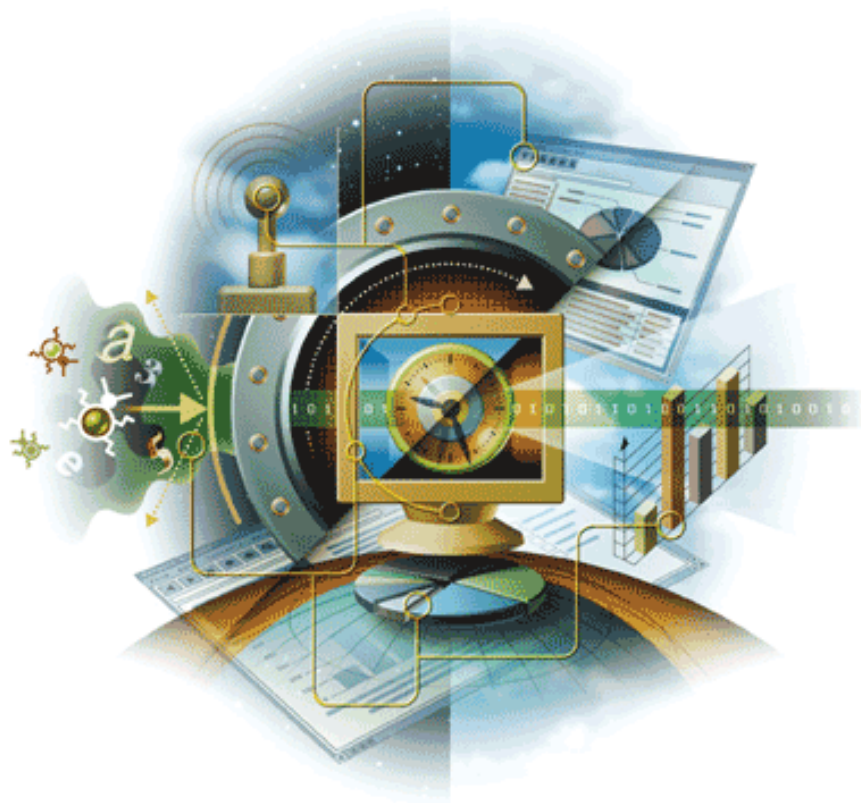


# VirusScan<sup>®</sup> Enterprise

version 8.5i

for use with ePolicy Orchestrator<sup>®</sup> 3.5 or later



**McAfee<sup>®</sup>**  
Proven Security

Industry-leading intrusion prevention solutions

**McAfee<sup>®</sup>**



# VirusScan<sup>®</sup> Enterprise

version 8.5i

for use with ePolicy Orchestrator<sup>®</sup> 3.5 or later

**McAfee<sup>®</sup>**  
Proven Security

Industry-leading intrusion prevention solutions

---

**McAfee<sup>®</sup>**

## 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, MCAFFEE, MCAFFEE (AND IN KATAKANA), MCAFFEE AND DESIGN, MCAFFEE.COM, MCAFFEE 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), WEBSCAN, 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 MCAFFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

### Attributions

This product includes or may include:

- Software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).
- Cryptographic software written by Eric A. Young and software written by Tim J. Hudson.
- Some software programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar Free Software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code. The GPL requires that for any software covered under the GPL which is distributed to someone in an executable binary format, that the source code also be made available to those users. For any such software covered under the GPL, the source code is made available on this CD. If any Free Software licenses require that McAfee provide rights to use, copy or modify a software program that are broader than the rights granted in this agreement, then such rights shall take precedence over the rights and restrictions herein.
- Software originally written by Henry Spencer, Copyright 1992, 1993, 1994, 1997 Henry Spencer.
- Software originally written by Robert Nordier, Copyright © 1996-7 Robert Nordier.
- Software written by Douglas W. Sauder.
- Software developed by the Apache Software Foundation (<http://www.apache.org/>). A copy of the license agreement for this software can be found at [www.apache.org/licenses/LICENSE-2.0.txt](http://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](http://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](mailto: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](mailto: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](mailto: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](mailto: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

<b>1</b>	<b>Getting Started</b>	<b>6</b>
	Using this guide	6
	Audience	6
	Conventions	7
	Placing VirusScan Enterprise under management	8
	Adding policies	9
	Adding new reports	9
	Adding the product package file	10
	Preserving settings during product upgrade	10
	Adding the help package file	11
<b>2</b>	<b>Policies</b>	<b>12</b>
	About configuring policies	13
	Configuring policies	16
	On-Access General Policies	16
	On-Access Default Processes Policies	20
	On-Access Low-Risk Processes Policies	25
	On-Access High-Risk Processes Policies	27
	On-Delivery E-mail Scan Policies	29
	User Interface Policies	35
	Alert Policies	38
	Access Protection Policies	40
	Buffer Overflow Protection Policies	42
	Unwanted Programs Policies	45
	Quarantine Manager Policies	46
	Enforcing policies	46
<b>3</b>	<b>Tasks</b>	<b>47</b>
	About tasks	47
	Creating and configuring tasks	48
	On-demand scan tasks	48
	Update tasks	55
	Restore from quarantine task	57
	Deployment task	59
	Scheduling tasks	61
	Task tab	61
	Schedule tab	62
<b>4</b>	<b>Reports and Queries</b>	<b>63</b>
	Accessing reports and queries	64
	Filtering reports	65
<b>A</b>	<b>Getting More Information</b>	<b>67</b>
	Product documentation	67
	Contact information	68
	<b>Index</b>	<b>69</b>

# 1

## Getting Started

You can use ePolicy Orchestrator® 3.5 or later to centrally manage and enforce VirusScan Enterprise 8.5*i* policies, then review detection reports and queries.

