Product Guide
Revision 1.0

Virex®
version 7.6

McAfee®
System Protection

Industry-leading intrusion prevention solutions

McAfee® SECURITY

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, © 1989. ♦ Software copyrighted by Gunnar Ritter. ♦ Software copyrighted by Sun Microsystems®, Inc. © 2003. ♦ Software copyrighted by Gisle Aas. © 1995-2003. ♦ Software copyrighted by Michael A. Chase, © 1999-2000. ♦ Software copyrighted by Neil Winton, © 1995-1996. ♦ Software copyrighted by RSA Data Security, Inc., © 1990-1992. ♦ Software copyrighted by Sean M. Burke, © 1999, 2000. ♦ Software copyrighted by Martijn Koster, © 1995. ♦ Software copyrighted by Brad Appleton, © 1996-1999. ♦ Software copyrighted by Michael G. Schwern, © 2001. ♦ Software copyrighted by Graham Barr, © 1998. ♦ Software copyrighted by Larry Wall and Clark Cooper, © 1998-2000. ♦ Software copyrighted by Frodo 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.

Contents

1 Introducing Virex 7.6

What's in this guide?

This guide introduces McAfee® Virex® software version 7.6, 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.

What is Virex 7.6?

Virex 7.6 is an anti-virus application that helps you keep your Apple computer free of viruses, Trojan horses and other malicious code. It scans volumes, files, and folders and provides detailed reports of what it finds. Virex 7.6 features on-demand scanning, scan and update scheduling, online help 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. The Virex 7.6 design is based on Cocoa, the specialized Mac OS X application environment.

How does Virex 7.6 work?

Virex protects your system from viruses that may reside on other computers such as Macintosh computers, Windows computers, UNIX computers, and volumes such as USB devices and CDs. The Virex Active Scanner, Background Scanner, and Mounted Volumes Scanner are background processes that continuously check your system, its files, CDs, and USB devices for possible viruses and other harmful programs.

What you can do with Virex 7.6

The Virex 7.6 anti-virus scanners give you powerful features that you can customize to meet your needs:

- Virex 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 Virex 7.6, you can scan a single file, a file directory, your whole drive, or mounted volumes such as CDs, .DMG files, and USB devices such as pen drives and cameras.
- Advanced heuristic scanning detects previously unknown macro and program viruses.
- The HealthCheck component monitors anti-virus scanners to ensure they do not quit, and restarts them if they do, to ensure that you are always protected.
- You can perform On-Demand scanning and automate scheduled scans.
- Scheduled and automated updates ensure that your anti-virus protection is kept up-to-date, guarding against viruses and other threats as they emerge.

What's new in this release

Virex 7.6 includes ePolicy Orchestrator manageability.

Previous release	Virex 7.5.1 did not have ePolicy Orchestrator manageability feature.
Current release	This release integrates Virex 7.6 with ePolicy Orchestrator 3.02 and above providing you with a single point of control for your systems running Virex 7.6 software.
Benefits	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 Virex on the target systems across your network; you do not need to configure them individually from the Virex Preferences window.
For more information	See *ePolicy Orchestrator Product Guide, Virex 7.6 Configuration Guide (for use with ePolicy Orchestrator)* and *Non Windows Agent* ReadMe*.

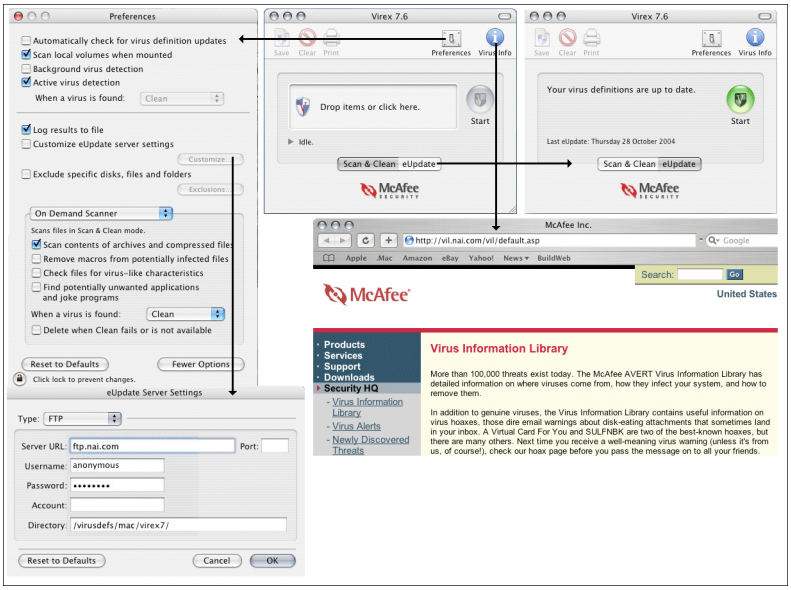
*. Non Windows Agent (NWA) is also known as ePolicy Orchestrator Agent for Mac OS X.

