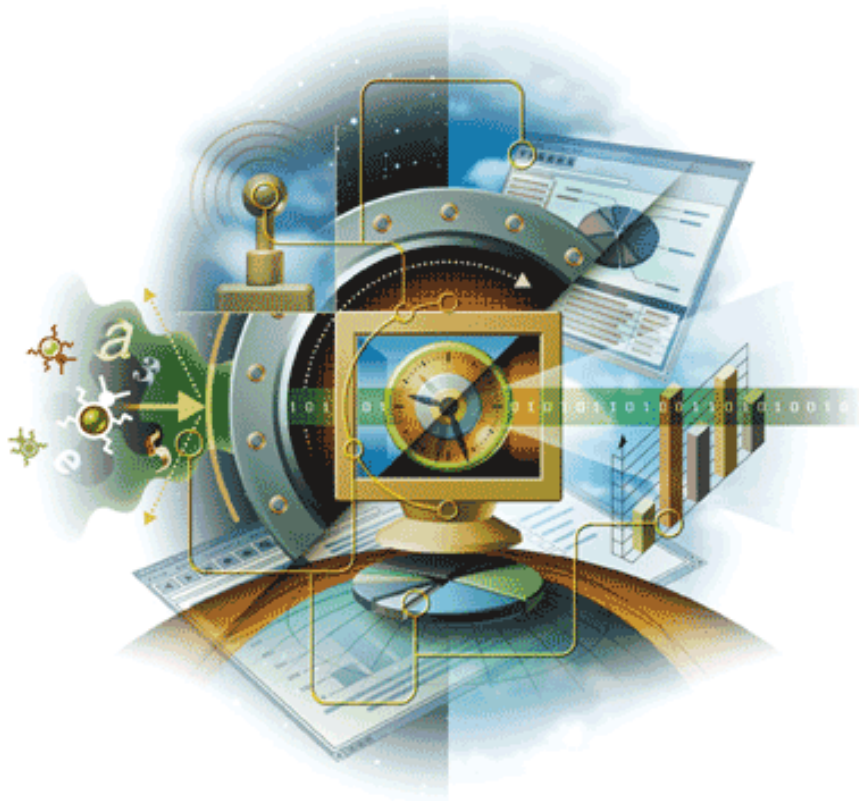


VirusScan[®] Enterprise

version 8.5i



McAfee[®]
Proven Security

Industry-leading intrusion prevention solutions

McAfee[®]

VirusScan[®] Enterprise

version 8.5i

McAfee[®]
Proven Security

Industry-leading intrusion prevention solutions

McAfee[®]

COPYRIGHT

Copyright © 2006 McAfee, Inc. All Rights Reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc., or its suppliers or affiliate companies.

TRADEMARK ATTRIBUTIONS

ACTIVE FIREWALL, ACTIVE SECURITY, ACTIVESECURITY (AND IN KATAKANA), ACTIVESHIELD, CLEAN-UP, DESIGN (STYLIZED E), DESIGN (STYLIZED N), ENTERCEPT, EPOLICY ORCHESTRATOR, FIRST AID, FOUNDSTONE, GROUPSHIELD, GROUPSHIELD (AND IN KATAKANA), INTRUSHIELD, INTRUSION PREVENTION THROUGH INNOVATION, MCAFEE, MCAFEE (AND IN KATAKANA), MCAFEE AND DESIGN, MCAFEE.COM, MCAFEE VIRUSSCAN, NET TOOLS, NET TOOLS (AND IN KATAKANA), NETSCAN, NETSHIELD, NUTS & BOLTS, OIL CHANGE, PRIMESUPPORT, SPAMKILLER, THREATSCAN, TOTAL VIRUS DEFENSE, VIREX, VIRUS FORUM, VIRUSCAN, VIRUSSCAN, VIRUSSCAN (AND IN KATAKANA), WEBCAN, WEBSHIELD, WEBSHIELD (AND IN KATAKANA) are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. The color red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners.

LICENSE INFORMATION

License Agreement

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

Attributions

This product includes or may include:

- Software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).
- Cryptographic software written by Eric A. Young and software written by Tim J. Hudson.
- Some software programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar Free Software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code. The GPL requires that for any software covered under the GPL which is distributed to someone in an executable binary format, that the source code also be made available to those users. For any such software covered under the GPL, the source code is made available on this CD. If any Free Software licenses require that McAfee provide rights to use, copy or modify a software program that are broader than the rights granted in this agreement, then such rights shall take precedence over the rights and restrictions herein.
- Software originally written by Henry Spencer, Copyright 1992, 1993, 1994, 1997 Henry Spencer.
- Software originally written by Robert Nordier, Copyright © 1996-7 Robert Nordier.
- Software written by Douglas W. Sauder.
- Software developed by the Apache Software Foundation (<http://www.apache.org/>). A copy of the license agreement for this software can be found at www.apache.org/licenses/LICENSE-2.0.txt.
- International Components for Unicode ("ICU") Copyright ©1995-2002 International Business Machines Corporation and others.
- Software developed by CrystalClear Software, Inc., Copyright ©2000 CrystalClear Software, Inc.
- FEAD® Optimizer® technology, Copyright Netopsystems AG, Berlin, Germany.
- Outside In® Viewer Technology ©1992-2001 Stellent Chicago, Inc. and/or Outside In® HTML Export, © 2001 Stellent Chicago, Inc.
- Software copyrighted by Thai Open Source Software Center Ltd. and Clark Cooper, © 1998, 1999, 2000.
- Software copyrighted by Expat maintainers.
- Software copyrighted by The Regents of the University of California, © 1996, 1989, 1998-2000.
- Software copyrighted by Gunnar Ritter.
- Software copyrighted by Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A., © 2003.
- Software copyrighted by Gisle Aas, © 1995-2003.
- Software copyrighted by Michael A. Chase, © 1999-2000.
- Software copyrighted by Neil Winton, ©1995-1996.
- Software copyrighted by RSA Data Security, Inc., © 1990-1992.
- Software copyrighted by Sean M. Burke, © 1999, 2000.
- Software copyrighted by Martijn Koster, © 1995.
- Software copyrighted by Brad Appleton, © 1996-1999.
- Software copyrighted by Michael G. Schwern, ©2001.
- Software copyrighted by Graham Barr, © 1998.
- Software copyrighted by Larry Wall and Clark Cooper, © 1998-2000.
- Software copyrighted by Frodo Looijaard, © 1997.
- Software copyrighted by the Python Software Foundation, Copyright © 2001, 2002, 2003. A copy of the license agreement for this software can be found at www.python.org.
- Software copyrighted by Beman Dawes, © 1994-1999, 2002.
- Software written by Andrew Lumsdaine, Lie-Quan Lee, Jeremy G. Siek © 1997-2000 University of Notre Dame.
- Software copyrighted by Simone Bordet & Marco Cravero, © 2002.
- Software copyrighted by Stephen Purcell, © 2001.
- Software developed by the Indiana University Extreme! Lab (<http://www.extreme.indiana.edu/>).
- Software copyrighted by International Business Machines Corporation and others, © 1995-2003.
- Software developed by the University of California, Berkeley and its contributors.
- Software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>).
- Software copyrighted by Kevlin Henney, © 2000-2002.
- Software copyrighted by Peter Dimov and Multi Media Ltd. © 2001, 2002.
- Software copyrighted by David Abrahams, © 2001, 2002. See <http://www.boost.org/libs/bind/bind.html> for documentation.
- Software copyrighted by Steve Cleary, Beman Dawes, Howard Hinnant & John Maddock, © 2000.
- Software copyrighted by Boost.org, © 1999-2002.
- Software copyrighted by Nicolai M. Josuttis, © 1999.
- Software copyrighted by Jeremy Siek, © 1999-2001.
- Software copyrighted by Daryle Walker, © 2001.
- Software copyrighted by Chuck Allison and Jeremy Siek, © 2001, 2002.
- Software copyrighted by Samuel Kremp, © 2001. See <http://www.boost.org> for updates, documentation, and revision history.
- Software copyrighted by Doug Gregor (gregod@cs.rpi.edu), © 2001, 2002.
- Software copyrighted by Cadenza New Zealand Ltd., © 2000.
- Software copyrighted by Jens Maurer, ©2000, 2001.
- Software copyrighted by Jaakko Järvi (jaakko.jarvi@cs.utu.fi), ©1999, 2000.
- Software copyrighted by Ronald Garcia, © 2002.
- Software copyrighted by David Abrahams, Jeremy Siek, and Daryle Walker, ©1999-2001.
- Software copyrighted by Stephen Cleary (shammah@voyager.net), ©2000.
- Software copyrighted by Housemarque Oy <<http://www.housemarque.com>>, © 2001.
- Software copyrighted by Paul Moore, © 1999.
- Software copyrighted by Dr. John Maddock, © 1998-2002.
- Software copyrighted by Greg Colvin and Beman Dawes, © 1998, 1999.
- Software copyrighted by Peter Dimov, © 2001, 2002.
- Software copyrighted by Jeremy Siek and John R. Bandela, © 2001.
- Software copyrighted by Joerg Walter and Mathias Koch, © 2000-2002.
- Software copyrighted by Carnegie Mellon University © 1989, 1991, 1992.
- Software copyrighted by Cambridge Broadband Ltd., © 2001-2003.
- Software copyrighted by Sparta, Inc., © 2003-2004.
- Software copyrighted by Cisco, Inc. and Information Network Center of Beijing University of Posts and Telecommunications, © 2004.
- Software copyrighted by Simon Josefsson, © 2003.
- Software copyrighted by Thomas Jacob, © 2003-2004.
- Software copyrighted by Advanced Software Engineering Limited, © 2004.
- Software copyrighted by Todd C. Miller, © 1998.
- Software copyrighted by The Regents of the University of California, © 1990, 1993, with code derived from software contributed to Berkeley by Chris Torek.

PATENT INFORMATION

Protected by US Patents 6,006,035; 6,029,256; 6,035,423; 6,151,643; 6,230,288; 6,266,811; 6,269,456; 6,457,076; 6,496,875; 6,542,943; 6,594,686; 6,611,925; 6,622,150; 6,668,289; 6,697,950; 6,735,700; 6,748,534; 6,763,403; 6,763,466; 6,775,780; 6,851,058; 6,886,099; 6,898,712; 6,928,555; 6,931,540; 6,938,161; 6,944,775; 6,963,978; 6,968,461; 6,971,023; 6,973,577; 6,973,578.

Contents

1	Introduction	8
	Using this guide	8
	Using VirusScan Enterprise	10
	What to do first	11

Prevention

2	User Interface Security	13
	About user interface security	13
	Configuring user interface security	13
	Display Options tab	14
	Password Options tab	15
	Unlocking and locking the user interface	16
3	Access Protection	17
	About access protection	17
	Configuring access protection	20
	Access Protection tab	21
	Reports tab	28
4	Buffer Overflow Protection	30
	About buffer overflow protection	30
	Configuring buffer overflow protection	31
	Buffer Overflow Protection tab	32
	Reports tab	34
5	Unwanted Programs Policy	36
	About unwanted programs protection	36
	Configuring the unwanted programs policy	37
	Detection tab	38
	User-Defined Detection tab	41

Detection

6	AutoUpdate	44
	About AutoUpdate	44
	Using the AutoUpdate repository list	50
	Importing the repository list	50
	Configuring the repository list	51
	Using AutoUpdate tasks	55
	Creating AutoUpdate tasks	55
	Configuring AutoUpdate tasks	56
	Running AutoUpdate tasks	58

Using mirror tasks	58
Creating mirror tasks	58
Configuring mirror tasks	59
Running mirror tasks	61
Rolling back DAT files	62
7 On-Access Scanner	63
About on-access scanning	63
Configuring on-access scan properties	68
General settings	68
Process settings	75
8 On-Demand Scanner	85
About on-demand scanning	85
Creating on-demand scan tasks	88
Configuring on-demand scan properties	88
Where tab	89
Detection tab	91
Advanced tab	92
Actions tab	93
Unwanted Programs tab	95
Reports tab	96
Running on-demand scans	98
9 E-mail Scanners	99
About e-mail scanning	99
Configuring e-mail scan properties	100
Detection tab	101
Advanced tab	102
Actions tab	103
Alerts tab	105
Unwanted Programs tab	106
Reports tab	108
Notes Scanner Settings tab	110
Running on-demand e-mail scans	111
Microsoft Outlook scans	111
Lotus Notes scans	112

Response

10 Alerts and Notifications	114
About alerts and notifications	114
Configuring alerts	114
Alert Manager Alerts tab	115
Additional Alerting Options tab	116
11 Quarantine Manager Policy	117
About quarantined items	117
Configuring the quarantine policy and managing quarantined items	117
Policy tab	118
Manager tab	119
12 Detection Response	121
Getting information about detections	122
Alerts and notifications	122
Viewing scan results	122
Taking action on detections	126
Access protection detections	127
Buffer overflow detections	127

Unwanted program detections	129
On-access scan detections	129
On-demand scan detections	131
E-mail scan detections	132
Managing quarantined items	133
13 Troubleshooting	135
Utilities for troubleshooting	135
Minimum Escalation Requirements tool	135
Repair Installation utility	136
Frequently asked questions	136
Installation	137
Potentially unwanted program	137
Blocked programs	137
Cookie detections	138
General	138
Error codes for updating	140

Supplemental Information

A User Interface Options	142
About the VirusScan Enterprise interface	142
Accessing the interface	142
VirusScan Console	143
Right-click features	145
System tray icon	146
Start menu	146
Command line	146
B Adding & Excluding Scan Items	147
About scanning items	147
Configuring scanning items	148
Adding file type extensions	148
Specifying user-defined file types	149
Excluding files, folders and drives	150
C Scheduling Tasks	153
About scheduling tasks	153
Configuring the schedule	154
Task tab	154
Schedule tab	155
D Command-line Options	160
About command-line scanning	160
Configuring on-demand scanning options	160
Configuring update task options	162
E Remote Administration	164
F Getting Information	165
Product documentation	165
Other resources	166
Contact information	168
Glossary	169
Index	174

1

Introduction

McAfee VirusScan Enterprise offers easily scalable protection, fast performance, and mobile design to protect your environment from viruses, worms, Trojan horses, as well as potentially unwanted code and programs. It can scan local and network drives, and Microsoft Outlook and Lotus Notes e-mail messages and attachments, then take the actions you configured to protect your environment.

This guide describes how to configure and use VirusScan Enterprise 8.5i.



For information about managing VirusScan Enterprise with McAfee ePolicy Orchestrator® see the *VirusScan Enterprise Configuration Guide for use with ePolicy Orchestrator*.

This section describes:

- [Using this guide.](#)
- [Using VirusScan Enterprise on page 10.](#)
- [What to do first on page 11.](#)

Using this guide

Audience

This information is intended primarily for two audiences:

- Network administrators who are responsible for their company's security program.
- Users who are responsible for updating detection definition (DAT) files on their workstations, or configuring the software's detection options.

Conventions

This guide uses the following conventions:

Bold 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:

`C:\Program Files\McAfee\EPO\3.5.0`

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.

Using VirusScan Enterprise

Use the VirusScan Enterprise software to protect your environment from potential threats. Each component or feature plays a part in defending your computer.

Interfaces:

VirusScan Console	The graphical interface to the product.
Command-line Options	Configure and perform on-demand scanning and update tasks from the command line.

Prevention:

User Interface Security	Restrict users from accessing all or portions of the user interface by setting display and password protection.
Access Protection	Protect your computer from unwanted changes using access protection rules.
Buffer Overflow Protection	Prevent exploited buffer overflows from executing arbitrary code on your computer.
Unwanted Programs Policy	Block potentially unwanted programs such as spyware and adware from accessing your computer.

Detection:

AutoUpdate	Get automatic updates of detection definitions, scanning engine, and product upgrades from the McAfee download website.
On-Access Scanner	Detect potential threats that arrive on disks, from your network, or from various sources on the Internet.
On-Demand Scanner	Detect potential threats using immediate and scheduled scan tasks.
E-mail Scanners	Detect potential threats on Microsoft Outlook or Lotus Notes e-mail clients using on-delivery and on-demand scanning of messages, attachments, and public folders.

Response:

Alerts and Notifications	Receive messages when detections occur.
Quarantine Manager Policy	Manage quarantined items and/or automatically delete quarantined items after a specified length of time.
Detection Response	Get detection information and take action on detections.
Troubleshooting	Troubleshooting utilities, frequently asked questions, and error codes for updating.

Supplemental Information:

User Interface Options	Options for accessing the VirusScan Enterprise interface.
Adding & Excluding Scan Items	Fine-tune the list of file types scanned for each of the scanners.
Scheduling Tasks	Schedule on-demand and update tasks at specific times or intervals.
Command-line Options	Configure VirusScan Enterprise features from the command line.
Remote Administration	Connect to remote computers.
Getting Information	Product documentation, other resources, and contact information.
Glossary	Product and industry term definitions.

What to do first

When installed, VirusScan Enterprise is configured to use the detection definitions that were packaged with the product and provide general security for your environment. We recommend that you get the latest detection definitions and customize the configuration to meet your requirements before you deploy the product to client computers.

Take these actions immediately after installing the product:

- 1 Set user interface security.** Configure the display and password options to prevent users from accessing specific components or the entire VirusScan Enterprise user interface. See [User Interface Security on page 13](#).
- 2 Update detection definitions.** Perform an **Update Now** task to ensure that you have the most recent detection definitions. See [AutoUpdate on page 44](#).
- 3 Prevent intrusions.** Configure these features to prevent potential threats from accessing your computers:
 - [Access Protection on page 17](#). Configure access protection rules to prevent unwanted changes to your computer and enable the option to prevent McAfee processes from being terminated.
 - [Buffer Overflow Protection on page 30](#). Enable buffer overflow detection and specify exclusions.
 - [Unwanted Programs Policy on page 36](#). Configure the policy that the on-access, on-demand, and e-mail scanners use to detect potentially unwanted programs. Select categories of unwanted program categories to detect from a pre-defined list, then define additional programs to detect or exclude.
- 4 Detect intrusions.** Configure these features to detect potential threats on your computers, then notify you and take action when detections occur:
 - [AutoUpdate on page 44](#). Configure update tasks to get the most current detection definitions, scanning engine and product upgrades.
 - [On-Access Scanner on page 63](#). Configure the scanner to detect and take action on potential threats as they are accessed in your environment. Enable scanning of unwanted programs.
 - [On-Demand Scanner on page 85](#). Configure scan tasks to detect and take action on potential threats in your environment. Enable scanning of unwanted programs.
 - [E-mail Scanners on page 99](#). Configure on-delivery and on-demand scanning of Microsoft Outlook and Lotus Notes e-mail clients. Enable scanning of unwanted programs.
- 5 Detection notification and quarantine management.** Configure these features to alert you when detections occur and manage quarantined items:
 - [Alerts and Notifications on page 114](#). Configure how and when you receive detection notifications and alerts.
 - [Quarantine Manager Policy on page 117](#). Configure the number of days to keep quarantined items before automatically deleting them.



SECTION 1

Prevention

Develop an effective strategy to stop intrusions before they gain access to your environment. Your strategy should include these actions:

- Define your security needs to ensure that all of your data sources are protected.
- Configure the software to secure the user interface and protect your environment from access violations, buffer overflows, and potentially unwanted programs.

Chapter 2, User Interface Security

Chapter 3, Access Protection

Chapter 4, Buffer Overflow Protection

Chapter 5, Unwanted Programs Policy

2

User Interface Security

This section describes:

- [About user interface security.](#)
- [Configuring user interface security.](#)
- [Unlocking and locking the user interface on page 16.](#)

About user interface security

Setting security for the interface on client computers is an important part of protecting your environment. As an administrator, you can control the access users have to the VirusScan Enterprise interface. Specify a password to prevent users from accessing or changing selected features. You can also lock and unlock the user interface as necessary.

Configuring user interface security

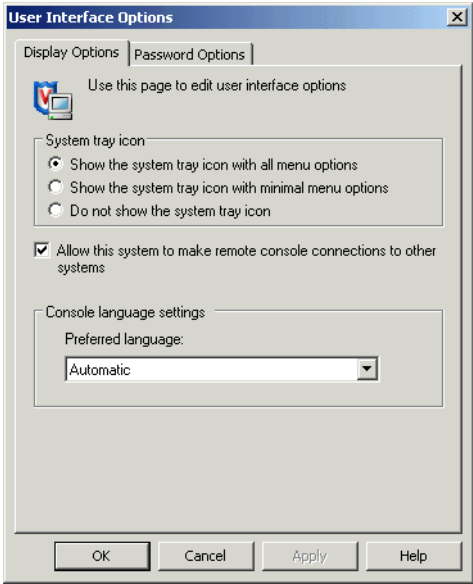
From the Tools menu, select User Interface Options.

Tab or Button	Options or Actions
Display Options tab	■ Specify which system tray icon options users can view. ■ Allow connections to remote computers. ■ Configure the console language.
Password Options tab	■ Specify password security for the entire system or selected items.

Display Options tab

Determine which system tray options users can access.

Figure 2-1 User Interface Options — Display Options tab

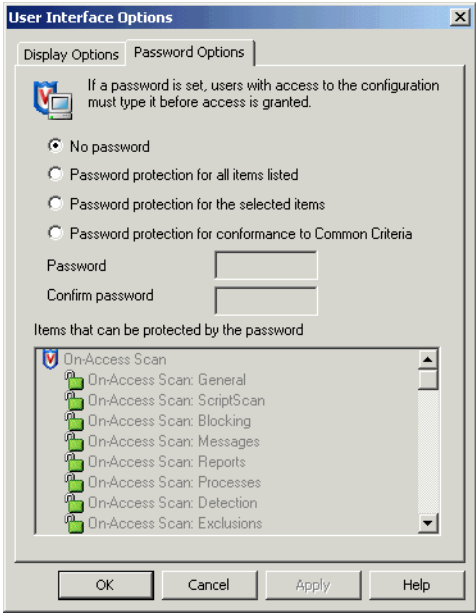


Option or Button	Description
Show the system tray icon with all menu options	Allow users to see all options on the system tray menu.
Show the system tray icon with minimal menu options	Hide all options on the system tray menu except About VirusScan Enterprise and On-Access Scan Statistics .
Do not show the system tray icon	Hide the system tray icon from all users.
Allow this system to make remote console connection to other systems	Connect to remote computers. Notes and Tips - You must have administrator rights and the Remote Registry Service must be running. - See Remote Administration on page 164 for more information.
Preferred language	Specify which language to use for the console text. Notes and Tips - The language can be automatically selected or you can select a specific language. - If you change the preferred language, the change is applied when you restart the computer.

Password Options tab

Set password security for the entire system or selected items.

Figure 2-2 User Interface Options — Password Options tab



Option or Button	Description
No password	No password is required to access configuration settings.
Password protection for all items listed	Specify one password for all the items in the list. Notes and Tips Setting a password impacts users: Non-administrators — <i>Users without administrator rights.</i> Non-administrators run all VirusScan Enterprise applications in read-only mode. They can view some configuration parameters, run saved scans, and run immediate scans and updates. They cannot change any configuration parameters, create, delete, or modify saved scan or update tasks. Administrators — <i>Users with administrator rights.</i> Administrators must type the password to access the protected tabs and controls in read/write mode. If a password is not provided for a protected item, they view it in read-only mode.
Password protection for the selected items	Specify one password for selected items in the list. Notes and Tips You do not need to enter a password for items that are not locked.

Option or Button	Description
Password protection for conformance to Common Criteria	Secure the interface as required for government agencies that must use only National Information Assurance Partnership (NIAP) Common Criteria validated security products.  Notes and Tips This secures all configuration options from users without administrative credentials except that workstation users can: ■ Perform an immediate on-demand scan of their own workstation. ■ Include or exclude files from an immediate on-demand scan. ■ Include or exclude archives, such as a .ZIP file, from an immediate on-demand scan. ■ View on-demand scan and on-access scanning activity logs.
Password	Type the password.
Confirm the password	Type the password again to confirm it.
Items that can be protected by the password	Select the items that you want to protect with the password.  Notes and Tips ■ A red locked padlock indicates that a password is required for the item. ■ A green unlocked padlock indicates that the item is read/write accessible. ■ Administrators can lock or unlock the interface through the VirusScan Console.

Unlocking and locking the user interface

If password protection is selected for any item, the **User Interface Options** dialog box is automatically protected as well. If a password has been set and a logged in user logs out, the administrator must unlock the user interface before it can be accessed again.

From the VirusScan Console:

- To unlock the user interface, select **Tools | Unlock User Interface**, then type the password and click **OK**.
- To lock the user interface, select **Tools | Lock User Interface**.

3

Access Protection

This section describes:

- [About access protection.](#)
- [Configuring access protection on page 20.](#)

About access protection

Access protection prevents unwanted changes to your computer by restricting access to specified ports, files and folders, shares, and registry keys and values. It also protects McAfee processes by preventing users from stopping them. This protection is critical before and during outbreaks.

This feature uses predefined and user-defined rules to specify which items can and cannot be accessed. Each rule can be configured to block and/or report access violations when they occur.



The on-access scanner must be enabled for the access protection feature to detect attempts to access ports, files, folders, shares, and registry keys and values.

This section describes:

- [How are rule categories defined? on page 18.](#)
- [How do protection levels apply to rules? on page 19.](#)
- [How do I include or exclude specific processes? on page 19.](#)
- [What happens when an access violation occurs? on page 20.](#)

How are rule categories defined?

Rules are separated into three categories:

Anti-virus

These preconfigured rules protect your computer from specific malware threats. You can enable, disable, and change the configuration, but you cannot delete these rules.

Two rule examples are:

- Prevent disabling or changing of critical processes, remote creation or modification of executable files, hijacking of executables, Windows Process spoofing, and mass mailing worms from sending mail.
- Protect phone book files from password and e-mail stealers.

These protection levels apply to Anti-virus rules:

- Standard Protection
- Maximum Protection
- Outbreak Control

See [How do protection levels apply to rules? on page 19](#).

Common

These preconfigured rules prevent modification of commonly used files and settings. You can enable, disable, and change the configuration, but you cannot delete these rules.

Three rule examples are:

- Prevent modification of McAfee files and settings.
- Protect Mozilla and Firefox files and settings, Internet Explorer settings, and network settings.
- Prevent installation of Browser Helper Objects and automatically running programs from the Temp folder.

These protection levels apply to Common rules.

- Standard Protection
- Maximum Protection

See [How do protection levels apply to rules? on page 19](#).

User-defined

These custom rules supplement the protection provided by the **Anti-virus** and **Common** rules.

See [Configuring access protection on page 20](#) for details.

How do protection levels apply to rules?

Anti-virus and Common rules are separated by the level of protection they provide:

- **Standard Protection** — Anti-virus and common rules that protect some critical settings and files from being modified, but generally allow you to install and execute legitimate software.
- **Maximum Protection** — Anti-virus and common rules that protect most critical settings and files from being modified. This level provides more protection, but might prevent you from installing legitimate software. If you cannot install software, we recommend that you disable the **Access Protection** feature first, then enable it again after installation.
- **Outbreak Control** — Anti-virus rules that block destructive code from accessing the computer until a DAT file is released. These rules are preconfigured to block access to shares during an outbreak.

When you installed VirusScan Enterprise, you chose either **Standard Protection** or **Maximum Protection**. That selection determines which protection level is enabled by default for each rule category. For example, if you selected **Standard Protection** during installation, all of the rules in the **Anti-virus Standard Protection** and the **Common Standard Protection** categories are enabled by default. After installation, review each rule's configuration, then enable or disable rules as necessary to meet your security needs. For example, you might decide that enabling some **Anti-virus Standard Protection** rules and some **Anti-virus Maximum Protection** rules provides the best level of protection for your environment.

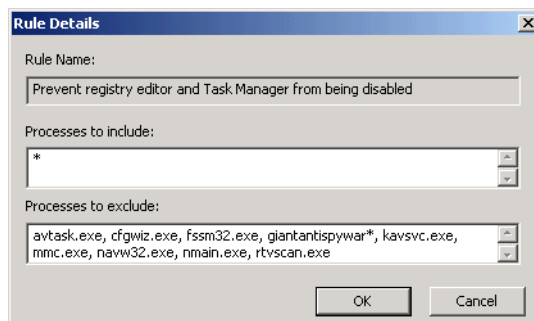
How do I include or exclude specific processes?

Edit the rule details to specify processes that you want to detect or exclude from detection:

- **Processes to include** — Restrict access to these processes. Use the exact process name or use a wildcard to specify a broad range of processes such as *.EXE, then add exclusions for specific processes that are legitimate, such as SETUP.EXE.
- **Processes to exclude** — Allow access to these processes. Use the exact process name.

For example:

Figure 3-1 Sample Rule



Option or Button	Description
Rule Name	Prevent registry editor and Task Manager from being disabled.
Processes to include	Specify * to include all processes.
Processes to exclude	Specify these exclusions: avtask.exe, cfgwiz.exe, fssm32.exe, giantantispyswar*, kavsvc.exe, mmc.exe, navw32.exe, nmain.exe, rtvscan.exe.

What happens when an access violation occurs?

When an access violations occurs:

- The system tray icon  temporarily changes to . The red frame remains visible for 30 minutes unless you reset it.



To reset the icon, open the **Access Protection Activity Log** from the system tray icon. Opening the activity log by any other method does not reset the icon to its normal state.

- Information is recorded in the activity, log if you selected the **Report** option for the rule that detected the violation.
- The event is recorded in the local event log and to SNMP, if you configured **Alert Properties** to do so.
- The event is reported to Alert Manager and/or ePolicy Orchestrator, if those products are configured to do so.
- The **Block** and/or **Report** action is taken depending on which actions are configured for the rule that detected the violation.

Configuring access protection

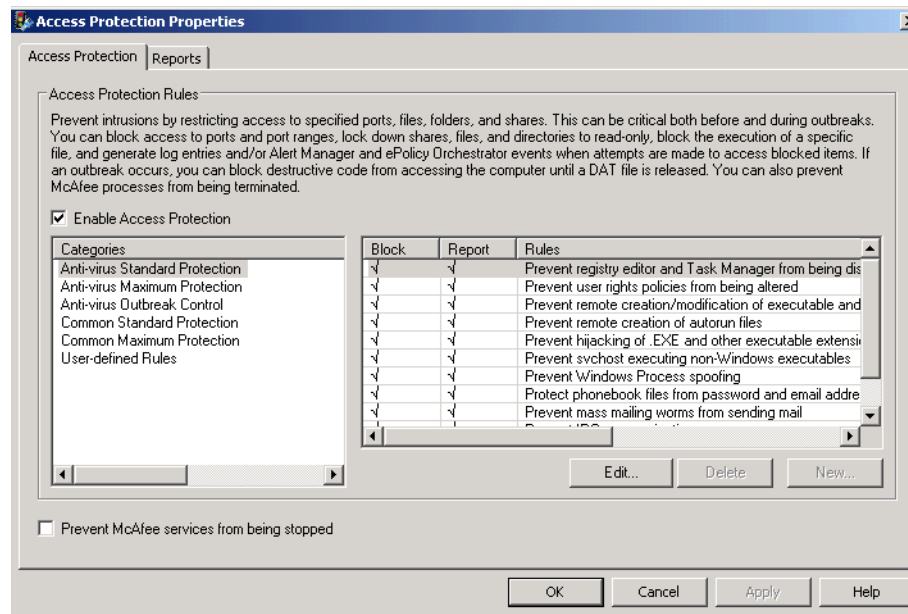
From the VirusScan Console, open the Access Protection Properties dialog box.

Tab or Button	Options or Actions
Access Protection tab	■ Enable access protection. ■ Configure rules. ■ Prevent McAfee processes from being stopped.
Reports tab	■ Enable activity logging. ■ Specify the log file name and location. ■ Specify the log file size limit. ■ Select the log file format. ■ View the log file.

Access Protection tab

Configure access protection rules and prevent McAfee processes from being stopped.

Figure 3-2 Access Protection Properties — Access Protection tab



Option or Button	Description
Enable access protection	Enables the access protection feature.  Notes and Tips On-access scanning must also be enabled for access protection to detect access attempts on specified items.
Categories	Rules are organized into these categories: ■ Anti-virus Standard Protection — Anti-virus rules that protect some critical settings and files from being modified, but generally allow you to install and execute legitimate software. ■ Anti-virus Maximum Protection — Rules that protect most critical settings and files from modification, but might prevent you from installing legitimate software. ■ Anti-virus Outbreak Control — Rules that block destructive code from accessing the computer during an outbreak, until a DAT file is released. These rules are preconfigured to block access to shares during an outbreak. ■ Common Standard Protection — Rules that protect some commonly used files and settings from being modified, but generally allow you to install and execute legitimate software. ■ Common Maximum Protection — Rules that protect most commonly used files and settings from being modified, but might prevent you from installing legitimate software. ■ User-defined Rules — Custom rules defined by the user to supplement the protection provided by the Anti-virus and Common rules.  Notes and Tips The choice you made when you installed VirusScan Enterprise determines whether Standard Protection rules or Maximum Protection rules are enabled by default. See How do protection levels apply to rules? on page 19 for more information.
Block	Blocks the process that is specified in the Rule Details. Select Block to enable the rule or deselect it to disable the rule.  Notes and Tips To block access attempts without logging, select Block but do not select Report.
Report	Enables reporting of attempts to violate access protection. When a detection occurs, information is recorded in the activity log.  Notes and Tips To receive a warning without blocking access attempts, select Report, but do not select Block. This is useful when the full impact of a rule is not known. Monitor the logs and/or reports for a short while to determine whether to block access.
Rules	Use the Anti-virus, Common, and User-defined rules to protect your computer from unwanted changes.  Notes and Tips The rules are configured according to the type of rule: ■ Anti-virus and Common rules are preconfigured. See Configuring Anti-virus and Common rules on page 23. ■ User-defined rules can be configured to meet your needs. See Configuring user-defined rules on page 23.
Add	Create a new user-defined rule. See Adding new user-defined rules on page 24.

Option or Button	Description
Delete	Remove an existing user-defined rule.
Edit	Change an existing rule.
Prevent McAfee processes from being stopped	Prevent users without debug privileges from terminating McAfee processes.  Notes and Tips ■ Users with debug program privileges can still stop McAfee processes even though you select this option. ■ Administrators have debug program privileges by default for Windows XP and Windows 2003 operating systems. Remove these privileges from the user's permissions so that they cannot stop McAfee processes.

Configuring Anti-virus and Common rules

Use predefined **Anti-virus** and/or **Common** rules to protect your computer from unwanted changes. These rules can be enabled and edited, but they cannot be deleted.

