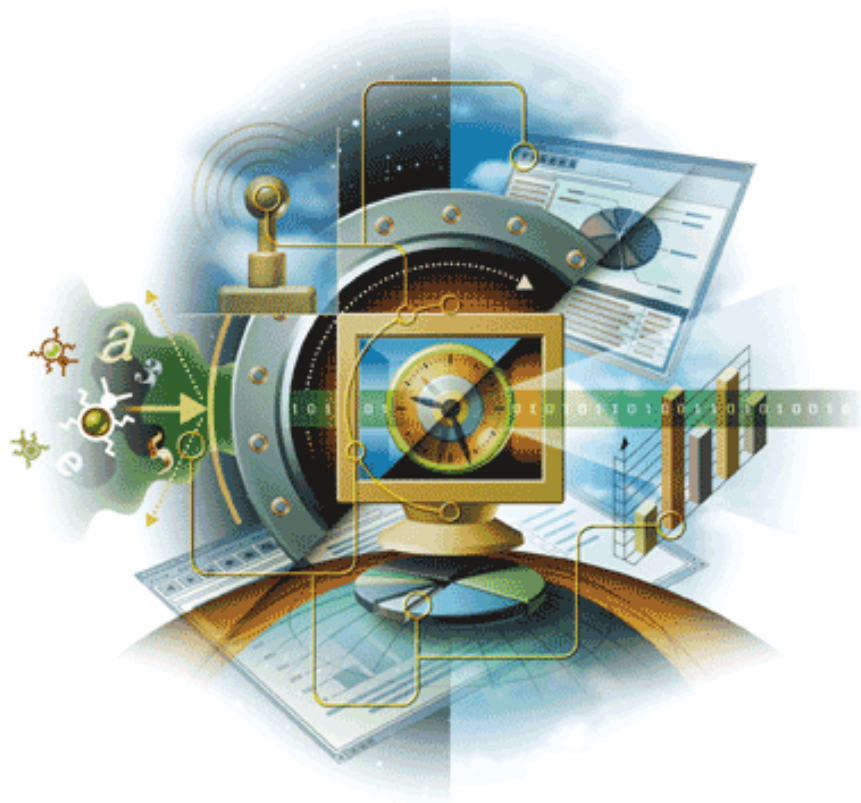


Virex®

version 7.6

A utiliser avec ePolicy Orchestrator



McAfee®
System Protection

Solutions de pointe du marché en matière de prévention des intrusions



COPYRIGHT

Copyright © 2004-2005 McAfee, Inc. Tous droits réservés.

Aucune partie de cette publication ne peut être reproduite, transmise, transcrite, stockée dans un système d'archivage ou traduite dans toute autre langue, sous quelque forme ou par quelque moyen que ce soit sans l'autorisation écrite de McAfee, Inc., de ses fournisseurs ou de ses sociétés affiliées. Pour obtenir cette autorisation, envoyez un courrier à l'attention du service juridique de McAfee à l'adresse suivante : 5000 Headquarters Drive, Plano, Texas 75024, USA, ou appelez au +1-972-963-8000.

MENTION DES MARQUES

Active Firewall, Active Security, ActiveSecurity (et en katakana), ActiveShield, AntiVirus Anyware et design, Clean-Up, Design (E stylisé), Design (N stylisé), Intercept, Enterprise SecureCast, Enterprise SecureCast (et en katakana), ePolicy Orchestrator, First Aid, ForceField, GMT, GroupShield, GroupShield (et en katakana), Guard Dog, HomeGuard, Hunter, IntruShield, Intrusion Prevention Through Innovation, M et design, McAfee, McAfee (et en katakana), McAfee et design, McAfee.com, McAfee VirusScan, NA Network Associates, Net Tools, Net Tools (et en katakana), NetCrypto, NetOctopus, NetScan, NetShield, Network Associates, Network Associates Colliseum, NetXray, NotesGuard, Nuts & Bolts, Oil Change, PC Medic, PCNotary, PrimeSupport, RingFence, Router PM, SecureCast, SecureSelect, SpamKiller, Stalker, ThreatScan, TIS, TMEG, Total Virus Defense, Trusted Mail, Uninstaller, Virex, Virus Forum, VirusScan, VirusScan (et en katakana), WebScan, WebShield, WebShield (et en katakana), WebStalker, WebWall, What's The State Of Your IDS?, Who's Watching Your Network, Your E-Business Defender, Your Network. Our Business. sont des marques déposées ou des marques de McAfee, Inc. et/ou de ses sociétés affiliées aux Etats-Unis et/ou dans d'autres pays. La couleur rouge utilisée pour identifier des fonctionnalités liées à la sécurité est propre aux produits de marque McAfee®. Toutes les autres marques, déposées ou non, mentionnées dans ce document sont la propriété exclusive de leurs détenteurs respectifs.

INFORMATIONS SUR LA LICENCE

Accord de licence

A L'ATTENTION DE TOUS LES UTILISATEURS : LISEZ ATTENTIVEMENT L'ACCORD JURIDIQUE CORRESPONDANT A LA LICENCE QUE VOUS AVEZ ACHETEE. IL DEFINIT LES CONDITIONS GENERALES D'UTILISATION DU LOGICIEL SOUS LICENCE. SI VOUS IGNOREZ LE TYPE DE LICENCE QUE VOUS AVEZ ACQUIS, REPORTEZ-VOUS AUX DOCUMENTS COMMERCIAUX ET AUTRES DOCUMENTS D'OCTROI DE LICENCE, OU AU BON DE COMMANDE, QUI ACCOMPAGNENT VOTRE PRODIGIEL OU QUI VOUS ONT ETE TRANSMIS SEPARATEMENT DANS LE CADRE DE VOTRE ACHAT (SOUS LA FORME D'UN LIVRET, D'UN FICHIER INCLUS SUR LE CD DU PRODUIT OU D'UN FICHIER DISPONIBLE SUR LE SITE WEB A PARTIR DUQUEL VOUS AVEZ TELECHARGE LE PRODIGIEL). SI VOUS N'ETES PAS D'ACCORD AVEC CERTAINS TERMES DE CET ACCORD, N'INSTALLEZ PAS LE LOGICIEL. LE CAS ECHEANT, VOUS POUVEZ RENVoyer LE PRODUIT A MCAFEE OU A L'ENDROIT OU VOUS L'AVEZ ACHETE AFIN D'EN OBTENIR LE REMBOURSEMENT INTEGRAL.

Mentions

Ce produit contient ou peut contenir :

- Composants logiciels développés dans le cadre du Projet OpenSSL et figurant dans le Toolkit OpenSSL (<http://www.openssl.org/>). • Composants logiciels cryptographiques écrits par Eric A. Young et composants logiciels écrits par Tim J. Hudson. • Certains programmes logiciels qui sont concédés sous licence (ou sous-licence) à l'utilisateur conformément à la Licence Publique Générale du GNU ou d'autres licences de logiciels gratuits similaires qui permettent notamment à l'utilisateur de copier, de modifier et de redistribuer certains programmes, ou parties de programmes, et d'avoir accès au code source. La GPL stipule que, pour tout logiciel couvert distribué à d'autres utilisateurs dans un format binaire exécutable, le code source doit également être mis à disposition. Pour tous ces logiciels couverts par la GPL, le code source est disponible sur ce CD. Si des licences de logiciels libres requièrent que McAfee accorde un droit d'utilisation, de copie ou de modification d'un logiciel plus étendu que celui octroyé dans cet accord, ce droit prime sur les droits et restrictions de cet accord. • Logiciel initialement écrit par Henry Spencer, Copyright 1992, 1993, 1994, 1997 Henry Spencer. • Logiciel initialement écrit par Robert Nordier, Copyright © 1996-7 Robert Nordier. • Logiciel écrit par Douglas W. Sauder. • Logiciel développé par Apache Software Foundation (<http://www.apache.org/>). Une copie de l'accord de licence de ce logiciel est disponible à l'adresse www.apache.org/licenses/LICENSE-2.0.txt. • International Components for Unicode (« ICU ») Copyright © 1995-2002 International Business Machines Corporation et autres. • Logiciel développé par CrystalClear Software, Inc., Copyright © 2000 CrystalClear Software, Inc. • Technologie FEAD® Optimizer®, Copyright Netop Systems AG, Berlin, Allemagne. • Outside In® Viewer Technology © 1992-2001 Stellent Chicago, Inc. et/ou Outside In® HTML Export, © 2001 Stellent Chicago, Inc. • Logiciel protégé par les droits d'auteur de Thai Open Source Software Center Ltd. et Clark Cooper, © 1998, 1999, 2000. • Logiciel protégé par les droits d'auteur d'Expat maintainers. • Logiciel protégé par les droits d'auteur de The Regents of the University of California, © 1989. • Logiciel protégé par les droits d'auteur de Gunnar Ritter. • Logiciel protégé par les droits d'auteur de Sun Microsystems®, Inc. © 2003. • Logiciel protégé par les droits d'auteur de Gisle Aas. © 1995-2003. • Logiciel protégé par les droits d'auteur de Michael A. Chase, © 1999-2000. • Logiciel protégé par les droits d'auteur de Neil Winton, © 1995-1996. • Logiciel protégé par les droits d'auteur de RSA Data Security, Inc., © 1990-1992. • Logiciel protégé par les droits d'auteur de Sean M. Burke, © 1999, 2000. • Logiciel protégé par les droits d'auteur de Martijn Koster, © 1995. • Logiciel protégé par les droits d'auteur de Brad Appleton, © 1996-1999. • Logiciel protégé par les droits d'auteur de Michael G. Schwern, © 2001. • Logiciel protégé par les droits d'auteur de Graham Barr, © 1998. • Logiciel protégé par les droits d'auteur de Larry Wall et Clark Cooper, © 1998-2000. • Logiciel protégé par les droits d'auteur de Frodo Looijaard, © 1997. • Logiciel protégé par les droits d'auteur de la Python Software Foundation, Copyright © 2001, 2002, 2003. Une copie de l'accord de licence de ce logiciel est disponible à l'adresse www.python.org. • Logiciel protégé par les droits d'auteur de Beman Dawes, © 1994-1999, 2002. • Logiciel écrit par Andrew Lumsdaine, Lie-Quan Lee, Jeremy G. Siek © 1997-2000 University of Notre Dame. • Logiciel protégé par les droits d'auteur de Simone Bordet et Marco Cravero, © 2002. • Logiciel protégé par les droits d'auteur de Stephen Purcell, © 2001. • Logiciel développé par Indiana University Extreme! Lab (<http://www.extreme.indiana.edu/>). • Logiciel protégé par les droits d'auteur de International Business Machines Corporation et autres, © 1995-2003. • Logiciel développé par l'University of California, Berkeley et ses donateurs. • Logiciel développé par Ralf S. Engelschall <rse@engelschall.com> dans le cadre du projet mod_ssl (<http://www.modssl.org/>). • Logiciel protégé par les droits d'auteur de Kevlin Henney, © 2000-2002. • Logiciel protégé par les droits d'auteur de Peter Dimov et Multi Media Ltd. © 2001, 2002. • Logiciel protégé par les droits d'auteur de David Abrahams, © 2001, 2002. Consultez le site <http://www.boost.org/libs/bind/bind.html> pour obtenir de la documentation. • Logiciel protégé par les droits d'auteur de Steve Cleary, Beman Dawes, Howard Hinnant et John Maddock, © 2000. • Logiciel protégé par les droits d'auteur de Boost.org, © 1999-2002. • Logiciel protégé par les droits d'auteur de Nicolai M. Josuttis, © 1999. • Logiciel protégé par les droits d'auteur de Jeremy Siek, © 1999-2001. • Logiciel protégé par les droits d'auteur de Daryle Walker, © 2001. • Logiciel protégé par les droits d'auteur de Chuck Allison et Jeremy Siek, © 2001, 2002. • Logiciel protégé par les droits d'auteur de Samuel Kremp, © 2001. Consultez le site <http://www.boost.org> pour obtenir des mises à jour, de la documentation et l'historique des révisions. • Logiciel protégé par les droits d'auteur de Doug Gregor (gregod@cs.rpi.edu), © 2001, 2002. • Logiciel protégé par les droits d'auteur de Cadenza New Zealand Ltd., © 2000. • Logiciel protégé par les droits d'auteur de Jens Maurer, © 2000, 2001. • Logiciel protégé par les droits d'auteur de Jaakko Järvi (jaakko.jarvi@cs.utu.fi), © 1999, 2000. • Logiciel protégé par les droits d'auteur de Ronald Garcia, © 2002. • Logiciel protégé par les droits d'auteur de David Abrahams, Jeremy Siek et Daryle Walker, © 1999-2001. • Logiciel protégé par les droits d'auteur de Stephen Cleary (shammah@voyager.net), © 2000. • Logiciel protégé par les droits d'auteur de Housemarque Oy <<http://www.housemarque.com>>, © 2001. • Logiciel protégé par les droits d'auteur de Paul Moore, © 1999. • Logiciel protégé par les droits d'auteur du Dr. John Maddock, © 1998-2002. • Logiciel protégé par les droits d'auteur de Greg Colvin et Beman Dawes, © 1998, 1999. • Logiciel protégé par les droits d'auteur de Peter Dimov, © 2001, 2002. • Logiciel protégé par les droits d'auteur de Jeremy Siek et John R. Bandela, © 2001. • Logiciel protégé par les droits d'auteur de Joerg Walter et Mathias Koch, © 2000-2002.

Sommaire

1	Introduction	5
	Contenu du guide	5
	Configuration requise pour l'utilisation d'ePolicy Orchestrator pour gérer Virex	6
	Présentation de la console ePolicy Orchestrator	6
	Public concerné	7
	Conventions	7
	Ressources	8
	Obtention d'informations sur le produit	8
	Liens internes au produit	9
	Services liés aux produits	10
	Contacts	11
2	Installation	13
	Introduction	13
	Configuration système requise	13
	Configuration de la console ePolicy Orchestrator pour la gestion de Virex 7.6	13
	Enregistrement des fichiers .NAP pour la gestion de Virex 7.6	14
	Installation de l'agent sur les systèmes Macintosh	17
	Répertoire d'installation de l'agent	17
	Installation de l'agent	18
	Installation de Virex 7.6	24
	Désinstallation	24
	Suppression des fichiers NAP Virex du serveur ePolicy Orchestrator	24
	Suppression de l'agent ePolicy Orchestrator du serveur ePolicy Orchestrator	25
	Désinstallation de l'agent ePolicy Orchestrator de Mac OS X	25
3	Définition des stratégies ePolicy Orchestrator pour Virex 7.6	27
	Définition des stratégies dans ePolicy Orchestrator	27
	Général	30
	eUpdate	31
	Analyseur actif	32
	Analyseur en arrière-plan	33
	Analyseur de volumes installés	34
	Analyseur à la demande	35
	Planification des analyses et des mises à jour automatiques via eUpdate	36
	A propos des tâches planifiées	36
	eUpdate	41
	Affichage des propriétés du serveur ePolicy Orchestrator	43
4	Contrôle de l'agent à distance	45
	Affichage des propriétés de l'agent	45
	Application des stratégies pour un agent ePolicy Orchestrator	46
	Options de l'agent	46
	Événements	47
	Affichage des événements du serveur	50
	Consignation	51

5	Rapports	53
	Rapports	53
	Configuration des rapports	54
	Glossaire	55
	Index	59

1

Introduction

Contenu du guide

Ce guide indique comment configurer Virex 7.6 en utilisant le logiciel de gestion McAfee ePolicy Orchestrator version 3.0.2 et ultérieure. Pour utiliser efficacement ce guide, vous devez déjà bien connaître le logiciel ePolicy Orchestrator. Pour plus d'informations, consultez le *Guide produit d'ePolicy Orchestrator*. Le logiciel ePolicy Orchestrator fournit un point de contrôle unique pour tous vos produits antivirus McAfee, vous permettant de gérer toutes les stratégies antivirus et d'afficher les rapports sur les événements antivirus et l'activité des virus dans un environnement d'entreprise. Avec ePolicy Orchestrator, vous pouvez configurer Virex sur les ordinateurs cible de votre réseau ; vous n'avez pas besoin de les configurer individuellement à partir de la boîte de dialogue **Préférences** de Virex.

Ce guide contient les informations suivantes :

- Ajout d'une configuration d'agent ePolicy Orchestrator au serveur ePolicy Orchestrator.
- Définition des stratégies antivirus sur les systèmes cible, en vue de configurer les fonctions de Virex suivantes :
 - Stratégies générales de contrôle des fonctions globales de Virex.
 - Stratégies du serveur eUpdate.
 - Stratégies de l'analyseur actif.
 - Stratégies de l'analyseur en arrière-plan.
 - Stratégies de l'analyseur de volumes montés.
 - Stratégies de l'analyseur à la demande.
- Configuration de l'agent ePolicy Orchestrator pour Mac OS X.
 - Intervalles de communication de l'agent.
 - Intervalles d'application des stratégies.
 - Transmission des événements.
 - Consignation.



