VirusScan® for Mac

Version 8.5

McAfee®
System Protection

Proven security

McAfee®

Contents

1   Introducing VirusScan for Mac

What's in this guide?

This guide introduces VirusScan for Mac, 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 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.

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, and USB devices, such as pen drives, iPods and cameras. Advanced heuristic scanning detects previously unknown macro and program viruses.

The HealthCheck feature monitors VirusScan for Mac components to ensure they do not quit, and restarts them if they do, to ensure that your anti-virus protection is always active. You can perform On-Demand scanning and On-Access scanning. 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

- On-Access scanning

- Universal binary support

- Apple Mail scanning

- 5100 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 click the drop items or click the pane 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. You can also 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 on 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 the drop items or click the pane 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 that appends 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.

Uvscan command-line scanner

The Uvscan command-line scanner is a standalone On-Demand scanner for OS X environments. It allows advanced users to access On-Demand scanner functions from a terminal shell. This guide does not include information on how to use Uvscan. However, some information is available from Uvscan's *man* pages. You can access the Uvscan command-line scanner at **/usr/local/vscanx**.

HealthCheck

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

HealthCheck keeps track of current preference and the exclusion list, and continues these when restarting a scanner. If any components quit, HealthCheck restarts the component without any user intervention. HealthCheck has no user interface; it is an internal component of the VirusScan anti-virus software.

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 **Schedule Editor** console. Automated scans and updates can be set on a daily, weekly, or monthly basis. To access the VirusScan Schedule Editor, select **Scheduled Tasks** under **View** in the main menu. You can also open the 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 use the 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 3.5 and 3.6 (patch 2) 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.

> 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. The use of ePolicy Orchestrator is optional and you can use all the functionality of VirusScan as a standalone product.

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

Product Guide — This guide introduces the product, describes its features, and gives details on how to install and configure the software, ongoing operation and maintenance. This guide (*VirusScan Product Guide*) is available in .PDF in the **Documentation** folder of the product package.

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

Configuration Guide — For use with ePolicy Orchestrator®. This guide 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 Configuration Guide - for use with ePolicy Orchestrator* in .PDF) is available in the ePolicy Orchestrator Server package.

Non-Windows Agent Release Notes — See the Non-Windows Agent Release Notes for Macintosh. This file describes the agent features, lists any known behavior or other issues with the product release, and describes the ePolicy Orchestrator Agent installation process.

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 webside 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

VirusScan installs and runs on any of the following Apple computers, running the Apple Macintosh OS X operating system, version 10.4.0 (or later):

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

The computer must have a minimum of 256 MB RAM and 70 MB of free disk space.

> ℹ️ This product does not use the Classic operating system.

ePolicy Orchestrator requirements

VirusScan integrates with ePolicy Orchestrator versions 3.5 and 3.6 (patch 2).

> ℹ️ 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. The use of ePolicy Orchestrator is optional and you can use all the functionality of VirusScan as a standalone product.

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.

> (i) You must have administrative privileges to install this product.

Standard installation

You 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** icon, or 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.

5 The **Authentication** dialog box appears.

6 Type your user name and administrator password and click **OK**.

7 A message notifies you when the installation finishes. Click **OK**.

8 Restart your computer after installing VirusScan. This will ensure that all VirusScan components start properly.

VirusScan is now located in your computer's **Applications** folder.

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. Restart your computer after this message appears. This will ensure that all VirusScan components start properly.

Upgrade installation

VirusScan for Mac version 8.5 software is available as an upgrade from the following McAfee software product:

■ VirusScan for Mactel version 8.0

⚠️ You cannot upgrade earlier versions of Virex software to VirusScan for Mac version 8.5.

If you are upgrading from VirusScan for Mactel version 8.0 and have been using an internal FTP server for obtaining antivirus updates, see *Updating DAT files on page 26* for details on how to configure your FTP server for downloading the required DAT files.

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. Click **AntiVirus testfile** 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**. Scan this downloaded file with VirusScan, it will report finding the EICAR test file.

ℹ️ 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.

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 click **Enter**.

> ℹ️ 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**.