- 1 Select the **Anti-virus** or **Common** category in the left pane, then select the specific rule in the right pane.
- 2 Configure the **Block** and/or **Report** options.
- 3 Click **Edit** to configure **Rule Details**. See [How do I include or exclude specific processes? on page 19](#) for details.

Configuring user-defined rules

Create user-defined rules to supplement the protection provided by the **Anti-virus** and **Common** rules.

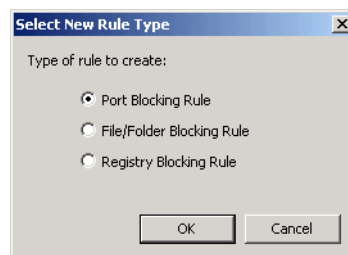
This section describes:

- [Adding new user-defined rules on page 24.](#)
- [Editing user-defined rules on page 24.](#)
- [Configuring port blocking rules on page 25.](#)
- [Configuring file/folder blocking rules on page 26.](#)
- [Configuring registry blocking rules on page 27.](#)
- [Removing user-defined rules on page 28.](#)

Adding new user-defined rules

- 1 Select the User-defined Rules category in the left pane, then click **New**.
- 2 Select the rule type.

Figure 3-3 Types of user-defined rules



Option or Button	Description
Port Blocking Rule	Blocks incoming or outgoing network traffic on specific ports or ranges of ports. See Configuring port blocking rules on page 25 . Notes and Tips When you block a port, Transmission Control Protocol (TCP) and User Datagram Protocol (UCDP) accesses are blocked.
File/Folder Blocking Rule	Blocks read or write access to files and folders. See Configuring file/folder blocking rules on page 26 . Notes and Tips Once you restrict access to a file or folder, the restriction remains in place until the administrator removes it. This helps prevent intrusions and stops them from spreading during an outbreak.
Registry Blocking Rule	Protects registry keys or values by blocking these actions: read from, write to, create, or delete. See Configuring registry blocking rules on page 27 .

Editing user-defined rules

- 1 Select the User-defined Rules category in the left pane, then select the rule you want to edit in the right pane.
- 2 Change the **Block** and **Report** actions as necessary.
- 3 Click **Edit** to change the configuration. See these sections for more information:
 - [Configuring port blocking rules on page 25](#).
 - [Configuring file/folder blocking rules on page 26](#).
 - [Configuring registry blocking rules on page 27](#).

Configuring port blocking rules

Block users from accessing specified inbound and/or outbound ports.

Figure 3-4 Network Port Access Protection Rule

Network Port Access Protection Rule

Rule Name:
New rule

Processes to include:

Processes to exclude:

Ports to block:
Enter a single port to be blocked, or enter both a beginning and ending port to block an inclusive range of ports.
Starting Port: Ending Port:

Direction

☐ Inbound - prevent systems on the network from accessing these local ports.

☐ Outbound - prevent local processes from accessing these ports on the network.

OK Cancel

Option or Button	Description
Rule Name	Type the name for this rule.
Processes to include	Restrict access to the specified ports.
Processes to exclude	Allow access to the specified ports.
Starting Port	Specify the first port number. This can be a single port or the starting number of a range of ports. Notes and Tips If you block access to a port that is used by the ePolicy Orchestrator agent, the Entercept agent, or the Host Intrusion Prevention agent, the agent's processes are trusted and are allowed to communicate with the blocked port. All other traffic not related to these agent processes is blocked.
Ending Port	Specify the last port number in a range of ports.
Inbound	Prevent systems on the network from accessing the specified ports.
Outbound	Prevent local processes from accessing the specified ports on the network.

Configuring file/folder blocking rules

Prevent users from taking action on specified files or folders.

Figure 3-5 File/folder blocking rule

Option or Button	Description
Rule name	Type the name for this rule.
Processes to include	Restrict access to the specified ports.
Processes to exclude	Allow access to the specified ports.
File or folder name to block	Block access to the specified file or folder.
Browse file	Navigate to the file.
Browse folder	Navigate to the folder.
Read access to files	Block read access to the specified files.
Write access to files	Block write access to the specified files.
Files being executed	Block files from being executed in the specified folder.
New files being created	Block new files from being created in the specified folder.
Files being deleted	Block files from being deleted from the specified folder.

Configuring registry blocking rules

Block users from taking action on specified registry keys or values

Figure 3-6 Registry Access Protection Rule

Option or Button	Description
Rule Name	Specify the name for this rule.
Processes to include	Restrict these processes from access.
Processes to exclude	Allow access to these processes.
Registry key or value to protect	Protect this registry key or value: ■ Select a root key or value from the drop-down list. ■ Type a key or value in the text box. Notes and Tips Selecting the root key or value from the drop-down list is optional. Use either of these methods to specify the key or value: ■ Select the root key or value from the drop-down list, then type the remaining path to the key or value in the text box. ■ Type the full path to the key or value in the text box.
Rule type	Select the type of rule: ■ Key — This rule protects the specified key. ■ Value — This rule protects the specified value.
Read from key or value	Block reading from the specified key or value.
Write to key or value	Block writing to the specified key or value.
Create key or value	Block creating the specified key or value.
Delete key or value	Block deleting the specified key or value.

Removing user-defined rules

- 1 Select the **User-defined Rules** category in the left pane, then select the rule you want to remove in the right pane.
- 2 Click **Delete**.

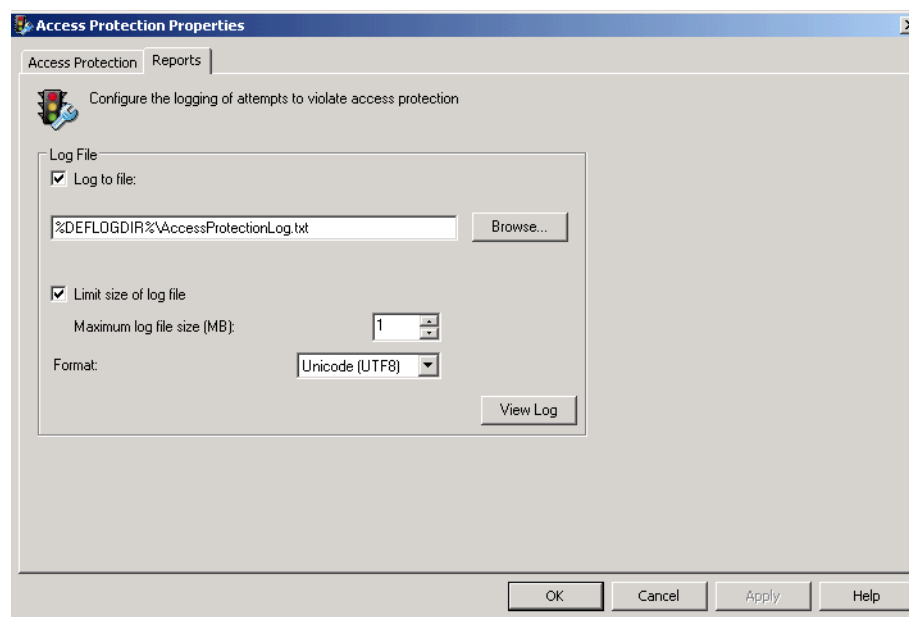


To disable a rule without deleting it, deselect the **Block** and **Report** actions. You can enable the rule again if necessary.

Reports tab

Configure activity log information.

Figure 3-7 Access Protection Properties — Reports tab



Option or Button	Description
Log to file	Record access protection activity in a log file. Accept the default location for the file or browse to a new location. The default log name is ACCESSPROTECTIONLOG.TXT. The default location is: <drive>:\Documents and Settings\All Users\Application Data\McAfee\DesktopProtection\  Notes and Tips ■ The log file can track activity on your network and note which settings you used to detect and respond to any potential threat that the scanner found. The recorded information helps determine which files you need to either replace from backup copies or delete. ■ The default location depends on which operating system you are using.
Limit size of log file	Restrict the log file to the size you specify.  Notes and Tips If the data in the log file exceeds the file size you set, the oldest 20 percent of the entries are deleted and new data is appended to the file.
Maximum log file size	Specify the maximum size for the log file.  Notes and Tips Accept the default size (1MB) or set a size from 1MB to 999MB.
Format	Select the format of the log file: ■ Unicode (UTF8) ■ Unicode (UTF16) ■ ANSI  Notes and Tips ■ <i>Default = Unicode (UTF8).</i> ■ The format you choose depends on the information you are storing. If you are storing western text (every character is one byte), we recommend using ANSI format. If you are storing eastern text (every character is one or two bytes), or sharing information within a multi-national organization, we recommend using one of the Unicode formats.
View Log	View the existing log file.

4

Buffer Overflow Protection

This section describes:

- [About buffer overflow protection.](#)
- [Configuring buffer overflow protection on page 31.](#)

About buffer overflow protection

VirusScan Enterprise protects your computer from buffer overflow exploits.

This section describes:

- [What is a buffer overflow exploit?](#)
- [How does buffer overflow protection work? on page 31.](#)

What is a buffer overflow exploit?

A buffer overflow exploit is an attack technique that exploits a software design defect in an application or process to force it to execute code on the computer. Applications have fixed-size buffers that hold data. If an attacker sends too much data or code into one of these buffers, the buffer overflows. The computer then executes the code that overflowed as a program. Since the code execution occurs in the security content of the application, which is often at a highly-privileged or administrative level, intruders gain access to execute commands not usually accessible to them. An attacker can use this vulnerability to execute custom hacking code on the computer and compromise its security and data integrity.

How does buffer overflow protection work?

Buffer overflow protection prevents exploited buffer overflows from executing arbitrary code on your computer. It monitors usermode API calls and recognizes when they are called as a result of buffer overflow.

When a detection occurs, information is recorded in the activity log and displayed in the On-Access Scan Messages dialog box if you configured those options to do so.

VirusScan Enterprise uses a Buffer Overflow and Access Protection DAT file to protect approximately 20 applications, including Internet Explorer, Microsoft Outlook, Outlook Express, Microsoft Word, and MSN Messenger.

Configuring buffer overflow protection

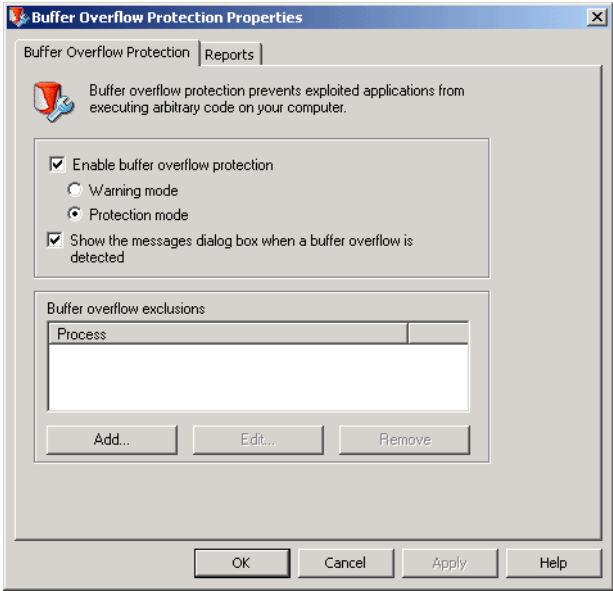
From the VirusScan Console, open the Buffer Overflow Protection Properties dialog box.

Tab or Button	Options or Actions
Buffer Overflow Protection tab	■ Enable buffer overflow protection. ■ Configure the detection mode to warn and/or protect you from buffer overflows. ■ Display the On-Access Scan Messages dialog box when a detection occurs.
Reports tab	■ Enable activity logging. ■ Specify the log file name and location. ■ Specify the log file size limit. ■ Select the log file format. ■ View the log file.

Buffer Overflow Protection tab

Prevent buffer overflow exploits from executing arbitrary code on your computer.

Figure 4-1 Buffer Overflow Protection — Buffer Overflow Protection tab



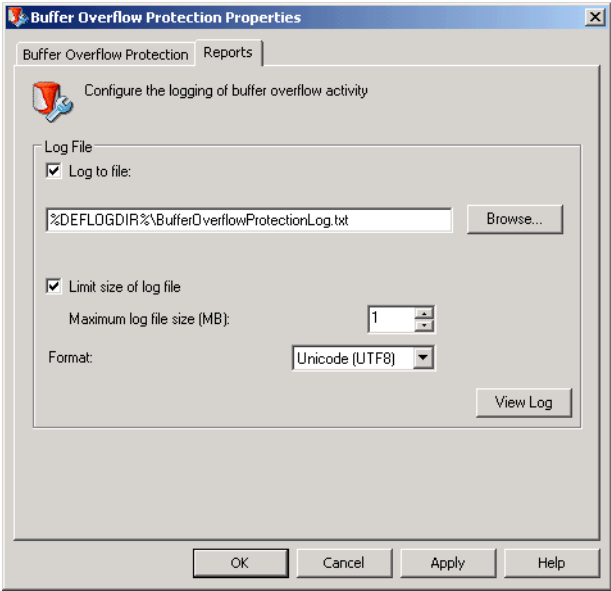
Option or Button	Description
Enable buffer overflow protection	Enables the buffer overflow protection feature.
Warning mode	Sends a warning when a buffer overflow is detected. No other action is taken. Notes and Tips This mode is useful when the full impact of a buffer overflow is not known. Use the feature in Warning Mode for a short while and review the log file during that time to help determine whether to change to Protection Mode.
Protection Mode	Blocks buffer overflows as they are detected and terminates the detected thread. Notes and Tips This can also result in termination of the application.
Show the messages dialog box when a buffer overflow is detected	Displays the On-Access Scan Messages dialog box when a detection occurs.

Option or Button	Description
Process	List of process names that are excluded from detection. These can be processes that generate false positives.  Notes and Tips ■ Specify the process name that owns the writable memory that is making the call. ■ You can type the process name alone or include its path. If you type the process name only, such as for OUTLOOK.EXE, that process is excluded whenever it is executed, no matter where it is located. If you type the process name including the path, such as C:\Program files\OUTLOOK.EXE, that process is excluded only when it is executed from the specified path. ■ Wildcards are not allowed. ■ See Buffer overflow detections on page 127 for more information.
Add	Add a new buffer overflow exclusion.  Notes and Tips See Buffer overflow exclusion on page 128.
Edit	Change an existing buffer overflow detection.  Notes and Tips See Buffer overflow exclusion on page 128.
Remove	Delete an existing buffer overflow detection.

Reports tab

Configure activity log information.

Figure 4-2 Buffer Overflow Protection – Reports tab



Option or Button	Description
Log to file	Record buffer overflow protection activity in a log file. Accept the default location for the file or browse to a new location. The default log name is BUFFEROVERFLOWPROTECTIONLOG.TXT. The default location is: <pre><drive>:\Documents and Settings\All Users\Application Data\McAfee\DesktopProtection\</pre> Notes and Tips ■ The log file can track activity on your network and note which settings you used to detect and respond to any potential threat that the scanner found. The recorded information helps determine which files you need to either replace from backup copies or delete. ■ The default location depends on which operating system you are using.
Limit size of log file	Restrict the log file to the size you specify. Notes and Tips If the data in the log file exceeds the file size you set, the oldest 20 percent of the entries are deleted and new data is appended to the file.
Maximum log file size	Specify the maximum size for the log file. Notes and Tips Accept the default size (1MB) or set a size from 1MB to 999MB.

Option or Button	Description
Format	Select the format of the log file: ■ Unicode (UTF8) ■ Unicode (UTF16) ■ ANSI  Notes and Tips ■ <i>Default = Unicode (UTF8).</i> ■ The format you choose depends on which information you are storing. If you are storing western text (every character is one byte), we recommend using the ANSI format. If you are storing eastern text (every character is one or two bytes), or sharing information within a multi-national organization, we recommend using one of the Unicode formats.
View Log	View the existing log file.

5

Unwanted Programs Policy

This section describes:

- [About unwanted programs protection.](#)
- [Configuring the unwanted programs policy on page 37.](#)

About unwanted programs protection

VirusScan Enterprise protects your computer from unwanted programs that are a nuisance or present a security risk.

This section describes:

- [What are potentially unwanted programs?](#)
- [How does the unwanted programs policy work? on page 37.](#)

What are potentially unwanted programs?

Software programs written by legitimate companies that may alter the security state or the privacy policy of the computer on which they are installed. This software can but does not necessarily include spyware, adware, and dialers. These programs can be downloaded in conjunction with a program that the user wants. Security-minded users recognize such programs and, in some case, remove them.

How does the unwanted programs policy work?

Each of the VirusScan Enterprise scanners independently uses the configured policy. This allows you to detect potentially unwanted programs as they are accessed, using immediate or scheduled scan tasks, and/or when included with e-mail.

Configuration is a two-step process:

- 1 Define which programs to detect and exclude in the **Unwanted Programs Policy**:
 - Select whole categories of programs or specific programs within a category from a pre-defined list which comes from the current DAT file.
 - Define exclusions.
 - Create a list of user-defined programs to detect.
- 2 For each scanner: on-access, on-demand, and e-mail, enable the policy and specify the actions to take when an unwanted program is detected.

Configuring the unwanted programs policy

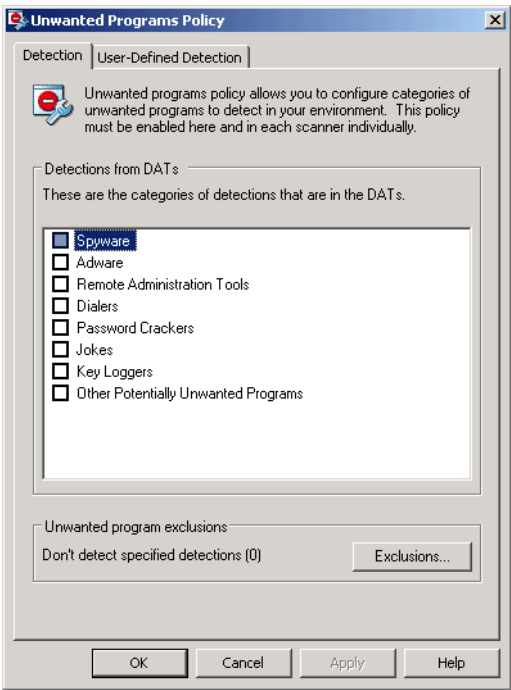
From the VirusScan Console, open the Unwanted Programs Policy dialog box.

Tab	Options or Actions
<i>Detection tab</i>	■ Select the categories of unwanted programs to detect. For example, spyware, adware, etc. These categories are defined by the current DAT file. ■ Specify exclusions.
<i>User-Defined Detection tab</i>	Define additional unwanted program for detection.

Detection tab

Select categories of potentially unwanted programs to detect and create exclusions for programs that you do not want to detect.

Figure 5-1 Unwanted Programs Policy — Detection tab



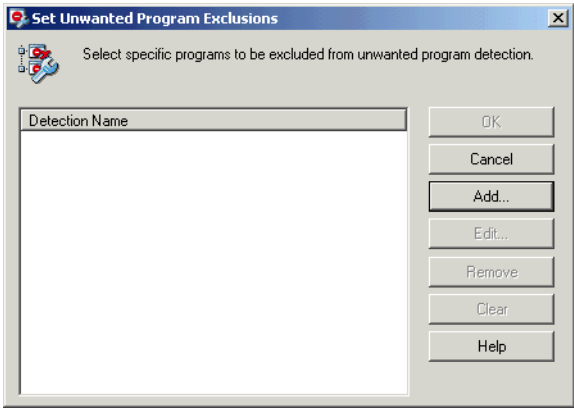
Option or Button	Description
Detections from DATs	Specify the categories of potentially unwanted programs to detect.
Exclusions	Specify files or programs to exclude from detection.
	Notes and Tips
	See Excluding unwanted programs on page 39 for more information.

Excluding unwanted programs

Even though you selected a category for detection, there may be specific files or programs within that category that you don't want to detect.

From the Unwanted Programs Policy dialog box, click Exclusions.

Figure 5-2 Unwanted Programs Policy — Set Unwanted Program Exclusions

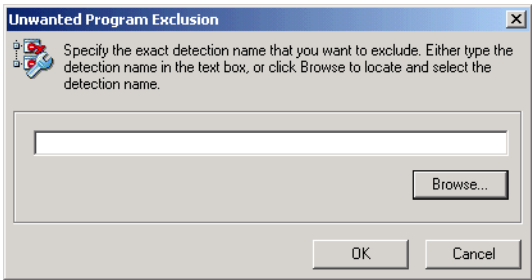


Option or Button	Description
Detection Name	The name of the file or program.
Add	Add a new file or program to exclude. Notes and Tips See Adding an exclusion on page 40.
Edit	Change an existing exclusion. ■ Select a Detection Name, then click Edit. ■ Make changes as necessary.
Remove	Delete an existing exclusion. Select a Detection Name in the left pane, then click Remove .
Clear	Remove all exclusions.

Adding an exclusion

From the Set Unwanted Program Exclusions dialog box, click Add.

Figure 5-3 Unwanted Program Policy – Add exclusion

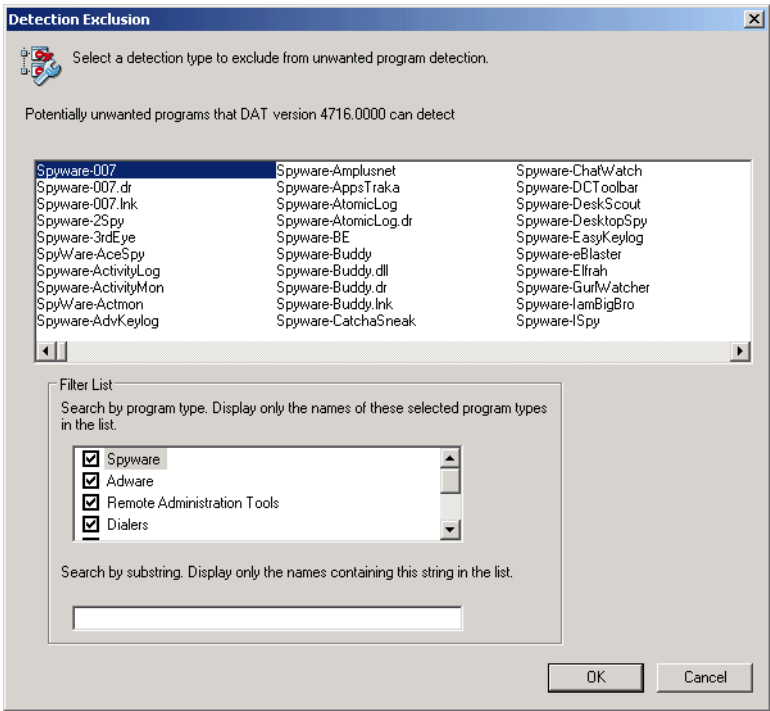


Option or Button	Description
Detection Name	Specify the exact name of the file or program to exclude from detection.
Browse	Display the list of unwanted programs from the current DAT file.
Notes and Tips See Selecting detection types for exclusion on page 40 for details.	

Selecting detection types for exclusion

From the Set Unwanted Program Exclusions dialog box, click Add, then click Browse.

Figure 5-4 Unwanted Program Policy – Detection Exclusion

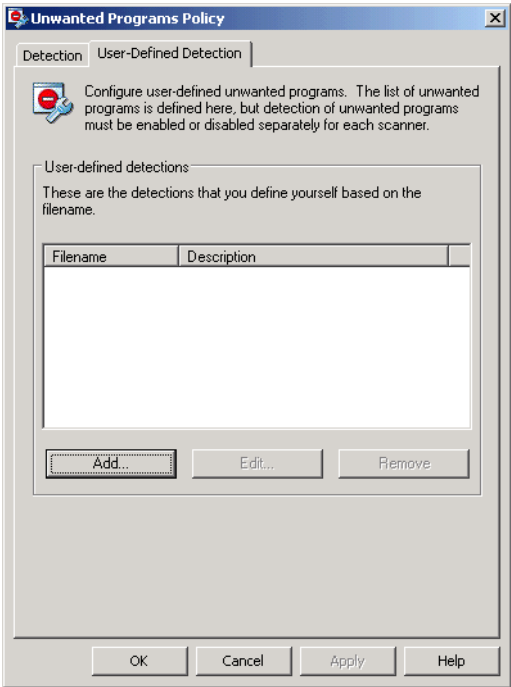


Option or Button	Description
Potentially unwanted programs that DAT version xxxx can detect	Select one or more programs to exclude from detection.
Filter List	Select the types of programs to exclude from detection.
Search by substring	Type a string or file name to exclude from detection.

User-Defined Detection tab

Specify individual files or programs to treat as unwanted programs.

Figure 5-5 Unwanted Programs Policy — User-Defined Detection tab

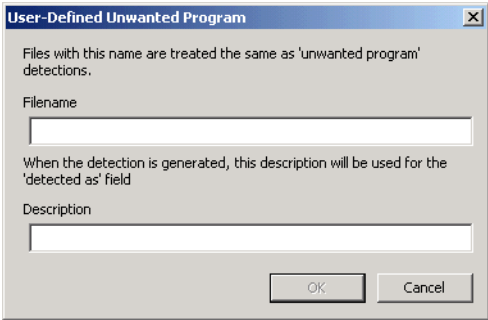


Option or Button	Description
Filename	The name of the file or program.
Description	The description of the file or program.
Add	Add a new file or program to detect.
Edit	Change an existing user-defined detection.
Remove	Delete an existing user-defined detection.

Adding user-defined detections

Specify the file name and description for unwanted programs.

Figure 5-6 Unwanted Programs Policy — Add or edit a user-defined file



Option or Button	Description
Filename	Specify the name of the file or program that you want to detect.
Description	Specify the description that you want to display in the notification when the specified file is detected.

SECTION 2

Detection

Develop an effective strategy to detect intrusions when they occur. Your strategy should include these actions:

- Configure update tasks to get the most current detection definitions.
- Configure the on-access scanner to detect threats as they are accessed.
- Configure on-demand scan tasks to perform regular scans of your environment.
- Configure the e-mail scanners to protect your Microsoft Outlook and Lotus Notes e-mail clients.

[Chapter 6, AutoUpdate](#)

[Chapter 7, On-Access Scanner](#)

[Chapter 8, On-Demand Scanner](#)

[Chapter 9, E-mail Scanners](#)

6

AutoUpdate

This section describes:

- [About AutoUpdate.](#)
- [Using the AutoUpdate repository list on page 50.](#)
- [Using AutoUpdate tasks on page 55.](#)
- [Using mirror tasks on page 58.](#)
- [Rolling back DAT files on page 62.](#)

About AutoUpdate

VirusScan Enterprise software depends on the scanning engine and the information in the detection definition (DAT) files to identify and take action on threats. New threats appear on a regular basis. To meet this challenge, McAfee releases new DAT files every day, incorporating the results of its ongoing research. The AutoUpdate feature uses an update task to automatically retrieve the most current DAT files, EXTRA.DAT file, scanning engine, product updates, Service Packs, and Patches.

This section describes:

- [What update strategy should I use? on page 45.](#)
- [How do AutoUpdate tasks work? on page 45.](#)
- [How does the AutoUpdate repository list work? on page 48.](#)
- [How do mirror tasks work? on page 49.](#)

What update strategy should I use?

Updates can be accomplished using many methods. You can use update tasks, manual updates, login scripts, or schedule updates with management tools. This section describes using the AutoUpdate task. Any other methods are beyond of the scope of this guide.

An efficient updating strategy generally requires that at least one client or server in your organization retrieve updates from the McAfee download site. From there, the files can be replicated throughout your organization, providing access for all other computers. Ideally, you should minimize the amount of data transferred across your network by automating the process of copying the updated files to your share sites.

The main factors to consider for efficient updating, are the number of clients and the number of sites. You might also consider the number of systems at each remote site and how remote sites access the Internet. However, the basic concepts of using a central repository to retrieve updates and scheduling update tasks to keep your environment up-to-date apply to any size organization.

Using an update task allows you to:

- Schedule network-wide DAT file rollouts at convenient times and with minimal intervention from either administrators or network users. You might, for example, stagger your update tasks, or set a schedule that phases in, or rotates, DAT file updates to different parts of the network.
- Split duties for rollout administration among different servers or domain controllers, among different regions of wide-area networks, or across other network divisions. Keeping update traffic primarily internal can also reduce the potential for network security breaches.
- Reduce the waiting time required to download new DAT or upgraded engine files. Traffic on McAfee computers increases dramatically on regular DAT file publishing dates and whenever new product versions are available. Avoiding the competition for network bandwidth enables you to deploy your new software with minimal interruptions.

How do AutoUpdate tasks work?

The AutoUpdate task performs scheduled or immediate updates. You can update DAT files, the scanning engine, and the EXTRA.DAT file.

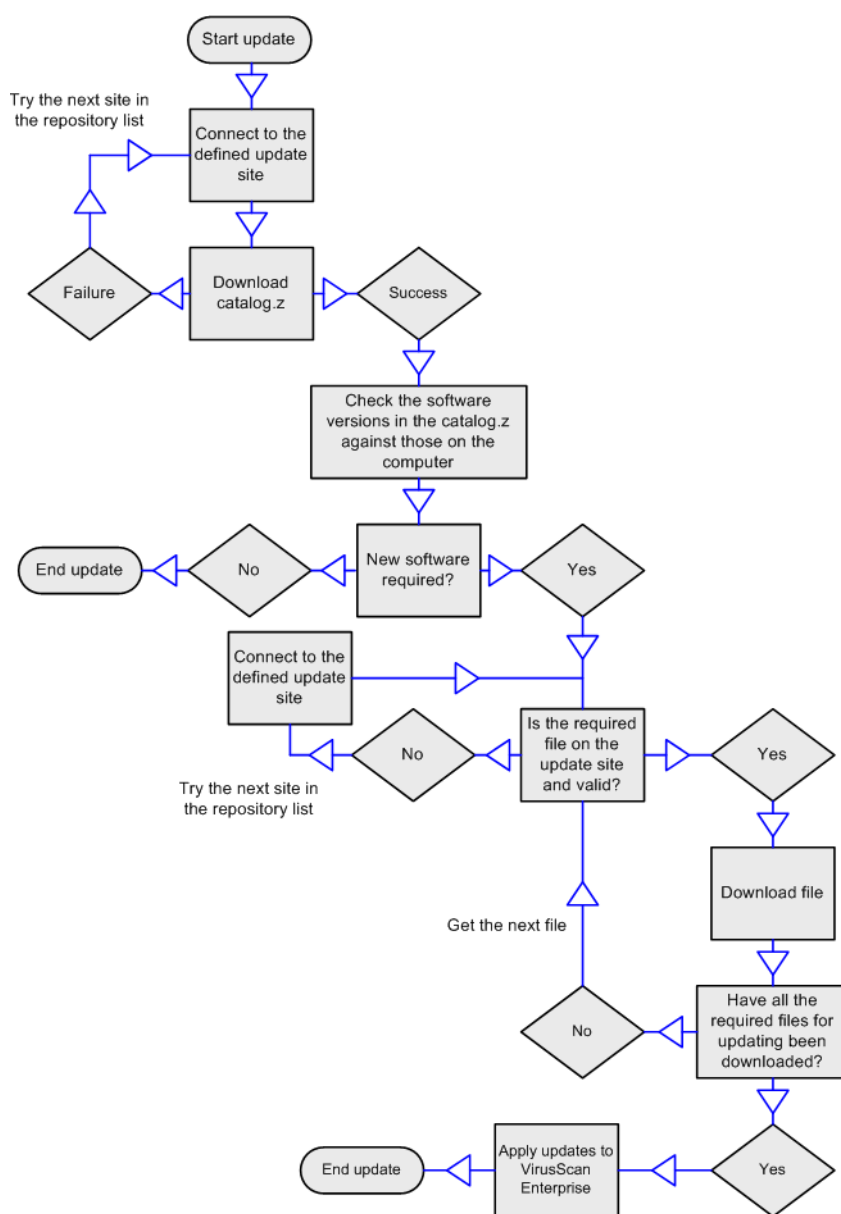
VirusScan Enterprise provides a default update task that is scheduled to update every day at 5:00 p.m. with one-hour randomization. The default update task is named **AutoUpdate**. You can rename and reconfigure the default **AutoUpdate** task. You can also create additional update tasks to meet your updating requirements.

This section describes:

- [Overview of an AutoUpdate task on page 46.](#)
- [What happens during an AutoUpdate task? on page 47.](#)

Overview of an AutoUpdate task

This diagram shows how a typical AutoUpdate task works:



What happens during an AutoUpdate task?

These activities occur when you run an update task:

- A connection is made to the first *enabled* repository (update site) in the repository list. If this repository is not available, the next site is contacted, and so on until a connection is made, or until the end of the list is reached.
- An encrypted CATALOG.Z file downloads from the repository. The CATALOG.Z file contains the fundamental data required to update. This data is used to determine which files and/or updates are available.
- The software versions in the CATALOG.Z are checked against the versions on the computer. If new software updates are available, they are downloaded.
- Once the update is checked into the repository, the update is verified to confirm that it is applicable to VirusScan Enterprise and that the version is newer than the current version. Once this is verified, VirusScan Enterprise downloads the update when the next update task runs.

If the update task is interrupted for any reason during the update:

- A task updating from an HTTP, UNC, or local site resumes where it left off the next time the update task starts.
- A task updating from an FTP site does not resume if interrupted during a single file download. However, if the task is downloading several files and is interrupted, the task resumes before the file that was being downloaded at the time of the interruption.

An EXTRA.DAT file can be used as a temporary measure in an emergency. The EXTRA.DAT is downloaded from the repository on each update. This ensures that if you modify and re-check in the EXTRA.DAT in as a package, all VirusScan Enterprise clients download and use the same updated EXTRA.DAT package. For example, you may use the EXTRA.DAT as an improved detector for the same potentially unwanted program or additional detection for other new potentially unwanted programs. VirusScan Enterprise supports using only one EXTRA.DAT file.



When you have finished using the EXTRA.DAT file, you should remove it from the master repository and run a replication task to ensure it is removed from all distributed repository sites. This stops VirusScan Enterprise clients from attempting to download the EXTRA.DAT file during an update.

By default, detection for the new potentially unwanted program in the EXTRA.DAT is ignored once the new detection definition is added to the weekly DAT files.

How does the AutoUpdate repository list work?

The AutoUpdate repository list (SITELIST.XML) specifies the configuration information necessary to perform an AutoUpdate task. For example:

- Repository information and location.
- Repository order preference.
- Proxy settings, where required.
- Encrypted credentials required to access each repository.

When an AutoUpdate task is performed, a connection is made to the first *enabled* repository (update site) in the repository list. If this repository is not available, the next repository is contacted, and so on until a connection is made, or until the end of the list is reached.

