User Guide
Revision 1.0

VirusScan® for Mac

Version 8.6

McAfee®
System Protection

Proven security

McAfee®

COPYRIGHT

TRADEMARK ATTRIBUTIONS

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 MCAFEE 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 Stellent Chicago, Inc. and/or Outside In® HTML Export, © 2001 Stellent 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, © 1996, 1989, 1998-2000. • Software copyrighted by Gunnar Ritter. • Software copyrighted by Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A., © 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 Looijaard, © 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 <rse@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. • Software copyrighted by Carnegie Mellon University © 1989, 1991, 1992. • Software copyrighted by Cambridge Broadband Ltd., © 2001-2003. • Software copyrighted by Sparta, Inc., © 2003-2004. • Software copyrighted by Cisco, Inc. and Information Network Center of Beijing University of Posts and Telecommunications, © 2004. • Software copyrighted by Simon Josefsson, © 2003. • Software copyrighted by Thomas Jacob, © 2003-2004. • Software copyrighted by Advanced Software Engineering Limited, © 2004. • Software copyrighted by Todd C. Miller, © 1998. • Software copyrighted by The Regents of the University of California, © 1990, 1993, with code derived from software contributed to Berkeley by Chris Torek.

Issued November 2007 / VirusScan® for Mac software version 8.6

DBN-001-EN

Contents

1 Introducing VirusScan for Mac

What's in this guide?

This guide introduces VirusScan for Mac 8.6 and provides the following information on how to keep your computer free of viruses:

- Overview of the product.
- Descriptions of product features.
- Descriptions of all new features in this release of the software.
- Detailed instructions for installing the software.
- Detailed instructions for configuring and deploying the software.
- Procedures for performing tasks.
- Troubleshooting information.
- Integration with ePolicy Orchestrator 3.6 (Patch 2), 3.6.1, and 4.0.

What is VirusScan?

VirusScan for Mac is an anti-virus application that helps you keep your Macintosh computer free of viruses, Trojan horses and other malware. VirusScan features On-Demand scanning, Apple Mail scanning, eUpdate scheduling, online Help, On-Access scanning and drag-and-drop scanning. In addition, you are only one click away from the comprehensive online Virus Information Library which will keep you informed of all new threats.

VirusScan protects your system from viruses that may reside on other computers such as Macintosh computers, Windows computers, UNIX computers, and externally mounted volumes such as USB device, Firewire devices and CDs/DVDs.

This version of VirusScan also provides anti-virus support for Mac OS X 10.5 (Leopard) operating system.

What you can do with VirusScan

VirusScan detects and cleans program viruses, macro viruses, and Trojan horses for all types of Macintosh, Windows, and UNIX files, including compressed files and OLE compound documents.

With VirusScan, you can scan a single file, a file directory, your whole drive, or mounted volumes such as CDs, .DMG files, network mounted files, Apple Mail messages, and USB devices such as pen drives, iPods and cameras. Advanced heuristic scanning detects previously unknown macro and program viruses.

What's new in this release

- Support for Mac OS X Leopard (10.5)
- On-Access scanning performance optimization
- On-Demand scanning performance optimization
- Support for ePolicy Orchestrator 4.0
- Incremental DAT updates
- 5200 scanning engine support

VirusScan features

VirusScan incorporates its previous powerful features with new safeguards and tools for you to protect your computer system. The online Help system provides you with troubleshooting assistance and procedures for tasks.

VirusScan console

The VirusScan console enables you to configure VirusScan through an easy-to-use interface.

Using the console, you can configure the On-Demand scanner as well as perform On-Demand scans through the drop-zone (an area on the VirusScan console that allows you to drag and drop files that you want to scan). You can also click **Drop items or click here** to open the **Select a file or folders to Scan & Clean** dialog box to select the file(s) or folder(s) for the On-Demand scan and clean.

Also, you can configure and enable the On-Access scanner from the VirusScan console and enable automatic updating of your virus definitions using eUpdate.

To access the VirusScan console, double-click the **VirusScan** icon in your computer's **Applications** folder.

On-Demand scanner

The On-Demand scanner allows you to initiate a scan at any time by dragging and dropping selected file(s) into the console. You can also click **Drop items or click here** to open the **Select a file or folders to Scan & Clean** dialog box to select the file(s) or folder(s) to perform scan and clean.

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. The scanner notifies you when it finds a virus and generates a log of its actions.

To access the On-Demand scanner, drag the file(s) you want to scan and drop them into the **VirusScan** icon or into the drop-zone in the console.

On-Access scanner

The On-Access scanner provides continuous monitoring of all files in use to determine if a virus or other potentially unwanted code is present. A scan takes place automatically every time a file is read from the disk, and/or written to the disk, either by the user or by system processes.

With the On-Access scanner, continuous policy enforcement is provided for multiple files, directories or volumes, including volumes on remote computers connected through the network. You can configure what the scanner looks for and how it responds to infected files. The scanner notifies you, in the **Reporter** pop-up window, if it finds a virus or other malware.

You enable the On-Access scanner from the VirusScan console.

VirusScan Schedule Editor

The VirusScan Schedule Editor enables you to schedule automated scans and updates for the anti-virus definitions (DAT) files that are available online. You can schedule scans and updates through the **VirusScan Schedule Editor** console. Automated scans and updates can be set on a daily, weekly, or monthly basis. To access the VirusScan Schedule Editor, do any one of these tasks:

- Click **Scheduler** on the VirusScan console.
- Select **Scheduled Tasks** under **View** in the main menu.
- Open VirusScan Schedule Editor directly from the `/Applications/Utilities` folder.

eUpdate

eUpdate allows you to update DAT files and the anti-virus engine. eUpdate continuously updates your anti-virus software with new information on viruses and scanning capabilities. eUpdate automatically checks for new updates when there is an Internet connection, and updates the virus definitions when new ones are available. You can also use VirusScan Schedule Editor to configure eUpdate to check for updates according to your own schedule.

To initiate an eUpdate manually, click the **eUpdate** tab on the VirusScan console, then the **Start** button. Support for eUpdate is provided using the FTP protocol.

ePolicy Orchestrator Manageability

VirusScan integrates with McAfee ePolicy Orchestrator versions 3.6 (patch 2), 3.6.1, and 4.0 allowing you to use this software in a managed environment. The ePolicy Orchestrator software provides a central hub of McAfee System Protection Solutions. Administrators can mitigate the risk of rogue, non-compliant systems, keep protection up-to-date, configure and enforce protection policies, and monitor security status from one centralized, enterprise-scalable console. Using ePolicy Orchestrator, you can configure VirusScan for Mac on the target systems across your network; you do not need to configure these computers individually from the **Preferences** window.

> The use of ePolicy Orchestrator is optional and you can use all the functionalities of VirusScan as a standalone product.
>
> You will be able to use ePolicy Orchestrator related functionality only if you have ePolicy Orchestrator and Non-Windows Agent installed and configured to manage VirusScan in an enterprise environment.

Audience

This information is intended for network administrators who are responsible for their company's anti-virus and security program.

Conventions

This guide uses the following conventions:

Bold Condensed All words from the interface, including options, menus, buttons, and dialog box names.

Example:
Type the **User** name and **Password** of the appropriate account.

`Courier` The path of a folder or program; text that represents something the user types exactly (for example, a command at the system prompt).

Examples:
The default location for the program is:

```
/Applications/Utilities
```

Run this command on the client computer:

```
scan --help
```

Italic For emphasis or when introducing a new term; for names of product documentation and topics (headings) within the material.

Example:
Refer to the *VirusScan Enterprise Product Guide* for more information.

Blue A web address (URL) and/or a live link.

Example:
Visit the McAfee website at:

`http://www.mcafee.com`

<TERM> Angle brackets enclose a generic term.

Example:
In the console tree, right-click <SERVER>.

Note: Supplemental information; for example, another 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 using a hardware product.

Getting product information

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

Standard documentation

User Guide — This guide introduces the product, describes its features, and gives details on how to install and configure the software, ongoing operation and maintenance. It also introduces ePolicy Orchestrator manageability features for VirusScan, and provides detailed instructions for installing, configuring and managing the software in an enterprise environment.This guide (*VirusScan User Guide*) is available in .PDF in the Documentation folder of the product package.

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

VirusScan for Mac Release Notes — This file describes the product features, last-minute additions or changes to the documentation, lists any known behavior or other issues with the product release, and describes the installation process. This file is available in the Documentation folder of the product package.

License — The McAfee License Agreement (.PDF) booklet that includes all of the license types you can purchase for your product. The License Agreement gives general terms and conditions for the use of the licensed product. Read it carefully. If you install the product, you agree to the license terms. This McAfee Software License agreement is available in the Documentation folder of the product package.

Links from within the product

The Help menu in the product provides links to some useful resources:

- VirusScan Help
- Submit a Sample
- Technical Support
- Virus Information Library

VirusScan Help

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

Submit a sample

Use this link to submit potentially infected files to McAfee for analysis. You will receive information about your files, including solutions and real-time fixes, if required.

Technical Support

Use this link to access the McAfee Technical Support website for product documentation, FAQs, or troubleshooting hints and tips.

Virus Information Library

Use the Virus Information Library link to access the McAfee® Avert® Labs Virus Information Library. This website 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 warnings that you receive via email. 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, we recommend you view our hoax page before you pass the message on to your friends or colleagues.

To access the Virus Information Library:

1. Open VirusScan.
2. From the **Help** menu, select **Virus Information Library**.

Contact information

Threat Center: McAfee Avert® Labs http://www.mcafee.com/us/threat_center/default.asp

Avert Labs Threat Library
http://vil.nai.com

Avert Labs WebImmune & Submit a Sample *(Logon credentials required)*
https://www.webimmune.net/default.asp

Avert Labs DAT Notification Service
http://vil.nai.com/vil/signup_DAT_notification.aspx

Download Site http://www.mcafee.com/us/downloads/

Product Upgrades *(Valid grant number required)*

Security Updates (DATs, engine)

HotFix and Patch Releases

- **For Security Vulnerabilities** *(Available to the public)*
- **For Products** *(ServicePortal account and valid grant number required)*

Product Evaluation

McAfee Beta Program

Technical Support http://www.mcafee.com/us/support/

KnowledgeBase Search
http://knowledge.mcafee.com/

McAfee Technical Support ServicePortal *(Logon credentials required)*
https://mysupport.mcafee.com/eservice_enu/start.swe

Customer Service

Web
http://www.mcafee.com/us/support/index.html
http://www.mcafee.com/us/about/contact/index.html

Phone — 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

Professional Services

Enterprise: http://www.mcafee.com/us/enterprise/services/index.html

Small and Medium Business: http://www.mcafee.com/us/smb/services/index.html

2 Installing VirusScan for Mac

This section gives information on installing the VirusScan software and includes details on:

- *System requirements*
- *Installing VirusScan*
- *Upgrade installation*
- *Testing your installation*
- *Uninstalling VirusScan*

System requirements

To install VirusScan for Mac software, you require PowerPC or Intel based Mac computer, Mac OS X Tiger (10.4.6 or later) or Mac OS X Leopard (10.5) operating system, 512 MB (or higher) RAM, minimum 45 MB of free disk space.

ePolicy Orchestrator requirements

VirusScan integrates with ePolicy Orchestrator versions 3.6 (patch 2), 3.6.1, and 4.0. However, please note that the use of ePolicy Orchestrator is optional and VirusScan for Mac can be used as a standalone product.