Ce guide ne fournit pas d'informations détaillées sur l'installation et l'utilisation du logiciel ePolicy Orchestrator. Ces informations figurent dans le *Guide produit d'ePolicy Orchestrator*.

Configuration requise pour l'utilisation d'ePolicy Orchestrator pour gérer Virex

Pour que le logiciel ePolicy Orchestrator puisse configurer Virex :

- Enregistrez le fichier Virex 7.6 NAP dans le référentiel du logiciel ePolicy Orchestrator.
- Enregistrez le fichier¹ de l'agent non-Windows dans ePolicy Orchestrator.
- Installez Virex sur le système Macintosh.
- Installez l'agent ePolicy Orchestrator sur le système Macintosh.

Présentation de la console ePolicy Orchestrator

La console de gestion Microsoft (MMC) est l'interface utilisée pour exploiter ePolicy Orchestrator et ses différentes fonctions. Elle permet d'enregistrer et de configurer les produits antivirus Virex gérés via ePolicy Orchestrator.

Lorsque vous vous connectez pour la première fois au serveur, la console s'affiche et sa racine apparaît en surbrillance dans le volet gauche. L'apparence de la console change en fonction des éléments sélectionnés dans l'arborescence de la console ou le volet des détails. La console utilise les fonctionnalités standard de la console MMC.

Sous les menus situés en haut de la fenêtre, la console est divisée en deux panneaux ou volets.

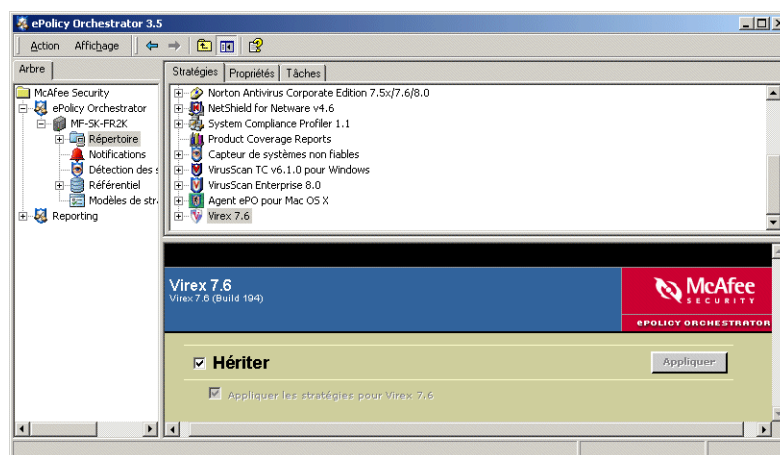


Figure 1-1 Console ePolicy Orchestrator

- L'**arborescence de la console** est située à gauche de la console. Elle affiche les serveurs, les postes de travail et les périphériques que vous pouvez administrer.
- Le **volet de détails** occupe la partie droite de la console. Selon l'élément de l'arborescence de la console sélectionné, le volet de détails peut être divisé en volets **supérieur** et **inférieur**.






¹ L'agent non-Windows (NWA - Non Windows Agent) est également connu sous le nom d'Agent ePolicy Orchestrator sous Mac OS X.

Public concerné

Ce guide est conçu à l'attention des administrateurs système et des administrateurs de réseau responsables de la gestion du programme antivirus de leur société.

Conventions

Ce guide utilise les conventions suivantes :

Bold Serif	Tous les termes apparaissant sur l'interface utilisateur, y compris les noms d'options, de menus, de boutons et de boîtes de dialogue. Exemple : Entrez le Nom d'utilisateur et le Mot de passe du compte demandé.
Courier	Chemin d'un dossier ou d'un programme ; adresse Web (URL) ; texte que l'utilisateur saisit lui-même (par exemple, une commande à l'invite du système). Exemples : L'emplacement par défaut du programme est le suivant : C:\Program Files\McAfee\EPO\3.5.0 Visitez le site Web de McAfee à l'adresse : http://www.mcafee.com Exécutez cette commande sur l'ordinateur client : C:\SETUP.EXE
<i>Italiques</i>	Introduction d'un nouveau terme ; emphase ; titres des manuels et des rubriques (têtes de chapitre) dans la documentation des produits. Exemple : Pour plus d'informations, consultez le <i>Guide produit de Virex 7.6</i> .
<TERME>	Des chevrons encadrent les termes génériques. Exemple : Dans l'arborescence de la console, sous ePolicy Orchestrator , cliquez avec le bouton droit de la souris sur <SERVEUR>.
	Remarque : information complémentaire, par exemple, une autre méthode pour exécuter la même commande.
	Astuce : conseils et recommandations de McAfee en matière de prévention des menaces, de performances et d'efficacité.
	Attention : conseils importants destinés à protéger votre système informatique, votre entreprise, votre installation logicielle ou vos données.
	Avertissement : conseil important pour mettre en garde un utilisateur contre des blessures corporelles lors de l'utilisation ou de la manipulation d'un produit matériel.
	Nouveau : fonction ou option qui n'existait pas dans les versions antérieures du produit ou qui a été repensée et améliorée.

Ressources

Les produits McAfee® sont le fruit d'une expérience acquise au fil des ans et d'une volonté constante de satisfaire la clientèle. L'équipe McAfee PrimeSupport® réunit des techniciens de support hautement qualifiés, rompus aux interventions rapides, pour vous offrir des solutions sur mesure et une assistance technique de nature à assurer la réussite de vos projets critiques, avec un niveau de service répondant aux besoins de chaque entreprise. McAfee Research, leader mondial en matière de systèmes d'information et de sécurité, reste à la pointe de l'innovation en termes de développement et de perfectionnement de toutes nos technologies.

Pour plus d'informations, reportez-vous aux sections suivantes :

- Obtention d'informations sur le produit.
- Liens internes au produit.
- Services liés aux produits.
- Contacts.

Obtention d'informations sur le produit

Sauf indication contraire, la documentation relative au produit est proposée sous la forme de fichiers au format .PDF sur le CD du produit ou sur le site de téléchargement de McAfee.

Guide produit : présentation du produit et de ses fonctionnalités, instructions détaillées pour la configuration du logiciel, informations sur le déploiement, les tâches récurrentes et les procédures.

- *Guide produit Virex 7.6*

Aide : informations générales et détaillées accessibles depuis l'application.

Guide de configuration : à utiliser avec *ePolicy Orchestrator*®. Procédures de déploiement et d'administration des produits Virex via le logiciel de gestion ePolicy Orchestrator.

Notes de version[^] : fichier *Ouvrez-moi*. Informations sur le produit, description des problèmes résolus, liste des problèmes connus et ajouts ou corrections de dernière minute apportés au produit ou à sa documentation.

Contacts[^] : informations permettant de contacter les services et ressources McAfee, à savoir support technique, service clientèle, Security HQ (centre de recherche AVERT), programme bêta et formation. Ce fichier contient également les numéros de téléphone et de fax, les adresses postales et les adresses web des bureaux de la société aux Etats-Unis et dans le monde entier.

Licence : livret de l'accord de licence McAfee, comprenant tous les types de licence disponibles pour le produit concerné. Cet accord définit les conditions générales d'utilisation du logiciel sous licence.

* Guide imprimé qui accompagne le CD du produit. Remarque : dans certaines langues, les manuels ne sont disponibles qu'au format .PDF.

[^] Fichiers texte fournis avec l'application logicielle et sur le CD du produit.

Liens internes au produit

Le produit propose des liens vers des ressources particulièrement utiles :

- Aide en ligne.
- Bibliothèque d'informations sur les virus.
- Support technique pour ePolicy Orchestrator.
- Outil MER.
- AVERT Web Immune.
- Page d'accueil de McAfee.

Aide en ligne

Ce lien donne accès aux rubriques de l'aide en ligne du logiciel.



Si le système d'aide intégré au logiciel (accessible depuis le menu **Aide**) ne s'affiche pas correctement sur votre ordinateur, il se peut que votre version de Microsoft® Internet Explorer ne prenne pas correctement en charge les contrôles ActiveX. Ces derniers sont requis pour l'affichage du fichier d'aide. Installez la dernière version d'Internet Explorer.

Bibliothèque d'informations sur les virus

Le lien **Virus Information Library** vous connecte à la bibliothèque d'informations sur les virus du centre AVERT (Anti-virus & Vulnerability Emergency Response Team) de McAfee. Ce site Web rassemble des données détaillées sur l'origine des virus, leurs modes de propagation et les procédures permettant de les éliminer.

Outre les informations sur les véritables virus, cette bibliothèque contient des renseignements utiles sur les canulars, tels que les avertissements de virus envoyés par e-mail. Parmi les innombrables exemples de canulars de ce type, citons *Virtual Card For You* et *SULFNBK*. La prochaine fois que vous recevrez un avertissement bien intentionné signalant l'existence d'un virus, consultez la page de la bibliothèque consacrée aux canulars avant de transmettre le message à vos amis.

Pour accéder à la bibliothèque d'informations sur les virus :

- 1 Ouvrez ePolicy Orchestrator.
- 2 Sur la **Page de départ**, sélectionnez le lien **Virus Information Library**.

Support technique pour ePolicy Orchestrator

Le lien **Support technique** vous donne accès au site web PrimeSupport ServicePortal (KnowledgeCenter) de McAfee. Parcourez ce site pour consulter les questions fréquemment posées ou la documentation, et pour utiliser la fonction de recherche assistée dans notre base de connaissances.

- 1 Ouvrez ePolicy Orchestrator.
- 2 Sur la **Page de départ**, cliquez sur le lien **Support technique pour ePolicy Orchestrator**.

Outil MER

Le lien vers l'outil MER vous donne accès au site web PrimeSupport ServicePortal (KnowledgeCenter) de McAfee. Connectez-vous au site de support pour enregistrer les escalades.

- 1 Ouvrez ePolicy Orchestrator.
- 2 Sur la **Page de départ**, cliquez sur le lien **Outil MER**.

AVERT Web Immune

Le lien AVERT Web Immune vous connecte au site web Avert Web Immune.

- 1 Ouvrez ePolicy Orchestrator.
- 2 Sur la **Page de départ**, cliquez sur le lien **AVERT Web Immune**.

Page d'accueil de McAfee

Le lien Page d'accueil de McAfee Security vous permet d'accéder directement à la page d'accueil du site Web McAfee Security.

- 1 Ouvrez ePolicy Orchestrator.
- 2 Sur la **Page de départ**, cliquez sur le lien **Page d'accueil McAfee Security**.

Services liés aux produits

Les services suivants vous aident à tirer le meilleur parti de vos produits McAfee :

- Programme bêta.
- Correctifs (HotFix) et patches.
- Support des produits en fin de vie.

Programme bêta

Le programme bêta de McAfee vous permet d'essayer nos produits avant leur distribution définitive auprès du public. Vous pouvez ainsi découvrir et tester les nouvelles fonctionnalités des produits existants ou essayer les nouveaux produits. Les utilisateurs participant à ce programme peuvent tester et mettre en œuvre, plus tôt que les autres, des fonctions mises à jour ou inédites, dans un environnement sûr. Ils peuvent en outre nous suggérer d'inclure de nouvelles fonctions ou traiter directement avec les techniciens McAfee.

Pour plus d'informations, visitez notre site à l'adresse :

<http://www.mcafeesecurity.com/us/downloads/beta/mcafeebetahome.htm>

Correctifs (HotFix) et patches

Les correctifs (HotFix) et les patches mettent à la disposition des utilisateurs des éléments mis à jour tels que fichiers, pilotes ou exécutables, avant la distribution d'une version principale d'un produit. Pour accéder aux derniers HotFix et patches, visitez notre site à l'adresse :

<http://www.mcafeesecurity.com/us/downloads/updates/hotfixes.asp>

Support des produits en fin de vie

Vos logiciels antivirus doivent être tenus à jour pour rester efficaces contre les virus et les autres codes et logiciels potentiellement nuisibles. Il est important de mettre à jour régulièrement vos fichiers de définitions de virus (fichiers DAT). Pour que votre logiciel puisse contrer les menaces en permanence, nous apportons fréquemment des modifications structurelles au fonctionnement conjoint des fichiers DAT et du moteur d'analyse antivirus. Il est donc essentiel d'actualiser le moteur dès qu'une nouvelle version est publiée. Si vous utilisez un moteur devenu obsolète, un grand nombre des nouvelles menaces émergentes ne seront pas détectées.

Lorsque nous publions un nouveau moteur, nous communiquons la date après laquelle le moteur existant ne sera plus pris en charge. Pour connaître notre politique relative à la fin de vie des produits et consulter la liste des moteurs et produits supports, visitez notre site à l'adresse :

http://www.mcafeesecurity.com/us/products/mcafee/end_of_life.htm

Contacts

Support technique

Page d'accueil	http://www.mcafeesecurity.com/fr/support/technical_support
Recherche dans la base de connaissances	https://knowledgemap.nai.com/phpclient/homepage.aspx
Portail de services PrimeSupport*	https://mysupport.nai.com

Programme bêta de McAfee

<http://www.mcafeesecurity.com/us/downloads/beta/mcafeebetahome.htm>

Security Headquarters — AVERT (Anti-virus & Vulnerability Emergency Response Team)

Page d'accueil	http://www.mcafeesecurity.com/fr/security/home.asp
Bibliothèque d'informations sur les virus	http://vil.nai.com
AVERT WebImmune, * envoi d'échantillons	https://www.webimmune.net/default.asp
Service AVERT de notification de fichiers DAT	http://vil.mcafeesecurity.com/vil/join-DAT-list.asp

Site de téléchargement

Page d'accueil	http://www.mcafeesecurity.com/fr/downloads/
Mises à jour des fichiers DAT et du moteur d'analyse	http://www.mcafeesecurity.com/fr/downloads/
	ftp://ftp.mcafeesecurity.com/pub/antivirus/datfiles/4.x
Mises à niveau des produits*	https://secure.nai.com/fr/forms/downloads/upgrades/login.asp

Formation

Formation sur site	http://www.mcafeesecurity.com/fr/services/security/home.htm
Université McAfee	http://www.mcafeesecurity.com/fr/services/education/mcafee/university.htm

Service clientèle

E-mail	https://secure.nai.com/fr/forms/support/request_form.asp
Web	http://www.mcafeesecurity.com/fr/index.asp http://www.mcafeesecurity.com/fr/support/default.asp
Numéro vert pour les Etats-Unis, le Canada et l'Amérique latine :	+1-888-VIRUS NO ou +1-888-847-8766 Du lundi au vendredi, de 8 heures à 20 heures (Heure du centre)

Pour plus d'informations sur les contacts McAfee (notamment les numéros verts des autres régions géographiques), reportez-vous au fichier Contact qui accompagne cette version du produit.

* Informations de connexion obligatoires.

2 Installation

Introduction

L'agent est un composant distribué d'ePolicy Orchestrator installé sur chaque ordinateur Macintosh du réseau. Il collecte et envoie des informations entre le serveur ePolicy Orchestrator et les référentiels, et gère les installations Virex 7.6 sur tout le réseau. La configuration de l'agent et de ses paramètres de stratégie détermine la façon dont il simplifie la communication et les mises à jour au sein de votre environnement.

Configuration système requise

L'agent peut être installé sur les systèmes d'exploitation Macintosh tels que :

- MAC OS 10.2.6
- MAC OS 10.2.8
- MAC OS 10.3.x

ainsi que sur chacune des plates-formes Macintosh suivantes :

- G3
- G4
- G5

Configuration de la console ePolicy Orchestrator pour la gestion de Virex 7.6

Lorsqu'un agent ePolicy Orchestrator est installé en intégralité sur un ordinateur, vous pouvez utiliser en toute simplicité la fonctionnalité de génération de rapports. Pour configurer la génération de rapports sur vos ordinateurs :

- Vérifiez que vous avez configuré l'adresse IP et le port du serveur ePolicy Orchestrator à partir de l'interface utilisateur du configurateur ePolicy Orchestrator de l'ordinateur client.

Enregistrement des fichiers .NAP pour la gestion de Virex 7.6

Fichier .NAP (Network Associate Package) : l'extension .NAP désigne les fichiers programme du logiciel McAfee installés dans le référentiel logiciel à des fins de gestion par ePolicy Orchestrator. Le serveur ePolicy Orchestrator s'installe avec l'ensemble des pages de stratégies relatives aux principaux produits pris en charge disponibles à la publication de votre version de ePolicy Orchestrator. Pour gérer Virex 7.6, vous devez tout d'abord ajouter les fichiers .NAP appropriés au référentiel logiciel.

