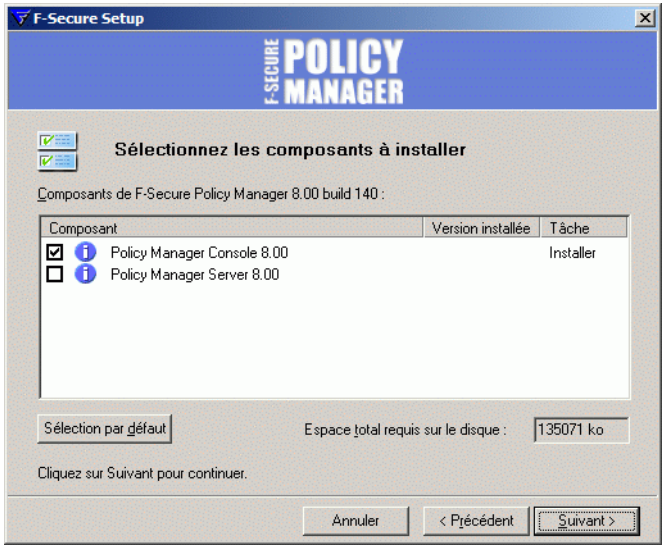
Etape 2. Prenez connaissance du contenu de l'écran d'accueil, puis suivez les instructions relatives à l'installation. Sélectionnez la langue d'installation dans le menu déroulant. Cliquez sur **Suivant** pour continuer.



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

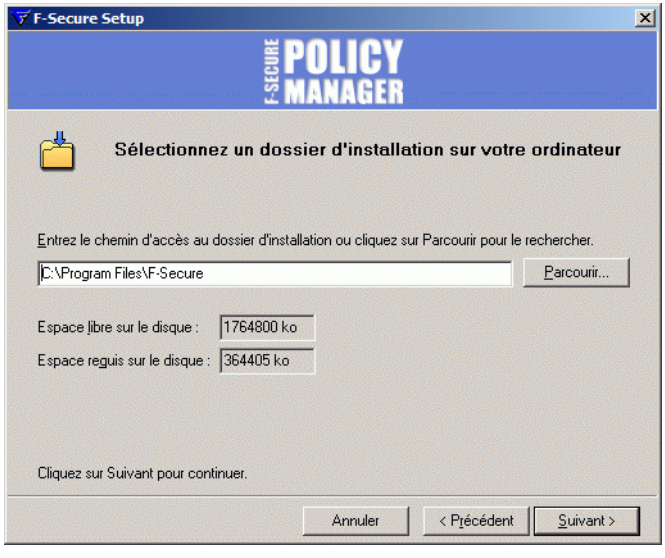


Etape 4. Sélectionnez F-Secure Policy Manager Console. Cliquez sur **Suivant** pour continuer.

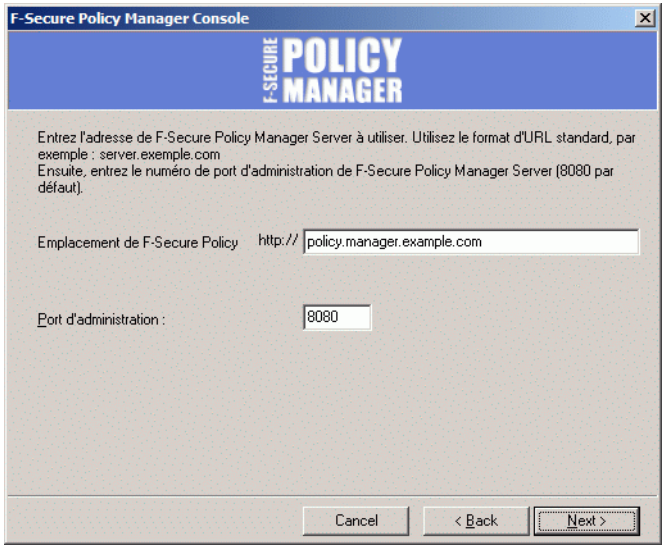


Etape 5. Choisissez le dossier de destination. Cliquez sur **Suivant**.

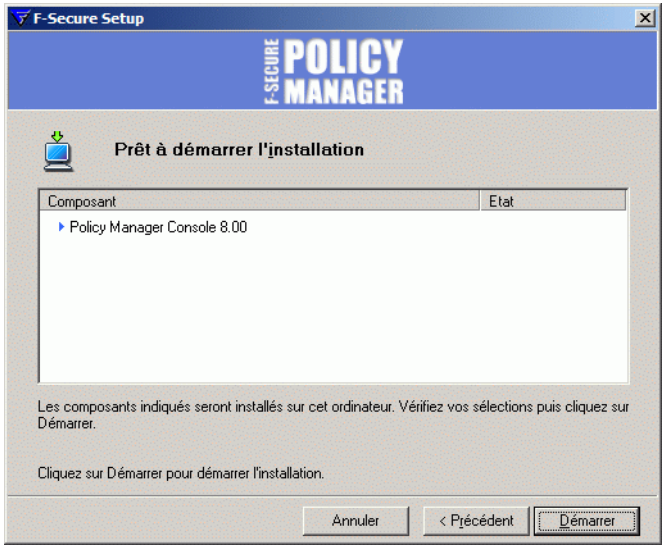
Nous vous recommandons d'utiliser le répertoire d'installation par défaut. Utilisez la fonction **Parcourir** pour installer F-Secure Policy Manager Console dans un autre répertoire.



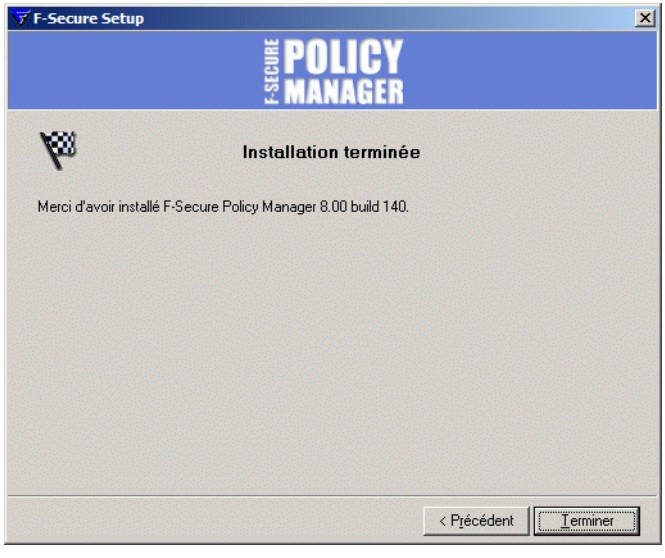
Etape 6. Spécifiez l'adresse de F-Secure Policy Manager Server, ainsi que le numéro du port d'administration. Cliquez sur **Suivant** pour continuer.



Etape 7. Examinez les modifications que le programme d'installation va apporter. Cliquez sur **Suivant** pour continuer.

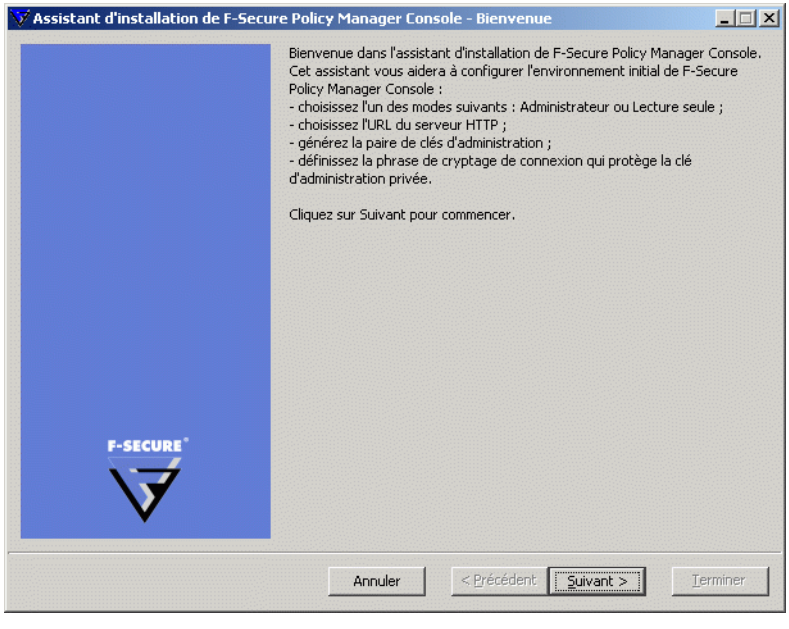


Etape 8. Cliquez sur **Terminer** pour fermer le programme d'installation.



Etape 9. Exécutez *F-Secure Policy Manager Console* en cliquant sur *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.

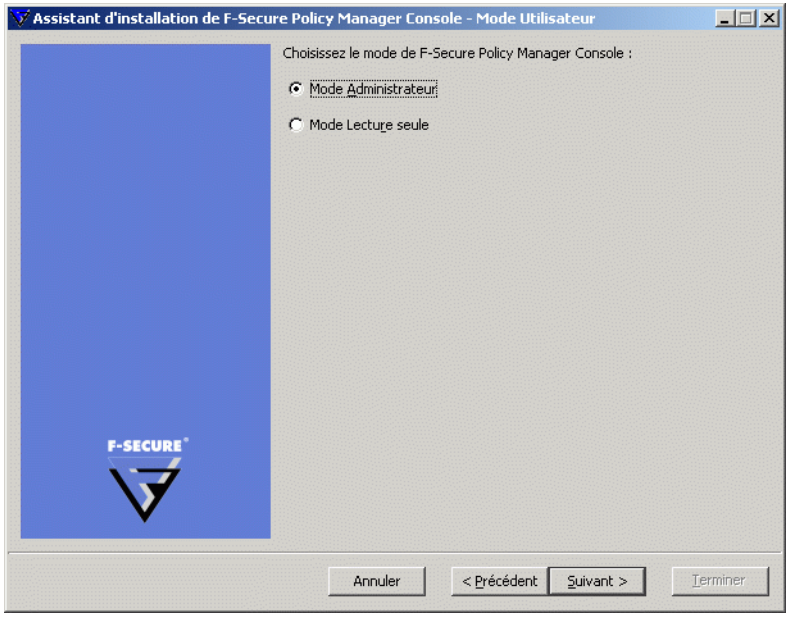
La première page de l'Assistant d'installation de F-Secure Policy Manager Console résume le processus d'installation. Cliquez sur **Suivant** pour continuer.



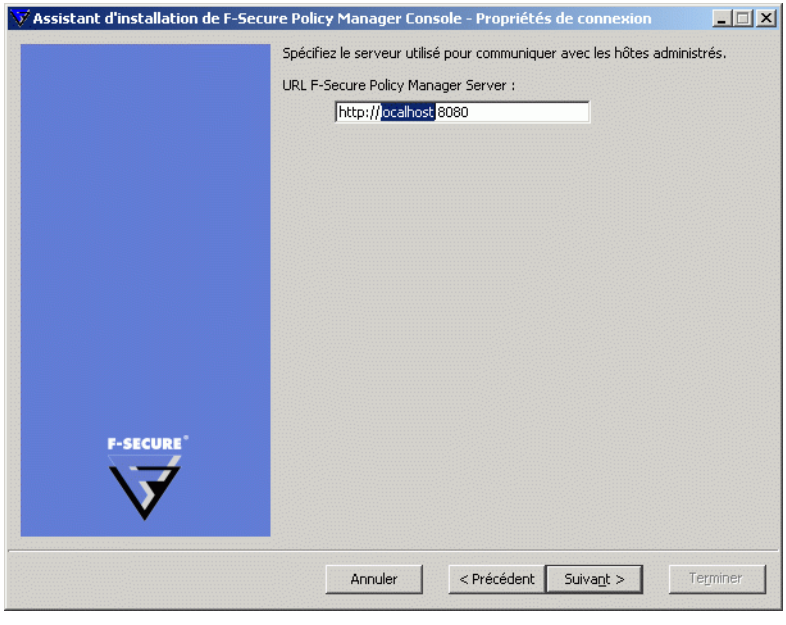
Etape 10. Sélectionnez le mode d'utilisation correspondant à vos besoins :

- *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*.

Cliquez sur **Suivant** pour continuer.



Etape 11. Saisissez l'adresse du serveur F-Secure Policy Manager Server utilisé pour la communication avec les hôtes gérés.

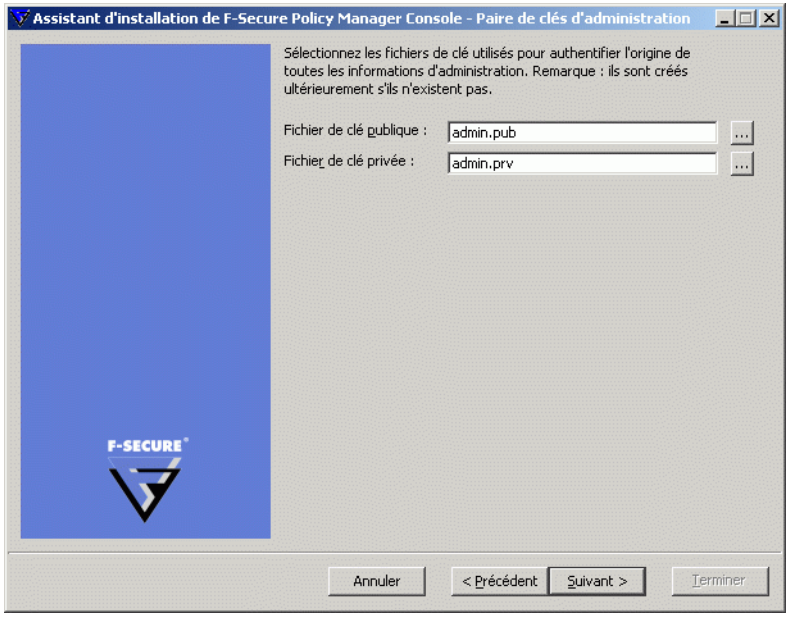


Etape 12. Entrez le chemin d'accès au répertoire où vous souhaitez stocker les fichiers de clé privée et de clé publique de l'administrateur. Par défaut, les fichiers de clé sont enregistrés dans le répertoire d'installation de F-Secure Policy Manager Console.

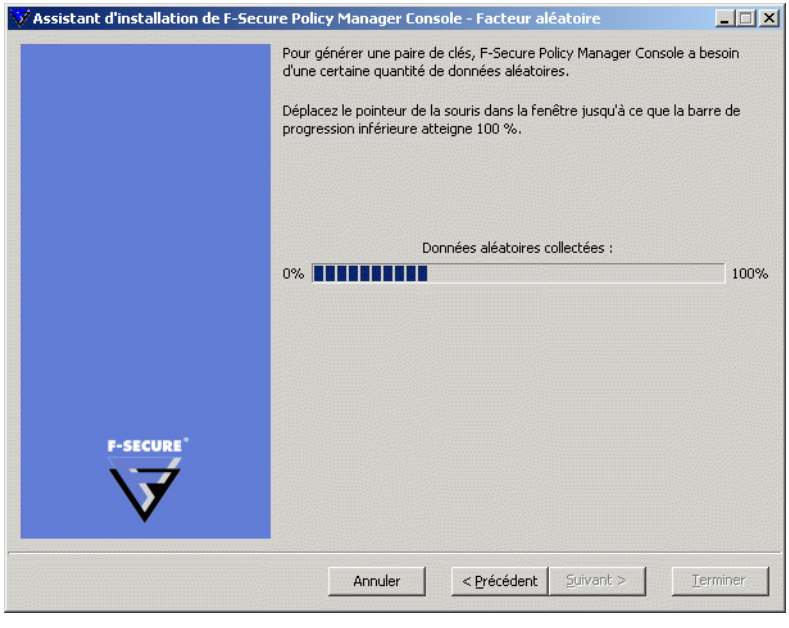
Program Files\F-Secure\Administrator.

Cliquez sur **Suivant** pour continuer.

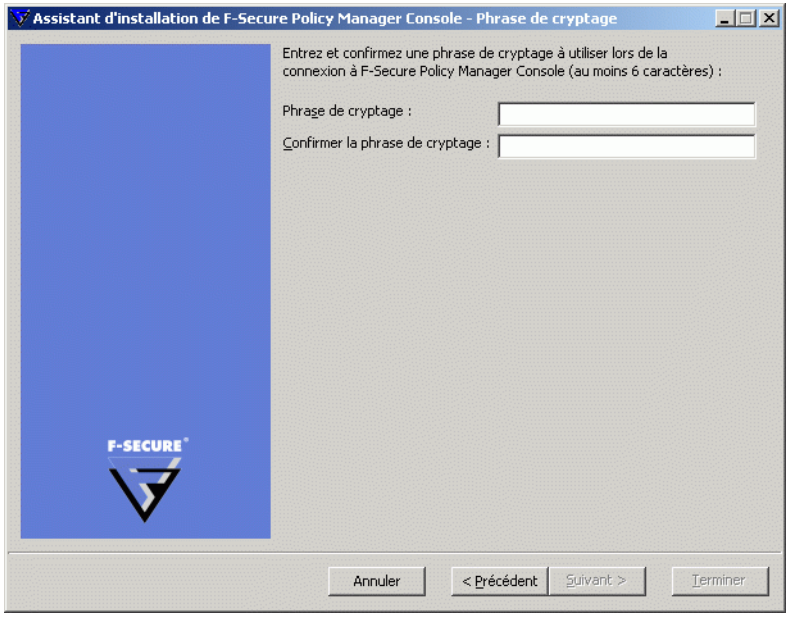
Si la paire de clés n'existe pas encore, elle sera créée plus tard, au cours du processus de configuration.



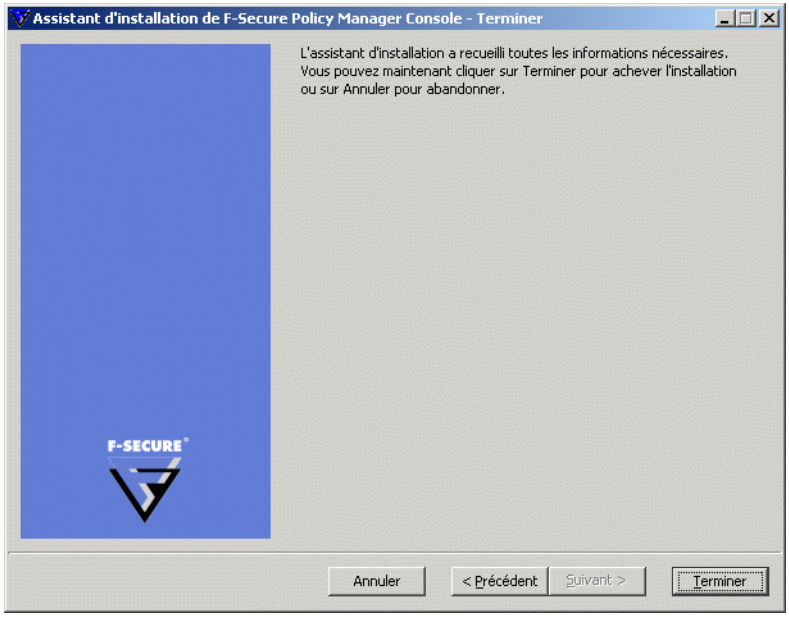
Etape 13. Déplacez votre curseur dans la fenêtre afin d'initialiser le facteur aléatoire utilisé par le générateur du jeu de clés d'administration. L'utilisation des déplacements de la souris assure que le facteur de l'algorithme de génération de jeu de clés est suffisamment aléatoire. Lorsque l'indicateur d'avancement atteint 100 %, la boîte de dialogue *Phrase de cryptage* s'affiche automatiquement.



Etape 14. 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**.



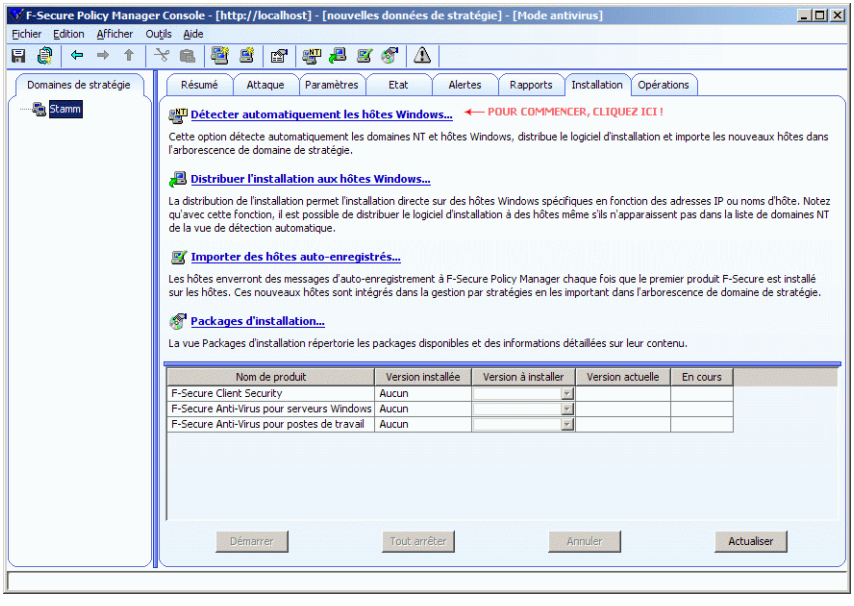
Etape 15. Cliquez sur **Terminer** pour terminer le processus de configuration.



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

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

Etape 16. L'assistant d'installation crée le groupe d'utilisateurs `FSPM users`. L'utilisateur qui avait ouvert une session et qui a procédé à l'installation est automatiquement ajouté à ce groupe. Pour autoriser un autre utilisateur à exécuter F-Secure Policy Manager, vous devez l'ajouter manuellement au groupe d'utilisateurs `FSPM users`.



F-Secure Policy Manager Console démarre en mode antivirus, qui constitue une interface utilisateur optimisée pour la gestion de F-Secure Client Security et F-Secure Anti-Virus pour les stations de travail. Si vous comptez utiliser F-Secure Policy Manager Console pour gérer un autre produit F-Secure, vous devez utiliser l'interface utilisateur en mode avancé. Pour y accéder, cliquez sur le menu *Affichage* et sélectionnez l'option *Mode avancé*.

Lorsque vous configurez les stations de travail, vous devez y installer une copie du fichier de clé *Admin.pub* (ou leur donner l'accès à ce fichier). Si vous installez 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-ROM, vous devez transférer manuellement une copie du fichier de clés *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.

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.

4.3 Désinstallation de F-Secure Policy Manager Console

Pour désinstaller F-Secure Policy Manager Console (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 Certificate Wizard), puis cliquez sur le bouton **Ajouter/Supprimer**.
3. La boîte de dialogue *F-Secure Désinstallation* s'affiche. Cliquez sur **Démarrer** pour démarrer la désinstallation.
4. Au terme de la désinstallation, cliquez sur **Fermer**.
5. Cliquez sur OK pour fermer la boîte de dialogue *Ajout/Suppression de programmes*.

5 Utilisation de F-Secure Policy Manager Console

5.1 Présentation

F-Secure Policy Manager Console est une console d'administration distante destinée aux produits de sécurité les plus courants de F-Secure. Elle fournit une plate-forme commune à toutes les fonctions de gestion de la sécurité requises dans un réseau d'entreprise.

Un administrateur peut créer différentes stratégies de sécurité pour chaque hôte ou une stratégie unique pour plusieurs hôtes. Cette stratégie peut être diffusée sur un réseau vers les postes de travail, les serveurs et les passerelles de sécurité.

Avec F-Secure Policy Manager Console, vous pouvez :

- configuration des valeurs des attributs des produits gérés ;
- configuration des droits des utilisateurs à afficher ou modifier les valeurs des attributs définies à distance par l'administrateur ;
- regroupement des hôtes administrés sous des domaines de stratégie partageant des valeurs d'attributs communes ;
- administration simplifiée des hiérarchies de domaines et des hôtes ;
- création de définitions de stratégie signées, y compris les valeurs d'attributs et les restrictions ;
- affichage des informations d'état ;
- gestion des alertes ;
- gérer les rapports d'analyse de F-Secure Anti-Virus ;
- gestion des installations distantes ;
- visualisation des rapports au format HTML ou exportation des rapports vers différents formats.

F-Secure Policy Manager Console génère la définition de stratégie et affiche l’état et les alertes. Chaque hôte administré dispose d'un module (F-Secure Management Agent) responsable de l'exécution de la stratégie sur l'hôte.

L’environnement conceptuel de F-Secure Policy Manager Console consiste en plusieurs hôtes pouvant être regroupés en domaines de stratégie. Les stratégies sont orientées hôte. Même dans un environnement multi-utilisateurs, tous les utilisateurs d'un hôte donné partagent des paramètres communs.

F-Secure Policy Manager Console reconnaît deux types d’utilisateurs : les administrateurs et les utilisateurs en mode Lecture seule.

L'administrateur a accès à la clé privée d'administration. Cette clé est stockée dans un fichier que plusieurs utilisateurs peuvent partager en fonction de leurs droits d'administration. L’administrateur utilise F-Secure Policy Manager Console pour définir les stratégies de différents domaines et hôtes individuels.

En mode *Lecture seule*, l'utilisateur peut effectuer les opérations suivantes :

- afficher les stratégies, les statistiques, les informations d'état relatives aux opérations, les numéros de version des produits installés, les messages d'alerte et les rapports ;
- Modifiez les propriétés de F-Secure Policy Manager Console car son installation est basée sur l’utilisateur et que les modifications ne peuvent être appliquées aux autres utilisateurs.