This guide describes how to place VirusScan Enterprise under ePolicy Orchestrator management, configure policies and tasks, and where to find detection information. For additional information about using VirusScan Enterprise or ePolicy Orchestrator, refer to each product's documentation.

We assume that you have installed ePolicy Orchestrator 3.5 or later and have the necessary privileges to perform the steps described in this guide.

This section describes:

- [Using this guide.](#)
- [Placing VirusScan Enterprise under management on page 8.](#)

---

### Using this guide

When using this guide, consider the audience and guide conventions.

### 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.

**Condensed** **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 web site 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.

---

## Placing VirusScan Enterprise under management

These VirusScan Enterprise 8.5i files are used with ePolicy Orchestrator:

- VSE850.NAP — The policies file.
- VSE850REPORTS.NAP — The extended reports file.
- PKGCATALOG.Z — The product package file.
- PKGCATALOG.Z — The online Help package file.
- EPOPOLICYMIGRATION.EXE — The preserve settings executable file.

These files are included in the VirusScan Enterprise 8.5i product package. The product package includes two compressed (.ZIP) files and other product files:

- The product build package .ZIP file contains the product installation files, the two .NAP files, the product package file, and the preserve settings executable file.
- The help package .ZIP file contains the online Help package file and the localized Help files.

This section describes:

- [Adding policies on page 9.](#)
- [Adding new reports on page 9.](#)
- [Adding the product package file on page 10.](#)
- [Preserving settings during product upgrade on page 10.](#)
- [Adding the help package file on page 11.](#)



## Adding policies

The VSE850.NAP file contains the VirusScan Enterprise 8.5i policy pages.

- 1 From the ePolicy Orchestrator console, select **Repository**, then select **Check in NAP** in the details pane.
- 2 Select **Add new software to be managed**, then click **Next**.
- 3 From the **Select a Software Package** dialog box, locate the VSE850.NAP file, then select it and click **Open**.

See [Policies on page 12](#) and [Tasks on page 47](#) for more information.

## Adding new reports

The VSE850REPORTS.NAP file contains the latest VirusScan Enterprise reports. Adding new reports is a two-part process.

### Check the .NAP file in to the Repository

- 1 From the ePolicy Orchestrator console, select **Repository**, then select **Check in NAP** in the details pane.
- 2 Select **Add new reports**, then click **Next**.
- 3 From the **Select a Software Package** dialog box, locate the VSE850REPORTS.NAP file, then select it and click **Open**.

### Add the reports to the Reporting console

After checking the VSE850REPORTS.NAP file in to the repository, you must add the new reports to the **Reporting** console.



Reports are run from the console, not the server. When you check the VSE850REPORTS.NAP file into the **Report Repository**, it is installed on the server. For the console to display the new reports, you must log into the **Reporting** console using ePolicy Orchestrator authentication. When you do, the **Reporting** console recognizes that new reports are available and downloads them.

- 1 In the ePolicy Orchestrator console tree, expand **Reporting**, then expand **ePO Databases**.
- 2 Under **ePO Databases**, right-click a database, then select **Connect** to open the **ePO Database Login** dialog box.



If you are already logged in, you must **Disconnect**, then **Connect** again.

- 3 Type the **Username** and **Password**.
- 4 Ensure that **Authentication Type** is **ePO authentication**, then click **OK**.
- 5 Click **Yes** to download the new reports.

## Adding the product package file

The product PKGCATALOG.Z file contains references to the product installation binary files.

- 1 From the ePolicy Orchestrator console, select **Repository**, then select **Check in package** in the details pane.
- 2 Click **Next** to continue.
- 3 Select **Products or updates**, then click **Next**.
- 4 Specify the path to the product PKGCATALOG.Z file or click **Browse** to locate and select it.



If you created a customized package file with McAfee Installation Designer and plan to use it, you can select it at this time.

- 5 Click **Next**, then click **Finish** to check the package in.

## Preserving settings during product upgrade

The EPOPOLICYMIGRATION.EXE is an executable program that preserves configuration settings from the previous version of VirusScan Enterprise. After installing the .NAP files and the PKGCATALOG.Z files, run this executable on the server where ePolicy Orchestrator is installed.

If you are installing VirusScan Enterprise on a computer with an earlier version of VirusScan Enterprise, you can preserving settings from the earlier version.