Recherche des fichiers *.NAP de Virex 7.6 à ajouter au référentiel

McAfee distribue des fichiers .NAP pour tous les antivirus et produits de sécurité pris en charge par ePolicy Orchestrator. Le fichier .NAP d'un produit donné se situe, à l'instar des autres fichiers d'installation, sur le CD du produit ou dans le fichier ZIP du produit, téléchargé depuis le site Web de McAfee. Les fichiers .NAP correspondant à Virex 7.6 sont disponibles dans le sous-dossier **ePolicy Orchestrator Server Components** du CD du produit ou du fichier ZIP téléchargé. Le fichier .NAP possède toujours l'extension .NAP. Son nom correspond au code du nom du produit suivi du numéro de version, par exemple NWA-MAC300.NAP.

Les pages de stratégie ne sont pas ajoutées au référentiel maître, mais stockées sur le serveur ePolicy Orchestrator. Par conséquent, les fichiers NAP ne sont ni répliqués sur les référentiels distribués, ni mis à jour sur les ordinateurs Macintosh.

Ajout du fichier .NAP de l'agent Macintosh non-Windows (NWA)

Pour enregistrer le fichier NAP d'un agent Macintosh non-Windows sur le serveur ePolicy Orchestrator :

- 1 Localisez le fichier NAP sur le CD du produit ou dans le fichier ZIP téléchargé depuis le site Web de McAfee, puis enregistrez-le dans un dossier temporaire accessible à partir du serveur ePolicy Orchestrator.
- 2 Connectez-vous au serveur ePolicy Orchestrator avec des droits d'administrateur.
- 3 Dans l'arborescence de la console ePolicy Orchestrator, cliquez avec le bouton droit de la souris sur le **Référentiel** puis sélectionnez **Configurer le référentiel**. L'Assistant **Configuration du Référentiel de logiciels** s'affiche.



Figure 2-1 Assistant Configuration du Référentiel de logiciels



Lorsque vous double-cliquez sur **Référentiel** dans l'arborescence de la console ePolicy Orchestrator, puis que vous cliquez sur le lien **Archiver NAP** dans le volet de détails, l'Assistant **Configuration du Référentiel de logiciels** s'affiche.

- 4 Dans l'Assistant **Configuration du Référentiel de logiciels**, sélectionnez **Ajout de nouveaux logiciels à gérer**, puis cliquez sur **Suivant**.

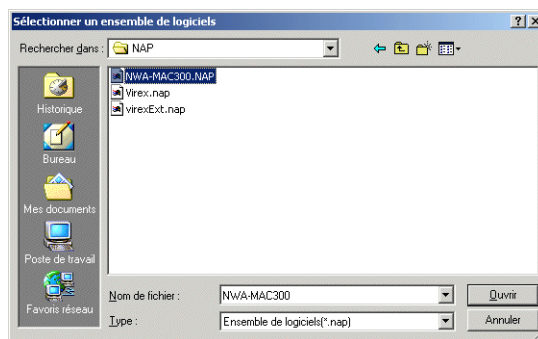


Figure 2-2 Boîte de dialogue Sélectionner un ensemble de logiciels

- 5 Dans la boîte de dialogue **Sélectionner un ensemble de logiciels**, sélectionnez le fichier **NWA-MAC300.NAP** que vous avez placé dans un dossier temporaire à l'étape 1.
- 6 Cliquez sur **Ouvrir** pour permettre à ePolicy Orchestrator de charger le fichier .NAP.

Ajout d'un fichier .NAP Virex

Pour ajouter un fichier .NAP Virex sur le serveur ePolicy Orchestrator :

- 1 Localisez le fichier .NAP sur le CD du produit ou dans le fichier ZIP téléchargé depuis le site Web de McAfee, puis enregistrez-le dans un dossier temporaire accessible à partir du serveur ePolicy Orchestrator.
- 2 Connectez-vous au serveur ePolicy Orchestrator avec des droits d'administrateur.
- 3 Dans l'arborescence de la console ePolicy Orchestrator, cliquez avec le bouton droit de la souris sur le **Référentiel** puis sélectionnez **Configurer le référentiel**. L'Assistant **Configuration du Référentiel de logiciels** s'affiche.



Figure 2-3 Assistant Configuration du Référentiel de logiciels



Lorsque vous double-cliquez sur **Référentiel** dans l'arborescence de la console ePolicy Orchestrator, puis que vous cliquez sur le lien **Archiver NAP** dans le volet de détails, l'Assistant **Configuration du Référentiel de logiciels** s'affiche.

- 4 Dans l'Assistant **Configuration du Référentiel de logiciels**, sélectionnez **Ajout de nouveaux logiciels à gérer**, puis cliquez sur **Suivant**.

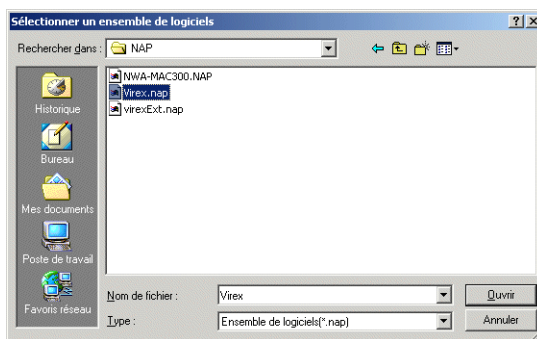


Figure 2-4 Boîte de dialogue Sélectionner un ensemble de logiciels

- 5 Dans la boîte de dialogue **Sélectionner un ensemble de logiciels**, sélectionnez le fichier **Virex.NAP** que vous avez enregistré dans un dossier temporaire à l'étape 1.
- 6 Cliquez sur **Ouvrir** pour permettre à ePolicy Orchestrator de charger le fichier .NAP.

Ajout d'un fichier .NAP de rapports

Pour ajouter un fichier .NAP de rapports sur le serveur ePolicy Orchestrator :

- 1 Localisez le fichier .NAP sur le CD du produit ou dans le fichier ZIP téléchargé depuis le site Web de McAfee, puis enregistrez-le dans un dossier temporaire accessible à partir du serveur ePolicy Orchestrator.
- 2 Connectez-vous au serveur ePolicy Orchestrator avec des droits d'administrateur.
- 3 Dans l'arborescence de la console ePolicy Orchestrator, cliquez avec le bouton droit de la souris sur le **Référentiel** puis sélectionnez **Configurer le référentiel**. L'Assistant **Configuration du Référentiel de logiciels** s'affiche.



Figure 2-5 Assistant Configuration du Référentiel de logiciels



Lorsque vous double-cliquez sur **Référentiel** dans l'arborescence de la console ePolicy Orchestrator, puis que vous cliquez sur le lien **Archiver NAP** dans le volet de détails situé à droite, l'Assistant **Configuration du Référentiel de logiciels** s'affiche.

- 4 Dans l'Assistant **Configuration du Référentiel de logiciels**, sélectionnez **Ajout de nouveaux rapports** et cliquez sur **Suivant**.

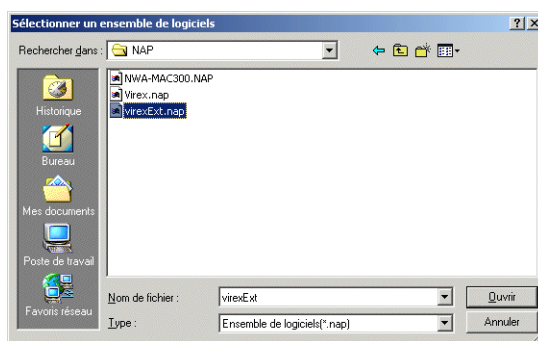


Figure 2-6 Boîte de dialogue Sélectionner un ensemble de logiciels

- 5 Dans la boîte de dialogue **Sélectionner un ensemble de logiciels**, sélectionnez le fichier **VirexExt.NAP** que vous avez enregistré dans un dossier temporaire à l'**étape 1**, puis cliquez sur **Ouvrir** pour permettre à ePolicy Orchestrator de charger le fichier .NAP de rapports dans le référentiel.

Lorsque ePolicy Orchestrator a terminé de charger les fichiers .NAP, l'agent s'affiche dans la liste des stratégies, qui occupe la partie supérieure du volet de détails.

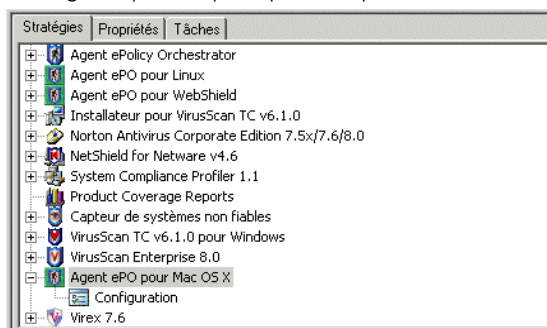


Figure 2-7 Onglet Stratégies

Installation de l'agent sur les systèmes Macintosh

Répertoire d'installation de l'agent

L'agent est installé dans le dossier /Library/NETAepoagt et utilise le dossier /Library/NETASSOC pour toutes les informations relatives à la configuration.



Il est impossible de modifier le répertoire d'installation de l'agent ePolicy Orchestrator sous Macintosh OS X.

Installation de l'agent

Vous pouvez installer l'agent ePolicy Orchestrator pour Macintosh via une installation standard (interface graphique) ou une ligne de commande (installation silencieuse).

Installation standard

- 1 Recherchez le fichier **nwa.dmg** qui figure sur le CD du produit ou dans le fichier ZIP d'installation téléchargé depuis le site Web McAfee, puis enregistrez-le dans un répertoire temporaire.



Ce fichier se trouve dans le répertoire **ePO Agent** du fichier **ePO Components.ZIP** sur le CD du produit.

- 2 Double-cliquez sur **nwa.dmg** pour extraire les fichiers suivants :
 - NWA.pkg
 - cmdinstall
- 3 Double-cliquez sur **NWA.pkg**. La fenêtre **Bienvenue dans le programme d'installation de l'agent ePO pour Mac OS X** apparaît :

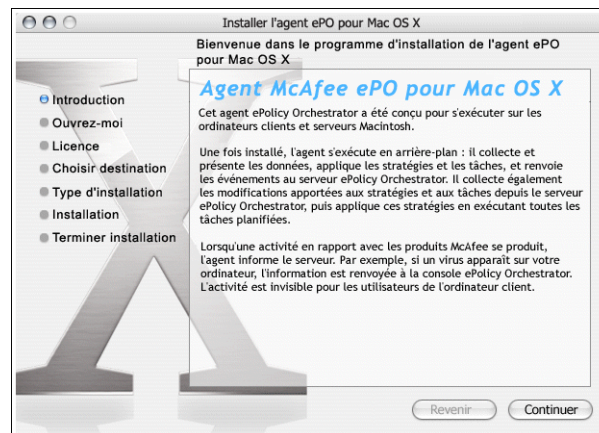


Figure 2-8 Fenêtre d'installation de l'agent ePO - Introduction

- 4 Cliquez sur **Continuer**. La fenêtre **Ouvrez-moi** apparaît. Elle décrit les fonctions de l'agent, et répertorie tous les comportements et problèmes connus avec la présente version du produit.



Figure 2-9 Fenêtre d'installation de l'agent ePO - Ouvrez-moi

- 5 Cliquez sur **Continuer**. La fenêtre **Contrat de licence** apparaît.

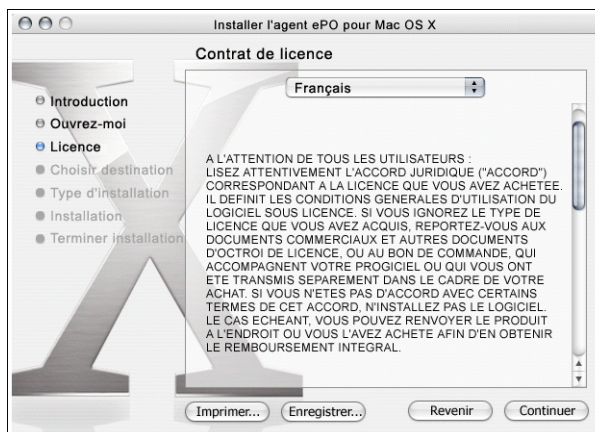


Figure 2-10 Fenêtre d'installation de l'agent ePO - Licence



Lisez et acceptez le contrat de licence. Si vous n'êtes pas d'accord avec ses conditions, vous ne pourrez pas poursuivre l'installation.

- 6 Cliquez sur **Continuer**. La fenêtre **Sélectionnez un volume de destination** apparaît.

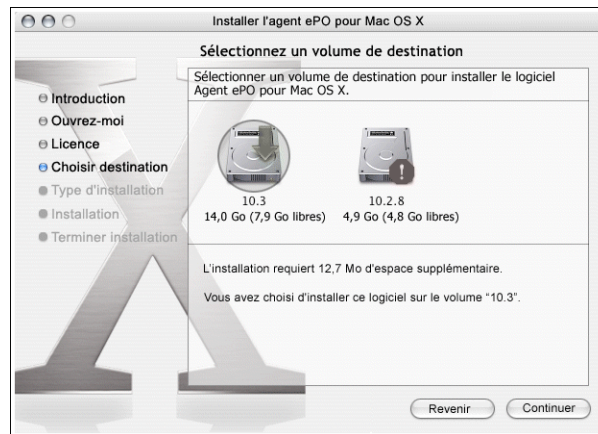


Figure 2-11 Fenêtre d'installation de l'agent ePO - Sélectionnez un volume de destination

Sélectionnez le répertoire dans lequel vous souhaitez installer l'agent ePolicy Orchestrator, puis cliquez sur **Continuer**. La fenêtre **Installation simplifiée** apparaît.

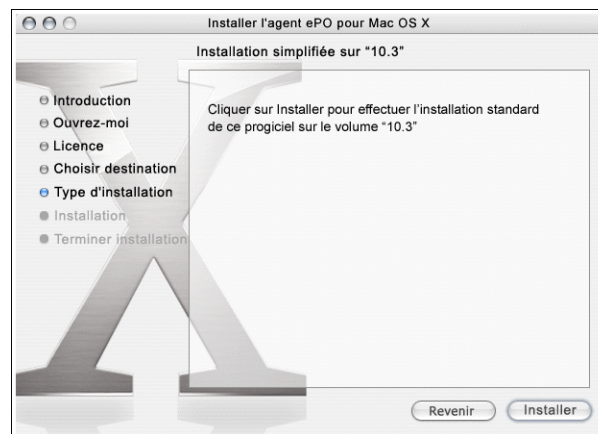


Figure 2-12 Assistant d'installation de l'agent ePO - Installation simplifiée



La fenêtre **Installation simplifiée** contenant le bouton **Installer** apparaît lorsque :

- Vous installez l'agent pour la première fois.
- Vous réinstallez l'agent après avoir désinstallé la précédente version de l'agent ePolicy Orchestrator.

Si vous mettez à niveau l'agent ePolicy Orchestrator, la fenêtre suivante apparaît.

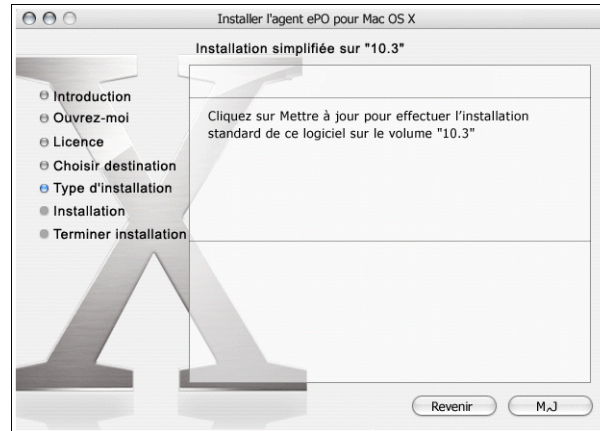


Figure 2-13 Fenêtre d'installation de l'agent ePO - Mise à niveau de l'installation

- 7 Cliquez sur **M.J** pour continuer. Le programme d'installation vous demande de vous authentifier avant de continuer. Saisissez votre mot de passe, puis cliquez sur **OK**. La fenêtre **Installation du logiciel** apparaît.