> ℹ️ 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*

■ *Configuring the scanners*

■ *Using the On-Demand scanner*

■ *Using the On-Access scanner*

■ *Updating DAT files*

■ *Using the VirusScan Schedule Editor*

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.
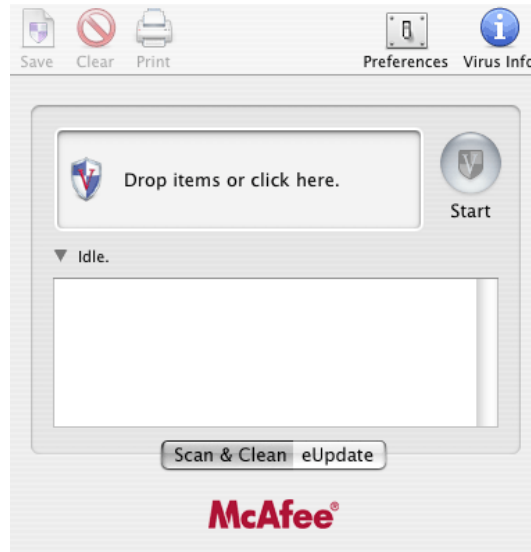
Figure 3-1 VirusScan console

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.

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.

> (i) Scanner preferences are global settings that apply to all users.

The preferences are saved automatically when you select them.

> (i) 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.
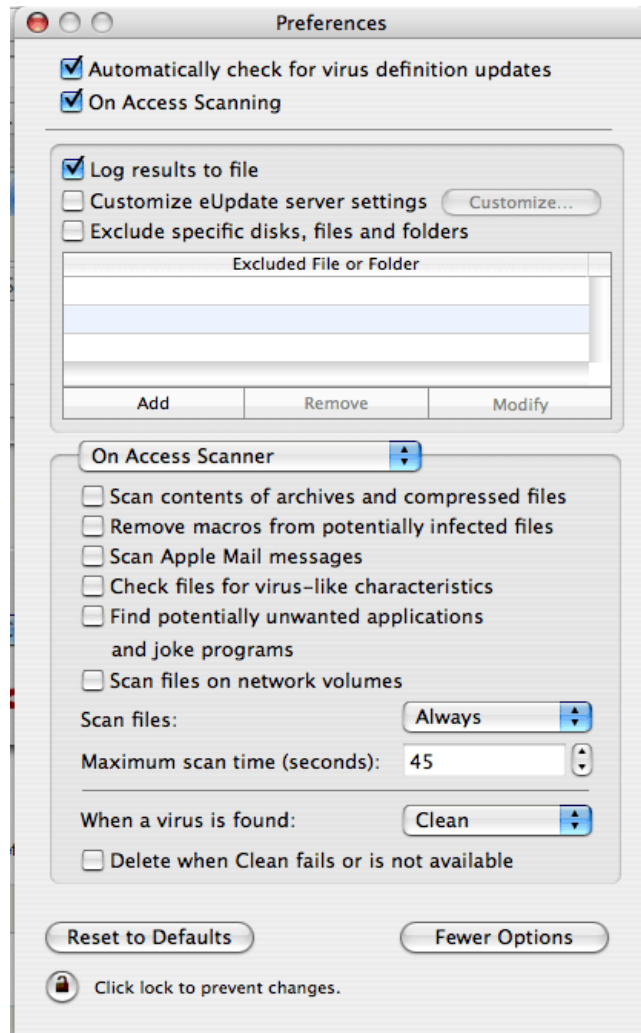
Figure 3-2 General preferences

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 then 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 **Exclude File or Folder** list. Click **Modify**. The **Open** dialog box appears. Select the file or folder to replace the existing exclusion.

3 You can then 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* or *Configuring the On-Access Scanner on page 23* for details.

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 dropdown menu (if not already selected) to display the On-Demand scanning version of this dialog box.

..

Figure 3-3 On-Demand preferences

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.
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.
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 when the primary action is **Clean**.