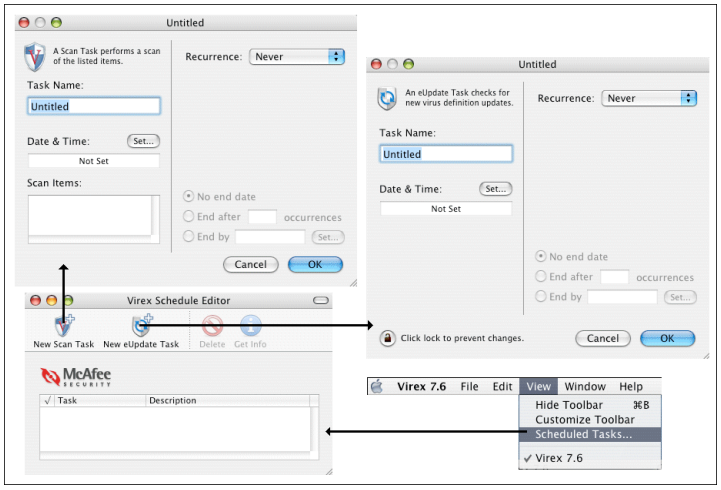
You will be able to use ePolicy Orchestrator related functionality only if you have ePolicy Orchestrator server installed and configured to manage Virex 7.6. The use of ePolicy Orchestrator is optional and you can use all the functionality of Virex 7.6 as a standalone product.

Virex 7.6 features

Virex 7.6 incorporates its previous powerful features with new safeguards and tools for you to protect your computer system. For more information on new features, please see *Getting Started* on page 25. The online help system provides you with troubleshooting assistance and procedures for tasks.

The following image map diagrams show the common dialog boxes you will encounter while using Virex.





Virex 7.6 Console

The Virex 7.6 console enables the configuration of Virex through an easy-to-use interface. In earlier versions of Virex, the console featured limited functionality.

Through the updated console, you can schedule tasks, configure the Active Scanner, Background Scanner, Mounted Volumes Scanner, and On-demand Scanner as well as perform On-demand scans through the drop-zone (an area on the Virex console that allows you to drag and drop files that you want to scan) and a file open dialog box. The console is also used to start eUpdates. To access the Virex console, double-click on the Virex 7.6 shield icon inside your computer's **Applications** folder.

Active Scanner

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

The Active Scanner scans files when they are written to your hard drive (all partitions) and all removable drives. It starts when your computer starts and runs until the computer is shut down; the scanner is running on your computer by default. You can configure what the scanner looks for and how it will respond to infected files. Preferences for Active Scanner are found under **Preferences** on the **Virex 7.6** menu.

Background Scanner

The Background Scanner permanently scans all files on your system. The scanner protects your computer by continuously searching your system for infected files.

This scan is a low-resource operation so there is no performance decrease to your computer. You can configure what the scanner looks for and how it responds to infected files. Preferences for the scanner are found under **Preferences** on the **Virex 7.6** menu.

Mounted Volumes Scanner

The Mounted Volumes Scanner initiates a scan of a volume such as a CD or camera when one is locally mounted. With this scanner you can scan a large volume or device for infection before interfacing it with your system. This limits your system's exposure to malicious viruses.

This feature only works with locally inserted or ejectable media, such as Zip drives, CD, DVD, or OS X .DMG files. It also scans USB card devices such as pen drives and cameras, and Firewire devices such as iPod. It does not scan volumes on remote machines connected through the network. The scanner operates in the background and interacts with the user. The Mounted Volumes Scanner is *not* running on your computer by default. To turn this scanner on, use the **Preferences** option on the **Virex 7.6** menu.

On-Demand Scanner

The On-Demand Scanner allows you to initiate a scan at any time by dragging and dropping selected files into the console or through a file open dialog box.

With the On-Demand Scanner you can select multiple files, directories, or volumes. Scan results are summarized in a report that can be saved or printed. You can configure what the scanner looks for and how it responds to infected files. You can also configure an exclusion list that is shared with the Active Scanner, Background Scanner and Mounted Volumes Scanner. The scanner notifies you when it finds a virus and generates a log that appends its actions. To access the On-Demand Scanner, drag the file(s) you want to scan and drop them into the Virex shield icon or into the Drop Zone in the Virex console.

Uvscan Command-line Scanner

The Uvscan Command-line Scanner is a stand-alone on-demand scanner for OS X environments. It allows advanced users to access the same on-demand scanner functionality as the **Virex 7.6** Console, but from a terminal shell. As the functionality is the same, this guide does not include information on how to use Uvscan. Some help is available from its *man* pages. You can access the Uvscan Command-line scanner at /usr/local/vscanx.

Core Scanner

The Core Scanner utilizes the latest virus-scanning engine to provide functionality for the Active Scanner, the Background Scanner, and the Mounted Volumes Scanner. This scanner provides queuing for scan tasks and powerful scanning tools to operate the individual scanners. The Core Scanner is running by default.

HealthCheck

HealthCheck ensures your system is protected and any outage is minimized by monitoring the operation of all other scanners and restarting them if they fail.

HealthCheck monitors the Active Scanner, Background Scanner, Mounted Volumes Scanner, Core Scanner, and eUpdate components. It keeps track of current preferences and the exclusion list and continues them when restarting a scanner. If any of the components have quit, HealthCheck restarts the scanner without any user intervention. HealthCheck has no user interface; it is an internal component to the anti-virus system.

VirexReporter

The VirexReporter reports infected files found by scanners. The VirexReporter provides tracking and reporting to the anti-virus scanning so you can see where threats to your system may be coming from.

VirexReporter automatically launches when an infected file is found. When an infection is found by the Core Scanner, a window appears with a list of the items found by the Core Scanner and the action taken.