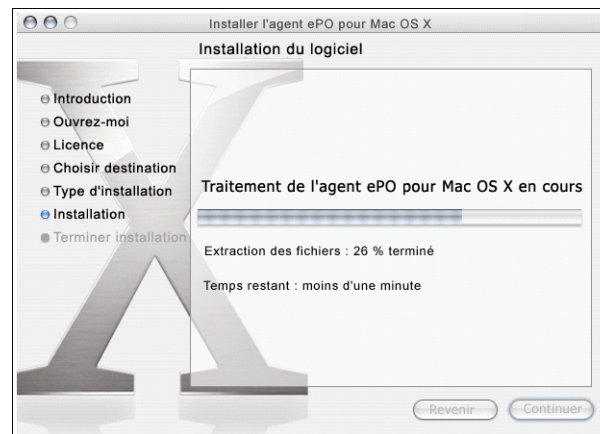


Figure 2-14 Fenêtre d'installation de l'agent ePO - Installation du logiciel

Au cours de ce processus, le programme d'installation vous demande d'authentifier le **configureur de l'agent ePO**. Tapez votre mot de passe et cliquez sur **OK**. La boîte de dialogue **Configureur de l'agent ePO** apparaît.

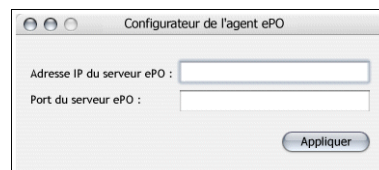


Figure 2-15 Boîte de dialogue du configureur de l'agent ePO

- 8 Indiquez l'**adresse IP du serveur ePO** et le numéro du **port du serveur ePO**. Cliquez sur **Appliquer**. La fenêtre **Installation du logiciel** apparaît.



Figure 2-16 Fenêtre d'installation de l'agent ePO - Installation du logiciel

- 9 Cliquez sur **Redémarrer** pour terminer le processus d'installation.

Installation silencieuse (ligne de commande)

- 1 Recherchez le fichier **nwa.dmg** qui figure sur le CD du produit ou dans le fichier ZIP d'installation téléchargé depuis le site Web McAfee et enregistrez-le dans un répertoire temporaire.



Ce fichier se trouve dans le répertoire **ePO Agent** du fichier **ePO Components.ZIP** sur le CD du produit.

- 2 Double-cliquez sur **nwa.dmg** pour extraire les fichiers suivants :

- NWA.pkg
- cmdinstall

- 3 Ouvrez la fenêtre du **terminal** et sélectionnez le répertoire de travail NAINWA.



Vous devez posséder des droits administrateur pour exécuter cette commande.

- 4 Dans la fenêtre du **terminal**, exécutez `sudo ./cmdinstall <Adresse IP du serveur ePO>:<Port du serveur ePO>`

```

Terminal - bash - 85x41
Manoj-Ts-Computer : /Volumes/NAINWA manoj$ sudo ./cmdinstall 172.16.197.94.79
Password:
The working directory is /Volumes/NAINWA
Creating temporary folder /tmp/NAINWA.rESFqHq3
Dumping the server .inf file
172.16.197.94
79
installer [2420]: Installer Language: English
installer [2420]: Requirement: requires "certain InstallationCheck criteria" PASS for
root=(none), domain=0
installer [2420]: Requirement: requires "certain file content criteria" PASS for root=
(none), domain=0
installer [2420]: Requirement: requires "certain InstallationCheck criteria" PASS for
root=/, domain=0
installer [2420]: Requirement: requires "certain InstallationCheck criteria" PSS for
installer [2420]: Requirement: requires "certain file content criteria" PASS for root=
/, domain=0
installer [2420]: Requirement: requires "certain InstallationCheck criteria" PASS for
root=/, domain=0
installer [2420]: === Starting check on volume /
installer [2420]: Requirement: requires "certain file content criteria" PASS for root=
/, domain=0
installer: Package name is ePO Agent for Mac OS X
installer: Upgrading volume mounted at /.
installer: Preparing the Disk ....
  
```

Figure 2-17 Fenêtre du terminal - Fenêtre de lancement

- 5 Lorsque l'installation silencieuse est terminée, la fenêtre du **terminal** suivante s'affiche :

```

Terminal - bash - 85x24
#
installer: Processing ePO Agent for Mac OS X.....
#
installer: Finishing Installation
###installer[709]: Registered /Library/NETAepoagt/bin/ePO Agent Configurator.app.
###
installer:
##
installer: Optimizing System Performance.....
#installer[709]: Running task: /usr/bin/update_prebinding
installer[709]: 1970-02-15 10:56:34.539 update_prebinding[829] Start of update_prebin
ding
installer: Optimizing volume "10.3": 0% complete
installer: Optimizing volume "10.3": 5% complete
installer: Optimizing volume "10.3": 30% complete
installer: Optimizing volume "10.3": 100% complete
installer[709]: 1970-02-15 10:56:41.284 update_prebinding[829] Update_prebinding done
installer[709]: 1970-02-15 10:56:41.293 update_prebinding[829] 1 files successfully p
rebound, 0 files unsuccessfully prebound.
installer[709]: Finished task: /usr/bin/update_prebinding
installer: The upgrade was successful.
  
```

Figure 2-18 Fenêtre du terminal - Installation/Mise à niveau terminée

- 6 Vous avez correctement installé/mis à niveau votre agent ePolicy Orchestrator pour Mac OS X.

Installation de Virex 7.6



Pour savoir comment installer le logiciel Virex 7.6 sur les systèmes Macintosh, reportez-vous au *Guide produit de Virex 7.6*.

Désinstallation

Suppression des fichiers NAP Virex du serveur ePolicy Orchestrator

Vous pouvez supprimer les fichiers NAP Virex du serveur ePolicy Orchestrator.

Pour supprimer des fichiers NAP Virex :

- 1 Connectez-vous au serveur de base de données ePolicy Orchestrator.
- 2 Sélectionnez **Virex** sous **Référentiel | Produits gérés | MAC OS X** dans l'arborescence de la console.

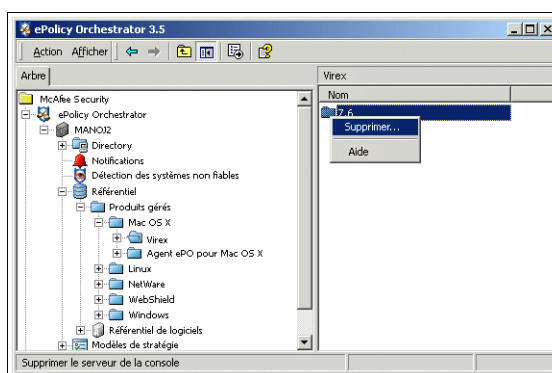


Figure 2-19 Fichiers NAP Virex - Suppression

- 3 Cliquez avec le bouton droit de la souris sur **Virex** et sélectionnez **Supprimer** pour désinstaller les fichiers NAP Virex du serveur ePolicy Orchestrator.

Suppression de l'agent ePolicy Orchestrator du serveur ePolicy Orchestrator



Vous **ne pouvez pas** supprimer l'**agent ePolicy Orchestrator pour MAC OS X** du serveur ePolicy Orchestrator après l'avoir enregistré.

Désinstallation de l'agent ePolicy Orchestrator de Mac OS X

Vous pouvez désinstaller l'agent ePolicy Orchestrator d'un ordinateur Macintosh à partir de la ligne de commande.

Depuis la ligne de commande

- 1 Connectez-vous en tant qu'utilisateur root.



Par défaut, l'utilisateur root d'un système Macintosh est désactivé ; il vous faudra alors l'activer. Si vous vous êtes connecté en tant que simple utilisateur, ouvrez une fenêtre de **terminal**, et entrez « **su** », puis le mot de passe de l'utilisateur root afin de vous connecter en tant qu'utilisateur root.

- 2 Placez-vous dans le répertoire /Library/NETAepoagt.
- 3 Exécutez cmduninst.

3

Définition des stratégies ePolicy Orchestrator pour Virex 7.6

Ce chapitre explique comment définir et faire appliquer les stratégies Virex à partir d'ePolicy Orchestrator. Deux étapes principales sont nécessaires :

- Dans ePolicy Orchestrator, vous sélectionnez le nom des ordinateurs et des stratégies Virex qui vont s'appliquer à ces ordinateurs (par exemple, vous souhaitez qu'une recherche de virus soit effectuée sur les ordinateurs A et B). Vous pouvez définir plusieurs stratégies à appliquer à différents ordinateurs ou groupes d'ordinateurs.
- Vous demandez à ePolicy Orchestrator d'appliquer ces stratégies sur les ordinateurs concernés. L'agent communique avec le serveur pour rechercher les nouvelles stratégies. L'ordinateur va alors respecter la stratégie, en ignorant toute autre stratégie précédemment configurée dans la boîte de dialogue **Préférences** de Virex.

Définition des stratégies dans ePolicy Orchestrator

La console ePolicy Orchestrator vous permet d'appliquer des stratégies à un ordinateur ou à un groupe d'ordinateurs. Elles prennent le pas sur les configurations définies pour chaque ordinateur. Pour plus d'informations sur les stratégies et leur mode d'application, reportez-vous au *Guide produit d'ePolicy Orchestrator*.

Avant de configurer une stratégie, sélectionnez, dans l'arborescence de la console, le groupe d'ordinateurs dont les stratégies Virex doivent être modifiées. Vous pouvez modifier les stratégies Virex depuis les pages et onglets Virex du volet de détails de la console ePolicy Orchestrator. Ces pages sont très similaires aux pages et aux boîtes de dialogue accessibles directement depuis l'interface utilisateur de Virex. Pour plus d'informations sur les options de configurations de Virex 7.6, reportez-vous au *Guide produit de Virex*.

Après avoir modifié une stratégie et enregistré les modifications sur l'ordinateur ou le groupe d'ordinateurs concerné, vous êtes prêt à déployer les nouveaux paramètres via l'agent ePolicy Orchestrator. [Reportez-vous à Application des stratégies, page 29.](#)

Pour modifier les stratégies Virex dans ePolicy Orchestrator :

- 1 Connectez-vous au serveur ePolicy Orchestrator.
- 2 Dans l'arborescence de la console, cliquez sur ePolicy Orchestrator | <SERVEUR> | Répertoire, puis sélectionnez le site, le groupe, l'ordinateur ou le répertoire entier. Les onglets **Stratégies**, **Propriétés** et **Tâches** s'affichent dans la partie supérieure du volet de détails.

- 3 Dans la partie supérieure du volet de détails, cliquez sur l'onglet **Stratégies**, puis sur **Virex**. Une seule entrée s'affiche sous l'élément Virex.

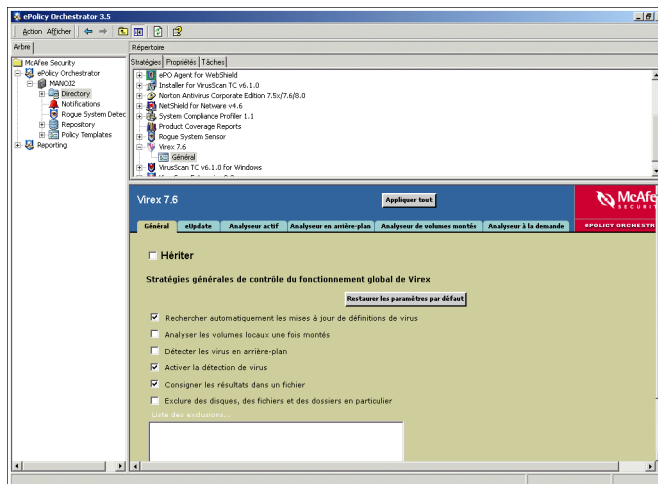


Figure 3-1 Console ePolicy Orchestrator – Virex

La partie inférieure du panneau de détails répertorie les options de configuration détectées dans l'interface Virex.

- Général
 - eUpdate
 - Analyseur actif
 - Analyseur en arrière-plan
 - Analyseur de volumes montés
 - Analyseur à la demande
- 4 Dans la partie inférieure du volet de détails, sélectionnez une option, par exemple **Général**.
- 5 Dans la page **Général**, désactivez la case **Hériter**.
- 6 Configurez les options nécessaires.



Ces pages sont identiques à celles des menus Virex. Pour plus d'informations, reportez-vous au *Guide produit de Virex 7.6*.

- 7 Cliquez sur **Appliquer** pour enregistrer ces paramètres. Vous pouvez poursuivre la configuration des stratégies, puis cliquer sur **Appliquer tout** pour appliquer toutes les stratégies que vous avez configurées.

Application des stratégies

Après avoir configuré des stratégies, vous devez les faire appliquer aux ordinateurs sur lesquels est installé Virex.

- 1 Dans l'arborescence de la console, sous Répertoire, sélectionnez le site, le groupe, l'ordinateur ou le répertoire entier.
- 2 Dans la partie supérieure du volet de détails, cliquez sur l'onglet **Stratégies**, puis sélectionnez **Virex**. La page **Virex** s'affiche dans la partie inférieure du volet de détails.
- 3 Désélectionnez **Hériter**.
- 4 Sélectionnez **Appliquer les stratégies pour Virex 7.6**.
- 5 Cliquez sur **Appliquer** pour enregistrer ces paramètres.

Le logiciel ePolicy Orchestrator mettra les stratégies configurées à la disposition de l'agent ePolicy Orchestrator installé sur les ordinateurs Virex.



Figure 3-2 Appliquer les stratégies pour Virex 7.6

Général

L'onglet **Général** permet d'appliquer des stratégies générales contrôlant le fonctionnement global de Virex 7.6 (par exemple, la recherche automatique de mises à jour des définitions de virus, l'analyse des volumes locaux dès leur installation, la consignation du résultat des analyses, la détection des virus en arrière-plan et la création de listes d'exclusion destinées à certains disques, fichiers et dossiers spécifiques).

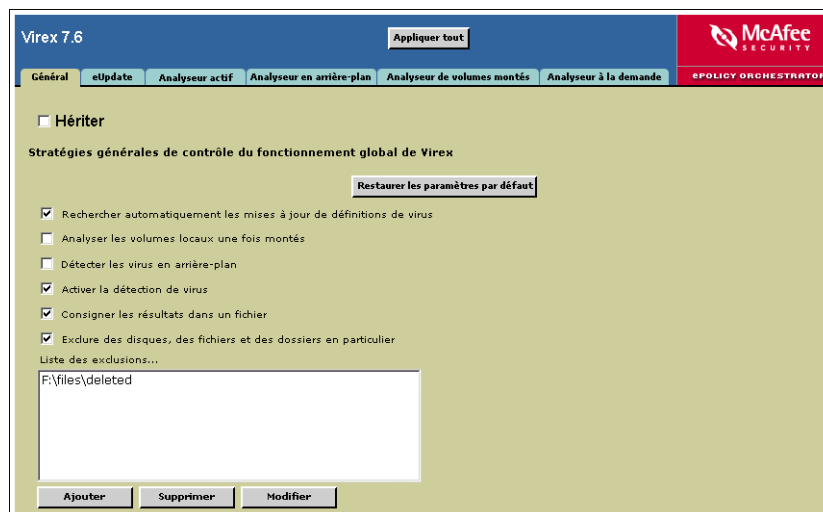


Figure 3-3 Onglet Général

Vous pouvez appliquer les stratégies générales suivantes :

Rechercher automatiquement les mises à jour de définitions de virus	Active/désactive la recherche automatique de mises à jour via eUpdate.
Analyser les volumes locaux une fois montés	Active/désactive l'analyseur de volumes installés.
Détection des virus en arrière-plan	Active/désactive l'analyseur d'arrière-plan.
Activer la détection de virus	Active/désactive l'analyseur actif.
Consigner les résultats dans un fichier	Active/désactive la consignation des résultats dans un fichier.
Exclure des disques, des fichiers et des dossiers en particulier	<p>Configure les éléments à exclure de l'analyse. Les exclusions sont répertoriées dans un fichier texte nommé VShieldExclude.txt. Si celui-ci n'est pas sélectionné, aucune exclusion ne sera définie.</p> <p>Pour ajouter une exclusion :</p> <ul style="list-style-type: none"> ■ Cliquez sur Ajouter. La boîte de dialogue Ajouter un élément à analyser – Page Web s'affiche. Saisissez le chemin complet d'accès au fichier, au répertoire ou au disque à exclure, puis cliquez sur OK. Les exclusions figureront dans la Liste des exclusions. <p>Pour supprimer une exclusion :</p> <ul style="list-style-type: none"> ■ Sélectionnez l'exclusion à supprimer dans la Liste des exclusions, puis cliquez sur Supprimer. <p>Pour modifier une exclusion :</p> <ul style="list-style-type: none"> ■ Sélectionnez l'exclusion à modifier dans la Liste des exclusions, puis cliquez sur Modifier.

eUpdate

L'onglet **eUpdate** vous permet de mettre à jour les fichiers .DAT ainsi que le moteur d'analyse antivirus. Cette fonction tient votre logiciel antivirus à jour en permanence en lui ajoutant les dernières informations sur les virus et les plus récentes capacités d'analyse disponibles. Vous pouvez mettre à jour vos fichiers .DAT et vos fichiers de moteur via FTP ou HTTP.