5 Click the **Lock** icon 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 dropdown menu (if not already selected) to display the On-Access scanning version of this dialog box
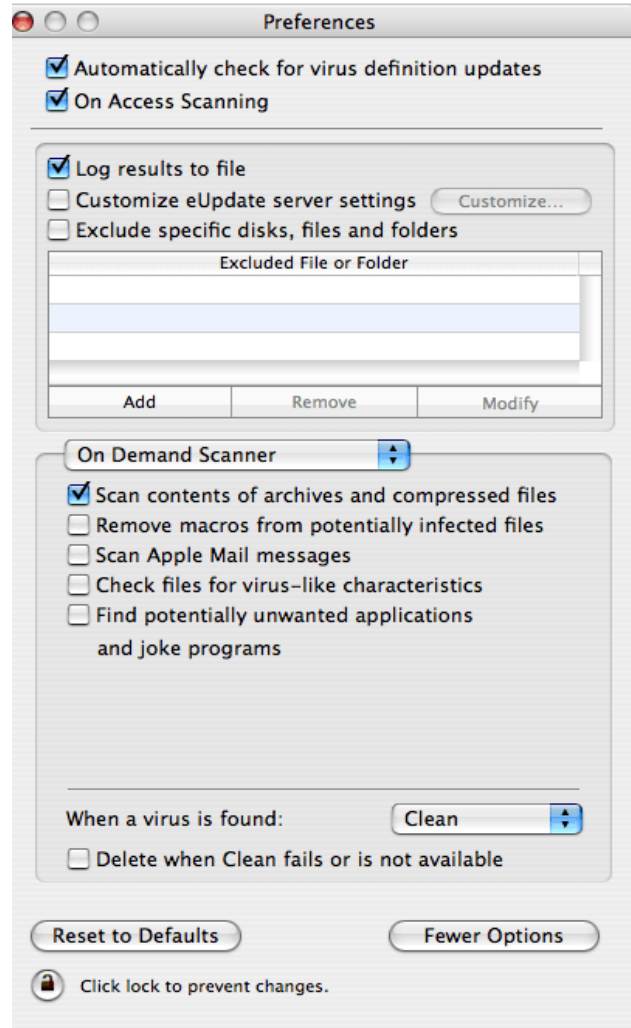
.
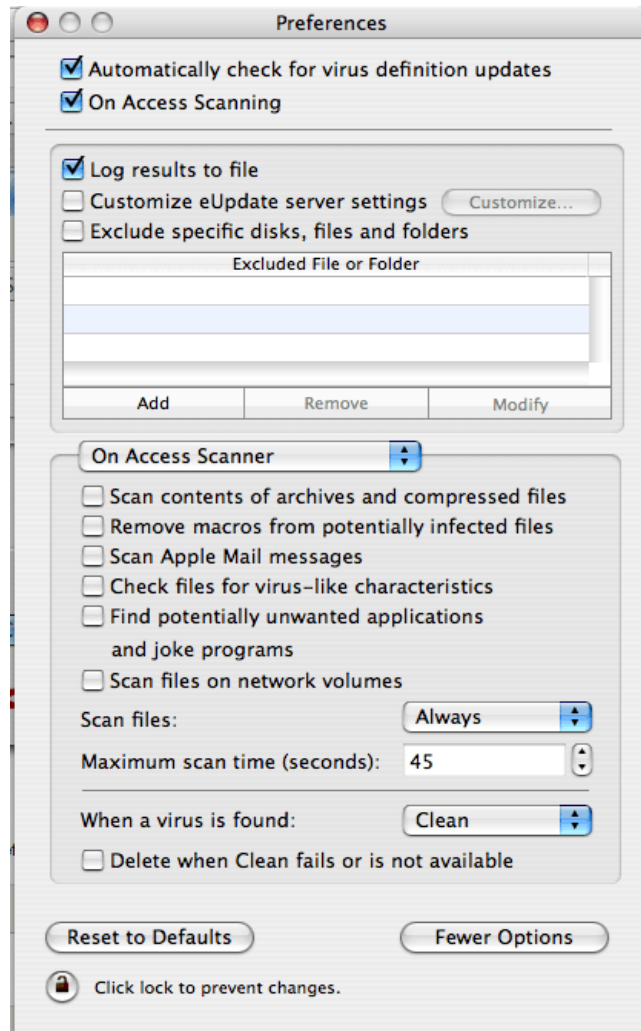
Figure 3-4 On-Access preferences

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.
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.
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.
Scan files on network volumes	Sets the scanner to scan files accessed from network volumes.

Table 3-3 Advanced Preferences for On-Access scanning

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 the **Lock** icon 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 **File Open** 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.

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**.

> ℹ️ 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 (24 hours) 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.

