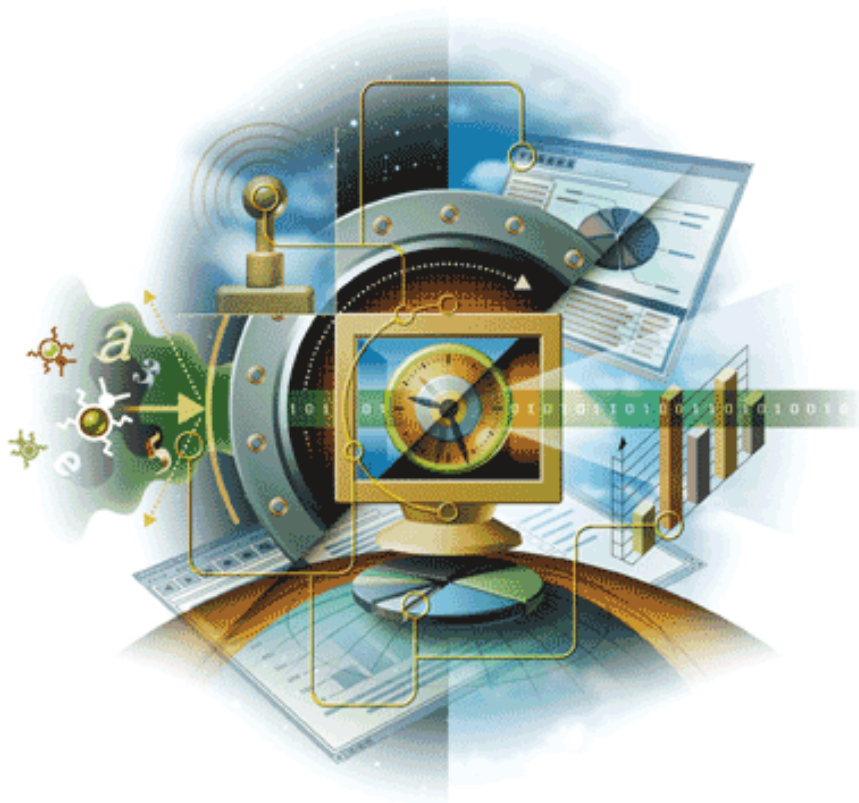


Virex®

version 7.7

for use with ePolicy Orchestrator



McAfee®
System Protection

Industry-leading intrusion prevention solutions



COPYRIGHT

Copyright © 2004-2005 McAfee, Inc. All Rights Reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc., or its suppliers or affiliate companies. To obtain this permission, write to the attention of the McAfee legal department at: 5000 Headquarters Drive, Plano, Texas 75024, or call +1-972-963-8000.

TRADEMARK ATTRIBUTIONS

Active Firewall, Active Security, ActiveSecurity (and in Katakana), ActiveShield, AntiVirus Anyware and design, Clean-Up, Design (Stylized E), Design (Stylized N), Intercept, Enterprise SecureCast, Enterprise SecureCast (and in Katakana), ePolicy Orchestrator, First Aid, ForceField, GMT, GroupShield, GroupShield (and in Katakana), Guard Dog, HomeGuard, Hunter, IntruShield, Intrusion Prevention Through Innovation, M and Design, McAfee, McAfee (and in Katakana), McAfee and Design, McAfee.com, McAfee VirusScan, NA Network Associates, Net Tools, Net Tools (and in 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 (And In Katakana), Webscan, Webshield, Webshield (And In Katakana), Webstalker, WebWall, What's The State Of Your IDS?, Who's Watching Your Network, Your E-Business Defender, Your Network. Our Business. are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. Red in connection with security is distinctive of McAfee® brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners.

LICENSE INFORMATION

License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANIES YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEB SITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Attributions

This product includes or may include:

- Software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).
- Cryptographic software written by Eric A. Young and software written by Tim J. Hudson.
- Some software programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar Free Software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code. The GPL requires that for any software covered under the GPL which is distributed to someone in an executable binary format, that the source code also be made available to those users. For any such software covered under the GPL, the source code is made available on this CD. If any Free Software licenses require that McAfee provide rights to use, copy or modify a software program that are broader than the rights granted in this agreement, then such rights shall take precedence over the rights and restrictions herein.
- Software originally written by Henry Spencer, Copyright 1992, 1993, 1994, 1997 Henry Spencer.
- Software originally written by Robert Nordier, Copyright © 1996-7 Robert Nordier.
- Software written by Douglas W. Sauder.
- Software developed by the Apache Software Foundation (<http://www.apache.org/>). A copy of the license agreement for this software can be found at www.apache.org/licenses/LICENSE-2.0.txt.
- International Components for Unicode ("ICU") Copyright © 1995-2002 International Business Machines Corporation and others.
- Software developed by CrystalClear Software, Inc., Copyright © 2000 CrystalClear Software, Inc.
- FEAD™ Optimizer™ technology, Copyright Netopsystems AG, Berlin, Germany.
- Outside In™ Viewer Technology © 1992-2001 Stellant Chicago, Inc. and/or Outside In™ HTML Export, © 2001 Stellant Chicago, Inc.
- Software copyrighted by Thai Open Source Software Center Ltd. and Clark Cooper, © 1998, 1999, 2000.
- Software copyrighted by Expat maintainers.
- Software copyrighted by The Regents of the University of California, © 1989.
- Software copyrighted by Gunnar Ritter.
- Software copyrighted by Sun Microsystems®, Inc. © 2003.
- Software copyrighted by Gisle Aas. © 1995-2003.
- Software copyrighted by Michael A. Chase, © 1999-2000.
- Software copyrighted by Neil Winton, © 1995-1996.
- Software copyrighted by RSA Data Security, Inc., © 1990-1992.
- Software copyrighted by Sean M. Burke, © 1999, 2000.
- Software copyrighted by Martijn Koster, © 1995.
- Software copyrighted by Brad Appleton, © 1996-1999.
- Software copyrighted by Michael G. Schwern, © 2001.
- Software copyrighted by Graham Barr, © 1998.
- Software copyrighted by Larry Wall and Clark Cooper, © 1998-2000.
- Software copyrighted by Frodo Looijgaard, © 1997.
- Software copyrighted by the Python Software Foundation, Copyright © 2001, 2002, 2003. A copy of the license agreement for this software can be found at www.python.org.
- Software copyrighted by Beman Dawes, © 1994-1999, 2002.
- Software written by Andrew Lumsdaine, Lie-Quan Lee, Jeremy G. Siek © 1997-2000 University of Notre Dame.
- Software copyrighted by Simone Bordet & Marco Cravero, © 2002.
- Software copyrighted by Stephen Purcell, © 2001.
- Software developed by the Indiana University Extreme! Lab (<http://www.extreme.indiana.edu/>).
- Software copyrighted by International Business Machines Corporation and others, © 1995-2003.
- Software developed by the University of California, Berkeley and its contributors.
- Software developed by Ralf S. Engelschall <rs@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>).
- Software copyrighted by Kevlin Henney, © 2000-2002.
- Software copyrighted by Peter Dimov and Multi Media Ltd. © 2001, 2002.
- Software copyrighted by David Abrahams, © 2001, 2002. See <http://www.boost.org/libs/bind/bind.html> for documentation.
- Software copyrighted by Steve Cleary, Beman Dawes, Howard Hinnant & John Maddock, © 2000.
- Software copyrighted by Boost.org, © 1999-2002.
- Software copyrighted by Nicolai M. Josuttis, © 1999.
- Software copyrighted by Jeremy Siek, © 1999-2001.
- Software copyrighted by Daryle Walker, © 2001.
- Software copyrighted by Chuck Allison and Jeremy Siek, © 2001, 2002.
- Software copyrighted by Samuel Krempp, © 2001. See <http://www.boost.org> for updates, documentation, and revision history.
- Software copyrighted by Doug Gregor (gregod@cs.rpi.edu), © 2001, 2002.
- Software copyrighted by Cadenza New Zealand Ltd., © 2000.
- Software copyrighted by Jens Maurer, © 2000, 2001.
- Software copyrighted by Jaakko Järvi (jaakko.jarvi@cs.utu.fi), © 1999, 2000.
- Software copyrighted by Ronald Garcia, © 2002.
- Software copyrighted by David Abrahams, Jeremy Siek, and Daryle Walker, © 1999-2001.
- Software copyrighted by Stephen Cleary (shammah@voyager.net), © 2000.
- Software copyrighted by Housemarque Oy <<http://www.housemarque.com>>, © 2001.
- Software copyrighted by Paul Moore, © 1999.
- Software copyrighted by Dr. John Maddock, © 1998-2002.
- Software copyrighted by Greg Colvin and Beman Dawes, © 1998, 1999.
- Software copyrighted by Peter Dimov, © 2001, 2002.
- Software copyrighted by Jeremy Siek and John R. Bandela, © 2001.
- Software copyrighted by Joerg Walter and Mathias Koch, © 2000-2002.

Contents

1	Introduction	5
	What's in this guide?	5
	Pre-requisites for using ePolicy Orchestrator to manage Virex	6
	Introducing ePolicy Orchestrator console	6
	Audience	7
	Conventions	7
	Resources	8
	Getting product information	8
	Links from within the product	8
	Product services	10
	Contact information	11
2	Installation	13
	Introduction	13
	System Requirement	13
	Configuring ePolicy Orchestrator console for managing Virex	13
	Check in NAP files to manage Virex	14
	Installing agent for Macintosh systems	16
	Agent installation directory	16
	Installing agent	16
	Installing Virex	19
	Uninstallation	19
	Removing Virex NAP from ePolicy Orchestrator Server	19
	Removing ePolicy Orchestrator Agent from ePolicy Orchestrator server	20
	Removing ePolicy Orchestrator Agent from Mac OS X	20
3	Setting up ePolicy Orchestrator policies for Virex	21
	Setting policies within ePolicy Orchestrator	21
	General	23
	eUpdate	24
	Active Scanner	25
	Background Scanner	27
	Mounted Volumes Scanner	28
	On Demand Scanner	29
	Scheduling scans and eUpdates	30
	About scheduled tasks	30
	eUpdate	34
	Viewing ePolicy Orchestrator Server Properties	35
4	Controlling agent remotely	37
	Viewing agent properties	37
	Enforcing policies for ePolicy Orchestrator agent	38
	Agent Options	38
	Events	39
	Viewing server events	41
	Logging	42

5	Reports	45
	Reports	45
	Configuring Reports	46
	Glossary	47
	Index	51

1

Introduction

What's in this guide?

This guide describes how to configure Virex using McAfee ePolicy Orchestrator management software version 3.0.2 and later. To use this guide effectively, you need to be familiar with the ePolicy Orchestrator. For more information, see the *ePolicy Orchestrator Product Guide*. The ePolicy Orchestrator software provides a single point of control for your McAfee anti-virus products, from which to manage anti-virus policies and view reports of anti-virus events and virus activity in an enterprise environment. Using ePolicy Orchestrator, you can configure Virex on the target computers across your network; you do not need to configure them individually from the Virex **Preferences** dialog box.

This guide includes the following information:

- Adding ePolicy Orchestrator agent configuration to Policy Orchestrator server.
- Setting anti-virus policies on the target systems to configure the following Virex features:
 - General policies controlling overall functions for Virex.
 - eUpdate server policies.
 - Active Scanner policies.
 - Background Scanner policies.
 - Mounted Volumes Scanner policies.
 - On Demand Scanner policies.
- Configuring ePolicy Orchestrator Agent for Mac OS X.
 - Agent Communication interval.
 - Policy enforcement interval.
 - Event forwarding.
 - Logging.



This guide does not provide detailed information about installing or using ePolicy Orchestrator software. That information is provided in the *ePolicy Orchestrator Product Guide*.