Virex Schedule Editor

The Virex Schedule Editor enables you to schedule automated scans and updates to virus definition (DAT) files and software components that are available online.

You can schedule scans and updates through the Virex Schedule Editor on the console. Automated scans and updates can be set on a daily, weekly, or monthly basis. To access the Schedule Editor, select **Scheduled Task** under **View** in the Virex console menu.

eUpdate

eUpdate allows you to update DAT files and the virus-scanning engine. eUpdate keeps your anti-virus software continuously updated with new information on viruses and scanning capabilities.

eUpdate automatically checks for new updates when there is an Internet connection and launches the console when one is available. You can configure eUpdate to check for updates on your own schedule through the Virex Schedule Editor. To initiate an eUpdate, click on the **eUpdate** tab on the console and then the **Start** button. This support is provided through HTTP or FTP.

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 Serif	All words from the user interface, including options, menus, buttons, and dialog box names. Example: Type the **User** name and **Password** of the desired account.

`Courier`	The path of a folder or program; a web address (URL); text that represents something the user types exactly (for example, a command at the system prompt).
	Examples:
	The default location for the program is:
	`C:\Program Files\McAfee\EPO\3.5.0`
	Visit the McAfee web site at:
	`http://www.mcafee.com`
	Run this command on the client computer:
	`C:\SETUP.EXE`

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.
<TERM>	Angle brackets enclose a generic term. Example: In the console tree under **ePolicy Orchestrator**, right-click <SERVER>.
	**Note:** Supplemental information; for example, an alternate method of executing the same command.
	**Tip:** Suggestions for best practices and recommendations from McAfee for threat prevention, performance and efficiency.
	**Caution:** Important advice to protect your computer system, enterprise, software installation, or data.
	**Warning:** Important advice to protect a user from bodily harm when interacting with a hardware product.
	**New:** New or redesigned feature or option of this release of the product.

Resources

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

Refer to these sections for additional resources:

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

Getting product information

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

Product Guide — Product introduction and features, detailed instructions for configuring the software, information on deployment, recurring tasks, and operating procedures.

- *Virex 7.6 Product Guide*

Help — High-level and detailed information accessed from the software application: Help menu and/or Help button for page-level help; right-click option for *What's This?* help.

Configuration Guide++ — *For use with ePolicy Orchestrator®*. See *Virex Configuration guide* (*for use with ePolicy Orchestrator*). This guide is available in the ePolicy Orchestrator Server package. This guide introduces ePolicy Orchestrator manageability features for Virex, and provides detailed instructions for installing, configuring and managing Virex in an enterprise environment.

Non Windows Agent[1] ReadMe++ — *See Non Windows Agent ReadMe* file for Macintosh. This ReadMe describes the agent features, lists any known behavior or other issues with the product release, and describes the ePolicy Orchestrator Agent installation process.

1 Non Windows Agent is also known as ePolicy Orchestrator Agent.

Release Notes^ — *ReadMe*. Product information, resolved issues, any known issues, and last-minute additions or changes to the product or its documentation.

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

License — The McAfee License Agreement booklet that includes all of the license types you can purchase for your product. The License Agreement sets forth general terms and conditions for the use of the licensed product.

---

* A printed manual that accompanies the product CD. Note: Some language manuals may be available only as a .PDF file.

^ Text files included with the software application and on the product CD.

++ You will be able to use ePolicy Orchestrator related functionality only if you have ePolicy Orchestrator server installed and configured to manage Virex 7.6. The use of ePolicy Orchestrator is optional. You can use all the functionality of Virex 7.6 as a standalone product.

Links from within the product

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

- Online help
- Virus Information Library
- ReadMe
- Product Guide
- License

Online Help

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

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

Virus Information Library

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

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

To access the Virus Information Library:

1 Open the Virex product interface.

2 Select **Virus Information Library** from the **Help** menu.

ReadMe

Use the **ReadMe** link to access the ReadMe file of Virex 7.6.

Product Guide

Use the **Product Guide** link to access the **Virex 7.6 Product Guide** in PDF (Portable Document Format).

License

Use the **License** link to access the **McAfee Software License Agreement**.

Product services

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

- Beta program
- HotFixes and Patches
- Product "end-of-life" support

Beta program

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

To find out more, visit:

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

HotFixes and Patches

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

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

Product "end-of-life" support

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

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

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

Contact information

Technical Support

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

McAfee Beta Program

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

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

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

Download Site

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

Training

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

Customer Service

E-mail	https://secure.nai.com/us/forms/support/request_form.asp
Web	http://www.mcafeesecurity.com/us/index.asp
	http://www.mcafeesecurity.com/us/support/default.asp
US, Canada, and Latin America toll-free:	**+1-888-VIRUS NO** or **+1-888-847-8766**
	Monday – Friday, 8 a.m. – 8 p.m., Central Time

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

* Logon credentials required.

2 Installing Virex 7.6

This chapter provides you with information you require to install Virex 7.6 software. This chapter also provides information on:

- System requirements for Virex.
- ePolicy Orchestrator requirements for Virex.
- Installing Virex.
- How to test if your Virex installation is working properly.
- How to uninstall Virex.