> You will be able to use ePolicy Orchestrator related functionality only if you have ePolicy Orchestrator and Non-Windows Agent installed and configured to manage VirusScan in an enterprise environment.

Installing VirusScan

VirusScan for Mac can be installed through either a standard (graphical interface) installation or a command-line (silent) installation. Once you have installed the product, its ReadMe file is available in the **Documentation** folder of the product package. Refer to this file for known issues, online resources, and other useful information.

With VirusScan you use the eUpdate feature to connect to a Web location and download new DAT files. To find out more about eUpdate and other VirusScan features, see *Getting Started* on page 17.

> You must have administrative privileges to install this product.

Standard installation

You can install VirusScan using the VirusScan install file, either on the product CD or in the installation .ZIP file downloaded from the McAfee website and saved to a temporary folder.

To install VirusScan:

1 Double-click the **VirusScan.pkg** file to start the Installer.

2 Follow the on-screen steps to install the software.

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

4 Click **Install** to perform the installation. The **Authentication** dialog box appears.

5 Type your user name and administrator password and click **OK**. A message notifies you when the installation finishes. Click **Close**.

The VirusScan for Mac installer installs the VirusScan application inside the `Applications` folder and the VirusScan Schedule Editor application inside the `Application/Utilities` folder of your computer.

> You need not restart your computer after installing VirusScan for Mac 8.6 (unlike the earlier versions).

Command-line (silent) installation

1 Locate the **VirusScan.pkg** file, either on the product CD or in the installation .ZIP downloaded from the McAfee web site, and save it to a temporary location.

2 Open the **Terminal** window and change the working folder to the one where the **VirusScan.pkg** file is located.

3 In the **Terminal** window, execute:

```
sudo installer -pkg VirusScan.pkg -target /
```

4 Enter your system password when prompted to do so.

5 A message notifies you when the installation finishes. Close the **Terminal** window.

Upgrade installation

You can upgrade to VirusScan for Mac v8.6 from earlier VirusScan versions (8.0 and 8.5). After the upgrade, the preferences are migrated from the earlier versions to the current version (v8.6).

Testing your installation

You can test VirusScan by using the European Institute of Computer Anti-Virus Research (EICAR) standard anti-virus test file. This file is a combined effort by anti-virus vendors throughout the world to implement one standard by which customers can verify their anti-virus software.

To test your installation:

1. Go to the EICAR.ORG website `http://www.eicar.org` and download the AntiVirus test file, Eicar.zip.
2. Run the On-Demand Scanner on the downloaded ZIP file. VirusScan will report finding the EICAR test file.

> This file is *not* a virus and is available for testing anti-virus software. You can delete this file when you have finished testing the software to avoid alarming unsuspecting users.

If the test is successful, you are now ready to start using the VirusScan software.

Uninstalling VirusScan

You can uninstall VirusScan by using an uninstall file (**VirusScan Uninstall.command**), either on the product CD, or in the installation .ZIP file downloaded from the McAfee website and saved to a temporary folder. You can also execute uninstall command from terminal.

To uninstall VirusScan:

1. Do one of the following:
   - Double-click the **VirusScan Uninstall.command** icon.
   - Drag the **VirusScan Uninstall.command** icon, drop it in the **Terminal** window and press **Enter**.
   - In the **Terminal** window, change the directory to `/usr/local/vscanx`, then execute **VirusScan Uninstall.command**.

   > To open the **Terminal** application, double-click the application located under `/Applications/Utilities`.

   The **Terminal** window prompts you for your administrator password.
2. Type your administrator password and click **Enter**.

> Your administrator password will not be displayed in the **Terminal** window.

When the uninstallation process finishes successfully, a message appears in the **Terminal** window to show the VirusScan software has been removed from your computer.

3 Getting Started

This chapter describes VirusScan, and how it helps keep your computer free of viruses. It includes the following topics:

Using the VirusScan console

The VirusScan console allows you to use and configure On-Demand scanning and On-Access scanning. The console connects you to the McAfee Virus Information Library, does eUpdates, and prints and saves virus scan reports.

The VirusScan console also contains a drag-and-drop pane for On-Demand scanning. You can initiate an On-Demand scan at any time by dragging files into the center pane of the console, dropping them into the drag-and-drop pane, then clicking the **Start** button. If you add another file after the scan has completed, the new file will replace the first scan.

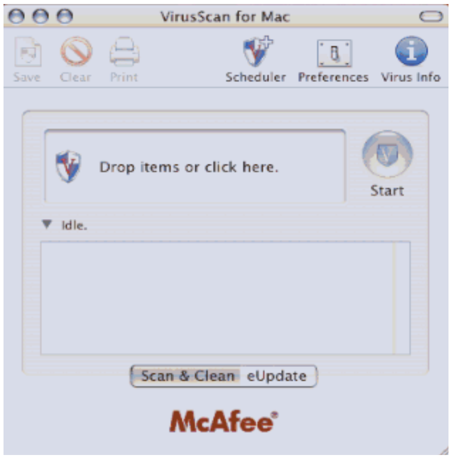
The VirusScan console

The VirusScan console displays standard Macintosh and specialized anti-virus components, including:

- Title bar displaying the name of the program that is currently running.

- Close, minimize, maximize, and hide tool bar buttons to resize or hide the interface.

Figure 3-1 VirusScan console



Toolbar

The toolbar displays these buttons:

Saves the virus scan report as a Rich Text File (.RTF).

Clears the current report showing on the status panel.

Prints the current report.

Allows you to schedule a scan task and an eUpdate task.

Opens the **Preferences** dialog box, allowing you to:

- Set preferences for the On-Demand scanner.
- Set preferences for the On-Access scanner.
- Set preferences for the action to take if a virus is found.
- Log results to a file.
- Configure eUpdate server settings.
- Configure the exclusion list.
- Automatically check for virus definitions updates.

Opens your default browser and directs you to the McAfee Virus Information Library.

Menu bar

The menu bar shows standard drop-down menus common to all screens: **File**, **Edit**, **View**, **Window**, and **Help**.

Configuring the scanners

You can configure the settings for both the On-Demand scanner and the On-Access scanner using the **Preferences** dialog box. Two versions of this dialog box are available; one for configuring the On-Demand scanner, the other for the On-Access scanner. Both scanners have the same general preferences, while advanced scanning options are scanner-specific.

Scanner preferences are global settings that apply to all users.

The preferences are saved automatically when you select them.

You need administrative privileges to modify preferences.

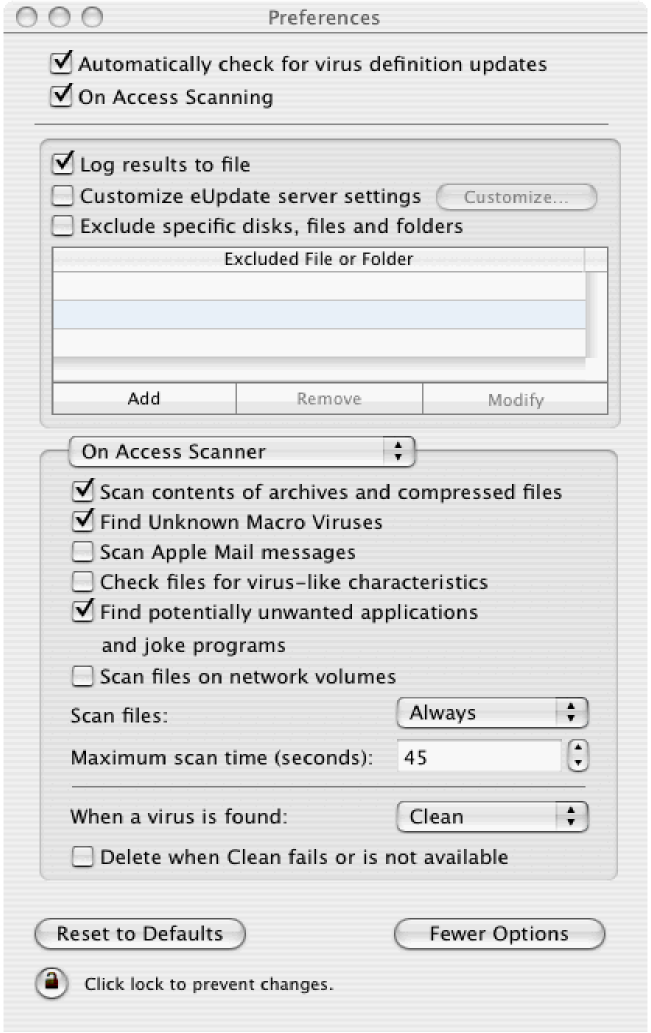
Configuring general preferences

General preferences apply to both the On-Demand scanner and the On-Access scanner. They are the same for both.

To configure general preferences:

1 Click **Preferences** on the tool bar to display the **Preferences** dialog box. The top panel in this dialog box contains general preferences options that apply to both the On-Demand scanner and the On-Access scanner.

Figure 3-2 General preferences



☑ Automatically check for virus definition updates

☑ On Access Scanning

☑ Log results to file

□ Customize eUpdate server settings

□ Exclude specific disks, files and folders

Excluded File or Folder

On Access Scanner

☑ Scan contents of archives and compressed files

☑ Find Unknown Macro Viruses

□ Scan Apple Mail messages

□ Check files for virus-like characteristics

☑ Find potentially unwanted applications and joke programs

□ Scan files on network volumes

Scan files: Always

Maximum scan time (seconds): 45

When a virus is found: Clean

□ Delete when Clean fails or is not available

2 Select your general scanning preferences for the On-Demand and On-Access scanners; Table 3-1 shows the available general preferences.

Table 3-1 General preferences for On-Demand and On-Access scanners

Automatically check for virus definition updates	Enables/disables automatic eUpdates.
On-Access Scanning	Enables/disables On-Access scanning.
Log results to file	Enables/disables logging results to a file.

Table 3-1 General preferences for On-Demand and On-Access scanners

Customize eUpdate Server Settings	Manages your update server with user name and password. Click **Customize** to modify the FTP settings for eUpdate.
Exclude specific disks, files and folders	Configures your scanning exclusions. If this is not selected, you will not have any exclusions set. **To add an exclusion:** ■ Click **Add** in the **Exclude File or Folder** list. Select the file or folder from the **Open** dialog box. **To remove an exclusion:** ■ Select the file or folder from the **Exclude File or Folder** list. Click **Remove**. **To modify an exclusion:** ■ Select the file or folder from the **Excluded File or Folder** list. Click **Modify**. The **Open** dialog box appears. Select the file or folder to replace the existing exclusion.

3. Set the advanced preferences you require. These are shown in the lower pane in the **Preferences** dialog box. Two different sets of preferences are available; one for the On-Demand scanner, the other for the On-Access scanner. See *Configuring the On-Demand scanner on page 21* and *Configuring the On-Access scanner on page 23* for details.

4. Click **Lock** to prevent changes to the preferences.

5. Click **Close** in the upper left-hand corner to exit the **Preferences** dialog box.

Configuring the On-Demand scanner

The On-Demand scanner allows you to initiate a scan at any time. You configure the On-Demand scanner advanced preferences using options available in the lower pane of the Preferences dialog.