En mode Lecture seule, l'utilisateur ne peut pas effectuer les opérations suivantes :

- modifier la structure des domaines ou les propriétés des domaines et des hôtes ;
- modifier les paramètres des produits ;
- exécuter des opérations ;
- installer des produits ;
- enregistrer des données de stratégie ;
- distribuez des stratégies.
- supprimer des messages d'alerte ou des rapports.

Il ne peut y avoir qu'une seule connexion à F-Secure Policy Manager Server en mode Administrateur à la fois. Cependant, il peut y avoir plusieurs connexions en lecture seule simultanées à F-Secure Policy Manager Server.

5.2 Fonctions de base de F-Secure Policy Manager Console

Les sections suivantes décrivent la procédure d'ouverture de session, les commandes de menu et les tâches de base de F-Secure Policy Manager Console.

5.2.1 Ouverture de session

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

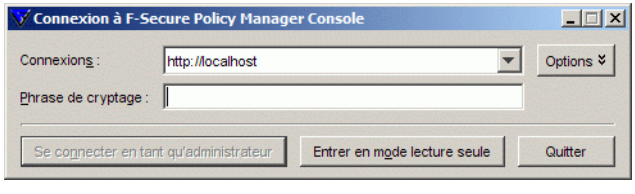


Figure 5-1 F-Secure Policy Manager Console Boîte de dialogue d'ouverture de session

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.

Il est également possible de définir des connexions multiples à un serveur unique. 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 démarrer le programme en mode Lecture seule, auquel cas vous n'avez pas besoin d'entrer une phrase de cryptage. Le cas échéant, cependant, vous ne pourrez effectuer aucune modification.

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

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

Propriétés de connexion

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

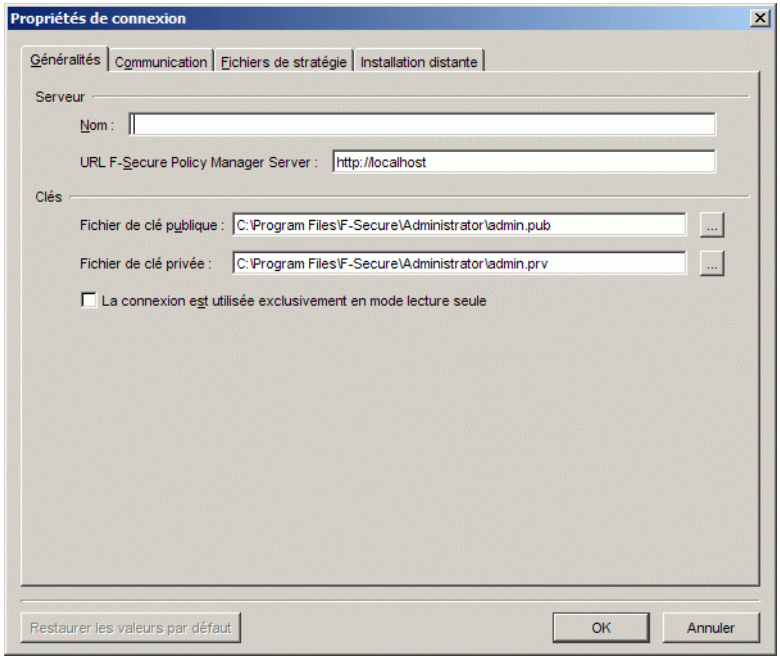


Figure 5-2 Boîte de dialogue Propriétés de connexion

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 Fichier de clé publique et Fichier de clé privée indiquent quel jeu de clés d'administration doit être utilisé pour la connexion en question. Si les fichiers de clés spécifiés n'existent pas, F-Secure Policy Manager Console génère une nouvelle paire de clés.

Préférences de communication

Cliquez sur l'onglet *Communication* pour personnaliser les paramètres de communication. Pour modifier les intervalles d'interrogation, cliquez sur **Options d'intervalle d'interrogation**.

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. Les hôtes déconnectés sont signalés par une icône de notification dans l'arborescence, et ils sont placés dans la liste Hôtes déconnectés de la vue Etat du domaine. 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, il se peut qu'un ordinateur portable soit incapable d'accéder quotidiennement au serveur, mais dans la plupart des cas, ce comportement est tout à fait acceptable.

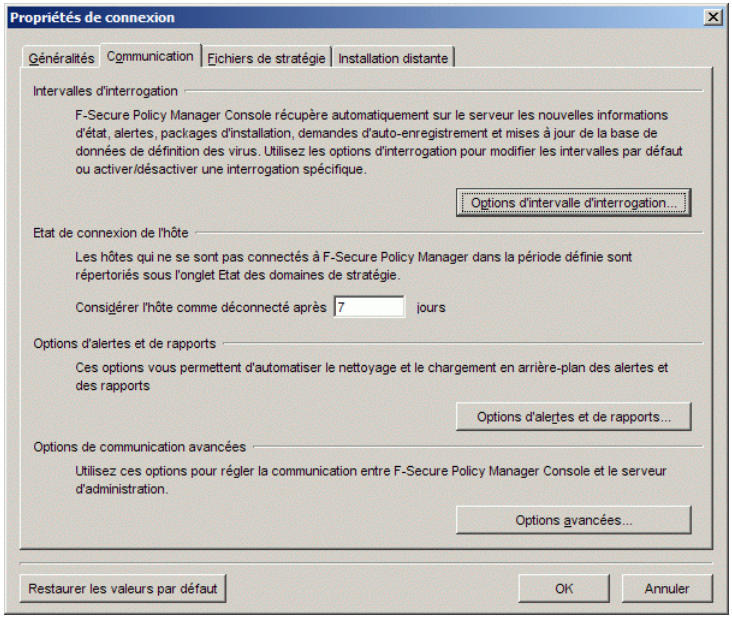


Figure 5-3 Boîte de dialogue Propriétés de connexion > Communication

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, désactivez complètement les récupérations inutiles. Pour ce faire,

décochez l'élément de récupération que vous souhaitez désactiver. L'option *Désactiver toutes les interrogations* permet de désactiver l'ensemble des éléments d'interrogation. Que l'interrogation automatique soit désactivée ou non, les opérations d'actualisation manuelle peuvent servir à actualiser les informations sélectionnées.

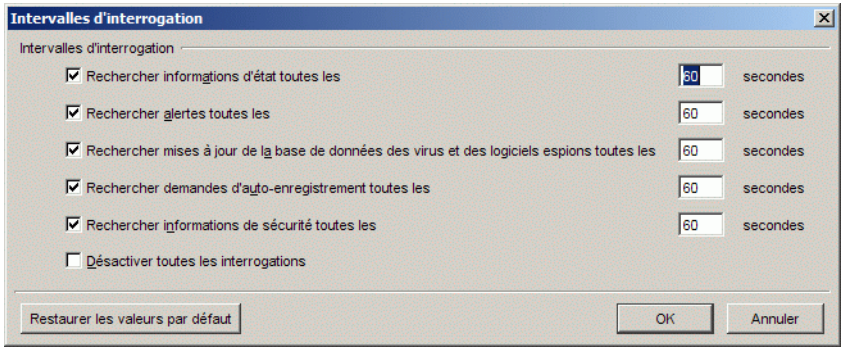


Figure 5-4 Boîte de dialogue Intervalles d'interrogation

Pour plus d'informations sur les autres paramètres spécifiques à la connexion, reportez-vous à la section "*Préférences*", *138*. Une fois F-Secure Policy Manager Console lancé, ces paramètres peuvent être modifiés normalement depuis la vue *Préférences*.

5.2.2 Gestion de F-Secure Client Security

Lorsque vous lancez F-Secure Policy Manager Console pour la première fois, l'interface utilisateur en mode antivirus simplifié s'ouvre. Ce mode est optimisé pour l'administration de F-Secure Client Security. En utilisant l'interface utilisateur en mode antivirus, vous pouvez réaliser les tâches de gestion de F-Secure Client Security ou de F-Secure Anti-Virus pour les stations de travail.

Pour plus d'informations sur l'interface utilisateur en mode antivirus, reportez-vous au Guide de l'administrateur de F-Secure Client Security.

Vous devriez être en mesure de réaliser la plupart des tâches avec l'interface utilisateur en mode antivirus. En revanche, si vous devez administrer des produits autres que F-Secure Client Security, vous devrez utiliser l'interface utilisateur en mode avancé.

5.2.3 L'interface utilisateur en mode avancé

Pour utiliser toutes les fonctionnalités disponibles dans F-Secure Policy Manager Console, vous devez modifier l'interface utilisateur en mode avancé. Pour y parvenir, sélectionnez **Affichage > Mode avancé**.

L'interface utilisateur en mode avancé s'affiche sur les quatre volets suivants : *Domaine de stratégie*, *Propriétés*, *Affichage produit* et *Messages* (invisible en l'absence de message).

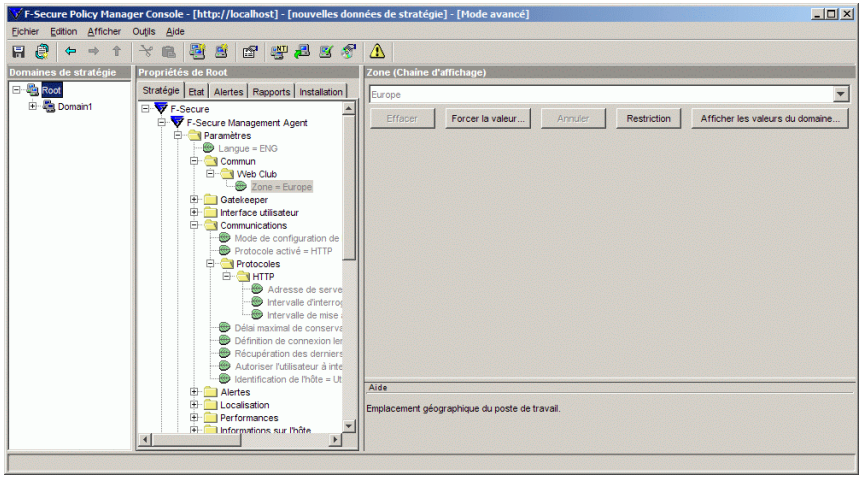


Figure 5-5 Interface utilisateur de F-Secure Policy Manager Console

5.2.4 Volet Domaine de stratégie

Dans le volet Domaine de stratégie, vous pouvez effectuer les opérations suivantes :

- Ajouter un nouveau domaine de stratégie (cliquez 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 hôte (cliquez sur l'icône ).
- Rechercher un hôte.
- Afficher les propriétés d'un domaine ou d'un hôte. Les noms attribués à chaque hôte et domaine doivent être sans ambiguïté.
- Importer des hôtes auto-enregistrés.
- Détecter automatiquement des hôtes d'un domaine Windows.
- Supprimer des hôtes ou des domaines.
- Déplacer des hôtes ou des domaines à l'aide des fonctions Couper et Coller.
- Exporter un fichier de stratégie.

Une fois le domaine ou l'hôte sélectionné, vous pouvez accéder à ces commandes depuis le menu *Edition*.

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.

5.2.5 Volet Propriétés

La définition de stratégies consiste à spécifier des valeurs de paramètres par défaut et les valeurs autorisées, ainsi que les restrictions d'accès à ces paramètres. Les stratégies s'appliquant à un domaine ou un hôte sont définies dans le volet Propriétés.

Ce volet contient les sous-arborescences (« branches »), les tables, les lignes et les variables des stratégies. Les sous-arborescences sont utilisées uniquement pour développer les structures. Les tables peuvent contenir autant de lignes que vous le souhaitez.

Le volet Propriétés contient les onglets suivants :

- **Stratégie** : cet onglet vous permet d'utiliser le volet Affichage produit pour définir les paramètres, les restrictions et les opérations des domaines ou des hôtes. Ces modifications sont appliquées une fois que la stratégie a été diffusée et que F-Secure Management Agent a recherché le fichier de stratégie.
- **Etat** : sous chaque produit affiché sous cet onglet, figurent deux catégories d'état : *Paramètres* et *Statistiques*. La catégorie *Paramètres* affiche les paramètres locaux qui ont été modifiés de façon explicite sur l'hôte ; les valeurs par défaut ou celles qui ont été définies dans la stratégie de base ne sont pas affichées. La catégorie *Statistiques* affiche les statistiques relatives à chaque hôte, et ce pour chaque produit. Si un domaine de stratégie est sélectionné, l'onglet Etat présente le nombre d'hôtes du domaine, et les hôtes qui sont déconnectés de F-Secure Policy Manager.
- **Alertes** : cet onglet affiche la liste des alertes émanant des hôtes dans le domaine sélectionné. Il affiche également l'alerte sélectionnée dans le volet Affichage produit, ainsi que les rapports correspondant aux alertes.
- **Rapports** : cet onglet affiche tous les rapports émanant de l'hôte sélectionné.
- **Installation** : affiche les options d'installation.

5.2.6 Volet Affichage produit

La fonction du volet *Affichage produit* dépend de l'onglet qui est sélectionné dans le volet *Propriétés* :

- Onglet **Stratégie** : le volet *Affichage produit* vous permet de définir la valeur d'une variable de stratégie. Toutes les modifications concernent l'hôte ou le domaine de stratégie sélectionné. Un éditeur par défaut est prédéfini pour chaque type

de variable de stratégie. L'éditeur s'affiche lorsque vous sélectionnez le type de variable sous l'onglet *Stratégie*. Certains nœuds non terminaux, tables et sous-arborescences peuvent être associés à des éditeurs personnalisés spécifiques. Ces éditeurs personnalisent F-Secure Policy Manager Console pour chaque produit installé. Il existe également des éditeurs de restriction qui s'ouvrent dans le volet *Affichage produit* ou sous forme de boîte de dialogue séparée.

- Onglet **Etat** : le volet *Affichage produit* vous permet de visualiser (1) les « paramètres », qui sont les modifications locales signalées par l'hôte, ainsi que les (2) statistiques.
- Onglet **Alertes** : lorsqu'une alerte est sélectionnée sous l'onglet *Alertes*, les détails relatifs à l'alerte s'affichent dans le volet *Affichage produit*.
- Onglet **Rapports** : lorsqu'un rapport est sélectionné sous l'onglet *Rapports*, les détails relatifs au rapport s'affichent dans le volet *Affichage produit*.
- **Installation** : le volet *Affichage produit* permet de consulter et de modifier les informations d'installation.

L'arborescence traditionnelle de la base de données MIB F-Secure Policy Manager Console contient tous les paramètres/activités (stratégie) et les paramètres/statistiques (état) dans une arborescence MIB spécifique à un composant du produit.

L'affichage produit de F-Secure Management Agent est présenté à la page suivante à titre d'exemple. Tous les affichages Produit possèdent les mêmes activités et fonctionnalités génériques.

Utilisation de l'aide

Dans la plupart des cas, l'affichage produit fournit les mêmes textes d'aide que les nœuds de l'arborescence MIB. En outre, chaque onglet possède un texte d'aide spécifique. Ce texte suit les clics de souris (tous les onglets ainsi que les éditeurs de stratégies et d'état) et l'activation des zones (uniquement en cas de sélection de l'onglet *Stratégie* du volet *Propriétés*). Vous pouvez cliquer sur l'intitulé d'une zone ou dans la zone de saisie pour activer le texte d'aide correspondant.

Modification des paramètres de stratégie

Sélectionnez un produit (ex. : F-Secure Management Agent) et l'onglet *Stratégie* de l'onglet Propriétés. F-Secure Policy Manager Console affichera un volet Affichage produit pour le produit sélectionné et contiendra les paramètres les plus fréquemment utilisés ainsi que les éditeurs de restriction de l'arborescence MIB, dans les catégories ci-après :

- Communication : paramètres de communication.
- Alertes : paramètres relatifs aux alertes.
- Transmission des alertes : pour plus d'informations, reportez-vous à la section *"Configuration de la transmission des alertes"* à la page 131.
- Certificats : définition de certificats approuvés.
- Répertoire des certificats : définition des paramètres des répertoires où les certificats sont stockés.
- A propos de : contient un lien vers F-Secure Web Club (pour plus d'informations, reportez-vous à la section "*Web Club*", *224*).

Vous pouvez modifier les paramètres de stratégie de manière normale et employer le paramètre de restriction (final, masqué) pour définir les droits d'accès des utilisateurs.

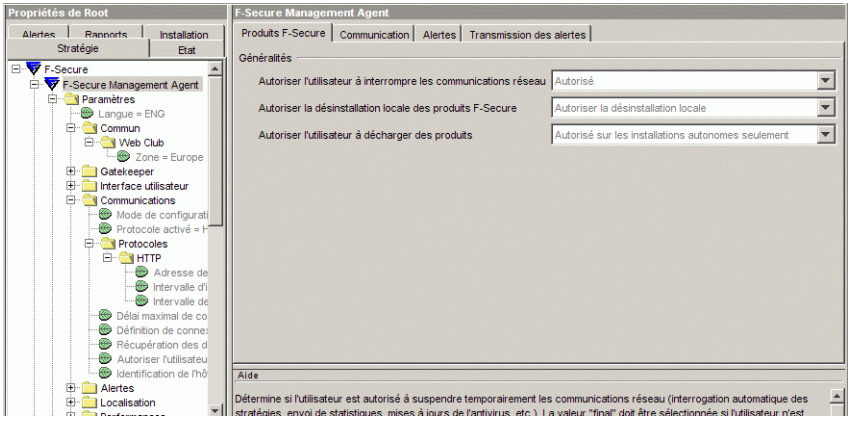


Figure 5-6 Volet Affichage produit

Utilisation du menu contextuel pour les paramètres de stratégie

La plupart des zones de saisie de l'affichage Produit comprennent un menu contextuel (activé par un clic du bouton droit de la souris). Le menu contextuel contient les commandes suivantes : *Aller à, Effacer, Forcer la valeur* et *Afficher les valeurs du domaine*.

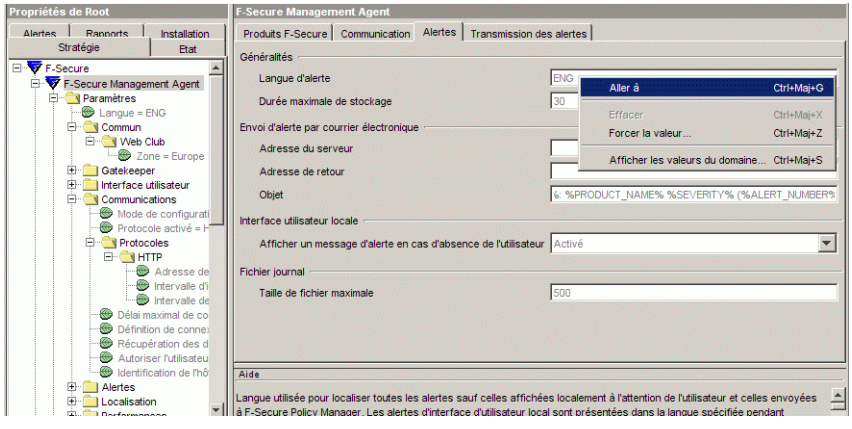


Figure 5-7 Menu contextuel

Raccourci vers le nœud de l'arborescence MIB

Il est parfois utile de savoir quel paramètre de l'arborescence MIB sera modifié en cas d'édition d'un élément d'un affichage Produit. La commande *Aller à* du menu contextuel permet d'afficher le nœud correspondant de l'arborescence MIB dans le volet *Propriétés*.

Notez que, dans la plupart des cas, l'arborescence MIB fournit davantage de paramètres. Ceux-ci sont toutefois moins fréquemment utilisés. Par exemple, elle permet d'éditer les restrictions des paramètres de stratégie pour lesquels l'affichage Produit ne contient pas directement d'éditeur de restrictions.

Effacer

La commande *Effacer* fonctionne de la même manière que dans l'arborescence MIB. Lorsque la valeur actuelle est effacée, la zone affiche la valeur héritée (de couleur grise) ou est vide. La commande *Effacer* n'est disponible que si une valeur a été définie pour le domaine ou l'hôte actuellement sélectionné.

Forcer la valeur

La commande *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 le volet *Domaines de stratégie*. Il est possible d'ouvrir simultanément plusieurs boîtes de dialogue de valeurs de domaine.

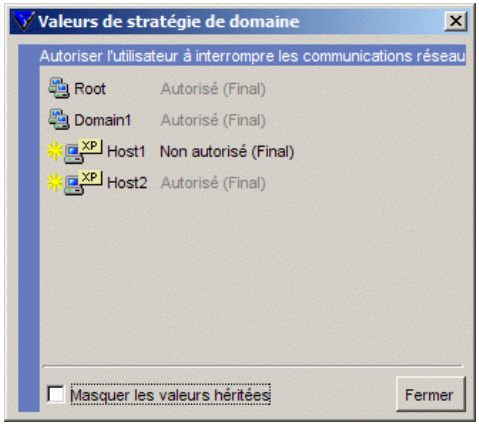


Figure 5-8 Boîte de dialogue Afficher les valeurs du domaine

Affichage de l'état

Ouvrez l'onglet *Etat* et sélectionnez le produit dans le volet *Propriétés*. F-Secure Policy Manager Console affichera un volet Affichage produit, dans lequel vous trouverez les paramètres locaux et statistiques les plus importants.

Il est impossible de modifier les valeurs. Par contre, vous pouvez consulter les textes d'aide MIB en cliquant sur une zone ou sur son libellé.

Pour les domaines de stratégie, l'onglet *Etat* affiche l'état récapitulatif au niveau du domaine : le nombre d'hôtes du domaine et la liste des hôtes déconnectés.

Figure 5-9 Onglet Etat

Cliquez sur un hôte déconnecté afin de modifier rapidement la sélection de domaine de stratégie pour cet hôte. Ce faisant, vous pouvez déterminer si l'hôte déconnecté a réussi à envoyer quelques alertes ou des statistiques utiles avant sa déconnexion. Ces informations peuvent vous aider à déterminer pourquoi l'hôte a été déconnecté. Si la raison est évidente (par exemple si le logiciel F-Secure a été désinstallé de l'hôte), vous pouvez supprimer l'hôte normalement. Après avoir examiné un hôte déconnecté, la manière la plus pratique de revenir au niveau précédent du domaine consiste à cliquer sur le bouton  de la barre d'outils.

La vue Etat du domaine comprend également deux raccourcis qui permettent de traiter un nombre élevé d'hôtes déconnectés : la sélection de tous les hôtes déconnectés et leur suppression. Ces deux actions sont accessibles via le menu contextuel du nœud Hôte déconnecté de l'arborescence.

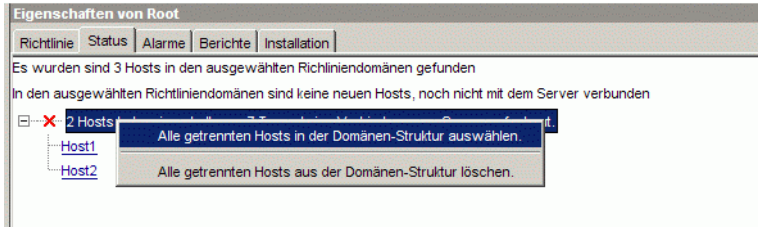


Figure 5-10 Exemple des raccourcis disponibles dans la vue Etat du domaine

AVERTISSEMENT : La suppression de tous les hôtes déconnectés est une opération potentiellement dangereuse. Certains hôtes existants peuvent, pour l'une ou l'autre raison, être déconnectés temporairement pendant une période supérieure au délai autorisé. Vérifiez toujours la valeur du délai de déconnexion dans la zone Préférences avant de supprimer des hôtes. Si un hôte existant est supprimé accidentellement, vous effacerez ses alertes, rapports, états et paramètres de stratégie. Par contre, l'hôte enverra un message d'auto-enregistrement lorsqu'il s'apercevra qu'il a été supprimé de F-Secure Policy Manager. L'hôte pourra ensuite être réimporté dans l'arborescence du domaine. Toutefois, par rapport à Policy Manager, il sera considéré comme un nouvel hôte.

5.2.7 Volet Messages

F-Secure Policy Manager Console consigne les messages relatifs aux différents événements dans le volet *Message*. Contrairement aux volets *Alertes* et *Rapports*, les événements du volet *Message* ne sont générés que par F-Secure Policy Manager Console.

Il existe trois catégories de messages : informations, avertissements et erreurs. Chaque onglet du volet Messages contient des messages de trois niveaux de gravité. Vous pouvez supprimer une catégorie à l'aide du menu contextuel qui s'affiche lorsque vous cliquez sur un onglet avec le

bouton droit de la souris. Lorsque vous cliquez sur un message avec le bouton droit de la souris, un menu contextuel s'affiche vous permettant de couper, copier et supprimer le message.

Par défaut, les messages sont répertoriés sous la forme de fichiers dans le sous-répertoire des messages du répertoire d'installation local de F-Secure Policy Manager Console. Les fichiers journaux des messages sont stockés en anglais et dans la langue que vous avez paramétrée pour F-Secure Policy Manager Console. Un fichier journal différent est créé pour chaque catégorie de message (noms des onglets dans le volet Messages). Utilisez la page Préférences - Emplacements pour spécifier le répertoire du fichier journal et activer ou désactiver la tenue du journal. Les fonctions de la page Messages ne sont pas affectées lorsque vous activez ou que vous désactivez l'enregistrement de messages.