Pre-requisites for using ePolicy Orchestrator to manage Virex

Before ePolicy Orchestrator software can configure Virex:

- Check-in Virex 7.7 NAP file in the ePolicy Orchestrator software repository.
- Check-in the Non Windows Agent¹ file in the ePolicy Orchestrator.
- Install Virex 7.7 on the Macintosh system.
- Install the ePolicy Orchestrator agent on Macintosh system.

Introducing ePolicy Orchestrator console

The Microsoft Management Console (MMC) is your interface to the ePolicy Orchestrator product and its features. Here you register and configure the Virex anti-virus products that are managed through ePolicy Orchestrator.

When you first log on to the server, the console appears with the Console Root highlighted in the left pane. The console's appearance changes to reflect the items you have selected in the console tree or in the details pane. The console uses standard MMC features.

Below the menus at the top of the window, the console is divided into two sides or panes.

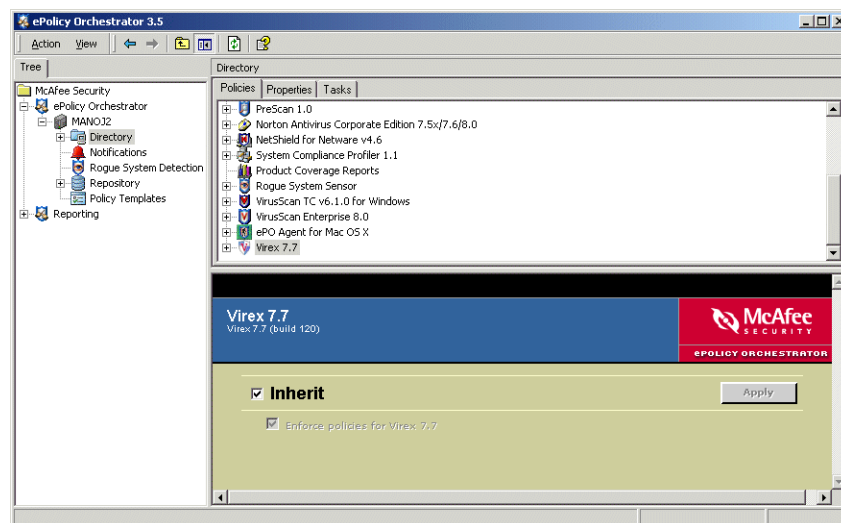


Figure 1-1 ePolicy Orchestrator console

- The **Console tree** is the left of the console. It shows the servers, workstation, and appliances that you can administer.
- The **Details pane** is the right of the console. Depending on the item selected in the console tree, the details pane might have an **Upper details pane** and **Lower details pane**.






¹ Non Windows Agent (NWA) is also known as ePolicy Orchestrator Agent for Mac OS X.

Audience

This guide is designed for system and network administrators who are responsible for their company's anti-virus program.

Conventions

This guide uses the following conventions:

Bold Serif	All words from the user interface, including options, menus, buttons, and dialog box names. Example: Type the User name and Password of the desired account.
Courier	The path of a folder or program; a web address (URL); text that represents something the user types exactly (for example, a command at the system prompt). Examples: The default location for the program is: C:\Program Files\McAfee\EPO\3.5.0 Visit the McAfee web site at: http://www.mcafee.com Run this command on the client computer: C:\SETUP.EXE
<i>Italic</i>	For emphasis or when introducing a new term; for names of product documentation and topics (headings) within the material. Example: Refer to the <i>Virex 7.7 Product Guide</i> for more information.
<TERM>	Angle brackets enclose a generic term. Example: In the console tree under ePolicy Orchestrator , right-click <SERVER>.
	Note: Supplemental information; for example, an alternate method of executing the same command.
	Tip: Suggestions for best practices and recommendations from McAfee for threat prevention, performance and efficiency.
	Caution: Important advice to protect your computer system, enterprise, software installation, or data.
	Warning: Important advice to protect a user from bodily harm when interacting with a hardware product.
	New: New or redesigned feature or option of this release of the product.

Resources

McAfee® products denote years of experience, and commitment to customer satisfaction. The McAfee PrimeSupport® team of responsive, highly skilled support technicians provides tailored solutions, delivering detailed technical assistance in managing the success of mission critical projects — all with service levels to meet the needs of every customer organization. McAfee Research, a world leader in information systems and security research, continues to spearhead innovation in the development and refinement of all our technologies.

Refer to these sections for additional resources:

- Getting product information.
- Links from within the product.
- Product services.
- Contact information.

Getting product information

Unless otherwise noted, the product documentation is provided as Adobe Acrobat .PDF files available on the product CD or from the McAfee download site.

Product Guide — Product introduction and features, detailed instructions for configuring the software, information on deployment, recurring tasks, and operating procedures. This guide (*Virex Product Guide* in PDF) is available in the **Documentation** folder of the product package.

Help — High-level and detailed information accessed from the software application.

Configuration Guide — *For use with ePolicy Orchestrator®*. Procedures for deploying and managing Virex through the ePolicy Orchestrator management software. This guide (*Virex Configuration Guide - for use with ePolicy Orchestrator* in PDF) is available in the ePolicy Orchestrator Server package.

Release Notes — *ReadMe*. Product information, resolved issues, any known issues, and last-minute additions or changes to the product or its documentation. This *ReadMe* is available in the **Documentation** folder of the product package.

Contacts — Contact information for McAfee services and resources: technical support, customer service, Security Headquarters (AVERT Anti-Virus & Vulnerability Emergency Response Team), beta program, and training. This file also includes phone numbers, street addresses, web addresses, and fax numbers for company offices in the United States and around the world.

License — The McAfee License Agreement booklet that includes all of the license types you can purchase for your product. The License Agreement sets forth general terms and conditions for the use of the licensed product. This McAfee Software license agreement is available in the **Documentation** folder of the product package.

Links from within the product

The product provides links to some useful resources:

- Online Help.

- Virus Information Library.
- Technical Support for ePolicy Orchestrator.
- Minimum Escalation Resource Tool.
- AVERT Web Immune.
- McAfee Security Home Page.

Online Help

Use this link to access the online Help topics for the product.



If the product's built-in help system (accessed from within the software by clicking the **Help** menu) displays incorrectly on your system, your version of Microsoft® Internet Explorer may not be using ActiveX controls properly. These controls are required to display the help file. Make sure that you install the latest version of Internet Explorer.

Virus Information Library

Use the **Virus Information** link to access the McAfee Anti-Virus & Vulnerability Emergency Response Team (AVERT) Virus Information Library. This web site has detailed information on where viruses come from, how they infect your system, and how to remove them.

In addition to genuine viruses, the Virus Information Library contains useful information on virus hoaxes, such as those virus warning that you receive via e-mail. A *Virtual Card For You* and *SULFNBK* are two of the best-known hoaxes, but there are many others. Next time you receive a well-meaning virus warning, view our hoax page before you pass the message on to your friends.

To access the Virus Information Library:

- 1 Open ePolicy Orchestrator.
- 2 Select **Virus Information Library** link from the **Start Page**.

Technical Support for ePolicy Orchestrator

Use the **Technical Support** link to access the McAfee PrimeSupport KnowledgeCenter Service Portal web site. Browse this site to view frequently asked questions (FAQs), documentation, and perform a guided knowledge search.

- 1 Open ePolicy Orchestrator.
- 2 Click **Technical Support for ePolicy Orchestrator** link from the **Start Page**.

Minimum Escalation Resource Tool

Use the Minimum Escalation Resource Tool link to access the McAfee PrimeSupport KnowledgeCenter Service Portal web site. Login to the support site for registering escalations.

- 1 Open ePolicy Orchestrator.
- 2 Click **Minimum Escalation Resource Tool** link from the **Start Page**.

AVERT Web Immune

Use the AVERT Web Immune link to access the Avert Web Immune Portal web site.

- 1 Open ePolicy Orchestrator.

- 2 Click **AVERT Web Immune** link from the **Start Page**.

McAfee Security Home Page

Use the McAfee Security Home Page link to access the McAfee Security Home Page web site.

- 1 Open ePolicy Orchestrator.
- 2 Click **McAfee Security Home Page** link from the **Start Page**.

Product services

The following services are available to help you get the most from your McAfee products:

- Beta program.
- HotFixes and Patches.
- Product “end-of-life” support.

Beta program

The McAfee beta program enables you to try our products before full release to the public — you can learn about and test new features for existing products, as well as try out entirely new products. This program can help you test and implement updated and new features earlier, and in a safe environment. You get the chance to suggest new product features, as well as deal directly with McAfee engineering staff.

To find out more, visit:

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

HotFixes and Patches

HotFixes and Patches are released with updated files, drivers, executables, etc., between the major releases of a product. To access the latest HotFixes and Patches, visit:

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

Product “end-of-life” support

Your anti-virus software must be kept up-to-date to remain effective against viruses and other potentially harmful software. It is important to update the virus definition (DAT) files regularly. To enable the software to counter the continuing threat, we often make architectural changes to the way that the DAT files and virus-scanning engine work together. It is therefore important that you update your engine when a new version is released. An older engine will not catch many of the new emerging threats.

When we release a new engine, we announce the date after which the existing engine will no longer be supported. For information on our product “end-of-life” policy and for a full list of supported engines and products, visit:

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

Contact information

Technical Support

Home Page	http://www.mcafeesecurity.com/us/support/technical_support
KnowledgeBase Search	https://knowledgemap.nai.com/phpclient/homepage.aspx
PrimeSupport Service Portal *	https://mysupport.nai.com

McAfee Beta Program

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

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

Home Page	http://www.mcafeesecurity.com/us/security/home.asp
Virus Information Library	http://vil.nai.com
AVERT WebImmune, *	https://www.webimmune.net/default.asp
Submitting a Sample	
AVERT DAT Notification Service	http://vil.mcafeesecurity.com/vil/join-DAT-list.asp

Download Site

Home Page	http://www.mcafeesecurity.com/us/downloads/
DAT File and Engine Updates	http://www.mcafeesecurity.com/us/downloads/updates/default.asp ftp://ftp.mcafeesecurity.com/pub/antivirus/datfiles/4.x
Product Upgrades *	https://secure.nai.com/us/forms/downloads/upgrades/login.asp

Training

On-Site Training	http://www.mcafeesecurity.com/us/services/security/home.htm
McAfee University	http://www.mcafeesecurity.com/us/services/education/mcafee/university.htm

Customer Service

E-mail	https://secure.nai.com/us/forms/support/request_form.asp
Web	http://www.mcafeesecurity.com/us/index.asp http://www.mcafeesecurity.com/us/support/default.asp

US, Canada, and Latin America
toll-free:

+1-888-VIRUS NO or **+1-888-847-8766**

Monday – Friday, 8 a.m. – 8 p.m., Central Time

For additional information on contacting McAfee — including toll-free numbers for other geographic areas — see the Contact file that accompanies this product release.

* Logon credentials required.

2 Installation

Introduction

The agent is the distributed component of ePolicy Orchestrator that is installed on each Macintosh computer on the network. The agent collects and sends information between the ePolicy Orchestrator server, repositories and manage Virex installations across the network. How you configure the agent and its policy settings determines how it facilitates communication and updating in your environment.

System Requirement

The agent can be installed on Macintosh operating systems such as:

- Mac OS 10.2.6
- Mac OS 10.2.8
- Mac OS 10.3.x
- Mac OS 10.4.x

and on any of the following Macintosh platforms:

- G3
- G4
- G5

Configuring ePolicy Orchestrator console for managing Virex

The computer that has an ePolicy Orchestrator Agent fully installed, enables you to easily make reporting available. In order to set up reporting for your computers you need to perform the following steps:

- Ensure that you have configured the ePolicy Orchestrator server IP address and port from your client computer's ePolicy Orchestrator Configurator user interface.

Check in NAP files to manage Virex

Network Associate Package file (NAP file). This file extension used to designate McAfee software program files that are installed in the software repository for ePolicy Orchestrator to manage. ePolicy Orchestrator server installs with a set of policy pages for major supported products that are available when your version of ePolicy Orchestrator was released. To manage Virex, you must first add the appropriate NAP files of the product to the software repository.