System requirements

Virex installs and runs on any Apple computer that meets these requirements:

- Apple Macintosh OS X (10.2.6 or later) operating system.
- 266 MHZ Power PC G3 (or later) with 128 MB RAM.
- 40 MB of free disk space.
- Virex 7.6 requires the BSD subsystem to be installed in order to function correctly. The BSD subsystem is installed by default as part of Mac OS X, but you can choose not to install it. If you have installed Mac OS X without the BSD subsystem, insert the Mac OS X CD and install the BSD subsystem before continuing.

This product does not use Classic. The Virex 7.6 Installer installs the Virex 7.6 software in the Applications folder of your computer. For Virex known issues, refer to the ReadMe in the **Help** menu.

The operating system must be installed and running correctly before you install the Virex software.

ePolicy Orchestrator requirements

Virex 7.6 integrates with ePolicy Orchestrator version 3.02 or later.

You will be able to use ePolicy Orchestrator related functionality only if you have ePolicy Orchestrator server installed and configured to manage Virex 7.6. The use of ePolicy Orchestrator is optional and you can use all the functionality of Virex 7.6 as a standalone product.

Installing Virex

The procedures for installing Virex on Mac OS 10.2.X Jaguar differ from installation on Mac OS 10.3.X Panther.

To install Virex on Mac OS 10.2.X Jaguar:

1. Double-click the Virex package icon to start the Installer.
2. Type your user name and system password in the **Authentication** dialog box. You will need administrative privileges to install. Click **OK**.
3. The **Virex Installer** window appears.
4. Follow the on-screen steps to install the software.
5. Read and accept the license agreement. If you do not accept the license agreement, the installation cannot continue.
6. Click **Install** to perform an **Easy Install**.
7. When the Installer finishes it notifies you with a dialog box. Restart your computer after installing Virex. This will ensure that all of the scanners start properly.

To install Virex on Mac OS 10.3.X Panther:

1. Double-click the Virex package icon 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 an **Easy Install**.
5. The **Authentication** dialog box appears.

6 Type your user name and system password. You will need administrative privileges to complete the installation. Click **OK**.

7 When the Installer finishes it notifies you with a dialog box. Restart your computer after installing Virex. This will ensure that all of the scanners start properly.

Virex 7.6 is now located in your computer's applications folder. The ReadMe file is included in the **Help** menu. Refer to this file for known issues, online resources, and other useful information.

By default, the Active Scanner is on while the Background and Mounted Scanners are off. You need to manually configure scanners for functions like checking files for virus-like characteristics. See *Configuring the Scanners* on page 27.

With Virex 7.6 you use the eUpdate feature to connect to a Web location and download new DAT files. To find out more about eUpdate and other Virex features, see *Getting Started*.

Upgrade Installation

1 Double-click the Virex package icon to start the Installer. Follow the on-screen steps to install the software.

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

3 Select the destination volume to install Virex 7.6 software and click **Continue**. The **Easy Install** window appears.

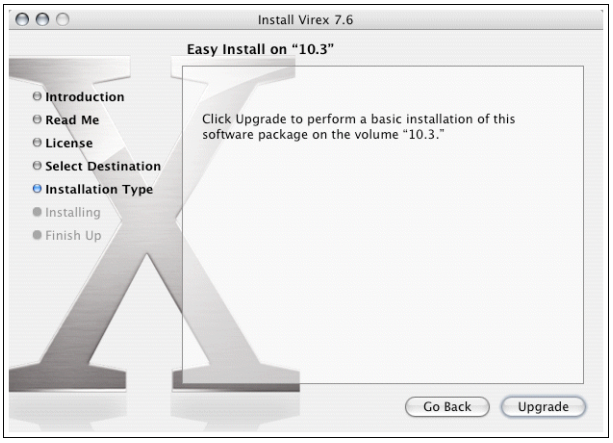


Figure 2-1 Easy Install - Upgrade window

4 Click **Upgrade** to reinstall or upgrade Virex.

5 The **Authentication** dialog box appears.

6 Type your user name and system password. You will need administrative privileges to complete the installation. Click **OK**.

7 When the Installer finishes installing the package it notifies you with a dialog box. Restart your computer after installing Virex. This ensures that all of the scanners start properly.

Testing your installation

You can test Virex by using the 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 web site (http://www.eicar.org). Click **AntiVirus testfile EICAR.COM** on the left side of the screen.

2 Scroll down the page to the download area. Obtain the EICAR test file by clicking **eicar.com**. When Virex scans this file, it will report finding the test file.

This file is not a virus. Delete the file when you have finished testing to avoid alarming unsuspecting users.

If the test is successful, you are now ready to start using the Virex software. The online help system that is part of the application tells you how to scan and clean files, folders and so on, update the "Virus definition (DAT) files" and get report information. To get online help, either select **Virex Help** from the **Help** menu or search the Mac Help Center.

Uninstalling Virex

You can uninstall Virex 7.6 by using the uninstall command on your installation CD.

To uninstall Virex:

1 Open the Virex 7.6 CD and choose one of the following options:

- Click **Virex Uninstall.command** icon.
- Drag **Virex Uninstall.command** icon and drop it in the Terminal window.

The Terminal window prompts you for the system password.

2 Type your system password.

Your system password will not be displayed in the Terminal window.

3 **Enter**.