- Configuration settings for saved tasks.
- User-specified extensions.
- Exclusions settings.
- Access protection rules are preserved using this logic:
  - 1 The rules from the previous VirusScan Enterprise version are read from the ePolicy Orchestrator database.
  - 2 Each of the VirusScan Enterprise rules are compared against all of the VirusScan Enterprise 8.0 default rules.
  - 3 If no exact match is found when comparing rules to the default rules, then the rule is added to the list of rules to preserve.
  - 4 For port blocking rules, if the rule differs from the default rule only in its inclusions, then the rule is placed in a separate list of rules to be merged with the equivalent VirusScan Enterprise 8.5i rules.
  - 5 The white list for each of the port rules, from [Step 4](#), is merged with the white list of the equivalent VirusScan Enterprise 8.5i rule, and a newly formed rule is written to the ePolicy Orchestrator database for use by VirusScan Enterprise 8.5i.
  - 6 The modified default rules, if any from [Step 3](#), are converted to the new VirusScan Enterprise 8.5i rule format and written to the ePolicy Orchestrator database. These preserved rules are included in the user-defined rules.



The decision to combine the white lists of the port blocking rules that have only had their white list modified is based on the assumption that the user has specific software that they do not want blocked by the default port blocking rule.

- Detection definition (DAT) file version, if the previous version is later than the version in the installation package.
- Scanning engine version, if the previous version is later than the version in the installation package.
- Log file names and locations are preserved.



Although the name and location are preserved, the log file format is changed from ANSI to UTF8. When the format is changed, the log file is renamed to \*.BAK.

The registry keys containing installation file locations and product versions are not preserved.

## Adding the help package file

The online Help PKGCATALOG.Z file contains the localized help files.

- 1 In the ePolicy Orchestrator console tree, select **Repository**, then select **Check in package** in the details pane.
- 2 Click **Next** to continue.
- 3 Select **Products or updates**, then click **Next**.
- 4 Specify the path to the online Help PKGCATALOG.Z file or click **Browse** to locate and select it.
- 5 Click **Next**, then click **Finish** to check the package into the repository.



Deploy this PKGCATALOG.Z file to client computers so that users can download the Help file to their local computers. The first time a user accesses VirusScan Enterprise Help after installing the product, they are asked if they want to download the Help file. We recommend that they click **Yes** to download the Help file and install it in your installation directory.

# 2

## Policies

Configure VirusScan Enterprise policies to protect your environment from viruses, worms, Trojan horses, and potentially unwanted programs and code, then report on detections. Configuration options and descriptions are provided here. For additional information about how VirusScan Enterprise works or configuring options, see the VirusScan Enterprise Product Guide.

This section describes:

- [About configuring policies on page 13.](#)
- [Configuring policies on page 16.](#)
- [Enforcing policies on page 46.](#)

## About configuring policies


Policies are accessed from the ePolicy Orchestrator console:

- 1 In the ePolicy Orchestrator console tree, select the entire **Directory**, a site, a group, or a single computer.
- 2 Select the **Policies** tab in the details pane to display the **Assign Policies for Directory** pane.













Figure 2-1 Assign Policies for Directory



Use the options in this pane to configure product policies, access the **Policy Catalog**, and copy or paste policy assignments.

- 3 Select **Show all products** to expand the list of products, then click  next to **VirusScan Enterprise 8.5.0** to display the policy categories.

**Figure 2-2 VirusScan Enterprise 8.5.0 Policies**

Category	Policy Name	Inherited From	Inherited By	Lock	Edit Row
<b>Enforce Policies</b>	Yes	Global Default	 all inherit	<input type="checkbox"/>	<input type="button" value="Edit"/>
On-Access General Policies	McAfee Default	Global Default	 all inherit	<input type="checkbox"/>	<input type="button" value="Edit"/>
On-Access Default Processes Policies	McAfee Default	Global Default	 all inherit	<input type="checkbox"/>	<input type="button" value="Edit"/>
On-Access Low-Risk Processes Policies	McAfee Default	Global Default	 all inherit	<input type="checkbox"/>	<input type="button" value="Edit"/>
On-Access High-Risk Processes Policies	McAfee Default	Global Default	 all inherit	<input type="checkbox"/>	<input type="button" value="Edit"/>
On Delivery E-Mail Scan Policies	McAfee Default	Global Default	 all inherit	<input type="checkbox"/>	<input type="button" value="Edit"/>
User Interface Policies	McAfee Default	Global Default	 all inherit	<input type="checkbox"/>	<input type="button" value="Edit"/>
Alert Policies	McAfee Default	Global Default	 all inherit	<input type="checkbox"/>	<input type="button" value="Edit"/>
Access Protection Policies	McAfee Default	Global Default	 all inherit	<input type="checkbox"/>	<input type="button" value="Edit"/>
Buffer Overflow Protection Policies	McAfee Default	Global Default	 all inherit	<input type="checkbox"/>	<input type="button" value="Edit"/>
Unwanted Programs Policies	McAfee Default	Global Default	 all inherit	<input type="checkbox"/>	<input type="button" value="Edit"/>
Quarantine Manager Policies	McAfee Default	Global Default	 all inherit	<input type="checkbox"/>	<input type="button" value="Edit"/>

- Each VirusScan Enterprise 8.5.0 policy category corresponds to a feature in VirusScan Enterprise 8.5i and contains configurable options for that feature.