To configure the On-Demand scanner:

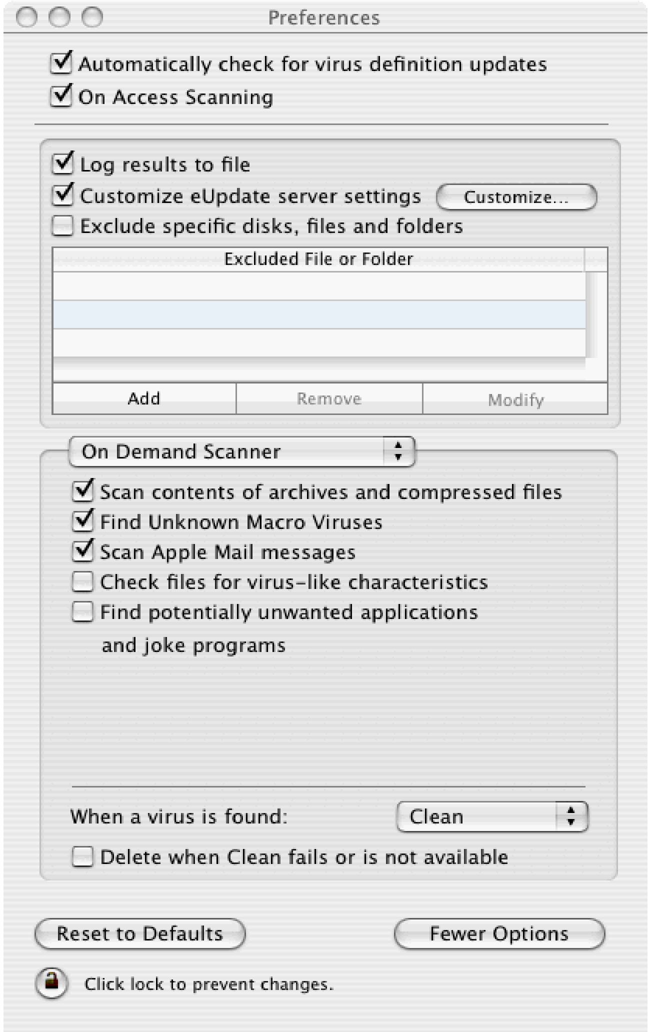
1. Click **Preferences** on the tool bar to display the **Preferences** dialog box.

2. Click **More Options** in the lower right-hand corner of the dialog box to reveal Advanced Preferences.

3. Select **On-Demand Scanner** from the drop-down menu (if not already selected) to display the On-Demand scanning version of this dialog box.

.

Figure 3-3 On-Demand preferences



☑ Automatically check for virus definition updates
☑ On Access Scanning

☑ Log results to file
☑ Customize eUpdate server settings
☐ Exclude specific disks, files and folders

On Demand Scanner

☑ Scan contents of archives and compressed files
☑ Find Unknown Macro Viruses
☑ Scan Apple Mail messages
☐ Check files for virus-like characteristics
☐ Find potentially unwanted applications and joke programs

When a virus is found: Clean

☐ Delete when Clean fails or is not available

Click lock to prevent changes.

4 Select your advanced scanning preferences for the On-Demand scanner, Table 3-2 shows the available preferences.

Table 3-2 Advanced Preferences for On-Demand scanner

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.
Find Unknown Macro Viruses	If a file contains potentially infected macro (unknown infection), it will be scanned and cleaned/deleted, as part of the clean.
Scan Apple Mail messages	Enables/disables the On-Demand scanner to check Apple Mail messages for infection.
Check files for virus-like characteristics	Enables/disables the On-Demand scanner to check for files that show characteristics of viruses or worms and may contain unknown infections.
Find potentially unwanted applications and joke programs	Enables/disables the On-Demand scanner to check for unwanted programs or joke programs.

Table 3-2 Advanced Preferences for On-Demand scanner

When a virus is found: ■ Clean ■ Delete ■ Notify	Selects the primary action for the On-Demand scanner.
Delete when Clean fails or is not available	Selects the secondary action for the On-Demand scanner. This is available only when the primary action is **Clean**.

5 Click **Lock** to prevent changes to the preferences.

6 Click **Close** in the upper left-hand corner to exit the **Preferences** dialog box.

Configuring the On-Access scanner

The On-Access scanner continually monitors all files that are in use to determine if a virus or other malware is present. An On-Access scan takes place whenever a file is read from the disk, written to the disk, or both, depending on the preferences you set for this scanner.

You configure the On-Access scanner advanced scanner preferences using options available in the lower pane of the Preferences dialog.

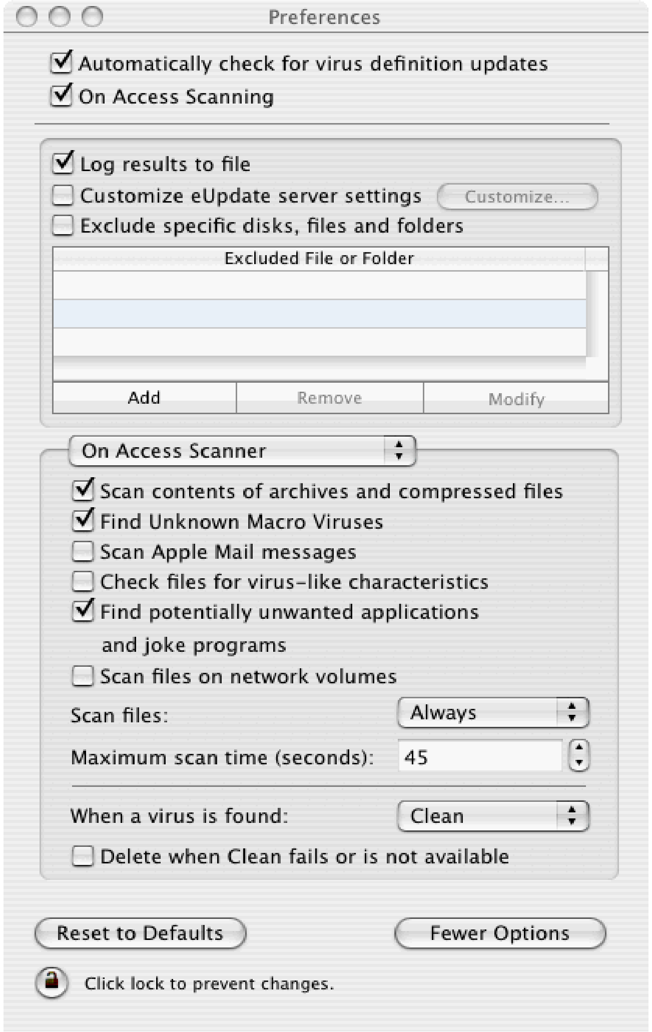
To configure the On-Access scanner:

1 Click **Preferences** on the tool bar to display the **Preferences** dialog box.

2 Click **More Options** in the lower right-hand corner of the dialog box to reveal Advanced Preferences.

3 Select **On-Access Scanner** from the drop-down menu (if not already selected) to display the On-Access scanning version of this dialog box.

.



Preferences

☑ Automatically check for virus definition updates
☑ On Access Scanning

☑ Log results to file
□ Customize eUpdate server settings
□ Exclude specific disks, files and folders

On Access Scanner

☑ Scan contents of archives and compressed files
☑ Find Unknown Macro Viruses
□ Scan Apple Mail messages
□ Check files for virus-like characteristics
☑ Find potentially unwanted applications and joke programs
□ Scan files on network volumes

Scan files: Always

Maximum scan time (seconds): 45

When a virus is found: Clean

□ Delete when Clean fails or is not available

Click lock to prevent changes.

Figure 3-4 On-Access preferences

4 Select your scanning preferences for the On-Access scanner; Table 3-3 shows the available preferences.

Table 3-3 Advanced Preferences for On-Access scanning

Scan contents of archives and compressed files	Sets the selected scanner to scan into archives and other compressed files. On by default for the On-Access scanner. Note that the On-Access scanner will not scan inside stuffit archives.
Find Unknown Macro Viruses	If a file contains potentially infected macro (unknown infection), it will be scanned and cleaned/deleted, as part of the clean.
Scan Apple Mail messages	Enables/disables the On-Access scanner to check Apple Mail messages for infection.
Check files for virus-like characteristics	Enables/disables the On-Access scanner to check for files that show characteristics of viruses or worms and may contain unknown infections.
Find potentially unwanted applications and joke programs	Enables/disables the On-Access scanner to check for unwanted programs or joke programs.

Table 3-3 Advanced Preferences for On-Access scanning

Scan files on network volumes	Sets the scanner to scan files accessed from network volumes.
Scan files: ■ Always ■ Read ■ Write	Determines if the On-Access scanner is to scan files that are read from the disk, written to the disk, or both.
Maximum scan time	The maximum length of time, in seconds, that a scan can last per file. (A compressed file is not treated as one file; this timeout applies to the last individual file, and not to the last top level container file).
When a virus is found: ■ Clean ■ Delete ■ Notify	Selects the primary action for the On-Access scanner.
Delete when Clean fails or is not available	Selects the secondary action for the selected scanner. This is available only when the primary action is **Clean**.

5 Click **Lock** to prevent changes to the preferences.

6 Click **Close** in the upper left-hand corner to exit the **Preferences** dialog box.

Using the On-Demand scanner

The On-Demand scanner allows you to initiate a scan at any time in the following ways:

- By dragging and dropping file(s) into the **VirusScan** dock icon, the **VirusScan** icon in the Finder, or into the drag-and-drop pane in the console.
- Through the **Select a file or folders to Scan & Clean** dialog box.

You can select multiple files or directories and the results are summarized in the reporting window.

To perform On-Demand scanning:

1 Open the VirusScan console.

2 Drag and drop the file, folder, or volume you want to scan into the drag-and-drop pane of the main console. To select a group of files, do one of the following:

- Hold down the **Shift** key while selecting the files you want.
- Click the drag-and-drop pane. A file selection screen appears. Select the file, group of files, directory, or volume you want to scan, then click **Select Location**.
- Drag the file, folder, or volume to the **VirusScan** dock icon in the **Finder** view.

3 Click **Start** on the console to initiate scanning.

The **Status Line** shows the name of the file being scanned and the status of the scan. The **arrow** beside the status line hides or reveals the **Reporting** window. The **Reporting** window is hidden by default.

A scan report appears in the **Reporting** window. The report notes the time of the scan, the total files scanned, and the actions taken. The console shows the status of the scan in a line between the drag-and-drop pane and the report panel. The status panel shows **Idle** when it is not scanning.

Using the On-Access scanner

The On-Access scanner provides continuous, automatic policy enforcement for multiple files, directories and volumes, including volumes on remote computers connected through the network. Simply enable the On-Access scanner for it to run.

To enable On-Access scanning:

1 Open the VirusScan console.

2 Click **Preferences** on the tool bar to display the **Preferences** dialog box.

3 Select the **On-Access Scanning** checkbox to enable On-Access scanning.

The scanner notifies you in the **Reporter** pop-up window if it finds a virus or other malware.