5.2.8 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.

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.

5.2.9 Options 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 une 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.
Modifier	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.
	Détecter automatiquement les 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.
	Volet Messages	Affiche ou masque le volet Messages en bas de l'écran.
	Ouvrir pour un nouveau message	S'il est sélectionné, le volet Message s'ouvre automatiquement quand un nouveau message est reçu.
	Retour	Accède au domaine ou à l'hôte précédent dans l'historique de sélection de l'arborescence.
	Suivant	Accède au domaine ou à l'hôte suivant dans l'historique de sélection de l'arborescence.
	Domaine parent	Accède au domaine parent.
	Toutes les alertes	Affiche toutes les alertes dans la page Alertes du volet Propriétés.
	Mode avancé	Active l'interface utilisateur en mode avancé, qui est décrite dans le présent manuel.
	Mode antivirus	Active l'interface utilisateur en mode antivirus, qui est optimisée pour une gestion centralisée de F-Secure Client Security.
	Actualiser <Elément>	Permet d'actualiser manuellement l'affichage du rapport, de l'état ou de l'alerte. L'élément de menu varie en fonction de l'onglet sélectionné dans le volet Propriétés.

	Actualiser tout	Permet d'actualiser manuellement toutes les données concernant l'interface : stratégie, état, alertes, rapports, packages d'installation et demandes d'auto-enregistrement.
Outils	Packages d'installation	Affiche dans une boîte de dialogue les informations relatives aux packages d'installation.
	Modifier la phrase de cryptage	Change la phrase de cryptage de connexion (la phrase de cryptage protégeant la clé privée de 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.
	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.

5.3 Administration des domaines et des hôtes

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

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

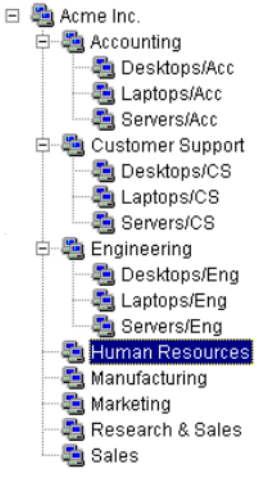


Figure 5-11 Exemple de structure de domaines de stratégie

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

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

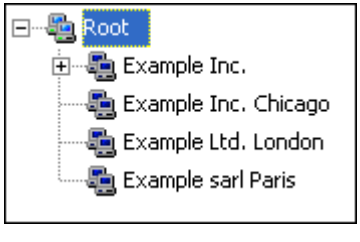


Figure 5-12 Exemple de structure de domaines de stratégie : bureaux nationaux en tant que sous-domaines

5.3.1 Ajout de domaines de stratégie

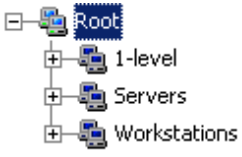


Figure 5-13 Exemple de domaine de stratégie avec des sous-domaines

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.

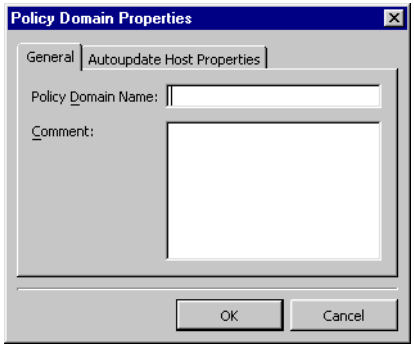


Figure 5-14 Boîte de dialogue Propriétés du domaine de stratégie

Vous êtes alors invité à entrer le nom de la stratégie de domaine. Une icône représentant le domaine est créée dans le volet *Domaine de stratégie* .

5.3.2 Ajout d'hôtes

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

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

Domaines Windows

Dans un domaine Windows, la méthode la plus pratique pour ajouter des hôtes dans votre domaine de stratégie consiste à importer ceux-ci à l'aide du composant d'installation intelligente de F-Secure en sélectionnant la commande « Autodécouvrir hôtes Windows » du menu *Edition* de F-Secure Policy Manager Console. Notez que cela installe également F-Secure Management Agent 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*. Au terme de l'opération de découverte automatique, le nouvel hôte est automatiquement ajouté à l'arborescence du domaine de stratégie. Pour plus d'informations, reportez-vous à la section “*Diffusion des logiciels*”, *104*.

Hôtes auto-enregistrés

Il est également possible d’importer les hôtes dans F-Secure Policy Manager Console en utilisant la fonction d’auto-enregistrement. Cette opération n’est réalisable qu’une fois F-Secure Management Agent installé sur les hôtes et après l’envoi d’une demande d’auto-enregistrement par les hôtes. F-Secure Management Agent devra être installé à partir d’un CD-ROM, d’un script de connexion ou d’une autre manière. Pour importer des hôtes auto-enregistrés, 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*”, *99*.

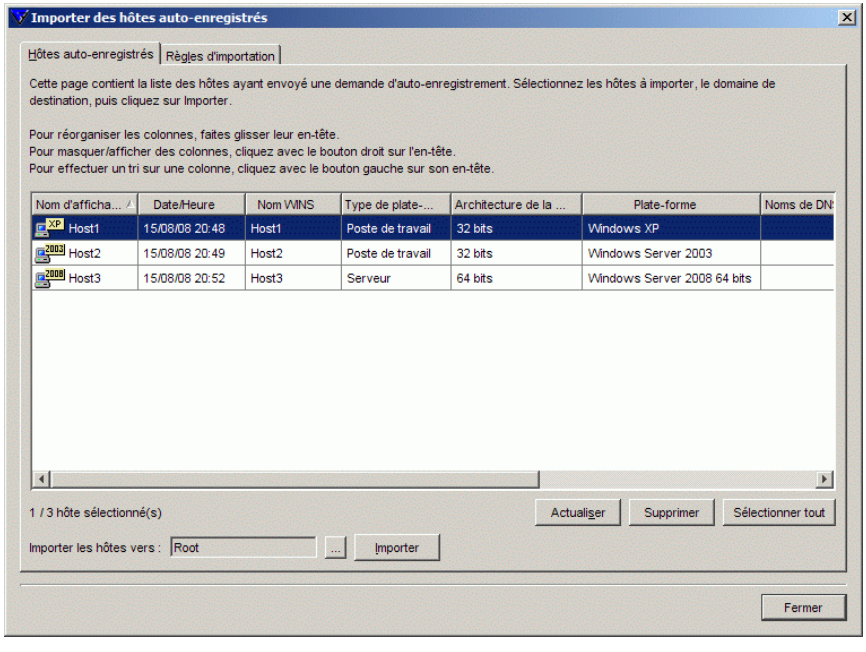


Figure 5-15 Boîte de dialogue Importer des hôtes auto-enregistrés > Onglet Hôtes auto-enregistrés

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 fichier JAR d'installation distante personnalisé”, 118*). 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. Il est

possible de modifier l'ordre des colonnes en les faisant glisser à l'emplacement souhaité. La largeur des colonnes peut également être modifiée. Le menu contextuel du tableau (cliquez avec le bouton droit de la souris sur la barre d'en-tête du tableau) peut être utilisé pour spécifier les propriétés d'auto-enregistrement à afficher dans le tableau.

Règles d'importation pour l'auto-enregistrement

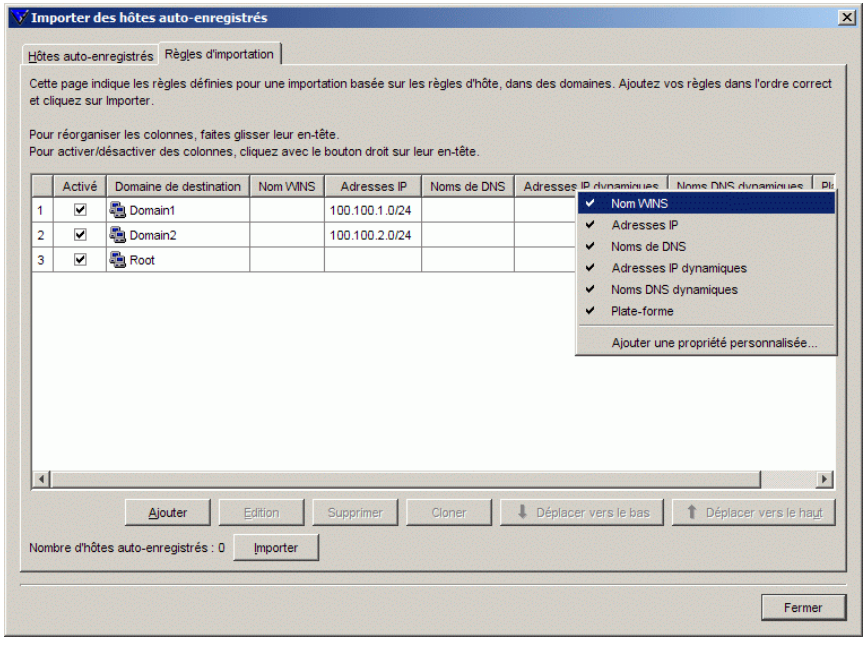


Figure 5-16 Boîte de dialogue Importer des hôtes auto-enregistrés > Onglet Règles d'importation

Vous pouvez définir les règles d'importation des hôtes auto-enregistrés à partir de l'onglet *Règles d'importation* dans la fenêtre *Importer des hôtes auto-enregistrés*. Les critères d'importation suivants peuvent être utilisés dans les règles :

- *Nom WINS, Nom DNS, Nom DNS dynamique, Propriétés personnalisées*
  - L'astérisque (*) peut être utilisé comme caractère générique. Il 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*
  - Ces critères prennent en charge la correspondance exacte

d’adresse IP (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 contenues dans les colonnes actuellement visibles sont utilisées comme critères de correspondance lors de l’importation des hôtes dans le domaine de stratégie. Les valeurs contenues dans les colonnes masquées sont ignorées.

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

Pour ajouter une nouvelle propriété personnalisée :

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. Saisissez le nom de la propriété personnalisée (par exemple, le nom du service). Cliquez ensuite sur **OK**.
3. La nouvelle propriété personnalisée apparaît dans le tableau. Elle peut désormais être utilisée comme critère d’importation dans de nouvelles règles d'importation d’auto-enregistrement.

Pour créer une nouvelle règle d’importation d’auto-enregistrement :

1. Cliquez sur **Ajouter** dans l’onglet *Règles d’importation*. La boîte de dialogue *Sélectionner le domaine de stratégie de destination pour la règle* contenant les domaines et sous-domaines existants s'affiche.
2. Sélectionnez le domaine pour lequel vous créez la règle et cliquez sur **OK**.

3. Vous pouvez désormais définir les critères d'importation. Sélectionnez la ligne que vous venez de créer, cliquez dans la cellule à renseigner, puis cliquez sur **Modifier**. Saisissez la valeur dans la cellule.

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

Si vous 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 désormais modifier les critères dans la ligne dupliquée.

Lorsque vous voulez débuter l'importation, sélectionnez l'onglet *Hôtes auto-enregistrés* et cliquez sur **Importer**. Les règles d'importation définies seront validées avant le début de l'importation. Une fois 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 ensemble de conditions vide est traité comme une correspondance absolue.

Création manuelle d'hôtes

Pour créer un hôte manuellement, choisissez un domaine de stratégie, puis sélectionnez l'option *Nouvel hôte* dans le menu *Edition* ou cliquez sur le bouton **Ajouter un hôte** (ou sur `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.

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.

Cas particuliers : vous pouvez générer des stratégies pour des hôtes qui n'ouvriront jamais directement le répertoire de communication (c'est-à-dire lorsqu'il est impossible d'importer l'hôte). Il est, par exemple, possible de générer des fichiers de stratégie de base pour un ordinateur

n'ayant pas accès à F-Secure Policy Manager Server. Le fichier de stratégie de base doit être transféré manuellement ou grâce à un autre mécanisme de transmission externe. Pour ce faire, choisissez la commande *Exporter le fichier de stratégie de l'hôte* du menu *Edition*.

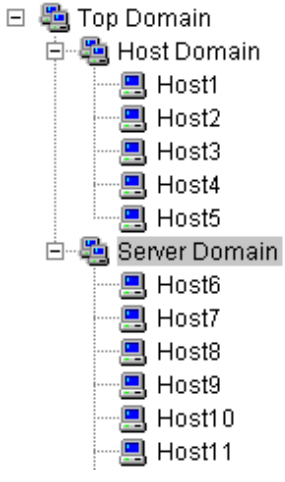


Figure 5-17 Exemple de domaine avec des hôtes et des serveurs dans leurs propres sous-domaines

Les hôtes sur lesquels F-Secure Management Agent n'est pas installé ne peuvent être administrés via F-Secure Policy Manager Console car ils n'ont aucun moyen de récupérer les stratégies. De plus, ils ne disposent d'aucune information d'état.
Toute modification apportée à la structure du domaine est implémentée, même si l'on quitte F-Secure Policy Manager Console sans enregistrer les modifications à la stratégie courante.

5.3.3 Propriétés d'hôte

Les noms d'hôte sur le réseau peuvent être des adresses IP, des noms de domaine ou des noms WINS. Pour afficher les propriétés d'un hôte, cliquez dessus à l'aide du bouton droit de la souris. Dans le menu qui s'affiche, cliquez sur *Propriétés*. Vous pouvez également employer la combinaison de touches `Alt + Entrée`). Pour modifier les propriétés des hôtes, désactivez la case à cocher *Mise à jour automatique des propriétés d'hôte* de l'onglet *Identités*, dans la boîte de dialogue *Propriétés d'hôte*. Vous pouvez ouvrir la boîte de dialogue *Propriétés d'hôte* en choisissant *Propriétés* dans le menu *Edition*, ou en cliquant sur  dans la barre d'outils.

Le nom réseau de l'hôte est le nom que celui-ci utilise en interne sur le réseau pour accéder aux stratégies.

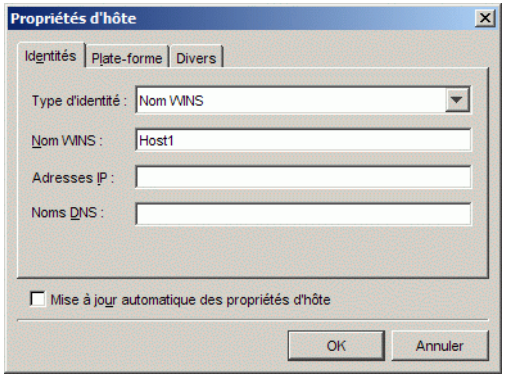


Figure 5-18 Boîte de dialogue Propriétés d'hôte

Chaque hôte possède un identifiant utilisateur (UID). Il s'agit d'un identifiant unique : une chaîne de caractères et de nombres utilisée pour identifier de façon unique chaque hôte du système.

Sous l'onglet *Plate-forme*, vous pouvez ajouter le système d'exploitation de l'hôte aux propriétés. Le *nom de plate-forme* désigne le nom du système d'exploitation. Les numéros de version des systèmes d'exploitation sont les suivants :

Windows 2000	5.0
Windows XP	5.1/5.10
Windows Vista	6.0

Vous pouvez définir un alias pour l'hôte sous l'onglet *Divers*. Si un alias est défini, celui-ci remplace l'identité réelle de l'hôte dans l'arborescence du domaine affichée à l'écran.

5.4 Diffusion des logiciels

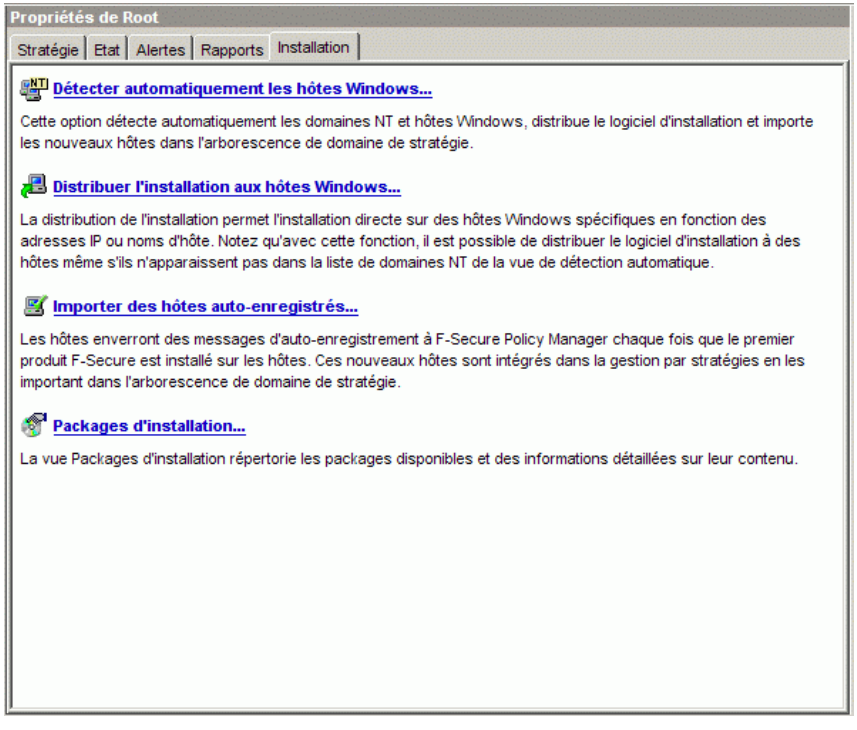
F-Secure Policy Manager propose plusieurs méthodes d'installation et de mise à jour des applications gérées :

- **Installations distantes** - F-Secure Policy Manager peut installer des logiciels sur de nouveaux hôtes qui ne sont pas encore administrés de manière centralisée. Les hôtes peuvent être recherchés à partir de domaines Windows à l'aide de la fonction *Autodécouvrir hôtes Windows*ou l'hôte cible peut être défini directement à l'aide de son nom WINS ou de son adresse IP via la fonction *Distribuer l'installation aux hôtes Windows*. Les fonctions d'installation à distance sont utiles pour les nouvelles installations, mais aussi pour mettre à jour ou réparer des installations si les procédures par stratégies ne conviennent pas.
- **Installations par stratégies** : F-Secure Policy Manager peut démarrer les opérations d'installation et de mise à jour à l'aide de stratégies. Pour ce faire, les hôtes doivent déjà être administrés de manière centralisée, c'est-à-dire qu'ils doivent figurer dans un domaine de stratégie de F-Secure Policy Manager Console.
- **Installations locales et mises à jour à partir du CD-ROM** : vous pouvez effectuer l'installation de manière indépendante sur l'hôte en l'exécutant directement à partir du CD-ROM. Une fois

l'installation terminée, F-Secure Management Agent envoie un message d'enregistrement à F-Secure Policy Manager. L'administrateur peut alors visualiser et accepter le nouvel hôte en sélectionnant la commande Importer les hôtes enregistrés automatiquement dans le menu Edition de F-Secure Policy Manager Console.

- **Installation et mises à jour locales à l'aide de fichiers préconfigurés** : au lieu d'utiliser le programme d'installation standard du CD-ROM, vous pouvez vous servir de F-Secure Policy Manager pour préparer un package d'installation personnalisé (JAR ou MSI) comportant les informations relatives aux paramètres définis pour l'installation. L'installation peut être réalisée de façon automatique sur l'ordinateur de l'utilisateur final car le fichier préconfiguré contient tous les paramètres habituellement demandés à l'utilisateur.
- **Mises à jour de base de données de définitions de virus F-Secure** - F-Secure Policy Manager peut mettre à jour les dernières bases de données antivirus en les téléchargeant automatiquement à partir du site de mise à jour automatique de F-Secure. Les hôtes administrés chargent les mises à jour depuis F-Secure Policy Manager en fonction de leur stratégie, en procédant automatiquement ou à l'aide d'actions déclenchées à distance. Pour plus d'informations, reportez-vous à la section "*Mises à jour automatiques avec l' Agent de mise à jour automatique F-Secure*", *151*.

Les raccourcis vers toutes les fonctions d'installation sont regroupés dans le volet Propriétés de l'onglet *Installation*.



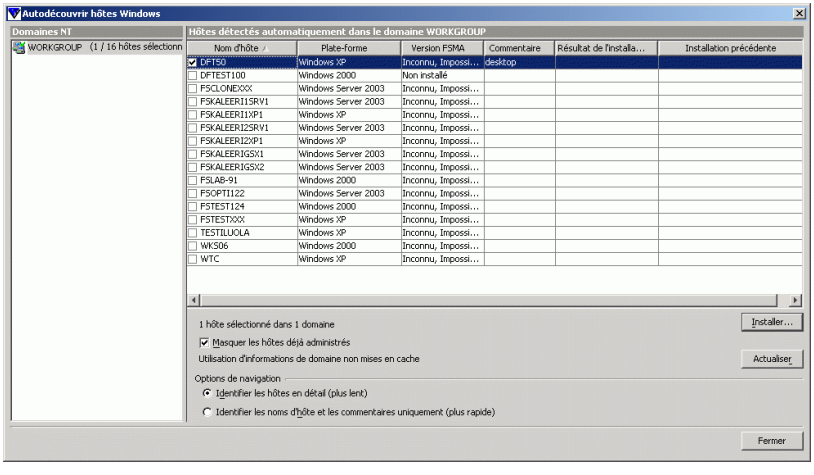
5.4.1 Installations distantes de F-Secure

La seule différence entre les fonctions *Autodécouvrir hôtes Windows* et *Distribuer l'installation aux hôtes Windows* réside dans la manière dont les hôtes de destination sont sélectionnés. La fonction de découverte automatique examine les domaines Windows, et l'utilisateur peut sélectionner les hôtes de destination dans une liste. La fonction *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.

Détecter automatiquement les hôtes Windows

Pour effectuer l'installation :

1. Sélectionnez le domaine de stratégie des hôtes sur lesquels vous allez installer F-Secure Management Agent.
2. Ouvrez le menu *Edition* et choisissez la commande *Autodécouvrir 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`).
   - *Activer tout* : active les cases à cocher de tous les hôtes du domaine Windows sélectionné.
   - *Désactiver tout* : désactive les cases à cocher de tous les hôtes du domaine Windows sélectionné.

   Cliquez sur **Installer** pour continuer.

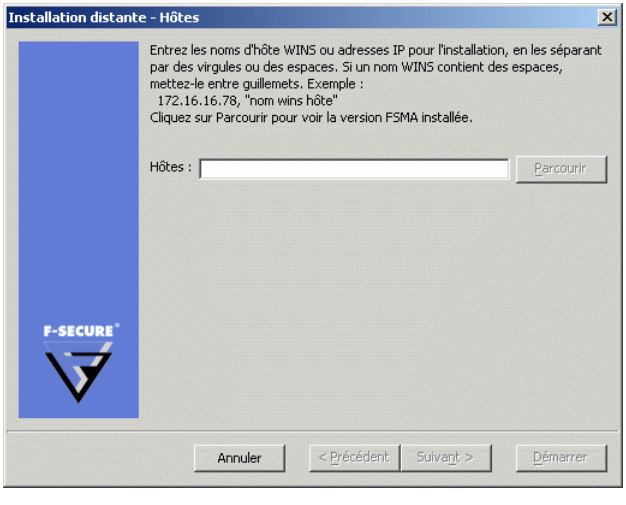
5. Une fois les hôtes de destination sélectionnés, passez à la section “*Installation distante après sélection de l’hôte de destination*”*, 110*, où vous trouverez des instructions sur l'installation à distance des applications sur les hôtes.

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 Management Agent.
2. Ouvrez le menu *Edition* et choisissez *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.

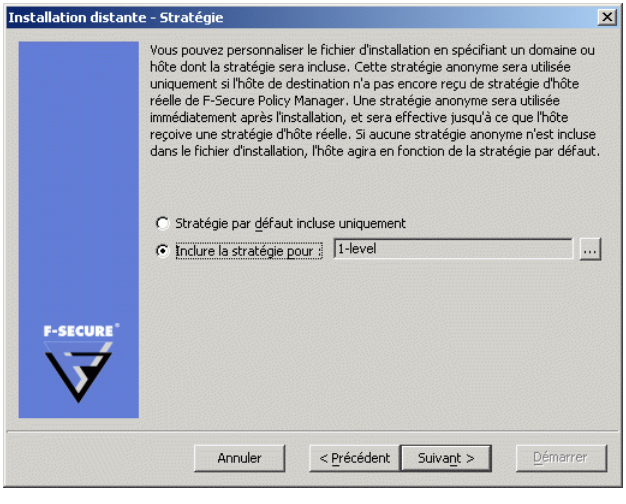


4. Une fois les hôtes de destination sélectionnés, passez à la section “*Installation distante après sélection de l’hôte de destination*”*, 110*, où vous trouverez des instructions sur l'installation à distance des applications sur les hôtes.

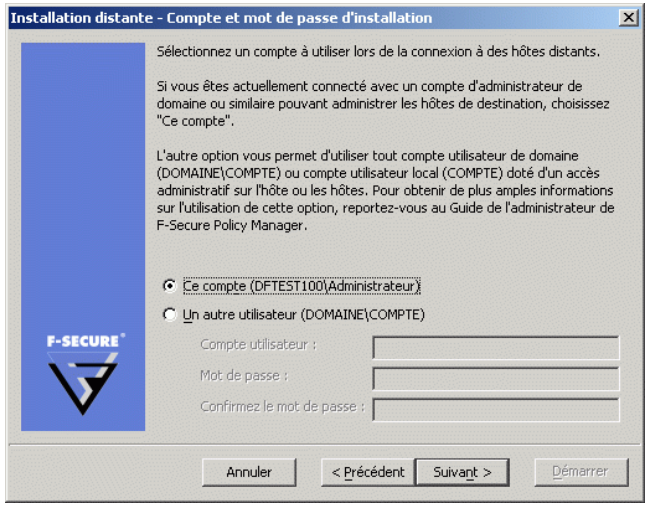
Installation distante après sélection de l’hôte de destination

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, interrompez les connexions actives avant de lancer l'installation distante.