The location of the AutoUpdate repository list depends on your operating system. For example, for Windows XP:

```
C:\Documents and Settings\All Users\Application Data\McAfee\Common  
Framework
```

How do mirror tasks work?

The mirror task replicates the update files from the first accessible repository defined in the repository list, to a mirror site on your network. The most common use of this task is to mirror the contents of the McAfee download site to a local server.

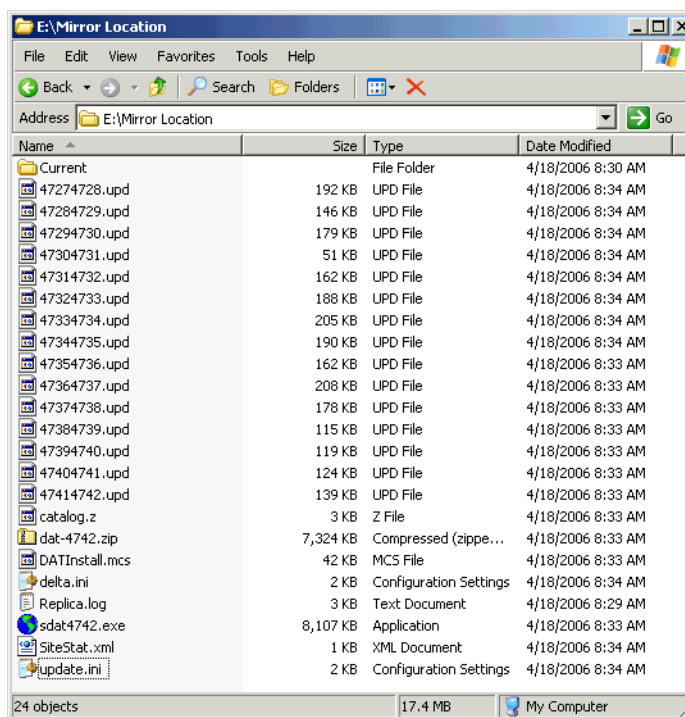
The VirusScan Enterprise software relies on a directory structure to update itself. When mirroring a site, it is important to replicate the entire directory structure.



This directory structure also supports previous versions of VirusScan and NetShield, as long as the entire directory structure is replicated in the same locations that VirusScan 4.5.1 used for updating.

This is an example of a repository directory structure after using a mirror task to replicate the McAfee repository:

Figure 6-1 Mirrored site



After you replicate the McAfee site that contains the update files, computers on your network can download the files from the mirror site. This approach is *practical* because it allows you to update any computer on your network, whether or not it has Internet access; and *efficient* because your computers are communicating with a server that is probably closer than a McAfee Internet site, economizing access and download time.

Using the AutoUpdate repository list

You can import and configure the AutoUpdate repository list before, during or after installation. This guide addresses post installation options.



You must use McAfee AutoUpdate Architect if you plan to:

- Import a customized AutoUpdate repository list.
- Specify source repositories from which to obtain software.
- Use multiple update locations that can replicate from a master repository.

This section describes:

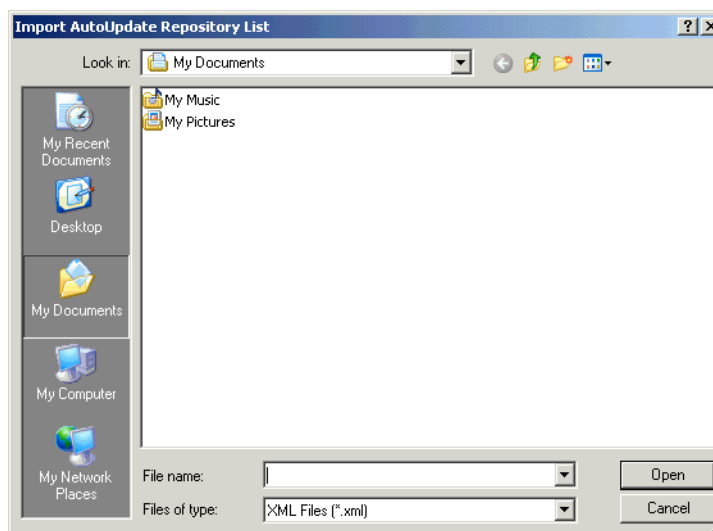
- [Importing the repository list.](#)
- [Configuring the repository list on page 51.](#)

Importing the repository list

You can use the default repository list, SITELIST.XML, provided with VirusScan Enterprise or import your own repository list. If using your own repository list, it must be named SITELIST.XML.

From the VirusScan Console, select Tools| Import AutoUpdate Repository List.

Figure 6-2 Import repository list



Option or Button	Description
Look in	Navigate to the SITELIST.XML file.
File name	Select the SITELIST.XML file, then click Open to import the repository list.

Configuring the repository list

The repository list includes the repositories from which you retrieve updates. Create and configure as many repositories as you need. Some sites may be used all the time while others are used only occasionally.

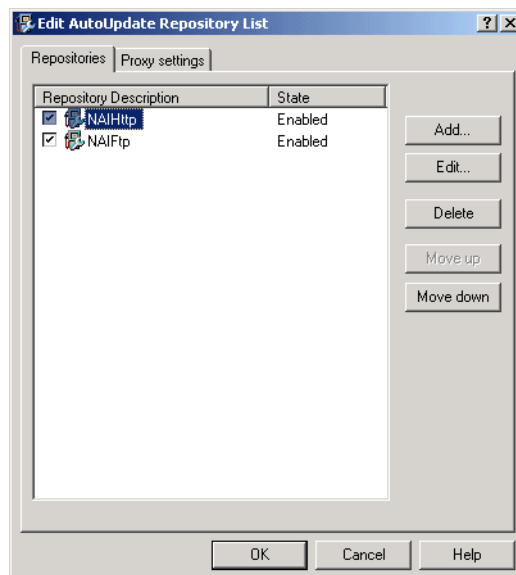
From the VirusScan Console, select Tools, then select Edit AutoUpdate Repository List.

Tab or Button	Options or Actions
Repositories tab	- Specify the repositories from which you get updates. - Configure the order in which the repositories are accessed.
Proxy settings tab	Specify which proxy settings to use when updating.

Repositories tab

Configure the repositories where you get updates.

Figure 6-3 Edit AutoUpdate Repository List – Repositories tab



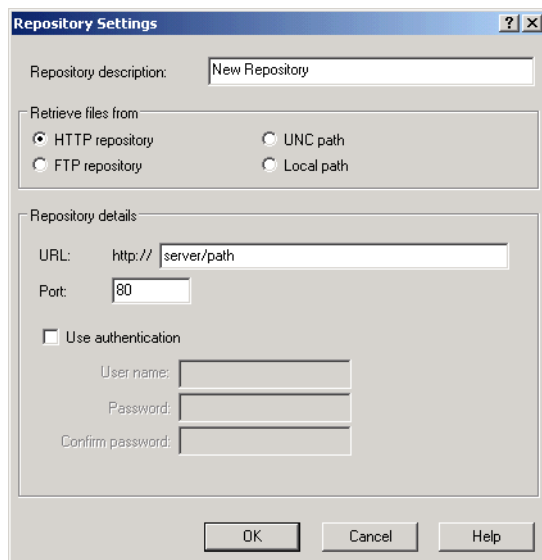
Option or Button	Description
Repository description	Specify the name of the repository.  Notes and Tips The list is preconfigured with an HTTP and an FTP repository. http://update.nai.com/Products/CommonUpdater ftp://ftp.nai.com/CommonUpdater The HTTP repository is the default download site.
State	Enabled — A defined repository that can be used during the AutoUpdate process. Disabled — A defined repository that you do not want to access during the AutoUpdate process. This might be a repository that you use occasionally, but not all of the time.  Notes and Tips Create as many repository sites as necessary, then enable and disable them.
Add	Add a new repository to the list.
Edit	Edit the selected repository.
Delete	Delete the selected repository.
Move up	Move the selected repository up in the list.
Move down	Move the selected repository down in the list.

Adding or editing repositories

Choose from these options:

- To add a repository, click **Add**.
- To edit a repository, select the repository, then click **Edit**.

Figure 6-4 Adding or Editing Repository Settings



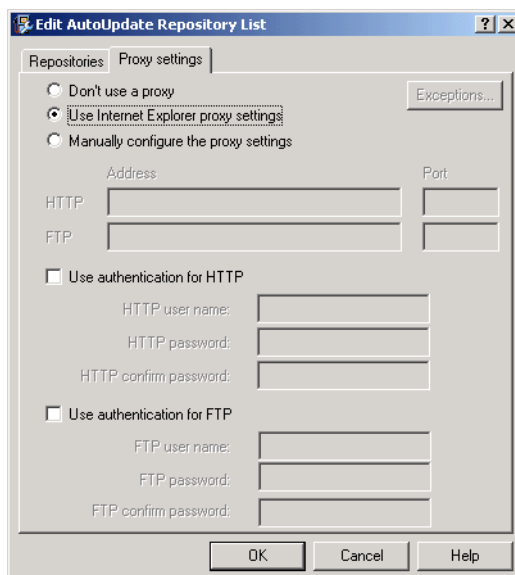
Option or Button	Description
Repository description	Specify the name of the repository.
Retrieve files from	■ HTTP repository — Retrieve files from the HTTP repository location that you designate. ■ FTP repository — Retrieve files from the FTP repository location that you designate. ■ UNC path — Retrieve files from the UNC path location that you designate. ■ Local path — Retrieve files from the local path that you designate.  Notes and Tips ■ <i>Default = HTTP repository.</i> ■ An HTTP site, like FTP, offers updating independent of network security, but supports higher levels of concurrent connections than FTP. ■ An FTP site offers flexibility of updating without having to adhere to network security permissions. FTP has been less prone to unwanted code attack than HTTP, so it may offer better tolerance. ■ A UNC site is the quickest and easiest to set up. Cross domain UNC updates require security permissions for each domain, which makes update configuration more involved.
URL	Available only if you selected HTTP repository or FTP repository. ■ HTTP. Type the location for the HTTP server and folder where the update files are located. ■ FTP. Type the location for the FTP server and folder where the update files are located.
Path	Available only if you selected UNC path or Local path. ■ UNC path. Using UNC notation (\servername\path\), type the path of the repository where the update files are located. ■ Local path. Type the path of the local folder in which you have placed the update files, or click Browse to navigate to the folder. The path can be that of a folder on a local drive or a network drive.
Port	Available only if you selected HTTP repository or FTP repository. Type the port number for the HTTP or FTP server you specified.
Use authentication	Use the specified credentials for accessing the repository.
Use anonymous login	 Notes and Tips
Use logged on account	■ The title of this option differs depending on which option you selected in the Retrieve files from section. ■ The credentials you specify are used by AutoUpdate to access the repository so that it can download the required update files. When configuring the account credentials on the repository, you ensure that the account has read permissions to the folders containing the update files. Download credentials are required for FTP and UNC repositories, but are optional for HTTP repositories. FTP updates support anonymous repository connections. With UNC updates you can also use the logged on account, making use of the logged on user's permissions to access the repository.
User name	Type the user name.
Password	Type the password.
Confirm	Type the password again to confirm it.

Proxy settings tab

Proxy servers are used as part of internet security to hide internet users' computers from the internet and improve access speed by caching commonly accessed sites.

If your network uses a proxy server, you can specify which proxy settings to use, the address of the proxy server, and whether to use authentication. Proxy information is stored in the AutoUpdate repository list (SITE.LIST.XML). The proxy settings you configure here apply to all repositories in this repository list.

Figure 6-5 Edit AutoUpdate Repository List — Proxy settings tab



Option or Button	Description
Don't use a proxy	Do not specify a proxy server.
Use Internet Explorer proxy settings	Use the proxy settings for the currently installed version of Internet Explorer.  Notes and Tips Default = Use Internet Explorer proxy settings.
Manually configure the proxy settings	Configure the proxy settings to meet your specific needs.
Exceptions	Available only if you selected Manually configure the proxy settings . Specify proxy exceptions. Click Exceptions to open the Proxy Exceptions dialog box: Specify exceptions — Select this option to enter proxy exceptions. Use semicolons (;) to separate entries — For example: internal1;internal2
HTTP	Type the address of the HTTP proxy server.
FTP	Type the address of the FTP proxy server.
Port	Type the port number of the HTTP or FTP proxy server.
Use authentication for HTTP	Use the specified credentials for accessing the HTTP proxy.
HTTP user name	Type the HTTP user name.
HTTP password	Type the HTTP password.

Option or Button	Description
HTTP confirm password	Type the HTTP password again to confirm it.
Use authentication for FTP	Use the specified credentials for accessing the FTP proxy.
FTP user name	Type the FTP user name.
FTP password	Type the FTP password.
FTP confirm password	Type the FTP password again to confirm it.

Using AutoUpdate tasks

This section describes:

- [Creating AutoUpdate tasks on page 55.](#)
- [Configuring AutoUpdate tasks on page 56.](#)
- [Running AutoUpdate tasks on page 58.](#)

Creating AutoUpdate tasks

You can use the default AutoUpdate task and create new ones as needed.

- 1 Use one of these methods to create a new AutoUpdate task:
 - Right-click a blank area in the **VirusScan Console**, then select **New Update Task**.
 - From the **Task** menu, select **New Update task**.

A new update task appears, highlighted, in the **VirusScan Console** task list.

- 2 Accept the default task name or type a new name for the task, then press ENTER to open the **AutoUpdate Properties** dialog box. See [Configuring AutoUpdate tasks on page 56](#) for detailed configuration information.

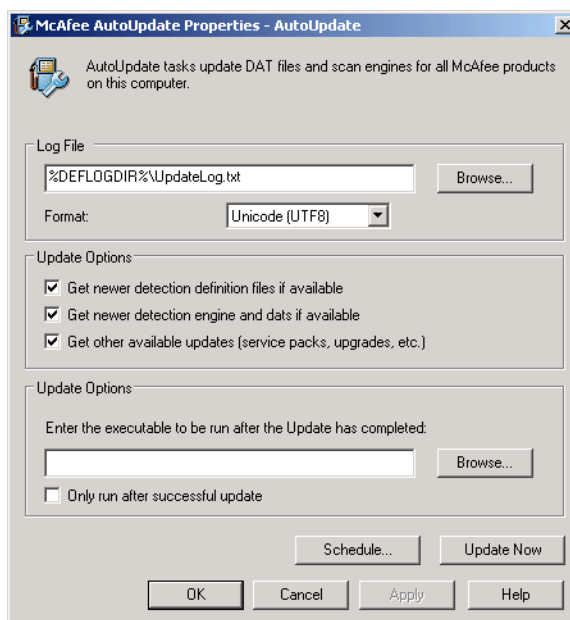


If you create update tasks via ePolicy Orchestrator and enable task visibility, these update tasks appear in the **VirusScan Console**. They are *read-only* and cannot be configured from the **VirusScan Console**. See the *VirusScan Enterprise Configuration Guide for use with ePolicy Orchestrator* for more information.

Configuring AutoUpdate tasks

From the VirusScan Console, open the AutoUpdate Properties dialog box.

Figure 6-6 AutoUpdate Properties



Option or Button	Description
Log File	Specify the location and name for the log file. Accept the default location or browse to a new location. The default log name is UPDATELOG.TXT. The default location is <drive>:\Documents and Settings\All Users\Application Data\McAfee\DesktopProtection\  Notes and Tips ■ The log file can track activity on your network and note which settings you used to perform the task. The recorded information helps you troubleshoot any issues that occurred. ■ The default location depends on which operating system you are using.
Format	Select the format of the log file: ■ Unicode (UTF8) ■ Unicode (UTF16) ■ ANSI  Notes and Tips ■ <i>Default = Unicode (UTF8).</i> ■ The format you choose depends on how important size of file and data integrity is. ■ ANSI format is usually the smallest file, which may work well if you are storing western text (every character is one byte) but may not work well with eastern text (every character is one or two bytes). If you are sharing information within a multi-national organization we recommend using one of the Unicode formats; either UTF8 or UTF16.
Get newer detection definition files if available	Get the most current version of the DAT files if a newer version is available.
Get new detection engine and DATs if available	Get the most current version of the engine and/or DAT files if newer versions are available.
Get other available updates (service packs, upgrades, etc.)	Get the most current version of other updates, such as service packs and product upgrades.
Enter the executable to be run after the Update has completed	Specify an executable file to start after the AutoUpdate task finishes running. Specify the path to the executable you want to run, or click Browse to locate it. For example, you can start a network message utility that notifies the administrator that the update completed successfully.  Notes and Tips The program file that you specify must be executable by the currently logged on user. If the currently logged on user does not have access to the folder containing the program files, or if there is no currently logged on user, the program does not run.
Only run after successful update	Run the executable program only after a successful update. If the update is not successful, the program you specified does not run.
Schedule	Schedule the update task. See Scheduling Tasks on page 153 for more information.
Update Now	Perform the update task immediately.

Running AutoUpdate tasks

Once you have configured an update task, you can run it using one of these methods:

Update as scheduled

A scheduled update task automatically runs according to the schedule you specified.

Update Now

Start the update task immediately using one of these methods:

- Select the **AutoUpdate** task in the **VirusScan Console**, then right-click and select **Start**.
- Open the **AutoUpdate Properties** dialog box and click **Update Now**.

Using mirror tasks

This section describes:

- [Creating mirror tasks](#).
- [Configuring mirror tasks on page 59](#).
- [Running mirror tasks on page 61](#).

Creating mirror tasks

You can create a mirror task for each mirror location you need.

- 1 Use one of these methods to create a new mirror task:

- Right-click a blank area in the **VirusScan Console**, then select **New Mirror Task**.
- Select **New Mirror task** from the **Task** menu.

A new mirror task appears, highlighted, in the **VirusScan Console** task list.

- 2 Accept the default task name or type a new name for your task, then press ENTER to open the **AutoUpdate Properties — Mirror Task** dialog box. See [Configuring mirror tasks on page 59](#) for details.

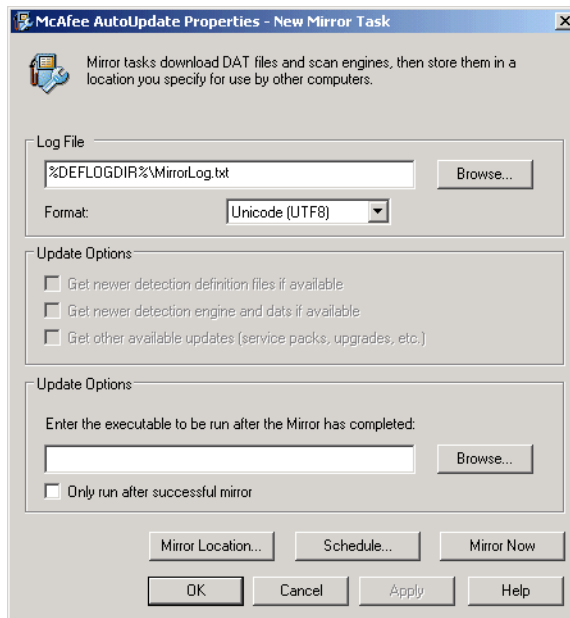


If you create mirror tasks via ePolicy Orchestrator and enable task visibility, these mirror tasks appear in the **VirusScan Console**. They are *read-only* and cannot be configured from the **VirusScan Console**. See the *VirusScan Enterprise Configuration Guide for use with ePolicy Orchestrator* for more information.

Configuring mirror tasks

From the VirusScan Console, open the AutoUpdate Properties — Mirror Tasks dialog box.

Figure 6-7 AutoUpdate Properties — Mirror Task



Option or Button	Description
Log File	Specify the location and name for the log file. Accept the default location or browse to a new location. The default log name is MIRRORLOG.TXT. The default location is <drive>:\Documents and Settings\All Users\Application Data\McAfee\DesktopProtection\  Notes and Tips ■ The log file can track activity on your network and note which settings you used to perform the task. The recorded information helps you troubleshoot any issues that occurred. ■ The default location depends on which operating system you are using.
Format	Select the format of the log file; ■ Unicode (UTF8) ■ Unicode (UTF16) ■ ANSI  Notes and Tips ■ <i>Default = Unicode (UTF8).</i> ■ The format you choose depends on how important size of file and data integrity is. ■ ANSI format is usually the smallest file, which may work well if you are storing western text (every character is one byte) but may not work well with eastern text (every character is one or two bytes). If you are sharing information within a multi-national organization we recommend using one of the Unicode formats; either UTF8 or UTF16.
Get newer detection definition files if available	This option does not apply to mirror tasks.
Get new detection engine and DATs if available	This option does not apply to mirror tasks.
Get other available updates (service packs, upgrades, etc.)	This option does not apply to mirror tasks.
Enter the executable to be run after the Mirror has completed	Specify an executable file to start after the mirror task finishes running. Specify the path to the executable you want to run, or click Browse to locate it. For example, you can start a network message utility that notifies the administrator that the mirror task completed successfully.  Notes and Tips The program file that you specify must be executable by the currently logged on user. If the currently logged on user does not have access to the folder containing the program files, or if there is no currently logged on user, the program does not run.
Only run after successful mirror	Run the executable program only after a successful mirror. If the mirror is not successful, the program you specified does not run.

Option or Button	Description
Mirror Location	Specify the path to the destination on the local system that you are using for the mirror site.  Notes and Tips System variables are supported.
Schedule	Define the schedule for this update task.  Notes and Tips - See Scheduling Tasks on page 153 for more information. - We do not recommend that you schedule an AutoUpdate task and a mirror task to run at the same time. Both tasks use the McAfee Common Framework service, consequently running both tasks at the same time may result in a conflict.
Mirror Now	Perform the mirror task immediately.

Running mirror tasks

Mirror as scheduled

A scheduled mirror task automatically runs according to the schedule you specified.



We do not recommend that you schedule an AutoUpdate task and a mirror task to run at the same time. Both tasks use the McAfee Common Framework service, consequently running both tasks at the same time may result in a conflict.

Mirror Now

Start the update task immediately using one of these methods:

- Select the mirror task in the **VirusScanConsole**, then right-click and select **Start**.
- Open the **AutoUpdate Properties — Mirror Task** dialog box and click **Mirror Now**.

Rolling back DAT files

If you find your current DAT files are corrupted or incompatible, you can roll back the DAT files to the last backed up version.

When you update DAT files, the old version is stored in this location:

```
<drive>:\Program Files\Common Files\McAfee\Engine\OldDats
```