Updating DAT files

Daily, by default, eUpdate automatically connects to the eUpdate server via your Internet connection, and checks for new DAT files. Updates can traverse proxy servers. You can schedule additional eUpdates through the **VirusScan Schedule Editor**.

Automatic and scheduled eUpdate and On-Demand scans can be run simultaneously.

Why do you need to update?

To ensure that you are protected against the latest threats, you should keep your anti-virus software up-to-date by updating the DAT files and engine regularly:

- New viruses and worms emerge frequently. McAfee regularly releases updated DAT files to ensure VirusScan can detect such viruses and worms.
- Virus-scanning engine upgrades are occasionally available. These enable VirusScan to employ the latest virus-detection techniques.

How does eUpdate work?

eUpdate enables you to obtain and apply new DAT files or upgrades to your anti-virus software while connected to the Internet. If an update exists, VirusScan will automatically attempt to download and install the update. If a day lapses without updating, VirusScan will automatically download the update. This ensures your system is up-to-date at all times.

Configuring eUpdate settings

DAT files can be updated from an FTP server. McAfee provides an FTP server to eUpdate your DAT files.

McAfee FTP server

By default, VirusScan is configured to access the McAfee FTP server to download the latest DAT files. After you install VirusScan, it automatically connects to the FTP server to download and update your DAT files while you are connected to the Internet.

Configuring the internal FTP server

To use an internal FTP eUpdate repository for your Macintosh computers on your network, you need to configure an internal FTP eUpdate server. In this case, you have to download the DAT files everyday from the McAfee FTP server (`ftp://ftp.mcafee.com/commonupdater`) onto the internal FTP server you have configured.

To configure the internal FTP server:

1 Download the DAT file from `ftp://ftp.mcafee.com/commonupdater`.

2 Copy the DAT file to a folder on the FTP eUpdate server.

To access the FTP server from Preferences:

1 Open the ViruScan console to modify the settings in the **eUpdate Server Settings** dialog box.

2 Click **Preferences** on the tool bar. The **Preferences** dialog box appears. Select the **Customize eUpdate Server Settings** option.

3 Click the **Customize** button. The **eUpdate Server Settings** dialog box appears.

4 Type the URL of the internal FTP server in the **Server URL**.

5 Type the location to where you have downloaded the DAT file in **Directory**.

6 Click **OK**.

Example:

1 Create a directory named "commonupdater" under your ftp server's top level directory.

2 Open `ftp://ftp.mcafee.com/commonupdater`.

3 Download the following files from `ftp://ftp.mcafee.com/commonupdater/` to `<your ftpserver>/commonupdater/` location:

- oem.ini
- all .gem files
- gdeltaavv.ini

4 Download `ftp://ftp.mcafee.com/commonupdater/current/VSCANDAT1000/DAT/0000/avvdat-xxxx.zip` to `<your ftpserver>/commonupdater/current/VSCANDAT1000/DAT/0000/`.

5 Virus Definitions are updated daily. Hence, you need to repeat Step 1 to 4 daily if you want to keep your local update repository up-to-date.

How do you eUpdate through proxy server?

WebProxy (HTTP) proxy settings are supported. Refer to Apple's documentation for details on how to configure these proxy settings on the Max OS X.

You must also ensure that anonymous access is enabled on the FTP server in order for eUpdate to work.

VirusScan does not support proxy server authentication.

Using the VirusScan Schedule Editor

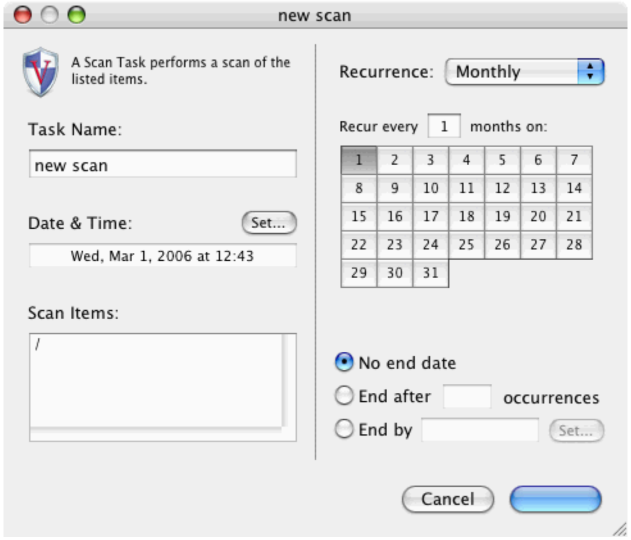
The VirusScan Schedule Editor allows you to create repetitive scans on a group of files or folders. You can schedule daily, weekly, and monthly scans.

To schedule a scan:

1 Click **Scheduler** on the VirusScan console. Alternatively, you can select **Scheduled Tasks** from the **View** menu. The **VirusScan Schedule Editor** dialog box appears.

2 Click **New Scan Task** . An **Untitled** dialog box appears.

Figure 3-5 New Scan dialog box



new scan

A Scan Task performs a scan of the listed items.

Task Name: new scan

Date & Time: Wed, Mar 1, 2006 at 12:43

Scan Items: /

Recurrence: Monthly

Recur every 1 months on:

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

● No end date

○ End after occurrences

○ End by

3 Name the task. Use a name that describes the scan you are scheduling.

4 Click **Set** to specify the **Date & Time** of the scheduled scan.

5 Choose the items you want scanned. You can do this by:

- Dragging and dropping items into the **Scan Items** pane.
- Clicking on the **Scan Items** pane. A **Choose Item** dialog box appears. Click **Choose** when you have selected the file(s) to scan.

6 Select **Recurrence**. Choose from:

- **Daily**: Type the sequence of days that the scan will run.
- **Weekly**: Select the day(s) of the week on which you want the scan to occur.
- **Monthly**: Select the day(s) of the month on which the scan will occur, and the sequence of months.
- **Never**: Select this option if you do not want the scan to reoccur.

7 Specify when the schedule should end, and click **OK**.

Your new scan task appears in a list of all scheduled scans and eUpdates in the VirusScan Schedule Editor. To enable or disable scheduled tasks, select the checkbox next to the task item.

> If the computer is switched off when a task is scheduled to run, VirusScan will skip the task when the computer is turned back on.

Scheduling eUpdates

The VirusScan Schedule Editor allows you to schedule repetitive updates to your computers DAT files and the virus-scanning engine. This support is provided through FTP.

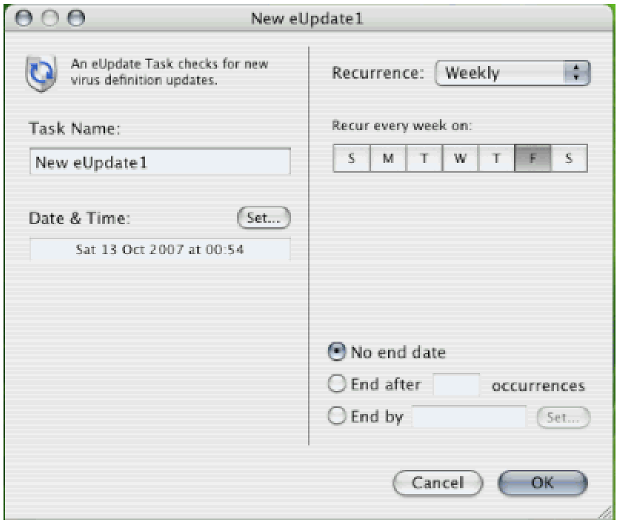
eUpdate is programmed to check for new updates on its own. However, you can schedule additional eUpdates or modify the existing schedule.

To schedule an eUpdate:

1 From the **View** menu, select **Scheduled Tasks**. The **VirusScan Schedule Editor** dialog box appears.

2 Click **New eUpdate Task**. An **Untitled** window appears.

Figure 3-6 New eUpdate dialog box



New eUpdate1

An eUpdate Task checks for new virus definition updates.

Task Name: New eUpdate1

Date & Time: Sat 13 Oct 2007 at 00:54

Recurrence: Weekly

Recur every week on: S M T W T [✓ F] S

● No end date
○ End after occurrences
○ End by

3 Type a name for the task. We recommend using a name that describes the task you are scheduling.

4 Click **Set** to specify a **Date & Time** for the update to occur.

5 Select **Recurrence**. Choose from:

- **Daily**: Type the sequence of days you want the eUpdate to connect.
- **Weekly**: Select the day(s) of the week on which you want the eUpdate to occur.
- **Monthly**: Select the day(s) of the month you want the automatic update, and the sequence of months.
- **Never**: Select this option if you do not want the automatic update to reoccur.

6 Select an end date and click **OK**.

Your new eUpdate task appears in a list of all scheduled scans and eUpdates in the VirusScan Schedule Editor. To enable or disable eUpdate tasks, select the check box next to the appropriate task item. eUpdate will automatically start when an update is available.

To initiate an unscheduled eUpdate:

1 Open the VirusScan console.

2 Click the **eUpdate** tab to switch to the eUpdate pane.

3 Click **Start** to check if new virus definitions are available for download.

4 Integrating with ePolicy Orchestrator 3.6

Introduction

This section describes how to configure VirusScan for Mac using McAfee ePolicy Orchestrator® management software versions 3.6 and 3.6.1. To use this guide effectively, you need to be familiar with ePolicy Orchestrator. For more information, see the *ePolicy Orchestrator Product Guides*. The ePolicy Orchestrator software provides a single point of control for your McAfee anti-virus products, 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 VirusScan for Mac on the target computers across your network; you do not need to configure them individually.

This section includes the following information:

- Adding ePolicy Orchestrator agent configuration to ePolicy Orchestrator server.
- Setting anti-virus policies on the target systems to configure the following VirusScan for Mac features:
  - General policies controlling overall functions for VirusScan for Mac.
  - eUpdate server policies.
  - On-Demand scanner policies.
  - On-Access scanner policies.
- Configuring ePolicy Orchestrator agent features for Macintosh computers:
  - Agent communication interval.
  - Policy enforcement interval.
  - Event forwarding.
  - Logging.

> This guide does not provide detailed information about installing or using ePolicy Orchestrator software. See *ePolicy Orchestrator Product Guides*.

Prerequisites for using ePolicy Orchestrator to manage VirusScan for Mac

Before you can use the ePolicy Orchestrator software to manage VirusScan for Mac:

- Check in the appropriate Network Associate Package (.NAP) files for VirusScan for Mac in the ePolicy Orchestrator software repository.
- Check in the Non-Windows Agent (NWA) file to the ePolicy Orchestrator repository.

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

- Install the ePolicy Orchestrator agent on your Macintosh computer.