Where can I find the *.NAP files for Virex that I want to add to the repository?

McAfee releases NAP files for all anti-virus and security products supported by ePolicy Orchestrator. The NAP file for a given product is available with the other installation files for that product. These can be either on the product CD or in the product ZIP file if you downloaded the installation files from the McAfee web site. The NAP files for Virex is available in the **ePolicy Orchestrator Server Components** sub folder on the product CD or in the product ZIP file. The NAP file always has a .NAP file extension and is named with a product name code and version number, such as NWA-MAC300.NAP.

Policy pages are not added to the master repository; they are stored on the ePolicy Orchestrator server. Because of this, NAP files are not replicated to distributed repositories or updated to Macintosh computers.

Adding Macintosh Non Windows Agent (NWA) .NAP file

To check in a Macintosh Non-Windows Agent NAP file to the ePolicy Orchestrator server:

- 1 Locate the NAP file, either on the product CD or in the installation ZIP file that you downloaded from the McAfee web site, and save it to a temporary folder accessible from the ePolicy Orchestrator server.
- 2 Log on to the ePolicy Orchestrator server with administrative rights.
- 3 In the ePolicy Orchestrator console tree, right-click **Repository** and select **Configure Repository**. The **Configure Software Repository** wizard appears.

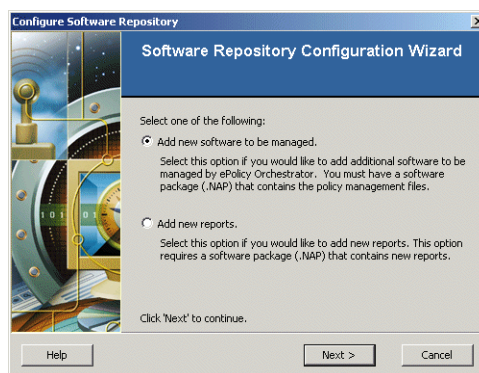


Figure 2-1 Configure Software Repository wizard



If you double-click **Repository** in the ePolicy Orchestrator console tree and click the **Check in NAP** link in the right-hand details pane, the **Configure Software Repository** wizard appears.

- 4 In the **Configure Software Repository** wizard, select **Add new software to be managed** and click **Next**.

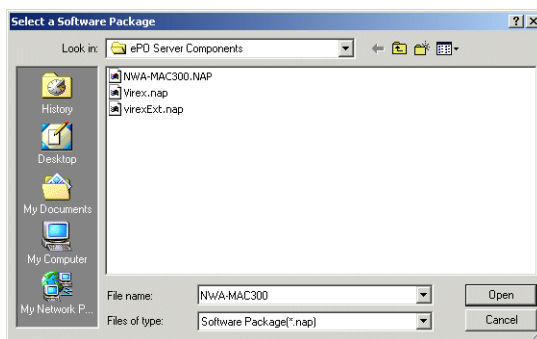


Figure 2-2 Select a Software Package dialog box

- 5 In the **Select a Software Package** dialog box, browse to and select **NWA-MAC300.NAP** file you saved to a temporary folder in **Step 1**.
- 6 Click **Open** to enable ePolicy Orchestrator to load NAP file.

Adding Virex .NAP file

To add a Virex .NAP file to the ePolicy Orchestrator server:

- 1 Locate the NAP file, either on the product CD or in the installation ZIP file downloaded from the McAfee web site, and save it to a temporary folder accessible from the ePolicy Orchestrator server.
- 2 Log on to the ePolicy Orchestrator server with administrative rights.
- 3 In the ePolicy Orchestrator console tree, right-click **Repository** and select **Configure Repository**. The **Configure Software Repository** wizard appears.
- 4 In the **Configure Software Repository** wizard, select **Add new software to be managed** and click **Next**.
- 5 In the **Select a Software Package** dialog box, browse to and select **Virex.NAP** file you saved to a temporary folder in **Step 1**.
- 6 Click **Open** to enable ePolicy Orchestrator to load NAP file.

Adding Report .NAP file

To add report NAP file to the ePolicy Orchestrator server:

- 1 Locate the NAP file, either on the product CD or in the installation ZIP file downloaded from the McAfee web site, and save it to a temporary folder accessible from the ePolicy Orchestrator server.
- 2 Log on to the ePolicy Orchestrator server with administrative rights.
- 3 In the ePolicy Orchestrator console tree, right-click **Repository** and select **Configure Repository**. The **Configure Software Repository** wizard appears.
- 4 In the **Configure Software Repository** wizard, select **Add new reports** and click **Next**.

- 5 In the **Select a Software Package** dialog box, browse to and select the **VirexExt.NAP** file you saved to a temporary folder in **Step 1**, and click **Open** to enable ePolicy Orchestrator to load the report NAP file into the repository.

Once ePolicy Orchestrator completes loading the NAP files, the agent will appear in the policy list in the upper details pane.

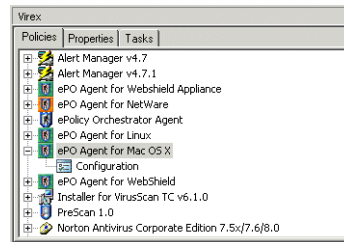


Figure 2-3 Policies tab

Installing agent for Macintosh systems

Agent installation directory

The agent is installed in /Library/NETAepoagt and also uses /Library/NETASSOC for configuration related data.



You cannot change the installation directory of Macintosh OS X ePolicy Orchestrator Agent.

Installing agent

The ePolicy Orchestrator Agent for Macintosh can be installed either through a standard (graphical interface) installation, or at a command line (silent install).

Standard Installation

- 1 Locate the **nwa.dmg**, either on the product CD or in the installation ZIP file downloaded from the McAfee web site, and save it to a temporary folder.



nwa.dmg is located in the **ePO Agent** folder of the **ePO Components.ZIP** file on the product CD.

- 2 Double-click **nwa.dmg**. This extracts the following files:
 - NWA.pkg
 - cmdinstall

- 3 Double-click **NWA.pkg**. The **Welcome to the ePO Agent for Mac OS X installer** window appears.

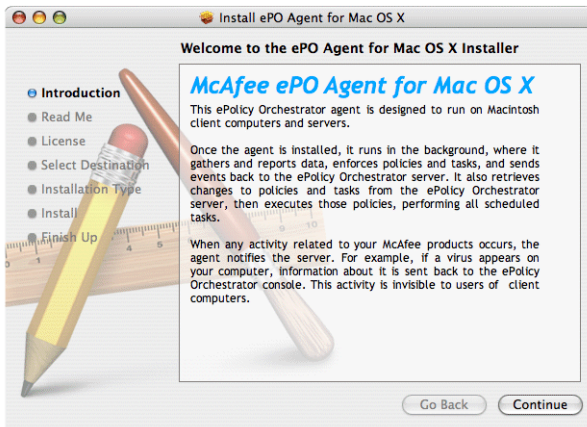


Figure 2-4 ePO Agent installation window - Introduction

- 4 Click **Continue**. The **ReadMe** window appears. This ReadMe describes the agent features, lists any known behavior or other issues with the agent release.
- 5 Click **Continue**. The **Software License agreement** window appears.



Read and accept the license agreement. If you do not accept the license agreement, the installation cannot continue.

- 6 Click **Continue**. The **Select a Destination** windows appears. Select the volume you need to install the ePolicy Orchestrator Agent and click **Continue**. The **Easy Install** window appears.



The **Easy Install** window with the **Install** button appears when:

- You are installing the agent for the first time.
- You are reinstalling the agent after you have uninstalled the previous ePolicy Orchestrator Agent installation.

If you are upgrading the ePolicy Orchestrator Agent the following window is displayed.

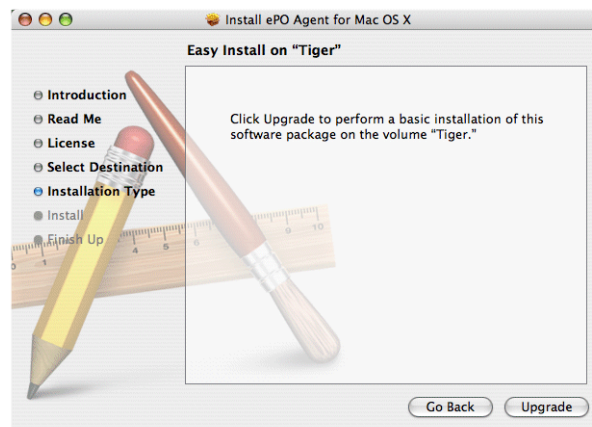


Figure 2-5 ePO Agent installation window - Upgrade

- 7 Click **Install/Upgrade** to continue. Installer will require you to authenticate before you continue. Type your password and click **OK**. The **Install Software** window appears.

During this process, the installer will require you to authenticate the **ePO Agent Configurator**. Type your password and click **OK**. The **ePO Agent Configurator** dialog box appears.

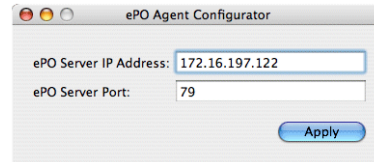


Figure 2-6 ePO Agent Configurator dialog box

- 8 Type the **ePO Server IP address** and the **ePO Server Port** number. Click **Apply**. The **Install Software** window appears.
- 9 Click **Restart** to complete the installation process.

Silent Installation (Command line)

- 1 Locate the **nwa.dmg**, either on the product CD or in the installation ZIP file downloaded from the McAfee web site, and save it to a temporary folder.



nwa.dmg is located in the **ePO Agent** folder of the **ePO Components.ZIP** file on the product CD.

- 2 Double-click **nwa.dmg**. This extracts the following files:
 - NWA.pkg
 - cmdinstall
- 3 Open the **Terminal** window and change the working directory to NAINWA.



You need to be have administrator rights to execute this command.

- 4 In the **Terminal** window, execute `sudo ./cmdinstall <ePO Server IP Address>:<ePO Server Port>`

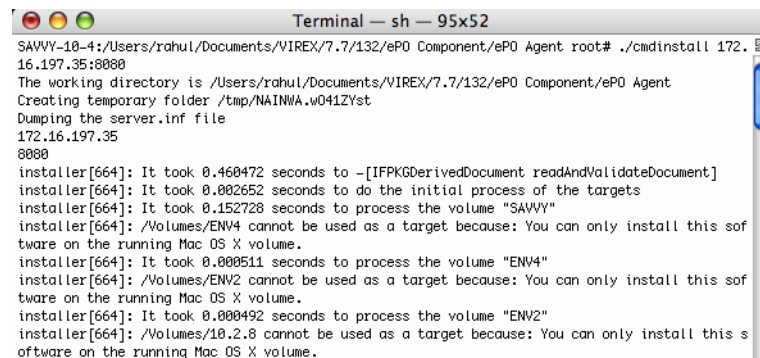


Figure 2-7 Terminal window - Start

- 5 When the silent installation completes, the **Terminal** window shows:

```

installer: Optimizing volume "SAVVY ": 99% complete
installer: Optimizing volume "SAVVY ": 99% complete
installer: Optimizing volume "SAVVY ": 99% complete
installer: Optimizing volume "SAVVY ": 100% complete
installer: Optimizing volume "SAVVY ": 100% complete
installer: Optimizing volume "SAVVY ": 100% complete
##
installer:
#
installer: The software was successfully installed.....
installer: The install was successful.
installer: The install recommends restarting now.
./cmdinstall: line 172: cd: /Users/rahul/Documents/VIREX/7.7/132/ePO: No such file or directory
Cleaning /tmp/NAINWA.w041Zyst
SAVVY-10-4:/Users/rahul/Documents/VIREX/7.7/132/ePO Component/ePO Agent root#

```

Figure 2-8 Terminal window - Install/Upgrade complete

- 6 You have successfully installed/upgraded your ePolicy Orchestrator Agent for Mac OS X.