When you roll back the DAT files, the current DAT files are replaced with the version in the *OldDats* folder, and a flag is set in the registry at this location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\DesktopProtection\szRolledbackDATS
```

Once the rollback occurs, you cannot go back to the previous version again. The next time an update occurs, the DAT version in the registry is compared with the DAT files in the update repository. If the new DAT files are the same as those in the registry, no update occurs.

To roll back the DAT files:

- 1 From the **VirusScan Console**, select **Tools | Rollback DATs**.
- 2 Click **Yes** to confirm that you want to roll back the DAT files.

The progress appears in the **McAfee AutoUpdate** dialog box.

- 3 Click **Close** when finished or allow the dialog box to close automatically.

7

On-Access Scanner

This section describes:

- [About on-access scanning.](#)
- [Configuring on-access scan properties on page 68.](#)

About on-access scanning

The on-access scanner examines files on your computer as they are accessed to provide continuous, real-time detection of threats. Both the Access Protection and Buffer Overflow Protection features also use the on-access scanner to detect access violations and buffer overflow exploits respectively.

- [How does on-access scanning work? on page 64.](#)
- [How does scanning compare when writing to disk and when reading from disk? on page 64.](#)
- [How does the script scanner work? on page 65.](#)
- [How do I configure general and process settings? on page 65.](#)
- [How do I know when to assign high-risk or low-risk to processes? on page 65.](#)

How does on-access scanning work?

The on-access scanner hooks into the system at the lowest levels (File-System Filter Driver), acts as part of the system (System Service), and delivers notifications via the interface when detections occur.

This is an example of a simplified scan:

When an attempt is made to open, close, or rename a file, the scanner intercepts the operation and takes these actions:

- 1 Determine if the file should be scanned:
 - The file's extension matches the configuration.
 - The file has not been cached.
 - The file has not been excluded.
 - The file has not been previously scanned.
- 2 If the file meets the scanning requirements, it is scanned:
 - If the file is clean, the result is cached and read, write, or rename operation is granted.
 - If the file contains a threat, the operation is denied and the configured action is taken.
 - The results are reported to activity log if the scanner was configured to do so.
- 3 If the file does not meet the scanning requirements, it is not scanned. It is cached and the operation is granted.

How does scanning compare when writing to disk and when reading from disk?

The on-access scanner treats scans differently depending on whether the user is writing to disk or reading from disk:

- When files are being written to disk, it scans these items:
 - Incoming files being written to the local hard drive.
 - Files being created on the local hard drive or a mapped network drive (this includes new files, modified files, or files being copied or moved from one drive to another).
- When files are being read from disk, it scans these items:
 - Outgoing files being read from the local hard drive.



Select **on network drives** in the **On-Access Scan Properties** dialog box to include remote network files.

- Any file being executed on the local hard drive.
- Any file opened on the local hard drive.
- Any file being renamed on the local hard drive, if the file properties have changed.

How does the script scanner work?

The script scanner operates as a proxy component to the real Windows scripting host component. It intercepts scripts, then scans them before they are executed.

- If the script is clean, it is passed on to the real scripting host component.
- If the script contains a potential threat, it is not executed.

The script scanner loads into the process that's running the script, so if that process crashes, you will see ScriptProxy.dll and Mytilus.dll in its memory space. It will load the DAT file and scan engine too, which significantly increases the memory footprint of that process.

How do I configure general and process settings?

When you open the On-Access Scan Properties dialog box, the **General Settings** and **Process Settings** icons in the left pane provide access to the configurable options in the right pane. Select an icon to view the tabs for that selection.

- **General Settings** — Apply to the scanning of all processes and include parameters such as maximum scan time, scanning scripts, blocking unwanted threats from a remote computer, sending messages when threats are detected, and reporting detections.
- **Process Settings** — Scan all processes with the same scanning configuration (policy) or configure different policies based on the risk assigned to each process. Parameters include assigning risk to processes, defining items to scan, performing heuristic scanning, scanning compressed files, taking actions on detections, and scanning for potentially unwanted programs.

How do I know when to assign high-risk or low-risk to processes?

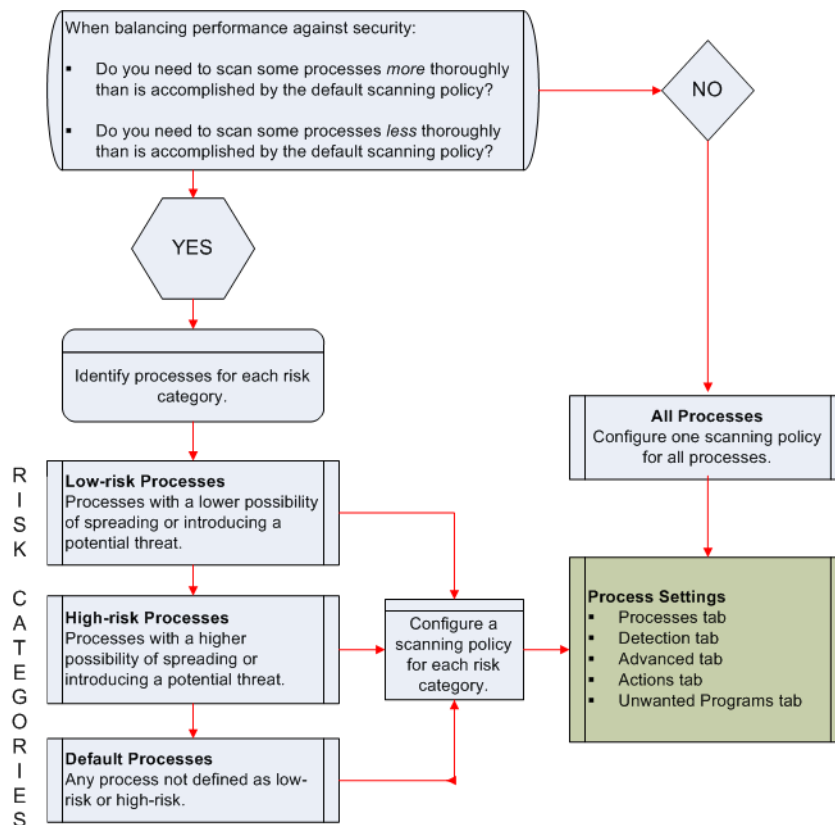
You can configure different scanning policies based on the risk you assign to each process.

This section describes:

- [Do I need more than one scanning policy? on page 66.](#)
- [How do I assign risk to a process? on page 67.](#)

Do I need more than one scanning policy?

Follow these steps to determine whether to configure more than one on-access scanning policy:



How do I assign risk to a process?

Once you decide that you need more than one scanning policy, identify your processes and determine which risk to assign to each one.

- 1 Determine which processes you are using:
 - Use the Windows Task Manager or Windows Performance Monitor to help you understand which processes are using the most CPU time and memory.
 - Review the list of high-risk and low-risk processes that are defined by default. Customize this list by adding or removing processes as needed. See [Processes tab on page 76](#) for more information.
- 2 Determine which program is responsible for each process. Remember that only the child processes of the defined parent process adhere to the scanning policy. For example, if you define the Microsoft Word executable file, WINWORD.EXE, as a high-risk process, any Microsoft Word documents that are accessed would be scanned according to the high-risk scanning policy. However, when the parent process Microsoft Word is launched, the WINWORD.EXE file is scanned according to the policy of the process that launched it.
- 3 Determine which risk applies to each process using these guidelines:
 - Low-risk — Processes with less possibility of spreading or introducing a potential threat. These can be processes that access many files, but in a way that has a lower risk of spreading potential threats. For example:

Backup software

Compiling processes
 - High-risk — Processes with a greater possibility of spreading or introducing a potential threat. For example:

Processes that launch other processes, such as Microsoft Windows Explorer or the command prompt.

Processes that execute scripts or macros, such as WINWORD or CSCRIPT.

Processes used for downloading from the internet, such as browsers, instant messengers, or mail clients.
 - Default — Any process not defined as low-risk or high-risk.

Configuring on-access scan properties

The on-access scan properties are separated into two types:

- [General settings on page 68.](#)
- [Process settings on page 75.](#)

General settings

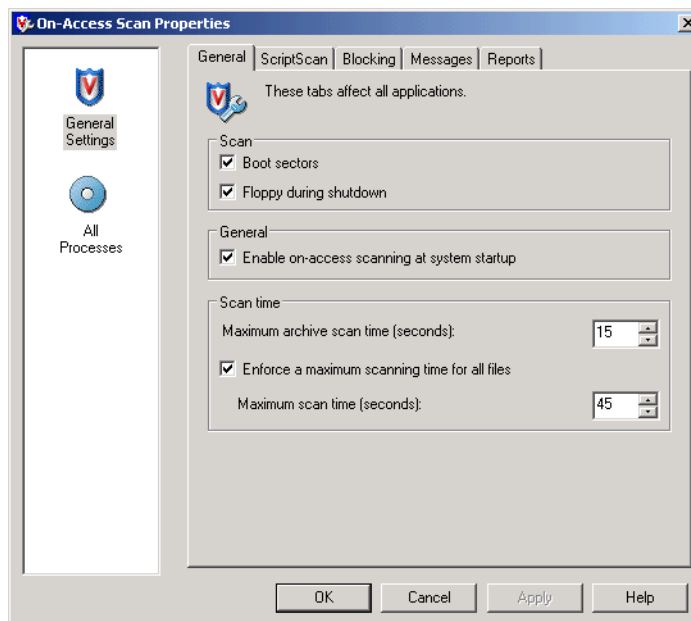
From the VirusScan Console, open the On-Access Scan Properties dialog box, then select General Settings in the left pane.

Tab or Button	Options or Actions
General tab	■ Scan boot sectors and/or floppy drives during shutdown. ■ Enable on-access scanning at system startup. ■ Maximum scan time for archives and all files.
ScriptScan tab	■ Enable scanning of scripts.
Blocking tab	■ Send a message when a remote computer writes a threat to this system and specify the message. ■ Block the connection when a remote computer writes a threat to this system. ■ Unblock the connection after the specified time. ■ Block the connection when a remote computer writes an unwanted program to this system.
Messages tab	■ Display the messages dialog box to local users when a detection occurs and specify the message. ■ Configure which actions users without administrative rights can take on messages.
Reports tab	■ Enable activity logging. ■ Specify the log file name and location. ■ Specify the log file size limit. ■ Select the log file format. ■ Specify what to log besides scanning activity. ■ View the log file.

General tab

Configure general options.

Figure 7-1 On-Access Scan Properties — General tab

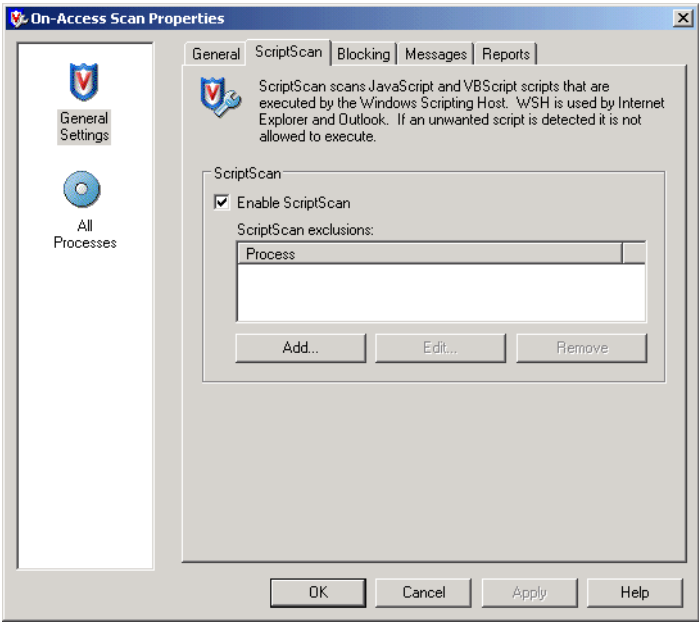


Option or Button	Description
Boot sectors	Scan boot sectors.
Floppy during shutdown	Scan floppy drives when the computer is shut down.
Enable on-access scanning at system startup	Enable the on-access scanner each time you start your computer.
Maximum archive scan time (seconds)	Specify the maximum archive and scanning time, in seconds, for all files. The time you select for the archive scan must be less than the time you select for scanning all files. Notes and Tips - Default = 15 seconds. - If a scan exceeds the time limit, the scan stops cleanly and logs a message. If the scan cannot be stopped cleanly, it terminates and starts again on the next scan.
Enforce a maximum scanning time for all files	Define a maximum scanning time and enforce it for all files.
Maximum scan time (seconds)	Accept the default or select the maximum number of seconds the scanner should spend scanning a file. Notes and Tips Default = 45 seconds.

ScriptScan tab

Prevent unwanted scripts from executing.

Figure 7-2 On-Access Scan Properties — ScriptScan tab

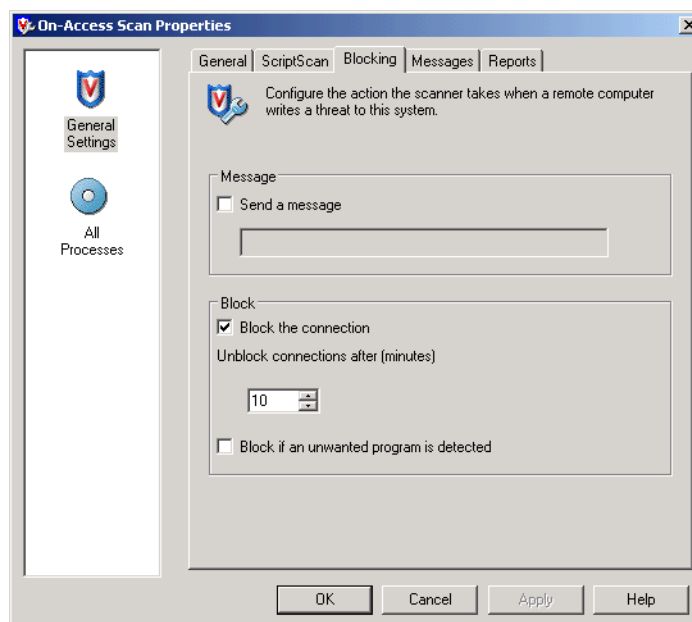


Option or Button	Description
Enable ScriptScan	Scan JavaScript and VBScript scripts before they are executed.
ScriptScan Exclusions	Specify ScriptScan exclusions by process name. Notes and Tips Wildcards are not allowed when specifying process names.

Blocking tab

Block connections from remote computers that have files with potential threats or unwanted programs in a shared folder.

Figure 7-3 On-Access Scan Properties — Blocking tab

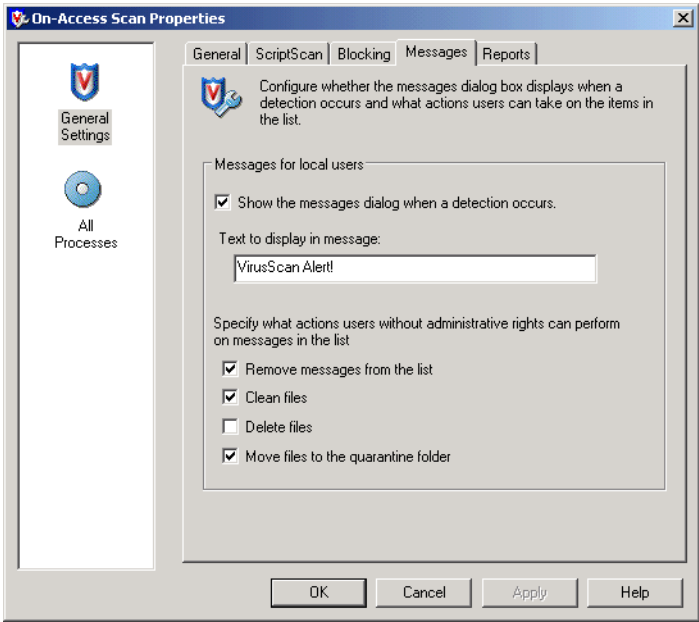


Option or Button	Description
Send a message	Notify the network user on the remote computer when a threat is detected. Type a custom message in the text box. Notes and Tips The Windows Messenger service must be running on the remote computer to receive this message.
Block the connection	Blocks the connection to any network user on a remote computer who attempts to read from, or write to, a threatened file in the shared folder. Notes and Tips The On-Access Scan Statistics dialog box displays a list of blocked computers.
Unblock the connection after (minutes)	Unlocks the connection after the specified number of minutes. Enter a number between 1 and 9999. Notes and Tips <i>Default = 10 minutes.</i>
Block if an unwanted program is detected	Blocks the connection to any user on a remote computer who attempts to write an unwanted program to the computer.

Messages tab

Configure message options for local users and users without administrative rights.

Figure 7-4 On-Access Scan Properties — Messages tab

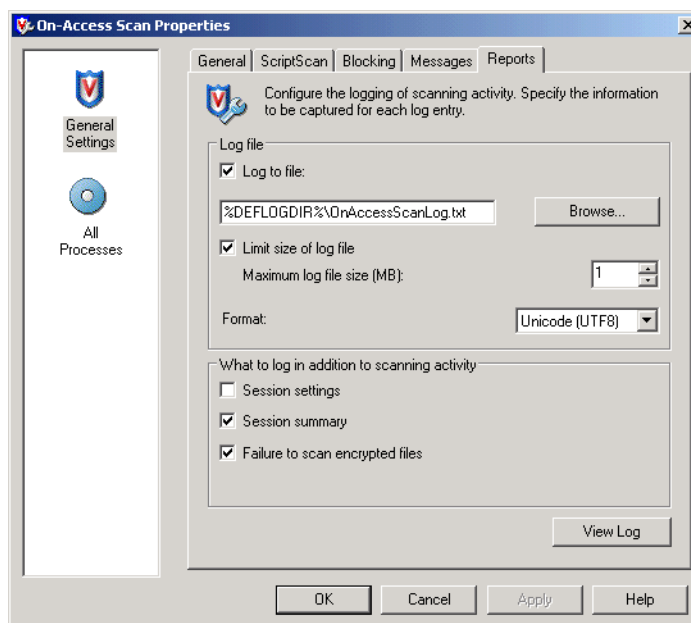


Option or Button	Description
Show the messages dialog box when a detection occurs	Display the On-Access Scan Messages dialog box to local users when a detection occurs.
Text to display in message	Accept the default message or type a custom message. Notes and Tips Default = VirusScan Alert!
Remove messages from the list	Allow users without administrator rights to delete messages from the list.
Clean files	Allow users without administrator rights to clean files referenced by the messages in the list.
Delete files	Allow users without administrator rights to delete files referenced by the messages in the list.

Reports tab

Configure activity log information.

Figure 7-5 On-Access Scan Properties — Reports tab



Option or Button	Description
Log to file	Record on-access scanning activity in a log file. Accept the default location for the file or browse to a new location. The default log name is ONACCESSSCANLOG.TXT. The default location is: <pre><drive>:\Documents and Settings\All Users\Application Data\McAfee\DesktopProtection\</pre> Notes and Tips ■ The log file can track activity on your network and note which settings you used to detect and respond to any potential threat that the scanner found. The recorded information helps determine which files you need to either replace from backup copies or delete. ■ The default location depends on which operating system you are using.
Limit size of log file	Restrict the log file to the size you specify. Notes and Tips If the data in the log file exceeds the file size you set, the oldest 20 percent of the entries are deleted and new data is appended to the file.
Maximum log file size	Specify the maximum size for the log file. Notes and Tips Accept the default size (1MB) or set a size from 1MB to 999MB.

Option or Button	Description
Format	Select the format of the log file: ■ Unicode (UTF8) ■ Unicode (UTF16) ■ ANSI  Notes and Tips ■ <i>Default = Unicode (UTF8).</i> ■ The format you choose depends on the information you are storing. If you are storing western text (every character is one byte), we recommend using the ANSI format. If you are storing eastern text (every character is one or two bytes), or sharing information within a multi-national organization, we recommend using one of the Unicode formats.
Session settings	Record the properties for each scanning session in the log file.
Session summary	Record a summary of the scanner's actions during each scanning session in the log file.  Notes and Tips Summary information includes the number of files scanned, the number and type of detections, the number of files cleaned or deleted, and other information.
Failure to scan encrypted files	Record the name of encrypted files that the scanner failed to scan.
View Log	View the existing log file.

Process settings

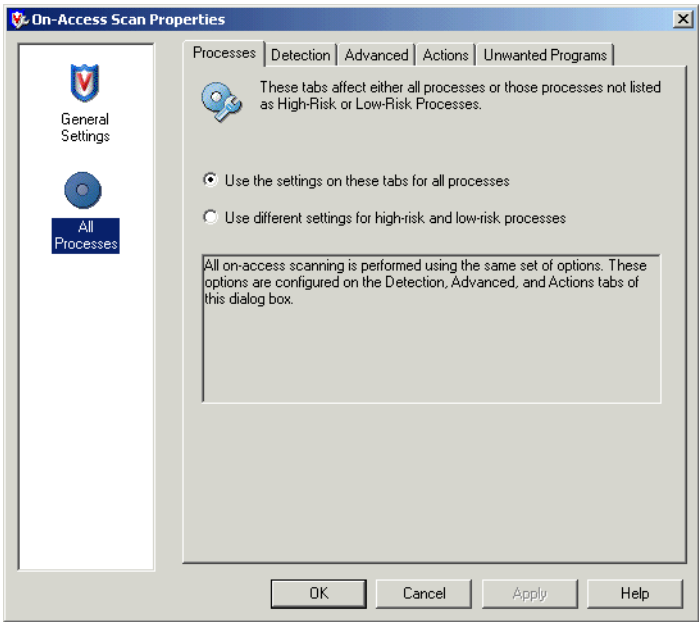
From the VirusScan Console, open the On-Access Scan Properties dialog box, then select All Processes in the left pane.

Tab or Button	Options or Actions
<i>Processes tab</i>	Choose to either: ■ Configure one scanning policy for all processes. ■ Configure different scanning policies for default, low-risk, and high-risk processes.
<i>Detection tab</i>	■ Configure whether to scan files on read, on write, or on network drives. ■ Configure which files and file types to scan. ■ Configure which disks, files, and folders to exclude from scanning.
<i>Advanced tab</i>	■ Scan for potential threats that resemble unwanted programs, Trojans, and macro viruses. ■ Scan inside archives and decode MIME encoded files. ■ Scan files opened for backup operations.
<i>Actions tab</i>	■ Primary action to take when a threat is detected. ■ Secondary action to take if the first action fails.
<i>Unwanted Programs tab</i>	■ Enable on-access scanning for unwanted programs. ■ Primary action to take when an unwanted program is detected. ■ Secondary action to take if the first action fails.

Processes tab

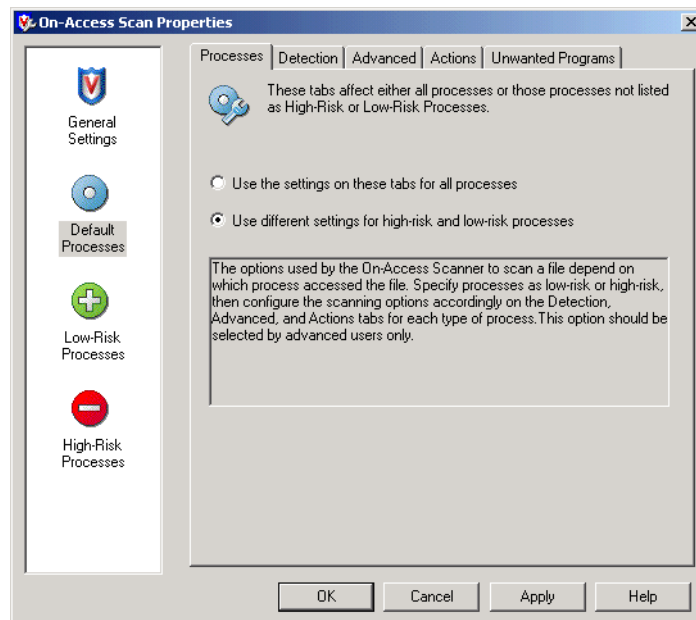
Configure one scanning policy for all processes or different scanning policies for default, low-risk and high-risk processes.

Figure 7-6 On-Access Scan Properties — All Processes



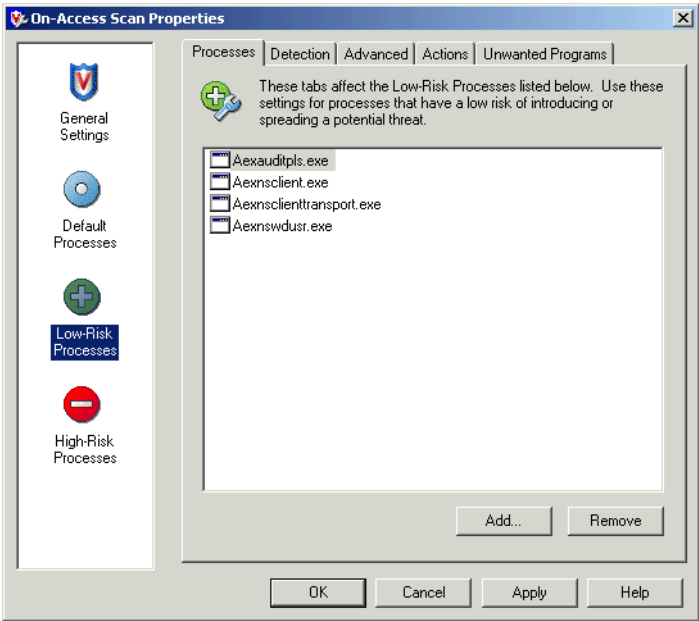
Option or Button	Description
Use the settings on these tabs for all processes	Configure one scanning policy for all processes.
Use different settings for high-risk and low-risk processes	Configure different scanning policies for high-risk, low-risk, and default processes. Notes and Tips ■ Before you select this option, the All Processes icon appears in the left pane. After you select this option the Default Processes, Low-Risk Processes, and High-Risk Processes icons appear in the left pane. ■ See How do I know when to assign high-risk or low-risk to processes? on page 65.

Figure 7-7 On-Access Scan Properties — Default processes



Option or Button	Description
Default Processes	Select the Default Processes icon to configure the scanning policy for processes that are not defined as low-risk or high-risk.

Figure 7-8 On-Access Scan Properties — Low-risk or high-risk processes

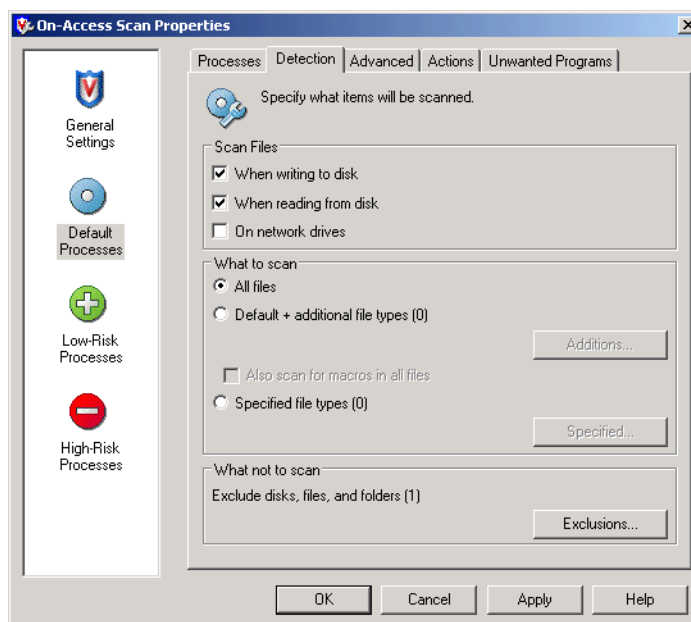


Option or Button	Description
Low-Risk Processes	Select the Low-Risk Processes icon to configure the scanning policy for processes that you identify as low-risk. ■ Review the default list of processes. ■ Click Add to include new processes in the list. ■ Click Remove to delete processes from the list.
High-Risk Processes	Select the High-Risk Processes icon to configure the scanning policy for processes that you identify as high-risk. ■ Review the default list of processes. ■ Click Add to include new processes in the list. ■ Click Remove to delete processes from the list.  Notes and Tips ■ The high-risk scanning policy is initially set the same as default processes to ensure that high-risk processes are scanned in depth. ■ The high-risk scanning policy is configured by default to give you the maximum protection. We do not recommend reducing the default level of scanning.

Detection tab

Configure detection options. If you are configuring different scanning policies for default, low-risk, and high-risk processes, the options on this tab must be configured for each process type.

Figure 7-9 On-Access Scan Properties — Detection tab



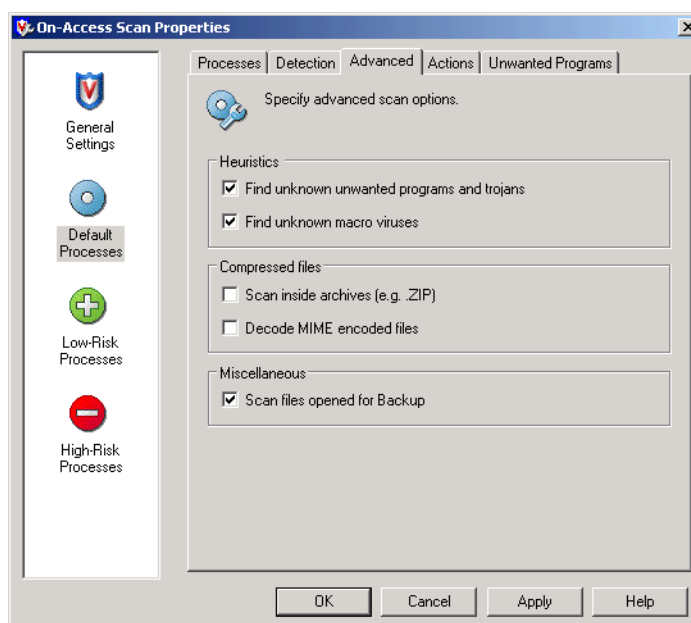
Option or Button	Description
When writing to disk	Scan all files as they are written to or modified on the computer or other data storage device.  Notes and Tips If you are copying or moving files from one computer to another, it is important that all computers be configured identically so that a file with a potential threat can't be copied from or written to a computer.
When reading from disk	Scan all files as they are read from the computer or other data storage device.
On network drives	Scan resources on mapped network drives.  Notes and Tips Scanning network resources might affect performance.
All files	Scan all files regardless of extension.
Default + additional file types	Scan the default list of extensions plus any additions you specify. The default list is defined by the current DAT file. ■ Select Default + additional file types. ■ Click Additions to open the Additional File Types dialog box.  Notes and Tips You cannot delete file types from the Scanned by default list. To exclude file types from this list, use the Exclusions feature.
Also scan for macros in all files	If you selected Default + additional file types , you can also search for known macro threats in all files.

Option or Button	Description
Specified file types	Create a list of user-specified extensions to be scanned. You can also remove any extensions you added previously. ■ Select Specified file types. ■ Click Specified to open the Specified File Types dialog box.  Notes and Tips See Specifying user-defined file types on page 149 for more information.
Exclude disks, files, and folders	Create a list of files, folders, and drives to exclude from scanning. You can also remove exclusions that you previously specified. Click Exclusions to open the Set Exclusions dialog box.  Notes and Tips See Excluding files, folders and drives on page 150 for more information.

Advanced tab

Configure heuristic scanning and scanning of compressed files and those opened for backup. If you are configuring different scanning policies for default, low-risk, and high-risk processes, the options on this tab must be configured for each process type.

Figure 7-10 On-Access Scan Properties — Advanced tab



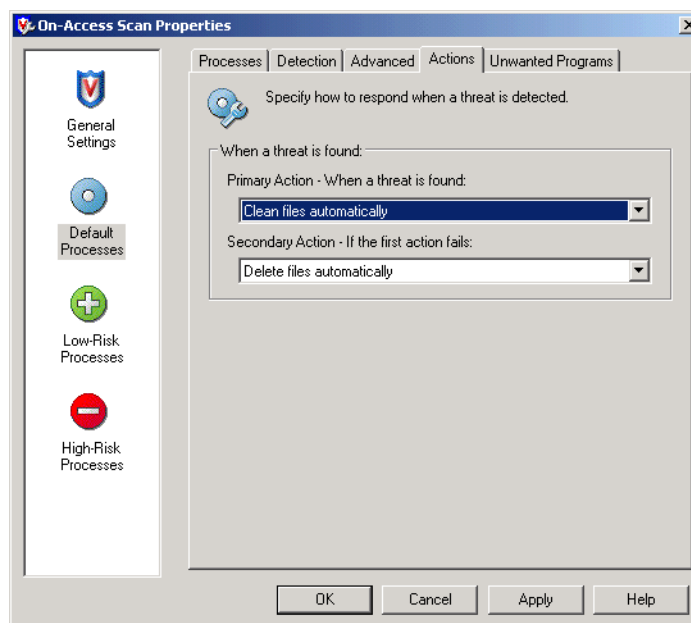
Option or Button	Description
Find unknown programs and trojans	Use heuristic scanning to detect executable files that have code resembling malware.
Find unknown macro viruses	Use heuristic scanning to detect unknown macro viruses.

Option or Button	Description
Scan inside archives	Examine archive (compressed) files and their contents.  Notes and Tips Although it provides better protection, scanning compressed files can increase the time required to perform a scan.
Decode MIME encoded files	Detect, decode, and scan Multipurpose Internet Mail Extensions (MIME) encoded files.
Scan files opened for Backup	Examine files that are open for backup operations.

Actions tab

Configure which actions to take when a threat is detected. If you are configuring different scanning policies for default, low-risk, and high-risk processes, the options on this tab must be configured for each process type

Figure 7-11 On-Access Scan Properties – Actions tab

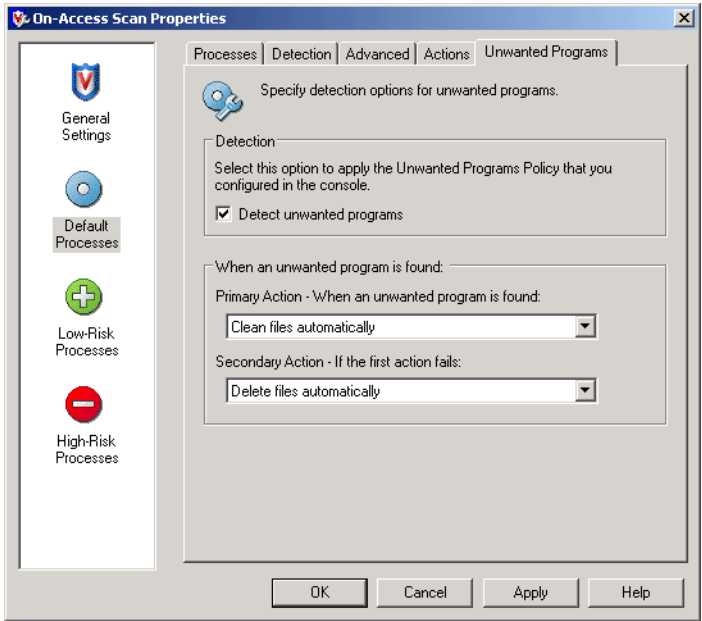


Option or Button	Description
Primary Action	Select the first action that you want the scanner to take when a threat is detected. ■ Clean files automatically — The scanner tries to remove the threat from the detected file. ■ Deny access to files — Deny all users access to any files with potential threats that the scanner finds. ■ Delete files automatically — The scanner deletes files with potential threats as soon as it detects them.  Notes and Tips ■ <i>Default = Clean files automatically.</i> ■ The action that is actually taken depends on how it is defined in the DAT file. For example, if the scanner cannot clean a file or if the file has been damaged beyond repair, the scanner may delete the file or take the secondary action, depending on how it was defined in the DAT file. ■ When the scanner denies access to files with potential threats, it also appends the filename with an .mcm extension, when the file is saved.
Secondary Action	Select the next action you want the scanner to take if the first action fails. ■ Deny access to files — Deny all users access to any files with potential threats that the scanner finds. ■ Delete files automatically — The scanner deletes files with potential threats as soon as it detects them.  Notes and Tips <i>Default = Delete files automatically.</i>

Unwanted Programs tab

Enable unwanted program detection and which actions are taken when detections occur. If you are configuring different scanning policies for default, low-risk, and high-risk processes, the options on this tab must be configured for each process type.

Figure 7-12 On-Access Scan Properties — Unwanted Programs tab



Option or Button	Description
Detect unwanted programs	Enables the on-access scanner to detect potentially unwanted programs.  Notes and Tips The on-access scanner uses the information you configured in the Unwanted Programs Policy to detect potentially unwanted programs. See Unwanted Programs Policy on page 36 .

Option or Button	Description
Primary Action	Select the first action that you want the scanner to take when a potentially unwanted program is detected. ■ Allow access to files — Give users access to detected files and/or programs. ■ Clean files automatically — Remove the threat from detected files and/or programs automatically. ■ Deny access to files — Prevent users from accessing detected files and/or programs. ■ Delete files automatically — Remove detected files and/or programs automatically.  Notes and Tips ■ <i>Default = Clean files automatically.</i> ■ Allow access to files is useful to monitor what is being detected before you decide which actions to take. Review the activity log to see which programs are being detected. No secondary action is allowed for this option.
Secondary Action	Select the next action you want the scanner to take if the first action fails. ■ Allow access to files — Give users access to detected files and/or programs. ■ Deny access to files — Prevent users from accessing detected files and/or programs. ■ Delete files automatically — Remove detected files and/or programs automatically.  Notes and Tips <i>Default = Delete files automatically.</i>

8

On-Demand Scanner

This section describes:

- [About on-demand scanning.](#)
- [Creating on-demand scan tasks on page 88.](#)
- [Configuring on-demand scan properties on page 88.](#)
- [Running on-demand scans on page 98.](#)

About on-demand scanning

The on-demand scanner provides a method for scanning all parts of your computer for potential threats, at convenient times or at regular intervals. Use on-demand scans to supplement the continuous protection that the on-access scanner offers, or to schedule regular scans when they do not interfere with your work.

- [What types of on-demand scan tasks can I use? on page 86](#)
- [What methods of on-demand scanning are used? on page 86.](#)
- [How is scan progress determined? on page 86.](#)
- [How does scanning of remote storage work? on page 87.](#)
- [How does system utilization work? on page 87.](#)

What types of on-demand scan tasks can I use?

This section describes the three types of on-demand scan tasks.

Full Scan task

Use this task to perform regular scheduled scans of your system. The default task is configured to scan system memory for installed rootkits and hidden processes, memory of all running processes, and all local drives physically connected to your computer. It can be used with default settings or you can configure it. You can create as many other on-demand scan tasks as you need.

One-time unsaved scan

Use this task when you need to scan an item quickly, but you want to configure the task settings.



You can configure and **Start** this task, but unless you save it, the task is discarded when you close the **On-Demand Scan Properties** dialog box. To save the task, click **Save As** in the **On-Demand Scan Properties** dialog box.

Right-click scan

Use this task to immediately scan a file or folder that you suspect is threatened.

From Windows Explorer, right-click a file or folder, then select **Scan for threats**.



This scan task cannot be configured. All scan settings are enabled by default.

See [Right-click features on page 145](#) for more information.

What methods of on-demand scanning are used?

The on-demand scanner uses these two methods of scanning:

In memory process scanning

This method examines all active processes prior to running the on-demand scan task. A detected potentially unwanted process is highlighted and the process is stopped. This means that a single pass with the on-demand scanner removes all instances of a potentially unwanted program.

Incremental or resumable scanning

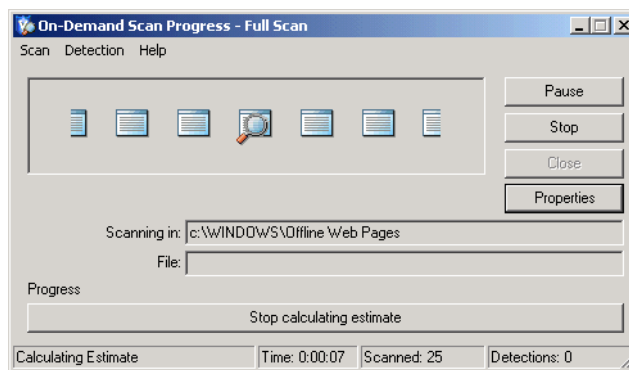
This method allows the scanner to start where it last left off. For a scan where you scheduled a start and stop time or a time limit, the scan stops when the time limit is reached. On the next scheduled scan, the on-demand scan continues from the point in the file and folder structure where the previous scan stopped.

How is scan progress determined?

Before the scanner begins the scan process, it automatically calculates the estimated amount of time this task will take. The progress is based on this estimate.

You can allow the scanner to complete the estimate calculation before starting the scan or stop the estimate which starts the scan immediately.

Figure 8-1 On-Demand Scan — Calculate estimate



Option or Button	Description
Stop calculating estimate	Stop the estimate calculation and start the scan immediately.  Notes and Tips This toggles between Stop calculating estimate and Calculate estimate.
Calculate estimate	Restart the estimate calculation. The scan starts automatically when the estimate is complete.  Notes and Tips This toggles between Calculate estimate and Stop calculating estimate.

How does scanning of remote storage work?

Remote Storage data storage is hierarchical, with two defined levels. The upper level, local storage, includes the NTFS disk volumes of the computer running Remote Storage on Windows 2000 Server. The lower level, remote storage, is located on the robotic tape library or stand-alone tape drive that is connected to the server computer.

Remote Storage automatically copies eligible files on your local volumes to a tape library, then monitors space available on the local volumes. File data is cached locally so that it can be accessed quickly as needed. When necessary, Remote Storage moves data from the local storage to remote storage. When you need to access a file on a volume managed by Remote Storage, open the file as usual. If the data for the file is no longer cached on your local volume, Remote Storage recalls the data from a tape library.

How does system utilization work?

When an on-demand scan starts, CPU and IO samples are taken over the first 30 seconds, then the scan is performed based on the utilization level you specified.

The system utilization you specify does not apply to encrypted files. The decryption is done by LSASS.EXE, not by the SCAN32 process. Scanning encrypted files is CPU intensive, therefore even if the system limit on the scanning thread is low, it is still scanning files fast enough that LSASS.EXE must keep busy to supply the decrypted data.

Creating on-demand scan tasks

You can use the default **Full Scan** task and create as many other tasks as you need.

To create a new on-demand scan task:

- From the VirusScan Console, select **Task | New On-Demand Scan**.
- Use the **Copy** and **Paste** commands to copy an existing task.

To create a one-time unsaved scan task:

- Right-click  in the system tray and select **On-Demand Scan**.
- Select **Start | Programs | McAfee | On-Demand Scan**.

Configuring on-demand scan properties

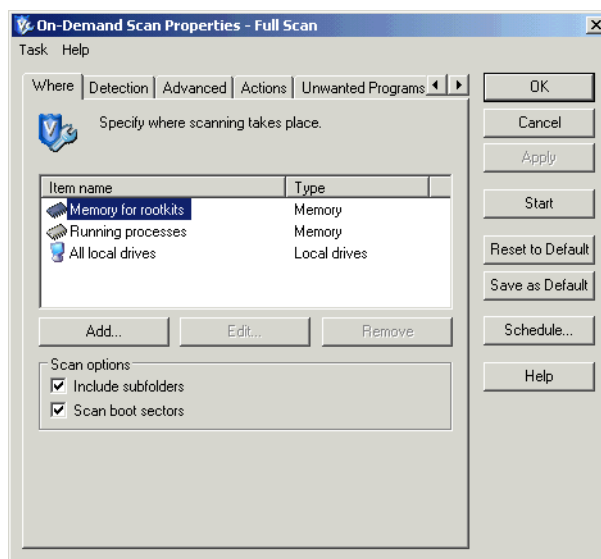
From the VirusScan Console, open the **On-Demand Scan Properties** dialog box.

Tab or Button	Options or Actions
Where tab	■ Specify which items to scan. ■ Include subfolders when scanning. ■ Include boot sectors when scanning.
Detection tab	■ Configure which files and file types to scan. ■ Configure which disks, files, and folders to exclude from scanning. ■ Scan inside archives and decode MIME encoded files.
Advanced tab	■ Scan for potential threats that resemble unwanted programs, Trojans, and macro viruses. ■ Scan files that have been backed up to storage. ■ Specify the system utilization percentage.
Actions tab	■ Primary action to take when a threat is detected. ■ Secondary action to take if the first action fails. ■ Specify which actions are allowed in the prompt dialog box.
Unwanted Programs tab	■ Enable on-demand scanning for unwanted programs. ■ Primary action to take when an unwanted program is detected. ■ Secondary action to take if the first action fails.
Reports tab	■ Enable activity logging. ■ Specify the log file name and location. ■ Specify the log file size limit. ■ Select the log file format. ■ Specify what to log besides scanning activity. ■ View the log file.
Start	Start this on-demand scan task now.
Reset to Default	Restore the default scan settings.
Save as Default	Save the current scanning configuration as the default configuration. All new tasks are created using this configuration.
Schedule	Schedule this task to run at specific dates and times, or intervals. See Scheduling Tasks on page 153 for more information.

Where tab

Configure the item types and locations to scan.

Figure 8-2 On-Demand Scan Properties — Where tab

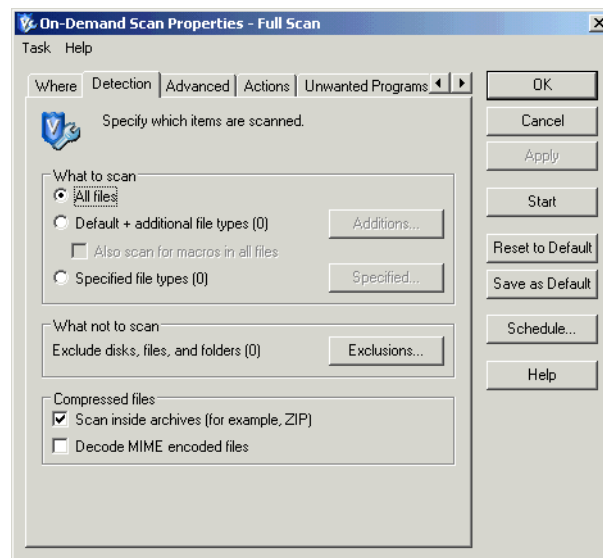


Option or Button	Description
Item Name	Select the items to scan. Click Add, Edit, or Remove to change the items in the list. ■ Memory for rootkits. Scans system memory for installed rootkits, hidden processes and other behavior that suggests malicious code is attempting to hide itself. This scan occurs before all other scans. ■ Running processes. Scans the memory of all running processes. Actions other than Clean are treated as Continue scanning. ■ Registered Files. Scans all files that are registered. The scanner first searches the registry for file names, then scans the files. The scanner removes references to potentially unwanted files from the registry. ■ My computer. Scans all drives physically attached to your computer or logically mapped to a drive letter on your computer. ■ All local drives. Scans all drives and their subfolders on your computer. ■ All fixed drives. Scans all drives physically connected to your computer. ■ All removable drives. Scans all removable drives or other storage devices connected to your computer. ■ All mapped drives. Scans network drives logically mapped to a network drive on your computer. ■ Home folder. Scans the home folder of the user who starts the scan. ■ User Profile folder. Scans the profile of the user who starts the scan, including the user's My Documents folder. ■ Windows folder. Scans the contents of the Windows folder. ■ Program Files folder. Scans the contents of the Program Files folder. ■ Temp folder. Scans the contents of the Temp folder. ■ Recycle bin. Scans the contents of the recycle bin. ■ Drive or folder. Scans the specified drive or folder. ■ File. Scans the specified file.  Notes and Tips ■ <i>Default = Memory for rootkits, running processes, and all local drives.</i> ■ Using the default list of scan items can result in a thorough scan that is very time consuming. Consider whether you want to narrow the scope of this scan for regular use.
Type	The type of scan for the selected item.
Include subfolders	The scanner examines all subfolders in the specified volumes. Deselect this option to scan only the root level of the volumes.
Scan boot sectors	The scanner examines the disk boot sector.  Notes and Tips It may be appropriate to disable boot sector analysis when a disk contains a unique or abnormal boot sector that cannot be scanned.

Detection tab

Configure detection options.

Figure 8-3 On-Demand Scan Properties — Detection tab



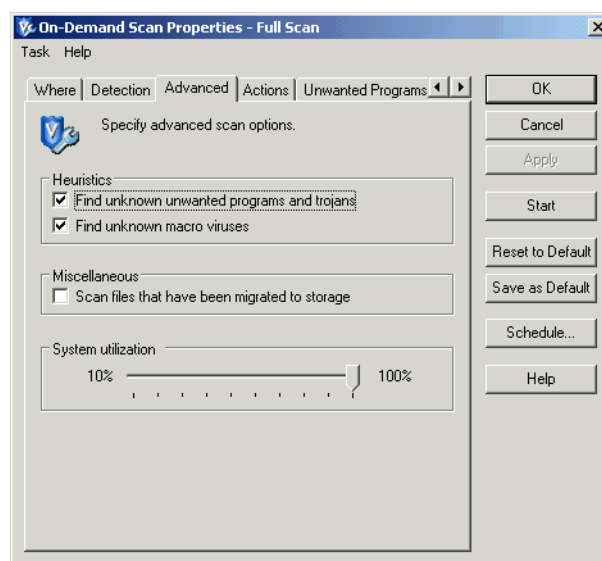
Option or Button	Description
All files	Scan all files, regardless of extension.
Default + additional file types	Scan the default list of extensions plus any additions you specify. The default list is defined by the current DAT file. ■ Select Default + additional file types. ■ Click Additions to open the Additional File Types dialog box. Notes and Tips ■ You cannot delete file types from the Scanned by default list. To exclude file types from this list, use the Exclusions feature. ■ See Adding file type extensions on page 148 for more information.
Specified file types	Create a list of user-specified extensions to be scanned. You can also remove any extensions you added previously. ■ Select Specified file types. ■ Click Specified to open the Specified File Types dialog box. Notes and Tips See Specifying user-defined file types on page 149 for more information.
Exclude disks, files, and folders	Create a list of files, folders, and drives to exclude from scanning. You can also remove exclusions that you previously specified. Click Exclusions to open the Set Exclusions dialog box. Notes and Tips See Excluding files, folders and drives on page 150 for more information.

Option or Button	Description
Scan inside archives	Examine archive (compressed) files and their contents.  Notes and Tips Although it provides better protection, scanning compressed files can increase the amount of time required to perform a scanning activity.
Decode MIME encoded files	Detect, decode, and scan Multipurpose Internet Mail Extensions (MIME) encoded files.

Advanced tab

Configure scanning of code resembling unwanted programs or malware, scanning of stored files, and specify the percentage of system utilization.

Figure 8-4 On-Demand Scan Properties— Advanced tab

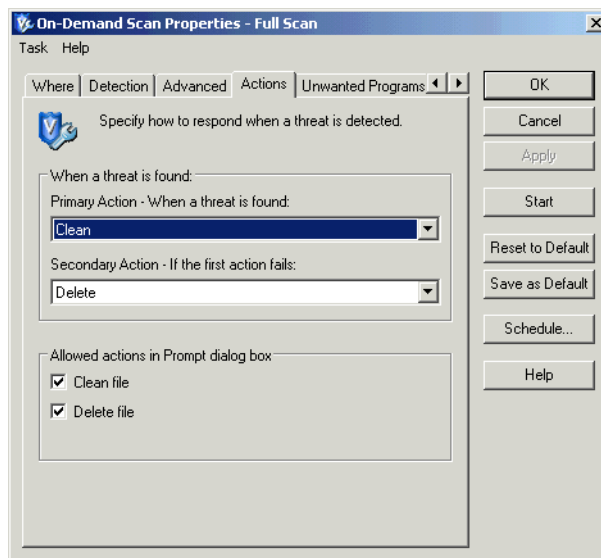


Option or Button	Description
Find unknown unwanted programs and trojans	Use heuristic scanning to detect executable files that have code resembling a potentially unwanted program or trojan.
Find unknown macro viruses	Use heuristic scanning to detect unknown macro viruses.
Scan files that have been migrated to storage	Scans cached files stored on Remote Storage.  Notes and Tips See How does scanning of remote storage work? on page 87 .
System utilization	Use the slider to set the utilization level for the scan. Each task runs independently; unaware of the limits for other tasks.  Notes and Tips - Default = 100%. - See How does system utilization work? on page 87.

Actions tab

Configure which actions to take when a threat is detected.

Figure 8-5 On-Demand Scan Properties – Actions tab

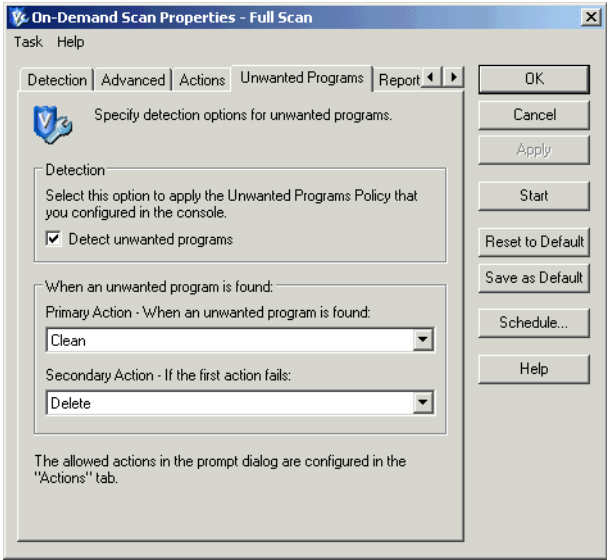


Option or Button	Description
Primary Action	Select the first action that you want the scanner to take when a threat is detected. ■ Clean — The scanner tries to remove the threat from the detected file. ■ Prompt for action — Prompt the user for action when a threat is detected. Select this option, then specify which actions users can take under Allowed action in Prompt dialog box. No secondary action is allowed for this option. ■ Continue scanning — Continue scanning when a file is detected. No secondary action is allowed for this option. ■ Delete — The scanner deletes files with potential threats as soon as it detects them.  Notes and Tips ■ <i>Default = Clean.</i> ■ The action that is actually taken depends on how it is defined in the DAT file. For example, if the scanner cannot clean a file or if the file has been damaged beyond repair, the scanner may delete the file or take the secondary action, depending on how it was defined in the DAT file. ■ If the action is set to delete and a file within an archive is detected, the entire archive file is deleted. ■ When the scanner denies access to files with potential threats, it also appends the filename with an .mcm extension, when the file is saved. ■ When Prompt for action is selected for a scheduled on-demand scan task, the Continue action is taken instead. This substitution occurs because scheduled on-demand scans may run at a time when no one is present to respond to the prompt.
Secondary Action	Select the next action you want the scanner to take if the first action fails. ■ Prompt for action — Prompt the user for action when a threat is detected. Select this option, then specify which actions users can take under Allowed action in Prompt dialog box. ■ Continue scanning — Continue scanning when a file is detected. ■ Delete — The scanner deletes files with potential threats as soon as it detects them.  Notes and Tips ■ <i>Default = Delete.</i> ■ When Prompt for action is selected for a scheduled on-demand scan task, the Continue action is taken instead. This substitution occurs because scheduled on-demand scans may run at a time when no one is present to respond to the prompt.
Allowed actions in Prompt dialog box	Select the actions that are allowed when the user is prompted for action. ■ Clean file — The scanner tries to remove the threat from the detected file. ■ Delete file — The scanner deletes files with potential threats as soon as it detects them.

Unwanted Programs tab

Enable unwanted program detection and which actions are taken when detections occur.

Figure 8-6 On-Demand Scan Properties — Unwanted Programs tab



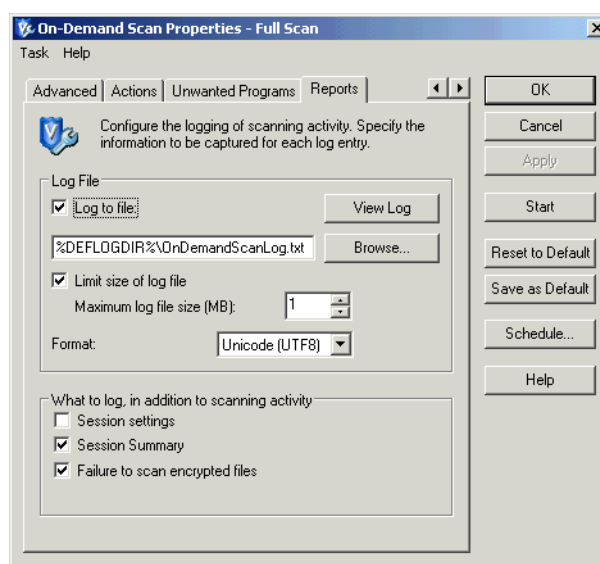
Option or Button	Description
Detect unwanted programs	Enables the on-demand scanning for potentially unwanted programs.  Notes and Tips The on-demand scanner uses the information you configured in the Unwanted Programs Policy to detect potentially unwanted programs. See Unwanted Programs Policy on page 36.

Option or Button	Description
Primary Action	Select the first action that you want the scanner to take when a threat is detected. ■ Clean — The scanner tries to remove the threat from the detected file. ■ Prompt for action — Prompt the user for action when a threat is detected. Select this option, then specify which actions users can take under Allowed action in Prompt dialog box. No secondary action is allowed for this option. ■ Continue scanning — Continue scanning when a file is detected. No secondary action is allowed for this option. ■ Delete — The scanner deletes files with potential threats as soon as it detects them.  Notes and Tips <i>Default = Clean.</i>
Secondary Action	Select the next action you want the scanner to take if the first action fails. ■ Prompt for action — Prompt the user for action when a threat is detected. Select this option, then specify which actions users can take under Allowed action in Prompt dialog box. ■ Continue scanning — Continue scanning when a file is detected. ■ Delete — The scanner deletes files with potential threats as soon as it detects them.  Notes and Tips <i>Default = Delete.</i>

Reports tab

Configure activity log information.

Figure 8-7 On-Demand Scan Properties — Reports tab



Option or Button	Description
Log to file	Record on-demand scanning activity in a log file. Accept the default location for the file or browse to a new location. The default log name is ONDEMANDSCANLOG.TXT. The default location is <drive>:\Documents and Settings\All Users\Application Data\McAfee\DesktopProtection\  Notes and Tips ■ The log file can track activity on your network and note which settings you used to detect and respond to any potential threat that the scanner found. The recorded information helps determine which files you need to either replace from backup copies or delete. ■ The default location depends on which operating system you are using.
Limit size of log file	Restrict the log file to the size you specify.  Notes and Tips If the data in the log file exceeds the file size you set, the oldest 20 percent of the log file entries are deleted and new data is appended to the file.
Maximum log file size	Specify the maximum size for the log file.  Notes and Tips Accept the default size (1MB) or set a size from 1MB to 999MB.
Format	Select the format of the log file: ■ Unicode (UTF8) ■ Unicode (UTF16) ■ ANSI  Notes and Tips ■ <i>Default = Unicode (UTF8).</i> ■ The format you choose depends on the information you are storing. If you are storing western text (every character is one byte), we recommend using the ANSI format. If you are storing eastern text (every character is one or two bytes), or sharing information within a multi-national organization, we recommend using one of the Unicode formats.
Session settings	Record the properties for each scanning session in the log file.
Session summary	Record a summary of the scanner's actions during each scanning session in the log file.  Notes and Tips Summary information includes the number of files scanned, the number and type of detections, the number of files cleaned or deleted, and other information.
Failure to scan encrypted files	Record the name of encrypted files that the scanner failed to scan.
View Log	View the existing log file.

Running on-demand scans

Once you have configured an on-demand scan task, there are two ways to run the task.

Scan as scheduled

A scheduled scan automatically runs according to the schedule you specified. This scan is not visible while it is running unless you choose to view its progress.

Use one of these methods to view the scheduled scan progress:

- Right-click the task in the **VirusScan Console** and select **Show Progress**.
- Open the **On-Demand Scan Properties** dialog box and click **Progress**.



For the scanner to run your task, your computer must be active. If your computer is down when the task is scheduled to start, the task starts at the next scheduled time if the computer is active, or when the computer starts if you selected the **Run missed task** option on the **Schedule Settings**, **Schedule** tab.