5. Prenez connaissance du résumé 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 ligne *Etat* indique *terminé*, 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'enregistrement automatique qui permettront de les importer.

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*.

If the installation fails, see "Codes d'erreur de l'installation distante avec FSII", 216 for explanations to most common error situations.

5.4.2 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 depuis 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. Les résultats de la désinstallation ne seront pas signalés.

Utilisation de l'éditeur d'installation

L’éditeur d’installation doit être utilisé sur les hôtes sur lesquels F-Secure Management Agent est installé. 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.

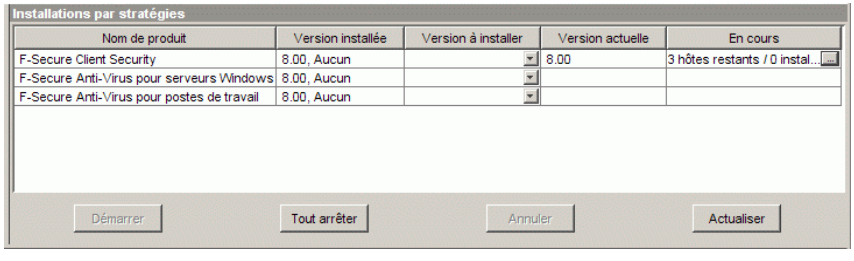


Figure 5-19 Editeur d'installation

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

Nom du 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.
Progression	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.

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.

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.

5.4.3 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.

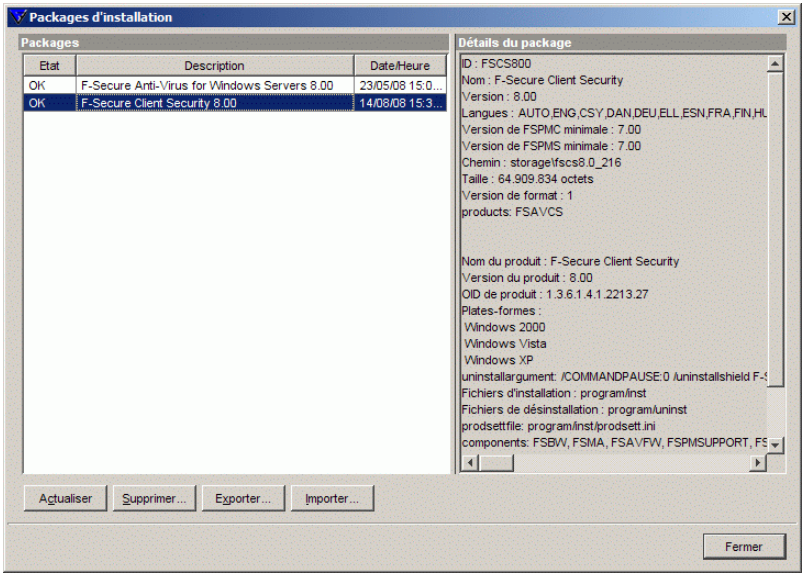
La procédure d'exportation dans les deux formats est la même (voir ci-dessous). Vous pouvez sélectionner le format de fichier pour le package personnalisé dans la boîte de dialogue *Exporter le package d'installation* (voir l'étape 4, ci-dessous).

Script de connexion sur les plates-formes Windows

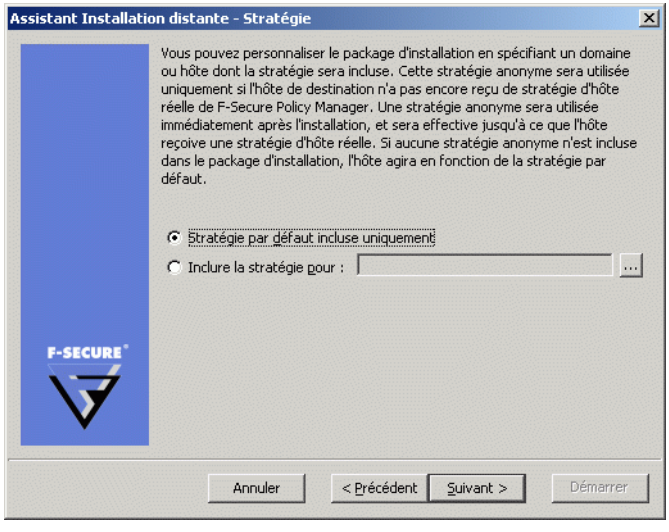
L’authentification peut s’effectuer de deux manières différentes : à l'aide d'un fichier d'installation distante personnalisé ou à l'aide d'un fichier MSI personnalisé.

Utilisation du fichier 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. Spécifiez le format de fichier, *JAR* ou *MSI*, et l'emplacement où vous souhaitez enregistrer le package d'installation personnalisé. Cliquez sur **Exporter**.
4. Indiquez l'emplacement où vous souhaitez enregistrer le package d'installation JAR personnalisé. Cliquez sur **Enregistrer**.
5. Sélectionnez les composants à installer. 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. 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.
8. Une page récapitulative présente les options choisies pour l'installation. Prenez-en connaissance, puis cliquez sur **Démarrer** pour accéder à l'Assistant d'installation.

   F-Secure Policy Manager Console affiche l'Assistant d'installation distante qui collecte toutes les informations d'installation nécessaires pour les produits sélectionnés. 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 (reportez-vous à la section “*Hôtes auto-enregistrés*”, *96*). 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.

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

9. 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. Termine 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. Reportez-vous à l'***Annexe B.*** *Codes d'erreur d'Ilaunchr* pour obtenir la liste des codes d'erreur de fin d'installation, ainsi qu'un exemple pouvant être utilisé dans les fichiers de commandes.

5.4.4 Transmission des informations

Toutes les informations d'installation sont fournies sous forme de fichiers via le F-Secure Policy Manager Server. Les packages d'installation consistent en des archives JAR que vous pouvez visualiser (avec WinZip, par exemple), tandis que les autres types de fichiers, comme les fichiers de stratégie et les fichiers INI, permettent de lancer le processus d'installation proprement dit.

Transmission des packages d'installation vers F-Secure Policy Manager Server

Avant que F-Secure Policy Manager Console puisse commencer l'installation, le package d'installation initial doit être transféré vers F-Secure Policy Manager Server. Les packages d'installation sont disponibles auprès de deux sources :

- le CD-ROM d'installation ;
- le site Web de F-Secure.

Normalement, les nouveaux packages d'installation distante sont installés à partir du CD-ROM, et le programme d'installation de F-Secure Policy Manager les déplace automatiquement sur le serveur. Si un package d'installation distante est obtenu d'une autre manière, vous pouvez l'importer en cliquant sur le bouton **Importer** de la vue Packages

d'installation, ou utiliser à cette fin la boîte de dialogue Packages d'installation. Alternativement, le package d'installation peut être copié manuellement vers le sous-répertoire */Install/Entry* du répertoire server.

F-Secure Policy Manager Console vérifie que le nouveau package d'installation est signé avec la clé privée de F-Secure Corporation avant d'en autoriser l'utilisation.

5.5 Gestion des stratégies

Cette section décrit la façon de configurer et distribuer les stratégies.

5.5.1 Paramètres

Pour configurer les paramètres d'une stratégie, parcourez l'arborescence de celle-ci et modifiez les valeurs des variables de stratégie.

Il existe deux types de variables de stratégie : (1) les nœuds non terminaux dépendant d'une arborescence et (2) les cellules de tableau. Toutes les variables de stratégie sont associées à un type. Vous pouvez définir leurs valeurs dans le volet Affichage produit. Le type d'une variable de stratégie peut être l'un des suivants :

- Entier : nombre entier normal
- Chaîne d'affichage : chaîne de texte ASCII 7 bits
- Adresse IP : adresse IP sur quatre octets
- Compteur : entier incrémenté
- Indicateur : entier non bouclé
- Cycles d'horloge : unités de temps écoulées (mesurées en centièmes de seconde)
- Chaîne d'octets : données binaires (ce type est également utilisé dans les chaînes de texte UNICODE)
- OID : identificateur unique
- Opaque : données binaires qui peuvent représenter d'autres types de données

La valeur d'une variable de stratégie peut être prédéfinie. Les valeurs par défaut agissent comme si elles étaient héritées du domaine racine supérieur. Elles apparaissent ainsi comme des valeurs héritées même si le domaine supérieur (racine) est sélectionné. Les valeurs par défaut peuvent être remplacées comme n'importe quelles autres valeurs.

Les valeurs correspondant au domaine de stratégie sélectionné font l'objet d'un codage couleur :

- Noir : valeurs modifiées au niveau du domaine de stratégie ou de l'hôte sélectionné.
- Gris : valeurs héritées.
- Rouge : valeurs incorrectes.
- Rouge atténué : valeurs héritées incorrectes.

5.5.2 Restrictions

On distingue deux types de restrictions : les restrictions d'**accès** et les restrictions de **valeurs**.

Les restrictions d'accès sont *Final* et *Masqué*. 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*. Le type *Masqué* cache simplement la valeur à l'utilisateur final. Contrairement à la restriction de type *Final*, une restriction de type *Masqué* n'est pas forcément prise en compte par l'application administrée.

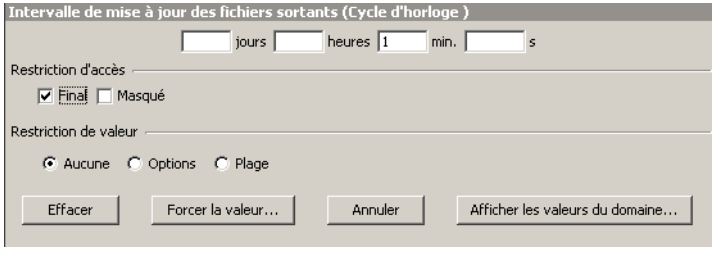


Figure 5-20 Editeur de restriction intégré

A l'aide des restrictions de valeurs, un administrateur peut limiter les valeurs d'une variable de stratégie à une liste de valeurs acceptables dans laquelle l'utilisateur peut faire son choix. Il a également la possibilité de restreindre les variables de type entier (Entier, Compteur et Indicateur) à une plage de valeurs acceptables. Une restriction supplémentaire, la restriction de type TAILLE FIXE, peut être appliquée aux tables. Grâce à cette restriction, l'utilisateur final n'est pas en mesure d'ajouter ou de supprimer des lignes dans des tables de taille fixe. Comme la restriction *Final* ne peut pas être utilisée pour une table vide, la restriction TAILLE FIXE doit être employée à cette fin (afin d'empêcher les utilisateurs finals de modifier les valeurs de la table).

Si une variable de la base de données MIB du produit contient déjà une définition de plage ou de choix, l'administrateur peut restreindre celle-ci davantage, mais pas l'étendre. Si aucune restriction de valeurs n'est définie, l'administrateur peut spécifier n'importe quelle restriction de plage ou de choix.

Les restrictions peuvent être modifiées dans le volet Affichage produit ou dans une boîte de dialogue séparée. Pour passer d'une possibilité à l'autre, sélectionnez *Editeurs de restriction intégrés* dans le menu *Affichage*. Si les éditeurs intégrés sont désactivés, le volet Affichage produit affiche les boutons de lancement des éditeurs de dialogue.

5.5.3 Enregistrement des données de stratégie actuelles

Les données de stratégie constituent une base de données qui contient des informations de stratégies pour chaque domaine de stratégie et chaque hôte.

Pour enregistrer les données de stratégie, choisissez la commande *Enregistrer* ou *Enregistrer sous* du menu *Fichier*. Il est conseillé d'opter pour *Enregistrer sous*, qui permet d'enregistrer les données de stratégie sous un nouveau nom. Vous pouvez ainsi réutiliser une ancienne configuration de stratégie si nécessaire.

5.5.4 Distribution des fichiers de stratégie

Une fois la configuration des domaines et des hôtes terminée, vous devez diffuser celle-ci sur les hôtes. Pour ce faire, cliquez sur  dans la barre d'outils ou choisissez *Distribuer* dans le menu *Fichier*. Vous pouvez également utiliser la combinaison de touches CTRL + D. F-Secure Policy Manager Console enregistre les données de stratégies en cours et génère des fichiers de stratégie de base à partir des données de stratégie enregistrées. Les fichiers de stratégie sont copiés dans le répertoire de communication, où ils sont récupérés à intervalles réguliers par le logiciel F-Secure des hôtes.

Aucune modification n'est prise en compte tant que la stratégie n'a pas été distribuée et que l'hôte n'a pas récupéré le fichier correspondant. Cela vaut également pour les opérations car elles sont implémentées à l'aide d'un mécanisme par stratégie.

5.5.5 Transmission des stratégies

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. Tout paramètre remplacé peut être de nouveau hérité à l'aide de l'opération *Effacer*. Le paramètre étant supprimé dans l'hôte ou le domaine de stratégie actuellement sélectionné, il est remplacé par le paramètre du domaine parent.

La transmission des stratégies simplifie la définition d'une stratégie commune. 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.

La combinaison de ces stratégies permet de tirer le meilleur parti des deux méthodes. Certains produits peuvent hériter leurs stratégies de domaines étendus, tandis que d'autres produits peuvent hériter leurs stratégies de sous-domaines, voire disposer de stratégies propres aux hôtes.

Si les modifications de stratégies sont déployées à plusieurs niveaux de la hiérarchie du domaine de stratégie, le suivi des modifications peut devenir complexe. Une méthode pratique consiste à employer la fonction *Afficher les valeurs du domaine* pour voir quelles modifications ont été apportées à un paramètre de stratégie précis.

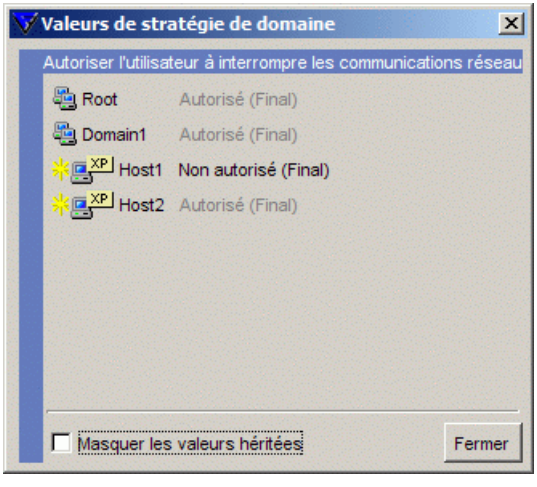


Figure 5-21 Boîte de dialogue Afficher les valeurs du domaine

S'il est nécessaire de rétablir les valeurs actuelles du domaine pour le sous-domaine ou l'hôte, vous pouvez utiliser l'opération Forcer la valeur afin d'écraser les valeurs du sous-domaine et de l'hôte en question.

Vous pouvez également utiliser l'outil de transmission de rapports, qui montre les endroits où les paramètres hérités ont été remplacés. Pour plus d'informations, reportez-vous à la section “Outil de transmission de rapports”, 133.

Héritage des index des tables

Lorsque vous effacez une ligne d'une table à l'aide du bouton **Effacer une ligne**, le contenu de la ligne sélectionnée est effacé. Le résultat de cette opération dépend des types de lignes par défaut définis dans les domaines parents et dans la base de données MIB.

- S'il existe une ligne qui possède les mêmes valeurs d'index que la ligne effacée, elle sera de nouveau héritée.
- S'il n'existe pas de ligne possédant les mêmes valeurs d'index que la ligne effacée, cette dernière restera vide après l'emploi de la fonction **Effacer une ligne**.

La ligne peut être héritée d'un domaine parent ou, en tant que ligne par défaut, d'une base MIB (définition des paramètres et contenant les valeurs par défaut pour tous les paramètres). La base de données MIB peut être considérée comme un « domaine au-dessus du domaine racine » en matière d'héritage des valeurs de nœuds non terminaux ou des lignes. Les valeurs par défaut de la base de données MIB sont transmises aux sous-domaines, sauf si elles sont supplantées au niveau du domaine. Pour écraser une ligne héritée, définissez une ligne possédant les mêmes valeurs de colonne d'index. Les valeurs par défaut de la base de données MIB sont obtenues en fonction de la version du produit installée sur les hôtes. Pour un domaine, les valeurs provenant de la version la plus récente du produit sont utilisées.

Certains produits F-Secure écrasent le déploiement des tables par défaut, si bien qu'ils n'utilisent pas le mode normal d'héritage de tables décrit ci-dessus.

Par exemple, les tables suivantes utilisent leur propre mécanisme sans héritage de base :

- Tableau des règles de protection Internet F-Secure
- Tableau des services de protection Internet F-Secure
- Tableau des niveaux de sécurité de protection Internet F-Secure

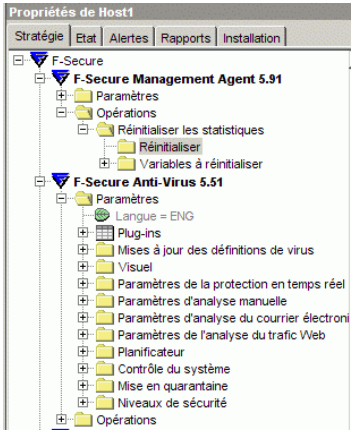
Reportez-vous à la documentation du produit concerné pour obtenir plus d'informations sur le comportement des tables dans de tels cas.

Les lignes héritées et dérivées localement se distinguent par leur couleur : les lignes héritées sont de couleur grise et les lignes dérivées localement de couleur noire.

5.6 Gestion des opérations et des tâches

Pour lancer une opération à partir de F-Secure Policy Manager Console :

1. Sélectionnez l'une des actions dans la branche *Opérations* du produit sélectionné, sous l'onglet *Stratégie* du volet *Propriétés*.



2. Cliquez sur **Démarrer** dans le volet Affichage produit pour lancer l'opération sélectionnée.
3. L'opération est lancée sur l'hôte dès que vous avez diffusé la nouvelle stratégie et que l'hôte a récupéré le fichier de stratégie. Vous pouvez cliquer à tout moment sur **Annuler** pour interrompre l'opération.

5.7 Alertes

Cette section décrit la façon d'afficher les alertes et les rapports et de configurer la transmission d'alertes.

5.7.1 Affichage des alertes et des rapports

Les hôtes peuvent émettre des alertes et des rapports en cas de problème avec un programme ou une opération. Lorsqu'une alerte est reçue, le bouton  s'allume. Pour afficher les alertes, cliquez sur  . L'onglet *Alertes* du volet *Propriétés* 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, le bouton **Accep.** est 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 produit donne des informations détaillées sur celle-ci. Les alertes d'analyse de F-Secure Anti-Virus peuvent également avoir un rapport attaché. Ce rapport s'affiche lui aussi dans le volet Affichage produit.

Pour afficher les rapports, cliquez sur l'onglet *Rapports* du volet Propriétés, ou choisissez *Messages* dans le volet Affichage produit. La structure de l'onglet *Rapports* est identique à celle de l'onglet *Alertes*.

Vous pouvez trier les tables Alertes et Rapports en cliquant sur l'en-tête de la colonne correspondante.

5.7.2 Configuration de la transmission des alertes

Vous pouvez configurer des alertes en modifiant la table Transmission des alertes, situé dans *F-Secure Management Agent>Paramètres>Alertes>Transmission des alertes*.

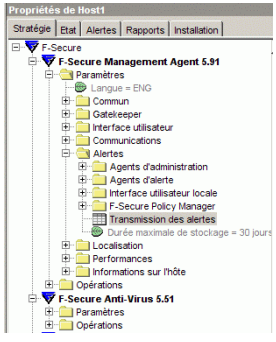


Figure 5-22 F-Secure Management Agent>Paramètres>Transmission des alertes

La même table se trouve dans la vue produit de F-Secure Management Agent, sous l'onglet *Transmission des alertes*.

Vous pouvez spécifier la destination des alertes en fonction de leur niveau de gravité. Il peut s'agir de F-Secure Policy Manager Console, de l'interface utilisateur locale, d'un agent d'alerte (comme l'Observateur d'événements NT, un fichier journal ou SMTP) ou d'une extension d'administration.

La table Transmission des alertes dispose de son propre jeu de valeurs par défaut.

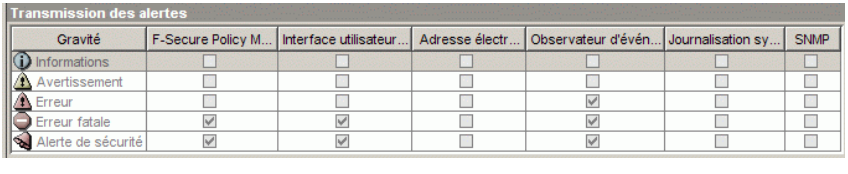


Figure 5-23 Table Transmission des alertes

Par défaut, les alertes d'information et d'avertissement ne sont ni envoyées à F-Secure Policy Manager Console ni affichées sur l'interface utilisateur. Ces alertes et notifications de faible priorité peuvent fournir des informations très utiles pour la résolution des problèmes ; toutefois, lorsqu'elles sont activées, le nombre des alertes émises augmente de façon substantielle. Si la structure de votre domaine est très étendue, la

définition de règles strictes de transfert d'alertes au niveau du domaine racine peut entraîner un afflux massif d'alertes vers F-Secure Policy Manager Console.

Il est possible de paramétrer davantage la destination des alertes en définissant les variables de stratégie dans les zones spécifiques de cette cible. Par exemple « Paramètres->Alertes->F-Secure Policy Manager Console->Intervalle avant nouvelle tentative d'envoi » permet de spécifier la fréquence à laquelle un hôte tentera d'envoyer des alertes vers F-Secure Policy Manager Console si les précédentes tentatives ont échoué.

5.8 Outil de transmission de rapports

L'outil de transmission de rapports permet aux utilisateurs d'afficher et d'exporter des rapports sur les données gérées par F-Secure Policy Manager Console. Les fonctions de visualisation et d'exportation sont un moyen efficace d'examiner simultanément les données de plusieurs hôtes/domaines.

Pour démarrer l'outil de transmission de rapports, dans le menu *Outils*, sélectionnez *Transmission de rapports…* . L'outil de transmission des rapports peut également être lancé à partir du menu contextuel du volet *Domaine de stratégie* de F-Secure Policy Manager Console.

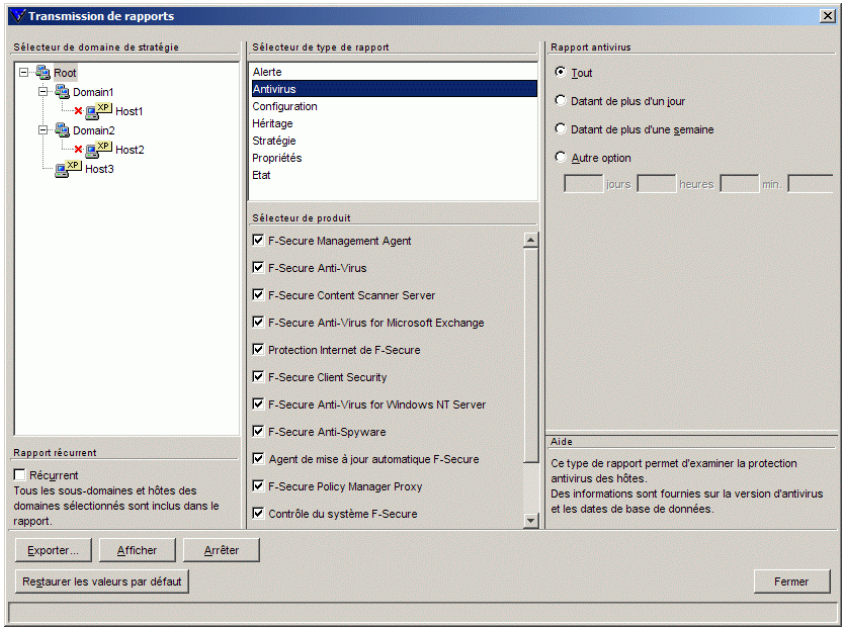


Figure 5-24 Outil de transmission de rapports

5.8.1 Volet Sélecteur de domaine de stratégie / d'hôte

Dans le volet Sélecteur de domaine de stratégie / d'hôte, vous pouvez sélectionner les domaines et/ou les hôtes dont les rapports vous intéressent. Le domaine sélectionné dans le volet Domaine de stratégie l'est par défaut dans l'outil de transmission de rapports.

Si vous activez la case à cocher *Récurrent* , tous les hôtes qui sont placés, de façon récurrente, sous les domaines sélectionnés de la hiérarchie de domaines sont également inclus dans le rapport.

5.8.2 Volet Sélecteur de type de rapport

Sous le volet Sélecteur de type de rapport, vous pouvez effectuer les opérations suivantes :

- sélectionner le type de rapport à établir ;
- sélectionner le filtrage par produits (seules les informations relatives aux produits sélectionnés sont incluses dans le rapport à établir).