Installing Virex



See *Virex 7.7 Product Guide* for installing Virex 7.7 software on Macintosh systems.

Uninstallation

Removing Virex NAP from ePolicy Orchestrator Server

You can uninstall the Virex NAP from the ePolicy Orchestrator server.

To remove the Virex NAP:

- 1 Log on to the ePolicy Orchestrator database server.
- 2 Select the **Virex** under **Repository | Managed Products | MAC OS X** in the console tree.

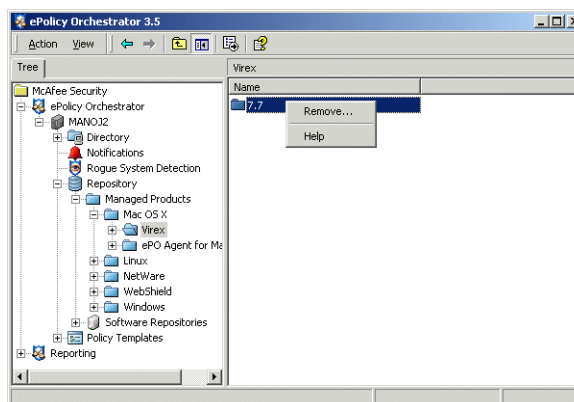


Figure 2-9 Virex NAP - Remove

- 3 Right-click on **Virex** and select **Remove** to uninstall Virex NAP from the ePolicy Orchestrator server.

Removing ePolicy Orchestrator Agent from ePolicy Orchestrator server



You **cannot** remove the **ePolicy Orchestrator Agent for MAC OS X** from the ePolicy Orchestrator server after you have checked it in.

Removing ePolicy Orchestrator Agent from Mac OS X

You can uninstall the ePolicy Orchestrator Agent from a Macintosh computer using the command line.

From the Command line

- 1 Log in as root user.



By default the root user on a Macintosh system is disabled, enable the root user if it is disabled. If you have logged in as user, open the **Terminal** window, type “**su**” and type the root password to log in as the root user.

- 2 Go to /Library/NETAepoagt
- 3 Run cmduninst

3

Setting up ePolicy Orchestrator policies for Virex

This chapter explains how you enforce Virex policies from ePolicy Orchestrator. There are two main steps:

- Within ePolicy Orchestrator, you select the names of the computers and the Virex policies that will apply to those computers. For example, you want computers A and B to scan for virus. You can set up many different policies that will apply to many individual computers or groups of computers.
- You ask ePolicy Orchestrator to enforce those policies on computers, the agent communicates with the server to check for new policies. The computer then observes your policy, ignoring any policy that was previously configured at the Virex **Preferences** dialog box.

Setting policies within ePolicy Orchestrator

ePolicy Orchestrator console allows you to enforce policies, across groups of computers or on a single computer. These policies override configurations set on individual computers. For information regarding policies and how they are enforced, see the *ePolicy Orchestrator Product Guide*.

Before configuring any policies, select the group of computers in the console tree for which you want to modify Virex policies. You can modify Virex policies from the Virex pages and tabs that are available in the details pane of the ePolicy Orchestrator console. These pages are nearly identical to the pages and dialog boxes that you can access from the Virex user interface directly. For complete information about these configuration options in Virex 7.7, see the *Virex 7.7 Product Guide*.

After you have modified the policy and save changes for the intended computer or group of computers, you are ready to deploy the new settings via the ePolicy Orchestrator Agent. [See Enforcing policies on page 22.](#)

To modify policies for Virex in ePolicy Orchestrator:

- 1 Log on to the ePolicy Orchestrator server.
- 2 In the console tree under ePolicy Orchestrator | <SERVER> | Directory, select the site, group, single computer, or the entire Directory. The **Policies**, **Properties**, and **Tasks** tabs appear in the upper details pane.
- 3 Select the **Policies** tab in the upper details pane, then expand Virex. A single entry appears beneath the Virex entry.

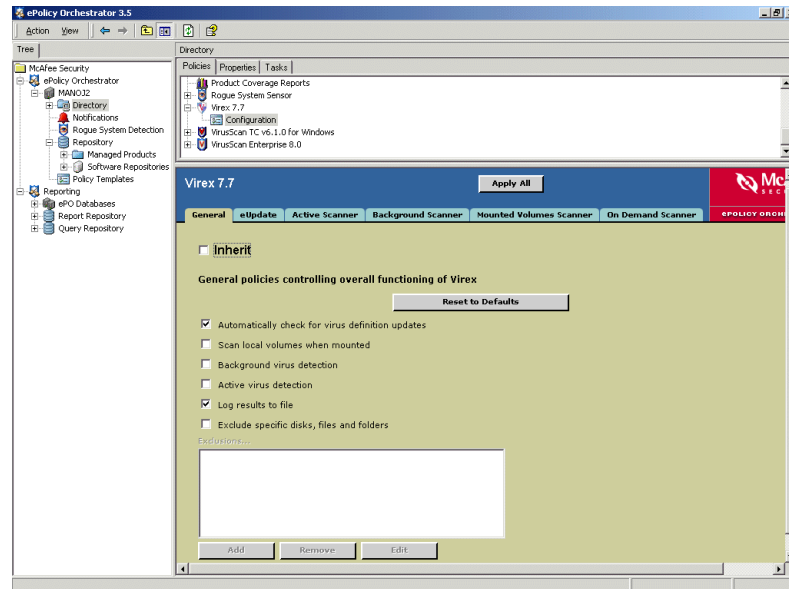


Figure 3-1 ePolicy Orchestrator console - Virex

The lower pane reflects the configuration options found within the Virex interface:

- General
 - eUpdate
 - Active Scanner
 - Background Scanner
 - Mounted Volumes Scanner
 - On Demand Scanner
- 4 In the lower details pane, select an option from the left pane, such as **General**.
 - 5 In the **General** page, deselect **Inherit**.
 - 6 Configure the required options.



These pages are identical to the pages within Virex. To learn more, see the Virex 7.7 Product Guide.

- 7 Click **Apply** to save these settings. You can continue to configure policies, then click **Apply All** to enforce all the policies that you configured.

Enforcing policies

After you have configured policies, you must enforce them onto the Virex installed computers.

- 1 In the console tree under Directory, select the site, group, single computer, or the entire Directory.

- 2 In the upper details pane on the **Policies** tab, select **Virex**. The **Virex** page appears in the lower details pane.
- 3 Deselect **Inherit**.
- 4 Select **Enforce Policies for Virex 7.7**.
- 5 Click **Apply** to save these settings.

The ePolicy Orchestrator software will make the policies that you configured available to the ePolicy Orchestrator Agent on the Virex computers.

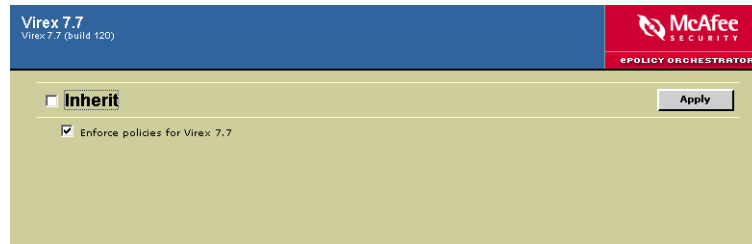


Figure 3-2 Enforce Policies for Virex 7.7

General

The **General** tab allows you to enforce general policies controlling overall functioning of Virex like automatically checking for virus definitions updates, scanning local volumes when they are mounted, logging scan results, detecting virus in the background and creating exclusion lists for specific disks, files and folders.

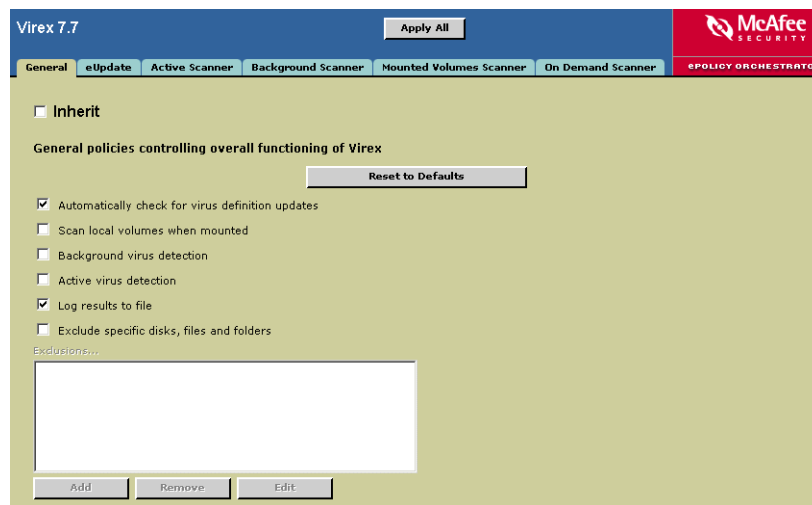


Figure 3-3 General tab

You can enforce the following General policies:

Automatically Check for virus definition updates	Enables/disables automatic eUpdates.
Scan local volumes when mounted	Enables/disables the Mounted Volumes scanner.
Background virus detection	Enables/disables the Background scanner.
Active virus detection	Enables/disables the Active scanner.
Log results to file	Enables/disables logging results to a file.
Exclude specific disks, files and folders	<p>Configures your scanning exclusions. The exclusions are stored as a list in a text file called VShieldExclude.txt, if this is not selected then you will not have any exclusions set.</p> <p>Add Exclusion:</p> <ul style="list-style-type: none"> Click Add, you will see the Add Scan Item -- Web Page Dialog. Type the full path of the file, directory or disk you want to exclude and click OK. The exclusions will be listed in the Exclusion list. <p>Remove Exclusion:</p> <ul style="list-style-type: none"> Select the exclusion in the Exclusion list and click Remove. <p>Edit Exclusion:</p> <ul style="list-style-type: none"> Select the exclusion in the Exclusion list and click Edit to modify the exclusion.

eUpdate

The **eUpdate** tab allows you customize DAT file and virus-scanning engine update settings. eUpdate keeps your anti-virus software continuously updated with new information on viruses and scanning capabilities. You can update your DAT and engine files using FTP or HTTP.

Virex 7.7

Apply All

General eUpdate Active Scanner Background Scanner Mounted Volumes Scanner On Demand Scanner ePOLICY ORCHESTRATOR

☐ Inherit

eUpdate Server policies

☒ Customize eUpdate Settings

Reset to Defaults

☒ FTP

Server URL: ftp.nai.com

Port: 21

Username: anonymous

Password: *****

Account:

Directory: /virusdefs/mac/virex7/

☐ HTTP

Server URL:

Username:

Password:

Figure 3-4 eUpdate tab

Customize eUpdate settings

You can enforce the following eUpdate settings for Virex:

FTP

File Transfer Protocol (FTP) is a way of sending and receiving files across the Internet. You need to specify the server details from where you need to transfer files to your computer to update your DAT and Engine files.

Server URL	Specify the server URL for downloading DAT and Engine updates.
Port	Specify the port number you want to use for FTP.
Username	Type the username.
Password	Type your password.
Account	Type your FTP account.
Directory	Specify the path where your DAT and Engine files are located.

HTTP

HTTP (Hypertext Transfer Protocol) is the set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. You need to specify the server URL from where you need to transfer files to your computer to update your DAT and Engine files.

Server URL	Specify the server URL for downloading DAT and Engine updates.
Username	Type the username.
Password	Type your password.

Active Scanner

The Active Scanner feature in Virex provides continuous anti-virus protection on the hard disk from network connections and the Internet. As the Active Scanner is continuously working on your computer, your system will not be exposed to the risk of infection.

The Active Scanner scans files when they are written to your hard drive (all partitions) and all removable drives. It starts when your computer starts and runs until the computer is shut down; the scanner is running on your computer by default. You can configure what the scanner looks for and how it will respond to infected files.