Figure 3-4 Onglet eUpdate

Personnalisation des paramètres eUpdate

Vous pouvez appliquer les paramètres eUpdate suivants à Virex :

FTP

Le protocole FTP (File Transfer Protocol) est une méthode d'envoi et de réception de fichiers sur Internet. Pour mettre à jour les fichiers .DAT et le moteur, vous devrez indiquer les détails du serveur sur lequel se trouvent les fichiers à copier sur votre ordinateur.

URL du serveur	Indiquez l'URL du serveur depuis lequel vous souhaitez télécharger les mises à jour des fichiers DAT et du moteur.
Port	Spécifiez le numéro de port à utiliser pour la communication FTP.
Nom d'utilisateur	Saisissez votre nom d'utilisateur.
Mot de passe	Saisissez votre mot de passe.
Compte	Saisissez votre compte FTP.
Répertoire	Spécifiez le chemin d'accès à vos fichiers de définitions de virus (DAT) et de moteur.

HTTP

Le protocole HTTP (HyperText Transfer Protocol) est l'ensemble des règles régissant le transfert des fichiers (texte, images graphiques, son, vidéo, ou autres fichiers multimédia) sur le Web. Pour mettre à jour les fichiers DAT et le moteur, vous devez spécifier l'URL du serveur qui héberge les fichiers à copier sur votre ordinateur.

URL du serveur	Indiquez l'URL du serveur depuis lequel vous souhaitez télécharger les mises à jour des fichiers DAT et du moteur.
Nom d'utilisateur	Saisissez votre nom d'utilisateur.
Mot de passe	Saisissez votre mot de passe.

Analyseur actif

L'analyseur actif de Virex fournit une protection antivirus continue du disque dur, lors des connexions réseau et sur Internet. Il fonctionne en permanence sur votre ordinateur, de sorte que votre système ne se trouve pas exposé aux risques d'infection.

L'analyseur actif analyse les fichiers lors de leur écriture sur le disque dur (toutes les partitions) et sur tous les lecteurs amovibles. Il se lance au démarrage de l'ordinateur et fonctionne jusqu'à l'arrêt de ce dernier ; cet analyseur est exécuté par défaut par votre ordinateur. Vous pouvez configurer l'objet de la recherche de l'analyseur, ainsi que l'attitude à adopter vis-à-vis des fichiers infectés.

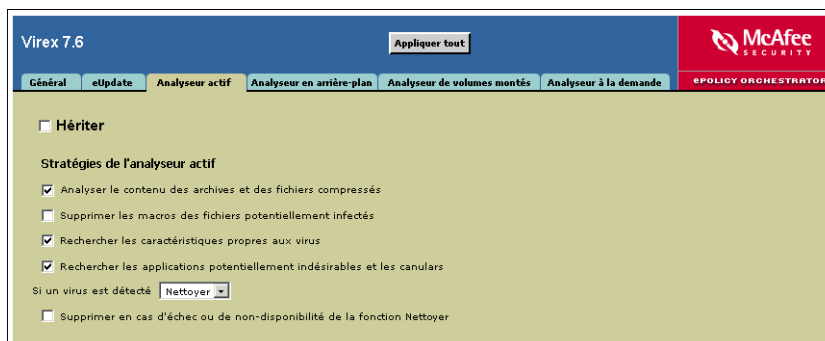


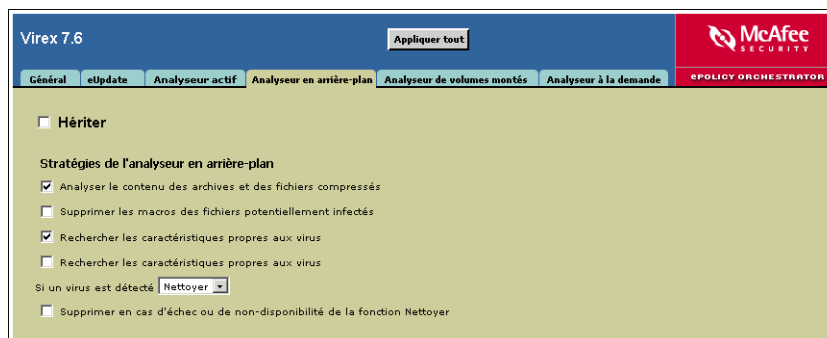
Figure 3-5 Onglet Analyseur actif

L'analyseur actif prend en charge les stratégies suivantes :

Analyser le contenu des archives et des fichiers compressés	Active l'analyse des archives et autres fichiers compressés par l'analyseur sélectionné. Cette option est activée par défaut pour les analyseurs en arrière-plan et à la demande.
Supprimer les macros des fichiers potentiellement infectés	Si un fichier infecté est détecté, toutes les macros qu'il contient sont supprimées lors du nettoyage.
Rechercher les caractéristiques propres aux virus	Active/désactive l'analyse heuristique, qui recherche les fichiers présentant des caractéristiques propres aux virus ou aux vers et susceptibles de contenir des infections encore inconnues. Cette option est activée par défaut pour l'analyseur en arrière-plan.
Rechercher les applications potentiellement indésirables et les canulars	Active/désactive la recherche de programmes indésirables et de canulars.
Si un virus est détecté : ■ Nettoyer ■ Supprimer ■ Avertir	Sélectionne l'action primaire de l'analyseur.
Supprimer en cas d'échec ou de non-disponibilité de la fonction Nettoyer	Sélectionne l'action secondaire de l'analyseur sélectionné. Cette option n'est disponible que lorsque l'action primaire consiste à nettoyer le fichier.

Analyseur en arrière-plan

L'analyseur en arrière-plan analyse en permanence l'ensemble des fichiers de votre système. Il protège votre ordinateur en recherchant en permanence des fichiers infectés au sein de votre système. Cette analyse nécessite très peu de ressources et n'affecte en rien les performances de votre ordinateur. Vous pouvez configurer l'objet de la recherche de l'analyseur, ainsi que l'attitude à adopter vis-à-vis des fichiers infectés.

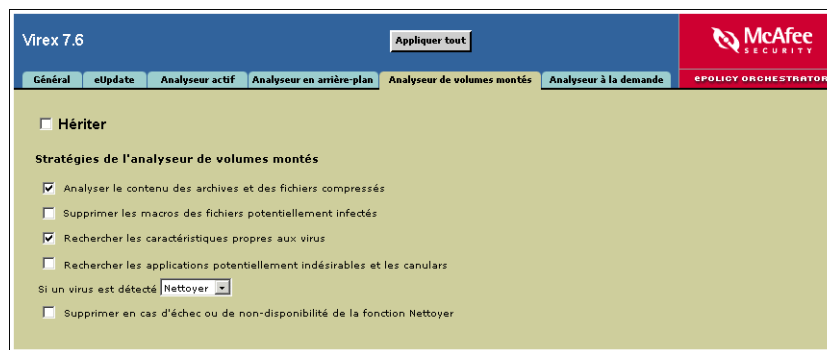
**Figure 3-6 Onglet Analyseur en arrière-plan**

L'analyseur en arrière-plan propose les stratégies suivantes :

Analyser le contenu des archives et des fichiers compressés	Active l'analyse des archives et autres fichiers compressés par l'analyseur sélectionné. Cette option est activée par défaut pour les analyseurs en arrière-plan et à la demande.
Supprimer les macros des fichiers potentiellement infectés	Si un fichier infecté est détecté, toutes les macros qu'il contient sont supprimées lors du nettoyage.
Rechercher les caractéristiques propres aux virus	Active/désactive l'analyse heuristique, qui recherche les fichiers présentant des caractéristiques propres aux virus ou aux vers et susceptibles de contenir des infections encore inconnues. Cette option est activée par défaut pour l'analyseur en arrière-plan.
Rechercher les applications potentiellement indésirables et les canulars	Active/désactive la recherche de programmes indésirables et de canulars.
Si un virus est détecté : ■ Nettoyer ■ Supprimer ■ Avertir	Sélectionne l'action primaire de l'analyseur.
Supprimer en cas d'échec ou de non-disponibilité de la fonction Nettoyer	Sélectionne l'action secondaire de l'analyseur sélectionné. Cette option n'est disponible que lorsque l'action primaire consiste à nettoyer le fichier.

Analyseur de volumes installés

L'analyseur de volumes installés lance l'analyse d'un volume tel qu'un CD ou un appareil photo installé localement. Il vous permet de rechercher des traces d'infection sur un volume ou un périphérique de grande taille avant de le connecter à votre système. Cela limite l'exposition de votre système aux virus. Cette fonctionnalité n'est opérationnelle qu'avec les supports insérés localement ou amovibles (lecteur ZIP, CD, DVD, fichiers .DMG OS X, etc). Elle permet également d'analyser les périphériques USB (clés USB ou appareils photo, par exemple) et les périphériques FireWire (comme un iPod). Elle n'analyse pas les volumes des ordinateurs distants reliés en réseau. L'analyseur travaille en arrière-plan et nécessite l'intervention de l'utilisateur.

**Figure 3-7 Analyseur de volumes montés**

Vous pouvez appliquer les stratégies de l'analyseur de volumes montés suivantes :

Analyser le contenu des archives et des fichiers compressés	Active l'analyse des archives et autres fichiers compressés par l'analyseur sélectionné.
Supprimer les macros des fichiers potentiellement infectés	Si un fichier infecté est détecté, toutes les macros qu'il contient sont supprimées lors du nettoyage.
Rechercher les caractéristiques propres aux virus	Active/désactive l'analyse heuristique, qui recherche les fichiers présentant des caractéristiques propres aux virus ou aux vers et susceptibles de contenir des infections encore inconnues.
Rechercher les applications potentiellement indésirables et les canulars	Active/désactive la recherche de programmes indésirables et de canulars.
Si un virus est détecté : ■ Nettoyer ■ Supprimer ■ Avertir	Sélectionne l'action primaire de l'analyseur.
Supprimer en cas d'échec ou de non-disponibilité de la fonction Nettoyer	Sélectionne l'action secondaire de l'analyseur sélectionné. Cette option n'est disponible que lorsque l'action primaire consiste à nettoyer le fichier.



Par défaut, l'analyseur de volumes installés n'est pas activé sur votre ordinateur.

Analyseur à la demande

L'analyseur à la demande permet de lancer une analyse à tout moment en déposant par glisser-déplacer les fichiers sélectionnés dans la console ou en utilisant une boîte de dialogue **Ouvrir**. Il vous autorise à sélectionner plusieurs fichiers, répertoires ou volumes. Les résultats de l'analyse sont récapitulés dans un rapport que vous pouvez enregistrer ou imprimer. Vous pouvez configurer l'objet de l'analyse, ainsi que l'attitude à adopter vis-à-vis des fichiers infectés. Vous pouvez également configurer une liste des exclusions commune aux analyseurs actifs, en arrière-plan et de volumes installés. L'analyseur vous avertit lorsqu'il détecte un virus et génère un journal répertoriant ses actions.

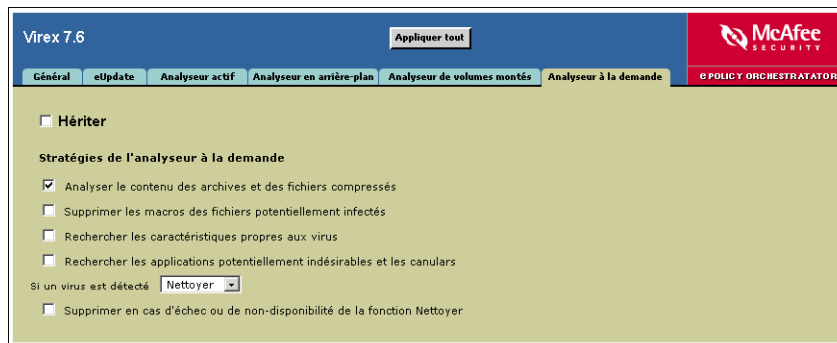


Figure 3-8 Onglet Analyseur à la demande

L'analyseur à la demande prend en charge les stratégies suivantes :

Analyser le contenu des archives et des fichiers compressés	Active l'analyse des archives et autres fichiers compressés par l'analyseur sélectionné. Cette option est activée par défaut pour l'analyseur à la demande.
Supprimer les macros des fichiers potentiellement infectés	Si un fichier infecté est détecté, toutes les macros qu'il contient sont supprimées lors du nettoyage.
Rechercher les caractéristiques propres aux virus	Active/désactive l'analyse heuristique, qui recherche les fichiers présentant des caractéristiques propres aux virus ou aux vers et susceptibles de contenir des infections encore inconnues.
Rechercher les applications potentiellement indésirables et les canulars	Active/désactive la recherche de programmes indésirables et de canulars.
Si un virus est détecté : ■ Nettoyer ■ Supprimer ■ Avertir	Sélectionne l'action primaire de l'analyseur.
Supprimer en cas d'échec ou de non-disponibilité de la fonction Nettoyer	Sélectionne l'action secondaire de l'analyseur sélectionné. Cette option n'est disponible que lorsque l'action primaire consiste à nettoyer le fichier.

Planification des analyses et des mises à jour automatiques via eUpdate

Lors des recherches antivirus, Virex utilise les informations contenues dans le fichier de définition de virus (fichier .DAT) pour trouver et supprimer les virus. De nombreux virus sont découverts chaque jour, et nous publions régulièrement de nouveaux fichiers DAT pour assurer une protection contre ces nouvelles menaces. Pour bénéficier la meilleure protection antivirus possible, vous pouvez configurer ePolicy Orchestrator de sorte qu'il indique à Virex où trouver les derniers fichiers .DAT, créer des planifications pour le remplacement des fichiers .DAT antérieurs et réaliser des analyses à la demande.

A propos des tâches planifiées

Avec ePolicy Orchestrator, vous pouvez planifier les tâches suivantes pour Virex :

- Analyse à la demande
- eUpdate

Les tâches planifiées d'un ordinateur peuvent être définies pour s'exécuter en fonction de l'heure locale ou GMT (heure du méridien Greenwich). Toutefois, ePolicy Orchestrator ne pouvant pas surveiller la progression de la tâche, nous vous conseillons de consulter régulièrement le journal du serveur.

Analyse à la demande

Virex peut rechercher, à la demande, du contenu suspect dans tous les fichiers de la base de données. Vous pouvez planifier un nombre illimité d'analyses à la demande ; ces analyses seront exécutées à intervalles définis ou au moment choisi par l'utilisateur. Si vous souhaitez qu'une planification ne soit pas exécutée automatiquement, vous pouvez la désactiver.

Création d'une tâche

Pour créer une tâche :

- Dans la partie supérieure du volet de détails, cliquez sur l'onglet **Tâches**. Cliquez avec le bouton droit dans le volet et sélectionnez l'option **Planifier les tâches**.

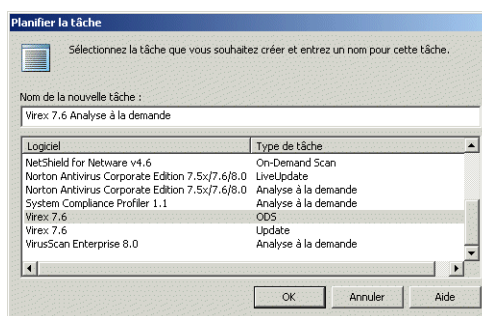


Figure 3-9 Planifier les tâches

- Dans le champ **Nom de la nouvelle tâche**, attribuez un nom à la tâche, puis sélectionnez le type de tâche à créer. Dans la liste déroulante **Type de tâche**, sélectionnez **Analyse à la demande**. Cliquez sur **OK**.
- La tâche créée s'affiche dans l'onglet **Tâche**.

Stratégies Propriétés Tâches						
Nom de la tâche	Dernière modification le	Créé à	Activé	Type de planific...	Date de début	Heure de début
Virex 7.6 Analyse à la demande	MCAFEe	MCAFEe	Faux	Quotidiennement	01/02/2005	12:44:00 (Locale)
Virex 7.6 Update	MCAFEe	MCAFEe	Faux	Quotidiennement	01/02/2005	14:12:00 (Locale)
Deployment	Répertoire	Répertoire	Faux	Quotidiennement	01/02/2005	00:00:00 (Locale)

Figure 3-10 Onglet Tâches

Modification d'une tâche

Pour modifier une tâche :

- Cliquez avec le bouton droit de la souris sur la tâche et sélectionnez l'option **Modifier la tâche**.