Policies can be created or modified from the **Directory** or **Policy Catalog**. Changing a policy at either of these locations changes the configuration on each node that uses that policy.

- Each policy category has been preconfigured with McAfee defaults. These default configurations cannot be changed, but you can use them to create duplicate policies. You can also create new policies for each category as required.



Click **McAfee Default** to view the default policy configuration.

- 4 To configure a policy, click **Edit**, then under **Policy Name**, select **New Policy** from the drop-down list.

**Figure 2-3 Create Policy**

Create new policy -- Web Page Dialog

Create and edit a duplicate of the following policy:

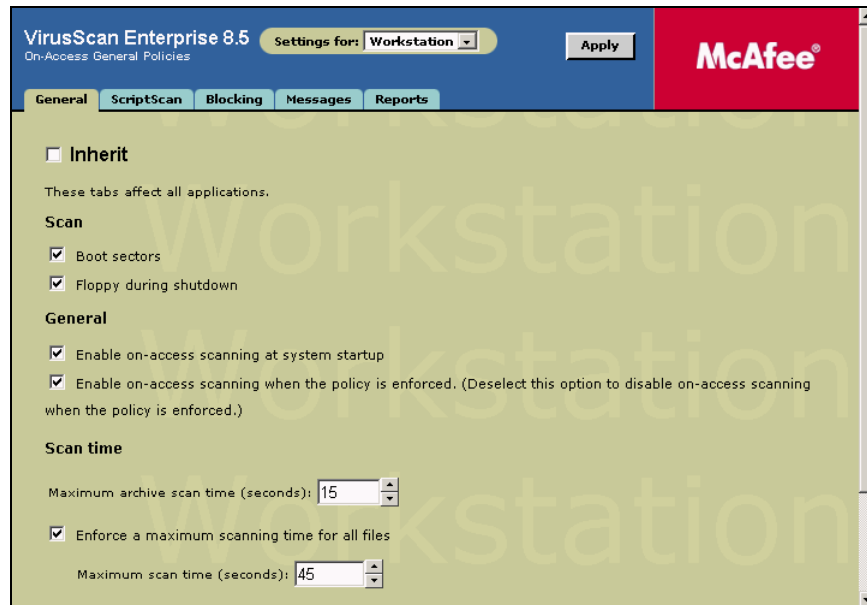
Duplicate the following policy: (McAfee Default)

Create a policy in which all tabs inherit

New policy name:

- a Choose to create a duplicate of an existing policy or create a new policy.
  - b Specify the policy name and click **OK** to open the policy pages for this policy.
- 5 Each policy is configured separately for workstations and servers. Each policy page gives you the option to select **Workstation** or **Server** from the **Settings for** drop-down list. For example:

Figure 2-4 Select Workstation or Server



If you are configuring different policies for workstation and server you must configure them separately. For example, select **Workstation** from the drop-down list and configure the workstation policy options, then select **Server** from the drop-down list and configure the server policy options.



The policy that applies on the client computer depends on the operating system that is installed. For example:

- The workstation policy is applied to computers with Windows NT4 Workstation, Windows 2000 Professional, Windows XP, and Windows Vista operating systems.
- The server policy is applied to computers with Windows NT Server, Windows 2000 Server, Windows Server 2003, and Windows Longhorn operating systems.

---

## Configuring policies

This section describes configuration options for each VirusScan Enterprise component.

Configure these policies:

- [On-Access General Policies](#).
- [On-Access Default Processes Policies](#) on page 20.
- [On-Access Low-Risk Processes Policies](#) on page 25.
- [On-Access High-Risk Processes Policies](#) on page 27.
- [On-Delivery E-mail Scan Policies](#) on page 29.
- [User Interface Policies](#) on page 35.
- [Alert Policies](#) on page 38.
- [Access Protection Policies](#) on page 40.
- [Buffer Overflow Protection Policies](#) on page 42.
- [Unwanted Programs Policies](#) on page 45.
- [Quarantine Manager Policies](#) on page 46.

### On-Access General Policies

The options on these tabs apply to all on-access scanning processes.



This section describes:

- [General tab](#) on page 17.
- [ScriptScan tab](#) on page 17.
- [Blocking tab](#) on page 18.
- [Messages tab](#) on page 18.
- [Reports tab](#) on page 19.




## General tab

Configure general on-access scanning options.

Option or Button	Description
Settings for	Select <b>Workstation</b> (default) or <b>Server</b> from the drop-down list.
Inherit	Deselect this option to configure the policy.
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.
Enable on-access scanning when the policy is enforced.	Enable the on-access scanner each time this policy is enforced.
Maximum archive scan time (seconds)	<p>Specify the maximum archive and scanning time, in seconds, for all files.</p> <p>The time you select for the archive scan must be less than the time you select for scanning all files.</p> <p> <b>Notes and Tips</b></p> <ul style="list-style-type: none"> <li>■ <i>Default = 15 seconds.</i></li> <li>■ 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.</li> </ul>
Enforce a maximum scanning time for all files	Define a maximum scanning time and enforce it for all files.
Maximum scan time (seconds)	<p>Accept the default or select the maximum number of seconds the scanner should spend scanning a file.</p> <p> <b>Notes and Tips</b></p> <p><i>Default = 45 seconds.</i></p>




## ScriptScan tab

Prevent unwanted scripts from executing and specify processes to exclude from detection.