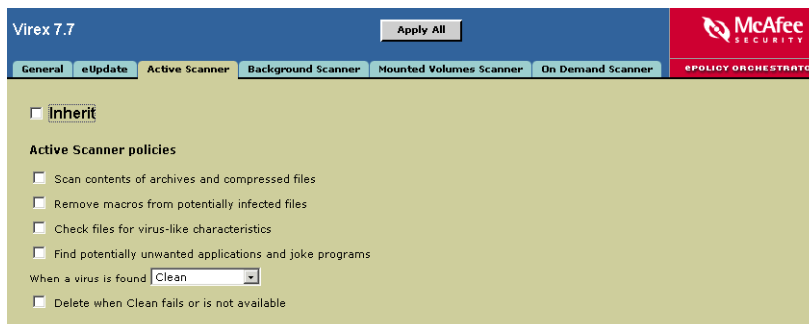


Figure 3-5 Active Scanner tab

You can enforce the following Active Scanner policies:

Scan contents of archives and compressed files	Sets the selected scanner to scan into archives and other compressed files. On by default for Background and On-Demand scanner.
Remove Macros from potentially infected files.	If an infected file is detected then all macros from the file will be removed as part of the cleaning process.
Check files for virus-like characteristics	Enables/disables heuristics, which scans for files that show characteristics of viruses or worms and may contain unknown infections. On by default for Background scanner.
Find potentially unwanted application and joke programs.	Enables/disables the scanner to check for unwanted programs or joke programs.
when virus found:	Selects the primary action of the scanner.
<ul style="list-style-type: none"> ■ Clean ■ Delete ■ Notify 	
Delete when Clean fails or is not available.	Selects the secondary action for the selected scanner. This is only available when the primary action is Clean.

Background Scanner

The Background Scanner is a feature that permanently scans all files on your system. The scanner protects your computer by continuously searching your system for infected files. This scan is a low-resource operation so there is no performance decrease to your computer. You can configure what the scanner looks for and how it responds to infected files.

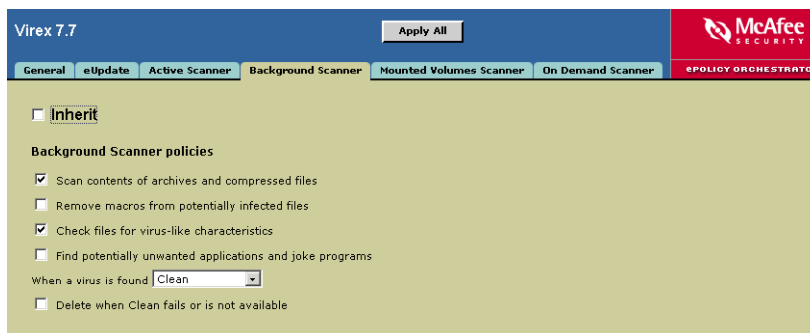


Figure 3-6 Background Scanner tab

You can enforce the following Background Scanner policies:

Scan contents of archives and compressed files	Sets the selected scanner to scan into archives and other compressed files. On by default for Background and On-Demand scanner.
Remove Macros from potentially infected files.	If an infected file is detected, then all macros from the file will be removed as part of the cleaning process.
Check files for virus-like characteristics.	Enables/disables heuristics, which scans for files that show characteristics of viruses or worms and may contain unknown infections. On by default for Background scanner.
Find potential unwanted application and joke programs.	Enables /disables the scanner to check for unwanted programs or joke programs.
when virus found: ■ Clean ■ Delete ■ Notify	Selects the primary action of the scanner.
Delete when Clean fails or is not available.	Selects the secondary action for the selected scanner. This is only available when the primary action is Clean.

Mounted Volumes Scanner

The Mounted Volumes Scanner initiates scanning of a volume such as a CD or camera when one is locally mounted. With this scanner you can scan a large volume or device for infection before interfacing it with your system. This limits your system's exposure to malicious viruses. This feature only works with locally inserted or ejectable media, such as Zip drives, CD, DVD, or OS X .DMG files. It also scans USB card devices such as pen drives and cameras, and Firewire devices such as iPod. It does not scan volumes on remote machines connected through the network. The scanner operates in the background and interacts with the user.

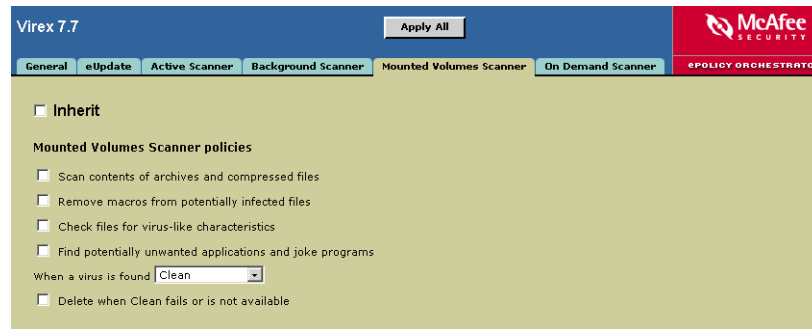


Figure 3-7 Mounted Volumes Scanner

You can enforce the following Mounted Volumes Scanner policies:

Scan contents of archives and compressed files	Sets the selected scanner to scan into archives and other compressed files.
Remove Macros from potentially infected files.	If an infected file is detected then all macros from the file will be removed as part of the cleaning process.
Check files for virus-like characteristics	Enables / Disables heuristics, which scans for files that show characteristics of viruses or worms and may contain unknown infections.
Find potentially unwanted application and joke programs.	Enables / Disables the scanner to check for unwanted programs or joke programs.
when virus found:	Selects the primary action of the scanner.
<ul style="list-style-type: none"> ■ Clean ■ Delete ■ Notify 	
Delete when Clean fails or is not available.	Selects the secondary action for the selected scanner. This is only available when the primary action is Clean.



The Mounted Volumes scanner is not running on your computer by default.

On Demand Scanner

The On Demand Scanner allows you to initiate a scan at any time by dragging and dropping selected files into the console or through a file **Open** dialog box. With the On-Demand Scanner, you can select multiple files, directories, or volumes. Scan results are summarized in a report that can be saved or printed. You can configure what the scanner looks for and how it responds to infected files. You can also configure an exclusion list that is shared with the Active Scanner, Background Scanner and Mounted Volumes Scanner. The scanner notifies you when it finds a virus and generates a log that appends its actions.

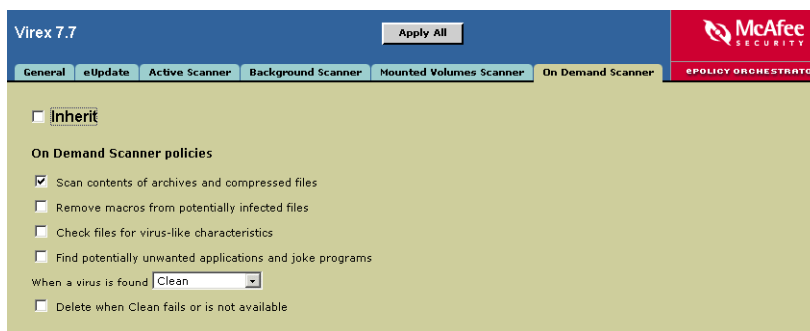


Figure 3-8 On Demand Scanner tab

You can enforce the following On Demand Scanner policies:

Scan contents of archives and compressed files	Sets the selected scanner to scan into archives and other compressed files. On by default for On-Demand scanner.
Remove Macros from potentially infected files.	If an infected file is detected then all macros from the file will be removed as part of the cleaning process.
Check files for virus-like characteristics.	Enables / Disables heuristics, which scans for files that show characteristics of viruses or worms and may contain unknown infections.
Find potentially unwanted application and joke programs.	Enables / Disables the scanner to check for unwanted programs or joke programs.
when virus found:	Selects the primary action of the scanner.
<ul style="list-style-type: none"> ■ Clean ■ Delete ■ Notify 	
Delete when Clean fails or is not available.	Selects the secondary action for the selected scanner. This is only available when the primary action is Clean.

Scheduling scans and eUpdates

When Virex scans for viruses, it uses information in the “virus definition (DAT) file” to find and remove viruses. Many new viruses are discovered daily, and we regularly create new DAT files to provide protection from these viruses. To ensure the best anti-virus protection, you can use ePolicy Orchestrator to inform Virex where to access the latest DAT files, and create schedules for replacing earlier DAT files, and running on-demand scans.

About scheduled tasks

Using ePolicy Orchestrator, you can create these types of scheduled tasks for the Virex software:

- On-demand scan
- eUpdate

Scheduled tasks for a computer could be set to execute based on the local time or GMT (Greenwich Mean Time). However, ePolicy Orchestrator cannot monitor the progress of the task, so we recommend that you periodically view the log on the server.

On Demand scan

Virex can perform on-demand scanning of your files, so that all files in the databases are checked for questionable content. You can create any number of on-demand scan schedules. The scan schedules can be configured to run at set intervals, and can be run at any time by the user. You can disable schedules that you do not want to run automatically.

Creating a new task

To create a new task:

- Click the **Tasks** tab in the upper details pane. Right-click in the pane, and select **Schedule Tasks** option.

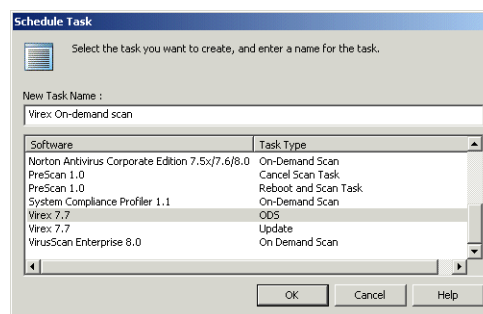


Figure 3-9 Schedule Tasks

- Type a name for the task in the **New Task Name** field and select the task you want to create. In the **Task Type** drop down list, select **On-Demand Scan**. Click **OK**.

- The created task is listed in the **Tasks** pane.

Directory							
Task Name	Last Modified At	Created At	Enabled	Schedule Type	Start Date	Start Time	
Deployment	Directory	Directory	False	Daily	9/20/2004	12:00:00 AM (Local)	
Virex On-demand scan	Directory	Directory	False	Daily	5/25/2005	2:14:00 PM (Local)	
Update Virex 7.7	Directory	Directory	False	Daily	5/25/2005	2:15:00 PM (Local)	

Figure 3-10 Tasks tab

Editing a task

To edit a task:

- Right-click the task and select the **Edit Task** option.

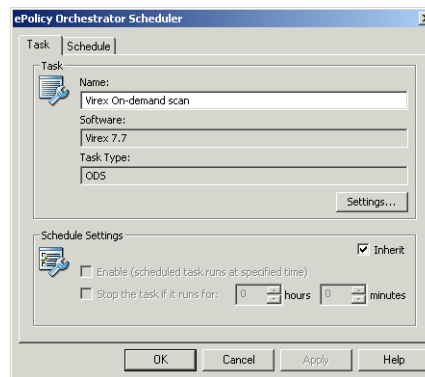


Figure 3-11 ePolicy Orchestrator Scheduler - Task tab

- Click **Setting** to include files and directory in the scheduled scan. [See On Demand Scanner on page 29.](#)

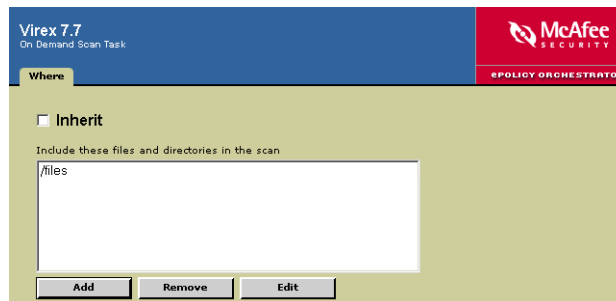


Figure 3-12 On Demand scan - Include files and directories



Deselect **Inherit** and select **Enable (schedule task runs at specified time)** to enable the task settings in the **Schedule Settings** pane.