4 When the uninstall command completes, the **Terminal** window shows:

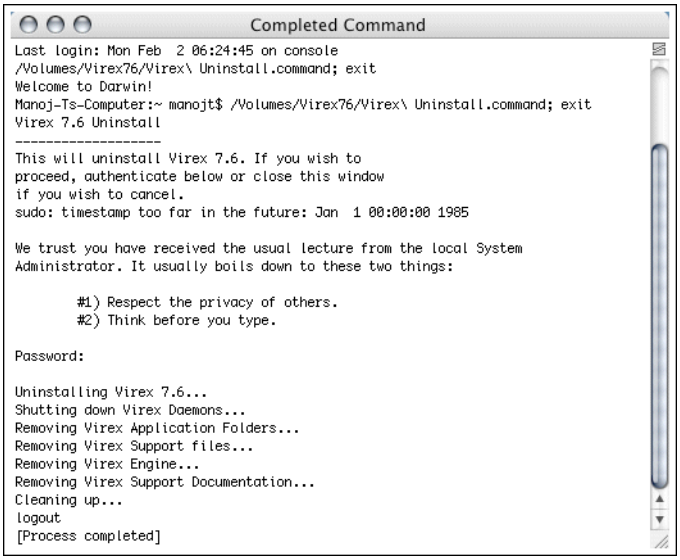


Figure 2-2 Terminal window

3 Getting Started

This chapter introduces Virex 7.6, how it helps keep your computer free of viruses and includes the following topics:

Using the Virex 7.6 Console

The Virex console allows you to use and configure on-demand scanning and set scanning preferences for Active Scanning, Background Scanning, and Mounted Volumes Scanning. The console connects you to the McAFee Virus Information Library, performs eUpdates, and prints and saves virus scan reports. The Virex console also contains a drag-and-drop pane for on-demand scanning and a report panel showing current scan reports.

With the drag-and-drop feature, you can initiate a scan at any time by dragging the file(s) into the center pane of the console. When you drop a file into the drag-and-drop pane, click on the **Start** button to initiate a scan. If you add another file after the scan has completed, the new file will replace the first scan.

The Virex Console

The Virex 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.

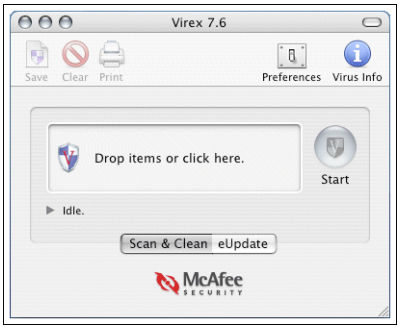


Figure 3-1 The Virex console

Tool bar

The tool bar 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.

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

- Set preferences for the Active Scanner, Background Scanner, On-Demand Scanner, and Mounted Volumes Scanner.
- Toggle Active, Background, and Mounted Volumes Scanners.
- Set preferences for the action to take if a virus is found.
- Log results to a file.
- Configure eUpdate Server Settings.
- Create an exclusion list.
- Automate virus definitions updates and virus scans.

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

Menu bar

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

Configuring the Scanners

The Active Scanner is on by default while the Background Scanner and Mounted Volumes Scanner are both off by default. Preferences are saved immediately when you select them.

To configure the Active Scanner, Background Scanner, Mounted Volumes Scanner, and On-Demand Scanner:

1 Click **Preferences** on the tool bar.

2 The **Preferences** dialog box appears.

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

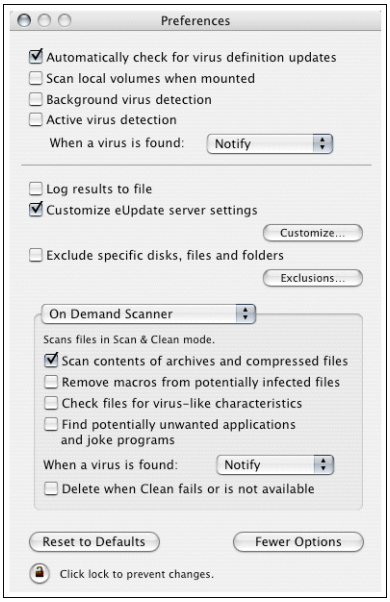


Figure 3-2 The Preferences dialog box

4 Select the scanner you want to configure from the center drop-down menu.

5 Select your scanning preferences:

Table 3-1 Preferences

Simple Preferences	
Automatically check for virus definition updates	Enables / disables automatic eUpdates.
Scan local volumes when mounted	Enables / disables the Mounted Volumes Scanner scanner.
Background virus detection	Enables / disables the Background Scanner.
Active virus detection	Enables / disables the Active Scanner.
When a virus is found: ■ Clean ■ Delete ■ Notify	Selects the primary action of the four scanners. This selection will be unavailable if one of the scanners is configured differently from the others.
Settings for Advanced Global Preferences	
Log results to file	Enables / disables logging results to a file.
Customize eUpdate Server Settings	Manages your update server with user name and password.
Customize...	Displays a dialog box for you to customize the HTTP or FTP settings for eUpdate.
Exclude specific disks, files and folders	Configures your scanning exclusions. The exclusions are stored as a list in a text file called VShieldExclude.txt. If this is not selected then you will not have any exclusions set.
Exclusions…	Opens the exclusion file in TextEdit.
Advanced Preference Settings for each scanner	
Scan contents of archives and compressed files	Sets the selected scanner to scan into archives and other compressed files. On by default for Background and On-Demand Scanners.
Remove macros from potentially infected files	If an infected file is detected then all macros from that file will be removed as part of the clean.
Check files for virus-like characteristics	Enables / disables heuristics, which scans for files that show characteristics of viruses or worms and may contain unknown infections. On by default for Background Scanner.
Find potentially unwanted applications and joke programs	Enables / disables the scanner to check for unwanted programs or joke programs.
Delete when Clean fails or is not available	Selects the secondary action for the selected scanner. This is only available when the primary action is Clean.