Les types de rapports suivants sont actuellement disponibles :

Rapport de stratégie	Ce type de rapport vous permet d'exporter/de visualiser les rapports contenant les valeurs de toutes les variables de stratégie des produits sélectionnés dans les domaines sélectionnés. Vous pouvez également cocher la case Transmission afin d'inclure les informations de transmission au rapport.
Rapport de transmission	Ce type de rapport vous permet d'exporter/de visualiser les rapports contenant les valeurs de toutes les variables de stratégie des produits sélectionnés dans les domaines et qui ne sont pas héritées d'un domaine supérieur, c'est-à-dire toutes les variables de stratégie remplacées dans les domaines sélectionnés.
Rapport d'état	Ce type de rapport vous permet d'exporter/de visualiser les rapports contenant les valeurs de toutes les variables locales de paramètres et d'état des produits sélectionnés dans les domaines.

Rapport de propriétés	Ce type de rapport vous permet d'exporter/de visualiser les rapports contenant les valeurs de tous les champs de propriétés des composants de domaine. Vous pouvez également utiliser les cases à cocher *Sélecteur de propriétés* pour indiquer les champs de propriétés que vous souhaitez inclure dans le rapport à établir.
Rapport d'alertes	Ce type de rapport vous permet d'exporter/de visualiser les rapports contenant les informations relatives à toutes les alertes des domaines. Vous pouvez également trier les alertes à l'aide de l'option Sélecteur d'ordre de tri en définissant l'ordre des champs de description d'alertes. Sélecteur de gravité permet de sélectionner les alertes de gravité à inclure dans le rapport à établir.
Rapport de configuration	Ce type de rapport vous permet d'exporter et de visualiser les rapports contenant les informations relatives aux produits installés parmi les produits sélectionnés dans les domaines.
Rapport d'antivirus	Ce type de rapport permet d'exporter et de visualiser les rapports contenant les valeurs de l'état du domaine des versions des produits et des mises à jour des bases de données des définitions de virus.

5.8.3 Volet Rapport

Le volet Rapports permet d'effectuer les opérations suivantes :

- Sélectionner des configurations en fonction du type du rapport actuellement sélectionné. Grâce à ces configurations, l'utilisateur peut mieux adapter le filtrage en fonction du rapport à établir ;
- Recherche de la description du type de rapport actuellement sélectionné.

Les configurations des types de rapports actuellement disponibles sont les suivantes :

- Les configurations correspondant aux rapports de stratégie vous permettent de sélectionner les informations relatives aux valeurs de stratégie que vous souhaitez inclure dans le rapport à établir.
- Les configurations correspondant aux rapports de propriétés vous permettent de sélectionner, parmi les propriétés d'identités, de plates-formes et les propriétés diverses et d'interrogation, les informations que vous souhaitez inclure dans le rapport à établir.
- Les configurations correspondant aux rapports d'alertes vous permettent de trier les alertes par champs de description d'alerte et de sélectionner par gravité les alertes que vous souhaitez inclure dans le rapport à établir.

5.8.4 Volet inférieur

Le volet inférieur vous permet d'effectuer les opérations suivantes :

- réinitialisation de tous les paramètres par défaut des composants de l'interface utilisateur ;
- démarrage du processus d'exportation de rapports ;
- démarrage du processus de visualisation de rapports ;
- arrêt du processus de génération de rapports ;
- fermeture de l'interface utilisateur de l'outil Transmission de rapports. Cela ne met pas fin à la génération d'un rapport ; ce dernier est exécuté en arrière-plan. Vous pouvez mettre fin à la génération du rapport à l'aide de la boîte de dialogue qui s'affiche.

Visualisation du rapport

Cliquez sur **Afficher** dans le volet inférieur pour générer un rapport du type sélectionné et employant les configurations choisies. Vous pouvez ensuite visualiser ce rapport au format HTML à l'aide de votre navigateur Web par défaut. Si aucun navigateur n'est défini, une boîte de dialogue s'affiche et vous invite à en définir un.

Exportation du rapport

Cliquez sur **Exporter** dans le volet inférieur pour générer un rapport du type sélectionné et employant les configurations choisies. Vous pouvez définir le chemin d'accès du fichier et le format du rapport à établir à l'aide de la boîte de dialogue *Enregistrer le fichier* qui s'affiche. Le rapport est alors exporté vers le fichier sélectionné au format choisi.

5.9 Préférences

Les paramètres de préférences sont soit partagés, soit appliqués à une connexion donnée.

5.9.1 Préférences spécifiques à une connexion

Pour modifier ces préférences, choisissez la commande *Préférences* du menu *Outils*. Seule la connexion actuelle est affectée.

Onglet	Paramètre	Signification
Communication	Intervalles d'interrogation	Intervalles d'interrogation de différents types de fichiers. Vous pouvez sélectionner ou désélectionner les cases afin d'activer ou de désactiver la récupération d'un type de fichier donné. Cochez la case Désactiver toutes les interrogations, si vous souhaitez toujours utiliser les opérations d'actualisation manuelle au lieu de l'interrogation automatique.
	Etat de connexion de l'hôte	Permet de définir le moment auquel les hôtes sont considérés comme déconnectés de F-Secure Policy Manager. Tous les hôtes qui n'ont pas contacté Policy Manager Server dans l'intervalle indiqué sont considérés comme déconnectés. Les hôtes déconnectés sont signalés par une icône de notification dans l'arborescence, et ils sont placés dans la liste Hôtes déconnectés de la vue Etat du domaine. Les icônes de notification de l'arborescence des domaines peuvent être désactivées dans **Aspect > Options du domaine de stratégie**. Notez qu'il est possible de définir un intervalle de moins d'un jour en entrant un nombre à décimales dans la zone de saisie. Par exemple, si vous entrez une valeur de « 0,5 », tous les hôtes qui n'ont pas contacté le serveur dans les 12 heures sont considérés comme déconnectés. Les valeurs inférieures à un jour ne servent normalement qu'à des fins de dépannage. Dans un environnement traditionnel, certains hôtes sont naturellement déconnectés du serveur de temps à autre. Par exemple, il se peut qu'un ordinateur portable soit incapable d'accéder quotidiennement au serveur, mais dans la plupart des cas, ce comportement est tout à fait acceptable.

	Options des alertes et des rapports	Ces options : ■ contrôlent la suppression automatique des alertes et des rapports anciens ■ le chargement en arrière-plan des alertes et des rapports
Options de communication avancées	Cache d'état	Vous pouvez définir le nombre d'hôtes pour lesquels F-Secure Policy Manager Console met en caches les informations d'état.
	Désactivation du chargement de l'état initial	Vous pouvez désactiver le chargement de l'état initial si vous voulez réduire le temps nécessaire au démarrage de F-Secure Policy Manager Console dans un environnement de grande taille. Il s'agit d'une option avancée qui doit être utilisée avec prudence, car elle provoque les différences fonctionnelles suivantes par rapport au traitement normal des états : 1. Aucun logiciel ne semble installé sur les hôtes. Cette modification influe sur le volet Propriétés et sur l'Editeur d'installation. 2. Les éléments d'état ne sont pas disponibles dans un premier temps. Cette modification influe sur le volet Propriétés et sur les affichages Produit quand l'onglet Etat est sélectionné. 3. Tous les hôtes reçoivent des stratégies générées à partir de la version la plus récente de la base de données MIB, car les informations de version de cette dernière ne sont pas disponibles. La désactivation de l'option de chargement de l'état initial n'influe pas sur l'actualisation d'état manuelle ni sur la recherche d'état périodique. Si nécessaire, vous pouvez désactiver la recherche d'état automatique. Pour ce faire, ouvrez le menu *Outils* et sélectionnez l'option *Préférences.* Sélectionnez l'onglet *Communications* et cliquez sur **Options d'intervalle d'interrogation**. Activez la case à cocher *Désactiver toutes les interrogations*.

Fichiers de stratégie	Optimisations de fichiers de stratégie	**Retrait** détermine si des caractères de séparation seront ajoutés au fichier lors de sa création, ce qui facilite sa lecture par un opérateur. Si vous *désactivez la mise en retrait*, aucun caractère de séparation n'est ajouté aux fichiers. Ceux-ci sont moins lisibles pour un opérateur, mais ils restent tout à fait corrects et peuvent toujours être lus par un ordinateur. Les séparateurs peuvent être des espaces ou des tabulations. Il est conseillé d'employer des tabulations, le fichier produit étant de taille plus réduite qu'en cas d'emploi d'espaces. **Inclure des commentaires** a une incidence sur la taille des fichiers de stratégie produits par F-Secure Policy Manager Console. Ces commentaires servent à rendre le fichier plus compréhensible par l'utilisateur s'il veut directement lire les valeurs dans le fichier. Ces paramètres ne sont employés qu'à des fins de débogage et doivent être désactivés pour une utilisation normale en environnement de production.
	Numéro de série du fichier de stratégie	Numéro de série des fichiers de stratégie de base générés. Le numéro de série s'incrémente automatiquement. Normalement, il n'est pas nécessaire de l'ajuster manuellement. Vous avez uniquement besoin d'augmenter cette valeur si des hôtes n'acceptent pas des fichiers de stratégie à cause de numéros de série trop petits (qu'ils signalent comme des erreurs). Dans ce cas, vous devez augmenter le numéro de série de façon à ce qu'il soit supérieur au numéro de série du dernier fichier de stratégie de base récupéré par les hôtes.
Installation distante	Délai d'installation	Délai maximal pendant lequel F-Secure Policy Manager Console attend les résultats d'une opération d'installation.

	Délai de navigation	Ce paramètre est important uniquement si l'option *Masquer les hôtes déjà administrés* est activée. Il s'agit de la durée maximale accordée pour accéder au Registre de l'hôte.
	Nombre maximal d'opérations réseau simultanées	Vous pouvez régler le nombre d'opérations sur le réseau. Il est conseillé de conserver la valeur par défaut, mais si vous employez une connexion réseau lente qui pose des problèmes lors d'installations distantes, diminuez le nombre de connexions réseau simultanées en conséquence.
	Indicateur d'avancement	Vous pouvez choisir si l'indicateur d'avancement doit être affiché pour l'utilisateur final au cours d'une installation distante.

5.9.2 Préférences partagées

Elles s’appliquent à toutes les connexions définies dans une installation spécifique de F-Secure Policy Manager Console.

Onglet	Paramètre	Signification
Aspect -> Options générales	Langue	Il s'agit du choix de la langue. Vous pouvez sélectionner la langue utilisée par votre système d'exploitation ou le paramètre Anglais par défaut. Tous les objets ne prenant pas en charge la langue utilisée par votre système d'exploitation seront affichés en anglais. Vous devez redémarrer F-Secure Policy Manager Console pour que les modifications soient appliquées.
Aspect -> Domaines de stratégie	Surbrillance des hôtes déconnectés	Vous pouvez mettre en surbrillance les hôtes déconnectés dans l'arborescence d'un domaine de stratégie.
	Police	Police utilisée dans F-Secure Policy Manager Console. Le changement de police entre en vigueur après le redémarrage du programme.
	Style	Définit l'aspect et le comportement des composants de l'interface utilisateur. La modification entre en vigueur après le redémarrage du programme.

Fichiers de stratégie	Produits	Permet de désactiver des MIB pour des produits que vous n'avez pas installés, et de les exclure des fichiers de stratégie distribués. La désactivation des MIB réduit la taille des fichiers de stratégie envoyés aux hôtes administrés. **AVERTISSEMENT : Ne désactivez les MIB que si vous êtes invité à le faire par F-Secure. Leur désactivation pour des produits qui sont installés sur certains hôtes administrés entraînera un dysfonctionnement du système.**
Installation distante	Effacer le cache	Pour libérer de l'espace sur le disque, vous pouvez effacer toutes les informations placées en mémoire cache et relatives aux hôtes examinés et aux logiciels installés.
Emplacement	Région de Web Club	Permet de choisir votre emplacement afin de vous connecter au serveur Web de F-Secure le plus proche.
	Chemin du navigateur HTML	Il s'agit du chemin d'accès complet du fichier exécutable du navigateur HTML. Utilisez le navigateur pour visualiser les pages d'aide en ligne, les pages Web Club et les rapports relatifs aux virus.
	Chemin des journaux de messages	Entrez un chemin vers un répertoire où seront créés les fichiers journaux pour chaque onglet de la vue Messages. Chaque fichier journal contient le titre de l'onglet correspondant et un message par ligne comprenant sa gravité et l'heure de création.
	Enregistrer les messages	Permet d'activer ou de désactiver l'enregistrement de messages. Nous vous recommandons vivement de conserver la consignation, car les informations du journal peuvent s'avérer très utiles pour le dépannage.
Antivirus	Définitions de virus	Cette valeur vous permet de définir le moment où les définitions de virus sont considérées comme obsolètes en mode antivirus.

6 MAINTENANCE DE F-SECURE POLICY MANAGER SERVER

6.1 Présentation

F-Secure Policy Manager Server peut être géré en sauvegardant et en restaurant souvent les données de console du serveur.

6.2 Sauvegarde et restauration des données de F-Secure Policy Manager Console

Nous vous recommandons vivement de sauvegarder régulièrement les informations d'administration les plus importantes. Au minimum, sauvegardez l'ensemble du répertoire *fsa\domains* du répertoire de communication. Normalement, le répertoire de communication se trouve dans le répertoire d'installation de F-Secure Policy Manager Server sous*commdir*\. Ce répertoire contient la structure du domaine de stratégie, ainsi que toutes les données de stratégie enregistrées.

Avant de sauvegarder le répertoire fsa\domains, assurez-vous qu'aucune session F-Secure Policy Manager Console n'est ouverte.

Il est également possible de sauvegarder tout le référentiel. Cela vous permet de récupérer non seulement la structure du domaine de stratégie mais aussi les alertes, les statistiques des hôtes et les opérations d'installation. Vous pouvez également récupérer rapidement les fichiers de stratégie. Lorsque vous ne sauvegardez que le sous-répertoire *fsa\domains* , vous devez distribuer les stratégies par la suite. La sauvegarde de la totalité du référentiel présente l'inconvénient que ce dernier peut contenir dix fois plus de données que le répertoire *fsa\domains*. L'autre inconvénient est que F-Secure Policy Manager Server doit être arrêté avant de réaliser la sauvegarde complète.

Pour sauvegarder le jeu de clés d'administration, copiez les fichiers *admin.prv* et *admin.pub* qui se trouve à la racine du répertoire d'installation local de F-Secure Policy Manager Console. Stockez le fichier *admin.prv* dans un emplacement sûr. Il est très important d'enregistrer une copie de sauvegarde du fichier de clés *admin.prv* .

Si vous perdez une clé d'administration (admin.pub ou admin.prv), vous devrez créer une nouvelle paire et distribuer la clé admin.pub respective sur tous les hôtes administrés en réinstallant chacun d'eux manuellement, les opérations par stratégie n'étant plus utilisables. La confiance entre F-Secure Policy Manager Console et les hotes gérés est fondée sur une signature numérique. Sans clé privée valide, il n'est pas possible de créer une signature valable que les hôtes acceptent.

Si vous souhaitez enregistrer les préférences F-Secure Policy Manager Console, sauvegardez le fichier *lib\Administrator.properties* du répertoire d'installation local.

Le fichier « Administrator.properties » est créé lors de la première exécution de F-Secure Policy Manager Console et contient des informations associées à la session, telles que la taille de la fenêtre ou l'URL du serveur.

Création de la sauvegarde

Vous avez le choix entre deux méthodes de création de la sauvegarde :

- Sauvegarde complète : la sauvegarde complète inclut la restauration de la structure des domaines de stratégie, les alertes, les statistiques des hôtes et les opérations d'installation.
- Sauvegarde des données de stratégie et de la structure de domaine : sauvegarde du répertoire *fsa\domains* du référentiel de Policy Manager Server (Commdir).

Sauvegarde complète

1. Fermez toutes les sessions de gestion de F-Secure Policy Manager Console.
2. Arrêtez le service F-Secure Policy Manager Server.

3. Sauvegardez le répertoire de communication.
4. Sauvegardez les fichiers *admin.prv* et *admin.pub* placés à la racine du répertoire d'installation local de F-Secure Policy Manager Console.
5. Sauvegardez le fichier *lib\Administrator.properties* dans le répertoire d'installation de F-Secure Policy Manager Console.
6. Redémarrez le service F-Secure Policy Manager Server.
7. Ouvrez à nouveau les sessions de gestion de F-Secure Policy Manager Console.

Sauvegarde des données de stratégie et de la structure de domaine

1. Fermez toutes les sessions de gestion de F-Secure Policy Manager Console.
2. Sauvegardez le répertoire *fsa\domains* et enregistrez la copie de sauvegarde en lieu sûr.
3. Ouvrez à nouveau les sessions de gestion de F-Secure Policy Manager Console.

Restauration de la sauvegarde

Si vous avez sauvegardé tout le contenu du répertoire de communication et les informations de console, comme les clés et les préférences (sauvegarde complète), procédez comme suit pour les restaurer :

1. Fermez toutes les sessions de gestion de F-Secure Policy Manager Console et arrêtez le service F-Secure Policy Manager Server.
2. Supprimez le répertoire de communication.
3. Copiez la sauvegarde du répertoire de communication à son emplacement correct.
4. Copiez le fichier *admin.pub* à la racine du répertoire d'installation de la console.
5. Copiez le fichier *admin.prv* à la racine du répertoire d'installation de la console.
6. Copiez les préférences de la console (*Administrator.properties*) dans le <répertoire d'installation de la console>`\lib`.

7. Redémarrez le service F-Secure Policy Manager Server.
8. Ouvrez à nouveau les sessions de gestion de F-Secure Policy Manager Console.
9. Distribuez des stratégies.
10. Si vous n'avez sauvegardé que la structure du domaine de stratégie (sauvegarde des données de stratégie et de la structure de domaine), procédez comme suit pour la restaurer :
11. Fermez toutes les sessions de gestion de F-Secure Policy Manager Console et arrêtez le service F-Secure Policy Manager Server.
12. Supprimez le contenu du <répertoire de communication>*fsa**domains*.
13. Copiez les données sauvegardées dans le répertoire indiqué ci-dessus.
14. Redémarrez le service F-Secure Policy Manager Server.
15. Ouvrez à nouveau toutes les sessions de gestion de F-Secure Policy Manager Console.
16. Distribuez des stratégies.

6.3 Duplication de logiciels à l'aide de fichiers image

F-Secure Anti-Virus peut être inclus lors de la duplication de logiciels à l'aide de fichiers image de disque. Cependant, chaque installation d'un produit comprend un code d'identification unique (ID unique) utilisé par F-Secure Policy Manager. Si vous employez une image de disque pour installer des logiciels sur de nouveaux ordinateurs, il se peut que plusieurs ordinateurs tentent d'utiliser le même ID unique. Cette situation peut contrarier le bon fonctionnement de F-Secure Policy Manager.

Procédez comme suit pour vous assurer que chaque ordinateur emploiera un ID unique personnalisé, même en cas d'emploi d'images de disque.

1. Installez le système et tous les logiciels à inclure dans le fichier image, avec entre autres F-Secure Anti-Virus. Configurez F-Secure Anti-Virus afin d'utiliser le composant F-Secure Policy Manager Server approprié. Cependant, n'importez **pas** l'hôte dans F-Secure

Policy Manager Console, si l'hôte a envoyé une demande d'auto-enregistrement à F-Secure Policy Manager Server. Vous ne devez importer que les hôtes sur lesquels le fichier image sera installé.

2. Exécutez la commande *fsmautil resetuid* à partir de l'invite de commande. Cet utilitaire se trouve généralement dans le répertoire *C:\Program Files\F-Secure\Common*. Ce répertoire peut être différent si vous employez une version localisée de Windows ou si vous avez choisi un chemin d'installation différent du chemin par défaut.
3. Arrêtez l'ordinateur. Ne redémarrez **pas** encore l'ordinateur.
4. Créez le fichier d'image de disque.
5. L'utilitaire réinitialise l'ID unique dans l'installation de F-Secure Anti-Virus. Un nouvel ID unique est créé automatiquement lors du redémarrage du système. L'opération s'effectue individuellement sur chaque ordinateur où le fichier image est installé. Ces ordinateurs enverront des demandes d'auto-enregistrement à F-Secure Policy Manager et les demandes seront traitées normalement.

7 MISE À JOUR DES BASES DE DONNÉES DE DÉFINITION DE VIRUS

7.1 Mises à jour automatiques avec l' Agent de mise à jour automatique F-Secure

Avec l'Agent de mise à jour automatique F-Secure, vous pouvez recevoir des mises à jour automatiques et des informations sans interrompre votre travail pour attendre le téléchargement des fichiers à partir du Web. L'Agent de mise à jour automatique F-Secure télécharge automatiquement les fichiers en tâche de fond en utilisant la bande passante non utilisée par d'autres applications Internet, afin que les utilisateurs puissent toujours être sûrs d'avoir les 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 automatiques dans les deux heures qui suivent leur publication par F-Secure. Les éventuels retards dépendent de la disponibilité de la connexion à Internet.

L'Agent de mise à jour automatique F-Secure est utilisé pour mettre à jour les produits F-Secure gérés indépendamment ou de manière centralisée. Par défaut, l'agent télécharge aussi les informations sur les virus. Vous pouvez désactiver ce téléchargement, si vous le souhaitez. Vous pouvez installer et utiliser l'Agent de mise à jour automatique F-Secure avec des produits de sécurité F-Secure Anti-Virus.

Fonctionnement

Lorsque l'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. Les nouvelles données sont automatiquement téléchargées. L'intervalle de récupération est défini par le serveur et ne peut être ajusté à partir du client.

Dans F-Secure Policy Manager 6.0 et versions ultérieures, l'agent de mise à jour automatique installé avec F-Secure 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.

Avantages de l'Agent de mise à jour automatique F-Secure

Téléchargements optimisés des mises à jour de définitions de virus

L'Agent de mise à jour automatique F-Secure détecte la date à laquelle la base de données des définitions de virus a été modifiée. Il s'appuie sur des algorithmes de quelques octets pour télécharger uniquement les modifications et non pas l'ensemble des fichiers ou de la base de données. Les modifications ne représentent généralement qu'une petite fraction de la mise à jour complète, ce qui permet aux utilisateurs distants disposant de modems lents d'obtenir aisément les mises à jour

quotidiennes. Cela permet également aux utilisateurs disposant d'une liaison permanente d'économiser une part non négligeable de la bande passante.

Possibilité de reprendre un transfert de données interrompu

L'Agent de mise à jour automatique F-Secure télécharge le contenu lors de plusieurs sessions. Si le téléchargement est interrompu, l'Agent de mise à jour automatique F-Secure enregistre ce qui a été téléchargé et poursuit le téléchargement des fichiers restants lors de la connexion suivante.

Mises à jour automatisées

Vous n'avez pas à rechercher les dernières mises à jour et à les télécharger manuellement. Avec l'Agent de mise à jour automatique F-Secure, vous obtenez automatiquement les mises à jour des définitions de virus dès qu'elles sont publiées par F-Secure.

7.2 Utilisation de l'agent de mise à jour automatique

Avec F-Secure Policy Manager 7.0 et versions ultérieures, l'Agent de mise à jour automatique F-Secure installé avec F-Secure Policy Manager est configuré en modifiant le fichier de configuration *fsaua.cfg*. Pour plus d'informations, reportez-vous à la section "*Configuration*" ci-dessous.

Vous pouvez vérifier que l'application fonctionne correctement en vous reportant au fichier journal. Pour plus d'informations, reportez-vous à la section "*Lire le fichier journal*", *155*.

7.2.1 Configuration

IMPORTANT : *Ces instructions de configuration s'appliquent uniquement à l'Agent de mise à jour automatique F-Secure installé avec F-Secure Policy Manager Server. Vous ne devez modifier que les paramètres mentionnées ci-dessous. Ne modifiez pas les autres paramètres dans le fichier de configuration.*

Etape 1. Pour configurer l'Agent de mise à jour automatique F-Secure, ouvrez le fichier de configuration *fsaua.cfg* situé dans

C:\Program Files\F-Secure\FSAUA\program\fsaua.cfg

Etape 2. Spécifiez les Proxies HTTP

La directive `http_proxies` contrôle les proxies HTTP utilisés par l'Agent de mise à jour automatique F-Secure.

Utilisez le format suivant :

```
http_proxies=[http://
][[domain\]user[:passwd]@]<address>[:port][,[http://
][[domain\]user[:passwd]@]<address>[:port]]
```

Exemples :

```
http_proxies=http://proxy1:8080/,http://backup_proxy:8880/,http://
domain\username:usernamespassword@ntlmproxy.domain.com:80
```

Etape 3. Spécifiez l'intervalle d'interrogation

La directive `poll_interval` spécifie la fréquence à laquelle l'Agent de mise à jour automatique F-Secure recherche de nouvelles mises à jour. Le paramètre par défaut est de 3600 secondes, soit 1 heure.

```
poll_interval=3600
```

Si l'intervalle d'interrogation minimum défini sur le serveur de mise à jour F-Secure est de 2 heures par exemple, les paramètres du fichier de configuration de l'Agent de mise à jour automatique F-Secure ne peuvent pas écraser cette limite.

Etape 4. Enregistrez le fichier et fermez-le.

Etape 5. Vous devez arrêter le service fsaua et le redémarrer pour que les modifications soient prises en compte. Pour ce faire, saisissez les commandes suivantes sur la ligne de commande :

```
net stop fsaua
net start fsaua
```

7.2.2 Lire le fichier journal

Le fichier *fsaua.log* est utilisé pour stocker les messages générés par l'Agent de mise à jour automatique F-Secure. Certains des messages fournissent des informations sur les opérations normales, tels que le démarrage et la fermeture. D'autres messages indiquent des erreurs.