Scan immediately

Use one of these methods to start an immediate on-demand scan:

- Create a one-time unsaved on-demand scan, configure it, then click **Start**.
- From the **VirusScan Console**, right-click an existing on-demand scan and select **Start**.
- From Windows Explorer, right-click a file, folder, drive, or other item, then select **Scan for threats**.



For scans where you have scheduled a start and stop time or a time limit, the scan stops when the time limit is reached. On the next scheduled scan, the on-demand scan continues from the point in the file and folder structure where the previous scan stopped.

9

E-mail Scanners

This section describes:

- [About e-mail scanning](#)
- [Configuring e-mail scan properties on page 100.](#)
- [Running on-demand e-mail scans on page 111.](#)

About e-mail scanning

The e-mail scanner consists of two separate functional components. The first works with MAPI based e-mail, such as Microsoft Outlook. The second works with Lotus Notes. The two client scanners behave differently in some cases. These differences are described here.

What types of e-mail scanning are used?

There are two types of e-mail scanning:

On-demand e-mail scanning

When invoked, it examines e-mail messages and attachments in the user's mailbox, personal folders, or Lotus Notes databases.

- Use the on-demand e-mail scanner to supplement the protection of the on-delivery e-mail scanner. For example, if you have had Microsoft Outlook or Lotus Notes closed or you are installing the VirusScan Enterprise product for the first time, we recommend running an on-demand e-mail scan first.
- Configure and invoke the on-demand e-mail scanner from your e-mail client.
 - Microsoft Outlook — Click  in the Outlook toolbar or select **Tools | E-mail Scan Properties**. When a scan is initiated, data is downloaded from the exchange to create a local file for scanning. This applies to both attachments and message bodies if you have it configured to scan both.
 - Lotus Notes — In the toolbar, select **Actions | On-Demand Scan Properties**. Scanning is on-access; scanning across the network.

On-delivery e-mail scanning

Automatically examines e-mail messages and attachments.

- For Microsoft Outlook, e-mail is scanned on delivery.
- For Lotus Notes, e-mail is scanned when accessed.

Configuring e-mail scan properties

This section describes how to configure the **On-Demand E-mail Scan Properties** and the **On-Delivery E-mail Scan Properties**. Any configuration differences are noted where they apply. The configuration settings you specify here apply to Microsoft Outlook and Lotus Notes.

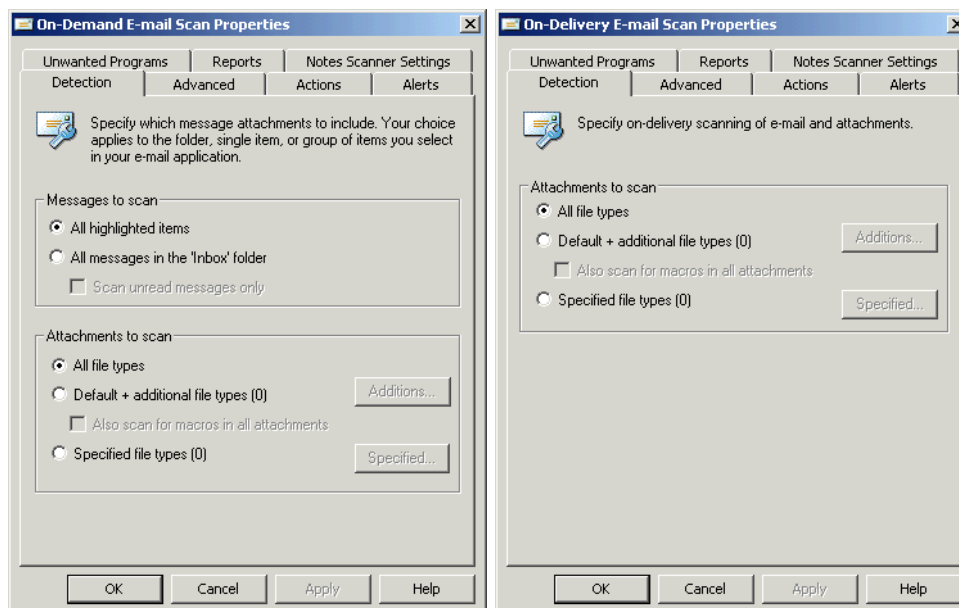
- From the e-mail client, open the **On-Demand E-mail Scan Properties** dialog box.
- From the VirusScan Console, open the **On-Delivery E-mail Scan Properties** dialog box.

Tab or Button	Options or Actions
Detection tab	■ Specify which messages and attachments to scan.
Advanced tab	■ Scan for potential threats that resemble malware. ■ Scan for unknown macro viruses. ■ Find attachments with multiple extensions. ■ Scan inside archives and decode MIME encoded files. ■ Scan e-mail message bodies.
Actions tab	■ Primary action to take when a threat is detected. ■ Secondary action to take if the first action fails.
Alerts tab	■ Notify another user when a threatened e-mail message is detected.
Unwanted Programs tab	■ Enable the e-mail scanner to scan for unwanted programs. ■ Primary action to take when an unwanted program is detected. ■ Secondary action to take if the first action fails.
Reports tab	■ Enable activity logging. ■ Specify the log file name and location. ■ Specify the log file size limit. ■ Select the log file format. ■ Specify what to log besides scanning activity. ■ View the log file.
Notes Scanner Settings tab	Specify Lotus Notes specific settings. ■ Scan all server databases. ■ Scan server mailboxes in the specified mailbox root folder. ■ Databases to ignore. ■ Notes applications to ignore.

Detection tab

Configure detection options for both the on-delivery e-mail scanner and the on-demand e-mail scanner.

Figure 9-1 On-Demand or On-Delivery Scan Properties — Detection tab



The Notes Scanner Settings tab is not available when viewing the On-Demand E-mail Scan Properties dialog box from Microsoft Outlook.

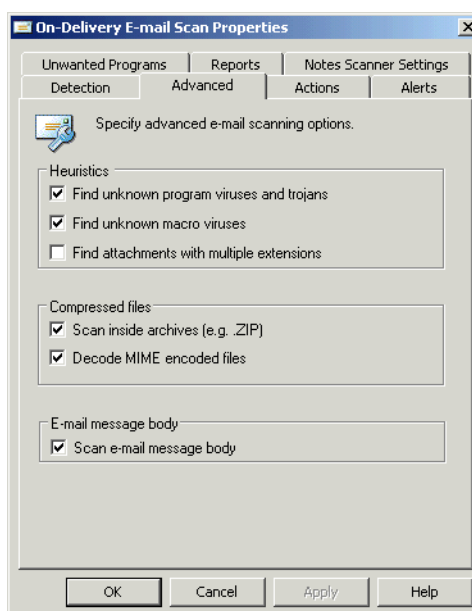
Option or Button	Description
All highlighted items	Scan selected e-mail messages and folders. This option is only available for on-demand e-mail scanning.
All messages in the Inbox folder	Scan all messages currently in the Inbox folder and its subfolders. This option is only available for on-demand e-mail scanning.
Scan unread messages only	Scan all unread messages currently in the Inbox folder and its subfolders. This option is only available for on-demand e-mail scanning.
All file types	Scan all types of files, regardless of extension.
Default + additional file types	Scan the default list of extensions plus any additions you specify. The default list is defined by the current DAT file. ■ Select Default + additional file types. ■ Click Additions to open the Additional File Types dialog box.  Notes and Tips ■ You cannot delete file types from the Scanned by default list. To exclude file types from this list, use the Exclusions feature. ■ See Adding file type extensions on page 148 for more information.

Option or Button	Description
Also scan for macro viruses in all attachments	Scan all attachments, regardless of extension, for macro viruses.
Specified file types	Create a list of user-specified extensions to be scanned. You can also remove any extensions you added previously. ■ Select Specified file types. ■ Click Specified to open the Specified File Types dialog box.  Notes and Tips See Specifying user-defined file types on page 149 for more information.

Advanced tab

Configure advanced settings for both the on-delivery e-mail scanner and the on-demand e-mail scanner.

Figure 9-2 E-mail Scan Properties — Advanced tab



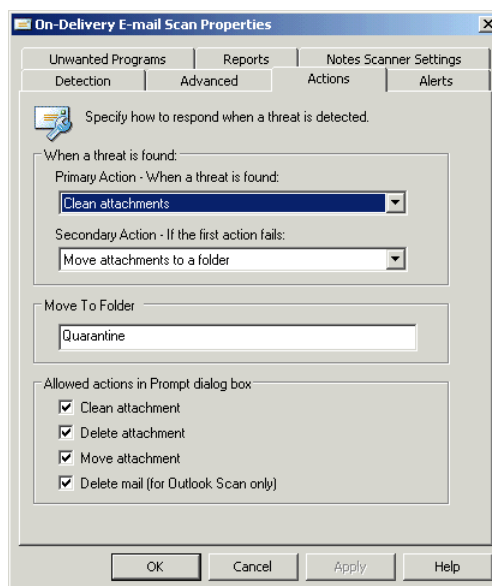
Option or Button	Description
Find unknown programs and trojans	Use heuristic scanning to detect executable files that have code resembling malware.
Find unknown macro viruses	Use heuristic scanning to detect unknown macro viruses.  Notes and Tips This option is not the same as Also scan for macro viruses in all attachments on the Detection tab, which instructs the scanner to find all known macro viruses. This option instructs the scanner to assess the probability that an unknown macro is a virus.

Option or Button	Description
Find attachments with multiple extensions	Treat attachments with multiple extensions as a threat.  Notes and Tips When you select this option, an E-mail Scan Warning dialog box appears. Click OK to confirm your selection.
Scan inside archives	Examine archive (compressed) files and their contents.  Notes and Tips Although it provides better protection, scanning compressed files can increase the amount of time required to perform a scan.
Decode MIME encoded files	Detect, decode, and scan Multipurpose Internet Mail Extensions (MIME) encoded files.
Scan e-mail message body	Scan the body of e-mail messages.  Notes and Tips This option is supported for Microsoft Outlook only.

Actions tab

Configure these action settings for both the on-delivery e-mail scanner and the on-demand e-mail scanner.

Figure 9-3 E-mail Scan Properties — Actions tab



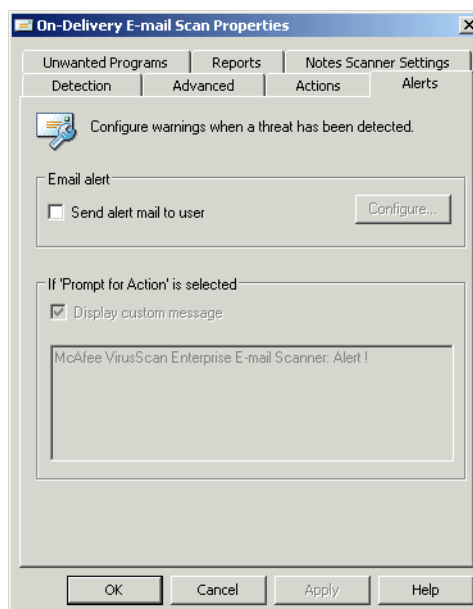
Option or Button	Description
Primary Action	Select the first action that you want the scanner to take when a threat is detected. ■ Clean attachments — The scanner tries to remove the threat from the attachment. ■ Prompt for action — Prompt the user for action when a threat is detected. Select this option, then specify which actions users can take under Allowed action in Prompt dialog box. No secondary action is allowed for this option. ■ Continue scanning — Continue scanning when an attachment with a threat is detected. No secondary action is allowed for this option. ■ Move attachments to a folder — The scanner moves attachments with potential threats to the designated folder. ■ Delete attachments — The scanner deletes attachments with potential threats as soon as it detects them. For Microsoft Outlook, the e-mail is deleted. For Lotus Notes, the attachment is deleted. ■ Delete mail (for Outlook Scan only) — The scanner deletes mail with potential threats. If you select this option as the primary action, no secondary action is allowed.  Notes and Tips ■ <i>Default = Clean attachments.</i> ■ The action that is actually taken depends on how it is defined in the DAT file. For example, if the scanner cannot clean a file or if the file has been damaged beyond repair, the scanner may delete the file or take the secondary action, depending on how it was defined in the DAT file.
Secondary Action	Select the next action you want the scanner to take if the first action fails. ■ Prompt for action — Prompt the user for action when a threat is detected. Select this option, then specify which actions users can take under Allowed action in Prompt dialog box. ■ Continue scanning — Continue scanning when an attachment with a threat is detected. ■ Move attachments to a folder — The scanner moves attachments with potential threats to the designated folder. ■ Delete attachments — The scanner deletes attachments with potential threats as soon as it detects them. For Microsoft Outlook, the e-mail is deleted. For Lotus Notes, the attachment is deleted. ■ Delete mail (for Outlook Scan only) — The scanner deletes mail with potential threats.  Notes and Tips <i>Default = Move attachments to a folder.</i>

Option or Button	Description
Move To Folder	Specify the location and name of the quarantine folder.  Notes and Tips The quarantine folder must be located on a hard drive. It should not be located on a floppy drive or CD drive. The default location for the quarantine folder varies depending on whether you are using Microsoft Outlook or Lotus Notes. ■ For Microsoft Outlook the quarantine folder is located in the Microsoft Outlook mailbox. ■ For Lotus Notes, the quarantine folder is located in the file system.
Allowed actions in Prompt dialog box	Select the actions that are allowed when the user is prompted for action. ■ Clean attachment ■ Delete attachment ■ Move attachment ■ Delete mail (for Outlook Scan only)

Alerts tab

Configure these alert settings for both the on-delivery e-mail scanner and the on-demand e-mail scanner.

Figure 9-4 E-mail Scan Properties — Alerts tab

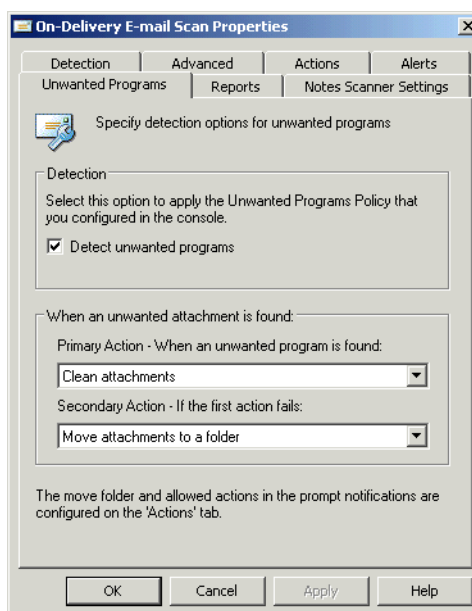


Option or Button	Description
Send alert mail to user	Notify another user when a threatened e-mail message is detected.  Notes and Tips Click Configure to open the Send Mail Configuration dialog box.
If Prompt for Action is selected	Notify users when a threatened e-mail message is detected and the Prompt for Action option is selected on the Actions tab. Accept the default message or specify a new one.  Notes and Tips <i>Default message = McAfee VirusScan Enterprise E-mail Scanner Alert!.</i>

Unwanted Programs tab

Configure these unwanted program detection settings for both the on-delivery e-mail scanner and the on-demand e-mail scanner.

Figure 9-5 E-mail Scan — Unwanted Programs tab

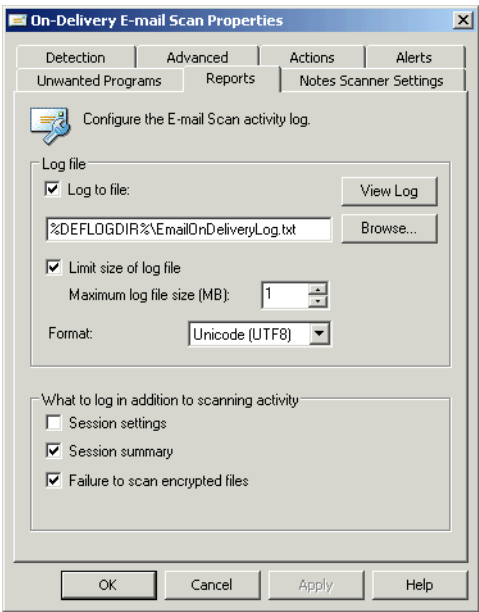


Option or Button	Description
Detect unwanted programs	Enables the e-mail scanner to detect potentially unwanted programs.  Notes and Tips The e-mail scanner uses the settings you configured in the Unwanted Programs Policy to detect potentially unwanted programs. See Unwanted Programs Policy on page 36.
Primary Action	Select the first action that you want the scanner to take when a threat is detected. ■ Clean attachments — The scanner tries to remove the threat from the attachment. ■ Prompt for action — Prompt the user for action when a threat is detected. Select this option, then specify which actions users can take under Allowed action in Prompt dialog box. No secondary action is allowed for this option. ■ Continue scanning — Continue scanning when an attachment with a threat is detected. No secondary action is allowed for this option. ■ Move attachments to a folder — The scanner moves attachments with potential threats to the designated folder. ■ Delete attachments — The scanner deletes attachments with potential threats as soon as it detects them. For Microsoft Outlook, the e-mail is deleted. For Lotus Notes, the attachment is deleted.  Notes and Tips <i>Default = Clean attachments.</i>
Secondary Action	Select the next action you want the scanner to take if the first action fails. ■ Prompt for action — Prompt the user for action when a threat is detected. Select this option, then specify which actions users can take under Allowed action in Prompt dialog box. No secondary action is allowed for this option. ■ Continue scanning — Continue scanning when an attachment with a threat is detected. No secondary action is allowed for this option. ■ Move attachments to a folder — The scanner moves attachments with potential threats to the designated folder. ■ Delete attachments — The scanner deletes attachments with potential threats as soon as it detects them. For Microsoft Outlook, the e-mail is deleted. For Lotus Notes, the attachment is deleted.  Notes and Tips <i>Default = Move attachments to a folder.</i>

Reports tab

Configure activity log information for both the on-delivery e-mail scanner and the on-demand e-mail scanner.

Figure 9-6 E-mail Scan Properties — Reports tab



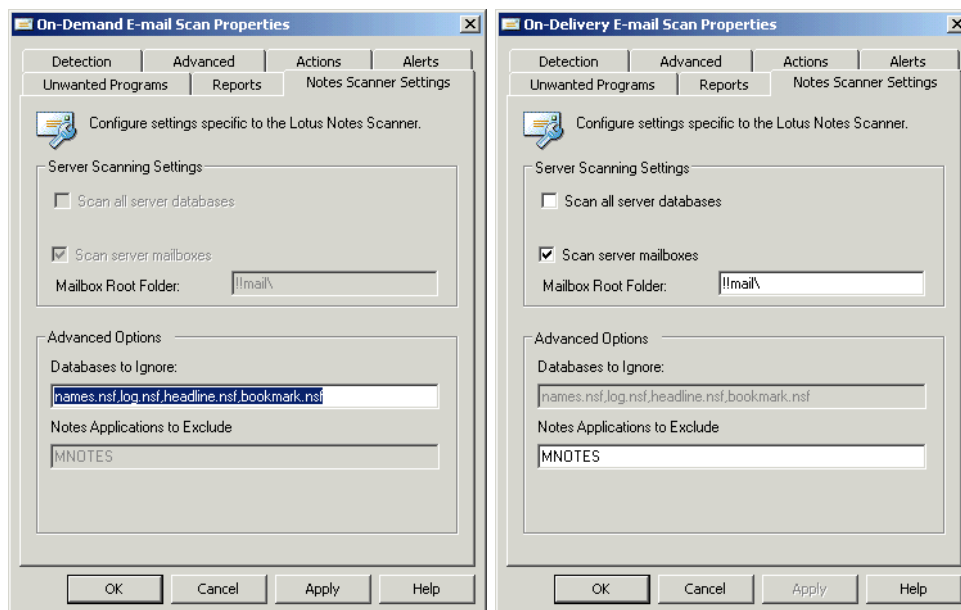
Option or Button	Description
Log to file	Record e-mail scanning activity in a log file. Accept the default location for the file or browse to a new location. The default log name is EMAILONDELIVERYLOG.TXT or EMAILONDEMANDLOG.TXT. The default location is <pre><drive>:\Documents and Settings\All Users\Application Data\McAfee\DesktopProtection\</pre> Notes and Tips ■ The log file can track activity on your network and note which settings you used to detect and respond to any potential threat that the scanner found. The recorded information helps determine which files you need to either replace from backup copies or delete. ■ The default location depends on which operating system you are using.
Limit size of log file	Restrict the log file to the size you specify. Notes and Tips If the data in the log file exceeds the file size you set, the oldest 20 percent of the log file entries are deleted and new data is appended to the file.
Maximum log file size	Specify the maximum size for the log file. Notes and Tips Accept the default size (1MB) or set a size from 1MB to 999MB.

Option or Button	Description
Format	Select the format of the log file: ■ Unicode (UTF8) ■ Unicode (UTF16) ■ ANSI  Notes and Tips ■ <i>Default = Unicode (UTF8).</i> ■ The format you choose depends on the information you are storing. If you are storing western text (every character is one byte), we recommend using the ANSI format. If you are storing eastern text (every character is one or two bytes), or sharing information within a multi-national organization, we recommend using one of the Unicode formats.
Session settings	Record the properties for each scanning session in the log file.
Session summary	Record a summary of the scanner's actions during each scanning session in the log file.  Notes and Tips Summary information includes the number of files scanned, the number and type of detections, the number of files moved, cleaned, or deleted, and other information.
Failure to scan encrypted files	Record the name of encrypted files that the scanner failed to scan.
View Log	View the existing log file.

Notes Scanner Settings tab

Configure these Lotus Notes settings for both the on-delivery e-mail scanner and the on-demand e-mail scanner.

Figure 9-7 On-Demand or On-Delivery Scan Properties — Notes Scanner Settings tab



Option or Button	Description
Scan all server databases	Scan all server databases for potential threats. This option is available only for on-delivery e-mail scanning.
Scan server mailboxes	Scan all server mailboxes for potential threats.
Mailbox Root Folder	Specify the location of the root folder. Accept the default location for the mailbox root folder or specify a new location. This option is available only for on-delivery e-mail scanning. Notes and Tips Default = !!mail\.
Databases to ignore	Specify which databases to ignore when scanning. This option is available only for on-demand e-mail scanning. Notes and Tips Default = names.nsf, log.nsf, headline.nsf, bookmark.nsf.
Notes Applications to Exclude	Specify which Lotus Notes applications to exclude from scanning. This option is available only for on-demand e-mail scanning. Notes and Tips Default = MNOTES.

Running on-demand e-mail scans

This section describes:

- [Microsoft Outlook scans](#).
- [Lotus Notes scans on page 112](#).

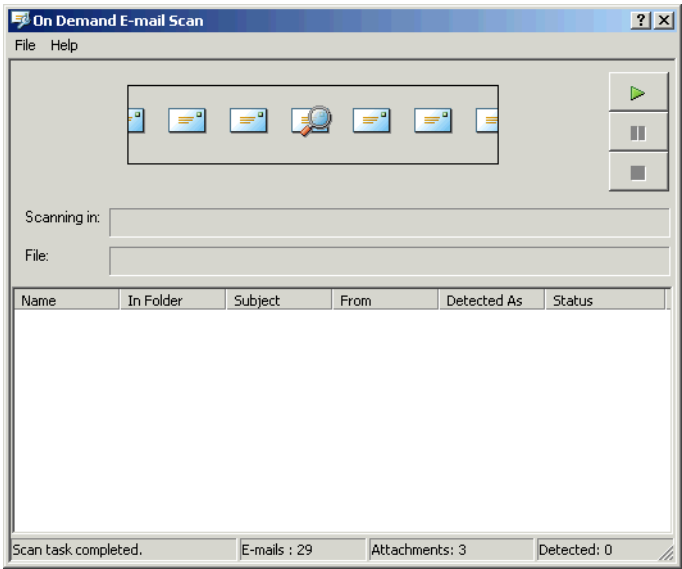
Microsoft Outlook scans

Use one of these methods to start an on-demand e-mail scan from Microsoft Outlook:

- From the Tools menu, select Scan for Threats.
- Click  in the Outlook toolbar.

The On-Demand E-mail Scan dialog box appears.

Figure 9-8 Microsoft Outlook — On-Demand E-mail Scan

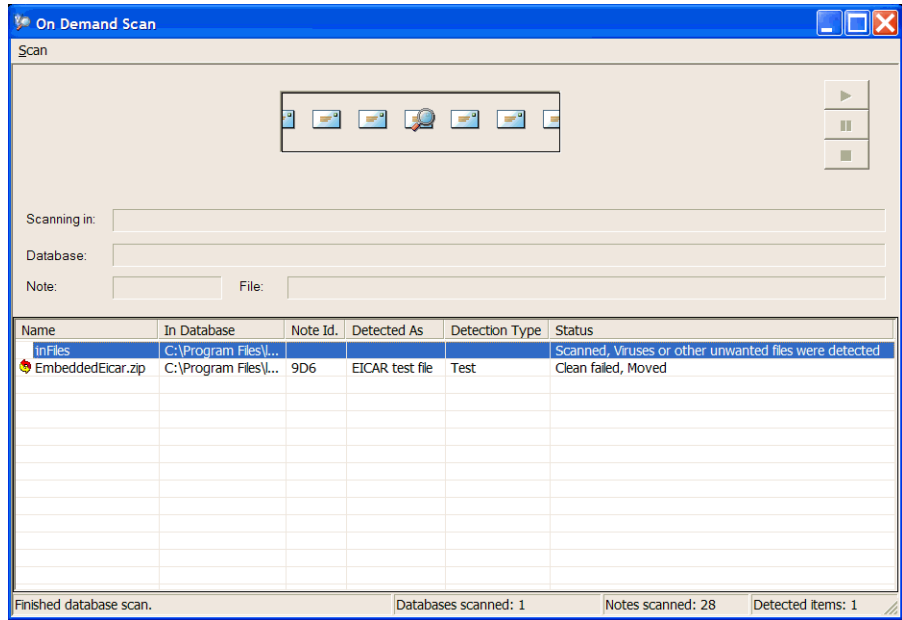


Option or Button	Description
Scanning in	Location currently being scanned.
File	File currently being scanned.
Name, In Folder, Subject, From, Detected As, Status	Detection details.
	Start the task.
	Pause the task.
	Stop the task.
Scan task completed	Displays the statistics and results for the scan.
	 Notes and Tips
	This toggles between Scan task in progress and Scan task completed.

Lotus Notes scans

From the Lotus Notes Actions menu, select Scan open database(s).
The On-Demand Scan dialog box appears.

Figure 9-9 Lotus Notes – On-Demand Scan



Option or Button	Description
Scanning in	Location currently being scanned.
Database	Database currently being scanned.
Note	Note currently being scanned.
File	File currently being scanned.
Name, In Database, Note id, Detected As, Detection Type, Status	Detection details.
	Start the task.
	Pause the task.
	Stop the task.
Finished database scan	Displays the statistics and results for the scan.



SECTION 3

Response

Configure alerts to notify you when detections occur, configure how long to keep quarantined items before they are automatically deleted, view scan results, and take action on detected items.

[Chapter 10, Alerts and Notifications](#)

[Chapter 11, Quarantine Manager Policy](#)

[Chapter 12, Detection Response](#)

[Chapter 13, Troubleshooting](#)

10 Alerts and Notifications

This section describes:

- [About alerts and notifications.](#)
- [Configuring alerts on page 114.](#)

About alerts and notifications

Being notified when a potential threat is detected is an important part of protecting your environment. You can use Alert Manager or VirusScan Enterprise local alerting to notify you when detections occur:

- Alert Manager is a discrete component that works with VirusScan Enterprise to handle alerts and events in real time. In a typical configuration, Alert Manager resides on a central server and listens for alerts sent to it by VirusScan Enterprise. Use it to configure where and how alerts are sent and what the alert message is.
- VirusScan Enterprise provides an interface for configuring Alert Manager and other alerting options that do not require Alert Manager. Filter alerts by severity to limit alert traffic sent to Alert Manager and configure local alerting options that do not require Alert Manager.

Configuring alerts

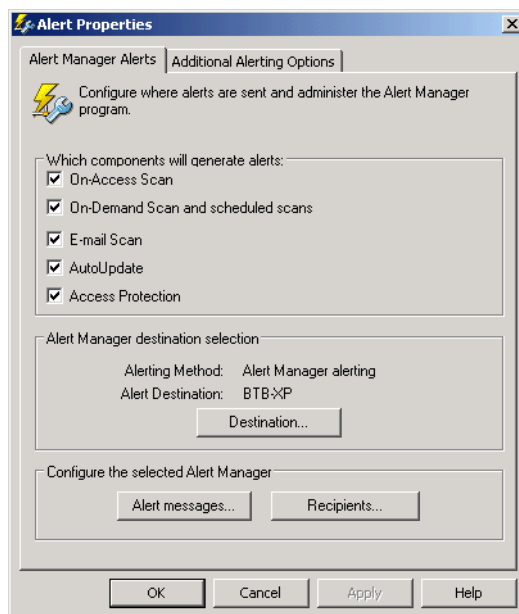
From the VirusScan Console, select Tools | Alerts.

Tab or Button	Options or Actions
Alert Manager Alerts tab	■ Specify which components generate alerts. ■ Configure Alert Manager.
Additional Alerting Options tab	■ Filter alerts by severity. ■ Configure local alerting.

Alert Manager Alerts tab

Select the components that you want to generate alerts and configure Alert Manager if it is installed.

Figure 10-1 Alert Properties — Alert Manager Alerts tab



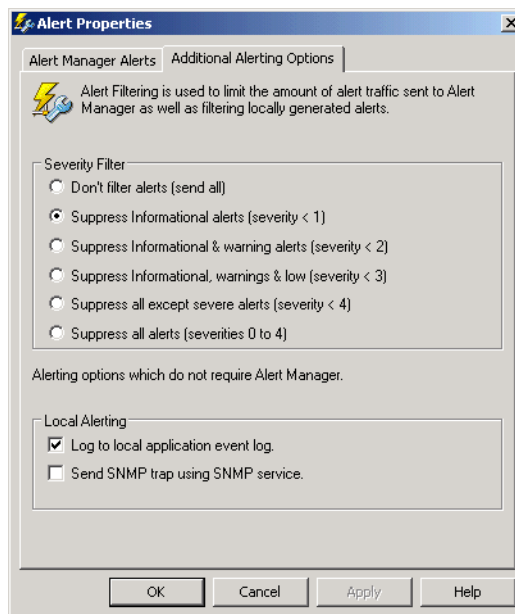
Option or Button	Description
On-Access Scan	Generate alerts when the on-access scanner detects threats.
On-Demand Scan and scheduled scans	Generate alerts when on-demand scan tasks detect threats.
E-mail Scan	Generate alerts when the e-mail scanner detects threats.
AutoUpdate	Generate alerts when update tasks detect threats.
Access Protection	Generate alerts when the access protection component detects threats.
Destination	Open the Alert Manager Client Configuration dialog box and configure these options: ■ Enable or disable the alerting feature. ■ Determine which method of alerting to use when an event occurs. ■ Specify which server receives alerts.
Alert Messages	Open the Alert Manager Messages dialog and configure priority levels for all system messages.
Recipients	Open the Alert Manager Properties dialog box to configure which recipients receive alert messages and the method by which messages are received. For example, e-mail or network messages.

See the *McAfee Alert Manager 4.7.1 Product Guide* for additional information about configuring Alert Manager.

Additional Alerting Options tab

Configure filter and local alerting options.

Figure 10-2 Alert Properties — Additional Alerting Options tab



Option or Button	Description
Don't filter alerts	Send all alerts.
Suppress informational alerts	Don't send informational alerts with a severity of less than one.
Suppress informational and warning alerts	Don't send informational and warning alerts with a severity of less than two.
Suppress informational, warning, and low	Don't send informational, warning, and low severity alerts with a severity of less than three.
Suppress all except severe alerts	Don't send any alerts except those with a severity of more than four.
Suppress all alerts	Do not send any alerts.
Log to local application event log.	Log information in the local application event log. This option does not require Alert Manager.
Send SNMP trap using SNMP service	If you are using SNMP, you can send SNMP trap alerts. This option does not require Alert Manager.

11

Quarantine Manager Policy

This section describes:

- [About quarantined items.](#)
- [Configuring the quarantine policy and managing quarantined items.](#)

About quarantined items

Detected files, registry keys, and registry values are backed up before they are cleaned or deleted by the on-access or on-demand scanner. The Quarantine Manager allows you to configure a policy to automatically delete quarantined items after a specified number of days and manage quarantined items. You can rescan, restore, and delete quarantined items as well as check them for false positives.

Configuring the quarantine policy and managing quarantined items

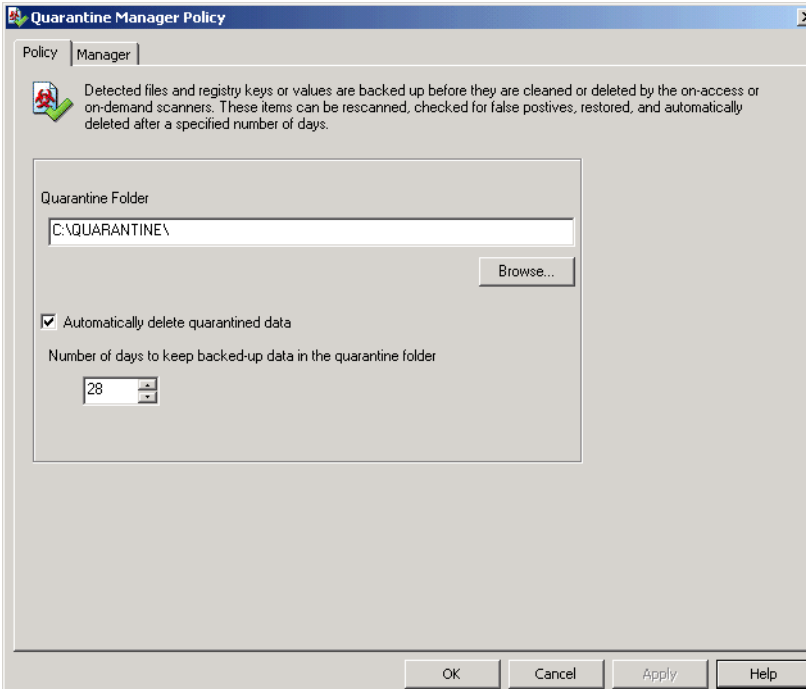
From the VirusScan Console, select Quarantine Manager Policy.

Tab or Button	Options or Actions
Policy tab	■ Location of the quarantine folder. ■ Automatically delete quarantined items. ■ Number of days to keep quarantined items.
Manager tab	■ List of quarantined items. ■ Right-click options to rescan, check for false positives, restore, delete, and view properties for each item.

Policy tab

Configure the quarantine location and the length of time to keep the quarantined items.

Figure 11-1 Quarantine Manager Policy — Policy tab

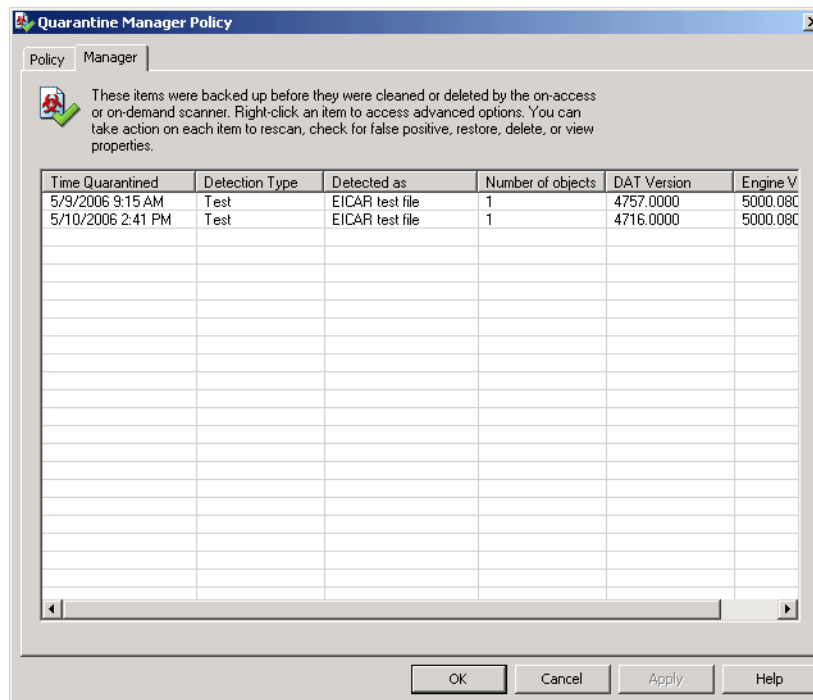


Option or Button	Description
Quarantine Directory	Specify the quarantine location.
Automatically delete quarantined data	Delete quarantined items after the specified number of days.
Number of days to keep backed-up data in the quarantine directory	Specify the number of days to keep the quarantined items before automatically deleting them. Notes and Tips Choose from 1 to 999 days.

Manager tab

View the list of quarantined items and their details, then take action on items as necessary. The list is indexed by the **Detection as** column. All changes resulting from the clean up of single detection name are stored in the details or properties of the backed up item.

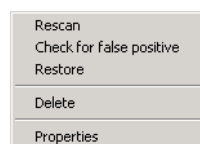
Figure 11-2 Quarantine Manager Policy — Manager tab



Option or Button	Description
Time Quarantined	The time that the item was quarantined.
Detection Type	The type of the item detected.
Detected as	The name of this item when detected.
Number of objects	The number of objects cleaned or deleted when detected.
DAT Version	The version of the DAT file that detected the item.
Engine Version	The version of the engine file that was used to detect the item.

Right-click an item to access advanced options:

Figure 11-3 Manager tab — Right-click options



Option or Button	Description
Rescan	Scans the selected item using the current DAT file, scanning engine, and scanning configuration.  Notes and Tips ■ If the rescanned item is still detected as a threat, do not restore it. Determine whether it is a valid threat. If it is not a valid threat, you can exclude it from scanning. ■ An item may be found clean upon rescan if it was a false positive that was fixed in the DAT file or if you changed the configuration to exclude the item. You can restore this item if necessary.
Check for false positive	Scans the item to determine if it was a false positive. If the item is found to be clean, you can restore it. If the item is still detected as a threat, but you think it's a false positive, you can: ■ Update the DAT file and rescan the item. A more current DAT file may contain information identifying the item as a false positive. ■ Submit sample to McAfee® Avert® Labs for analysis. See Submit a sample on page 166.
Restore	Restores the files and registry values to their original location. Once restored, the item is permanently deleted from the quarantine directory.
Delete	Permanently deletes the item from the quarantine directory.
Properties	Displays the names of the files and registry values that were altered when the detection was cleaned or deleted.

12

Detection Response

When VirusScan Enterprise detects a threat, you can receive notification and view the scan results, then take action on the detection.

This section describes:

- [Getting information about detections on page 122.](#)
- [Taking action on detections on page 126.](#)
- [Managing quarantined items on page 133.](#)

Getting information about detections

There are several way to get detection information.

This section describes:

- [Alerts and notifications.](#)
- [Viewing scan results on page 122.](#)

Alerts and notifications

You can receive an alert or notification when VirusScan Enterprise detects a threat, if you configured the software to do so.

There are several ways to receive notification:

Type of Notification	Description
Alerts	Configure alerts for each component. You can configure local alerts and/or Alert Manager to notify you when a detection occurs. ■ To configure local alerts and Alert Manager see Alerts and Notifications on page 114. ■ To configure On-Delivery and On-Demand E-mail alerts, see Alerts tab on page 105.
On-Access Scan Messages	Configure the On-Access Scan Messages dialog box to automatically display when on-access and buffer overflow detections occur. ■ See Messages tab on page 72 to configure the messages dialog box to display when an on-access detection occurs, ■ See Buffer Overflow Protection tab on page 32 to configure the messages dialog box to display when a buffer over flow detection occurs
On-Demand Scan Progress dialog box	Automatically displays the results of the scan while it is in progress for all on-demand scan tasks that are not scheduled. See On-Demand Scan Progress dialog box on page 131.
On-Demand E-Mail Scan dialog box	Automatically displays the results of the scan while Microsoft Outlook and Lotus Notes on-demand e-mail scans are running. See on page 132.

Viewing scan results

Scan results are recorded in activity log, the scan statistics dialog box, and in some cases in the On-Access Scan Messages dialog box.

This section describes:

- [Activity log on page 123.](#)
- [Scan statistics on page 123.](#)

Activity log

Each component records information in the activity log if you configured that component to do so.

The log file can serve as an important management tool for tracking activity on your network and for noting which settings were used for the detection. The information recorded in the file can help to determine how to respond to a detection.

For example:

- On-access, on-demand, and e-mail scanners — Which files you need to replace from backup copies or delete from your computer.
- Access protection — Which accesses were violated and which rules detected the violations.

To view the activity log:

- VirusScan Console:
 - Right-click a component or task in the task list and select **View Log**.



Unwanted Programs Policy and Quarantine Manager Policy do not have log files.

- Open the component's properties dialog box and select the **Reports** tab, then click **View Log**.
- Windows Explorer — Navigate to the activity log. The default location for each component's activity log is:

<drive>:\Documents and Settings\All User\Application Data\McAfee\VirusScan



This location may vary depending on what operating system you are using.

Scan statistics

Each component records scanning and detection results in the statistics dialog box.

- [On-Access Scan Statistics on page 124](#). This includes statistics for on-access scanning, access protection, and blocked items.
- [On-Demand Scan Statistics on page 125](#).
- [On-Delivery E-mail Scan Statistics on page 126](#).

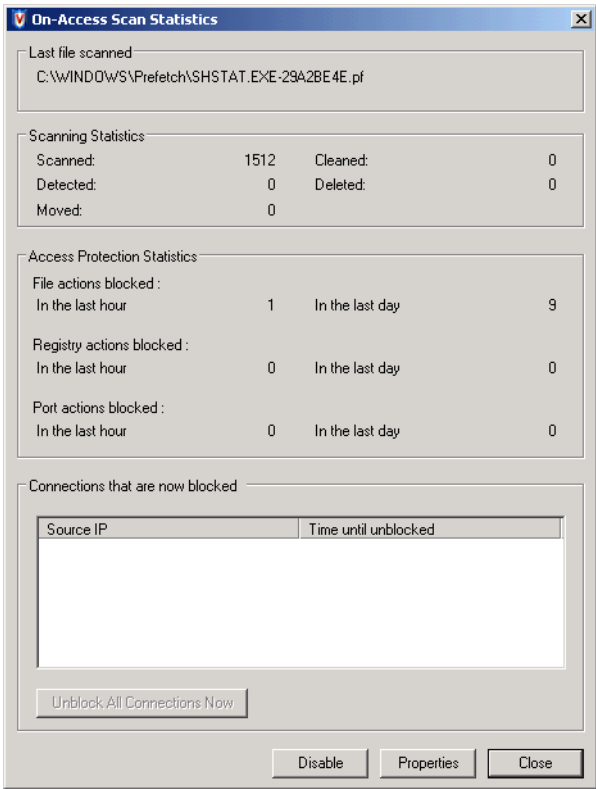
On-Access Scan Statistics

The On-Access Scan Statistics dialog box displays results for on-access scanning and access protection, and blocked items.

To open the On-Access Scan Statistics dialog box:

- Double-click  in the system tray.
- From the VirusScan Console, right-click On-Access Scanner in the task list, then select Statistics.

Figure 12-1 On-Access Scan Statistics



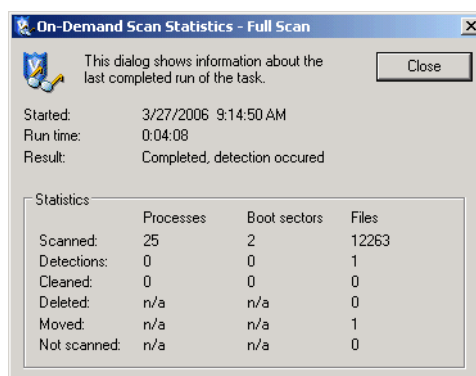
Option or Button	Description
Last file scanned	The location and name of the last file scanned.
Scanning Statistics	A summary of the number of files scanned, detected, and the actions taken on the detections.
Access Protection Statistics	A summary of the file actions, registry actions, and port actions that were blocked in both the last hour and the last day.
Connections that are now blocked	Displays the Source IP and time remaining until unblocked for each blocked connection.
Unblock All Connections Now	Unblock all connections that are now blocked.

Option or Button	Description
Disable	This function toggles between Disable and Enable. Click Disable to pause the on-access scanner or click Enable to resume it. This option is not visible if the user interface is configured to show minimal menu options.  Notes and Tips Disabling the on-access scanner also disables enforcement of access protection rules.
Properties	Open the On-Access Scan Properties dialog box. This option is not visible if the user interface is configured to show minimal menu options.  Notes and Tips Change the on-access scan properties. Changes are applied immediately.

On-Demand Scan Statistics

From the VirusScan Console, right-click the on-demand scan in the task list, then select **Statistics**.

Figure 12-2 On-Demand Scan Statistics

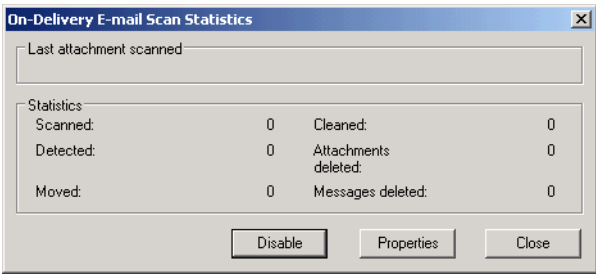


Area	Description
Upper pane	The start time, run time, and result of the last completed scan.
Lower pane	Statistical summary of the scan results.

On-Delivery E-mail Scan Statistics

From the VirusScan Console, right-click On-delivery E-mail Scanner in the task list, then select Statistics.

Figure 12-3 On-Delivery E-mail Scan Statistics



Area	Description
Last attachment scanned	Information about the last attachment scanned. Notes and Tips If your scan is still in progress, it shows the file that the scanner is currently examining and the status of the scan operation.
Statistics	Statistical summary of the scan results.
Disable	This function toggles between Disable and Enable. Click Disable to pause the on-delivery e-mail scanner or click Enable to resume it. This option is not visible if the user interface is configured to show minimal menu options.
Properties	Open the On-Delivery E-mail Scanner Properties dialog box. This option is not visible if the user interface is configured to show minimal menu options. Notes and Tips Change the on-delivery e-mail scan properties. Changes are applied immediately.

Taking action on detections

There are different ways to take action depending on which feature detects threats.

This section describes taking action on:

- [Access protection detections on page 127.](#)
- [Buffer overflow detections on page 127.](#)
- [Unwanted program detections on page 129.](#)
- [On-access scan detections on page 129.](#)
- [On-demand scan detections on page 131.](#)
- [E-mail scan detections on page 132.](#)

Access protection detections

Use the information in the statistics summary and the activity log to determine which accesses were violated and which rules detected the violations, then configure the access protection rules to allow users access to legitimate items and prevent users from accessing protected items.

Use these possible scenarios to help make a decision about what action to take.

Results	Possible Scenarios
Unwanted processes	■ If the violation was reported in the activity log but not blocked, select the Block option for this rule. ■ If the violation was blocked but not recorded in the activity file, select the Report option for this rule. ■ If the violation was reported in the activity log and blocked, no action is necessary. ■ If you are aware of an unwanted process that was not detected, edit the rule to include it.
Legitimate processes	■ If the violation was reported in the activity log but not blocked, deselect the Report option for this rule. ■ If the violation was reported in the activity log and blocked, edit the access protection rule to exclude the legitimate process.

Buffer overflow detections

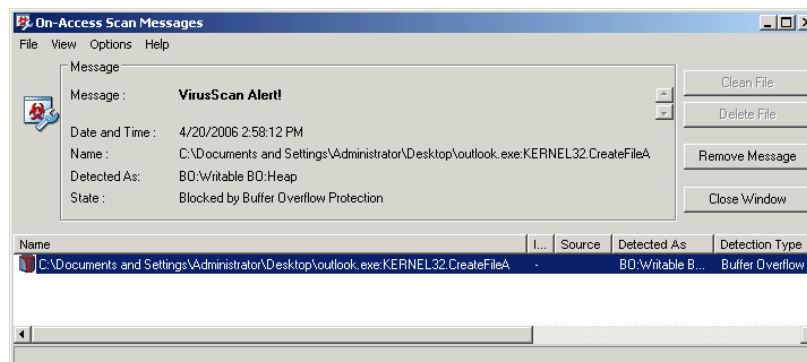
When a buffer overflow detection occurs:

- The scanner blocks the detection.
- A message is recorded in the **On-Access Scan Messages** dialog box. View the dialog box, then decide which action to take:
 - Remove the message — Select the item in the list, then click **Remove**.
 - Create an exclusion — See [Buffer overflow exclusion on page 128](#).
 - Submit a sample to McAfee® Avert® Labs for analysis — If the scanner detects something that you think it should not detect or does not detect something that you think it should, you can send a sample to Avert Labs. See [Submit a sample on page 166](#).

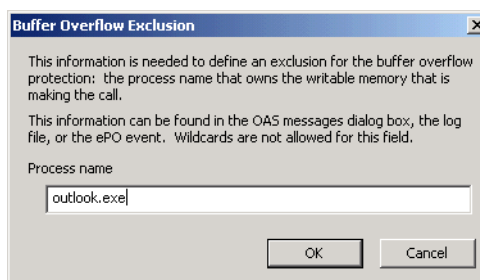
Buffer overflow exclusion

If the detected process is one that you legitimately use or a false positive, then create an exclusion.

Use the information in the On-Access Scan Messages dialog box to get information for the exclusion:

Figure 12-4 Sample buffer overflow detection

- 1 Review the information in the **Name** column to determine the name of the process that owns the writable memory that is making the call. In this example the process name is OUTLOOK.EXE.
- 2 Use the process name to create an exclusion.

Figure 12-5 Buffer overflow exclusion

Unwanted program detections

Each scanner; on-access, on-demand, e-mail, scans for unwanted programs based on the **Unwanted Programs Policy** you configured. When a detection occurs, the scanner that detected the potentially unwanted program applies the action that you configured on the **Unwanted Programs** tab for that scanner.

Review the information in the activity log, then decide what action to take:

- Fine-tune scanning items to make your scans more efficient.
 - If a legitimate program was detected, you can exclude it from detection. See [Excluding unwanted programs on page 39](#).
 - If an unwanted program was not detected, you can add it to the user-defined detection list. See [User-Defined Detection tab on page 41](#).
- Submit a sample to Avert Labs for analysis — If the scanner detects something that you think it should not detect or does not detect something that you think it should, you can send a sample to Avert Labs. See [Submit a sample on page 166](#).

On-access scan detections

When a detection occurs:

- The scanner takes action according to how you configured the **On-Access Scan Properties, Actions** tab.
- A message is recorded in the **On-Access Scan Messages** dialog box.

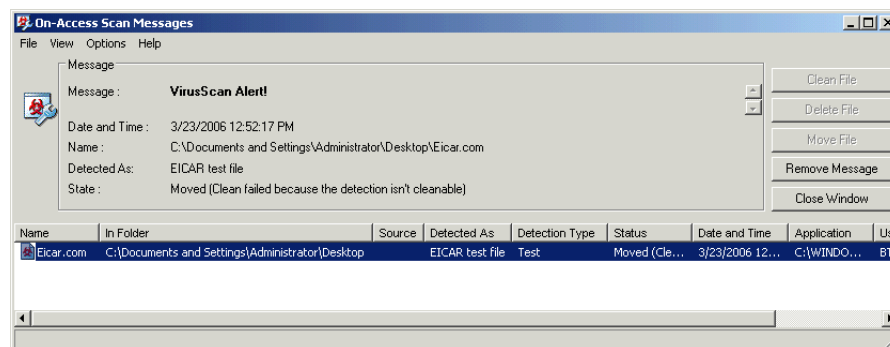
Review the information in the activity log and/or the **On-Access Scan Messages** dialog box, then decide what action to take.

- Fine-tune scanning items to make scanning more efficient. See [Adding & Excluding Scan Items on page 147](#).
- **On-Access Scan Messages** dialog box — Right-click an item in the list, then select the action. See [On-Access Scan Messages dialog box on page 129](#).
- Submit a sample to Avert Labs for analysis — If the scanner detects something that you think it should not detect or does not detect something that you think it should, you can send a sample to Avert Labs. See [Submit a sample on page 166](#).

On-Access Scan Messages dialog box

To open the **On-Access Scan Messages** dialog box, right-click  in the system tray and select **On-Access Scan Messages**.

Figure 12-6 On-Access Scan Messages



Option or Button	Description
File	Access menu options for the selected message. ■ Clean File — Attempts to clean the file referenced by the selected message. ■ Delete File — Deletes the file referenced by the selected message. The file name is recorded in the log so that you can restore it from the Quarantine Manager. ■ Select All (ctrl+a) — Selects all messages in the list. ■ Remove Message from List (ctrl+d) — Removes the selected message from the list. Messages that have been removed from the list are still visible in the log file. ■ Remove All Messages — Removes all message from the list. Messages that have been removed from the list are still visible in the log file. ■ Open On-Access Scanner Log File — Opens the on-access scanner activity log file. This option is available only from the File menu. ■ Open Access Protection Log File — Opens the access protection activity log file. This option is available only from the File menu.  Notes and Tips ■ If an action is not available for the current message, the corresponding icon, button, and menu items are disabled. For example, Clean is not available if the file has already been deleted, or Delete is not available if the administrator has suppressed the action. ■ Clean File — A file cannot be cleaned if the DAT file has no cleaner or it has been damaged beyond repair. If the file cannot be cleaned, the scanner appends an .mcm extension to the file name and denies access to it. An entry is recorded in the log file. In this case, we recommend that you delete the file and restore it from a clean backup copy.
Message	Displays details about the selected message.
Message List	Displays details about the detection.

On-demand scan detections

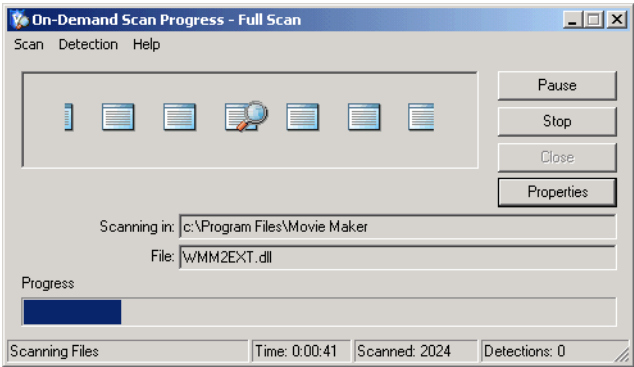
When a detection occurs, the scanner takes action according to how you configured the On-Demand Scan Properties, Actions tab.

Review the information in the activity log, then decide what action to take:

- Fine-tune scanning items to make your scans more efficient. See [Adding & Excluding Scan Items on page 147](#).
- If you configured the scanner to **Prompt for action**, then select the action from the On-Demand Scan Progress dialog box. See [On-Demand Scan Progress dialog box on page 131](#).
- Submit a sample to Avert Labs for analysis — If the scanner detects something that you think it should not detect or does not detect something that you think it should, you can send a sample to Avert Labs. See [Submit a sample on page 166](#).

On-Demand Scan Progress dialog box

Figure 12-7 On-Demand Scan Progress — Detection



Menu or Button	Description
Scan	Pause, continue, stop, start, open the properties dialog box, and start or stop calculating an estimate for the ongoing scan.
Detection	Clean or delete the detection.
Pause	Pause the task.
Continue	Resume the task.
Stop	Stop the task.
Properties	Open the On-Demand Scan Properties dialog box and change the scan properties. Notes and Tips The scan runs with the new settings when the next on-demand scan starts. If an on-demand scan is in process when you change the scan properties, the new settings do not take effect until the next on-demand scan starts.

E-mail scan detections

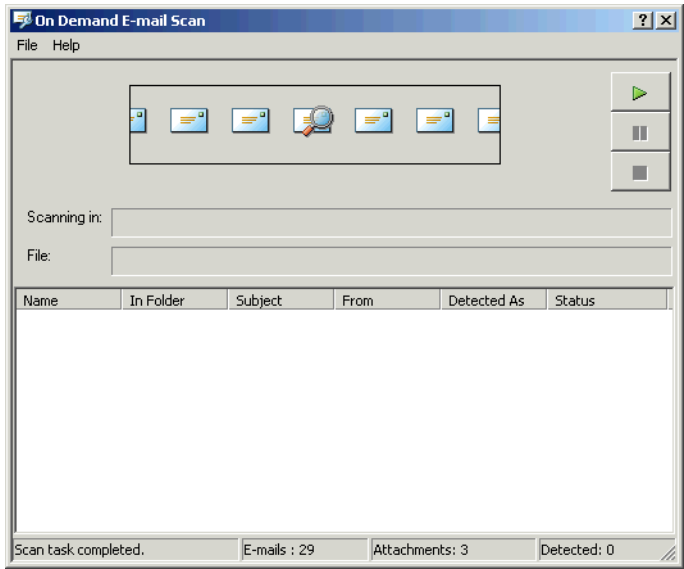
When a detection occurs, the scanner takes action according to how you configured the On-Demand or On-Delivery E-mail Scan Properties, Actions tab.

Review the information in the activity log, then decide what action to take:

- Fine-tune scanning items to make your scans more efficient. See [Adding & Excluding Scan Items on page 147](#).
- If you configured the scanner to **Prompt for action**, select the action from the On-Demand E-mail Scan dialog box. See [on page 132](#).
- Submit a sample to Avert Labs for analysis — If the scanner detects something that you think it should not detect or does not detect something that you think it should, you can send a sample to Avert Labs. See [Submit a sample on page 166](#).

On-Demand E-mail Scan dialog box

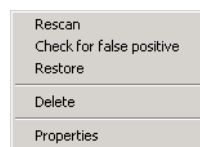
Figure 12-8 On-Demand E-mail Scan — Detection



Option or Button	Description
Scanning in	Location currently being scanned.
File	File currently being scanned.
Name, In Folder, Subject, From, Detected As, Status	Detection details.
	Start the task.
	Pause the task.
	Stop the task.
Scan task completed	Displays the statistics and results for the scan. Notes and Tips Toggles between Scan task in progress and Scan task completed .

Right-click an item to access advanced options:

Figure 12-10 Manager tab — Right-click options



Option or Button	Description
Rescan	Scan the selected item again.
Check for false positive	Scan the item to determine if it is a false positive.
Restore	Restore the selected item to its original location.
Delete	Delete the selected item.
Properties	Details about the quarantined item.

13 Troubleshooting

This section contains troubleshooting information for the VirusScan Enterprise product.

This section describes:

- [Utilities for troubleshooting.](#)
- [Frequently asked questions on page 136.](#)
- [Error codes for updating on page 140.](#)

Utilities for troubleshooting

The VirusScan Enterprise installation package includes two utilities to assist with troubleshooting the McAfee software on your system. These utilities are automatically installed with VirusScan Enterprise and are present on each computer running VirusScan Enterprise.

- [Minimum Escalation Requirements tool.](#)
- [Repair Installation utility on page 136.](#)

Minimum Escalation Requirements tool

The McAfee Minimum Escalation Requirements Tool (MERTool) is a utility that gathers reports and logs for McAfee software on your system. The tool must be launched manually and only collects information following user input. The information obtained can be used to help analyze problems.

To get more information about MERTool and access the utility, click the *MERTool* file that was installed with the VirusScan Enterprise product.

This file is located in the installation folder. If you accepted the default installation path, this file is located in:

```
<drive>:\Program Files\McAfee\VirusScan Enterprise\
```

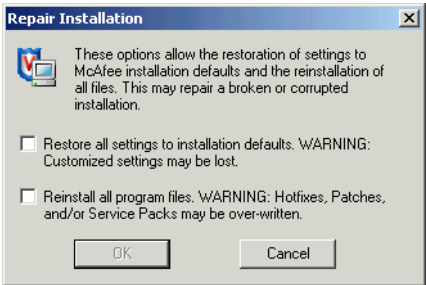
When you click the *MERTool* file, it accesses the URL for the MERTool website. Follow the instructions on the website.

Repair Installation utility

Use the VirusScan Enterprise repair installation utility to restore the program’s default installation settings and/or reinstall all of the program files.

From the VirusScan Console, select Help | Repair Installation.

Figure 13-1 Repair Installation



Option or Button	Description
Restore all settings to installation defaults	Restores the VirusScan Enterprise default installation settings. Notes and Tips Restoring default settings may result in losing your customized settings.
Reinstall all program files	Reinstalls the VirusScan Enterprise program files. Notes and Tips Reinstalling all program files may overwrite any HotFix, Patch, and/or Service Pack releases that were installed. If you choose this option, you must reinstall any HotFix, Patch, and/or Service Pack releases.

Frequently asked questions

This section contains troubleshooting information in the form of frequently asked questions. The questions are divided into these categories:

- [Installation on page 137.](#)
- [Potentially unwanted program on page 137.](#)
- [Blocked programs on page 137.](#)
- [Cookie detections on page 138.](#)
- [General on page 138.](#)

Installation

I just installed the software using the silent install method, and there is no VirusScan Enterprise icon in the Windows system tray.

The icon does not appear in the system tray until you restart your system. However, even though there is no icon, VirusScan Enterprise is running and your computer is protected.

Verify this by checking the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run  
ShStatEXE="C:\Program Files\McAfee\VirusScan Enterprise  
\SHSTAT.EXE" /STANDALONE
```