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

7 Click **Close** in the upper left-hand corner.

Scanner preferences are global settings that apply to all users.

The table below illustrates the preferences you would select to ensure protection for the common tasks.

Common Tasks and Preferences	
Scanning CD files before opening them	Select in Simple Preferences: ■ **Scan local volumes when mounted**
Detecting viruses when downloading files from the Internet to the hard drive	Select in Simple Preferences: ■ **Active virus detection** Select in Active Scanner Preferences: ■ **Check files for virus-like characteristics** ■ **Find potentially unwanted applications and joke programs** ■ **Scan contents of archives and compressed files**

Creating an exclusion list

The user-configurable exclusion list prevents the scanners from scanning specific files, directories, or volumes. The exclusion list is shared with the Active Scanner, Background Scanner and the Mounted Volumes Scanner.

To create an exclusion list:

1 Click **Preferences** on the tool bar. The **Preferences** dialog box appears.

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

3 Click **Exclude specific disks, files and folders**.

4 Click **Exclusions**. The **VShieldExclude.txt** file opens.

5 Type the full path name of each file, directory, and volume you want to exclude from the scan, for example:

```
/Users/herb/Documents/Recipes/cookbook.doc

/Users/herb/Documents/Music/
```

6 Close 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 Virex dock icon, the Virex icon in the Finder, or into the drag-and-drop pane in the console.
- Through the file open dialog box.

You can select multiple files, directories, or volumes and the results are summarized in the Virex Reporting Window.

To perform On-demand Scanning:

1. Open the Virex main 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 Virex 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 **Virex Reporting Window**. The **Virex Reporting Window** is hidden by default.

A scan report appears in the **Virex Reporting Window**. The report notes the time of the scan, 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.

Updating virus definitions (DAT files)

eUpdate automatically connects weekly by default to the eUpdate Server via your Internet connection, and checks for new "Virus definitions (DAT) files". You can schedule additional eUpdates through the Virex Schedule Editor or you can manually initiate an eUpdate at any time.

Why do you need to update?

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

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.

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, Virex will automatically attempt to download and install the update.

If you do not wish to install the update at this time, you may cancel the process by clicking the **Cancel** button. After canceling an eUpdate, the Virex Console will automatically switch to the eUpdate pane every time it launches to remind you to update. If a week lapses without updating, Virex will automatically download the update. This ensures your system is up-to-date at all times.

To initiate an unscheduled eUpdate:

1. Open the Virex 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.

Using the Virex Schedule Editor

The Virex Schedule Editor allows you to schedule on-demand scans and eUpdates.

Scheduling Scans

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

To schedule a scan:

1 Select **Scheduled Task** from the **View** menu on the console. The **Virex Schedule Editor** appears.

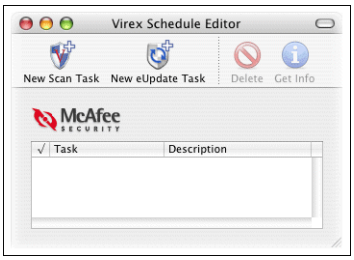


Figure 3-3 Virex Schedule Editor

2 Click **New Scan Task**. 

The **New Scan Task** dialog box appears.

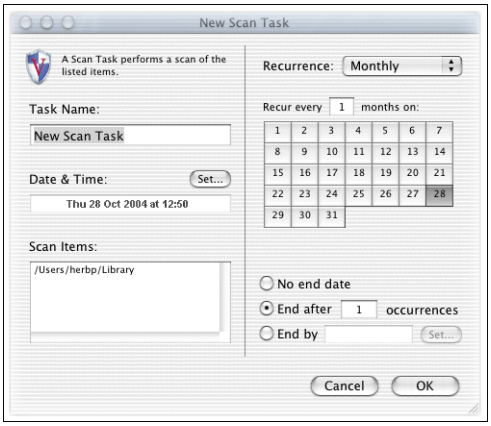


Figure 3-4 The New Scan Task dialog box

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

4 Use the **Set** button to specify the **Date & Time** of the scheduled scan. **UTC** is Universal Time Coordinated (Greenwich Mean Time).

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 **Daily**, **Weekly**, **Monthly,** or **Never**:

- **Daily**: Type the sequence of days that the scan will perform.
- **Weekly**: Select the day(s) of the week on which you want this to occur.
- **Monthly**: Select the day(s) of the month 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 Virex Schedule Editor. To enable or disable scheduled tasks, select the check box next to the task item.

If the computer is turned off during a scheduled task, Virex 7.6 will miss the task when the computer is turned back on.

Scheduling eUpdates

The Virex Schedule Editor allows you to schedule repetitive updates to your system's virus definition (DAT) files and the virus-scanning engine. This support is provided through HTTP or 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 Select **Scheduled Task** from **View** on the console.

The **Virex Schedule Editor** appears.

2 Click **New eUpdate Task**. 

The **New eUpdate Task** window appears.