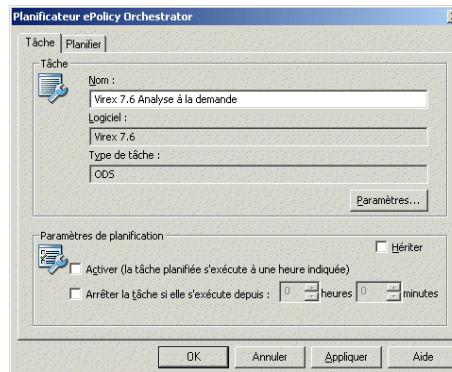


Figure 3-11 Planificateur ePolicy Orchestrator – onglet Tâche

- Cliquez sur **Paramètres** pour inclure des fichiers et répertoires dans l'analyse planifiée. *Reportez-vous à Analyseur à la demande, page 35.*

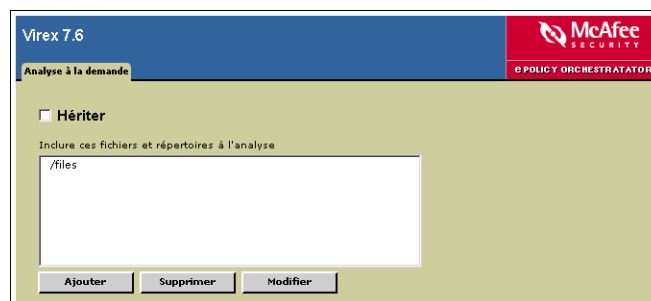


Figure 3-12 Analyse à la demande – Inclure ces fichiers et répertoires à l'analyse



Désélectionnez **Hériter** et sélectionnez **Activer (la tâche planifiée est exécutée à une heure précise)** pour activer les paramètres de la tâche dans le volet **Paramètres de planification**.

Inclure ces fichiers et répertoires à l'analyse	<p>Configure les éléments à inclure dans l'analyse.</p> <p>Pour inclure un élément :</p> <ul style="list-style-type: none"> ■ Cliquez sur Ajouter. La boîte de dialogue Ajouter un élément à analyser – Page Web s'affiche. Saisissez le chemin complet d'accès au fichier, au répertoire ou au disque à inclure dans l'analyse, puis cliquez sur OK. Les éléments inclus s'affichent dans la Liste des inclusions. <p>Pour supprimer un élément inclus :</p> <ul style="list-style-type: none"> ■ Sélectionnez l'élément à supprimer dans la Liste des inclusions, puis cliquez sur Supprimer. <p>Pour modifier un élément inclus :</p> <ul style="list-style-type: none"> ■ Sélectionnez l'élément à modifier dans la Liste des inclusions, puis cliquez sur Modifier. La boîte de dialogue Ajouter un élément à analyser – Page Web s'affiche ; elle vous permet de modifier le chemin d'accès au fichier ou au répertoire correspondant. Cliquez sur OK.
---	---

Paramètres de planification

Activer (la tâche planifiée est exécutée à une heure précise)	Sélectionnez cette option pour exécuter la tâche à l'horaire indiqué.
Arrêter la tâche si elle s'exécute depuis :	Indiquez la durée (en heures et minutes) après laquelle la tâche doit être annulée.

Onglet Planification

Il existe de nombreuses options de planification d'une tâche.

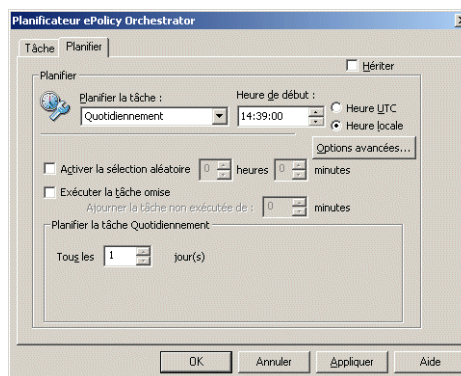


Figure 3-13 Planificateur ePolicy Orchestrator — Onglet Planificateur

Planifier la tâche	<p>Sélectionnez un type de tâche dans le menu déroulant. Vous avez le choix entre les options suivantes :</p> <ul style="list-style-type: none"> ■ Une fois/jour ■ Une fois/semaine ■ Une fois/mois ■ Une fois ■ Au démarrage du système ■ Exécuter immédiatement
Heure de début <ul style="list-style-type: none"> ■ Heure UTC ■ Heure locale 	<p>Spécifiez l'heure de début de la tâche planifiée. Sélectionnez l'heure locale pour lancer la tâche d'après l'heure système de l'ordinateur client. Cette option permet de programmer pendant les heures creuses l'exécution de tâches qui sollicitent fortement le processeur, comme les analyses à la demande.</p> <p>Si vous sélectionnez l'heure UTC, la tâche sera exécutée à l'heure de début UTC (ou GMT) définie. La tâche s'exécutera alors au même moment sur tous les clients Macintosh, quelle que soit leur heure système locale.</p>
Activer la lecture aléatoire	La tâche ne démarrera pas exactement à l'heure de début définie, mais après une durée aléatoire définie. Pour activer la randomisation, vous devez définir l'heure et les minutes.
Exécuter la tâche omise	Permet de lancer la tâche même si l'ordinateur Macintosh est arrêté ou indisponible à l'heure de début planifiée. La tâche sera alors exécutée aussitôt le Macintosh redevenu disponible.
Décaler la tâche non exécutée de	Cliquez sur Avancé dans la boîte de dialogue Options de planification avancées . Cette option définit le délai au terme duquel une tâche manquée sera exécutée à nouveau une fois l'ordinateur Macintosh redevenu disponible.
Date de début/Date de fin	Cliquez sur Avancé dans la boîte de dialogue Options de planification avancées . Saisissez des dates de début et de fin si vous souhaitez que la tâche soit exécutée dans une plage horaire définie, pendant quelques jours ou quelques semaines seulement.
Répéter la tâche	<p>Cliquez sur Avancé dans la boîte de dialogue Options planifiées. Utilisez cette option si vous voulez exécuter une tâche plusieurs fois au cours de la même journée. Pour cela, cochez la case Répéter la tâche et définissez l'intervalle de répétition souhaité.</p> <p>En général, cette option est utile pour exécuter une tâche d'actualisation du client plusieurs fois par jour, notamment aux périodes où un grand nombre de nouveaux virus sont mis en circulation. Elle vous permet également de planifier une tâche pour qu'elle se répète selon d'autres intervalles, de façon hebdomadaire ou mensuelle par exemple.</p>
Planifier la tâche Quotidiennement Tous les X jour(s)	<p>Spécifiez l'intervalle entre deux exécutions de la tâche ; cet intervalle peut être compris entre 1 et plusieurs jours.</p> <p>Si vous sélectionnez 1, la tâche est exécutée tous les deux jours.</p>

Suppression d'une tâche

Pour supprimer une tâche :

- Cliquez avec le bouton droit de la souris sur la tâche dans le volet **Tâches**, puis sélectionnez **Supprimer**.

eUpdate

Lorsque Virex réalise une analyse (conformément à vos paramètres), il utilise le moteur d'analyse antivirus et les fichiers de définitions de virus (DAT) actuels pour rechercher et supprimer les virus. De nombreux virus sont découverts chaque jour, et nous publions régulièrement de nouveaux fichiers de définition de virus pour assurer une protection contre ces nouvelles menaces. Pour que votre logiciel antivirus vous protège de façon optimale, vous devez l'actualiser avec les derniers fichiers DAT et le plus récent moteur d'analyse antivirus disponibles. Nous vous conseillons de mettre à jour les fichiers DAT Virex au moins une fois par semaine et de consulter régulièrement le site Web McAfee AVERT (Anti-Virus Emergency Response Team) pour voir si de nouveaux fichiers DAT s'y trouvent. Si vous possédez plusieurs serveurs sur un même domaine (tous exécutant Virex), vous pouvez utiliser l'un de ces serveurs pour télécharger les derniers fichiers DAT, puis configurer les autres pour qu'ils copient les fichiers depuis ce serveur. Vos serveurs peuvent télécharger des fichiers destinés à plusieurs systèmes d'exploitation, et ce, quel que soit leur système d'exploitation.

Spécification de l'emplacement des fichiers DAT

Vous pouvez spécifier l'emplacement des fichiers DAT via la page eUpdate.

[Reportez-vous à Personnalisation des paramètres eUpdate, page 31.](#)

Création d'une tâche eUpdate

- 1 Dans l'arborescence de la console, sous **ePolicy Orchestrator**, cliquez avec le bouton droit de la souris sur le répertoire, le site, le groupe ou l'hôte souhaité, puis sélectionnez **Planifier la tâche**. La boîte de dialogue **Planifier la tâche** s'affiche.

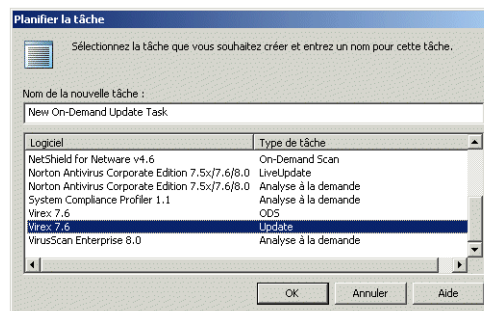


Figure 3-14 Nouvelle tâche de mise à jour

- 2 Dans la boîte de dialogue **Planifier la tâche**, saisissez un nom dans le champ **Nom de la nouvelle tâche**.
- 3 Dans la liste **Type de tâche/logiciel**, sélectionnez **Virex 7.6 – Mise à jour**.
- 4 Cliquez sur **OK** pour créer la tâche.

Configuration d'une tâche eUpdate

Après avoir créé une nouvelle tâche eUpdate, vous pouvez la configurer comme vous le souhaitez.

- 1 Dans l'onglet **Tâches** de la partie supérieure du volet de détails, cliquez avec le bouton droit de la souris sur une tâche, puis sélectionnez **Modifier la tâche**. La boîte de dialogue **Planificateur ePolicy Orchestrator** s'affiche.
- 2 Désélectionnez **Hériter**. [Reportez-vous à Modification d'une tâche, page 38.](#)
- 3 Cliquez sur **OK** pour revenir à la boîte de dialogue **Planificateur ePolicy Orchestrator**.
- 4 Pour supprimer une tâche Virex eUpdate, [Reportez-vous à Suppression d'une tâche, page 40.](#)

Désactivation d'une tâche eUpdate

- 1 Dans l'onglet **Tâches** de la partie supérieure du volet de détails, cliquez avec le bouton droit de la souris sur une tâche, puis sélectionnez **Modifier la tâche**. La boîte de dialogue **Planificateur ePolicy Orchestrator** s'affiche.
- 2 Modifiez les options nécessaires, puis cliquez sur les boutons **Paramètres** des onglets **Tâche** et **Planifier** de la boîte de dialogue **Planificateur ePolicy Orchestrator**. La page **Paramètres de tâche Virex eUpdate** s'affiche.

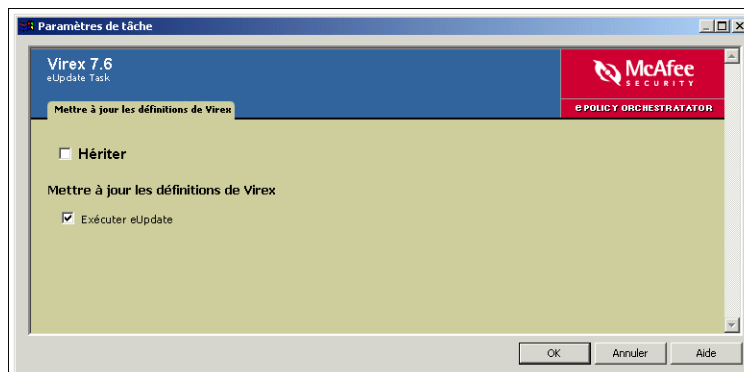


Figure 3-15 Mettre à jour les définitions de Virex - Exécuter eUpdate

- 3 Sur la page **Paramètres de la tâche Virex eUpdate**, désactivez la case **Hériter**.
- 4 Désactivez la case **Exécuter eUpdate**, puis sélectionnez **Hériter**.
- 5 Cliquez sur **OK** pour revenir à la boîte de dialogue **Planificateur ePolicy Orchestrator**.
- 6 Pour supprimer une tâche Virex eUpdate, [Reportez-vous à Suppression d'une tâche, page 40.](#)

Affichage des propriétés du serveur ePolicy Orchestrator

Le serveur ePolicy Orchestrator vous permet d'afficher différentes propriétés du système.

Pour afficher les propriétés du serveur :

- 1 Dans l'arborescence de la console, sélectionnez le répertoire, puis le serveur dont vous souhaitez afficher les paramètres.

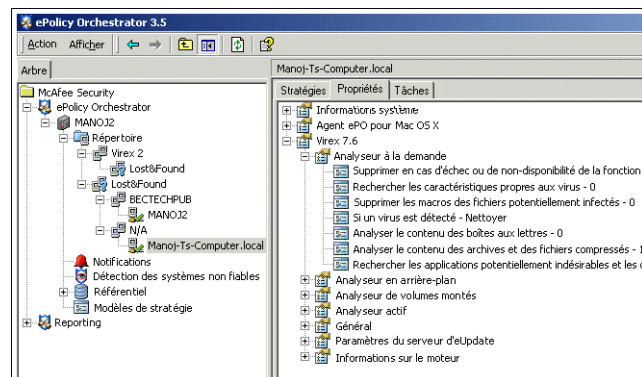


Figure 3-16 Répertoire d'arborescence de la console

- 2 Dans la partie supérieure du volet de détails, cliquez sur l'onglet **Propriétés**.
- 3 Dans le volet **Propriétés**, développez l'arborescence de l'élément **Virex 7.6** pour afficher toutes ses propriétés.
- 4 Cliquez sur le signe **+** en regard de chacune des propriétés pour en afficher les détails.

4

Contrôle de l'agent à distance

Affichage des propriétés de l'agent

Vous pouvez utiliser la console ePolicy Orchestrator pour afficher les propriétés actuelles de n'importe quel ordinateur. Ces propriétés répertorient les informations de base du système, comme le système d'exploitation, l'adresse IP du réseau, la mémoire RAM et la vitesse du processeur. Elles indiquent également les propriétés de l'agent et des produits antivirus ou de sécurité McAfee installés sur cet ordinateur.

Il peut s'avérer très utile de vérifier les stratégies de l'ordinateur lors d'un dépannage afin de vous assurer que les modifications apportées dans la console sont réellement appliquées sur le client Macintosh. L'agent renvoie les propriétés au serveur à chaque intervalle ASCII, ce qui permet de consulter les propriétés système des ordinateurs clients Macintosh partir de la console ePolicy Orchestrator.

Différences entre propriétés et stratégies

Les stratégies sont les règles que vous configurez pour l'agent ou pour des produits spécifiques dans les pages de stratégie au niveau du serveur ePolicy Orchestrator. Lorsque l'agent applique ces stratégies sur l'ordinateur client Macintosh, elles deviennent des propriétés. Les propriétés sont les paramètres en vigueur sur l'ordinateur client Macintosh.

Affichage des propriétés de l'agent

Pour consulter les propriétés que l'agent collecte pour les ordinateurs sélectionnés du Répertoire :

- 1 Dans l'arborescence de la console, sélectionnez l'ordinateur sur lequel est installé Virex.
- 2 Dans la partie supérieure du volet de détails, cliquez sur l'onglet **Propriétés** pour afficher les propriétés de l'ordinateur sélectionné.

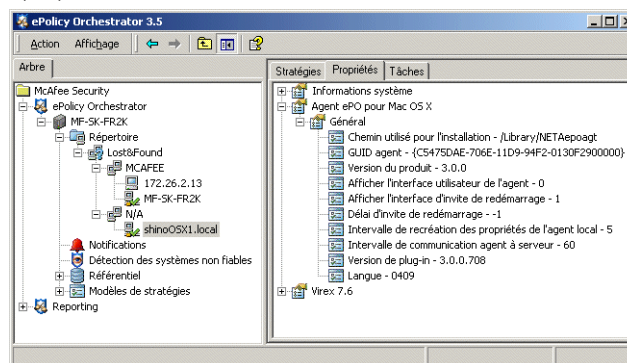


Figure 4-1 Affichage des propriétés de l'agent

- 3 Développez les types de propriétés pour afficher les informations détaillées à propos de celles-ci. Les propriétés de l'agent sont répertoriées sous l'agent ePolicy Orchestrator.

Application des stratégies pour un agent ePolicy Orchestrator

Après avoir configuré les stratégies, vous devez les appliquer pour les mettre à la disposition de l'agent ePolicy Orchestrator sur les hôtes Virex.