Include these files and directories in the scan.	<p>Configures your scanning inclusions.</p> <p>Add inclusion:</p> <ul style="list-style-type: none"> Click Add, you will see the Add Scan Item -- Web Page Dialog. Type the full path of the file, directory or disk you want to include and click OK. The inclusion will be listed in the Inclusion list. <p>Remove inclusion:</p> <ul style="list-style-type: none"> Select the inclusion in the Exclusion list and click Remove. <p>Edit inclusion:</p> <ul style="list-style-type: none"> Select the inclusion in the Inclusion list and click Edit. You will see the Add Scan Item -- Web Page Dialog, modify the full path of the file or directory you want to include in the scan and click OK.
--	--

Schedule Settings

Enable (schedule task runs at specified time)	Select to enable the task to run at a specified time.
Stop the task if it runs for:	Specify the hours and minutes to stop to limit the length of time the task can run before it is cancelled.

Schedule tab

There are many options when scheduling a task.

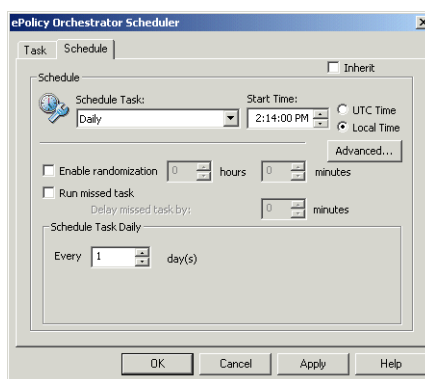


Figure 3-13 ePolicy Orchestrator Scheduler - Scheduler tab

Schedule Task	<p>Select the task type from the drop down. You can select any one of the following option.</p> <ul style="list-style-type: none"> ■ Daily ■ Weekly ■ Monthly ■ Once ■ At System Startup ■ Run Immediately
Start Time <ul style="list-style-type: none"> ■ UTC Time ■ Local Time 	<p>Specify the start time for the schedule. Select the local time to run the task at the scheduled interval at the client computer system time. This is useful for scheduling processor-intensive tasks, such as on-demand scan, to run during non-business hours.</p> <p>Selecting UTC will run the task when the start time occurs UTC (Universal Time Conversion is also known as GMT, or Greenwich Mean Time). Using this option will cause the task to run at the same time for all your Macintosh clients regardless of the local system time on the Macintosh systems.</p>
Enable randomization	The task does not run at exactly the specified start time, instead, it starts after a random, specified time. Specify the hours and minutes to enable randomization.
Run missed task	Ensures that the task is started if the Macintosh computer is shutdown or other wise not available during the scheduled start time. Selecting this option runs the task the next time the Macintosh computer becomes available.
Delay missed task by	Click Advanced on the Advanced Schedule Options dialog box. When running missed tasks, selecting this option sets a delay after the Macintosh computer becomes available before the missed tasks runs.
Start Date / End Date	Click Advanced on the Advanced Schedule Options dialog box. Type the start and end dates if you only want the task to run within a specified time frame for a few day or weeks for a temporary basis.
Repeat Task	<p>Click Advanced on the Advanced Scheduled Options dialog box. Use this option to run a task multiple times in the same day. To do this, check Repeat Task and then set the repeat interval appropriately.</p> <p>Typically, you might do this to run a client update task several times a day, especially if there are lots of new viruses appearing in the wild. You can also schedule the task to repeat during other intervals, such as weekly or monthly.</p>
Schedule Task Daily	Specify the interval to execute the schedule task; this would be an interval of 1 or several days. If you select 1, the schedule task is executed every other day.

Deleting a task

To delete a task:

- Right-click the task in the **Tasks** pane and select **Delete**.

eUpdate

When Virex performs a scan (according to your settings) it uses its anti-virus scanning engine and the current virus definition (DAT) files to find and remove viruses. Many new viruses are discovered daily, and we regularly create new virus definition files to provide protection from these viruses. Your anti-virus software can only provide full protection if you keep it up-to-date with the latest DAT file and virus-scanning engine. We recommend that you update Virex DAT files at least once a week, and regularly check the McAfee AVERT (Anti-Virus Emergency Response Team) web site for new DAT files. If you have multiple servers in the current domain (all running Virex), you can use one server to download the latest DAT file, then configure the others to copy the files from that server. Your servers can download files for a number of operating systems, regardless of the operating systems that are in use.

Specifying the location of the DAT files

You can specify the source of the DAT files using the eUpdate page. [See Customize eUpdate settings on page 25.](#)

Creating an eUpdate task

- 1 In the console tree under **ePolicy Orchestrator**, right-click directory or the site, group, or host, then select **Schedule Task**. The **Schedule Task** dialog box opens.

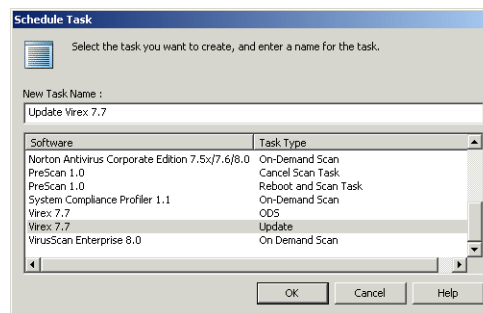


Figure 3-14 New update task

- 2 In the **Schedule Task** dialog box, Type a name in **New Task Name**.
- 3 Select **Virex 7.7 - Update** from the **Software/Task Type** list.
- 4 Click **OK** to create the Task.

Configuring an eUpdate task

After you have created a new eUpdate task, you can configure the task as required.

- 1 On the **Tasks** tab in the upper details pane, right-click the task, then select **Edit Task**. The **ePolicy Orchestrator Scheduler** dialog box appears.
- 2 Deselect **Inherit**. [See Editing a task on page 31.](#)
- 3 Click **OK** to return to **ePolicy Orchestrator Scheduler** dialog box.
- 4 To delete a Virex eUpdate task, [See Deleting a task on page 33.](#)

Disabling an eUpdate task

- 1 On the **Tasks** tab in the upper details pane, right-click the task, then select **Edit Task**. The **ePolicy Orchestrator Scheduler** dialog box appears.
- 2 Click **Settings button** when you have finished editing the required options, in the **ePolicy Orchestrator Scheduler** dialog box **Task** tab and **Schedule** tab. The **Virex eUpdate Task Settings** page appears.

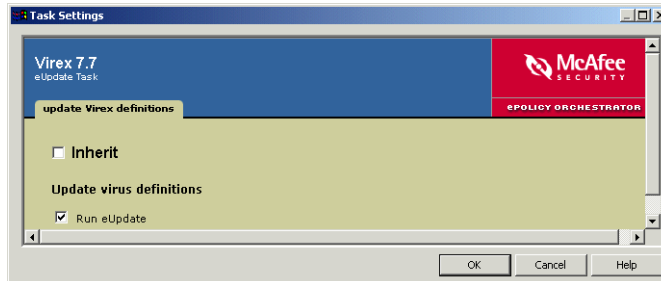


Figure 3-15 Update Virex Definitions - Run eUpdate

- 3 Deselect **Inherit** in the **Virex eUpdate Task Settings** page.
- 4 Deselect **Run eUpdate** and then select **Inherit**.
- 5 Click **OK** to return to **ePolicy Orchestrator Scheduler** dialog box.
- 6 To delete a Virex eUpdate task, [See Deleting a task on page 33](#).

Viewing ePolicy Orchestrator Server Properties

From ePolicy Orchestrator server, you can view various system properties.

To view the server properties:

- 1 Select the server in the console tree directory for which you want to view settings.

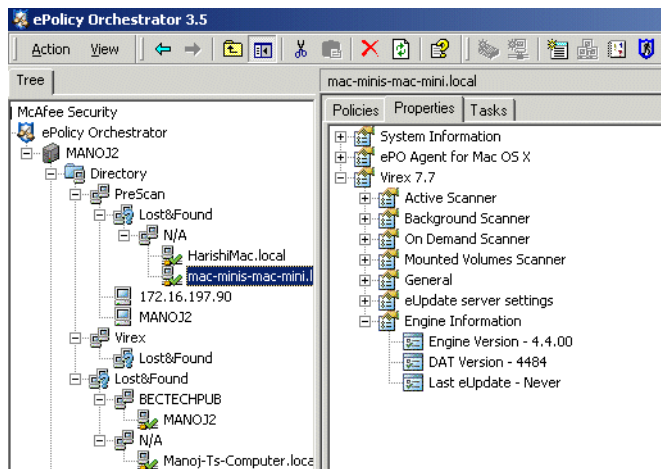


Figure 3-16 Console tree directory

- 2 In the upper details pane, click the **Properties** tab.
- 3 In the **Properties** pane, expand the **Virex 7.7** tree view to list its various properties.

- 4 Click + next to any property to view its details.

4

Controlling agent remotely

Viewing agent properties

You can use the ePolicy Orchestrator console to view current properties for a particular computer. These properties list basic system information, such as operating system, network IP address, RAM and processor speed. They also list properties for the agent and McAfee anti-virus or security products installed on that computer.

Especially when troubleshooting problems, it is a good idea to check computer policies to confirm that policy changes you have made in the console are actually being enforced on the Macintosh client. The agent sends properties back to the server at each ASCII, allowing you to see system properties on Macintosh client computers from the ePolicy Orchestrator console.

How are properties different from policies?

Policies are the rules you configure for the agent or for specific products in the policy pages on the ePolicy Orchestrator server. When the agent enforces these policies on the Macintosh client computer, they become properties. Properties are the settings that are actually in effect on the Macintosh client computer.

Viewing agent properties

To view the properties the agent collects for selected computers in the Directory:

- 1 In the console tree, select the computer where Virex is installed.

- 2 In the upper right details pane, click the **Properties** tab to display properties for the selected computer.

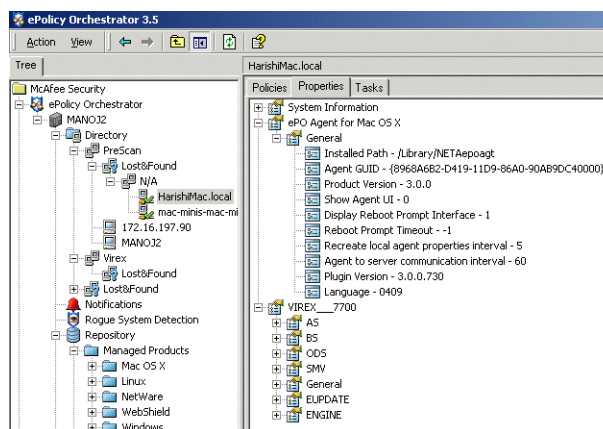


Figure 4-1 Viewing agent properties

- 3 Expand property types to view details on specific properties. Properties for the agent are listed under the ePolicy Orchestrator Agent.

Enforcing policies for ePolicy Orchestrator agent

After you have finished configuring policies, you must enforce them to make them available to the ePolicy Orchestrator agent on the Virex hosts.

In the ePolicy Orchestrator console tree, select the hosts for which you want to enforce policies.

- 1 In the upper details pane, select **ePO Agent for Mac OS X**.