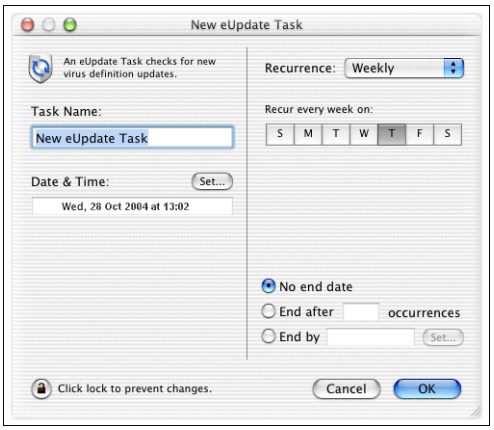


Figure 3-5 The New eUpdate Task dialog box

3 Click the lock in the lower left-hand corner of the pane so that you can modify the automatic eUpdating.

The **Authentication** dialog box appears.

4 Type an administrator user name and password. Click **OK**.

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

6 Use the **Set** button to specify a **Date & Time** for the update to occur.

7 Select **Recurrence**. Choose **Daily**, **Weekly**, **Monthly,** or **Never**:

- **Daily**: Type the sequence of days you want the eUpdate to connect.
- **Weekly**: Select the day(s) of the week on which you want this 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 scan to reoccur.

8 Select an end date.

9 Click the **Lock to prevent changes** to the schedule. Click **OK**.

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

All scheduled eUpdate tasks apply to all users in OS X. The eUpdate schedule includes a small period of randomization so that all Virex products do not update from the server at exactly the same time. Therefore, your eUpdates will occur at slightly different times, just before or after the time that you set.

Using VirexReporter

VirexReporter reports infected files. When the Core Scanner finds an infected file, the **Virus Alert** window appears with a list of the infected items and action taken.

Figure 3-6 The VirexReporter Virus Alert

To use the VirexReporter:

1 In the **Virus Alert** window, click the arrow beside **Show Details**.

The VirexReporter gives a list of infected items and the action taken by Virex.

2 Do one of the following:

- Select **Move To Trash** to move the infected file(s) to the trash.
- Select **Clean** to clear the file of the suspected virus.
- Select **Ignore** to leave the file as it is.

4 Troubleshooting

This chapter provides solutions to situations that you might encounter when installing or using Virex 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 Virex onto: it must be Mac OS X 10.2.6 or later. Another reason might be that an existing anti-virus program had been detected during installation, and must be removed for Virex to be installed successfully. Virex 7.6 requires the BSD subsystem to be installed in order to function correctly.

I just installed Virex onto my computer. Why is the scanner not working?
If the product does not appear to be scanning after installation, restart your computer to ensure that all scanners are performing.

What Virex files are installed and where?
Virex 7.6 is installed in /Applications, and Virex Schedule Editor is installed in /Applications/Utilities. Uvscan, VShield Status, DAT files, and daemons can be found at /usr/local/vscanx.

Scanning

Does Virex automatically scans files once they are created?

The Active Scanner will scan files as they are saved to the hard drive.

Why has Virex skipped scanning certain files?

Check to make sure they are not on the exclusion list. Virex will also not scan archives and compressed files unless configured to do so.

When Virex was scanning a file, I dragged & 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 Virex 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.

What are the advantages of turning on the Background Scanner?

The Background Scanner constantly scans your system for infected files. It is a low-resource process that increases your protection against viruses without affecting the performance of your computer.

Viruses and detection

Can Virex detect both Macintosh and Windows viruses?

Virex detects all known Macintosh and Windows viruses and worms.

Why is the Mounted Volumes Scanner not working?

Ensure that you enable the **Scan local volumes when mounted** in the **Preferences** dialog box.

Why has Virex stopped displaying items that are scanned?

Virex will only show the first 200,000 items that are scanned.

Why is the content in my log file cut off?

The size of a log file cannot exceed 120kb. When a log file does exceed 120kb, the file is reduced to 100kb. 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 **View Log** under **File** on the main menu.

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.

When I close the Virex program, is it still running in the background, or is the program shut down?

Once installed all scanners are loaded and running in the background. The Active Scanner is on by default, but the Background and Mounted Volumes Scanners are off unless turned on in **Preferences**.

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 Virex** from the Virex 7.6 menu on the menu bar of the Virex 7.6 application. The dates of the DAT versions only reflect when the DAT files were created.

How often are DAT files updated automatically in Virex?

eUpdate checks for new updates on its own every week via the Internet. Virex 7.6 does not offer daily updates. You can manually download daily updates from the McAfee Virus Information Library web site.

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 Virex, can I view the processes running?

In Mac OS 10.3.X Panther, use the Activity Monitor to view processes. In Mac OS 10.2.X Jaguar, use the Process Viewer. The running processes are VShield (Active Scanner), VShieldBKgd (Background Scanner), VShieldCore (Core Scanner), VShieldCheck (Health Check), VShieldMount (Mounted Volumes Scanner), and VShieldUpdate (eUpdate).

How do I configure Virex to scan ONLY when and what I want it to?

Click on Preferences in the Virex Console. Deselect the checkbox beside **Scan local volumes when mounted**, **Background virus detection**, and **Active virus detection**.

Disabling Virex leaves your computer vulnerable to viruses. Scanner preferences are global settings that apply to all users setup on your computer.