Dans l'arborescence de la console ePolicy Orchestrator, sélectionnez les hôtes sur lesquels vous souhaitez appliquer les stratégies.

- 1 Dans la partie supérieure du volet de détails, sélectionnez **Agent ePO pour Mac OS X**.

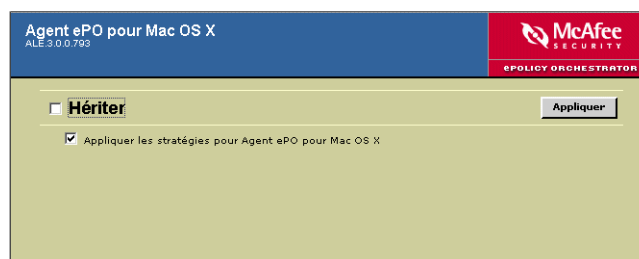


Figure 4-2 Application des stratégies de l'agent ePolicy Orchestrator pour Mac OS X

- 2 Désélectionnez **Hériter**.
- 3 Sélectionnez **Appliquer les stratégies pour Agent ePO pour Mac OS X**.
- 4 Cliquez sur **Appliquer** pour enregistrer ces paramètres. Le logiciel ePolicy Orchestrator rendra les stratégies que vous avez configurées disponibles pour l'agent installé sur les hôtes Virex.

Options de l'agent

Un agent est un composant distribué d'ePolicy Orchestrator installé sur chaque ordinateur Macintosh de votre réseau. Il collecte et envoie des informations entre le serveur ePolicy Orchestrator, les référentiels, les produits et les ordinateurs clients gérés. La configuration de l'agent et de ses paramètres de stratégie détermine son fonctionnement et simplifie la communication et les mises à jour au sein de votre environnement.

Pour configurer la règle de gestion de l'agent pour un ordinateur

- 1 Dans l'arborescence de la console ePolicy Orchestrator, sélectionnez l'ordinateur que vous avez ajouté pour Virex.
- 2 Dans l'onglet **Stratégies** (dans la partie supérieure du volet de détails), sélectionnez **Configuration** sous l'entrée de l'**agent ePO pour Mac OS X**. La page **Stratégie** s'affiche dans la partie inférieure du volet de détails.

- 3 Dans l'onglet **Options de l'agent**, désélectionnez **Hériter**.



Figure 4-3 ePolicy Orchestrator - Options de l'agent

- 4 Dans **Intervalle d'application des stratégies**, sélectionnez l'intervalle (en minutes) le mieux adapté à votre organisation. La valeur par défaut est de 5 minutes. Vous pouvez utiliser une valeur comprise entre 5 et 10 080 minutes (soit 1 semaine).
- 5 Dans **Intervalle de communication agent-serveur**, sélectionnez l'intervalle (en minutes) le mieux adapté à votre organisation. La valeur par défaut est de 60 minutes. Vous pouvez utiliser une valeur comprise entre 5 et 2 880 minutes (soit 2 jours).
- 6 Pour permettre au serveur ePolicy Orchestrator d'envoyer à l'agent des appels de réactivation, sélectionnez **Activer le support d'appel de réactivation de l'agent**.

Événements

Le serveur ePolicy Orchestrator reçoit des notifications de l'agent non-Windows. Vous devez configurer ses pages de stratégie pour transmettre immédiatement les événements au serveur ePolicy Orchestrator ou uniquement lors des intervalles de communication agent-serveur.

Si vous choisissez d'envoyer immédiatement les événements, tous les événements ayant une valeur de gravité supérieure ou égale à la valeur configurée pour l'agent seront immédiatement envoyés.

Si vous choisissez de ne pas envoyer les événements immédiatement, l'agent ne transmettra les événements, quelle que soit leur gravité, que lors des communications entre l'agent et le serveur.

Pour configurer la stratégie de l'agent ePolicy Orchestrator :

- 1 Connectez-vous au serveur ePolicy Orchestrator.
- 2 Sélectionnez le répertoire, site, groupe ou ordinateur de votre choix, puis sélectionnez l'onglet **Stratégies** dans la partie supérieure du volet de détails.
- 3 Sélectionnez **Agent ePolicy Orchestrator pour Mac OS X | Configuration** dans la partie supérieure du volet de détails.

- 4 Dans la partie inférieure du volet de détails, sélectionnez l'onglet **Événements**.

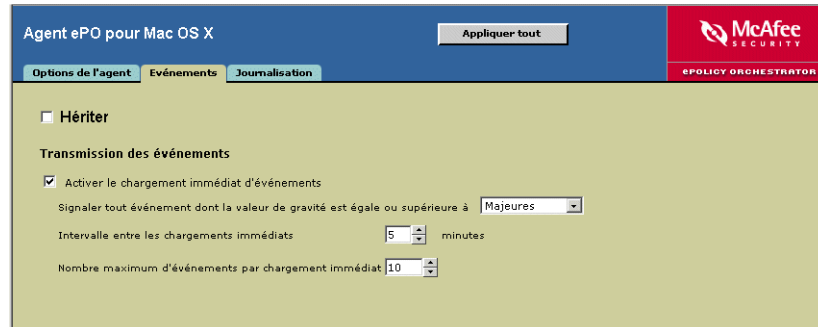


Figure 4-4 Onglet Événements

- 5 Désélectionnez **Hériter**.

Configurez les options de stratégie suivantes :

Transmission des événements

Sélectionnez **Activer le chargement immédiat des événements** pour que l'agent transmette immédiatement les événements au serveur.

Désactivez cette option dans le cas où l'agent doit uniquement transmettre les événements au prochain intervalle ASCII. Si cette option est sélectionnée, vous devez spécifier les éléments suivants :

- Le niveau de gravité le plus faible des événements à envoyer au serveur dans Télécharger les événements de priorité <gravité> et supérieure. Vous pouvez définir la gravité sur les valeurs suivantes : Critique, Majeur, Mineur, Avertissement et Informationnel. Par exemple, si vous sélectionnez Mineur, tous les événements de gravité mineure et de niveau supérieur sont transmis au serveur.
 - Intervalle de transmission des événements dans Intervalle entre les téléchargements immédiats. L'intervalle sélectionné ici détermine la fréquence la plus élevée de transmission des événements. Par exemple, si vous sélectionnez 5 minutes, l'agent transmet alors les événements au serveur toutes les cinq minutes au plus.
 - Nombre maximal d'événements à envoyer simultanément dans Nombre maximal d'événements par chargement immédiat. Si le nombre des événements dépasse cette limite, les événements restants sont envoyés lors de l'intervalle de transmission des événements suivant.
- 6 Cliquez sur **Appliquer tout** pour enregistrer les modifications apportées. Les modifications prendront effet lors du prochain intervalle de communication agent-serveur.

Suppression périodique d'événements anciens de la base de données

Vous pouvez supprimer périodiquement des événements de la base de données afin de freiner la croissance de cette dernière et d'en améliorer les performances. De nombreux événements, en particulier les événements mineurs et les événements informationnels, perdent de leur importance au fil du temps. Il est possible, et par ailleurs conseillé, de sauvegarder la base de données avant d'en supprimer tout type d'événement. Vous pouvez ensuite l'archiver et y recourir au titre de référence en cas de besoin.

Suivez cette procédure pour supprimer définitivement des événements de la base de données ePolicy Orchestrator.

- 1 Connectez-vous au serveur de base de données ePolicy Orchestrator de votre choix.
- 2 Dans l'arborescence de la console sous **Rapports | Bases de données ePO | <Serveur de base de données>**, sélectionnez **Événements**. Les onglets **Filtrage**, **Importer**, **Réparer** et **Suppression** apparaissent dans le volet de détails.

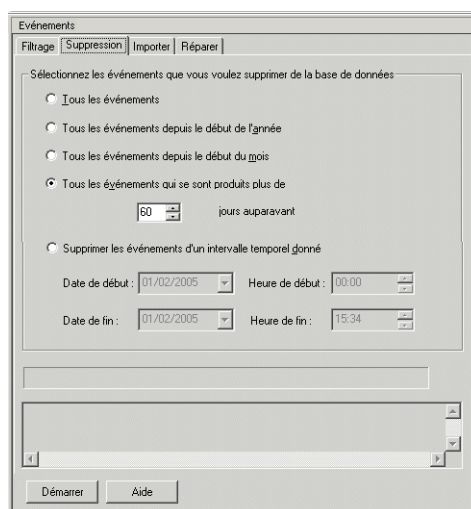


Figure 4-5 Onglet Événements - Suppression

- 3 Cliquez sur l'onglet **Suppression**.
- 4 Sélectionnez les événements que vous souhaitez supprimer de la base de données.
 - **Tous les événements** : sélectionnez cette option pour supprimer tous les événements de la base de données.
 - **Tous les événements depuis le début de l'année** : sélectionnez cette option pour supprimer tous les événements depuis le début de l'année calendaire en cours.
 - **Tous les événements depuis le début du mois** : sélectionnez cette option pour supprimer tous les événements depuis le début du mois en cours.

- **Tous les événements qui se sont produits plus de X jours auparavant :** sélectionnez cette option pour supprimer les événements plus anciens que le nombre de jours spécifié.
 - **Supprimer les événements d'un intervalle temporel donné :** sélectionnez cette option pour spécifier un intervalle de dates et supprimer tous les événements ayant eu lieu au cours de cet intervalle.
- 5 Cliquez sur **Démarrer** pour supprimer les événements spécifiés de la base de données.

Affichage des événements du serveur

Dans la console ePolicy Orchestrator, vous pouvez afficher, enregistrer et imprimer tous les événements d'information, d'avertissement et d'erreur de chaque serveur ePolicy Orchestrator. Il est utile de vérifier la fenêtre des événements du serveur afin de s'assurer de la réussite ou de l'échec des actions effectuées par le serveur, telles que la distribution d'agents, ou l'extraction de fichiers DAT mis à jour depuis un référentiel source.

Par ailleurs, vous pouvez également gérer les événements qui doivent être enregistrés dans la base de données ePolicy Orchestrator. Reportez-vous au *Guide produit d'ePolicy Orchestrator* pour savoir comment maintenir les bases de données ePolicy Orchestrator à jour et comment gérer les événements de ces bases de données.

Pour afficher, enregistrer ou imprimer les événements du serveur à partir de la console ePolicy Orchestrator :

- 1 Connectez-vous au serveur ePolicy Orchestrator.
- 2 Dans l'arborescence de la console, sous ePolicy Orchestrator, sélectionnez le nœud du serveur, puis cliquez sur l'onglet **Général** du volet de détails.
- 3 Cliquez sur **Événements du serveur** pour ouvrir la boîte de dialogue **Observateur d'événements du serveur**.

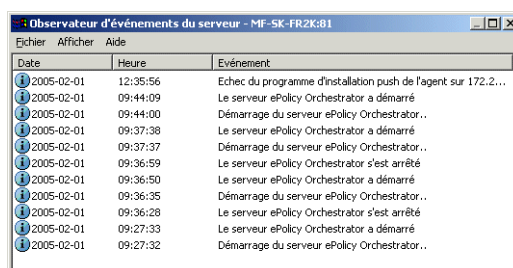


Figure 4-6 Observateur d'événement du serveur

- 4 Sélectionnez **Afficher** | **Actualiser** pour garantir que la liste d'événements est à jour.

Affichage des détails d'un événement spécifique

Pour afficher une description détaillée d'un événement du serveur, double-cliquez sur l'événement de votre choix. La boîte de dialogue **Détail de l'événement du serveur** s'affiche.

Enregistrement des événements dans un fichier journal

Pour enregistrer tous les événements du serveur dans un fichier journal (.log) du serveur, sélectionnez **Fichier | Enregistrer sous**. Pour n'enregistrer que des événements sélectionnés du serveur dans un fichier journal du serveur, sélectionnez les événements souhaités, puis **Fichier | Enregistrer sous**. Dans la boîte de dialogue **Enregistrer sous**, sélectionnez **Éléments sélectionnés seulement**.

Impression des événements du serveur

Pour imprimer tous les événements du serveur sur l'imprimante par défaut, cliquez sur **Imprimer** dans le menu **Fichier**. Pour n'imprimer que les événements du serveur sélectionnés sur l'imprimante par défaut, sélectionnez les événements souhaités, puis sélectionnez **Fichier | Imprimer**.

Consignation

L'agent installé sur l'ordinateur Macintosh génère constamment des événements logiciel au cours du fonctionnement normal. Il s'agit d'événements informationnels relatifs au fonctionnement normal, pouvant se rapporter à l'application de stratégies locales par l'agent ou encore au démarrage d'analyses à la demande. Ces événements sont consignés par l'agent et envoyés au serveur à chaque intervalle ASCII pour être enregistrés dans la base de données. Le déploiement classique d'ePolicy Orchestrator dans un réseau de grande envergure est susceptible de générer des milliers d'événements de ce type toutes les heures.

Pour configurer la stratégie de consignation d'ePolicy Orchestrator :

- 1 Connectez-vous au serveur ePolicy Orchestrator.
- 2 Sélectionnez le répertoire, site, groupe ou ordinateur de votre choix, puis sélectionnez l'onglet **Stratégies** dans la partie supérieure du volet de détails.
- 3 Sélectionnez **Agent ePolicy Orchestrator pour Mac OS X | Configuration** dans la partie supérieure du volet de détails.

4 Dans la partie inférieure du volet de détails, sélectionnez l'onglet **Consignation**.
Ces options permettent de configurer des stratégies relatives à la consignation de l'activité de l'agent dans un journal.



Figure 4-7 Onglet Consignation

Stratégies de journalisation de l'agent	Description des propriétés
Activer la journalisation	Active le journal de l'agent. Cochez cette case pour permettre la consignation dans le fichier /Library/NETAepoagt/Scratch/etc/log.
Activer l'enregistrement détaillé dans le journal	Active la consignation détaillée de l'activité de l'agent dans le journal agent_<ordinateur>.log. La taille de ce fichier journal peut croître très rapidement. Nous vous conseillons d'activer la consignation détaillée. En effet, lorsque seules les erreurs critiques sont enregistrées, les informations peuvent être insuffisantes pour dépanner certains problèmes de communication.

5

Rapports

Rapports

Depuis la console ePolicy Orchestrator, vous pouvez afficher des rapports indiquant la façon dont les hôtes Virex gèrent les infections, et vérifier la configuration définie sur ces hôtes. Vous pouvez également créer des rapports en utilisant les données envoyées par les agents non-Windows des bases de données ePolicy Orchestrator sélectionnées. Vous pouvez aussi enregistrer les sélections effectuées dans les boîtes de dialogue **Saisir les entrées de rapport** et **Filtre de données pour les rapports** pour une utilisation ultérieure.

Les rapports ePolicy Orchestrator offrent diverses possibilités :

- Filtrage du répertoire pour collecter uniquement les informations que vous souhaitez visualiser. Lors de la définition du filtre, vous pouvez choisir la partie de l'arborescence de la console ePolicy Orchestrator incluse dans le rapport.
- Filtrage des données, en utilisant des opérateurs logiques, afin de filtrer avec précision les données renvoyées servant à établir le rapport.
- Génération de rapports graphiques à partir des informations de la base de données et filtrage des rapports en fonction de vos besoins. Vous pouvez imprimer les rapports et les exporter pour les utiliser dans d'autres logiciels.
- Exécution de requêtes sur des ordinateurs, des événements et des installations.

Pour exécuter un rapport :

- 1 Connectez-vous au serveur de base de données ePolicy Orchestrator.
- 2 Sélectionnez le rapport Virex souhaité sous **Rapports | Bases de données ePO | <serveur de base de données> | Rapports | <groupe de rapports>** dans l'arborescence de la console.
 - Si la boîte de dialogue **Standards de protection actuels** apparaît, spécifiez les numéros de version des fichiers de définition de virus ou le moteur d'analyse des virus dont vous souhaitez des rapports.
 - Si la boîte de dialogue **Saisir les entrées de rapport** s'affiche, effectuez vos choix dans les onglets correspondants : **Règles**, **Mise en page**, **Groupe de données**, **Dans**, **Paramètres enregistrés**.



Ces onglets peuvent différer en fonction du rapport sélectionné. Pour plus d'informations sur les onglets de paramètres Règles, Mise en page, Groupements de données, Dans et Paramètres enregistrés, reportez-vous au *Guide produit d'ePolicy Orchestrator*.

- 3 Sélectionnez le rapport (**Versions de l'agent**) que vous souhaitez générer, puis définissez le filtre de données dans la boîte de dialogue **Filtre de données pour les rapports**. Cliquez sur **OK**.
- 4 Le rapport relatif aux **Versions de l'agent** est alors généré.