Option or Button	Description
Settings for	Select <b>Workstation</b> (default) or <b>Server</b> from the drop-down list.
Inherit	Deselect this option to configure the policy.
Enable ScriptScan	Scan JavaScript and VBScript scripts before they are executed.
Processes to exclude	<p>Add, edit, or remove ScriptScan exclusions by process name.</p> <p> <b>Notes and Tips</b></p> <p>Wildcards are not allowed when specifying these process names.</p>


## Blocking tab

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

Option or Button	Description
Settings for	Select <b>Workstation</b> (default) or <b>Server</b> from the drop-down list.
Inherit	Deselect this option to configure the policy.
Send a message	Notify the network user on the remote computer when a threat is detected. Type a custom message in the text box.   <b>Notes and Tips</b> 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.   <b>Notes and Tips</b> The <b>On-Access Scan Statistics</b> dialog box displays a list of blocked computers.
Unblock the connection after (minutes)	Unblocks the connection after the specified number of minutes. Enter a number between 1 and 9999.   <b>Notes and Tips</b> <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.

Option or Button	Description
Settings for	Select <b>Workstation</b> (default) or <b>Server</b> from the drop-down list.
Inherit	Deselect this option to configure the policy.
Show the messages dialog box when a detection occurs	Display the <b>On-Access Scan Messages</b> dialog box to local users when a detection occurs.
Text to display in message	Accept the default message or type a custom message.   <b>Notes and Tips</b> <i>Default = VirusScan Alert!</i>
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.

Option or Button	Description
Settings for	Select <b>Workstation</b> (default) or <b>Server</b> from the drop-down list.
Inherit	Deselect this option to configure the policy.
Log to file	<p>Record on-access scanning activity in a log file.</p> <p>Accept the default location for the file or select a new location.</p> <p>The default log name is ONACCESSSCANLOG.TXT.</p> <p>The default location is:</p> <pre>&lt;drive&gt;:\Documents and Settings\All Users\Application Data\McAfee\DesktopProtection\</pre> <p> <b>Notes and Tips</b></p> <ul style="list-style-type: none"> <li>■ 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. You can also use the restore task to restore quarantined items.</li> <li>■ The default location depends on which operating system you are using.</li> </ul>
Limit size of log file	<p>Restrict the log file to the size you specify.</p> <p> <b>Notes and Tips</b></p> <p>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.</p>
Maximum log file size	<p>Specify the maximum size for the log file.</p> <p> <b>Notes and Tips</b></p> <p>Accept the default size (1MB) or set a size from 1MB to 999MB.</p>
Format	<p>Select the format of the log file:</p> <ul style="list-style-type: none"> <li>■ Unicode (UTF8)</li> <li>■ Unicode (UTF16)</li> <li>■ ANSI</li> </ul> <p> <b>Notes and Tips</b></p> <ul style="list-style-type: none"> <li>■ <i>Default = Unicode (UTF8).</i></li> <li>■ The format you choose depends on the information you are storing.</li> </ul> <p>If you are storing western text (every character is one byte), we recommend using the ANSI format.</p> <p>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.</p>
Session settings	Record the properties for each scanning session in the log file.

Option or Button	Description
Session summary	Record a summary of the scanner's actions during each scanning session in the log file.   <b>Notes and Tips</b> 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.
User name	Name of the logged on user when the detection occurred.

## On-Access Default Processes Policies


Configure one scanning policy for all processes or just those defined as default processes. Default processes are any process not specified as low-risk or high-risk. See the *On-Access Scanning* section of the *VirusScan Enterprise Product Guide* for information about assigning risk to assign to a process.

This section describes:

- [Processes tab on page 20.](#)
- [Detection tab on page 21.](#)
- [Advanced tab on page 22.](#)
- [Actions tab on page 23.](#)
- [Unwanted Programs tab on page 24.](#)





### Processes tab

Configure the processes scanning options.

Option or Button	Description
Settings for	Select <b>Workstation</b> (default) or <b>Server</b> from the drop-down list.
Inherit	Deselect this option to configure the policy.
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.   <b>Notes and Tips</b> See the <i>VirusScan Enterprise Product Guide</i> for information about how to assign risk to processes.


## Detection tab

Configure detection options for on-access scanning.