Le fichier *fsaua.log* est situé dans
C:\Program Files\F-Secure\FSAUA\program

Lecture du journal

Chaque message du journal comporte les informations suivantes :

- La date et l'heure du message ont été générées.

  ```
  [ 3988]Thu Oct 26 12:40:39 2006(3): Downloaded
  'F-Secure Anti-Virus Update 2006-10-26_04' -
  'DFUpdates' version '1161851933' from
  fsbwserver.f-secure.com, 12445450 bytes (download
  size 3853577)
  ```

- Explication rapide de ce qui s'est passé. Lorsqu'une mise à jour est téléchargée, le nom et la version de la mise à jour sont indiqués.

  ```
  [ 3988]Thu Oct 26 12:40:39 2006(3): Downloaded
  'F-Secure Anti-Virus Update 2006-10-26_04' -
  'DFUpdates' version '1161851933' from
  fsbwserver.f-secure.com, 12445450 bytes (download
  size 3853577)
  ```

- Pour les mises à jour, le message indique également la source de la mise à jour et la taille du téléchargement.

  ```
  [ 3988]Thu Oct 26 12:40:39 2006(3): Downloaded
  'F-Secure Anti-Virus Update 2006-10-26_04' -
  'DFUpdates' version '1161851933' from
  fsbwserver.f-secure.com, 12445450 bytes (download
  size 3853577)
  ```

Messages dans fsaua.log

Des exemples de messages apparaissant dans le fichier journal sont présentés ci-dessous.

Message	Signification
`Update check completed successfully`	La connexion à la source des mises à jour a réussi.
`Update check completed successfully. No updates are available.`	La connexion à la source des mises à jour a réussi, mais il n'y avait rien à télécharger.
`Downloaded 'F-Secure Anti-Virus Update 2006-10-26_04' - 'DFUpdates' version '1161851933' from fsbwserver.f-secure.com, 12445450 bytes (download size 3853577)`	La connexion a réussi et des fichiers ont été téléchargés. Pour une liste des types de mises à jour apparaissant dans le journal, reportez-vous à "*Quelles sont les mises à jour consignées dans fsaua.log ?*", *157*.
`Installation of 'F-Secure Anti-Virus Update 2006-10-26_04' : Success`	Les fichiers ont été correctement placés dans le répertoire de destination (et les fichiers existants ont été supprimés). Ce résultat est celui de la mise à jour du répertoire de communication. Notez que l'Agent de mise à jour automatique F-Secure ne peut pas indiquer si les nouveaux fichiers ont été utilisés par les hôtes ou non.
`Update check failed. There was an error connecting fsbwserver.f-secure.com (DNS lookup failure)`	Message d'erreur indiquant que la vérification des mises à jour a échoué. Pour plus d'informations sur les erreurs les plus courantes et pour obtenir des instructions sur la résolution des problèmes, reportez-vous à "*Dépannage*", *160*.

Quelles sont les mises à jour consignées dans fsaua.log ?

Vous trouverez ci-dessous une liste de mises à jour disponibles dans le journal :

- 'F-Secure Anti-Virus Update 2006-10-24_01' - 'DFUpdates'
- 'F-Secure Spam Control Update 2006-10-19_02' - 'SCDB3'
- 'F-Secure Anti Spyware Update 2006-10-18_07' - 'SWCDB'
- 'F-Secure News Update 2006-10-20_01' - 'VirusNews'
- 'F-Secure Anti-Virus AVP Extended Update 2006-10-20_05' - 'avpe'
- 'F-Secure Anti-Virus Libra Update 2006-10-24_04' - 'libradb'
- 'F-Secure Anti-Virus Orion Update 2006-10-02_07' - 'oriondb'
- 'F-Secure Anti-Virus Misc Update 2006-10-09_03' - 'avmisc'
- 'F-Secure Housekeeper Update 2006-10-09_03' - 'hke-freebsd'
- 'F-Secure Housekeeper Update 2006-10-09_03' - 'hke-linux'
- 'F-Secure IDS Update 2006-10-09_03' - 'idsdb'
- 'F-Secure Hydra Update 2006-10-09_03' - 'hydrawin'
- 'F-Secure Hydra Update 2006-10-09_03' - 'hydralinux'
- 'F-Secure Universal System scanner update 2006-10-09_03' - 'mlcwin'
- 'F-Secure BlackLight Engine Update 2006-09-15_01' - 'BLENG'
- 'F-Secure Gemini Update 2006-09-05_04' - 'gemdb'
- 'F-Secure HIPS Update 2006-09-01_04' - 'hipscfg'
- 'F-Secure Pegasus Update 2006-09-29_03' - 'pegdb'

Comment vérifier que tout fonctionne à partir du journal ?

Quand tout fonctionne normalement, le résultat de la dernière installation pour chaque mise à jour téléchargée doit être indiqué comme « `Success` » (Réussie). Par exemple :

```
Installation of 'F-Secure Anti-Virus Update
2006-10-26_04' : Success
```

Vous pouvez également voir un résumé des statuts de mises à jour du contrôle du système, des logiciels espions et virus sur le server sous l'onglet *Résumé* dans F-Secure Policy Manager Console.

Pour vérifier le statut de la mise à jour sur un hôte géré de façon centralisée, allez à la page *Etat* > *Protection globale* dans F-Secure Policy Manager Console.

7.3 Activation forcée de l'agent de mise à jour automatique pour vérifier immédiatement les nouvelles mises à jour

Si vous devez forcer l'activation de l'Agent de mise à jour automatique F-Secure pour rechercher immédiatement de nouvelles mises à jour, vous devez arrêter et redémarrer le service fsaua. Pour ce faire, saisissez les commandes suivantes sur la ligne de commande :

```
net stop fsaua
net start fsaua
```

Ceci poussera l'Agent de mise à jour automatique F-Secure à se connecter au serveur de mise à jour et à rechercher de nouvelles mises à jour.

7.4 Mise à jour manuelle des bases de données

Si votre ordinateur n’est pas connecté à Internet, vous pouvez mettre à jour manuellement les bases de données.

1. Connectez-vous à http://support.f-secure.com/ à partir d'u autre ordinateur.
2. Téléchargez l'outil *fsdbupdate3.exe*.
3. Transférez l'outil *fsdbupdate3.exe* sur votre ordinateur, par exemple, en utilisant une carte mémoire ou tout autre support amovible.

7.5 Dépannage

Vous trouverez ci-dessous des exemples de problèmes qui peuvent être consignés comme messages d'erreur dans le fichier *fsaua.log*.

Problème :	**Un échec de consultation DNS a eu lieu ou la connexion a échoué, a été perdue ou refusée.**
Raison :	Problèmes de réseau
Solution :	Vérifiez que le réseau est correctement configuré.

Problème :	**Échec de l'authentification du proxy.**
Raison :	Le mot de passe saisi pour le proxy HTTP est incorrect.
Solution :	Vérifiez le mot de passe du proxy HTTP dans la directive `http_proxies` du fichier fsaua.cfg. Pour plus d'informations, reportez-vous à la section "*Configuration*", *153*.

Problème :	**Le disque est plein ou une erreur d'E/S s'est produite.**
Raison :	Il n'y a pas assez d'espace disque libre sur le lecteur sur lequel le répertoire de destination est situé.
Solution :	Libérez de l'espace disque afin que la mise à jour puisse s'effectuer.

Problème : **Une erreur serveur ou une erreur non spécifiée a eu lieu.**

Raison : Inconnu

Solution : -

8 F-Secure Policy Manager sous Linux

8.1 Présentation

F-Secure Policy Manager peut également être installé sous Linux.

8.1.1 Différences entre Windows et Linux

Lorsque F-Secure Policy Manager Console fonctionne sous Linux, les services suivants ne sont pas disponibles :

- Fonction d'installation en mode « push »
- Exportation d'un package Windows Installer (MSI)
- Détection automatique de postes de travail sur le réseau

8.1.2 Distributions prises en charge

F-Secure Policy Manager prend en charge un grand nombre de distributions Linux basées sur le système DEB (Debian package management) et sur le système RPM (Redhat Package Management). Les commandes sont différentes entre ces deux systèmes.

Distribution prise en charge	Package
Red Hat Enterprise Linux 5	RPM
Red Hat Enterprise Linux 4	RPM
Red Hat Enterprise Linux 3	RPM
SUSE Linux Enterprise Server 10	RPM
SUSE Linux Enterprise Server 9	RPM
SUSE Linux Enterprise Desktop 10	RPM
openSUSE 10.3	RPM
Debian GNU Linux Etch 4.0	DEB
Ubuntu 8.04 Hardy	DEB

8.2 Installation

L'installation de F-Secure Policy Manager comprend quatre composants. Il est important de respecter l'ordre suivant :

1. Agent de mise à jour automatique F-Secure
2. F-Secure Policy Manager Server
3. F-Secure Policy Manager Console
4. F-Secure Policy Manager Web Reporting.

F-Secure Policy Manager Server, F-Secure Policy Manager Web Reporting et l'Agent de mise à jour automatique F-Secure doivent être tous deux installés sur le même ordinateur. Ce peut être sous Windows ou sous Linux.

F-Secure Policy Manager Console peut être installé sur le même ordinateur ou sur un ordinateur différent. Ce peut être sous Windows ou sous Linux.

8.2.1 Installation de l'Agent de mise à jour automatique F-Secure

1. Connectez-vous en tant que `root`.
2. Ouvrez un terminal.
3. Pour effectuer l'installation, saisissez :

Distributions Debian	Distributions RPM
`dpkg -i f-secure-automatic-update-agent_<numéro_version>.<numéro_build>_i386.deb`	`rpm -i f-secure-automatic-update-agent-<numéro_version>.<numéro_build>-1.i386.rpm`

4. Pour procéder à la configuration, saisissez

   `/opt/f-secure/fsaua/bin/fsaua-config`

   et répondez aux questions. Appuyez sur ENTRÉE pour choisir le paramètre par défaut (indiqué entre crochets).

5. Si vous souhaitez configurer l'Agent de mise à jour automatique F-Secure pour utiliser les proxy HTTP, saisissez les adresses proxy HTTP lorsque le script de configuration les demande. Utilisez le format suivant :

   `http://[user:passwd@]address[:port]/[,proxy2[,proxyN]]`

6. Si vous souhaitez indiquer la fréquence selon laquelle l'Agent de mise à jour automatique F-Secure recherche de nouvelles mises à jour, saisissez un nouvel intervalle d'interrogation lorsque le script de configuration le demande. La valeur par défaut est de 3 600 secondes, soit 1 heure.

Si l'intervalle d'interrogation minimum défini sur le serveur de mise à jour F-Secure est de 2 heures par exemple, les paramètres du fichier de configuration de l'Agent de mise à jour automatique F-Secure ne peuvent pas écraser cette limite.

Une fois le script de configuration terminé, l'Agent de mise à jour automatique F-Secure est maintenant opérationnel et se lancera automatiquement à chaque redémarrage de l'ordinateur.

8.2.2 Installation de F-Secure Policy Manager Server

1. Connectez-vous en tant que `root`.
2. Ouvrez un terminal.
3. Pour effectuer l'installation, saisissez :

Distributions Debian	Distributions RPM
`dpkg -i f-secure-policy-manager-server_<numéro_version>.<numéro_build>_i386.deb`	`rpm -i f-secure-policy-manager-server-<numéro_version>.<numéro_révision>-1.i386.rpm`

4. Pour procéder à la configuration, saisissez :

   `/opt/f-secure/fspms/bin/fspms-config`

   et répondez aux questions.

Pour chacune des questions, appuyez sur ENTRÉE pour choisir le paramètre par défaut (indiqué entre crochets).

F-Secure Policy Manager Server est maintenant opérationnel et se lancera automatiquement à chaque redémarrage de l'ordinateur.

8.2.3 Installation de F-Secure Policy Manager Console

1. Connectez-vous en tant que `root`.
2. Ouvrez un terminal.
3. Pour effectuer l'installation, saisissez :

Distributions Debian	Distributions RPM
`dpkg -i f-secure-policy-manager-console_<numéro_version>.<numéro_build>_i386.deb`	`rpm -i f-secure-policy-manager-console-<numéro_version>.<numéro_révision>-1.i386.rpm`

Un nouveau groupe d'utilisateurs `fspmc` est créé automatiquement. Pour pouvoir exécuter F-Secure Policy Manager Console, les utilisateurs doivent être ajoutés au groupe d'utilisateurs `fspmc` :

4. Vérifiez les groupes dont l'utilisateur fait partie :

   `groups <id utilisateur>`

   Par exemple, si l'utilisateur s'appelle `Tom`, on obtient :

   `groups Tom`

5. Ajoutez cet utilisateur au groupe `fspmc` :

   `/usr/sbin/usermod -G fspmc<, les groupes dont l'utilisateur fait actuellement partie (en les séparant par des virgules)> <id utilisateur>`

Par exemple, si Tom fait partie des groupes `normal_users` et `administrators` la commande sera la suivante :

```
/usr/sbin/usermod -G fspmc,normal_users,administrators
Tom
```

La liste des groupes, séparés par des virgules, remplace les groupes dont l'utilisateur faisait partie auparavant.

6. Fermez la session.
7. Ouvrez une nouvelle session.
8. Pour démarrer, saisissez :

   ```
   /opt/f-secure/fspmc/fspmc
   ```

   La première fois que vous saisissez cette commande, vous devez répondre à quelques questions afin de terminer la configuration. Ces questions sont les mêmes que pour la version pour Windows (reportez-vous à la section "*Procédure d'installation*", *54*).

8.2.4 Installation de F-Secure Policy Manager Web Reporting

1. Connectez-vous en tant que `root`.
2. Ouvrez un terminal.
3. Pour effectuer l'installation, saisissez :

Distributions Debian	Distributions RPM
`dpkg -i f-secure-policy-manager-web-reporting_<numéro_version<.<numéro_build>_i386.deb`	`rpm -i f-secure-policy-manager-web-reporting-<numéro_version<.<numéro_build>-1.i386.rpm`

4. Pour procéder à la configuration, saisissez :

   ```
   /opt/f-secure/fspmwr/bin/fspmwr-config
   ```

   et répondez aux questions.

   Pour chacune des questions, appuyez sur ENTRÉE pour choisir le paramètre par défaut (indiqué entre crochets).

5. Pour démarrer, saisissez :

   ```
   /etc/init.d/fspmwr start
   ```

8.3 Configuration

Les composants de F-Secure Policy Manager possèdent des scripts de configuration distincts. Pour configurer chaque composant, saisissez la commande de configuration correspondante et répondez aux questions.

F-Secure Policy Manager Composant	Commande de configuration
F-Secure Policy Manager Server	/opt/f-secure/fspms/bin/fspms-config
F-Secure Policy Manager Web Reporting	/opt/f-secure/fspmwr/bin/fspmwr-config

8.4 Désinstallation

Désinstallez les quatre composants en respectant l'ordre suivant :

1. F-Secure Policy Manager Web Reporting
2. F-Secure Policy Manager Console
3. F-Secure Policy Manager Server
4. Agent de mise à jour automatique F-Secure.

8.4.1 Désinstallation de F-Secure Policy Manager Web Reporting

1. Connectez-vous en tant que `root`.
2. Ouvrez un terminal.

3. Saisissez la commande suivante :

Distributions Debian	Distributions RPM
`dpkg -r f-secure-policy-manager-web-reporting`	`rpm -e f-secure-policy-manager-web-reporting`

Les fichiers journaux et de configuration ne sont pas supprimés car ils sont irremplaçables et contiennent des informations précieuses. Pour les supprimer, saisissez les commandes suivantes :

```
rm -rf /opt/f-secure/fspmwr
```

8.4.2 Désinstallation de F-Secure Policy Manager Console

1. Connectez-vous en tant que `root`.
1. Ouvrez un terminal.
2. Saisissez la commande suivante :

Distributions Debian	Distributions RPM
`dpkg -r f-secure-policy-manager-console`	`rpm -e f-secure-policy-manager-console`

Les fichiers journaux et de configuration ne sont pas supprimés car ils sont irremplaçables et contiennent des informations précieuses. Pour les supprimer, saisissez les commandes suivantes :

```
rm -rf /opt/f-secure/fspmc
```

8.4.3 Désinstallation de F-Secure Policy Manager Server

1. Connectez-vous en tant que `root`.
2. Ouvrez un terminal.

3. Saisissez la commande suivante :

Distributions Debian	Distributions RPM
`dpkg -r f-secure-policy-manager-server`	`rpm -e f-secure-policy-manager-server`

Les fichiers journaux et de configuration ne sont pas supprimés car ils sont irremplaçables et contiennent des informations utiles. Pour les supprimer, saisissez les commandes suivantes :

```
rm -rf /var/opt/f-secure/fsaus
rm -rf /var/opt/f-secure/fspms
rm -rf /etc/opt/f-secure/fspms
rm -rf /etc/opt/f-secure/fsaus
```

8.4.4 Désinstallation de l'Agent de mise à jour automatique F-Secure

1. Connectez-vous en tant que `root`.
2. Ouvrez un terminal.
3. Saisissez la commande suivante :

   ```
   # /opt/f-secure/fsaua/fsaua-config uninstall
   ```
4. Saisissez la commande suivante :

Distributions Debian	Distributions RPM
`dpkg -r f-secure-automatic-update-agent`	`rpm -e f-secure-automatic-update-agent`

8.5 Questions fréquentes

Q. F-Secure Policy Manager Console ne démarre pas. Pourquoi ?

R. Les erreurs d'exécution et les avertissements sont consignés dans le fichier suivant :

```
/opt/f-secure/fspmc/lib/Administrator.error.log
```

Q. F-Secure Policy Manager Server ne démarre pas. Pourquoi ?

R. Les erreurs d'exécution, les avertissements et autres informations sont consignés dans le fichier suivant :

```
/opt/f-secure/fspms/logs/error_log
/opt/f-secure/fsaus/log/fsaus/log/log
/opt/f-secure/fsaus/log/fsaus/log/fsaus_watchdog_log
```

Ce problème est souvent dû au fait qu'un serveur utilise déjà le(s) port(s) 80 et/ou 8080. Pour vérifier cette information, procédez comme suit :

a. Connectez-vous en tant que `root`.

b. Saisissez la commande suivante :

```
netstat -t -p
```

ou

```
fuser -vn tcp 80 8080
```

Q. Comment procéder pour mettre à jour manuellement la base de données de définitions de virus ?

R. Exécutez l'outil de mise à jour en saisissant la commande suivante :

```
sudo -u fspms /opt/f-secure/fspms/bin/fsavupd
```

Q. Pourquoi F-Secure Policy Manager Server ne diffuse-t-il pas de nouvelles bases de données de définitions de virus ? F-Secure Policy Manager Server et l'Agent de mise à jour automatique F-Secure fonctionnent pourtant correctement.

R. Pour obtenir des informations sur les erreurs de communication possibles entre F-Secure Policy Manager Server et l'Agent de mise à jour automatique F-Secure, saisissez la commande suivante :

```
sudo -u fspms /opt/f-secure/fspms/bin/fsavupd --debug
```

Q. Dans la version pour Linux, où se trouvent les fichiers de F-Secure Policy Manager Console ?

R. Pour obtenir la liste de tous les fichiers et de leurs emplacements, saisissez la commande suivante :

Distributions Debian	Distributions RPM
`dpkg -L f-secure-policy-manager-console`	`rpm -ql f-secure-policy-manager-console`

Q. Où se trouvent les fichiers journaux de F-Secure Policy Manager Server, les fichiers de configuration et le répertoire de communication dans la version pour Linux ?

R. Pour obtenir la liste de tous les fichiers et de leurs emplacements, saisissez la commande suivante :

Distributions Debian	Distributions RPM
`dpkg -L f-secure-policy-manager-server`	`rpm -ql f-secure-policy-manager-server`

Emplacement de certains fichiers particulièrement importants :

Informations utiles	Emplacement dans le système de fichiers
Fichiers journaux	`/var/opt/f-secure/fspms/logs`
Fichiers de configuration	`/etc/opt/f-secure/fspms/`
Répertoire de communication	`/var/opt/f-secure/fspms/commdir`

Q. Comment procéder pour modifier les ports au niveau desquels F-Secure Policy Manager Server écoute les demandes ?

R. Reportez-vous à la section "*Différents scénarios d'installation possibles pour les environnements à haute sécurité :*", *27*.

Q. Comment procéder pour redémarrer F-Secure Policy Manager Server après avoir modifié le fichier de configuration ?

R. Pour redémarrer F-Secure Policy Manager Server, procédez comme suit :

a. Connectez-vous en tant que `root`.
b. Saisissez la commande suivante :

```
/etc/init.d/fspms restart
```

Q. Comment procéder pour savoir si F-Secure Policy Manager Server fonctionne correctement ?

R. Saisissez la commande suivante :

```
/etc/init.d/fspms status
```

Q. Comment procéder pour planifier les mises à jour automatiques de mes définitions de virus ?

R. Pour ce faire, exécutez le script de configuration de F-Secure Policy Manager Server:

```
/opt/f-secure/fspms/bin/fspms-config
```

Q. Comment procéder pour configurer l'Agent de mise à jour automatique F-Secure de manière à utiliser le Proxy F-Secure Policy Manager ?

R. Pour utiliser le Proxy F-Secure Policy Manager, procédez comme suit :

a. Ouvrez le fichier `/opt/f-secure/fsaua/etc/fsaua_config` dans un éditeur de texte

b. Ajoutez la ligne `update_proxies=host:port` au fichier. Exemple :

```
update_proxies=proxy.domain.com:80
```

S'il existe plusieurs proxy, énumérez-les en les séparant par des virgules. Exemple :

```
update_proxies=proxy.domain.com:80,back_up_proxy.domain2.com:80
```

c. Redémarrez l'Agent de mise à jour automatique F-Secure pour appliquer les modifications :

```
/etc/init.d/fsaua restart
```

Q. Comment procéder pour utiliser un proxy HTTP avec l'Agent de mise à jour automatique F-Secure ?

R. Les proxy HTTP sont définis par le biais du fichier `/opt/f-secure/fsaua/etc/fsaua_config`

a. Ouvrez le fichier `/opt/f-secure/fsaua/etc/fsaua_config` dans un éditeur de texte.

b. Ajoutez la ligne `http_proxies=user:password@host:port` au fichier. Exemple :

```
http_proxies=Tom:toms_password@proxy.domain.com:80
```

S'il existe plusieurs proxy, énumérez-les en les séparant par des virgules. Exemple :

```
http_proxies=Tom:toms_password@proxy.domain.com:80,Ann:anns_password@back_upproxy.domain2.com:80
```

c. Redémarrez l'Agent de mise à jour automatique F-Secure pour appliquer les modifications :

```
/etc/init.d/fsaua restart
```

Q. Comment procéder pour redémarrer l'Agent de mise à jour automatique F-Secure après avoir modifié le fichier de configuration ?

R. Pour redémarrer l'Agent de mise à jour automatique F-Secure, saisissez :

```
/etc/init.d/fsaua restart
```

9 WEB REPORTING

9.1 Présentation

Ce chapitre couvre les sujets suivants :

- une introduction à F-Secure Policy Manager Web Reporting et à ses fonctions
- des instructions sur la génération et l'affichage de rapports Web
- des instructions sur la configuration et la maintenance de l'application F-Secure Policy Manager Web Reporting (par exemple, comment restreindre ou accroître les possibilités d'accès aux rapports Web et comment sauvegarder et restaurer la base de données de Web Reporting).

Web Reporting installation is a part of F-Secure Policy Manager Server setup. For more information, see "Procédure d'installation", 31

For information about special considerations when installing F-Secure Policy Manager Web Reporting in high security environments, see "Installation de F-Secure Policy Manager Web Reporting dans des environnements à haute sécurité", 29.

9.2 Introduction

F-Secure Policy Manager Web Reporting est un système de rapports graphiques intégré à F-Secure Policy Manager Server. Les rapports graphiques détaillés de F-Secure Policy Manager Web Reporting vous permettent d'identifier des ordinateurs qui ne sont pas protégés oui qui sont vulnérables aux attaques de virus. Avec F-Secure Policy Manager Web Reporting, vous pouvez créer rapidement des rapports graphiques fondés sur des données de tendances historiques à l'aide d'une interface Web. Vous pouvez produire une large palette de rapports et de requêtes utiles à partir des informations d'état et des alertesF-Secure Client Security envoyées par F-Secure Management Agent à F-Secure Policy Manager Server. Vous avez la possibilité d'exporter ces rapports au format HTML.

F-Secure Policy Manager Web Reporting est intégré avec une base de données SQL qui garantit sa compatibilité pour chaque taille de société. Cette base de données regroupe toutes les données stockées dans F-Secure Policy Manager Server et recueille les nouvelles données dès leur arrivée. Les données collectées incluent la plupart des données contenues dans les alertes et une partie des données des fichiers de stratégie incrémentiels (*.ipf*). Vous pouvez définir la durée de conservation des données dans la base de données de Web Reporting et ainsi optimiser ses performances.

9.3 Configuration système requise pour le client Web Reporting

Pour afficher les rapports générés par F-Secure Policy Manager Web Reporting, un navigateur Web, tel que Internet Explorer ou Mozilla Firefox doit être installé dans votre ordinateur.