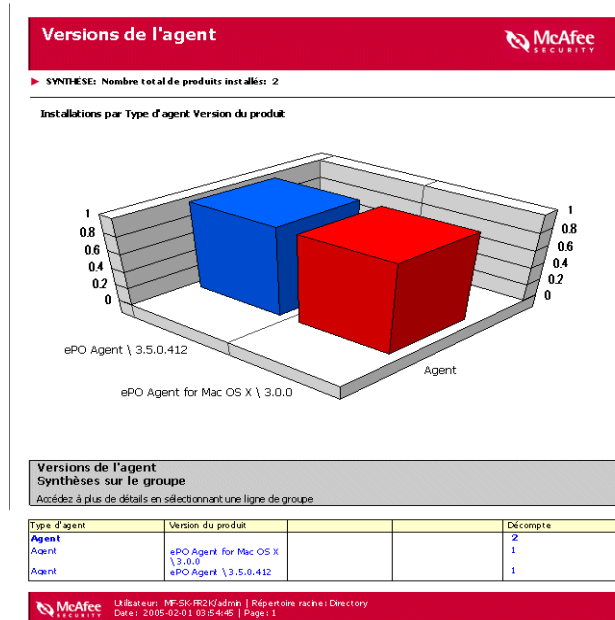


Figure 5-1 Exemple de rapport - Versions de l'agent

Configuration des rapports

Vous pouvez contrôler les données qui s'affichent dans les rapports de diverses manières. Vous pouvez définir le numéro de version des fichiers de signatures de virus, des moteurs d'analyse antivirus et des produits pris en charge qui doivent être installés sur les ordinateurs clients Macintosh afin de les rendre conformes aux stratégies de sécurité et antivirus définies pour votre entreprise. Vous pouvez également filtrer les résultats des rapports en fonction de critères liés aux produits sélectionnés (par exemple, par nom d'ordinateur, système d'exploitation, nom de virus ou action entreprise sur les fichiers infectés).

Une fois les résultats d'un rapport affichés, vous pouvez effectuer un certain nombre de tâches sur les données. Vous pouvez afficher les détails des données de rapports de votre choix (pour identifier, par exemple, les ordinateurs clients Macintosh qui ne disposent pas d'une version conforme de Virex). Certains rapports proposent même des liens vers d'autres rapports, appelés sous-rapports, qui fournissent des données sur le rapport actuel. Vous pouvez également imprimer les rapports ou exporter les données des rapports dans différents formats de fichiers, y compris HTML et Microsoft Excel.



Pour plus d'informations sur la configuration des rapports, reportez-vous au *Guide produit d'ePolicy Orchestrator*.

Glossaire

Agent ePolicy Orchestrator

Programme qui effectue des tâches en arrière-plan sur des ordinateurs gérés, sert d'intermédiaire pour toutes les requêtes entre le serveur ePolicy Orchestrator et les produits de sécurité ou antivirus installés sur ces ordinateurs et signale en retour au serveur l'état de ces tâches.

Agent inactif

Tout agent n'ayant pas communiqué avec le serveur ePolicy Orchestrator pendant une période spécifiée.

Alerte

Message ou notification concernant l'activité de l'ordinateur telle que la détection d'un virus. Ils peuvent être envoyés automatiquement selon une configuration prédéfinie, aux administrateurs système et utilisateurs par courrier électronique, pager, ou téléphone.

Voir aussi *Alert Manager*.

Analyse, analyser

Examen de fichiers pour détecter la présence d'un virus ou d'autre code potentiellement dangereux.

Voir aussi *analyse à l'accès* et *analyse à la demande*.

Analyse à la demande

Examen planifié de fichiers sélectionnés visant à déterminer s'ils contiennent un virus ou un autre code potentiellement indésirable. Cet examen peut s'effectuer immédiatement, à une prochaine date planifiée ou à des intervalles planifiés régulièrement.

Comparer à *Analyse à l'accès*.

Appel de réactivation de l'agent

Processus permettant d'établir la communication agent-serveur à partir du serveur.

Voir aussi *Appel de réactivation du SuperAgent*.

Application

Mise en vigueur de paramètres prédéfinis sur des ordinateurs clients à intervalles prédéterminés.

Arborescence de la console

Contenu de l'onglet **Arborescence**, dans le volet gauche de la console ePolicy Orchestrator. L'arborescence affiche les éléments disponibles dans la console.

Archivage

Ajout de fichiers au référentiel maître.

ASCI

Voir *intervalle de communication agent-serveur*.

Base de données ePolicy Orchestrator

Base de données qui stocke toutes les données reçues par le serveur ePolicy Orchestrator de l'agent ePolicy Orchestrator, ainsi que tous les paramètres configurés sur le serveur lui-même.

Voir aussi *Serveur de base de données ePolicy Orchestrator*.

Branche

Emplacement du référentiel maître qui permet de stocker et de distribuer différentes versions de mises à jour sélectionnées.

Voir aussi *Mise à jour sélective*.

Communication agent-serveur

Toute communication ayant lieu entre l'agent ePolicy Orchestrator et le serveur ePolicy Orchestrator et au cours de laquelle ceux-ci échangent des données. En règle générale, c'est l'agent qui établit toutes les communications avec le serveur.

Console distante ePolicy Orchestrator

Interface utilisateur ePolicy Orchestrator, lorsqu'elle est installée sur un ordinateur distinct du serveur ePolicy Orchestrator.

Voir aussi *Console ePolicy Orchestrator*.

Console ePolicy Orchestrator

Interface utilisateur du logiciel ePolicy Orchestrator utilisée pour contrôler et surveiller à distance des ordinateurs gérés.

Voir aussi *Console distante ePolicy Orchestrator*.

Contrôleur de l'agent

Interface utilisateur de l'agent que vous pouvez choisir d'afficher sur les ordinateurs gérés. Elle vous permet d'exécuter des tâches immédiatement alors qu'elles sont normalement déclenchées par l'agent selon des intervalles prédéfinis.

Déployer, déploiement

Action consistant à distribuer et à installer les programmes d'installation sur des ordinateurs clients depuis un emplacement centralisé.

Élément de l'arborescence de la console

Chacune des icônes de l'arborescence de la console ePolicy Orchestrator.

Événements

Données échangées durant une communication agent-serveur et comprenant des informations au sujet de chaque ordinateur géré (par exemple, matériel et logiciels) et de ses produits gérés (par exemple, paramètres de stratégie spécifiques et numéro de version du produit).

Événements du serveur

Activité ayant lieu sur le serveur ePolicy Orchestrator et enregistrée par l'Observateur d'événements Windows. Ces informations ne sont pas enregistrées dans la base de données ePolicy Orchestrator et ne sont donc pas disponibles pour la création de rapports.

Fichiers (d'installation) binaires

Programme d'installation et tous les autres fichiers requis pour installer des produits.

Fichier journal

Enregistrement des activités d'un composant de logiciel antivirus McAfee. Les fichiers journaux enregistrent les actions exécutées pendant une installation ou pendant les tâches d'analyse ou de mise à jour.

Voir aussi *Événements*.

Fichiers DAT

Fichiers de signatures de virus, permettant au logiciel antivirus de détecter et de traiter les virus et le code potentiellement indésirable apparent qui est incorporé dans des fichiers.

Voir aussi *Fichier EXTRA.DAT*, *Fichiers DAT incrémentiels* et *SuperDAT*.

Groupe

Dans l'arborescence de la console, ensemble logique d'entités regroupées pour en faciliter la gestion. Les groupes peuvent contenir d'autres groupes ou des ordinateurs, et vous pouvez leur assigner des intervalles d'adresses IP ou des masques de sous-réseau IP de façon à classer les ordinateurs en fonction de leur adresse IP. Si vous avez créé un groupe en important un domaine Windows NT, vous pouvez envoyer automatiquement le package d'installation de l'agent à l'ensemble des ordinateurs importés du domaine.

Groupe Perdu&Trouvé

Groupe où sont stockés temporairement les ordinateurs dont il n'est pas possible de déterminer l'emplacement approprié dans le **Répertoire**.

Hériter, héritage

Application d'un élément des paramètres définis pour l'élément situé juste au-dessus de lui au sein de la hiérarchie.

Heure UTC

Heure UTC (Temps Universel Coordonné). Fait référence à l'heure du méridien zéro, ou méridien de Greenwich.

Installation silencieuse

Méthode d'installation transparente d'un package logiciel sur un ordinateur, sans qu'aucune intervention de l'utilisateur ne soit requise.

Intervalle d'application des stratégies

Période durant laquelle l'agent applique les paramètres qu'il a reçus du serveur ePolicy Orchestrator. Ces paramètres s'appliquant localement, cet intervalle ne requiert pas de bande passante.

Intervalle de communication agent-serveur (ASCI)

Délai qui sépare deux communications agent-serveur prédéfinies.

Mise à niveau automatique (AutoUpgrade) de l'agent

Processus par lequel l'agent est mis à niveau automatiquement dès qu'une nouvelle version est disponible sur le serveur ePolicy Orchestrator.

Nettoyer, nettoyage

Mesure prise par l'analyseur lorsqu'un *virus*, un *cheval de Troie* ou un *ver* est détecté. L'action de nettoyage peut inclure la suppression du virus d'un fichier et la remise en état fonctionnelle du fichier ; la suppression des références au virus des fichiers système, des fichiers système .INI et du registre ; l'interruption des processus générés par le virus ; la suppression d'une macro ou d'un script Microsoft Visual Basic qui infecte un fichier ; la suppression d'un fichier s'il s'agit d'un cheval de Troie ou d'un ver ; le changement de nom d'un fichier qui ne peut être nettoyé.

Package d'installation de l'agent

Programme d'installation et tous les autres fichiers requis pour installer l'agent.

Packages de langue de l'agent

Ensemble de fichiers devant être distribués sur les ordinateurs clients pour y afficher l'interface utilisateur de l'agent dans des langues autres que l'anglais.

Priorité d'avertissement

Valeur que vous attribuez à chaque message d'alerte, à titre informatif. Vous disposez des options de priorité : **Critique**, **Majeur**, **Mineur**, **Avertissement** et **Informationnel**.

Propriétés

Données échangées durant une communication agent-serveur et comprenant des informations au sujet de chaque ordinateur géré (par exemple, matériel et logiciels) et de ses produits gérés (par exemple, paramètres de stratégie spécifiques et numéro de version du produit).

Référentiel

Emplacement où sont stockées les pages de stratégie utilisées pour gérer les produits.

Référentiels de logiciels distribués

Ensemble de sites Web ou d'ordinateurs placés sur le réseau de façon à fournir l'accès aux ordinateurs clients en optimisant la bande passante. Les référentiels distribués stockent les fichiers dont les ordinateurs clients ont besoin pour installer des produits pris en charge et leurs mises à jour.

Répertoire

Dans l'arborescence de la console, liste de tous les ordinateurs à gérer par ePolicy Orchestrator ; lien vers les interfaces principales de gestion de ces ordinateurs.

Serveur de base de données ePolicy Orchestrator

Ordinateur hébergeant la base de données ePolicy Orchestrator. Il peut s'agir de l'ordinateur même sur lequel est installé le serveur ePolicy Orchestrator ou d'un ordinateur distinct.

Serveur ePolicy Orchestrator

Composant principal du logiciel ePolicy Orchestrator.

Voir aussi *Agent ePolicy Orchestrator* et *Console ePolicy Orchestrator*.

Site

Dans l'arborescence de la console, ensemble logique d'entités regroupées pour en faciliter la gestion. Les sites peuvent contenir des groupes ou des ordinateurs et peuvent être organisés par intervalle d'adresses IP, masque de sous-réseau IP, emplacement, service et autres.

Stratégie

Paramètres de configuration d'un produit géré qui sont définis et administrés à partir d'ePolicy Orchestrator.

Tâche

Activité ponctuelle (*analyse à la demande*) ou récurrente (*mise à jour*) qui est planifiée pour s'exécuter des heures ou à des intervalles spécifiques.

Comparer à *Stratégie*.

Tâche d'analyse

Événement d'analyse unique.

Transmission immédiate des événements

Envoi immédiat vers le serveur ePolicy Orchestrator d'événements présentant un degré de gravité minimal spécifié dès qu'un nombre prédéfini d'événements sont disponibles. Cette communication s'effectue séparément des autres communications agent-serveur.

Utilitaire de rapport d'erreur

Utilitaire spécialement conçu pour suivre et enregistrer dans un fichier journal les défaillances du logiciel McAfee installé sur votre système. Les informations ainsi obtenues peuvent faciliter l'analyse des problèmes.

Ver

Virus qui se propage en créant des copies de lui-même sur d'autres lecteurs, systèmes ou réseaux.

Virus

Programme capable de se répliquer avec une intervention nulle ou minime de l'utilisateur. Le programme répliqué se répliquera à son tour.

Volet de détails

Volet droit de la console ePolicy Orchestrator qui présente les détails de l'élément actuellement sélectionné dans l'arborescence de la console. Selon l'élément de l'arborescence de la console sélectionné, le volet de détails peut être divisé en volets supérieur et inférieur.

Voir aussi *Volet de détails supérieur* et *Volet de détails inférieur*.

Volet de détails inférieur

Dans la console, le volet inférieur droit qui affiche les paramètres de configuration pour les produits répertoriés sous l'onglet **Stratégies** du volet de détails supérieur.

Voir aussi *Volet de détails* et *Volet de détails supérieur*.

Volet de détails supérieur

Dans la console, le volet supérieur droit qui contient les onglets **Stratégies**, **Propriétés** et **Tâches**.

Voir aussi *Volet de détails* et *Volet de détails inférieur*.

Index

A

- agent
 - affichage des propriétés, 45
 - application des stratégies, 46
 - configuration système
 - requis, 13
 - installation, 18
 - installation silencieuse, 22
 - installation standard, 18
 - ligne de commande, 22
 - options, 46
 - répertoire, 17
- AVERT
 - Anti-virus & Vulnerability Emergency Response Team, contacter, 11
 - service de notification de fichiers DAT, 11
 - WebImmune, 11

B

- bibliothèque d'informations sur les virus, 9, 11

C

- composants du serveur, 14
- consignation, 51
- contacter McAfee, 11

D

- définition des stratégies
 - analyseur à la demande, 35
 - analyseur actif, 32
 - analyseur de volumes installés, 34
 - analyseur en arrière-plan, 33
 - ePolicy Orchestrator, 27
 - général, 30
- définition des termes (*Voir* Glossaire)
- désinstallation
 - agent ePO de Mac OS X, 25
 - agent ePO du serveur ePO, 25
 - fichiers NAP Virex du serveur ePO, 24
- documentation produit, 8

E

- envoi d'un échantillon de virus, 11
- ePolicy Orchestrator
 - propriétés du serveur, 43
- eUpdate, 31
 - configuration, 42
 - création, 41
 - désactivation, 42
 - FTP, 31
 - HTTP, 32
- Événements
 - afficher les événements du serveur, 50
 - suppression d'événements, 49
- événements, 47

F

- fichier DAT
 - choix de l'emplacement, 41
 - mise à jour via le service de notification d'AVERT, 11
 - mise à jour, site web, 11
- fichiers .NAP
 - ajout d'un fichier .NAP de rapport, 16
 - ajout d'un fichier .NAP Virex, 15
 - ajout de l'agent non-Windows, 14
 - emplacement des fichiers .NAP, 14
 - enregistrement, 14
- formation produit, sur site, 11
- formation sur site, 11

G

- glossaire, 55

I

- informations sur le produit, ressources, 8

L

- liens vers des ressources dans le produit, 9

M

- manuels, 8
- mise à jour du logiciel antivirus, 52
- mise à niveau, site Web, 11

O

- obtention d'informations, 8
 - depuis le produit, 9
 - liste de contacts, 11

P

- planification des analyses et des mises à jour automatiques via eUpdate, 36
- PrimeSupport, 11
- PrimeSupport, portail de services, 11
- programme bêta, contacter, 11
- public concerné par ce manuel, 7

R

- rapports, 53
 - configuration, 54
- ressources et informations, 8

S

- Security HQ, contacter AVERT, 11 à 12
- service clientèle, contacter, 12
- service de notification, mises à jour de fichiers DAT, 11
- services de conseil, 11
- site Web de formation, 11
- site Web de téléchargement, 11 à 12
- soutien technique
 - accès depuis le produit, 9
 - informations de contact, 11

T

- tâche
 - modification, 38
 - suppression, 40

U

- Université McAfee, contact, 11
- utilisation de ce guide
 - conventions typographiques et symboles, 7

V

virus, envoi d'un échantillon
site web, [11](#)

W

WebImmune, [11](#)