Option or Button	Description
Settings for	Select <b>Workstation</b> (default) or <b>Server</b> from the drop-down list.
Inherit	Deselect this option to configure the policy.
When writing to disk	<p>Scan all files as they are written to or modified on the computer or other data storage device.</p> <p> <b>Notes and Tips</b></p> <p>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.</p>
When reading from disk	Scan all files as they are read from the computer or other data storage device.
On network drives	<p>Scan resources on mapped network drives.</p> <p> <b>Notes and Tips</b></p> <p>Scanning network resources might affect performance.</p>
All files	Scan all files regardless of extension.
Default + additional file types	<p>Scan the default list of extensions plus any additions you specify. The default list is defined by the current DAT file.</p> <ul style="list-style-type: none"> <li>■ Select <b>Default + additional file types</b>.</li> <li>■ Click <b>Additions</b> to open the <b>Additional File Types</b> dialog box.</li> </ul> <p> <b>Notes and Tips</b></p> <p>You cannot delete file types from the <b>Scanned by default</b> list. To exclude file types from this list, use the <b>Exclusions</b> feature.</p>
Also scan for macros in all files	If you selected <b>Default + additional file types</b> , you can also search for known macro threats in all files.
Specified file types	<p>Create a list of user-specified extensions to be scanned. You can also remove any extensions you added previously.</p> <ul style="list-style-type: none"> <li>■ Select <b>Specified file types</b>.</li> <li>■ Click <b>Specified</b> to open the <b>Specified File Types</b> dialog box.</li> </ul>
Overwrite client exclusions	<p>Use only exclusions that are specified in this policy.</p> <p> <b>Notes and Tips</b></p> <p>If this option is not selected, the client computer uses exclusions that were specified locally and the exclusions specified in this policy.</p>



## Advanced tab

Configure heuristic scanning and scanning of compressed files and those opened for backup.

Option or Button	Description
Settings for	Select <b>Workstation</b> (default) or <b>Server</b> from the drop-down list.
Inherit	Deselect this option to configure the policy.
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.
Scan inside archives	Examine archive (compressed) files and their contents.   <b>Notes and Tips</b> <ul style="list-style-type: none"> <li>■ Although it provides better protection, scanning inside archive files can increase the amount of time required to perform a scanning activity.</li> <li>■ If archive scanning is disabled, the on-access scanner still scans the files within the archive if they are extracted and written to disk.</li> </ul>
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.

Option or Button	Description
Settings for	Select <b>Workstation</b> (default) or <b>Server</b> from the drop-down list.
Inherit	Deselect this option to configure the policy.
Primary Action	<p>Select the first action that you want the scanner to take when a threat is detected.</p> <ul style="list-style-type: none"> <li>■ <b>Clean files automatically</b> — The scanner tries to remove the threat from the detected file.</li> <li>■ <b>Deny access to files</b> — Deny all users access to any files with potential threats that the scanner finds.</li> <li>■ <b>Delete files automatically</b> — The scanner deletes files with potential threats as soon as it detects them.</li> </ul> <p> <b>Notes and Tips</b></p> <ul style="list-style-type: none"> <li>■ <i>Default = Clean files automatically.</i></li> <li>■ 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.</li> <li>■ When the scanner denies access to files with potential threats, it also appends the filename with an .mcm extension, when the file is saved.</li> </ul>
Secondary Action	<p>Select the next action you want the scanner to take if the first action fails.</p> <ul style="list-style-type: none"> <li>■ <b>Deny access to files</b> — Deny all users access to any files with potential threats that the scanner finds.</li> <li>■ <b>Delete files automatically</b> — The scanner deletes files with potential threats as soon as it detects them.</li> </ul> <p> <b>Notes and Tips</b></p> <p><i>Default = Delete files automatically.</i></p>

## Unwanted Programs tab

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

Option or Button	Description
Settings for	Select <b>Workstation</b> (default) or <b>Server</b> from the drop-down list.
Inherit	Deselect this option to configure the policy.
Detect unwanted programs	<p>Enables the on-access scanner to detect potentially unwanted programs.</p> <p> <b>Notes and Tips</b></p> <p>The on-access scanner uses the information you configured in the <b>Unwanted Programs Policy</b> to detect potentially unwanted programs. See <a href="#">Unwanted Programs Policies on page 45</a>.</p>
Primary Action	<p>Select the first action that you want the scanner to take when a potentially unwanted program is detected.</p> <ul style="list-style-type: none"> <li>■ <b>Allow access to files</b> — Give users access to detected files and/or programs.</li> <li>■ <b>Clean files automatically</b> — Remove the threat from detected files and/or programs automatically.</li> <li>■ <b>Deny access to files</b> — Prevent users from accessing detected files and/or programs.</li> <li>■ <b>Delete files automatically</b>— Remove detected files and/or programs automatically.</li> </ul> <p> <b>Notes and Tips</b></p> <ul style="list-style-type: none"> <li>■ <i>Default = Clean files automatically.</i></li> <li>■ <b>Allow access to files</b> 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.</li> </ul>
Secondary Action	<p>Select the next action you want the scanner to take if the first action fails.</p> <ul style="list-style-type: none"> <li>■ <b>Allow access to files</b> — Give users access to detected files and/or programs.</li> <li>■ <b>Deny access to files</b> — Prevent users from accessing detected files and/or programs.</li> <li>■ <b>Delete files automatically</b>— Remove detected files and/or programs automatically.</li> </ul> <p> <b>Notes and Tips</b></p> <p><i>Default = Delete files automatically.</i></p>



## On-Access Low-Risk Processes Policies

Open the policy pages, then specify processes that you define as having a low-risk of introducing or spreading threats and configure scanning options for those processes.