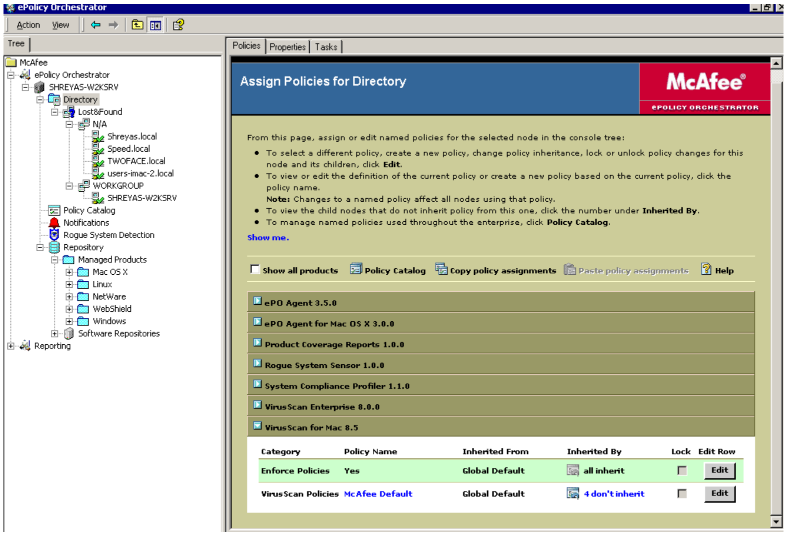
Introducing ePolicy Orchestrator console

The Microsoft Management Console (MMC) is your interface to the ePolicy Orchestrator product and its features. Here you register and configure the VirusScan for Mac anti-virus product that is managed through ePolicy Orchestrator. The console uses standard MMC features.

The console is divided into two sides or panes:

- The console tree is the navigation pane of the console. It shows the servers, workstation, and appliances that you can administer using ePolicy Orchestrator.
- The details pane is to 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.

Figure 4-1 ePolicy Orchestrator console



Assign Policies for Directory

From this page, assign or edit named policies for the selected node in the console tree:

- To select a different policy, create a new policy, change policy inheritance, lock or unlock policy changes for this node and its children, click **Edit**.
- To view or edit the definition of the current policy or create a new policy based on the current policy, click the policy name.
  Note: Changes to a named policy affect all nodes using that policy.
- To view the child nodes that do not inherit policy from this one, click the number under **Inherited By**.
- To manage named policies used throughout the enterprise, click **Policy Catalog**.

ePO Agent 3.5.0
ePO Agent for Mac OS X 3.0.0
Product Coverage Reports 1.0.0
Rogue System Sensor 1.0.0
System Compliance Profiler 1.1.0
VirusScan Enterprise 8.0.0
VirusScan for Mac 8.5

Category	Policy Name	Inherited From	Inherited By	Lock	Edit Row
Enforce Policies	Yes	Global Default	all inherit	□	Edit
VirusScan Policies	McAfee Default	Global Default	4 don't inherit	□	Edit

When you first log on to the server, the console appears with **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.

> For detailed information about using ePolicy Orchestrator, refer to the *ePolicy Orchestrator Product Guides*.

Installation

Introduction

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

System requirements

The agent can be installed on the Apple Macintosh OS X operating system, version 10.4.6 (or later), on any of the following Macintosh platforms:

- G3
- G4
- G5
- SMP (dual processor)
- Intel-based Macintosh computer

Checking in NAP files to manage VirusScan

To manage VirusScan through ePolicy Orchestrator, you must first add the product .NAP files to the software repository on the ePolicy Orchestrator server. The .NAP files contain VirusScan policy pages, where you control the product settings that are deployed through the ePolicy Orchestrator agent to the client computers.

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 VirusScan are available in the **ePolicy Orchestrator Server Components** subfolder on the product CD, or in the product .ZIP file. A .NAP file always has a .NAP 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 NAP file (NWA-MAC300.NAP)

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

1 Locate the NWA-MAC300.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.

> Alternatively, you can open the wizard by double-clicking **Repository** in the ePolicy Orchestrator console tree, then clicking **Check in NAP** in the details pane.

4 Select **Add new software to be managed** and click **Next**.

5 In the **Select a Software Package** dialog box, browse to and select the NWA-MAC300.NAP file you saved to a temporary folder in Step 1 on page 34.

6 Click **Open** to enable ePolicy Orchestrator to load the selected .NAP file.

Adding VirusScan for Mac NAP file (Virex.nap)

To add Virex.nap file to the ePolicy Orchestrator server:

1 Locate the **Virex.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 Select **Add new software to be managed** and click **Next**.

5 In the **Select a Software Package** dialog box, browse to and select the **Virex.nap** file you saved to a temporary folder in Step 1 on page 34.

6 Click **Open** to enable ePolicy Orchestrator to load the selected .NAP file.

Adding VirusScan for Mac Report NAP file (virexExt.nap)

To add virexExt.nap file to the ePolicy Orchestrator server:

1 Locate the **virexExt.nap** file, either on the product CD or in the installation .ZIP file downloaded from the McAfee website, 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 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 of *Adding VirusScan for Mac Report NAP file (virexExt.nap)* section, and click **Open** to enable ePolicy Orchestrator to load the report .NAP file into the repository.

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

Installing the ePolicy Orchestrator agent for Macintosh computers

The ePolicy Orchestrator agent for Macintosh computers can be installed through either a standard (graphical interface) installation, or a command-line (silent) install. The agent is installed in the `/Library/NETAepoagt` directory and also uses the `/Library/NETASSOC` directory for configuration related data.

> You cannot change the installation directory of the ePolicy Orchestrator agent.

Standard installation

1 Locate the **nwa.dmg** file, either on the product CD or in the installation .ZIP file downloaded from the McAfee website, 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 the **nwa.dmg** file. The following files appear.

- NWA.pkg
- cmdinstall

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

4 Click **Continue**. The **ReadMe** window appears. This ReadMe describes the agent features, and 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** window appears. Select the volume where you want to install the ePolicy Orchestrator agent and click **Continue**.

7 The **Easy Install** window appears.

> There are two versions of this window depending on whether you are installing/reinstalling the agent or upgrading it. If you are installing the agent for the first time, or reinstalling it after you have uninstalled the previous ePolicy Orchestrator agent installation, this window contains an **Install** button. If upgrading a previous version of ePolicy Orchestrator agent, this window contains an **Upgrade** button.

8 Click **Install/Upgrade** to continue.

9 You are required to authenticate your credentials. 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.

10 Type the **ePO Server IP address** and the **ePO Server Port** number. Click **Apply**. The **Install Software** window appears.

11 Click **Restart** to complete the installation process.

Silent installation (command-line)

1 Locate the **nwa.dmg 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.

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

2 Double-click the **nwa.dmg** file. The following files appear.

- NWA.pkg
- cmdinstall

3 Open the **Terminal** window and change the working directory to `/Volumes/NAINWA`.

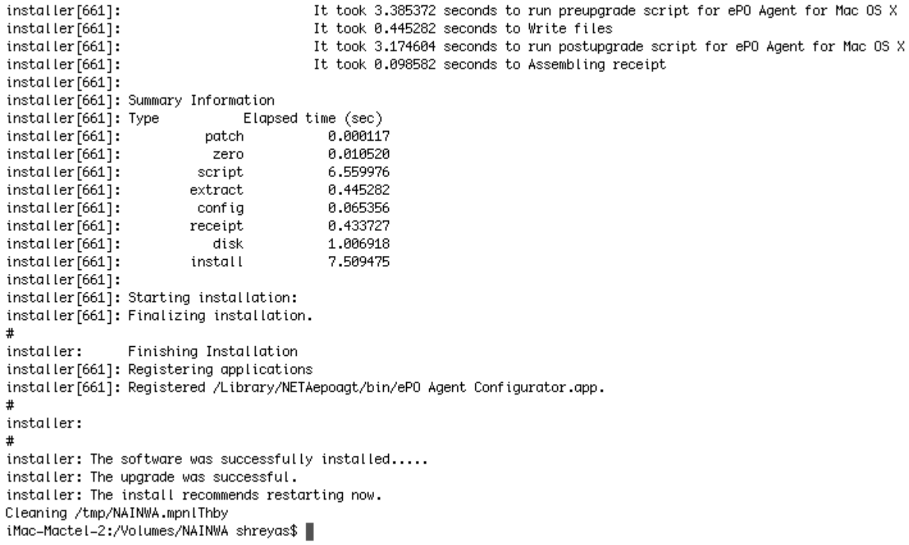
> You need to be have administrator rights to execute this command.

4 In the **Terminal** window, execute

```
sudo ./cmdinstall <ePO Server IP Address>:<ePO Server Port>
```

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

Figure 4-2 Terminal window - Install/Upgrade complete



```
installer[661]:                        It took 3.385372 seconds to run preupgrade script for ePO Agent for Mac OS X
installer[661]:                        It took 0.445282 seconds to Write files
installer[661]:                        It took 3.174604 seconds to run postupgrade script for ePO Agent for Mac OS X
installer[661]:                        It took 0.098582 seconds to Assembling receipt
installer[661]:
installer[661]: Summary Information
installer[661]: Type           Elapsed time (sec)
installer[661]:          patch           0.000117
installer[661]:           zero           0.010520
installer[661]:         script           6.559976
installer[661]:        extract           0.445282
installer[661]:         config           0.065356
installer[661]:        receipt           0.433727
installer[661]:           disk           1.006918
installer[661]:        install           7.509475
installer[661]:
installer[661]: Starting installation:
installer[661]: Finalizing installation.
#
installer:      Finishing Installation
installer[661]: Registering applications
installer[661]: Registered /Library/NETAepoagt/bin/ePO Agent Configurator.app.
#
installer:
#
installer: The software was successfully installed.....
installer: The upgrade was successful.
installer: The install recommends restarting now.
Cleaning /tmp/NAINWA.mpnlThby
iMac-Mactel-2:/Volumes/NAINWA shreyas$ █
```

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

Installing VirusScan for Mac

Refer to the section *Installing VirusScan for Mac* on page 13 for details on installing the software on Macintosh computers.

Uninstallation

Removing VirusScan for Mac from the ePolicy Orchestrator server

You can uninstall the VirusScan for Mac .NAP file from the ePolicy Orchestrator server.

To remove the VirusScan for Mac NAP file:

1 Log on to the ePolicy Orchestrator database server.

2 Select **VirusScan for Mac** under **Repository** | **Managed Products** | **MAC OS X** | in the console tree.

3 Right-click **VirusScan for Mac** and select **Remove** to uninstall the VirusScan .NAP file from the ePolicy Orchestrator server.

Removing ePolicy Orchestrator Agent for Mac OS X 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 VirusScan for Mac

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

To uninstall ePolicy Orchestrator agent using the command line:

1. Log in with administrative rights.
2. Go to the `/Library/NETAepoagt directory`.
3. Run `cmduninst.`

Setting policies within ePolicy Orchestrator

The 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.

Before configuring any policies, select the group of computers for which you want to modify VirusScan for Mac policies. You can modify VirusScan for Mac policies from the pages and tabs that are available in the details pane of the ePolicy Orchestrator console. These pages are nearly identical to those you can access directly from the VirusScan for Mac user interface.

After you have modified the appropriate polices and saved the changes for the intended computer or group of computers, you are ready to deploy the new settings via the ePolicy Orchestrator agent.

To modify policies for VirusScan for Mac 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 to which these policies are to apply. The **Policies**, **Properties**, and **Tasks** tabs appear in the details pane.

3 Select the **Policies** tab in the details pane, then expand **VirusScan for Mac 8.6**. **Enforce Policies** and **VirusScan Policies** appear beneath the **VirusScan for Mac 8.6** entry.

4 Under **Policy Name**, click **McAfee Default** for a **Category** to view the default policy settings.

> You cannot configure the **McAfee Default** policy settings for a selected **Category**. To configure a selected category, you *must* create a new policy for the selected **Category**.