Can I manually download virus definitions without using eUpdate?

On the Tool bar of the Virex Console, click the **Virus Info** button. This launches your default browser and directs you to the McAfee Virus Information Library. Click on **Downloads** on the left hand side of the screen to download DAT files.

How do I customize eUpdate Server Settings?

If you need information about how to change your eUpdate Server Settings, call Customer Service toll free at +1-888-847-8766 (US, Canada, and Latin America).

Where can I find the log files?

The following is a list of log files.

Table 4-1 - Log files

Log file	Description	Where can I find them
virex.log	This log file contains Virex related entries. You can also access this log file from the Virex Help menu.	/var/log/virex.log
VirexEPOLog.log	This log file contains entries made by VShieldEpoInterface daemon that communicates between ePolicy Orchestrator Agent and Virex.	/var/log/VirexEPOLog.log
log	This log file contains ePolicy Orchestrator Agent related entries.	/Library/NETAepoagt/scratch/etc/log

Error messages

Error messages - Virex application

The following is a list of possible error messages you can see while running Virex application and the possible reasons for their occurrence.

Table 4-2 Error messages - Virex application

Serial No.	Message	Possible Reason
1	The Virex Application can not be launched because the Health Check component is not responding. Please restart or re-install.	If you just installed Virex, you need to restart your computer to allow the daemons to load. If you have not just installed Virex, the Health Check daemon may have become corrupt and requires that you re-install.
2	Initialization of virex engine failed (error x).	The engine or DAT files have become corrupted or have been moved/deleted. Please re-install.
3	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.
4	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.
5	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.
6	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.
7	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 currently busy. Wait a few minutes then restart the eUpdate process and try again.
8	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 Virex has become outdated. It is recommended that you upgrade to the newest version of Virex to ensure the best virus protection possible.
9	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 Virex has become outdated. It is recommended that you upgrade to the newest version of Virex to ensure the best virus protection possible.

Table 4-2 Error messages - Virex application

Serial No.	Message	Possible Reason
10	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 Virex has become outdated. It is strongly recommended that you upgrade to the newest version of Virex to ensure the best virus protection possible.
11	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 Virex has become outdated. It is recommended that you eUpdate as soon as possible to ensure the best virus protection possible.
12	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 Virex has become outdated. It is recommended that you eUpdate as soon as possible to ensure the best virus protection possible.
13	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 Virex has become outdated. It is strongly recommended that you eUpdate as soon as possible to ensure the best virus protection possible.

Error messages - virex.log

The following is a list of possible error messages you can see in the virex.log and the possible reasons for their occurrence.

Table 4-3 -Error Messages - virex.log

Error No.	Message	Possible Reason
2	VShieldCore reports: [ActiveScanner] AV Engine reports object /Library/Caches/com.apple.LaunchServices.LocalCache.csstore~)[accessed by process 449] could not be scanned due to error 2.	Virex 7.6 is denied access to the file by the Mac OS X operating system, possibly because the file is being modified or is in use by another application. Try quitting the open applications before you rerun the scan.
10	VShieldCore reports: [ActiveScanner] AV Engine reports object (/dev/null) [accessed by process 438] could not be scanned due to error 10.	A special file can be critical files or objects of the Mac OS system. Quitting applications and rescanning does not scan such items. It is expected behavior that Virex 7.6 reports such errors.

Glossary

Active Scanner
A feature of Virex that scans files when they are written to your hard drive. It starts when your computer starts and runs until the computer is shut down.

Background Scanner
A Virex feature that continually scans all the files on your computer.

Core Scanner
This scanner provides queuing for scan tasks and powerful scanning tools to operate the individual scanners.

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.

DMG files
DMG files are self-mounting disk images.

EICAR
European Institute of Computer Anti-Virus Research. They have developed a string of characters that can be used to test the proper installation and operation of anti-virus software.

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

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.

HealthCheck
HealthCheck is a Virex feature that keeps track of current preferences and the exclusion list and continues them when restarting a scanner. If any of the components quit, HealthCheck restarts the scanner automatically.

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.

Incremental DAT files
New virus definitions that supplement the virus definitions currently installed. Allows the update utility to download only the newest DAT files rather than the entire DAT file set.

Joke program
A non-replicating program that may alarm or annoy an end user, but does not do any actual harm to files or data.

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

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.

Mounted Volumes
Mounted drives are sometimes considered mounted volumes. An example of a mounting process is when one inserts a CD into a drive. In this case, a volume (CD) gets mounted on the desktop.

Mounted Volumes Scanner
This scanner initiates a scan of a volume such as a CD or camera when you mount it to your system. This feature is only available with locally inserted or ejectable media, such as Zip drives, CD, DVD, or OS X.

McAfee Virus Information Library
This web site (http://vil.nai.com/vil/default.asp) has detailed information about the origins of viruses, how they infect your computer, and how to remove them. The site also discusses e-mail hoaxes.

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.

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.

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

Uvscan Command-line Scanner
This scanner allows advanced scanners to access the on-demand scanner from the terminal shell.

Virex Console
This is the most common user interface for Virex. This console allows you to schedule tasks, configure the scanners, and start eUpdates.

Virex Schedule Editor
This Virex feature allows you to schedule additional virus definition and software updates.

Virex Reporter
The Reporter shows you the results of the anti-viral scanning in the form of reports.

Virus
A program 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.

Index