> ⓘ If you are manually configuring an internal FTP eUpdate server, ensure that the URL ends with a slash "**/**" for successful eUpdate.
>
> For example: ftp://ftp.yourcompany.com/virus_updates/

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 periodically download the DAT files from the McAfee FTP server (ftp://ftp.nai.com/pub/antivirus/datfiles/4.x/) onto the internal FTP server you have configured.

To configure the internal FTP server:

1 Download the DAT file from ftp://ftp.nai.com/pub/antivirus/datfiles/4.x/

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

To access the FTP server from Preferences:

1 Open the VirusScan 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.
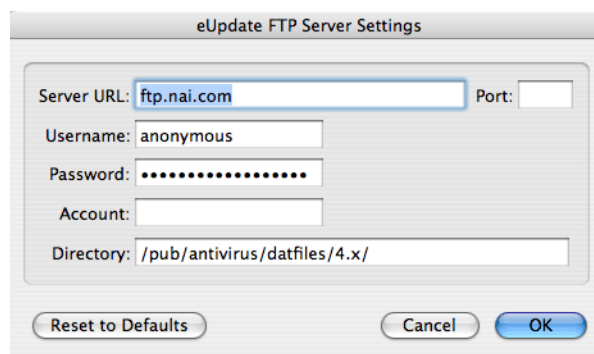

Figure 3-5 Customize eUpdate Server Settings

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 Download **update.ini** and <dat-4825.zip> from the FTP server.

Server URL: ftp://ftp.nai.com

Directory: /pub/antivirus/datfiles/4.x/

2 Copy **update.ini** and <dat-4825.zip> to ftp://<yourcompany.com>/virex_updates/

3 Change the file path to **/virex updates/** in your local copy of **update.ini** so that it refers to the directory in your local server.

For example:

[ZIP]
EngineVersion=0
DATVersion=4825
FileName=dat-4825.zip
FilePath=/virex updates/
FileSize=8056350
Checksum=37EC,968E
MD5=ca8e72e4365a174cbf3c8ef15a7280c6

4 In **VirusScan eUpdate Server Settings**, type the following:

Server URL: ftp://<yourcompany.com>

Directory: /virex_updates/

5 To get the latest version of the engine update file, next check the following entry in the **update.ini** file.

[Engine-MACOSXUB]
EngineVersion=5100
FileName=emub5100.zip
FileSize=xxxxxx
Checksum=xxxxx
MD5=xxxxxxxxxxxxxxxx
FilePath=/pub/antivirus/engine/5.x/

Then download the engine update file, **emub5100.zip** from the directory specified in **FilePath** and copy that file to ftp://<yourcompany.com>/virex_updates/. Finally, change the **FilePath** entry to **/virex updates/** in your local copy of **update.ini** so that it refers to the directory in your local server

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 From the **View** menu, select **Scheduled Tasks**. The **VirusScan Schedule Editor** dialog box appears.
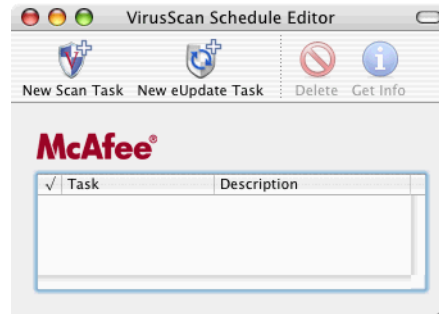
Figure 3-6 VirusScan Schedule Editor

2 Click **New Scan Task**   . An **Untitled** dialog box appears.
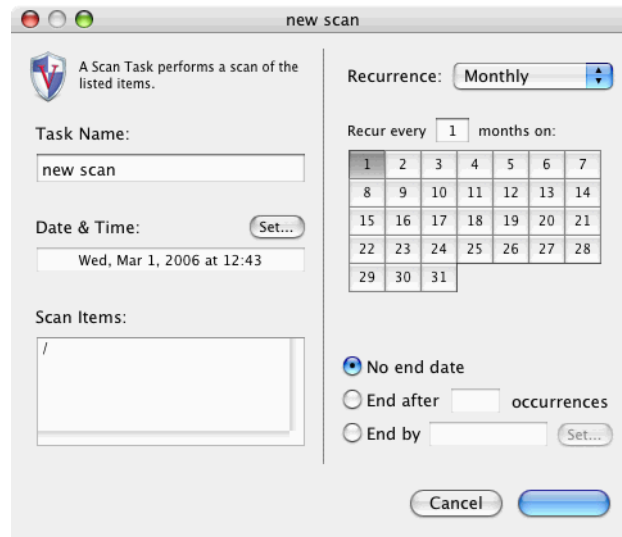
Figure 3-7 New Scan dialog box

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 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 check box next to the task item.