9.4 Génération et affichage des rapports

Les types généraux de rapports qu'il est possible de créer incluent, par exemple, des graphiques à barres et des graphiques à secteurs sur la sécurité actuelle, des rapports de tendance et des listes détaillées. Pour afficher les rapports et les modèles de rapports disponibles, sélectionnez l'une des pages (*Protection antivirus, Protection Internet, Alertes, Logiciels installés et Propriétés d'hôte*) dans l'interface utilisateur de Web Reporting.

Le lancement de F-Secure Policy Manager Web Reporting peut prendre beaucoup de temps dans des environnements de taille importante. Les rapports ne sont pas disponibles lorsque Web Reporting est en cours de démarrage et toute tentative d'accès risque d'entraîner l'affichage de messages d'erreur. Pour plus d'informations, reportez-vous à la section “*Messages d'erreur de Web Reporting et dépannage*”, *189*.

9.4.1 Paramètres requis pour l'affichage des rapports Web dans le navigateur

Il est conseillé, lorsque vous commencez à vous servir de Web Reporting, de vérifier les paramètres de votre navigateur afin de vous assurer qu'il charge toujours les rapports les plus récents et qu'il n'affiche pas les rapports ou parties de rapports placés dans la mémoire cache. Si certaines informations des rapports proviennent de la mémoire cache, votre navigateur risque d'afficher un message d'erreur.

Pour les navigateurs Netscape Communicator et Mozilla, les paramètres de mémoire cache recommandés sont les suivants :

Comparer la page du cache à celle du réseau

- *Chaque fois que je visualise la page.*
  Sélectionnez cette option pour que Netscape compare une page Web à la mémoire cache chaque fois que vous affichez celle-ci.
- *Lorsque la page est périmée.*
  Sélectionnez cette option pour que Netscape compare une page Web à la mémoire cache lorsque le serveur indique que celle-ci a expiré.

Pour le navigateur Microsoft Internet Explorer, les paramètres de mémoire cache recommandés sont les suivants :

Vérifier s'il existe une version plus récente des pages enregistrées :

- *A chaque visite de la page.*
  Sélectionnez cette option pour qu'Internet Explorer compare une page Web avec la mémoire cache chaque fois que vous l'affichez.
- *Automatiquement.*
  Sélectionnez cette option pour qu'Internet Explorer vérifie l'existence d'une nouvelle version de la page de manière automatique.

Cookies

Il est conseillé d'activer les cookies dans votre navigateur afin de faciliter la navigation dans l'arborescence du domaine de stratégie, par exemple. Si vous souhaitez uniquement ouvrir un rapport enregistré, l'activation des cookies n'est pas nécessaire.

9.4.2 Génération d'un rapport

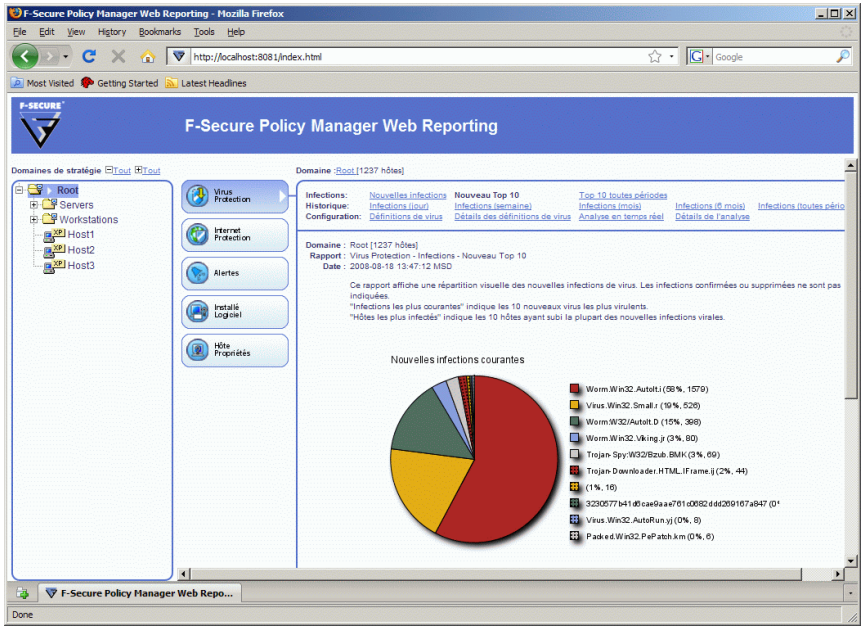
Vous pouvez générer un rapport Web comme suit :

1. Tout d'abord, ouvrez la page principale de F-Secure Policy Manager Web Reporting. Dans votre navigateur, entrez le nom ou l'adresse IP du serveur F-Secure Policy Manager Server suivie du port utilisé par Web Reporting (séparé par deux points). Par exemple, *fspms.exemple.com:8081*.

   Si vous accédez à Web Reporting de manière locale, ouvrez-le depuis le menu Démarrer : *Démarrer >F-Secure Policy Manager Server >Web Reporting*.

2. Attendez l'ouverture de la page de Web Reporting. Cette opération peut être longue dans des environnements de grande taille.

   Quand la page de F-Secure Policy Manager Web Reporting s'ouvre, elle affiche un rapport par défaut pour la catégorie de rapport sélectionnée. *Racine* est sélectionné par défaut dans le volet *Domaines de stratégie*.



3. Pour afficher un nouveau rapport, sélectionnez d'abord le domaine, le sous-domaine ou l'hôte pour lequel vous souhaitez générer le rapport.
4. Sélectionnez ensuite une catégorie de rapports (*Protection antivirus, Protection Internet, Alertes, Logiciels installés* et *Propriétés d'hôte*) et le rapport à générer.
5. Patientez pendant l'affichage du rapport dans la partie inférieure de la fenêtre principale.

9.4.3 Création d'un rapport imprimable

Pour obtenir une version imprimable de la page, cliquez sur l'icône située dans le coin supérieur droit de la page. Cette action ouvre une nouvelle fenêtre dans le navigateur avec le contenu du cadre principal sous un format imprimable. Vous pouvez alors imprimer la page à l'aide de la fonction d'impression standard du navigateur.

Vous avez également la possibilité d'enregistrer le rapport pour une utilisation ultérieure. Pour cela, utilisez les options *Enregistrer sous* ou *Enregistrer la page sous* de votre navigateur. Assurez-vous que l'option d'enregistrement utilisée permet bien l'enregistrement de la page Web complète, images incluses :

- Si vous utilisez Microsoft Internet Explorer, sélectionnez d'abord *Enregistrer sous* dans le menu *Fichier.* Dans la fenêtre *Enregistrer la page Web* qui s'ouvre, sélectionnez *Page Web complète* dans le menu déroulant *Type*.
- Si vous utilisez Mozilla, sélectionnez *Enregistrer la page sous* dans le menu *Fichier*.

9.4.4 Génération d'une URL spécifique pour la création automatique de rapports

Vous pouvez également générer une URL spécifique destinée à la création automatique de rapports. Autrement dit, vous n'aurez plus à sélectionner la catégorie du rapport, son type ni le domaine de stratégie à surveiller la prochaine fois que vous voulez générer le même rapport, car ces informations seront déjà incluses dans l'adresse URL spécifique au rapport.

Deux possibilités se présentent :

- Générer un rapport comportant les éléments à surveiller, puis ajouter un lien vers ce rapport sur votre ordinateur (Bureau, signets ou tout autre emplacement). La prochaine fois que vous ouvrirez F-Secure Policy Manager Web Reporting via ce lien, le rapport sera à nouveau généré et contiendra les toute dernières données.
- Vous pouvez également enregistrer le rapport que vous avez généré de manière à pouvoir comparer la situation présente avec les rapports ultérieurs. Créez tout d'abord une version imprimable de la page avant de l'enregistrer dans son intégralité dans le navigateur. Vous pourrez, de cette manière, conserver le rapport

tel qu'il était lors de l'enregistrement. Pour plus d'instructions, reportez-vous à la section “*Création d'un rapport imprimable*”, *181*.

9.5 Maintenance de Web Reporting

Cette section traite des tâches de maintenance de F-Secure Policy Manager Web Reporting les plus courantes.

9.5.1 Désactivation de Web Reporting

Vous pouvez désactiver F-Secure Policy Manager Web Reporting en utilisant les Services du Panneau de configuration comme indiqué ci-après :

1. Ouvrez la fenêtre Services du Panneau de configuration depuis le menu *Démarrer* de Windows.
2. Sélectionnez F-Secure Policy Manager Web Reporting dans la liste de services.
3. Ouvrez le menu *Action* et sélectionnez *Propriétés*. Cliquez sur **Arrêter** pour arrêter le service.
4. Choisissez le type de démarrage *Manuel*. Si vous ne souhaitez arrêter Web Reporting que temporairement, ignorez cette étape.
5. Cliquez sur **OK**.

Vous pouvez également désactiver Web Reporting en réexécutant le programme d'installation de F-Secure Policy Manager.

9.5.2 Activation de Web Reporting

Ces instructions vous permettent d'activer Web Reporting uniquement si vous l'aviez activé une première fois lors de l'installation et ensuite désactivé à l'aide des instructions précédentes.
Vous avez toujours la possibilité d'activer Web Reporting en réexécutant le programme d'installation.

Vous pouvez activer F-Secure Policy Manager Web Reporting en utilisant les Services du Panneau de configuration comme indiqué ci-après :

1. Ouvrez la fenêtre Services du Panneau de configuration depuis le menu Démarrer de Windows.
2. Sélectionnez F-Secure Policy Manager Web Reporting dans la liste de services.
3. Ouvrez le menu *Action* et sélectionnez *Propriétés*. Cliquez sur **Démarrer** pour lancer le service.
4. Choisissez le type de démarrage *Automatique*.
5. Cliquez sur **OK**.

Le module d'administration de Policy Manager doit également être activé pour que Web Reporting puisse fonctionner.

9.5.3 Restriction ou élargissement des possibilités d'accès aux rapports Web

Le répertoire *conf*\ dans le répertoire d'installation de F-Secure Policy Manager Server contient un fichier F-Secure Policy Manager Server*httpd.conf*. Ce fichier contient les informations de configuration de F-Secure Policy Manager Server et de F-Secure Policy Manager Web Reporting.

Après avoir modifié la configuration, vous devez arrêter F-Secure Policy Manager Server et le redémarrer pour que les modifications entrent en vigueur.

Les droits d'accès à Web Reporting peuvent être définis de trois manières : en autorisant l'accès uniquement depuis l'ordinateur local, depuis n'importe quel emplacement ou depuis un certain nombre d'hôtes définis par leur adresse IP.

Autoriser l'accès depuis n'importe quel emplacement (option par défaut)

Par défaut, F-Secure Policy Manager Web Reporting est accessible depuis tout ordinateur pouvant accéder au port Web Reporting sur le Policy Manager Server. Ce droit est accordé par le paramètre suivant du fichier *httpd.conf* :

```
Listen 8081
```

Autoriser l'accès depuis l'ordinateur local uniquement

L'accès à F-Secure Policy Manager Web Reporting peut également être autorisé depuis l'ordinateur local uniquement en configurant le paramètre du port Web Reporting dans le fichier *httpd.conf* de la façon suivante :

```
Listen 127.0.0.1:8081
```

Indiquer une liste d'hôtes ayant accès à Web Reporting

L'accès à F-Secure Policy Manager Web Reporting peut également être autorisé uniquement depuis certaines adresses IP définies séparément. Vous trouverez ci-dessous un exemple de modification de la section correspondante du fichier *httpd.conf* :

```
#Web Reporting listen
Listen 8081


# Web Reporting port:
<VirtualHost _default_:8081>
  JkMount /* ajp13
  ErrorDocument 500 "Policy Manager Web Reporting could not
be contacted by the Policy Manager Server.
  <Location / >
    Order Deny,Allow
    Deny from all
    Allow from ip-address-1
    Allow from ip-address-2
    Allow from ip-address-3
  </Location>
</VirtualHost>
```

La configuration une fois terminée, seuls les utilisateurs ayant accès aux ordinateurs dotés des adresses IP définies peuvent se servir de Web Reporting.

9.5.4 Modification du port de Web Reporting

La méthode recommandée pour modifier le port de F-Secure Policy Manager Web Reporting consiste à réexécuter le programme d'installation de F-Secure Policy Manager et à y modifier le port de Web Reporting. Pour plus d'informations, reportez-vous à la section “*Procédure d'installation*”, *31*.

Vous pouvez également changer de port en modifiant le fichier *httpd.conf*.

1. Arrêtez F-Secure Policy Manager Server.
2. Modifiez le port de Web Reporting (`Listen`) et les paramètres `VirtualHost` dans le fichier *httpd.conf* de manière qu'ils affichent le nouveau numéro de port.
3. Démarrez F-Secure Policy Manager Server.

S'il existe un conflit entre les ports, F-Secure Policy Manager Server ne démarre pas et génère un message d'erreur dans le fichier journal. Dans ce cas, essayez un autre port qui ne soit pas déjà utilisé.

9.5.5 Création d'une copie de sauvegarde de la base de données de Web Reporting

Il est possible de sauvegarder la base de données de Web Reporting sur un support de sauvegarde, comme suit :

1. Arrêtez le service F-Secure Policy Manager Web Reporting.
2. Copiez le fichier

   C:\Program Files\F-Secure\Management Server 5\Web Reporting\firebird\data\fspmwr.fdb

   sur le support de sauvegarde. Vous pouvez également recourir à un utilitaire de compression des données pour compresser le fichier. Son utilisation vous permet par ailleurs de vérifier que la base de données sauvegardée est restée intacte.
3. Redémarrez le service F-Secure Policy Manager Web Reporting.

Une copie de sauvegarde permet de protéger les historiques de toute corruption. Elle permet également de conserver les données plus anciennes qui auraient pu être supprimées lors d'une modification de la durée de stockage maximale appliquée à la base de données de Web Reporting (reportez-vous à la section "Modification de la durée maximale de stockage des données dans la base de données de Web Reporting", 188).

9.5.6 Restauration de la base de données de Web Reporting à partir d'une copie de sauvegarde

Vous pouvez restaurer la base de données F-Secure Policy Manager Web Reporting à partir d'une copie de sauvegarde comme indiqué ci-dessous :

1. Arrêtez le service F-Secure Policy Manager Web Reporting.
2. Copiez et décompressez le fichier *fspmwr.fdb* situé sur le support de sauvegarde dans le répertoire suivant :
3. *C:\Program Files\F-Secure\Management Server 5\Web Reporting\firebird\data*
4. Redémarrez le service F-Secure Policy Manager Web Reporting.

9.5.7 Modification de la durée maximale de stockage des données dans la base de données de Web Reporting

Vous pouvez définir la durée de conservation des tendances passées dans la base de données avant qu'elles ne soient supprimées. La durée définie par défaut est d'un an. Si vous souhaitez pouvoir générer des rapports de tendance sur une période supérieure à celle-ci, augmentez la durée. A l'inverse, pour conserver ces données sur une période plus courte, revoyez la valeur à la baisse.

1. Arrêtez le service F-Secure Policy Manager Web Reporting.
2. Dans le répertoire de Web Reporting, modifiez la durée maximale définie dans le fichier *fspmwr.conf*. L'unité de temps utilisée est la seconde. Vous trouverez ci-dessous un exemple de la section à modifier dans le fichier de configuration :

```
#
# The database data retaining time. The database data
older than the current time
# minus retaining time will be removed from the database
permanently.
#
# Value:   Use a retaining time measured in seconds.
# Default: An empty value will set the default retaining
time in use. The default
#          retaining time is 12 months.
#
fspmwr.db.retain.time=31536000
```

3. Redémarrez le service F-Secure Policy Manager Web Reporting.

   Le nouveau paramètre entre immédiatement en vigueur. Par exemple, si vous avez réduit la durée maximale de stockage des données dans la base de données, toutes les données antérieures à la nouvelle durée sont supprimées.

9.6 Messages d'erreur de Web Reporting et dépannage

Cette section traite des messages d'erreur de F-Secure Policy Manager Web Reporting et du dépannage de la base de données de Web Reporting.

9.6.1 Messages d'erreur

Message d'erreur du navigateur : « La connexion a été refusée lors de la tentative pour joindre <emplacement> »

Votre navigateur n'a pas pu entrer en contact avec Web Reporting. Votre lien renvoie peut-être vers un ordinateur ou un port incorrect, Web Reporting n'est pas installé sur cet ordinateur ou le service F-Secure Policy Manager Server n'est pas en cours d'exécution. Vérifiez chacun de ces points dans l'ordre indiqué. Il se peut également qu'un pare-feu empêche la connexion.

Message d'erreur : “F-Secure Policy Manager Server n'a pas pu contacter F-Secure Policy Manager Web Reporting. "

Si ce type de message d'erreur s'affiche sur votre ordinateur, c'est que F-Secure Policy Manager Web Reporting est en cours de démarrage. Patientez quelques instants pour savoir si le problème est bien dû aux démarrages en cours, puis rechargez la page.

Notez que ce message s'affiche également si vous avez désactivé manuellement Web Reporting dans la fenêtre Service du Panneau de configuration.

Le temps nécessaire au démarrage du service dépend de la taille de votre environnement. Pour le réduire, supprimez certaines alertes du répertoire CommDir.

Message d'erreur : « Web Reporting a perdu sa connexion à F-Secure Policy Manager Server à l'<emplacement>. Les données du rapport sont peut-être obsolètes et ne peuvent donc être affichées. »

Si le service Web Reporting ne peut pas entrer en contact avec F-Secure Policy Manager Server, cela peut signifier que F-Secure Policy Manager Server était en surcharge extrême pendant un long moment et que les données en cours ne sont pas exactes. Aucun rapport ne peut donc être affiché. Si le cas se présente, vous devez mettre votre matériel à niveau.

Si des messages d'erreur spécifiques à Web Reporting s'affichent, vous devriez pouvoir résoudre le problème en redémarrant le serveur F-Secure Policy Manager Server et le service Web Reporting.

Message d'erreur : « Web Reporting a perdu sa connexion à la base de données, il vous faut redémarrer le service Web Reporting. »

Si le service Web Reporting ne peut pas entrer en contact avec la base de données, redémarrez-le. Si le problème persiste, vous pouvez réinstaller Web Reporting, en conservant la base de données existante.

9.6.2 Dépannage

En général, si F-Secure Policy Manager Web Reporting ne fonctionne pas, essayez l'une des méthodes suivantes, dans cet ordre :

- Rechargez la page.
- Si le problème est dû au fait que les processus sont en cours de démarrage, patientez quelques instants, puis réessayez de recharger la page. Pour réduire le temps nécessaire au démarrage, supprimez les alertes inutiles du répertoire CommDir.
- Redémarrez le service F-Secure Policy Manager Web Reporting.
- Redémarrez F-Secure Policy Manager Server
- Redémarrez l'ordinateur.
- Réinstallez F-Secure Policy Manager Server tout en gardant la configuration existante.
- Si tout échoue, réinitialisez la base de données F-Secure Policy Manager Web Reporting ou restaurez-la à partir d'une copie de sauvegarde.

Réinitialisation de la base de données de Web Reporting

En temps normal, le serveur Web Reporting efface automatiquement toutes les données obsolètes de la base de données en fonction de la durée maximale définie pour le stockage des données. Toutefois, si la base de données se révèle être endommagée, vous pouvez la remplacer par un fichier de base de données vide. La procédure est la suivante :

1. Arrêtez le service F-Secure Policy Manager Web Reporting.
2. Copiez le fichier *fspmwr.fdb.empty* sur le fichier *fspmwr.fdb* pour remplacer *fspmwr.fdb*. Ils se trouvent tous deux dans le même répertoire. Si, par inadvertance, vous avez perdu le fichier *fspmwr.fdb.empty*, réinstallez F-Secure Policy Manager Server.
3. Démarrez le service F-Secure Policy Manager Web Reporting.

10 F-Secure Policy Manager Proxy

10.1 Présentation

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

F-Secure Policy Manager Proxy offre une solution aux problèmes de bande passante rencontrés dans les installations distribuées de F-Secure Anti-Virus pour Windows en réduisant sensiblement la charge sur les réseaux utilisant des connexions lentes. Il met en cache les mises à jour de base de données de définitions de virus récupérées à partir de F-Secure Policy Manager Server ou du serveur de mise à jour F-Secure.

F-Secure Policy Manager Proxy se trouve sur le même réseau distant que les hôtes qui l'emploient comme point de distribution des bases de données. Chaque réseau lent devrait idéalement comporter une installation de F-Secure Policy Manager Proxy. F-Secure Policy Manager Proxy charge les mises à jour de bases de données de définitions de virus directement depuis le serveur de distribution de F-Secure. Les hôtes exécutant F-Secure AntiVirus récupèrent ces mises à jour localement à partir de F-Secure Policy Manager Proxy. Les stations de travail des bureaux distants communiquent elles aussi avec 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.

11 DÉPANNAGE

11.1 Présentation

Ce chapitre comporte des informations sur le dépannage, ainsi que les questions fréquemment posées au sujet de F-Secure Policy Manager Server et F-Secure Policy Manager Console.

Pour obtenir des informations sur la configuration de F-Secure Policy Manager Server et sur le changement des ports sur lesquels le serveur écoute des demandes, reportez-vous à la section “*Configuration de F-Secure Policy Manager Server*”, *44*.

11.2 F-Secure Policy Manager Server et Console

Q. F-Secure Policy Manager Server ne démarre pas. Pourquoi ?

R. Vous trouverez des erreurs d'exécution, des avertissements et d'autres informations dans le fichier :

<F-Secure>\Management Server 5\logs\error.log

Si le journal Application dans l'Observateur d'événements (Outils d'administration dans NT/2000/2003) indique « *ServerRoot must be a valid directory* » ou « *Syntax error on line 6* » en provenance du service Apache, procédez comme suit :

Vérifiez d'abord la validité de la ligne ServerRoot qui est définie dans le fichier *httpd.conf* (ligne 6 par défaut). Si cette ligne est correcte, vérifiez que les droits d'accès au répertoire de communication (Propriétés/Sécurité/Autorisations) incluent le compte d'utilisateur `fsms_<NOMORDINATEUR>`. Si `fsms_<NOMORDINATEUR>` n'est pas indiqué comme utilisateur autorisé, ajoutez l'utilisateur manuellement et définissez les droits d'accès avec la valeur *Contrôle total*.

Propagez les droits d'accès au répertoire *Management Server 5* (par défaut *C:\Program Files\F-Secure\Management Server 5*) et à tous ses sous-répertoires. Après avoir effectué ces modifications, redémarrez le service F-Secure Policy Manager Server ou l'ordinateur.

Le compte `fsms_<NOMORDINATEUR>` est créé pendant l'installation de F-Secure Policy Manager Server et le service est démarré sous ce compte d'utilisateur. Lors d'une installation normale, les droits d'accès pour le répertoire Management Server 5 sont automatiquement définis de façon appropriée. Si le répertoire est copié manuellement ou, par exemple, s'il est restauré à partir d'une sauvegarde, les droits d'accès risquent d'être supprimés. Dans ce cas, procédez de la manière indiquée dans le paragraphe précédent.

Q. Où les fichiers journaux, les fichiers de configuration et le répertoire de communication sont-ils situés pour F-Secure Policy Manager Server ?

R. Les fichiers journaux se trouvent dans :

<F-Secure>\Management Server 5\logs

Les fichiers de configuration se trouvent dans :

<F-Secure>\Management Server 5\conf

Le F-Secure Policy Manager Server répertoire de communication se trouve dans :

<F-Secure>\\Management Server 5\commdir

Q. Où les fichiers journaux de F-Secure Policy Manager Console sont-ils situés ?

R. Le fichier journal est le suivant :

<F-Secure>\Administrator\lib\administrator.error.log

Q. Comment la modification du rôle du serveur arrête le fonctionnement de F-Secure Policy Manager Server ?

R. Un serveur contrôleur de domaine et un serveur membre/autonome utilisent différents types de comptes : comptes de domaine sur un contrôleur de domaine et comptes locaux sur un serveur membre. Comme F-Secure Policy Manager Server utilise son propre compte pour s'exécuter, ce compte devient non valide lors du changement de rôle.

La façon la plus facile de restaurer F-Secure Policy Manager Server après le changement de rôle du serveur est de réinstaller F-Secure Policy Manager Server avec l'option *Conserver les paramètres actuels* sélectionnée. Cette opération recréera le compte F-Secure Policy Manager Server et réinitialisera les droits d'accès à leur valeur correcte.

Si vous avez déplacé le répertoire commdir manuellement, vous devrez éventuellement rajouter un contrôle total pour le nouveau compte dans cette arborescence.

Q. Pourquoi F-Secure Policy Manager Server son propre compte pour démarrer au lieu du compte système ?

R. Le compte Policy Manager Server (`fsms_<NOMORDINATEUR>`) est utilisé pour des raisons de sécurité. En s'exécutant sous son propre compte, toute vulnérabilité de F-Secure Policy Manager Server en matière de sécurité ne l'affectera que lui seul, et non le système entier. Si un compte utilisateur était utilisé, l'ensemble du système pourrait être compromis dans l'éventualité peu probable d'un problème de sécurité dans F-Secure Policy Manager Server.

Q. Comment un renforcement de sécurité de Windows peut-il empêcher la bonne exécution de F-Secure Policy Manager Server ?