To create a new policy for a category:

1 Click **Edit** for a **Category** in the **VirusScan for Mac 8.6** entry in the ePolicy Orchestrator details pane.

2 Click the **Policy Name** drop-down list and select **New Policy**. The **Create a new policy** dialog box appears.

Create a new policy options

Duplicate the following policy	Creates a duplicate policy for the selected **Category**. Select the policy from the drop-down list.
Create a policy in which all tabs inherit	Creates a new policy in which all the policy tab settings are inherited.
New policy name	Type the new policy name for the **Category** you want to create.

3 Configure the required options from the original policy, then click **OK** to create the new policy.

4 Click **Apply** to save these settings.

To edit an existing policy:

1 Click ✎ for the selected **Category** in the **VirusScan for Mac 8.6** entry in the ePolicy Orchestrator details pane.

2 Configure the required options, then click **Apply** to save the policy.

To enforce policies:

1 Click **Edit** for **Enforce Policies** in the VirusScan for Mac entry in ePolicy Orchestrator.

2 Click the **Policy Name** drop-down list and select **Yes**.

3 Click **Apply** to enforce the policies that you just configured.

General tab

The **General** tab allows you to enforce general policies controlling overall functioning of VirusScan for Mac, such as automatically checking for virus definitions updates, performing On-Access scans, logging scan results, and creating exclusion lists for specific disks, files and folders.

You can enforce the following general policies:

Automatically check for virus definition updates	Enables/disables automatic eUpdates.
On-Access scan	Enables/disables On-Access scanning.
Log results to file	Enables/disables logging results to a file.
Exclude specific disks, files and folders	Excludes from scanning the items listed here. If this option is not selected, the scanner ignores the list of exclusions. Add Exclusion: ■ 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.** Remove Exclusion: ■ Select the exclusion in the **Exclusion list** and click **Remove**. Edit Exclusion: ■ Select the exclusion in the **Exclusion list** and click **Edit**.

eUpdate tab

The **eUpdate** tab allows you to customize DAT 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.

Customizing eUpdate settings

When updating your DAT and engine files, you must specify the details of the server from where the update files are to be transferred.

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

On-Access scanner tab

The On-Access scanner tab allows all files that are currently in use to be scanned automatically to determine if a virus or other malware is present. A scan takes place whenever a file is read from the disk, and/or written to the disk, either by the user or by system processes. Using the On-Access scanner, continuous policy enforcement can be provided for multiple files, directories, or volumes, including volumes on remote computers connected through the network. You can configure what the scanner looks for and how it responds to infected files. The scanner notifies you, in the **Reporter** pop-up window of the Macintosh computer, if it finds a virus or other malware.

You can enforce the following On-Access scanner policies:

Scan contents of archives and compressed files	Sets the scanner to scan inside archives and other compressed files. **Off** by default for the On-Access scanner. Note that the On-Access scanner will not scan inside stuffit archives.
Find Unknown Macro Viruses	If a file contains potentially infected macro (unknown infection), it will be scanned and cleaned/deleted, as part of the clean.
Scan Apple Mail messages	Sets the scanner to scan Apple Mail messages.
Check files for virus-like characteristics	Enables/disables heuristics, which scan 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.
Scan files on network volumes	Sets the scanner to scan files held on network volumes.
Scan files: ■ Always ■ Read ■ Write	Determines if the scanner is to scan files that are read from the disk, written to the disk, or both. By default, this is set to **Always** so files that are written to the disk or read from the disk are scanned.
When a virus is found: ■ Clean ■ Delete ■ Notify	Selects the primary action of the On-Access scanner when a virus is found.
Delete when Clean fails or is not available	Selects the secondary action for the scanner when a virus is found. This is only available when the primary action is **Clean**.
Maximum scan time	The maximum length of time, in seconds, that a scan can last for one file. (A compressed file is not treated as one file; this timeout applies to the last individual file, and not to the last top level container file.)

On-Demand scanner tab

The On-Demand scanner tab 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. The scanner notifies you when it finds a virus and generates a log that appends its actions.

You can enforce the following On-Demand scanner policies:

Scan contents of archives and compressed files	Sets the scanner to scan into archives and other compressed files. **On** by default for the On-Demand scanner.
Find Unknown Macro Viruses	If a file contains potentially infected macro (unknown infection), it will be scanned and cleaned/deleted, as part of the clean.
Scan Apple Mail messages	Sets the scanner to scan Apple Mail messages.
Check files for virus-like characteristics	Enables/disables heuristics, which scan 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 a virus is found: ■ Clean ■ Delete ■ Notify	Selects the primary action of the scanner when a virus is found.
Delete when Clean fails or is not available	Selects the secondary action for the selected scanner when a virus is found. This is only available when the primary action is **Clean**.

Scheduling scans and eUpdates

When VirusScan for Mac scans for viruses, it uses information in the DAT files to find and remove viruses. Many new viruses are discovered daily, and McAfee regularly creates new DAT files to provide protection from these viruses. To ensure the best anti-virus protection, you can use ePolicy Orchestrator to inform VirusScan for Mac where to access the latest DAT files, to create schedules for replacing earlier DAT files, and to run On-Demand scans.

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

- On-Demand scan
- eUpdate

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

On-Demand scans

VirusScan for Mac can perform On-Demand scanning of your files, so that all files on your computer are checked for viruses, Trojan horses and other malware. 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 also disable schedules that you do not want to run automatically.

Creating a new task

1. Click **Tasks** tab in the upper details pane. Right-click in the pane, and select **Schedule Tasks**.
2. Type a name for the task in the **New Task Name** field and select the task you want to create.
3. In the **Task Type** drop-down list, select **ODS**. Click **OK**.

   The created task is listed in the **Tasks** tab.

Editing a task

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

2 Click **Settings**. The **Where** page appears where you can include files and directories in the scheduled scan.

Include these files and directories in the scan.	Configures your scanning inclusions. Add inclusion: ■ 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.** Remove inclusion: ■ Select the inclusion in the **Exclusion list** and click **Remove**. Edit inclusion: ■ Select the inclusion in the **Inclusion list** and click **Edit**. In 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

3 Deselect **Inherit** to enable the settings in the **Schedule Settings** pane.

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 maximum hours and minutes the task can run before it is cancelled.

4 Click the **Schedule** tab to find these options:

Schedule Task	Select one of the available task types from the drop-down list: ■ Daily ■ Weekly ■ Monthly ■ Once ■ At System Startup ■ Run Immediately
Start Time ■ UTC Time ■ Local Time	Specify the start time for the scheduled task. Select the local time option to run the task using the scheduled interval at the client computer system time. This is useful for scheduling processor-intensive tasks, such as On-Demand scans, to run during non-business hours. Selecting the UTC Time option uses the Universal Time Conversion (also known as Greenwich Mean Time or GMT) to run the task. This option causes the task to run at the same time for all your Macintosh clients regardless of the local system time on the Macintosh systems.
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 otherwise not available at the scheduled start time. Selecting this option ensures the task is run 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 run.
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 for a specified period, such as for a few days or weeks.
Repeat Task	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. Typically, you might do this to run a client update task several times a day, especially if there are a lot of new viruses. You can also schedule the task to repeat during other intervals, such as weekly or monthly.
Schedule Task Daily	Specify the interval to execute the schedule task; this could be an interval of 1 or several days. If you select 1, the schedule task is executed every other day.

Deleting a task

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

eUpdate

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 DAT files daily, and regularly check the McAfee Avert Labs web site for new DAT files. If you have multiple servers in the current domain (all running VirusScan for Mac), you can use one server to download the latest DAT files, 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 tab.

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.

2 Type a name in New Task Name.

3 Select VirusScan for Mac 8.6 - 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 Click Settings, edit the required options in both the Task and Schedule tabs.

3 Deselect **Inherit**.

4 Select **Run eUpdate** and then select **Inherit**.

5 Click **OK** to return to **ePolicy Orchestrator Scheduler** dialog box.

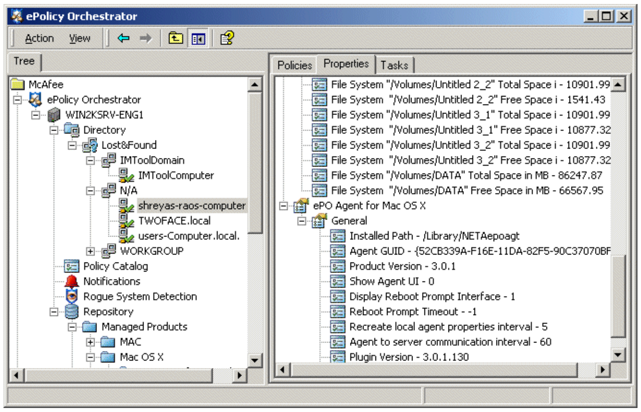
Viewing ePolicy Orchestrator properties

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

To view the properties:

1 In the console tree, select the server for which you want to view settings.

Figure 4-3 System Properties



File System "/Volumes/Untitled 2_2" Total Space i - 10901.99
File System "/Volumes/Untitled 2_2" Free Space i - 1541.43
File System "/Volumes/Untitled 3_1" Total Space i - 10901.99
File System "/Volumes/Untitled 3_1" Free Space i - 10877.32
File System "/Volumes/Untitled 3_2" Total Space i - 10901.99
File System "/Volumes/Untitled 3_2" Free Space i - 10877.32
File System "/Volumes/DATA" Total Space in MB - 86247.87
File System "/Volumes/DATA" Free Space in MB - 66567.95
Installed Path - /Library/NETAepoagt
Agent GUID - {52CB339A-F16E-11DA-82F5-90C37070BF
Product Version - 3.0.1
Show Agent UI - 0
Display Reboot Prompt Interface - 1
Reboot Prompt Timeout - -1
Recreate local agent properties interval - 5
Agent to server communication interval - 60
Plugin Version - 3.0.1.130

2 In the upper details pane, click the **Properties** tab.

3 In the **Properties** pane, expand the **VirusScan for Mac** tree view to list its various properties.

4 Click + next to a property to view its details.

Reports

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

All VirusScan for Mac reports fall under the **Antivirus** heading.