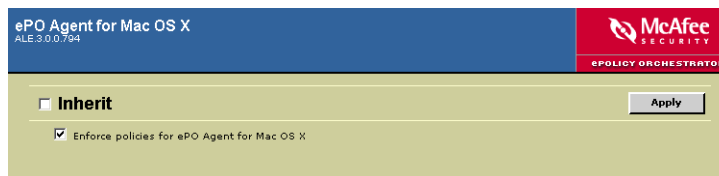


Figure 4-2 Enforce policies for ePolicy Orchestrator Agent for Mac OS X

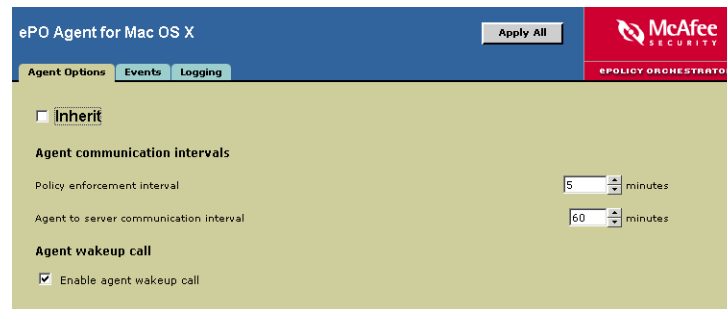
- 2 Deselect **Inherit**.
- 3 Select **Enforce policies** for ePolicy Orchestrator Agent for Mac OS X.
- 4 Click **Apply** to save the settings. The ePolicy Orchestrator software will make the policies that you configured available to the agent on the Virex hosts.

Agent Options

The agent is the distributed component of ePolicy Orchestrator that is installed on each Macintosh computer in your network. The agent collects and sends information between the ePolicy Orchestrator server, repositories, and managed client computers and products. How you configure the agent and its policy settings determines how it functions and facilitates communication and updating in your environment.

To configure the agent policy for a computer

- 1 In the ePolicy Orchestrator console tree, select the computer that you added for the Virex.
- 2 In the **Policies** tab (in the upper details pane), select **Configuration** under the **ePO Agent for Mac OS X** entry. The **Policy** page appears in the lower details pane.
- 3 On the **Agent Options** tab, deselect **Inherit**.

**Figure 4-3 ePolicy Orchestrator - Agent Options**

- 4 In **Policy Enforcement Interval**, choose an interval (in minutes) that best suits your organization. The default value is 5 minutes. You can use a value between 5 – 10,080 minutes (1 week).
- 5 In **Agent to server communication**, choose an interval (in minutes) that best suits your organization. The default value is 60 minutes. You can use a value between 5–2,880 minutes (2 days).
- 6 To allow the ePolicy Orchestrator server to send wake up calls to the agent, select **Enable agent wakeup call support**.

Events

The ePolicy Orchestrator server receives notifications from the Non Windows Agent. You must configure its policy pages to either forward events immediately to the ePolicy Orchestrator server or only at agent-to-server communication intervals.

If you choose to have events sent immediately, then all events with severity value equal or greater than the value configured for the agent is sent immediately.

If you choose not to have events sent immediately, then the agent forwards events irrespective of the severity only during the agent-to-server communication.

To set the ePolicy Orchestrator Agent policy:

- 1 Log in to the ePolicy Orchestrator server.
- 2 Select the Directory, or the desired site, group, or computer, then select the **Policies** tab in the upper details pane.
- 3 Select **ePolicy Orchestrator Agent for Mac OS X | Configuration** in the upper details pane.

- 4 In the lower details pane, select the **Events** tab.

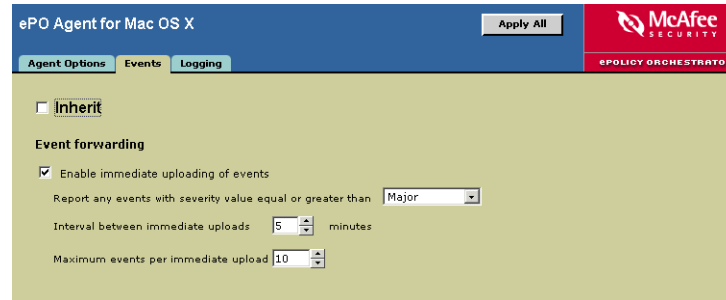


Figure 4-4 Events tab

- 5 Deselect **Inherit**.

Configure the following policy options:

Event forwarding

Select **Enable immediate uploading of events** to enable the agent to forward events to the server immediately.

Deselect this option to have the agent forward events only at the next ASCII. If this option is selected, you must specify:

- The lowest severity of events you want sent to the server in Upload events of priority <severity> and above. You can set severity values to Critical, Major, Minor, Warning, Informational. For example, if you select Minor, then all events with a severity of Minor or more severe get forwarded to the server.
 - The event forwarding interval in interval between immediate uploads. The quantity of time you select here determines the highest frequency that events are forwarded. For example, if you select 5 minutes then the agent forwards events to the server every five minutes at most.
 - The maximum number of events to send at a time in Maximum events per immediate upload. If the number of events exceeds this limit, the remaining events are sent during the next event forwarding interval.
- 6 Click **Apply All** to save these settings. Changes will take effect during the next agent-to-server communication.

Deleting old events from the database periodically

You may want to periodically delete events from the database to keep the database size down and improve performance. Many events, especially informational and minor events, are less useful over time. Furthermore, you can and should back up the database before deleting events of any kind from the database. You can archive this database and use it later for historical reporting if you need to.

Use this procedure to delete events permanently from the ePolicy Orchestrator database.

- 1 Log on to the desired ePolicy Orchestrator database server.

- 2 In the console tree under **Reporting | ePO Databases | <database server>**, select **Events**. The **Filtering**, **Import**, **Repair**, and **Removal** tabs appear in the details pane.

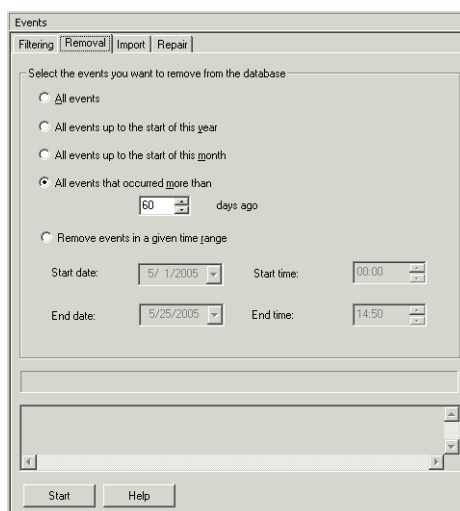


Figure 4-5 Events - Removal tab

- 3 Click the **Removal** tab.
- 4 Select the events that you want to remove from the database.
 - **All events** — Select this option to remove all events from the database.
 - **All events up to the start of the year** — Select this option to remove all events before the beginning of the current calendar year.
 - **All events up to the start of this month** - Select this option to remove all events before the beginning of the current month.
 - **All events that occurred more than X days ago** — Select this option to remove events older than the number of days you specify.
 - **Remove events in a given time range** — Select this option to specify a range of dates. Any events that occurred within the date range are removed.
- 5 Click **Start** to delete the specified events from the database.

Viewing server events

In the ePolicy Orchestrator console, you can view, save, and print all information, warning, and error events for each ePolicy Orchestrator server. Checking the server event window is a useful way to confirm the success or failure of actions initiated from the server, such as an agent push or pulling updated DAT files from a source repository.

In addition, you can also manage what events are saved in the ePolicy Orchestrator database. See *ePolicy Orchestrator product guide* on maintaining ePolicy Orchestrator Databases and about managing events in the database.

To view, save, or print server events from the ePolicy Orchestrator console:

- 1 Log on to the ePolicy Orchestrator server.

- 2 In the console tree under ePolicy Orchestrator, select the server node, then click the **General** tab in the details pane.
- 3 Click **Server Events** to open the **Server Event Viewer** dialog box.

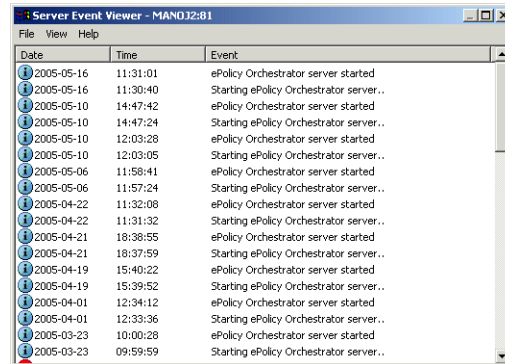


Figure 4-6 Server Event Viewer

- 4 Select **View | Refresh** to ensure the event list is current.

View details of a particular event

To view a detailed description of a server event, select and double-click the desired event. The **Server Event Detail** dialog box appears.

Save events to a log file

To save all server events to a Server Log (.log) file, select **File | Save As**. To save only selected server events to a Server Log file, select the desired events, then select **File | Save As**. In the **Save As** dialog box, select **Selected Items** only.

Print server events

To print all server events to the default printer, click **Print** on the **File** menu. To print only selected server events to the default printer, select the desired events, then select **File | Print**.

Logging

The agent on the Macintosh computer generates software events constantly during normal operation. These can range from informational events about regular operation, such as when the agent enforces policies locally or when it starts an on-demand scan. These events are logged by the agent and sent to the server at every ASCII and stored in the database. A typical deployment of ePolicy Orchestrator in a large network can generate thousands of these events every hour.

To set the ePolicy Orchestrator Logging policy:

- 1 Log in to the ePolicy Orchestrator server.
- 2 Select the Directory, or the desired site, group, or computer, then select the **Policies** tab in the upper details pane.

- 3 Select **ePolicy Orchestrator Agent for Mac OS X | Configuration** in the upper details pane.
- 4 In the lower details pane, select the **Logging** tab

These options allow you to configure policies for how the agent activity is logged.

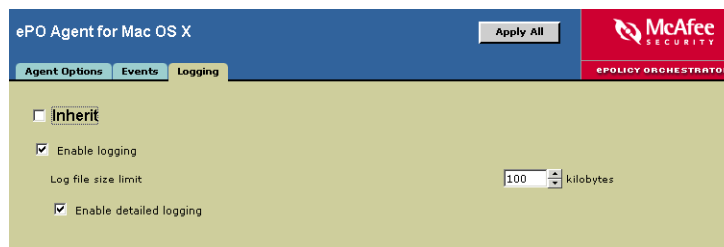


Figure 4-7 Logging tab

Logging agent policies	Property Description
Enable agent log	Choose whether to enable the agent log. Selecting this check box enables logging at /Library/NETAepoagt/Scratch/etc/log.
Enable detailed logging	Enable the detailed agent activity log agent_<computer>.log. The log file can grow very large. We recommend enabling detailed logging, otherwise only critical errors are logged that could be insufficient for troubleshooting specific communication problem.

5

Reports

Reports

From the ePolicy Orchestrator console, you can view reports which show how the Virex hosts are handling infections, and you can check the configuration that have been set up on the hosts. You can also create reports using data sent by Non Window Agent in the selected ePolicy Orchestrator database. You can also save the selections you make in the **Enter Report Inputs** and **Report Data Filter** dialog boxes for future use.

ePolicy Orchestrator reports allow you to:

- Set a directory filter to gather only the information that you want to view. When setting this filter you can choose which part of the ePolicy Orchestrator console tree is included in the report.
- Set a data filter, by using logical operators, to define precise filters on the data returned by for the report.
- Generate graphical reports from the information in the database, and filter the reports as desired. You can print the reports and export them for use in other software.
- Conduct queries of computers, events, and installations.

To run a report:

- 1 Log on to the ePolicy Orchestrator database server.
- 2 Select the desired Virex report under **Reporting | ePO Databases | <database server> | Reports | <report group>** in the console tree.
 - If the **Current Protection Standards** dialog box appears, specify the version numbers of virus definition files or the virus scanning engine on which you want to report.
 - If the **Enter Report Inputs** dialog box appears, make selections on any of the tabs that may appear: **Rules**, **Layout**, **Data Grouping**, **Within**, **Saved Settings**.



Tabs may vary based on which report is selected. See *ePolicy Orchestrator Product Guide* for more details on Rules, layout, Grouping, Within, and Saved settings tabs.

- 3 Select the report (**Agent Versions**) you want to generate, set the data filter in the **Report Data Filter** dialog box. Click **OK**.