Why can some users on my network configure their own settings in and others cannot?

The administrator might have configured the user interface so that tasks are password-protected. If so, users cannot change the settings.

Different Windows operating systems have different user privileges. Refer to your Microsoft Windows documentation for more information about user privileges.

Potentially unwanted program

I suspect I have a potentially unwanted program but VirusScan Enterprise is not detecting it.

Download the latest beta DAT file while it is still being tested prior to the official release, from this website:

<http://vil.nai.com/vil/virus-4d.asp>

Blocked programs

I installed VirusScan Enterprise and now one of my programs does not work.

The program may be blocked by an access protection rule.

- 1 Review the access protection log file to determine if the program was blocked by a rule.
- 2 If you find the program listed in the log, you can either enter it as an exclusion to the rule or disable the rule. See [Configuring access protection on page 20](#) for more information.

Cookie detections

When reviewing the cookie detections in the on-demand scan activity log, I noticed that the file name detection is always 00000000.ie for every detection. Why does VirusScan Enterprise assign the same file name for every on-demand scan cookie detection when other programs assign an individual or incremental file name to each cookie detection?

VirusScan Enterprise 8.5i assigns the same file name to each cookie detection because of the way the on-demand scanner detects and takes action on cookies. This behavior applies only to cookies detected by on-demand scans.

A cookie file may contain many cookies. The scan engine treats a cookie file as an archive and assigns a value as an offset from the beginning of the file (starting with zero). Because the scanner uses the scan engine to detect and take action on each detected cookie before it proceeds with the scan, the value starts at zero for each detection. The result is that every detection is assigned a 00000000.ie file name. Other products detect all cookies, assign each one an individual or incremental file name, then take action on each detection.

General

The VirusScan Enterprise icon in my system tray appears to be disabled.

If there is a red circle and line covering the VirusScan Enterprise icon, that indicates that the on-access scanner is disabled. Here are the most common causes and solutions. If none of these solves your problem, contact Technical Support.

- 1 Make sure that the on-access scanner is enabled:
 - a Right-click the VirusScan Enterprise icon in the system tray. If the on-access scanner is disabled, the menu displays **Enable On-Access Scan**.
 - b Select **Enable On-Access Scan**.
- 2 Make sure that the McShield service is running:
 - a Start the service manually from the Services Control Panel.
 - b Select **Start | Run**, then type **Net Start McShield**
 - c Set the service to start automatically from the Services Control Panel.

I get an error saying that I cannot download catalog.z.

This error can be caused by many things. Here are some suggestions to help determine the source of the problem.

If you are using the McAfee default download site for updates, determine if you can download the CATALOG.Z file via a web browser. Try downloading the file from this website:

<http://update.nai.com/Products/CommonUpdater/catalog.z>

- If you can't download the file, but you can see it (in other words, your browser does not allow you to download it), you have a proxy issue and need to talk to your network administrator.

- If you can download the file, VirusScan Enterprise should be able to download it as well. Contact technical support for assistance in troubleshooting your installation of VirusScan Enterprise.

What is the location of the HTTP download site?

The McAfee download site location is:

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

The CATALOG.Z file, which contains the latest updates, can be downloaded from this website:

<http://update.nai.com/Products/CommonUpdater/catalog.z>

What is the location of the FTP download site?

The FTP download site location is:

<ftp://ftp.mcafee.com/pub/antivirus/datfiles/4.x>

The CATALOG.Z file, which contains the latest updates, can be downloaded from this site:

<ftp://ftp.mcafee.com/CommonUpdater/catalog.z>

If I do detect a potentially unwanted program and I have chosen “prompt user for action,” what action should I choose (Clean, or Delete)?

Our general recommendation is to choose **Clean** if you are not sure what to do with a detected file. The on-access and on-demand scanners automatically back up items to the quarantine directory before they are cleaned or deleted.

Error codes for updating

When your AutoUpdate fails, review the update log. These are common error codes that you may encounter:

- **-215: Failed to get site status** — The software cannot verify if the repository is available. Attempt to manually download the PKGCATALOG.Z file using the network protocol. If this fails, verify the path and user credentials.
- **-302: Failed to get the agent's framework interface** — The scheduler interface is not available. Stop and restart the framework service.
- **-409: Master site not found** — The master repository for the update is not available, is inaccessible, or is in use. Attempt to manually download the PKGCATALOG.Z file using the network protocol. If this fails, verify the path and user credentials.
- **-414: Verify the Domain, User Name, and Password you provided are typed correctly. Verify that the user account has permissions to the location where the repository resides** — While creating the repository, the credentials entered were determined invalid when **Verify** was selected. Either now, or after the repository is created, correct the credential information. Click **Verify** again. Repeat this process until the credentials are verified.
- **-503: Product package not found** — Update files are not present in the repository or may be corrupt. Ensure that the repository is populated with the update files. If these files are present, create a replication or pull task to overwrite the current task setting. If the files were not present, populate the repository, then attempt to update again.
- **-530: Site catalog not found** — You performed a pull task from a repository that does not have a catalog file, or contains a corrupted catalog file. To correct this issue, verify that the source repository contains a valid catalog directory.
- **-531: Package catalog not found** — The PKGCATALOG.Z was not found in the repository. Try to download the file using the network protocol. If it cannot be downloaded, perform a replication or pull task (depending on the type of repository).
- **-601: Failed to download file** — The repository is not accessible. Try to download the file using network protocol. If it cannot be downloaded, verify the path and user rights. If the file is downloaded, try stopping and starting the service.
- **-602: Failed to upload file** — You performed a pull task but the master repository credentials or settings are invalid (or the location is not available). Verify the credentials and location.
- **-804: Sit status not found** — You performed a replication task but the master repository is not available (or the credentials are invalid). Verify that the master repository is active, accessible, and that the credentials are valid.
- **-1113: Replication has been done partially** — One or more repositories may be inaccessible at the time of replication. Consequently, not all repositories are up-to-date. Verify that all repositories are accessible and that no files are marked as



SECTION 4

Supplemental Information

[Appendix A, User Interface Options](#)

[Appendix B, Adding & Excluding Scan Items](#)

[Appendix C, Scheduling Tasks](#)

[Appendix D, Command-line Options](#)

[Appendix E, Remote Administration](#)

[Appendix F, Getting Information](#)

[Glossary](#)

[Index](#)

A

User Interface Options

This section describes:

- [About the VirusScan Enterprise interface.](#)
- [Accessing the interface.](#)

About the VirusScan Enterprise interface

Configure and use VirusScan Enterprise from its user interface or the command line.



For information about managing VirusScan Enterprise via ePolicy Orchestrator, refer to the *VirusScan Enterprise Configuration Guide*.

Accessing the interface

This section describes the most common ways to access features and commands:

- [VirusScan Console on page 143.](#)
- [Right-click features on page 145.](#)
- [System tray icon on page 146.](#)
- [Start menu on page 146.](#)
- [Command line on page 146.](#)

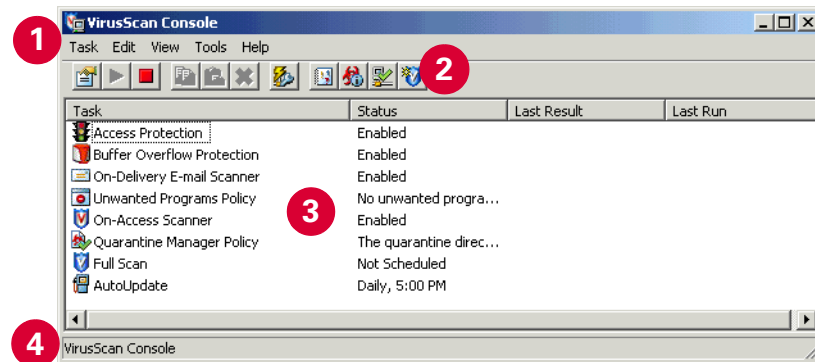
VirusScan Console

The VirusScan Console is the interface for the program's activities.

Use either of these methods to open the VirusScan Console:

- From the **Start** menu, select **Programs | McAfee | VirusScan Console**.
- Right-click the *VirusScan Enterprise* shield icon  in the system tray, then select **VirusScan Console**.

Figure A-1 VirusScan Console



- 1 Menu bar** — Use the menu items to create tasks, configure properties, and access additional information.

Task — Create and configure tasks such as scanning for threats or updating the DAT files.

Edit — Copy, paste, delete, or rename the selected task.

View — Display the Toolbar and/or Status bar and refresh the display.

Tools — Configure interface options for users, lock or unlock user interface security, enable the error reporting service, configure alerts, access the event viewer, open a remote console if you have administrator rights, import or edit the repository list, and roll back the DAT files.

Help — Access online Help topics, the Threat Library on the Avert Labs website, the Submit a Sample website, and the Technical Support website. You can also repair the product installation and view the **About** dialog box for copyright information and which versions of the product, license, definition files, scanning engine, extra driver, and patch are installed.



Each item on the menu has an associated shortcut key. The shortcut key is underlined for each item. These shortcut keys may not be available on some operating systems unless you use the keyboard (F10 or ALT) to access the menus.

2 Toolbar — Use the icons to access these commonly used commands:

Table A-1

Icon	Command
	Display properties of the selected task.
	Start the selected task.
	Stop the selected task.
	Copy the selected task.
	Paste the selected task.
	Delete the selected task.
	Configure alerting properties
	Launch the event viewer.
	Access the Information Library on the Avert Labs website.
	Connect to a remote computer if you have administrator rights.
	Create a new on-demand scan.

3 Task list — Displays the default tasks and any new tasks that you create as well as the status and last result for each task.

4 Status bar — Displays the status of the current activity.

Right-click features

Use right-click features for quick access to commonly used actions such as creating new tasks, viewing task statistics and logs, opening task property pages, scanning a specific file or folder, or performing an immediate update task.

Location	Description	Examples
The console	Right-click the VirusScan Console to display right-click features. These features vary, depending on whether you selected a task in the task list, and which task you select.	■ In the console, right-click a task to access its properties. Depending on which task you select, you may also be able to start, stop, enable or disable it, and view statistics and the activity log. In some cases, you can also rename or delete a task. ■ Right-click a blank area in the console to create a new scan or update task.
Windows Explorer	Right-click a selected file or folder to perform an immediate Full Scan of that item.	Perform an immediate scan on a file or folder that you suspect is threatened. When you start the scan, the on-demand scanner is invoked directly with all scan settings enabled. These scan settings cannot be customized.
The system tray	Right-click  to display menu items.	■ Open the VirusScan Console. ■ Disable or enable the on-access scanner. ■ Open the on-access scanner properties. ■ View the on-access scan statistics or messages. ■ Create a one-time configurable on-demand scan. ■ Perform an immediate update task. ■ Open the About dialog box.

System tray icon

Once VirusScan Enterprise is installed, the *shield* icon appears in the Windows system tray if you configured this feature during the installation process.

Note the following:

- The icon changes when the on-access scanner detects access protection violations. A red frame surrounds the icon for 30 minutes unless you reset it. For more information, see [What happens when an access violation occurs? on page 20](#).
- Double-click the icon to view **On-Access Scan Statistics**.
- Right-click the icon to display these menu options:
 - **VirusScan Console** — Opens the VirusScan Console.
 - **Disable On-Access Scan** — Toggles between disable and enable.



The access protection, buffer overflow protection, and script scan features use the on-access scanner. If the on-access scanner is disabled, you are not protected from access violations, buffer overflows, or execution of unwanted scripts.

- **On-Access Scan Properties** — Opens the on-access scanner property pages.
- **On-Access Scan Statistics** — Displays on-access scanner statistics from which you can enable or disable the on-access scanner and open the on-access scanner property pages.
- **On-Access Scan Messages** — Displays the on-access scanner messages, where you can take action on items in the list.
- **On-Demand Scan** — Opens the on-demand scanner property pages for an unsaved task, where you create a one-time on-demand scan task.
- **Update Now** — Performs an immediate AutoUpdate task.
- **About VirusScan Enterprise** — Displays information about the product, license, and which version(s) of the scan engine, detection definitions files, extra driver (extra.dat), and patches are installed.

Start menu

From the Windows **Start** menu, select **Programs | McAfee** to access these menu items:

- **VirusScan Console** — Opens the VirusScan Console.
- **On-Access Scan** — Opens the on-access scan property pages.
- **On-Demand Scan** — Opens the on-demand scan property pages where you configure and perform a one-time unsaved **Full Scan**.

Command line

Use the command line to perform activities from the Command Prompt. See [Command-line Options on page 160](#).

B

Adding & Excluding Scan Items

This section describes:

- [About scanning items.](#)
- [Configuring scanning items on page 148](#)

About scanning items

When configuring detection settings, each of the VirusScan Enterprise scanners allows you to fine-tune the list of file types scanned.

Using wildcards

When using wildcards, these limitations apply:

- Valid wildcards are question mark (?) for excluding single characters and asterisk (*) for excluding multiple characters.
- Wildcards can appear in front of a backslash (\) in a path. For example:

`C:\ABC\*XYZ` matches `C:\ABC\DEF\XYZ`.

- An exclusion containing question mark (?) characters applies if the number of characters matches the length of the file or folder name. For example:

The exclusion `w??` excludes `www`, but does not exclude `ww` or `wwwwww`.

- The syntax is extended to include a double asterisk (**), which means *zero or more of any characters including backslash*. This allows multiple-depth exclusions. For example:

`C:\ABC\**XYZ` matches `C:\ABC\DEF\XYZ` and `C:\ABC\DEF\DEF\XYZ`, etc.

Configuring scanning items

This section describes:

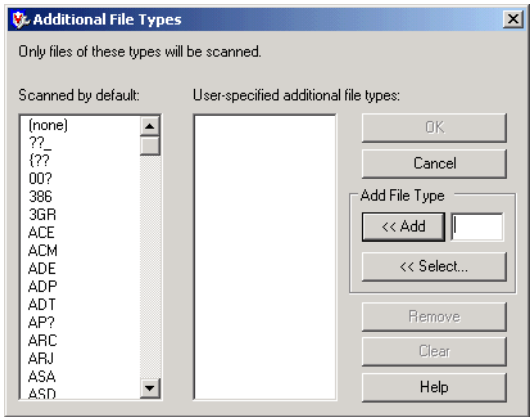
- [Adding file type extensions.](#)
- [Specifying user-defined file types on page 149.](#)
- [Excluding files, folders and drives on page 150.](#)

Adding file type extensions

Add file type extensions to fine tune your scanning capabilities. The maximum number of additional extensions that the scanner can accommodate is 1,000.

- 1 From the VirusScan Console, open the scanner’s property pages, then select the **Detection** tab.
- 2 Select **Default + additional file types**, then click **Additions**.

Figure B-1 Additional File Types



Option or Button	Description
Scanned by default	File types scanned by default.  Notes and Tips You cannot remove items from the default list, but you can exclude them. See Excluding files, folders and drives on page 150.
User-specified additional file types	File types added by the user.
Add	Add new file types to the user-specified list. Type a file extension in the text box, then click Add.  Notes and Tips You need to type only the first three letters of the file type extension. For example, if you type <code>htm</code>, the scanner searches for <code>htm</code> and <code>html</code> files. You can use a wildcard or any combination of characters with a wildcard.

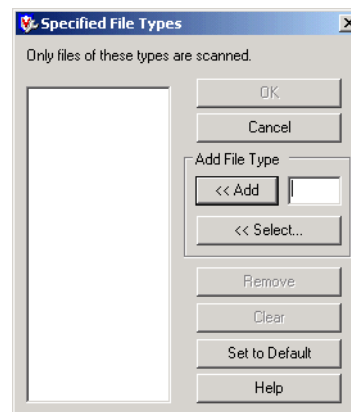
Option or Button	Description
Select	Select file types to add to the user-specified list. From the Select File Type dialog box, select one or more file type extensions from the list. Use CTRL + SHIFT to select more than one file type extension.
Remove	Delete file types from the user-specified list. Select one or more file types in the User-specified additional file types , then click Remove . Use CTRL + SHIFT to select more than one file type extension.
Clear	Remove all file types from the user-specified list.

Specifying user-defined file types

Create a specific list of extensions to fine tune your scanning capabilities. The maximum number of additional file type extensions that the scanner can accommodate is 1,000.

- 1 From the VirusScan Console or the e-mail client, open the scanner's property pages, then select the **Detection** tab.
- 2 Select **Specified file types**, then click **Specified**.

Figure B-2 Specified File Types



Option or Button	Description
Only files of these types are scanned	List of file types to be scanned.
Add	Add new file types to the user-specified list. Type a file extension in the text box, then click Add .  Notes and Tips You only need to type the first three letters of the file type extension. For example, if you type <code>htm</code> , the scanner searches for <code>htm</code> and <code>html</code> files. You can use a wildcard or any combination of characters with a wildcard.
Select	Select file types to add to the user-specified list. From the Select File Type dialog box, select one or more file type extensions from the list. Use CTRL + SHIFT to select more than one file type extension.

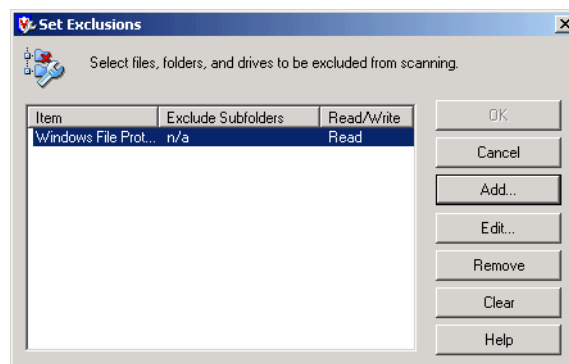
Option or Button	Description
Remove	Delete file types from the user-specified list. Select one or more file types in the User-specified additional file types , then click Remove . Use CTRL + SHIFT to select more than one file type extension.
Clear	Remove all file types from the user-specified list.
Set to Default	Replace the current list of user-specified file types with the default list.  Notes and Tips The default list of file types is defined by the current DAT file.

Excluding files, folders and drives

Specify files, folders, and drives to exclude from scanning operations. You can also remove any exclusions you specified previously.

- 1 From the VirusScan Console, open the on-access scanner or on-demand scan task's property pages, then select the **Detection** tab.
- 2 Click **Exclusions**.

Figure B-3 Set Exclusions



Option or Button	Description
Item	File, folder, or drive to exclude from scanning. Click the Add or Edit button to define this information.  Notes and Tips <i>Default = Windows File Protection.</i>
Exclude Subfolders	When scanning the item, do not scan its subfolders.
Read/Write	Do not scan this item when it is being read and/or written.
Add	Add new items to the list. See Adding or editing exclusion items on page 151 .
Edit	Change items in the list. See Adding or editing exclusion items on page 151 .

Option or Button	Description
Remove	Delete file types from the list. Select one or more file types in the User-specified additional file types, then click Remove.  Notes and Tips Use CTRL + SHIFT to select more than one extension.
Clear	Remove all file types from the user-specified list.

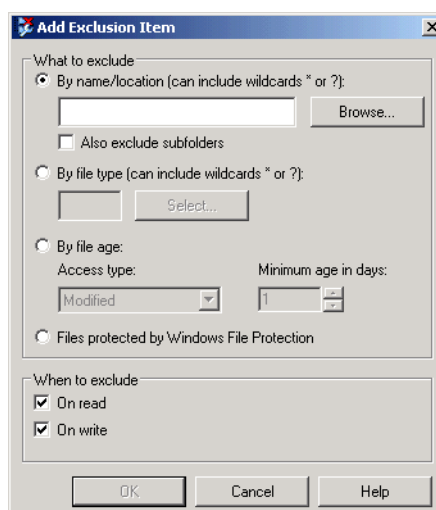
Adding or editing exclusion items

You can use wildcards when adding or editing exclusion items. See [Using wildcards on page 147](#).

Choose from these options:

- To add an item, click **Add**.
- To edit an item, select it in the list, then click **Edit**.

Figure B-4 Add Exclusion Item



Option or Button	Description
By name/location	Specify the name or location or click Browse to locate it.  Notes and Tips ■ <i>Default = By name/location.</i> ■ You can specify: - Full pathnames such as C:\WINNIT\SYSTEM*. - File names such as PAGEFILE.SYS, PAGEFILE.*, P*.*, or *.SYS. - Folder names such as BACKUP. For example, specifying BACKUP excludes all folders named BACKUP, wherever they are located. ■ When specifying a folder, you must append a backslash (\) to a path to indicate that it is intended to match a folder, or folders, when wildcards are used.
Also exclude subfolders	When scanning, exclude the subfolders of the folders that match the specified pattern.  Notes and Tips When the Also exclude subfolders option is not selected and a path does not end with a backslash (\), the path is treated as a file, or files, when wildcards are used
By file type	Specify a file type to exclude from scanning.
Select	Select file types to exclude from scanning. From the Select File Type dialog box, select one or more file type extensions from the list.  Notes and Tips Use CTRL + SHIFT to select more than one file type extension.
By file age	Exclude files by age.
Access type	If you selected By file age, select the type of access from these options: ■ Modified ■ Created ■ Accessed
Minimum age in days	If you selected By file age, specify the minimum age in number of days.  Notes and Tips The file must be at least the specified number of days old before it is excluded.
Files protected by Windows File Protection	Exclude a file based on its Windows File Protection status.
On read	Exclude the item from scanning when read from disk. This option is not available for on-demand scan tasks.
On write	Exclude the item from scanning when written to disk. This option is not available for on-demand scan tasks.



Scheduling Tasks

This section describes:

- [About scheduling tasks.](#)
- [Configuring the schedule on page 154.](#)

About scheduling tasks

You have the option to schedule on-demand, AutoUpdate, and mirror tasks to run at specific dates and times, or intervals.

To open the **Schedule Settings** dialog box for each type of task:

- **On-demand scan task** — From the VirusScan Console, open the On-Demand Scan Properties dialog box for the task, then click **Schedule**.
- **AutoUpdate task** — From the VirusScan Console, open the AutoUpdate Properties — AutoUpdate dialog box for the task, then click **Schedule**.
- **Mirror task** — From the VirusScan Console, open the AutoUpdate Properties — Mirror task dialog box for the task, then click **Schedule**.

Configuring the schedule

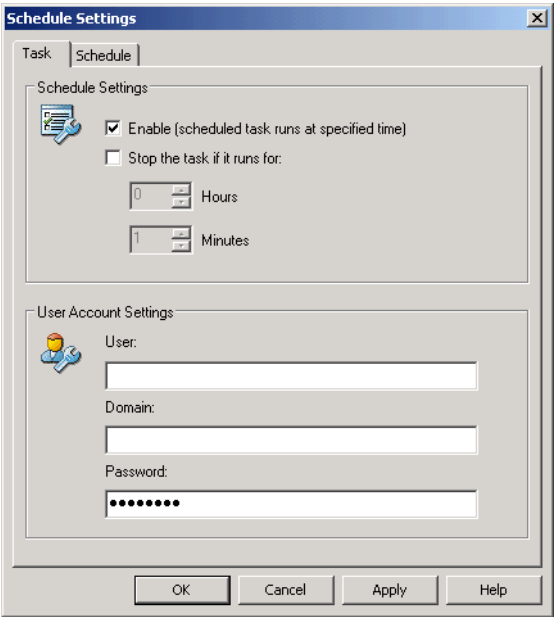
Open the schedule feature:

Tab or Button	Options or Actions
Task tab	■ Enable scheduled task to run a specified times. ■ Stop the task if it runs for the specified hours and minutes. ■ Specify user account settings; user name, domain, and password.
Schedule tab	Specify the schedule frequency and associated settings.

Task tab

Enable the schedule for this task and specify user account settings.

Figure C-1 Schedule Settings — Task tab



Option or Button	Description
Enable (scheduled task runs at specified time)	Schedule the task to run at a specified time. Notes and Tips This option must be selected to schedule the task.
Stop the task if it runs for	Stop the task after the number of hours and/or minutes that you specify. Notes and Tips If the task is interrupted before it completes, the next time it starts it resumes scanning from where it left off.
Hours	The number of hours after which the task will stop.
Minutes	The number of minutes after which the task will stop.

Option or Button	Description
User	Type the user ID under which this task executes.  Notes and Tips - The use of credentials is optional. If you do not type credentials here, the scheduled task runs under the local system account. - See Log on privileges on page 155 for more information.
Domain	Type the domain for the user ID you specified.
Password	Type the password for the user ID and domain you specified.

Log on privileges

If you schedule a task using credentials, the account that you specify needs to have *log on as a batch job* privilege. Without this privilege, the spawned process cannot access network resources, even though it has the correct credentials. This is documented Windows behavior.

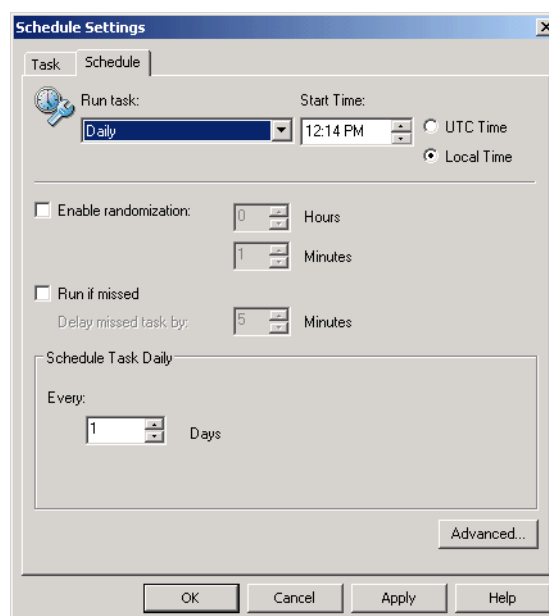
Access Local Security Policy to give an account this privilege:

- Select **Start | Programs | Administrative Tools | Local Security Policy** or **Start | Control Panel | Administrative Tools | Local Security Policy** depending on your operating system.
- In **Local Security Policy**, select **Security Settings | Local Policies | User Rights Assignments**.
- Double-click **Log on as a batch job**.
- Add the user to the list.
- Click **OK** to save these settings and close the dialog box.

Schedule tab

Specify the schedule frequency and other settings for this task.

Figure C-2 Schedule Settings — Schedule tab



Option or Button	Description
Run task	Select the frequency for this task from these options: ■ Daily — Run the task daily on the specified days. Daily tasks can be run every so many days, or every day Monday through Sunday. If you only want to run the task on specific days of the week, other than every day Monday through Sunday, we recommend that you use the weekly task frequency. ■ Weekly — Run the task daily on the specified week(s) and day(s). ■ Monthly — Run the task daily on the specified day(s) and month(s). ■ Once — Run the task once on the specified date. ■ At Startup — Run the task at system startup and specify whether to run the task once per day and the number of minutes to delay the task. ■ At Logon — Run the task at log on and specify whether to run the task once per day and the number of minutes to delay the task. ■ When Idle — Run the task when the computer is idle and specify the number of minutes that the computer is idle before starting the task. If the task is started and a user resumes use of the computer before the task completes, the task continues to run until complete. ■ Immediately — Run the task immediately. ■ On Dialup — Run the task on dialup.
Start Time	Select the start time for the scheduled task.
UTC Time	Coordinated Universal Time (UTC). Select this option to run the task simultaneously in all time zones.
Local Time	Run the task independently in each local time zone.  Notes and Tips <i>Default = Local Time.</i>
Enable randomization	Run the task at a random point within the interval of time you set. If you select this option, also specify the hours and/or minutes for the maximum time lapse.  Notes and Tips ■ Specify a time lapse interval between one minute (minimum) and 23 hours (maximum). For example, setting the task schedule to 1:00 and the randomization to three hours, would cause the task to run at any time between 1:00 and 4:00. ■ This option is not available when scheduling the task At Startup, At Logon, or When Idle.
Hours	The number of hours.  Notes and Tips Choose between 0 and 23 hours.
Minutes	The number of minutes.  Notes and Tips The number of minutes available for selection depends on which options you have selected. For example: ■ Enable randomization — Choose between 0 and 59 minutes. ■ Delay missed task by — Choose between 0 and 99 minutes.