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 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:

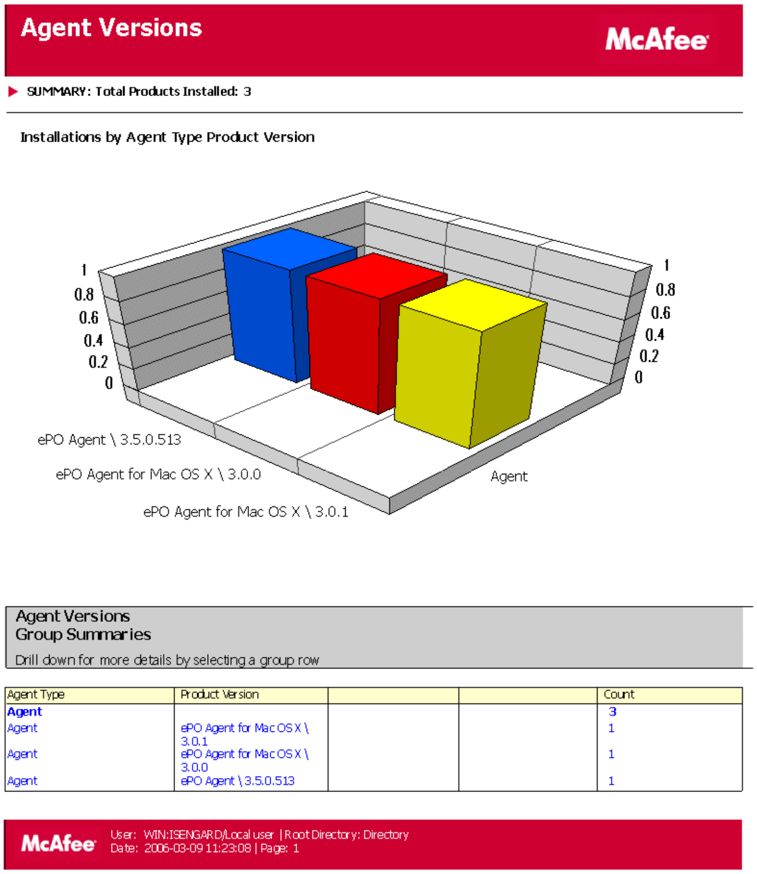
1. Log on to the ePolicy Orchestrator database server.
2. Select the desired VirusScan for Mac report under **Reporting** | **ePO Databases** | <**database server**> | **Reports** | <**report group**> in the console tree.
   - If the **Current Protection Standards** dialog box appears, specify the version 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 Guides* for more details on all the available settings tabs.

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

4 A report for **Agent Versions** is generated.

Figure 4-4 Sample report - Agent Versions


1
0.8
0.6
0.4
0.2
0
1
0.8
0.6
0.4
0.2
0
ePO Agent \ 3.5.0.513
ePO Agent for Mac OS X \ 3.0.0
ePO Agent for Mac OS X \ 3.0.1
Agent

Agent Versions

McAfee

▶ SUMMARY: Total Products Installed: 3

Installations by Agent Type Product Version

Agent Versions
Group Summaries

Drill down for more details by selecting a group row

Agent Type	Product Version			Count
Agent				**3**
Agent	ePO Agent for Mac OS X \ 3.0.1			1
Agent	ePO Agent for Mac OS X \ 3.0.0			1
Agent	ePO Agent \ 3.5.0.513			1

McAfee User: WIN:ISENGARD/Local user | Root Directory: Directory
Date: 2006-03-09 11:23:08 | Page: 1

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 required report data, (for example, to determine which Macintosh client computers do not have a compliant version of VirusScan for Mac 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.

5 Integrating with ePolicy Orchestrator 4.0

Introduction

This chapter describes how to configure VirusScan using McAfee ePolicy Orchestrator management software version 4.0. To use this chapter effectively, you need to be familiar with ePolicy Orchestrator 4.0.

ePolicy Orchestrator 4.0 provides a scalable platform for centralized policy management and enforcement on your security products and systems on which they reside. It also provides comprehensive reporting and product deployment capabilities, all through a single point of control.

> This guide does not provide detailed information about installing or using ePolicy Orchestrator software. See *ePolicy Orchestrator v4.0 Product Guide*.

Extensions

VirusScan extensions come pre-installed with ePolicy Orchestrator 4.0. You can install, remove and manage the VirusScan extension files. Extension files are in ZIP file format and must be installed before that product or component can be managed by ePolicy Orchestrator 4.0.

> In case you uninstall VirusScan extensions, the extensions are available at **Program Files | McAfee | ePolicyOrchestrator | Extensions**.

The two extension files for VirusScan are:

- VSCANMAC8600.ZIP
- VIREXREPORTS.ZIP

To install the VirusScan policy extension files

1. Using an administrative account, log on to the ePolicy Orchestrator server.
2. Click **Configuration** | **Extensions** | **Install Extension**. The **Install Extension** dialog box appears.
3. Click **Browse**, select the extension file VSCANMAC8600.ZIP and click **OK**.

To install the VirusScan report extension files

1. Using an administrative account, log on to the ePolicy Orchestrator server.

2 Click **Configuration** | **Extensions** | **Install Extension**. The **Install Extension** dialog box appears.

3 Click **Browse**, select the extension file **VIREXREPORTS.ZIP** and click **OK**.

Introducing ePolicy Orchestrator 4.0 Dashboard

Dashboards are a collection of pre-configured and/or user-selected monitors that provide current data about your detections.

The ePolicy Orchestrator dashboard consists of a collection of named dashboard monitors. Depending on the permissions assigned to your user account, you can create a new dashboard, manage existing dashboards, select active dashboards, and edit dashboard preferences

Creating a new dashboard

1 Using an administrative account, log on to the ePolicy Orchestrator server.

2 Click **Dashboards** | **Options** | **New DashBoard**. The **New DashBoard** page appears.

3 Enter a **Dashboard Name** and choose a desired **Dashboard Size** from the drop-down.

4 Click **New Monitor**.

5 Choose the **Category** as **Queries** and a desired VirusScan related query from the **Monitor** drop-down menu.

6 Click **OK**.

7 Repeat step 4 and 5 for the remaining monitors.

8 Click **Save**. The **Make Active** dialog box appears.

9 Click **Yes** to add this new dashboard to your active set.

Table 5-1 Dashboard Options

Options	**Description**
Dashboard Name	Specifies the name of the dashboard you select.
Dashboard Size	Specifies the dimensions (by number of dashboard monitors) of the selected dashboard.
Created by	Specifies the user name who created the selected dashboard.
Last modified by	Specifies the user name, date and time stamp of the last modification made to the selected dashboard.
Edit	Takes you to the **Edit Dashboard** page where you can make changes to the dashboard's name and size.
Delete	Deletes the selected dashboard.
Duplicate	Creates and saves a copy of the selected dashboard. This allows you to create and edit similar dashboards without having to create one from scratch.
Make Public	Adds the selected private dashboard to the Public Dashboards list, making it available to all users with permissions, to use public dashboards.
Make Active	Adds the selected dashboard to the Dashboards tab for easy access.

Systems

All the systems in the network are managed in the **Systems** tab. The **System Tree** contains all systems that are managed by the ePolicy Orchestrator. It is the primary interface for managing policies and tasks on these systems. You can organize or sort these systems into logical groups in the **System Tree**.

My Organization is the root of the **System Tree**. It includes a **Lost&Found** group that stores systems whose locations cannot be determined by the server. Depending on the methods you use to create and maintain the **System Tree** segments (systems), the server uses different characteristics to place the systems in the **System Tree**.

> ℹ For information on adding a new system, refer to the *ePolicy Orchestrator 4.0 Product Guide*.

Sending an Agent Wakeup Call

1. Using an administrative account, log on to the ePolicy Orchestrator server.
2. Click **Systems**.
3. Choose a group in the **System Tree**.
4. Select the desired **Computer Name**(s) of that group.
5. Click **More Actions** | **Wake Up Agent**. The **Wake Up Agents** page appears.
6. Choose a **Wake-up call type** and a **Randomization** period (0-60 minutes) during which the system(s) respond to the wakeup call sent by the ePolicy Orchestrator server.
7. Select **Get full product properties** for the agent(s) to send complete properties instead of sending only those that have changed since the last agent-to-server communication.
8. Click **OK**.

> ℹ Navigate to **Server Task Log** to see the status of the agent wakeup call.

Policies

You can create, edit, delete or assign a policy to a specific group/system in the **System Tree**.

Creating a new policy

1. Using an administrative account, log on to the ePolicy Orchestrator server.
2. Click **Systems** | **System Tree** and choose a desired group.
3. From **Policies**, select the desired **Product** from the drop-down. A list of policies managed by the chosen point product appears in the lower pane.
4. Locate a desired policy category, then click **Edit Assignment**. The **Policy assignment for: My Organization| Lost& Found | (chosen group)** page appears.
5. Click **Create new policy**. The **Create a new policy** dialog box appears.

6 Choose **McAfee Default** or **My Default** as desired.

The **McAfee Default** policies are read-only and cannot be edited, renamed, or deleted.

7 Enter a **New policy name**.

8 Click **OK**, then **Save**.

Enforcing Policies

You can enforce a policy to multiple managed systems within a group.

1 Using an administrative account, log on to the ePolicy Orchestrator server.

2 Click **Systems** | **System Tree** and choose a desired group.

3 Select the desired system(s).

4 Click **Assign Policy**. The **Assigning Policy for <n> system** page appears.

5 Select the desired **Product**, **Category**, and **Policy** from the drop-down, then click **Save**.

6 Select the systems again.

7 Send an agent wakeup call.

For instructions on sending an agent wake-up call, please refer to *Sending an Agent Wakeup Call* on page 51.

You can create and enforce VirusScan policies and view reports only after adding the VirusScan extension files.

Client tasks

ePolicy Orchestrator allows you to create, schedule and maintain client tasks that run on the managed systems. You can define client tasks for the entire **System Tree**, a specific group, or an individual system.

Using ePolicy Orchestrator 4.0, you can create these types of scheduled tasks for the VirusScan software:

- eUpdate task
- OnDemand scan task

The client tasks available in the drop-down depend on the extension files installed.

eUpdate task

Your software can only provide full protection if you keep it up-to-date with the latest anti-virus definitions (DATs) and virus-scanning engine. We recommend that you update DAT files daily and regularly check the McAfee AVERT (Anti-Virus Emergency Response Team) website for new DAT files.

Creating a new eUpdate task

1 Using an administrative account, log on to the ePolicy Orchestrator server.

2 Click **Systems** | **System Tree** and choose a desired group.

3 From the **Client Tasks**, select the desired group in the **System Tree** for which you want to create the eUpdate task.

4 Click **Create Task**. The **Client Task Builder** page appears.

5 Under **Description**, type a **Name** and **Notes** (if required) for the eUpdate task.

6 Choose **eUpdate Task (VirusScan 8.6)** as the **Type** of the task and click **Next**.

7 Schedule the task as desired and click **Next** to view the **Summary** of the eUpdate task, which includes the **Name**, **Notes**, **Product**, **Type** of the task, and the **Schedule** information.

8 Click **Save**.

9 Send an agent wake-up call.

> ⓘ For instructions on sending an agent wake-up call, please refer to *Sending an Agent Wakeup Call* on page 51.

> ⓘ Click **Edit** to change the description/schedule of an eUpdate task or **Delete** to remove it.

On-Demand scan task

You can create any number of on-demand scan schedules. The scan schedules can be configured to run at set intervals or can be run at any time by the user.

Creating an on-demand scan task

1 Using an administrative account, log on to the ePolicy Orchestrator server.

2 Click **Systems** | **System Tree** | **Client Tasks**.

3 Select the desired group in the **System Tree** for which you want to create the on-demand scan task.

4 Click **Create Task**. The **Client Task Builder** page appears.

5 Under **Description**, type a **Name** and **Notes** (if required) for the on-demand scan task.

6 Choose **On Demand Scan (VirusScan 8.6)** as the **Type** of the task and click **Next**.

7 Under **Configuration**, choose a policy from the drop-down.

8 Click **Next** and schedule the task as desired.

9 Click **Next** to view the **Summary** of the on-demand scan task, which includes the **Name**, **Notes**, **Product**, **Type** of the task, and the **Schedule** information.

10 Click **Save**.

11 Send an agent wakeup call.

ℹ For instructions on sending an agent wake-up call, please refer to *Sending an Agent Wakeup Call* on page 51.