4 Report for **Agent Versions** is generated.

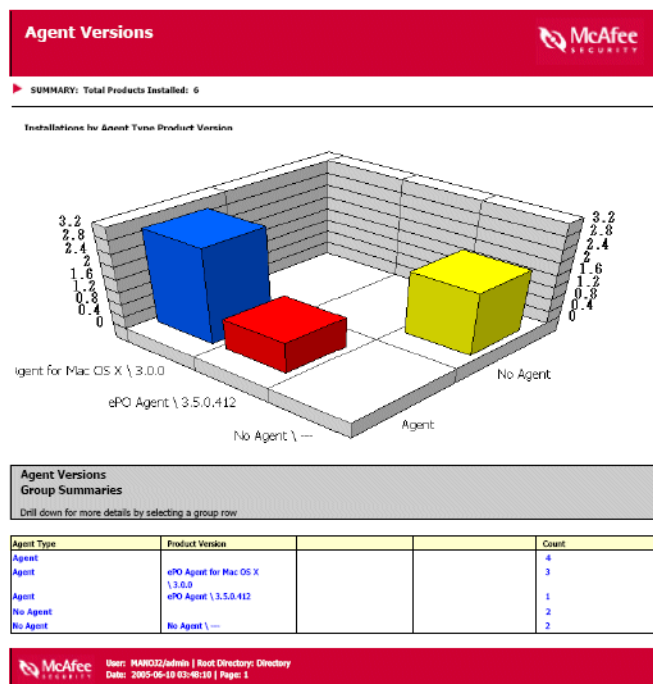


Figure 5-1 Sample Report - Agent Versions

Configuring Reports

There are several ways in which you can control what data appears on reports. You can define the version number of virus definition files, virus scanning engines, and supported products that need to be installed on Macintosh client computers for them to be considered compliant based on your company's anti-virus and security program. You can also limit the results of reports by selected product criteria. (For example, computer name, operating system, virus name, or action taken on infected files.)

Once the results of a report appear, you can then perform a number of tasks on the data. You can view details on desired report data. (For example, to determine which Macintosh client computers do not have a compliant version of Virex can be installed on them). Some reports even provide links to other reports, called sub-reports, that provide data related to the current report. You can also print reports or export report data into a variety of file formats, including HTML and Microsoft Excel.



See *ePolicy Orchestrator Product Guide* for more details on configuring reports.

Glossary

agent AutoUpgrade

The act of automatically upgrading the agent whenever a newer version is available on the ePolicy Orchestrator server.

agent installation package

The Setup program and all other files needed to install the agent.

agent language packages

The set of files that need to be distributed to client computers to view the agent user interface in languages other than English.

Agent Monitor

The agent user interface that appears optionally on managed computers. It allows you to run tasks immediately that are normally initiated by the agent at predefined intervals.

agent wakeup call

The ability to initiate agent-to-server communication from the server-side.

See also *SuperAgent wakeup call*.

agent-to-server communication

Any communication that occurs between ePolicy Orchestrator agent and the ePolicy Orchestrator server where agent and server exchange data. Typically, the agent initiates all communication with the server.

agent-to-server communications interval (ASCI)

The time period between predefined agent-to-server communication.

alert

A message or notification regarding computer activity such as virus detection. It can be sent automatically according to a predefined configuration, to system administrators and users, via e-mail, pager, or phone.

See also *Alert Manager*.

ASCI

See *agent-to-server communication interval*.

binary (Setup) files

The Setup program and all other files needed to install products.

branch

Locations on the master repository that allow you to store and distribute different versions of selected updates.

See also *selective updating*.

check in, checking in

The process of adding files to the master repository.

clean, cleaning

An action taken by the scanner when it detects a *virus*, a *Trojan horse* or a *worm*. The cleaning action can include removing the virus from a file and restoring the file to usability; removing references to the virus from system files, system .INI files, and the registry; ending the process generated by the virus; deleting a macro or a Microsoft Visual Basic script that is infecting a file; deleting a file if it is a Trojan horse or a worm; renaming a file that cannot be cleaned.

console tree

The contents of the **Tree** tab in the left pane of the ePolicy Orchestrator console; it shows the items that are available in the console.

console tree item

The individual icons in the console tree of the ePolicy Orchestrator console.

DAT files

Virus definition files, sometimes referred to as signature files, that allow the anti-virus software to detect and handle viruses and related potentially unwanted code embedded in files.

See also *EXTRA.DAT file*, *incremental DAT files*, and *SuperDAT*.

deploy, deployment

The act of distributing and installing Setup programs to client computers from a central location.

details pane

The right pane of the ePolicy Orchestrator console, which shows details of the currently selected console tree item. Depending on the console tree item selected, the details pane can be divided into upper and lower panes.

See also *upper details pane* and *lower details pane*.

directory

In the console tree, the list of all computers to be managed via ePolicy Orchestrator; the link to the primary interfaces for managing these computers.

distributed software repositories

A collection of web sites or computers located across the network in such a way as to provide bandwidth-efficient access to client computers. Distributed repositories store the files that client computers need to install supported products and updates to these products.

enforce, enforcement

The act of applying predefined settings on client computers at predetermined intervals.

ePolicy Orchestrator agent

A program that performs background tasks on managed computers, mediates all requests between the ePolicy Orchestrator server and the anti-virus and security products on these computers, and reports back to the server to indicate the status of these tasks.

ePolicy Orchestrator console

The user interface of the ePolicy Orchestrator software that is used to remotely control and monitor managed computers.

See also *ePolicy Orchestrator remote console*.

ePolicy Orchestrator database

The database that stores all data received by the ePolicy Orchestrator server from ePolicy Orchestrator agent and all settings made on the server itself.

See also *ePolicy Orchestrator database server*.

ePolicy Orchestrator database server

The computer that hosts the ePolicy Orchestrator database. This can be the same computer on which the ePolicy Orchestrator server is installed or a separate computer.

ePolicy Orchestrator remote console

The ePolicy Orchestrator user interface when it is installed on a separate computer from the ePolicy Orchestrator server.

See also *ePolicy Orchestrator console*.

ePolicy Orchestrator server

The back-end component of the ePolicy Orchestrator software.

See also *ePolicy Orchestrator agent* and *ePolicy Orchestrator console*.

error reporting utility

A utility specifically designed to track and log failures in the McAfee software on your system. The information that is obtained can be used to help analyze problems.

events

Data exchanged during agent-to-server communication that includes information about each managed computer (for example, hardware and software) and its managed products (for example, specific policy settings and the product version number).

group

In the console tree, a logical collection of entities assembled for ease of management. Groups can contain other groups or computers, and can be assigned IP address ranges or IP subnet masks to allow sorting computers by IP address. If you create a group by importing a Windows NT domain, you can automatically send the agent installation package to all imported computers in the domain.

immediate event forwarding

The act of immediately sending events of a specific severity or higher to the ePolicy Orchestrator server once a predefined number of events are available. This communication is done outside of other agent-to-server communication.

inactive agent

Any agent that has not communicated with the ePolicy Orchestrator server within a specified time period.

inherit, inheritance

The act of applying the settings defined for an item within a hierarchy from the item above it.

log file

A record of the activities of a component of McAfee anti-virus software. Log files record the actions taken during an installation or during the scanning or updating tasks.

See also *events*.

Lost&Found group

A group used to temporarily store computers whose appropriate location in the **Directory** cannot be determined.

lower details pane

In the console, the lower-right pane, which displays configuration settings for the products listed on the **Policies** tab in the upper details pane.

See also *details pane* and *upper details pane*.

on-demand scanning

A scheduled examination of selected files to determine if a virus or other potentially unwanted code is present. It can take place immediately, at a future scheduled time, or at regularly scheduled intervals.

Compare to *on-access scanning*.

policy

The configuration settings of managed product that are defined and managed from ePolicy Orchestrator.

policy enforcement interval

The time period during which the agent enforces the settings it has received from the ePolicy Orchestrator server. Because these settings are enforced locally, this interval does not require any bandwidth.

properties

Data exchanged during agent-to-server communication that includes information about each managed computer (for example, hardware and software) and its managed products (for example, specific policy settings and the product version number).

Repository

The location that stores policy pages used to manage products.

scan task

A single scan event.

scan, scanning

An examination of files to determine if a virus or other potentially unwanted code is present.

See *on-access scanning* and *on-demand scanning*.

server events

Activity on the ePolicy Orchestrator server that is recorded by the Windows Event Viewer. This information is not stored in the ePolicy Orchestrator database, so is not available for reporting purposes.

silent installation

An installation method that installs a software package onto a computer silently, without need for user intervention.

site

In the console tree, a logical collection of entities assembled for ease of management. Sites can contain groups or computers, and can be organized by IP address range, IP subnet mask, location, department, and others.

task

An activity (both one-time such as *on-demand scanning*, and routine such as *updating*) that is scheduled to occur at a specific time, or at specified intervals.

Compare to *policy*.

upper details pane

In the console, the upper-right pane, which contains the **Policies**, **Properties**, and **Tasks** tabs.

See also *details pane* and *lower details pane*.

UTC time

Coordinated Universal Time (UTC). This refers to time on the zero or Greenwich meridian.

virus

A program that is capable of replicating with little or no user intervention, and the replicated program(s) also replicate further.

warning priority

The value that you assign each alert message for informational purposes. Alert messages can be assigned a **Critical**, **Major**, **Minor**, **Warning**, or **Informational** priority.

worm

A virus that spreads by creating duplicates of itself on other drives, systems, or networks.

Index

A

- agent
 - directory, 16
 - enforcing policies, 38
 - installing, 16
 - command line, 18
 - silent installation, 18
 - standard installation, 16
 - options, 38
 - system requirement, 13
 - viewing properties, 37
- audience for this manual, 7
- AVERT
 - Anti-Virus & Vulnerability Emergency Response Team, contacting, 11
 - DAT notification service, 11
 - WebImmune, 11

B

- beta program, contacting, 11

C

- consulting services, 11
- contacting McAfee, 11
- customer service, contacting, 11

D

- DAT file
 - specify location, 34
 - updates via AVERT notification service, 11
 - updates, web site, 11
- definition of terms (See Glossary)
- documentation for the product, 8
- download web site, 11

E

- ePolicy Orchestrator
 - server properties, 35
- eUpdate, 24
 - configuring, 34
 - creating, 34
 - disabling, 35
 - FTP, 25
 - HTTP, 25
- events, 39

- deleting events, 40
- viewing server events, 41

G

- getting information, 8
 - list of contacts, 11
 - within the product, 8
- glossary, 47

L

- links to resources in the product, 8
- logging, 42

M

- manuals, 8
- McAfee University, contacting, 11

N

- NAP files
 - adding non windows agent, 14
 - adding report NAP file, 15
 - adding virex NAP file, 15
 - check in, 14
 - where can i find NAP files, 14
- notification service, DAT updates, 11

O

- on-site training, 11

P

- PrimeSupport, 11
- product documentation, 8
- product information, resources, 8
- product training, in-house, 11

R

- reports, 45
 - configuring, 46
- resources for information, 8

S

- scheduling scans and eUpdates, 30
- security headquarters, contacting AVERT, 11
- server components, 14
- service portal, PrimeSupport, 11
- setting policies

- active scanner, 25
- background scanner, 27
- epolicy orchestrator, 21
- general, 23
- mounted volumes scanner, 28
- on demand scanner, 29
- submitting a sample virus, 11

T

- task
 - deleting, 33
 - editing, 31
- technical support
 - accessing from the product, 9
 - contact information, 11
- training web site, 11
- training, on-site, 11

U

- uninstallation
 - ePO agent from ePO server, 20
 - ePO agent from Mac OS X, 20
 - virex NAP from ePO server, 19
- updating anti-virus software, 43
- upgrade web site, 11
- using this guide
 - typeface conventions and symbols, 7

V

- Virus Information Library, 9, 11
- virus, submitting a sample web site, 11

W

- WebImmune, 11