This section describes:

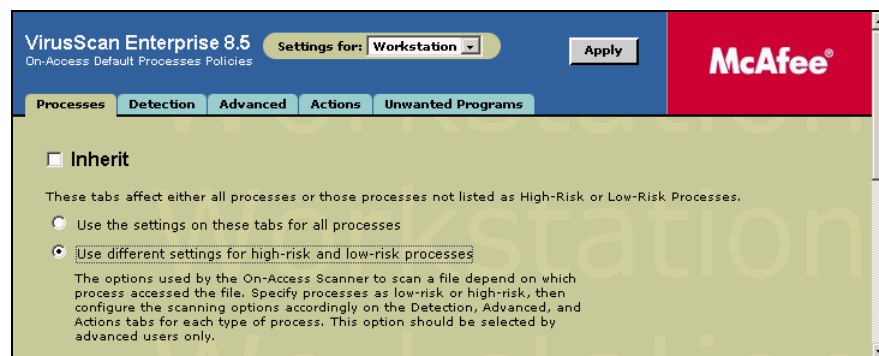
- [Processes tab](#).
- [Detection tab on page 26](#).
- [Advanced tab on page 26](#).
- [Actions tab on page 26](#).
- [Unwanted Programs tab on page 26](#).


### Processes tab

Specifying low-risk processes is a two-part process:

- 1 Select the option to use different settings on the Processes tab of the On-Access Default Process Policies page.

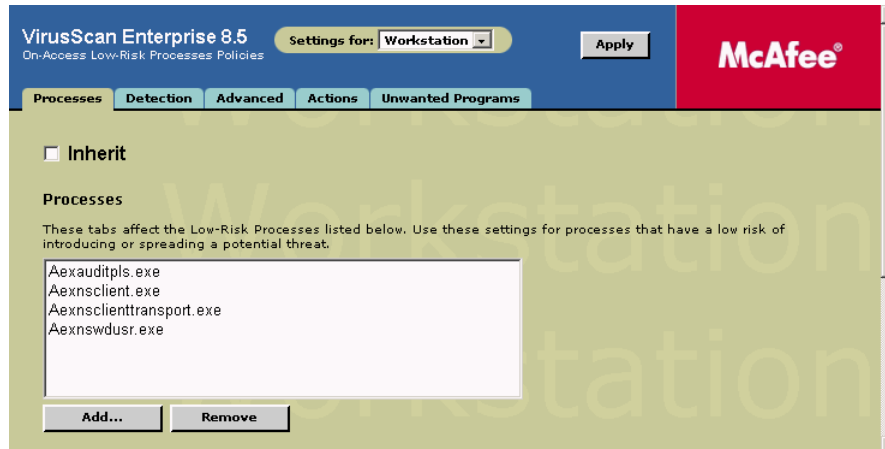
**Figure 2-5 On-Access Default Process Policies — Processes tab**



Option or Button	Description
Settings for	Select <b>Workstation</b> (default) or <b>Server</b> from the drop-down list.
Inherit	Deselect this option to configure the policy.
Use different settings for high-risk and low-risk processes	Configure different scanning policies for low-risk processes.  <b>Notes and Tips</b> See the <i>VirusScan Enterprise Product Guide</i> for information about how to assign risk to processes.

- 2 Specify low-risk processes on the Processes tab of the On-Access Low-Risk Processes Policies page.

**Figure 2-6 On-Access Low-Risk Processes Policies – Processes tab**



Option or Button	Description
Settings for	Select <b>Workstation</b> (default) or <b>Server</b> from the drop-down list.
Inherit	Deselect this option to configure the policy.
Processes	Specify the processes that you consider to be low-risk. <ul style="list-style-type: none"> <li>■ Review the default list of processes.</li> <li>■ Click <b>Add</b> to include new processes in the list.</li> <li>■ Click <b>Remove</b> to delete processes from the list.</li> </ul>
Add	Include processes in the list.
Remove	Delete processes from the list.

### Detection tab

See [Detection tab on page 21](#) for information about configuring these options.

### Advanced tab

See [Advanced tab on page 22](#) for information about configuring these options.

### Actions tab

See [Actions tab on page 23](#) for information about configuring these options.

### Unwanted Programs tab

See [Unwanted Programs tab on page 24](#) for information about configuring these options.

## On-Access High-Risk Processes Policies

Open the policy pages, then specify processes that you define as having a high-risk of introducing or spreading threats and configure scanning options for those processes.

This section describes:

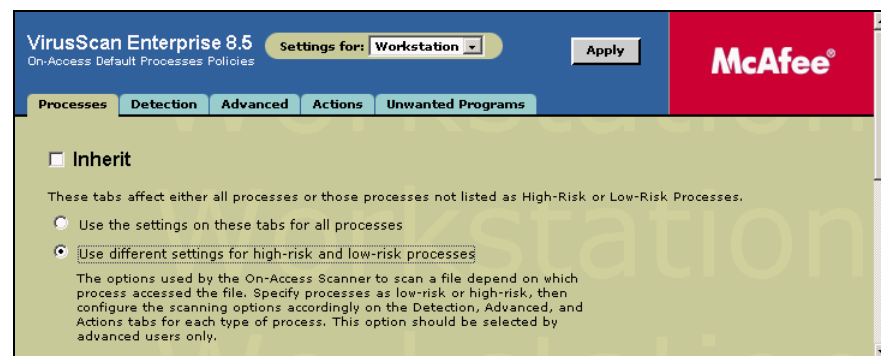
- [Processes tab](#)
- [Detection tab on page 21.](#)
- [Advanced tab on page 22.](#)
- [Actions tab on page 23.](#)
- [Unwanted Programs tab on page 24.](#)


### Processes tab

Specifying high-risk processes is a two-part process:

- 1 Select the option to use different settings on the Processes tab of the On-Access Default Process Policies page.