Option or Button	Description
Run if missed	Ensure that missed tasks run when the computer starts up again. If the computer was offline when a task was scheduled to be run, it may have been missed.  Notes and Tips This feature ensures that remote users and the network are fully protected if they happen to be offline when a task is scheduled to run.
Delay missed task by	Select the number of minutes by which you want to delay the missed task.  Notes and Tips Choose from 0 to 99 minutes.
Every day(s)	Run this task every so many days as specified.  Notes and Tips ■ Choose from 0 to 9999 days. ■ This option is only available when you schedule the task Daily.
Every week(s)	Run this task every so many weeks as specified. If you select this option, also specify the number of weeks and the day(s) of the week.  Notes and Tips ■ Choose from 0 to 99 weeks. ■ For day of the month, choose from Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday. ■ This option is only available when you schedule the task Weekly.
Day of the month	Run this task on a specific day of the month. If you select this option, also specify the number of day of the month.  Notes and Tips ■ Choose from 1 to 31 days. ■ This option is only available when you schedule the task Monthly.
Week day of the month	Run this task on the specified day of the month. If you select this option, also select occurrence and day of the month.  Notes and Tips ■ For occurrence, choose from First, Second, Third, Fourth, and Last. ■ For day of the month, choose from Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday. ■ This option is only available when scheduling the task Monthly.
Select Months	Specify which months to run this task.  Notes and Tips This option is only available when scheduling the task Monthly.
Run on	Specify the date on which you want to run this task.  Notes and Tips This option is only available when scheduling the task Once.

Option or Button	Description
Only run this task once a day	Run this task once per day.  Notes and Tips ■ If you do not select this option, the task runs every time startup or log on occurs. ■ This option is only available when scheduling the task At Startup, At Logon, or Run On Dialup.
Delay task by	Specify the number of minutes by which to delay this task.  Notes and Tips ■ Choose from 0 to 99. ■ This allows time for users to log on and logon scripts to execute. ■ This option is only available when scheduling the task At Startup or At Logon.
When computer has been idle for	Specify the number of minutes that the computer is idle before starting the task.  Notes and Tips ■ Choose from 0 to 999 minutes. ■ If the task is started and a user resumes use of the computer before the task completes, the task continues to run until complete. ■ This option is only available when scheduling the task When Idle.
Advanced	Configure advanced options.  Notes and Tips See Advanced scheduling options on page 159 for more information.

Advanced scheduling options

Figure C-3 Advanced Schedule Options

Advanced Schedule Options

Start Date: 4/19/2006

☐ End Date: 4/19/2006

☒ Repeat Task

Every: 1 Hours

Until:

☒ Time: 12:00 AM (Local)

☐ Duration: 0 Hours 1 Minutes

OK Cancel Help

Option or Button	Description
Start Date	Specify the date to start this task.
End Date	Specify the date to end this task.
Repeat Task	Repeat the task at the specified frequency. If you select this option, also specify how frequently to repeat this task.
Every	Specify how frequently to repeat this task. Also select whether you want the frequency to be hours or minutes.
Time (Local)	Repeat this task at the specified local time. If you select this option, also select the specific time.
Duration	Repeat this task for the specified hours and minutes. If you select this option, also select the hours and minutes.
Hours	The number of hours.  Notes and Tips Choose from 0 to 99.
Minutes	The number of minutes.  Notes and Tips Choose from 0 to 59.

D

Command-line Options

This section describes:

- [About command-line scanning.](#)
- [Configuring on-demand scanning options.](#)
- [Configuring update task options on page 162.](#)

About command-line scanning

You can install, configure, and run VirusScan Enterprise from the command line. Installation options are described in the *VirusScan Enterprise Installation Guide*. This section describes options for performing on-demand scanning and update tasks.

Configuring on-demand scanning options

The on-demand scanner uses SCAN32.EXE to detect threats.

The SCAN32 syntax does not require any specific order in its elements, except that you cannot separate a property and its value. The syntax consists of:

- **File name** — The name of the executable file: SCAN32.EXE.
- **Options** — The option is preceded by a forward slash (/) character and are *not* case-sensitive.

For example:

```
SCAN32 PROPERTY=VALUE[,VALUE] [/option]
```

Use these options for on-demand scanning:

Table D-1

Command-line Option	Description
ALL	Scans all files in the target folder.
ALLOLE	Scans default files plus all Microsoft Office documents.
ALWAYSEXIT	Forces exit from on-demand scan, even if scan completed with error/failure.
APPLYNVP	Scans for the potentially unwanted programs that are defined in the Unwanted Programs Policy.
ARCHIVE	Scans archive files such as .ZIP, .CAP, .LZH, and .UUE files.
AUTOEXIT	Exits the on-demand scanner upon completion of a non-interactive scan.
CLEAN	Cleans the detected target file when a potentially unwanted program is found.
CLEANA	Cleans the detected file when an unwanted program is found.
CONTINUE	Continues scanning after a potentially unwanted program is detected.
CONTINUE2	Continues scanning after a potentially unwanted program is detected and the primary action has failed.
CONTINUEA	Continues scanning after an unwanted program is detected.
CONTINUEA2	Continues scanning after an unwanted program is detected and the primary action has failed.
DEFEXT	Adds file extensions that you specify as parameters to the list of selected file types that are included in scanning.
DELETE	Deletes the detected file when a potentially unwanted program is found.
DELETE2	Deletes the detected file when a potentially unwanted program is found and the primary action has failed.
DELETEA	Deletes the file when an unwanted program is detected.
DELETEA2	Deletes the file when a potentially unwanted program is detected and the primary action has failed.
EDIT	Displays the scan properties dialog box.
EXT	Replaces the extensions on the list of selected file types that are included in scanning with the file extensions that you add, as parameters following this argument.
LOG	Logs detection reports to a previously specified log file.
LOGFORMAT <value>	Uses the specified format for the log file. Valid values are ANSI, UTF8, or UTF16.
LOGSETTINGS	Logs the configuration settings of a scan.
LOGSUMMARY	Logs a summary of scan results.
LOGUSER	Logs identifying information about the user who executes a scan.
MHEUR	Enables heuristic detection of macro threats.
MIME	Detects potentially unwanted programs in MIME (Multipurpose Internet Mail Extensions) encoded files.
NOESTIMATE	Does not calculate scan size before beginning scanning of files. Progress bar does not display.
PHEUR	Enables heuristic detection of non-macro threats.

Table D-1

Command-line Option	Description
PRIORITY	Sets the priority of the scan relative to other CPU processes. Requires an additional numerical parameter. A value of 1 assigns priority to all other CPU processes. A value of 5 assigns the highest priority to the scan.
PROMPT	Prompts the user for action when a potentially unwanted program is detected.
PROMPT2	Prompts the user for action when a potentially unwanted program is detected and the primary action has failed.
PROMPTA	Prompts the user for action when an unwanted program is detected.
PROMPTA2	Prompts the user for action when an unwanted program is detected and the primary action has failed.
RPTSIZE	Sets the size of the alert log, in Megabytes.
START	Runs the scan. Does not display the properties dialog box.
TASK	Launches the on-demand scanner task specified in the VirusScan Console . Requires additional parameter specifying the specified task ID as recorded in the registry at: hkey_local_machine\software\McAfee\DesktopProtection\Tasks
UINONE	Launches the scanner without making the user interface dialog visible.

Configuring update task options

VirusScan Enterprise uses MCUPDATE.EXE to perform update tasks.

The MCUPDATE syntax does not require any specific order in its elements, except that you cannot separate a property and its value. The syntax consists of:

- **File name** — The name of the executable file: MCUPDATE.EXE.
- **Options** — The option is preceded by a forward slash (/) character and are *not* case-sensitive.

For example:

```
MCUPDATE [/<type> [/TASK <guid>]] [/option]
```

The /TASK clause is optional, however if you use it, you must also specify an update task ID (guid). The task ID you select must be for an update or a rollback DATS task. Do not select a scan ID. If you do not specify a task ID, the default update task is used. Task IDs are located at:

```
hkey_local_machine\SOFTWARE\McAfee\DesktopProtection\Tasks\
```

The /OPTION clause is not required, however to perform a silent update task use /QUIET.



The /QUIET option is not supported for use with the rollback DATS task.

This example performs a silent update task:

```
MCUPDATE [/UPDATE] [/QUIET]
```

Use these options to perform update tasks from the command line:.

Table D-2

Command-line Option	Description
ROLLBACKDATS	Rolls the current DAT file back to the last backed up version.
UPDATE	Performs an update of the DAT file, scanning engine, product, or EXTRA.DAT.
/TASK	Launches the AutoUpdate or rollback DATs task specified in the VirusScan Console . Requires an additional parameter to specify the task ID as recorded in the registry at: hkey_local_machine\SOFTWARE\McAfee\DesktopProtection\Tasks
/QUIET	Performs the task silently.

E

Remote Administration

You can connect to remote computers to perform operations such as modifying or scheduling scanning or update tasks, or enabling and disabling the on-access scanner on a remote computer. To do so, you must have administrator rights and the Remote Registry Service must be running.



If you do not have administrator rights to connect to the remote computer, you receive an *Insufficient user rights, access denied* error message.

When you start the **VirusScan Remote Console**, the name of the computer you are connected to appears in the console title bar. If you have not connected to a computer elsewhere on the network, the title bar does not show the name of your local computer. When you open any task's properties dialog box from a remote console, the computer name displays in the properties dialog box title bar.

To administer a remote computer on which the VirusScan Enterprise program is installed:

- 1 From the **Tools** menu, select **Open Remote Console** or click  in the toolbar.

The **Connect to Remote Computer** dialog box appears.

- 2 Under **Connect to computer**, type the name of the computer that you want to administer, and select a computer from the list, or click **Browse** to locate the computer on the network.



If environment variables are used while configuring the path name of the file or folder for a remote task, be sure that the environmental variable exists on the remote computer. The **VirusScan Console** cannot validate environmental variables on the remote computer.

- 3 Click **OK** to make a connection attempt to the destination computer.



When you connect to the remote computer, the title bar changes to reflect that computer's name, and the tasks in the task list are those for the remote computer. You can add, delete, or reconfigure tasks for the remote computer.

The console reads the remote computer's registry and displays the tasks of the remote computer.

You can open multiple remote consoles. When you close the **Connect to Remote Computer** dialog box, the connection to the remote computer closes as well.

F

Getting Information

These sections describe where to find product and other information:

- [Product documentation.](#)
- [Other resources on page 166.](#)
- [Contact information on page 168.](#)

Product documentation

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

Installation Guide — System requirements and instructions for installing and starting the software.

Product Guide — Introduction to the product and its features; detailed instructions for configuring the software; information on deployment, recurring tasks, and operating procedures.

Help — High-level and detailed information accessed from the software application: Help menu and/or Help button for page-level help.



The first time you click **Help** after installing the product, you are asked if you want to download the Help file. Click **Yes** to download the Help file and install it in your installation directory.

Configuration Guide — *For use with ePolicy Orchestrator®.* Procedures for deploying and managing supported products through the ePolicy Orchestrator management software.

Release Notes — *ReadMe.* Product information, resolved issues, any known issues, and last-minute additions or changes to the product or its documentation. *A text file is included with the software application and on the product CD.*

Quick Reference Card — A handy card with information on basic product features, routine tasks that you perform often, and critical tasks that you perform occasionally. *A printed card accompanies the product CD.*

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

Other resources

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

- [Help Topics](#).
- [McAfee Avert® Labs Threat Library](#).
- [Submit a sample](#).
- [Technical Support on page 167](#).
- [About VirusScan Enterprise dialog box on page 167](#).

Help Topics

From the **Help** menu, select **Help Topics** to access the VirusScan Enterprise online Help.



The first time you click **Help** after installing the product, you are asked if you want to download the Help file. Click **Yes** to download the Help file and install it in your installation directory.

McAfee Avert® Labs Threat Library

From the **Help** menu, select **McAfee Avert Labs Threat Library** for detailed information about potential threats, how they affect your system, and how to remove them.

Submit a sample

From the **Help** menu, select **Submit a Sample** to access the WebImmune website. If you find a potential threat that is not being detected with the current DAT file, you can submit a sample of it to Avert Labs through WebImmune. They analyze the sample and considers it for inclusion in the DAT file.

If the scanner detects something that you think it should not detect, you can also submit a sample of it to Avert Labs through WebImmune. Avert analyzes it and considers excluding it from the DAT file.

Use one of these methods to submit a sample:

WebImmune — This method provides the fastest turnaround time on sample reviews and provides historical information of all samples that you have submitted.

- 1 Access the website at:

<https://www.webimmune.net/default.asp>

- 2 Log on to your free account, or create one.

- 3 Upload files directly to the Avert Labs automated systems for review. Items are escalated to the Avert Labs analysts if additional research is required.

More information about WebImmune can be found at:

<https://www.webimmune.net/faqs.asp>

E-mail — Send e-mails directly to the Avert Labs automated systems for review. Items are escalated to the Avert Labs analysts for additional research if necessary.

Submit the sample via e-mail to the global e-mail address at:

virus_research@avertlabs.com



Get additional regional addresses from the WebImmune website.

Standard Mail — This is the least preferred method. Submitting samples in this way causes the longest turnaround time for review of your sample.

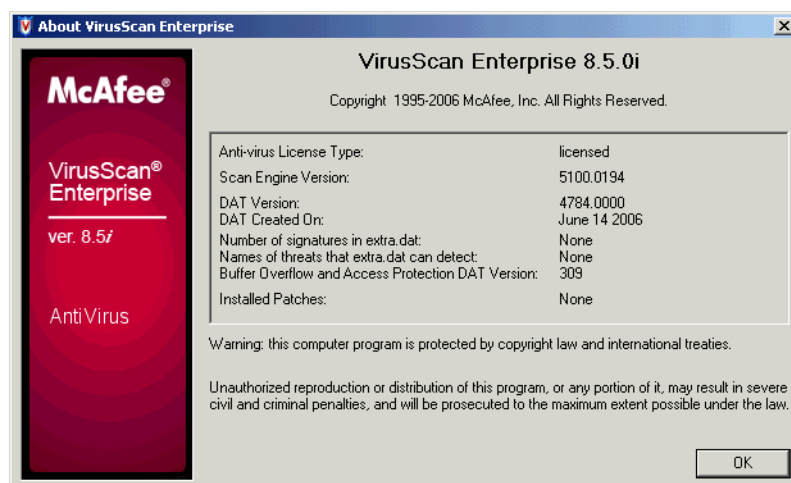
Technical Support

From the **Help** menu, select **Technical Support** to access the McAfee Customer Care website. Browse this site to view frequently asked questions (FAQs), documentation, and perform a guided knowledge search. Follow the directions on the website.

About VirusScan Enterprise dialog box

From the **Help** menu, select **About VirusScan Enterprise** to view important information about the product, license, and which version(s) of the scan engine, detection definitions files, extra driver (extra.dat), and patches are installed.

Figure F-1 About VirusScan Enterprise dialog box



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>

Glossary

access protection DAT file	See <i>detection definition files</i> .
action taken	How McAfee products responded to detections; for example, “cleaned” indicates that the detection was successfully removed from the corresponding file.
alert	A message or notification regarding computer activity such as detection. It can be sent automatically according to a predefined configuration, to system administrators and users, via e-mail, pager, or phone.
antispyware DAT file	See <i>detection definition files</i> .
alert notification	See <i>alert</i> .
anti-virus definition (DAT) file	See <i>detection definition files</i> .
anti-virus policy	See <i>policy</i> .
AutoUpdate	The automatic program in the McAfee software that updates that software program with the latest detection definition (DAT) files and scanning engine.
Avert Labs	McAfee Avert Labs; an anti-virus research center that supports the computing public and McAfee customers by researching the latest threats, and by uncovering threats that may arise in the future.
buffer overflow exploit	An attack technique that exploits an application’s buffer overflow to force it to execute arbitrary code.
clean, cleaning	An action taken by the scanner when it detects a threat such as a <i>virus</i> , <i>Trojan horse</i> , a <i>worm</i> , or a <i>potentially unwanted program</i> . The cleaning action can include removing the threat from a file and restoring the file to usability; removing references to the threats from system files, system .INI files, and the registry; ending the process generated by the threat; deleting a macro or a Microsoft Visual Basic script that is threatening a file; deleting a file if it is a virus, Trojan horse, or a worm; renaming a file that cannot be cleaned.
client computer	A computer on the client-side of the program.
command-line scanner	The McAfee scanner that runs from the Command Prompt.
common framework	The architecture that allows different McAfee products to share the common components and code, which are the Scheduler, AutoUpdate, and the ePolicy Orchestrator agent.

computers	The physical computers on the network.
configuration settings	See <i>policy</i> .
DAT files	See <i>detection definition files</i>
default process	In VirusScan Enterprise, any process that is not defined as a <i>low-risk process</i> or <i>high-risk process</i> .
detection definition files	Detection definition (DAT) files, sometimes referred to as signature files, that allow the product software to detect threats such as viruses, worms, Trojan horses, potentially unwanted programs, and related potentially unwanted code embedded in files. Types of detection definition files: - AntiSpyware DAT file - Anti-Virus DAT file - Access Protection DAT file See also <i>EXTRA.DAT file</i>, <i>incremental DAT files</i>, and <i>SuperDAT</i>.
denial-of-service attack (DoS)	A means of attack, an intrusion, against a computer, server or network that disrupts the ability to respond to legitimate connection requests. A denial-of-service attack overwhelms its target with false connection requests, so that the target ignores legitimate requests.
download site	The McAfee website from which you retrieve product, DAT, and/or engine updates. See also <i>update site</i>.
EICAR test file	European Institute of Computer Anti-Virus Research has developed a file consisting of a string of characters that can be used to test the proper installation and operation of anti-virus and anti-spyware software.
ePolicy Orchestrator console	The user interface of the ePolicy Orchestrator software that is used to remotely control and monitor managed computers. See also <i>ePolicy Orchestrator remote console</i>.
EXTRA.DAT file	Supplemental detection definition file that is created in response to an outbreak of a new threat or a new variant of an existing threat. See also <i>DAT files</i>, <i>incremental DAT files</i>, and <i>SUPERDAT</i>.
fallback repository	A type of distributed software repository used in the event that client computers cannot contact any of their predefined distributed repositories. Typically, another source repository is defined as the fallback repository. See also <i>replicate</i>, <i>replication</i>.
heuristic analysis, heuristics	A method of scanning that looks for patterns or activities that resemble threats, to detect new or previously undetected threats.
high-risk process	In VirusScan Enterprise, processes that McAfee considers to have a higher possibility of introducing or spreading a potential threat. For example, processes that launch other processes, such as Microsoft Windows Explorer or the command prompt; processes that execute, such as WINWORD or CSCRIPT; processes used for downloading from the Internet, such as browsers, instant messengers, and mail clients. See also <i>default process</i> and <i>low-risk process</i>.

HotFix releases (now Patches)	Intermediate releases of the product that fix specific issues.
incremental DAT files	New detection definitions that supplement the definitions currently installed, and are available for up to 15 weeks. Allows the update utility to download only the newest DAT files rather than the entire DAT file set. See also <i>DAT files</i> , <i>EXTRA.DAT file</i> and <i>SUPERDAT</i> .
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 file	A record of the activities of a component of McAfee software. Log files record the actions taken during an installation or during the scanning or updating tasks. See also <i>events</i> .
low-risk process	In VirusScan Enterprise, processes that McAfee considers to have a lower possibility of introducing or spreading a potential threat. For example, backup software or code compiler/linker processes. See also <i>default process</i> and <i>low-risk process</i> .
malware	Viruses and Trojan horses.
mass mailer virus	Potentially unwanted program such as Melissa and Bubbleboy that propagate themselves rapidly using e-mail services.
mirror, mirroring	The act of copying the contents of one distributed software repository to another outside of the normal replication process.
.MSI file	A Microsoft Windows Installer package that includes installation and configuration instructions for the software being deployed.
on-access scanning	An examination of files in use to determine if they contain a threat or other potentially unwanted code. It can take place whenever a file is read from the disk and/or written to the disk. Compare to <i>on-demand scanning</i> .
on-demand scanning	A scheduled examination of selected files to determine if a threat or other potentially unwanted code is present. It can take place immediately, at a future scheduled time, or at regularly scheduled intervals. Compare to <i>on-access scanning</i> .
package catalog file	A file that contains details about each update package, including the name of the product for which the update is intended, language version, and any installation dependencies.
packed executable	A file that, when run, extracts itself into memory only, never to disk.
Patch releases (previously HotFix release)	)Intermediate releases of the product that address specific issues.
port scanning	A hacking technique used to check TCP/IP ports to reveal which services are available in order to plan an exploit involving those services, and to determine the operating system of a particular computer.
potentially unwanted program	A programs that performs some unauthorized (and often harmful or undesirable) act such as spyware and adware,.

properties	Attributes or characteristics of an object used to define its state, appearance, or value.
protect mode	The mode in which an agent monitors activity on its host and carries out security measures.
quarantine folder	The location on a computer system that stores potentially unwanted programs until the system administrator can review them and decide on a course of action.
quarantine	Enforced isolation of a file or folder — for example, to prevent a threat or to isolate a spam e-mail message — until action can be taken to clean or remove the item.
Repository	The location that stores policy pages used to manage products.
repository list (SITELIST.XML)	The SITELIST.XML file that is used by those McAfee products that include the AutoUpdate program; it is used to access distributed repositories and retrieve packages.
rootkit	A set of software tools used to conceal running processes, files, or system data. Although there are legitimate uses, intruders frequently use rootkits to hide their access to and control of a system without the user's knowledge. A computer with a rootkit on it is called a <i>rooted</i> computer.
rule	Also known as a content rule; the description of how the product responds to undesirable content in document, e-mail message, or potentially unwanted program.
scan, scanning	An examination of files to determine if a threat or other potentially unwanted code is present. See <i>on-access scanning</i> and <i>on-demand scanning</i>.
scan action	The action that takes place when a threatened file is found.
scan task	A single scan event.
scanning engine	The mechanism that drives the scanning process.
security threat	See <i>threat</i> .
selective updating	The ability to specify which version of updates you want client computers to retrieve from distributed software repositories. See also <i>branch</i>.
signature	The description of a security threat or attack methodology.
signature files	See <i>detection definition files</i> .
silent installation	An installation method that installs a software package onto a computer silently, without need for user intervention.
SITELIST.XML	See <i>repository list</i> .
source repository	A type of distributed software repository from which the master repository retrieves files. Typically, the source repository is the McAfee website or another master repository. See also <i>pull</i>.

SuperDAT	A utility that installs updated detection definition (SDAT*.EXE) files and, when necessary, upgrades the scanning engine. See also <i>DAT files</i> , <i>EXTRA.DAT file</i> , and <i>incremental DAT files</i> .
SuperDAT (SDAT*.EXE) files	A standard application that you can double-click to start from within Microsoft Windows. The Microsoft version of the Installer includes a wizard that provides instructions in a series of panels.
SuperDAT Package Installer	An installation program that upgrades McAfee software programs. It automatically shuts down any active scans, services, or other memory-resident components that could interfere with the upgrade, then copies new files to their proper locations so that your software can use them immediately.
supplemental detection definition file	See <i>EXTRA.DAT file</i> .
system scan	A scan of the designated system.
task	An activity (both one-time such as <i>on-demand scanning</i> , and routine such as <i>updating</i>) that is scheduled to occur at a specific time, or at specified intervals. Compare to <i>policy</i> .
threat	A virus, Trojan horse, worm, potentially unwanted program, or other potentially unwanted code that places the security of your system or computer at risk.
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.
update package	Package files from McAfee that provide updates to a product. All packages are considered product updates with the exception of the product binary (Setup) files.
update site	The repository from which you retrieve product or DAT updates. See also <i>download site</i> .
updating	The process of installing updates to existing products or upgrading to new versions of products.
UTC time	Coordinated Universal Time (UTC). This refers to time on the zero or Greenwich meridian.
virus outbreak	See <i>outbreak</i> .
virus	A program that is capable of replicating with little or no user intervention, and the replicated program(s) also replicate further.
VirusScan Console	The control point for the program's activities.
warning priority	The value that you assign each alert message for informational purposes. Alert messages can be assigned a Critical , Major , Minor , Warning , or Informational priority.
worm	A virus that spreads by creating duplicates of itself on other drives, systems, or networks.

Index

A

- About dialog box [167](#)
- access protection
 - about [17](#)
 - access protection properties [21](#)
 - access violations [20](#)
 - configuring rules [21](#)
 - detections [127](#)
 - excluding processes [19](#)
 - levels of protection [19](#)
 - report properties [28](#)
 - rule categories [18](#)
- action
 - activity log [123](#)
 - detection alerts and notifications [122](#)
 - getting information about detections [122](#)
 - quarantined items [133](#)
 - responding to a threat [121](#)
 - viewing scan results [122](#)
- activity log, viewing [123](#)
- adding scan items [147](#)
 - about [147](#)
 - file types [148](#)
 - using wildcards [147](#)
- administration, remote console [164](#)
- alerts and notifications [114](#)
 - about [114](#)
 - alert filtering [116](#)
 - Alert Manager alerts [115](#)
 - configuring [114](#)
- audience for this guide [8](#)
- AutoUpdate
 - about [44](#)
 - activities during update [47](#)
 - command-line options [162](#)
 - download website
 - FTP [52](#)
 - HTTP [52](#)
 - error codes for updating [140](#)
 - immediate update [58](#)
 - proxy settings [54](#)

- repository
 - editing [51](#)
 - importing [50](#)
 - list [48](#)
- tasks
 - configuring [56](#)
 - creating [55](#)
 - description [45](#)
 - running [58](#)
 - update process overview [46](#)
 - updating strategies [45](#)
- Avert Labs
 - Threat Center [168](#)
 - Threat Library [166](#), [168](#)
 - submitting a sample [166](#)

B

- beta program website [168](#)
- blocked program questions, troubleshooting [137](#)
- buffer overflow protection [30](#)
 - about [30](#)
 - description [31](#)
 - detections [127](#)
 - exclusions [128](#)
 - exploit description [30](#)
 - protection properties [32](#)
 - report properties [34](#)

C

- CATALOG.Z file [47](#)
- command-line options [146](#), [160](#)
 - about [160](#)
 - on-demand scanning [160](#)
 - update task [162](#)
- configuring
 - access protection [20](#)
 - alerts and notifications [114](#)
 - AutoUpdate tasks [56](#)
 - buffer overflow protection [31](#)
 - e-mail scanning [100](#)
 - mirror tasks [59](#)
 - on-access scanning [68](#)
 - on-demand scanning [88](#)
 - quarantine policy [117](#)

- unwanted programs policy [37](#)
- user interface security [13](#)
- console, remote [164](#)
- cookie detection questions, troubleshooting [138](#)
- customer service, contacting [168](#)

D

- DAT files
 - Avert Labs notification service for updates [168](#)
 - rolling back [62](#)
 - updates, website [168](#)
- definition of terms (See Glossary)
- detecting intrusions [43](#)
- detections, response [121](#)
- display options [13](#)
- documentation, product [165](#)
- download website [168](#)

E

- e-mail scanning [99](#)
 - about [99](#)
 - action properties [103](#)
 - advanced properties [102](#)
 - alert properties [105](#)
 - detection properties [101](#)
 - detections [132](#)
- Lotus Notes
 - scanner properties [110](#)
 - scans [112](#)
- Microsoft Outlook scans [111](#)
- on-delivery scanning description [100](#)
- on-demand scanning description [99](#)
- report properties [108](#)
- running on-demand tasks [111](#)
- types of e-mail scanning [99](#)
- unwanted programs properties [106](#)

- evaluating McAfee products, download website [168](#)
- excluding scan items [147](#)
 - about [147](#)
 - using wildcards [147](#)

EXTRA.DAT [44](#), [47](#)

F

FAQ (frequently asked questions) [136](#)

features, described [10](#)

file type extensions

what not to scan [150](#)

what to scan [148](#), [149](#)

frequently asked questions (FAQ) [136](#)

FTP download website [52](#)

G

general questions, troubleshooting [138](#)

general settings, on-access scanning [68](#)

getting information [165](#)

About dialog box [167](#)

Avert Labs Threat Library [166](#)

help topics [166](#)

other resources [166](#)

product documentation [165](#)

Technical Support [167](#)

getting started [17](#)

glossary [169](#)–[173](#)

H

help topics [166](#)

high-risk process description [65](#)

HotFix and Patch releases (for products and security vulnerabilities) [168](#)

HTTP download website [52](#)

I

icon, tray [146](#)

information, getting [165](#)

About dialog box [167](#)

Avert Labs Threat Library [166](#)

help topics [166](#)

other resources [166](#)

product documentation [165](#)

Technical Support [167](#)

installation questions, troubleshooting [137](#)

intrusion

detection [43](#)

prevention [12](#)

response [113](#)

K

KnowledgeBase search [168](#)

L

locking user interface [16](#)

log file [123](#)

log on privileges [155](#)

low-risk process

description [65](#)

M

MERTool (Minimum Escalation Requirements Tool) [135](#)

Minimum Escalation Requirements Tool (MERTool) [135](#)

mirror task [49](#)

configuring [59](#)

creating tasks [58](#)

running tasks [61](#)

O

on-access scanning [63](#)

about [63](#)

action properties [81](#)

activity log

file format [57](#), [60](#), [109](#)

advanced properties [80](#)

assigning risk to a process [67](#)

blocking properties [71](#)

description [64](#)

detection properties [79](#)

detections [129](#)

general and process setting description [65](#)

general properties [69](#)

general settings [68](#)

high-risk and low-risk process description [65](#)

message properties [72](#)

process properties [76](#)

process settings [75](#)

report properties [73](#)

risk assignment [67](#)

scanning policies [66](#)

script scanner description [65](#)

ScriptScan properties [70](#)

statistics [124](#)

unwanted programs properties [83](#)

when reading or writing [64](#)

on-demand scanning [85](#)

about [85](#)

action properties [93](#)

advanced properties [92](#)

command-line options [160](#)

configuring tasks [88](#)

detection properties [91](#)

detections [131](#)

methods [86](#)

remote storage [87](#)

report properties [96](#)

running tasks [98](#)

scan progress [86](#)

system utilization [87](#)

task types [86](#)

unwanted programs properties [95](#)

where properties [89](#)

P

password options [15](#)

preventing intrusions [12](#)

privileges, log on [155](#)

process settings, on-access scanning [75](#)

product documentation, where to find [165](#)

product upgrades [168](#)

professional services, McAfee resources [168](#)

proxy settings for updating [54](#)

Q

quarantine manager [117](#)

about [117](#)

managing items [119](#)

policy [118](#)

taking action [133](#)

R

remote console

administration [164](#)

in Tools menu [164](#)

repair installation [136](#)

repository list

editing [51](#)

importing [50](#)

resources

About dialog box [167](#)

Avert Labs Threat Library [166](#)

Technical Support [167](#)

responding to intrusions [113](#)

right-click features [145](#)

S

scan items

about [147](#)

adding file type extensions [148](#)

excluding and adding [147](#)

excluding items [150](#)

specifying file type extensions [149](#)

using wildcards [147](#)

scan results

activity log [123](#)

viewing [122](#)

scanning

assigning risk to a process [65](#)

at system startup [69](#)

e-mail [99](#)

- immediately [98](#)
- on-access [63](#)
- on-demand [85](#)
- script [70](#)
- scheduling tasks [142](#), [153](#), [164](#)
 - about [153](#)
 - advanced properties [159](#)
 - log on privileges [155](#)
 - schedule properties [155](#)
 - task properties [154](#)
- script scanning
 - configuring [70](#)
 - description [65](#)
- security
 - updates, DAT files and engine [168](#)
 - user interface [13](#)
 - vulnerabilities, releases for [168](#)
- Security Headquarters (See Avert Labs)
- ServicePortal, technical support [168](#)
- specifying file types [149](#)
- start menu [146](#)
- submit a sample to Avert Labs
 - Threat Library [166](#)
 - WebImmune [168](#)
- system startup, scanning at [69](#)
- system tray icon [146](#)

T

- tasks
 - AutoUpdate
 - configuring [56](#)
 - creating [55](#)
 - mirror
 - configuring [59](#)
 - creating [58](#)
 - on-demand
 - configuring [88](#)
 - creating [86](#)
 - immediate [98](#)
 - scheduling [153](#)
 - about [153](#)
 - advanced properties [159](#)
 - log on privileges [155](#)
 - schedule properties [155](#)
 - task properties [154](#)
- technical support
 - accessing from Help menu [167](#)
 - contacting [168](#)
- Threat Center (See Avert Labs)
- threats
 - access protection [127](#)
 - activity log [123](#)
 - buffer overflow [127](#)

- detection alerts and notifications [122](#)
- e-mail scanning [132](#)
- getting information about detections [122](#)
- library [168](#)
- on-access scanning [129](#)
- on-demand scanning [131](#)
- quarantined items [133](#)
- response [121](#)
- scan statistics [123](#)
- taking action [126](#)
- unwanted programs [129](#)
- viewing scan results [122](#)
- training, McAfee resources [168](#)
- tray icon [146](#)
- troubleshooting [135](#)
 - error codes for updating [140](#)
 - frequently asked questions
 - blocked programs [137](#)
 - cookie detections [138](#)
 - general [138](#)
 - installation [137](#)
 - unwanted programs [137](#)
 - Minimum Escalation Requirements Tool [135](#)
 - repair installation utility [136](#)
 - utilities [135](#)

U

- unlocking user interface [16](#)
- unwanted programs [36](#)
 - about [36](#)
 - adding detections [42](#)
 - description [36](#)
 - detection properties [38](#)
 - detections [129](#)
 - enabling for on-access scanner [83](#)
 - enabling for on-demand scanner [95](#)
 - exclusions
 - adding [40](#)
 - by detection type [40](#)
 - frequently asked questions [137](#)
 - policy description [37](#)
 - user-defined detection properties [41](#)
- updating
 - activities [47](#)
 - configuring tasks [56](#)
 - download website
 - FTP [52](#)
 - HTTP [52](#)
 - editing repositories [51](#)
 - error codes [140](#)

- immediate updates [58](#)
- importing repositories [50](#)
- overview of process [46](#)
- proxy settings [54](#)
- repository list [48](#)
- upgrade website [168](#)
- user interface
 - about [142](#)
 - accessing [142](#)
 - command line [146](#)
 - right-click features [145](#)
 - security [13](#)
 - start menu [146](#)
 - system tray icon [146](#)
 - VirusScan Console [143](#)
- user interface security
 - about [13](#)
 - configuring [13](#)
 - display options [13](#)
 - locking and unlocking [16](#)
 - password options [15](#)
- using this guide [8](#)
 - audience [8](#)
- utilities
 - repair installation [136](#)
 - troubleshooting [135](#)

V

- Virus Information Library (See Avert Labs Threat Library)
- VirusScan Console [143](#)
 - configuring
 - AutoUpdate via (See AutoUpdate)
 - on-access scanning via (See on-access scanning)
 - on-demand scanning via (See on-demand scanning)
 - connecting to remote console via [164](#)
- VirusScan Enterprise
 - using features [10](#)
 - what to do first [11](#)

W

- WebImmune, Avert Labs Threat Center [168](#)
- what to do first [11](#)
- wildcards, using in scan items [147](#)