> **i** If the computer is switched off or you have logged out when a task is scheduled to run, VirusScan will skip the task when the computer is turned back on, or you log back in.

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.

> **i** You must have administrative privileges to schedule an update.

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 3-8 New eUpdate dialog box

3 Click the **Lock** icon in the lower left-hand corner of the pane so that you can modify the automatic eUpdating. The **Authentication** dialog box appears.

4 Type your user name and password. Click **OK**.

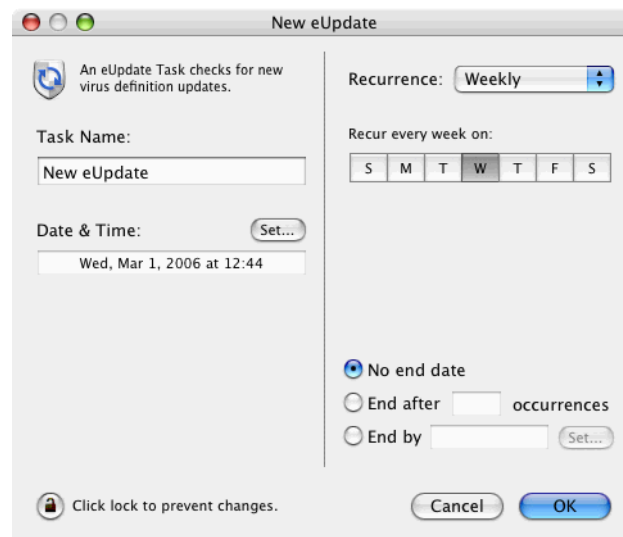**5** Type a name for the task. We recommend using a name that describes the task you are scheduling.

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

7 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.

8 Select an end date.

9 Click the **Lock** icon to prevent change to the schedule 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.

> A scheduled eUpdate task applies to all users of the computer. The eUpdate schedule includes a small period of randomization (within +/- 1 hour) so that all VirusScan products do not update from the server at exactly the same time. Therefore, eUpdates will occur at slightly different time than what you have set.

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 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 10.4.0 or later. 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.

I just installed VirusScan 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 the components are working.

What VirusScan files are installed and where?
VirusScan is installed in **/Applications**, and VirusScan Schedule Editor is installed in **/Applications/Utilities**. Uvscan, DAT files, 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**.

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 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 VirusScan, can I view the processes running?

The processes that are running are VShieldCheck (HealthCheck), and VShieldUpdate (eUpdate), and VShieldCore and VShieldScan (On-Access scanner daemons).

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?

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?

Table 4-1 lists the log files.

Table 4-1 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 4-2 lists all possible error messages you can see while running the VirusScan application, and the possible reasons for their occurrence.

Table 4-2 Error messages - VirusScan application

Serial No.	Message	Possible Reason
1	The VirusScan Application cannot be launched because the Health Check component is not responding. Please restart or re-install.	If you just installed VirusScan, you need to restart your computer to allow the daemons to load. If you have not just installed VirusScan, the Health Check daemon may have become corrupt and requires that you re-install.
2	Initialization of VirusScan 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.

Table 4-2 Error messages - VirusScan application

Serial No.	Message	Possible Reason
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 busy currently. 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 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 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.
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 VirusScan has become outdated. We recommend that you upgrade to the newest version of VirusScan 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 VirusScan has become outdated. We recommend 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 VirusScan has become outdated. We recommend 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 VirusScan has become outdated. We recommend that you eUpdate as soon as possible to ensure the best virus protection possible.

Glossary

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.
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.
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 VirusScan feature that keeps track of current preferences and the exclusion list, and continues them when restarting a component. If any of the components quit, HealthCheck restarts the relevant components 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.
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	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.
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.asp) 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.
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	A scanner which allows advanced users to access the On-Demand scanner from the Terminal shell.
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.
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

700-1451-01

McAfee®

mcafee.com