R. Les restrictions de droits d'accès, surtout les restrictions sous le répertoire *%SystemRoot%* (*c:\windows* ou *c:\winnt*) peuvent empêcher F-Secure Policy Manager Server de démarrer, puisque son propre compte (`fsms_<NOMORDINATEUR>`) doit pouvoir lire les fichiers DLL et SYS associés au réseau.

Vous devez permettre au compte `fsms_<NOMORDINATEUR>` de « lire » les répertoires suivants :

%SystemRoot%

%SystemRoot%\system32

%SystemRoot%\system32\drivers

Certaines restrictions de service peuvent également empêcher le service F-Secure Policy Manager Server de démarrer. Pour plus d'informations à ce sujet, consultez la documentation de Microsoft Windows Server.

Q. Pourquoi m’est-il impossible de me connecter à F-Secure Policy Manager Server ?

R. Si vous obtenez l'erreur « *Impossible de se connecter au serveur d'administration. Un autre administrateur doit être connecté* », vérifiez que personne d’autre n'est connecté à F-Secure Policy Manager Server avec F-Secure Policy Manager Console. Cette erreur peut également être provoquée par un arrêt incorrect de F-Secure Policy Manager Console. Pour régler le problème, vous pouvez soit attendre que F-Secure Policy Manager Server s’éteigne seul (<=5 minutes), soit supprimer le fichier *admin.lck* dans Commdir, puis redémarrer le service F-Secure Policy Manager Server.

Q. Pourquoi la connexion entre F-Secure Policy Manager Console et F-Secure Policy Manager Server est-elle interrompue ?

R. Si F-Secure Policy Manager Console est exécuté sur un ordinateur différent de celui où est exécuté F-Secure Policy Manager Server, la connexion peut être altérée par les problèmes de réseau. Il a été souvent observé, par exemple, qu'un changement de commutateur réseau peut entraîner des problèmes de perte de connexion entre F-Secure Policy Manager Console et F-Secure Policy Manager Server. Généralement, ces problèmes sont corrigés par la mise à jour des pilotes réseau à la dernière version sur les ordinateurs concernés ou en reconfigurant les ordinateurs F-Secure Policy Manager Console et F-Secure Policy Manager Server.

Si F-Secure Policy Manager Console est installé sur le même ordinateur que F-Secure Policy Manager Server, il existe un risque que F-Secure Policy Manager Server pâtissent d'une charge réseau telle qu'il ne dispose plus d'une seule connexion disponible. F-Secure Policy Manager Console et tous les hôtes se disputent les mêmes ressources réseau.

Avec les paramètres par défaut, F-Secure Policy Manager Server ne peut gérer que 150 connexions simultanées. Vous pouvez accroître le nombre de connexions simultanées en augmentant la valeur `ThreadsPerChild` dans le fichier *httpd.conf* et en redémarrant ensuite F-Secure Policy Manager Server. Les autres solutions possibles consistent à augmenter les intervalles d'interrogation des hôtes, à modifier les délais de déconnexion du réseau Windows en les réduisant ou en augmentant le nombre de ports réseau Windows.

Paramètres réseau Windows pratiques :

`HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\MaxUserPort (nombre maximal de ports réseau, valeur par défaut = 5000)`

`HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpTimedWaitDelay (délai d'attente avant fermeture d'une connexion réseau inactive, valeur par défaut = 240 secondes).`

La commande`netstat -an` permet de vérifier si un trop grand nombre de connexions sont ouvertes sur le serveur.

11.3 F-Secure Policy Manager Web Reporting

Q. Où les fichiers journaux et de configuration de F-Secure Policy Manager Web Reporting sont-ils situés ?

R. Les fichiers journaux se trouvent dans :

<F-Secure>\Management Server 5\Web Reporting\logs

Les fichiers de configuration se trouvent dans :

<F-Secure>\Management Server 5\Web Reporting\fspmwr.conf

<F-Secure>\Management Server 5\Web Reporting\jetty\etc\fspmwr.xml

<F-Secure>\Management Server 5\Web Reporting\firebird\aliases.conf

<F-Secure>\Management Server 5\Web Reporting\firebird\firebird.conf

Voir aussi les fichiers de configurations de F-Secure Policy Manager Server :

<F-Secure>\Management Server 5\conf\httpd.conf

<F-Secure>\Management Server 5\conf\workers.properties

11.4 Distribution des stratégies

Q. Lors de la distribution d'une stratégie, F-Secure Policy Manager Console affiche un message d'erreur relatif à une valeur de stratégie incorrecte. Que dois-je faire ?

R. Voir ci-dessous pour des informations sur les messages d'erreur susceptibles de s'afficher pendant la distribution des stratégies, leurs causes et des solutions éventuelles.

Messages d'erreur :	**« <nom du paramètre> » a une valeur en dehors de la restriction** **« <nom du paramètre>>» a une restriction incorrecte** **« <nom du paramètre> » possède une valeur incorrecte : "« <valeur> »**
Raison 1 :	La valeur sélectionnée dans une liste de choix ne fait pas partie des choix d'un sous-domaine ou d'un hôte, les limites de restriction spécifiées sont trop hautes ou trop basses, ou une liste de choix vide a été spécifiée. Lorsqu'un domaine comprend des hôtes sur lesquels différentes versions de produits sont installées, les paramètres de la base de données MIB de la version la plus récente sont utilisés pour modifier les valeurs de stratégie. De ce fait, la distribution de la stratégie peut échouer sur les hôtes dotés de versions antérieures du logiciel car ces dernières ne prennent pas en charge les nouveaux paramètres ou nouvelles valeurs de la stratégie.

Solution : Divisez les hôtes en sous-domaines de façon à pouvoir définir la nouvelle valeur pour les hôtes bénéficiant de la version la plus récente du logiciel et à utiliser des valeurs de stratégie plus anciennes pour les autres hôtes. Pour ce faire :

1. Regroupez les hôtes en sous-domaines basés sur la version du produit installé. 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.
2. Définissez la plupart des paramètres sur le domaine racine, puis créez des sous-domaines pour les exceptions.+ C'est une bonne solution si vous ne disposez que de quelques hôtes avec une ancienne version du logiciel.

Raison 2 : Vous avez saisi une valeur entière non compris dans les restrictions de plage.

Message d'erreur : «<nom du paramètre> » est requis mais n'est pas défini

Raison : Le paramètre est requis, mais il est vide.

Solution : Saisissez une valeur ou appliquez l'opération **Effacer** pour rétablir l'héritage de la valeur à partir du domaine ou MIB parent. Si la valeur est vide à plusieurs niveaux du domaine, vous devrez peut-être effectuer l'opération **Effacer** plusieurs fois.

A Prise en charge de SNMP

A.1 Présentation

Cette section traite des aspects suivants de la prise en charge de SNMP :

- F-Secure Management Agent avec agent SNMP
- Installation F-Secure Management Agent avec prise en charge de SNMP
- F-Secure Management Agent Base d'informations de gestion (MIB)
- Interruptions SNMP envoyées par F-Secure Management Agent
- Modules complémentaires de gestion de réseau

La prise en charge de SNMP est actuellement implémentée pour toutes les versions de Windows NT, y compris Windows 2000, Windows XP et Windows Server 2003, Windows Server 2008 et Windows Vista.

A.1.1 Prise en charge de SNMP pour F-Secure Management Agent

Windows NT

La version NT de la prise en charge de SNMP pour F-Secure Management Agent implémente l'agent principal de Windows NT comme un service. Windows Sockets doit être installé avec les protocoles TCP/IP ou IPX/SPX, car le service SNMP l'utilise pour les communications réseau.

L'agent principal est un agent SNMP extensible, qui lui permet de servir d'autres MIB. L'agent SNMP de NT à proprement parler ne contient d'infrastructure pour aucune MIB. En revanche, il est responsable de la récupération des requêtes SNMP pour le serveur ou le poste de travail NT et de la transmission de celles-ci aux modules appropriés en vue de leur résolution.

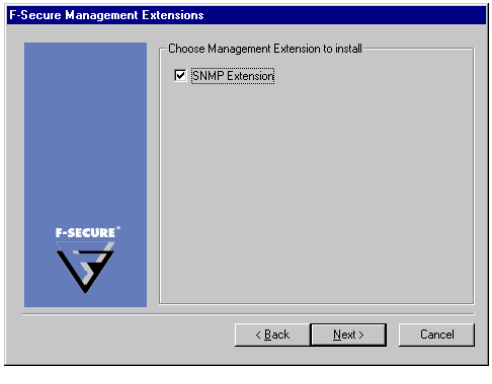
L'extension d'administration SNMP de F-Secure SNMP est un agent d'extension SNMP Windows NT, chargé et déchargé avec l'agent principal. Le service SNMP est lancé normalement au démarrage de

Windows NT 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.

A.2 Installation de F-Secure Management Agent avec prise en charge de SNMP

A.2.1 Installation de l'extension d'administration SNMP de F-Secure

La prise en charge de SNMP pour F-Secure Management Agent est installée lors de l'installation des extensions de gestion.



Si l'agent principal SNMP est déjà installé lorsque vous installez F-Secure SNMP Management Extension, vous devrez réinstaller le Service Pack correspondant (voir Configuration de l'agent principal SNMP).

A.3 Configuration de l'agent principal SNMP

Le service SNMP est installé à partir de la section Réseau du Panneau de configuration de Windows. L'option Service SNMP peut être définie dans la fenêtre Options d'installation TCP/IP. Une fois que vous avez installé le service SNMP sur votre ordinateur, vous devez le configurer correctement avant de pouvoir l'exécuter.

Pour configurer SNMP, vous devez ouvrir une session en tant qu'administrateur sur l'ordinateur local. Les informations de configuration de SNMP identifient les destinations des interruptions et les communautés. Une communauté est un groupe d'hôtes auquel appartient un ordinateur Windows NT exécutant le service SNMP. Vous pouvez spécifier une ou plusieurs communautés auxquelles l'ordinateur enverra des interruptions. Le nom de la communauté est inclus dans l'interruption.

Lorsque le service SNMP reçoit une demande d'informations qui ne contient pas le nom correct d'une communauté et qui ne correspond pas à un nom d'hôte approuvé pour le service, le service SNMP peut envoyer une interruption vers la destination de l'interruption indiquant l'échec de l'authentification de la demande.

Les destinations des interruptions correspondent aux noms ou adresses IP des hôtes auxquels le service SNMP doit envoyer les interruptions avec le nom de la communauté sélectionné.

Si vous voulez utiliser SNMP pour les statistiques plutôt que pour identifier des communautés ou des interruptions, vous pouvez spécifier le nom de communauté « public » lorsque vous configurez le service SNMP.

Utilisez la boîte de dialogue Configuration de la sécurité SNMP pour définir les paramètres de sécurité des services SNMP. Cette boîte de dialogue s'affiche lorsque vous cliquez sur le bouton **Sécurité** dans la boîte de dialogue Configuration du service SNMP.

La sécurité SNMP vous permet de spécifier les communautés et les hôtes dont un ordinateur accepte les requêtes et de définir l'envoi d'une interruption d'authentification lorsqu'une communauté ou un hôte non autorisé demande des informations.

A.4 Base d'informations de gestion (MIB)

Une base d'informations de gestion (MIB, Management Information Base) décrit un ensemble d'objets administrés sur un agent SNMP. Un système d'administration peut manipuler ces objets si l'agent SNMP a associé une DLL d'agent d'extension à cette MIB.

Les fichiers MIB SNMP sont automatiquement installés sous F-Secure Policy Manager Console dans le répertoire *Administrator\snmp-mib* lors de l'installation de F-Secure Policy Manager Console. Chaque produit possède son propre fichier MIB SNMP.

L'entrée correspondant à chaque objet administré est associée à un identificateur unique (OID). Chaque entrée contient aussi une description du type de l'objet (comme un compteur, une chaîne, une jauge ou une adresse), le type d'accès à l'objet (par exemple en lecture seule ou en lecture/écriture), les restrictions de taille et les informations sur les valeurs acceptées.

Un OID est un identificateur unique affecté à un objet spécifique. Cet identificateur consiste en une séquence de nombres qui identifie la source de l'objet, ainsi que l'objet lui-même. Les identificateurs uniques sont organisés en arborescence et la séquence de nombres identifie les différentes ramifications de la sous-arborescence dont un objet donné fait partie. La racine de l'arborescence constitue la jonction ISO (International Standards Organization, ou Organisation internationale de normalisation). Sa valeur est égale à 1. Chaque ramification de la racine représente une identification supplémentaire de la source d'un objet donné. Tous les objets SNMP appartiennent à la branche identifiée par *iso.org.dod.internet* ou *1.3.6.l*. Chaque composant supplémentaire dans cette notation décimale pointée précise davantage l'emplacement exact d'un objet. Les segments numériques associés à chaque ramification sont définis par l'IETF (groupe de travail responsable des standards d'Internet) pour assurer que chaque branche est unique.

Les interruptions sont des messages SNMP émis par un agent sur un poste d'administration préconfiguré. Elles permettent de signaler tout événement significatif aux consoles d'administration. Elles sont généralement utilisées pour signaler le démarrage et l'interruption d'un service, des erreurs graves, etc.

Les interruptions sont envoyées au poste d'administration via l'agent SNMP uniquement si vous avez sélectionné le transfert des interruptions dans la table de redirection du produit dans F-Secure Policy Manager Console. Pour plus d'informations sur la redirection des interruptions, reportez-vous à la section *“Configuration de la transmission des alertes”, 131*.

B ANNEXE : Codes d'erreur d'llaunchr

B.1 Présentation

Après l'exécution de la commande *Ilaunchr.exe*, les résultats d'installation s'affichent à l'aide des codes standard. Le script de connexion vous permet de rechercher la cause du problème. Voici un exemple que vous pouvez insérer dans votre script de connexion :

```
Start /Wait ILaunchr.exe \\server\share\mysuite.jar /U
if errorlevel 100 Go to Some_Setup_Error_occurred
if errorlevel 5 Go to Some_Ilaunchr_Error_occurred
if errorlevel 3 Go to Problem_with_JAR_package
if errorlevel 2 Go to User_does_not_have_admin_rights
if errorlevel 1 Go to FSMA_was_already_installed
if errorlevel 0 Echo Installation was OK!
```

B.2 Codes d'erreur

0	Installation OK.
1	FSMA déjà installé.
2	L'utilisateur ne dispose pas des droits d'administrateur.
3	Fichier JAR introuvable.
4	Fichier JAR endommagé.
6	Erreur survenue lors de la décompression d'un fichier d'installation.
7	Espace insuffisant sur le disque de destination pour l'installation.
8	Le fichier *package.ini* est introuvable dans le fichier JAR.
9	Le fichier *package.ini* ne contient aucune instruction de fonctionnement.
10	Paramètres incorrects sur la ligne de commande ou dans le fichier *.ini*.
11	Erreur d'initialisation d'un nouveau processus de travail.
12	Erreur de création du processus destiné au programme d'installation.
13	Impossible de créer un répertoire temporaire.
14	Erreur indéfinie.

100	Données nécessaires à l'installation silencieuse introuvables. Fichier JAR incorrect.
101	Mise à jour désactivée. (Tentative de mise à jour de l'installation lors de l'exécution du programme d'installation)
102	Le programme d'installation n'a pas pu lire le fichier *product.ini*.
103	Données incorrectes rencontrées dans *prodsett.ini*.
104	Management Agent a interrompu l'installation ou un conflit de logiciel a été détecté. Installation interrompue.
105	La clé du CD est erronée ou introuvable. Installation interrompue.
110	Espace disque insuffisant.
111	Le lecteur de destination n'est pas local.
120	L'utilisateur ne dispose pas des droits d'accès administrateur au poste.
130	Le programme d'installation n'a pas pu copier les fichiers non compressés dans le répertoire de destination.
131	Le programme d'installation n'a pas pu copier le plugin de désinstallation du produit dans le répertoire de destination.
132	Le programme d'installation n'a pas pu copier le fichier *product.ini* dans le répertoire temporaire.

133	Erreur survenue lors de la sauvegarde du fichier du produit dans le répertoire de destination.
134	Impossible de copier *prodsett.ini*.
140	Une version plus récente de la solution Suite a été détectée.
150	Le programme d'installation n'a pas pu charger la DLL du plugin du produit.
151	Le programme d'installation n'a pas pu charger la DLL de prise en charge de l'installation.
152	Le programme d'installation n'a pas pu charger la DLL wrapper.
160	Le programme d'installation n'a pas pu initialiser le fichier Cab.
170	Le plugin d'installation de Management Agent a retourné une erreur.
171	Le plugin a retourné un code inattendu.
172	Le plugin a retourné un code wrapper.
173	L'une des opérations d'installation ou de désinstallation précédentes n'a pas été terminée. Un redémarrage est nécessaire pour la terminer.
174	L'ordinateur de destination a été redémarré afin de terminer une des opérations d'installation ou de désinstallation précédentes. Veuillez relancer l'installation.

200	Réussite partielle. L'installation de certains produits a échoué.

C Codes d'erreur de l'installation distante avec FSII

C.1 Présentation

Cette annexe décrit les codes d'erreur les plus courants ainsi que les messages qui apparaissent durant le processus Autodécouvrir hôtes Windows.

C.2 Codes d'erreur Windows

Code d'erreur	Description
1057	Le nom du compte utilisateur est incorrect ou n'existe pas.
5	Accès refusé : si vous utilisez l'option « Ce compte », il est important que l'administrateur soit connecté à l'ordinateur F-Secure Policy Manager Console avec des droits d'administrateur du domaine. En ce qui concerne les domaines sécurisés, veillez à vous connecter à F-Secure Policy Manager Console avec le compte associé au domaine.
1069	Echec de connexion. Dans la plupart des cas, le mot de passe saisi est incorrect.
1722	Le serveur RPC n'est pas disponible. Ce message d'erreur apparaît lorsque vous redémarrez l'hôte immédiatement après l'installation alors queF-Secure Policy Manager Console n'a pas terminé la vérification de l'installation.
1219	F-Secure Policy Manager Console a ouvert des connexions réseau vers la station de travail cible. Fermez ces connexions avant de tenter d'en ouvrir avec un autre compte d'utilisateur.

C.3 Messages d'erreur

Q. Le droit requis n'est pas attribué au compte actuel. Il doit être ajouté manuellement.

R. Par défaut, même l'administrateur ne dispose pas du droit requis « Acteur dans un système d'exploitation » sur l'ordinateur F-Secure Policy Manager Console. Si vous ne disposez pas de ce droit, Windows NT empêche l'authentification par FSII des comptes utilisateur saisis. Afin d'ajouter ce droit au compte de l'administrateur sur la F-Secure Policy Manager Console, ouvrez le Gestionnaire des utilisateurs Windows NT > Stratégies > Droits utilisateur.

Q. Management Agent a interrompu l'installation ou un conflit de logiciel a été détecté. Installation interrompue.

R. Le programme d'installation de Management Agent annule l'ensemble de l'installation dans les cas suivants :

1. Un conflit avec un logiciel tiers est détecté.
2. Il existe de nombreuses autres possibilité, notamment : l'adresse URL de Policy Manager Server n'est pas correcte.

Q. La clé du CD est erronée ou introuvable. Installation interrompue.

R. L'installation sur l'hôte distant ne démarre pas en raison d'une saisie incorrecte de la clé du CD. Vérifiez la syntaxe.

Q. Espace disque insuffisant sur l'hôte de destination.

R. L'hôte de destination ne dispose pas d'un espace disque suffisant. Généralement, au moins 20 Mo sont nécessaires.

Q. L'installation de Management Agent a échoué en raison d'une erreur FSMAINST fatale. Reportez-vous au fichier journal de l'hôte afin d'obtenir des détails.

R. Un erreur d'installation fatale s'est produite lors de l'installation de F-Secure Management Agent. Il est recommandé de l'installer manuellement sur l'hôte. Vous pouvez également rechercher le mot clé ERREUR dans le fichier *fswssdbg.log* situé dans le répertoire Windows de l'hôte de destination.

Q. Produit F-Secure plus récent détecté, installation interrompue

R. Si une version plus récente d'un produit est installée sur l'hôte de destination, l'installation ne peut démarrer que lorsque celle-ci est désinstallée.

Q. Données incorrectes rencontrées dans prodsett.ini.

R. Le fichier de configuration *prodsett.ini* comporte des informations incorrectes. Si vous l'avez modifié manuellement, assurez-vous que la syntaxe utilisée est correcte. Pour l'installation, il est plutôt recommandé d'exporter les fichiers JAR à l'aide de la commande ILAUNCHR que de modifier directement *prodsett.ini*.

D ANNEXE : Notation NSC pour les masques de réseau

D.1 Présentation

La notation NSC est une norme de notation abrégée qui associe une adresse réseau au masque de réseau correspondant.

Elle définit le nombre de bits uniques contigus dans le masque de réseau en ajoutant après l'adresse réseau une barre oblique suivie d'un nombre. Vous pouvez voir un exemple simple ci-dessous :

Adresse réseau	Masque de réseau	Notation NSC
192.168.0.0	255.255.0.0	192.168.0.0/16
192.168.1.0	255.255.255.0	192.168.1.0/24
192.168.1.255	255.255.255.255	192.168.1.255/32

La notation NSC est incompatible avec les réseaux utilisant des masques de réseau de type « peigne » dans lesquels les bits uniques ne sont pas tous contigus. Le tableau suivant indique le nombre de bits pour chaque masque de réseau autorisé.

.0.0.0/0 est une définition de réseau spéciale réservée à l'itinéraire par défaut.

Masque de réseau	Bits	Masque de réseau	Bits
128.0.0.0	1	255.128.0.0	9
192.0.0.0	2	255.192.0.0	10
224.0.0.0	3	255.224.0.0	11
240.0.0.0	4	255.240.0.0	12
248.0.0.0	5	255.248.0.0	13
252.0.0.0	6	255.252.0.0	14
254.0.0.0	7	255.254.0.0	15
255.0.0.0	8	255.255.0.0	16

Masque de réseau	Bits	Masque de réseau	Bits
255.255.128.0	17	255.255.255.128	25
255.255.192.0	18	255.255.255.192	26
255.255.224.0	19	255.255.255.224	27
255.255.240.0	20	255.255.255.240	28
255.255.248.0	21	255.255.255.248	29
255.255.252.0	22	255.255.255.252	30
255.255.254.0	23	255.255.255.254	31
255.255.255.0	24	255.255.255.255	32

Support technique

Présentation

Le support technique est disponible par courrier électronique et 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

GLOSSAIRE

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.

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.

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.

Corrompu

Relatif à des données modifiées ou altérées sans l'autorisation ou l'accord de l'utilisateur.

Nom de domaine

Nom unique qui identifie un site Internet (par exemple, F-Secure.com).

DNS (système de nom de domaine)

Service qui convertit les noms de sites symboliques en adresses IP. Ce système utilise une base de données distribuée.

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.

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.

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.

Connexion

Nom du compte utilisé pour accéder au système d'un ordinateur.

Mbit

Mégabit.

MD5

Fonction de hachage sécurisé publiée dans le document RFC 1321.

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.

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.

Ping

Envoi de paquets ICMP et attente de paquets en réponse afin de vérifier les connexions vers un ou plusieurs ordinateurs distants.

Stratégie

Conditions requises pour que les utilisateurs d'un système puissent accéder aux ressources de ce système.

Gestion par stratégies

Contrôle des opérations et configuration d'un système à l'aide de stratégies.

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.

Protocole

Algorithme ou procédure pas à pas appliqué par plusieurs parties.

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.

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.

Serveur

Ordinateur ou composant logiciel qui fournit un type de service spécifique au logiciel client.

Service

Application qui s'exécute sur un hôte sans tenir compte de l'utilisateur connecté et qui propose des services à d'autres applications.

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 grande distance).

TCP/IP

(Transmission Control Protocol/Internet Protocol, ou protocole de contrôle de transmission/protocole Internet) Ensemble de protocoles qui définit 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.

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.

Base de données des définitions des virus

Base de données utilisée 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.

A propos de F-Secure Corporation

F-Secure Corporation protège les particuliers et les entreprises contre les virus informatiques et les autres menaces qui se répandent par le biais d'Internet et des réseaux de téléphonie mobile. Nous souhaitons devenir le fournisseur de services de sécurité le plus fiable du marché. La vitesse de notre réponse constitue l'un des éléments clés de cette réussite. Selon des études indépendantes réalisées en 2004, 2005 et 2006, notre délai de réponse aux nouvelles menaces est sensiblement plus court que celui de nos principaux concurrents. Nos solutions primées s'adaptent aux stations de travail, aux passerelles, aux serveurs et aux téléphones mobiles. Elles incluent des antivirus et des pare-feu pour ordinateur de bureau, tous dotés de solutions de prévention des intrusions, d'antispam et d'antispyware. Fondée en 1988, la société F-Secure est cotée sur le marché boursier d'Helsinki (Helsinki Exchanges) depuis 1999 et connaît une croissance supérieure à tous ses concurrents cotés à la bourse. Son siège social se trouve à Helsinki (Finlande) et la société possède des filiales dans le monde entier. La protection F-Secure est également disponible comme service par le biais des principaux fournisseurs de services Internet, tels que Deutsche Telekom, France Telecom, PCCW et Charter Communications. F-Secure est leader sur le marché mondial des solutions de protection pour téléphones mobiles, distribuées par les opérateurs mobiles comme T-Mobile et Swisscom, et par les fabricants comme Nokia. Retrouvez en temps réel les dernières menaces virales sur le blog de F-Secure Data Security Lab, à l'adresse suivante : http://www.f-secure.com/weblog/