ℹ Click **Edit** to change the description/schedule of an on-demand scan task or **Delete** to remove it.

Uninstallation

Removing the product extension

1 Using an administrative account, log on to the ePolicy Orchestrator server.

2 Click **Configuration | Extensions**.

3 Choose the extension file **VirusScan**, click **Remove**.

4 Select the option **Force removal, bypassing any checks or errors**.

5 Click **OK**.

Removing the report extension

1 Using an administrative account, log on to the ePolicy Orchestrator server.

2 Click **Configuration | Extensions**.

3 Choose the extension file **VirusScan Reports**, click **Remove**.

4 Select the option **Force removal, bypassing any checks or errors**.

5 Click **OK**.

6 Troubleshooting

This chapter provides solutions to situations that you might encounter when installing or using VirusScan software.

The following topics are included:

- *Frequently asked questions*
- *Error messages*

Frequently asked questions

Installation

Why is the installer not working?
Check the platform you are trying to install VirusScan onto: it must be Mac OS X version 10.4.6 (or later) or Mac OS X Leopard version 10.5, PowerPC or Intel-based Mac computer. The computer must have a minimum of 512 MB RAM and 45 MB of free disk space. Alternatively, an existing anti-virus program might have been detected during installation, which must be removed for VirusScan to be installed successfully. VirusScan also requires the BSD subsystem to be installed in order to function correctly.

What VirusScan files are installed and where?
VirusScan is installed in `/Applications`, VirusScan Schedule Editor is installed in `/Applications/Utilities`, and VirusScan Reporter is installed in `/Library/Application Support`. DAT files, dynamic libraries, and daemons can be found at `/usr/local/vscanx`.

Scanning

Why has VirusScan skipped scanning certain files?
Check to make sure the skipped files are not on the exclusion list. In addition, VirusScan will not scan archives and compressed files unless configured to do so.

When VirusScan was scanning a file, I dragged-and-dropped another file to be scanned. What happened to the file?

During a scan, you cannot add files to the scanning queue. Dragging multiple items simultaneously queues the scan; that is, dragging-and-dropping three folders or files would cause the scanner to perform three scans. Dragging one folder containing multiple files causes the scanner to perform one scan.

Why is VirusScan not scanning my computer at regular intervals?

Check that you have an On-Demand scan schedule set up to scan your computer, it is enabled, and it is configured to run regularly.

Viruses and detection

Can VirusScan detect both Macintosh and Windows viruses?

VirusScan detects all known Macintosh and Windows viruses and worms.

Why has VirusScan stopped displaying items that are scanned?

VirusScan will only show the first 200,000 items that have been scanned and found to be infected.

Why is the content in my log file cut off?

The size of a log file cannot exceed 512 KB. When a log file does exceed 512 KB, the file is renamed to VirusScan.log.0 and a new VirusScan.log is created. A maximum of two backup log files are kept. If you specifically want to keep a copy of the existing log file, we recommend that you save old log files before starting a new scan. To view the log file, select File | View Log.

General information

Can I undo the changes I made to the Preference settings?

If you have saved unwanted preferences, the settings can be reset to their default by clicking Reset to Defaults on the lower left corner of the Preferences window. There is no way to undo preference setting changes once they are made; settings in the Preferences menu are saved as soon as any change is made. We recommend that you make a note of your current preference settings before changing them.

Is there rollback support with eUpdate?

eUpdate only supports current or new updates. There is no rollback support.

Are Macintosh virus definitions included in the updates?

The eUpdates include both Macintosh and Windows virus definitions.

How do I find out the version number and date of the virus definitions (DAT) files?

Select About VirusScan from the VirusScan menu on the menu bar of the application. The dates of the DAT versions reflect only when the DAT files were created.

How often are DAT files updated automatically in VirusScan?

eUpdate checks for new updates automatically every day via the Internet. You can also manually download daily updates from the McAfee Virus Information Library website.

Why can't I connect to the eUpdate Server to perform an unscheduled eUpdate?

Check to see if you are connected to the Internet. The eUpdate server may also be busy.

Advanced troubleshooting

After installing VirusScan, can I view the processes running?

The processes that are running are VShieldScanManager and VShieldScanner.

Can I manually download virus definitions without using eUpdate?

From the Toolbar of the VirusScan Console, click **Virus Info**. This launches your default browser and directs you to the McAfee Virus Information Library. Click the **Downloads** link on the left-hand side of the screen to download the DAT files.

How do I customize eUpdate Server Settings?

1. Click **Preferences** on the tool bar to display the Preferences dialog box.
2. Click **More Options**.
3. Select the option **Customize eUpdate server settings**, then click **Customize**.
4. Configure the eUpdate FTP server settings and click **OK**.
5. Click **Close**.

Where can I find the log files?

Table 6-1 lists the log files.

Table 6-1 Log files

Log file	Description	Where can I find them
VirusScan.log	Contains VirusScan related entries.	You can access this log file from `/var/log/VirusScan.log`
log	Contains ePolicy Orchestrator Agent related entries.	You can access this log file from `/Library/NETAepoagt/scratch/etc/log`

Error messages

Table 6-2 lists all possible error messages you can see while running the VirusScan application, and the possible reasons for their occurrence.

Table 6-2 Error messages - VirusScan application

Serial No.	Message	Possible Reason
1	Initialization of VirusScan engine failed (error x).	The engine or DAT files have become corrupt or have been moved/deleted. Please re-install.
2	The Report could not be saved. Maybe the disk is full or there is no data to be written.	Your disk may not have enough space to save the report. Free up some room and try to save again.

Table 6-2 Error messages - VirusScan application

Serial No.	Message	Possible Reason
3	The URL for the Virus Information Library could not be opened. Your browser may not be correctly installed.	Please ensure that your browser is installed correctly.
4	An error occurred while installing the update. The eUpdate was not completed.	There was an error when attempting to install the update. Please restart the eUpdate process and try again.
5	An error occurred while unpacking the update. The eUpdate was not completed.	There was an error when attempting to unpack the update for installation. Please restart the eUpdate process and try again.
6	An error occurred while downloading the update. The eUpdate was not completed.	There was an error when attempting to download the update. The server may be busy currently. Wait a few minutes then restart the eUpdate process and try again.
7	This software product is becoming close to the end of its designed life. To maintain correct anti-virus capability, it is recommended that the product is updated as soon as possible.	Your version of VirusScan has become outdated. We recommend that you upgrade to the newest version of VirusScan to ensure the best virus protection possible.
8	This software product is coming very close to the end of its designed life and its further use can no longer be supported. To maintain correct anti-virus capability, it is now important that the product is updated as soon as possible.	Your version of VirusScan has become outdated. We recommend that you upgrade to the newest version of VirusScan to ensure the best virus protection possible.
9	This software product can no longer provide satisfactory virus protection. To maintain correct anti-virus capability, it is now necessary that the product is updated.	Your version of VirusScan has become outdated. We recommend that you upgrade to the newest version of VirusScan to ensure the best virus protection possible.
10	The scanning engine installed for this product is coming close to the end of its designed life. To maintain correct anti-virus capability, it is recommended that the scanning engine is updated as soon as possible.	The engine included with VirusScan has become outdated. We recommend that you perform an eUpdate task as soon as possible to ensure the best virus protection possible.
11	The scanning engine installed for this product is coming very close to the end of its designed life and its further use can no longer be supported. To maintain correct anti-virus capability, it is now important that the scanning engine is updated as soon as possible.	The engine included with VirusScan has become outdated. We recommend that you perform an eUpdate task as soon as possible to ensure the best virus protection possible.
12	The scanning engine installed for this product can no longer provide satisfactory virus protection. To provide correct anti-virus capability, it is now necessary to update the scanning engine.	The engine included with VirusScan has become outdated. We recommend that you perform an eUpdate task as soon as possible to ensure the best virus protection possible.

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-server communication from the server-side.

agent-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-server communications interval (ASCI) The time period between predefined agent-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 email, pager, or phone.

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.

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; and 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.

Daemon
A program that runs constantly and exists to handle service requests the computer system receives. The daemon program then forwards these requests to other programs or processes.

DAT files
Virus definition files that allow the anti-virus software to recognize viruses and related potentially unwanted code embedded in files.

EICAR
European Institute of Computer Anti-Virus Research. EICAR has developed files that can be used to test the proper installation and operation of anti-virus software.

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

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.

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

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.

ePolicy Orchestrator server
The back-end component of the ePolicy Orchestrator software.

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.

eUpdate
eUpdate allow you to update your DAT files and the virus-scanning engine. It automatically checks daily for new updates when there is an Internet connection.

events
Data exchanged during agent-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 numbers).

Extra DAT files

Supplemental virus definition file that is created in response to an outbreak of a new virus or a new variant of an existing virus.

Firewall

A program that acts as a filter between your computer and the network or Internet. It can scan all traffic arriving at your computer (incoming traffic) and all traffic sent by your computer (outgoing traffic). It scans traffic at the packet level, and either blocks it or allows it, based on rules that you set up.

FTP

File Transfer Protocol. It is a common way to move files between two Internet sites.

Global Administrator

A user account with read, write, and delete permissions, and rights to all operations. Operations that affect the entire installation are reserved for use only by global administrator user accounts.

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 the sorting of 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.

HTTP

HyperText Transfer Protocol. It is a protocol for moving files across the Internet. It requires an HTTP client program on one end and an HTTP server program on the other.

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-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.

Joke program

A non-replicating program that may alarm or annoy users, but contains no malware and does not do any actual harm to files or data.

Log/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 scanning, or updating tasks.

Lost&Found group

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

Macro

In some programs, like word-processing programs, a macro is a saved sequence of commands that can be stored and then recalled with a single command or keyboard stroke.

McAfee Virus Information Library

The Virus Information Library (`http://vil.nai.com/vil/default.aspx`) has detailed information about the origins of viruses, how they infect your computer, and how to remove them. The site also contains information on hoaxes.

On-Access scanner

The On-Access scanner continuously monitors all files in use to determine if a virus or other potentially unwanted malware is present. It takes place whenever a file is read from the disk, and/or written to the disk. Multiple directories and volumes can be scanned.

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. You can scan multiple files, directories, and volumes.

On-access scanning

A continuous examination of files in use to determine if a virus or other malware is present. It can take place whenever a file is read from the disk, and/or written to the disk. Multiple directories and volumes can be scanned.

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.

policy

The configuration settings of managed products 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-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.

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 of 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*.

Trojan horse

A program that either pretends to have, or is described as having, a set of useful or desirable features, but actually contains a damaging payload. Trojan horses are not technically viruses, because they do not replicate.

upper details pane

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

UTC time

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

VirusScan Console

The most common user interface for VirusScan. This console allows you to configure the On-Demand scanner and the On-Access scanner, run On-Demand scans, and start eUpdates.

VirusScan Schedule Editor

Allows you to schedule additional virus definition and software updates.

Virus

A program containing malware that can alter or destroy files or programs that is capable of replicating with little or no user intervention, and the replicated program(s) also replicate further.

Worm

A virus that spreads by creating duplicates of itself on other drives, systems, or networks. It does not attach itself to additional programs but can alter, install, or destroy files and programs.

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.

Index

McAfee®

mcafee.com