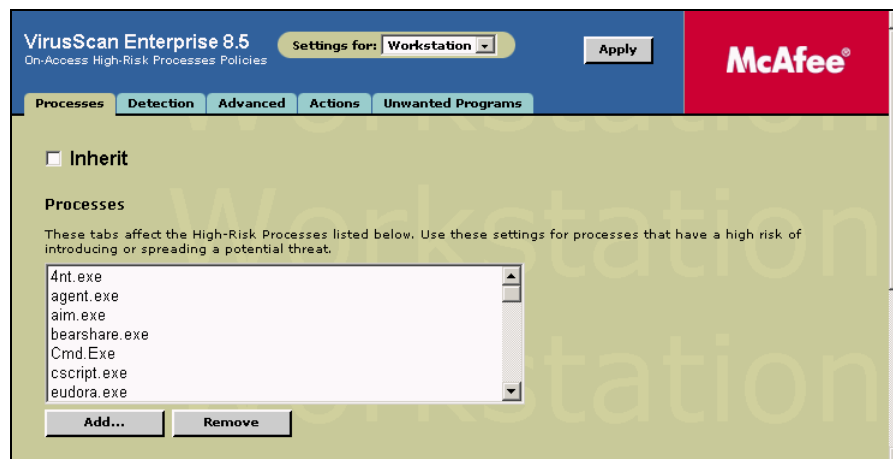
**Figure 2-7 On-Access Default Process Policies — Processes tab**



Option or Button	Description
Settings for	Select <b>Workstation</b> (default) or <b>Server</b> from the drop-down list.
Inherit	Deselect this option to configure the policy.
Use different settings for high-risk and low-risk processes	Configure different scanning policies for high-risk processes.  <b>Notes and Tips</b> See the <i>VirusScan Enterprise Product Guide</i> for information about how to assign risk to processes.

- Specify high-risk processes on the Processes tab of the On-Access High-Risk Processes Policies page.

**Figure 2-8 On-Access High-Risk Processes Policies — Processes tab**



Option or Button	Description
Settings for	Select <b>Workstation</b> (default) or <b>Server</b> from the drop-down list.
Inherit	Deselect this option to configure the policy.
High-Risk Processes	<p>Specify the processes that you consider to be high-risk.</p> <ul style="list-style-type: none"> <li>Review the default list of processes.</li> <li>Click <b>Add</b> to include new processes in the list.</li> <li>Click <b>Remove</b> to delete processes from the list.</li> </ul> <p><b>Notes and Tips</b></p> <ul style="list-style-type: none"> <li>The high-risk scanning policy is initially set the same as default processes to ensure that high-risk processes are scanned in depth.</li> <li>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.</li> </ul>

### Detection tab

See [Detection tab on page 21](#) for information about configuring these options.

### Advanced tab

See [Advanced tab on page 22](#) for information about configuring these options.

### Actions tab

See [Actions tab on page 23](#) for information about configuring these options.

### Unwanted Programs tab

See [Unwanted Programs tab on page 24](#) for information about configuring these options.

## On-Delivery E-mail Scan Policies


Open the policy pages, then configure options for scanning e-mail messages and attachments.

This section describes:

- [Detection tab](#).
- [Advanced tab on page 30](#).
- [Actions tab on page 31](#).
- [Alerts tab on page 32](#).
- [Unwanted Programs tab on page 33](#).
- [Reports tab on page 34](#).
- [Notes Scanner Settings tab on page 35](#).





### Detection tab

Configure options for detecting threats in e-mail and attachments as they are delivered.

Option or Button	Description
Settings for	Select <b>Workstation</b> (default) or <b>Server</b> from the drop-down list.
Inherit	Deselect this option to configure the policy.
Enable on-delivery e-mail scanning	Scan Microsoft Outlook and Lotus Notes e-mail messages and attachments.   <b>Notes and Tips</b> <ul style="list-style-type: none"> <li>■ For Microsoft Outlook, e-mail is scanned on delivery.</li> <li>■ For Lotus Notes, e-mail is scanned when accessed.</li> </ul>
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. <ul style="list-style-type: none"> <li>■ Select <b>Default + additional file types</b>.</li> <li>■ Click <b>Additions</b> to open the <b>Additional File Types</b> dialog box.</li> </ul>
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. <ul style="list-style-type: none"> <li>■ Select <b>Specified file types</b>.</li> <li>■ Click <b>Specified</b> to open the <b>Specified File Types</b> dialog box.</li> </ul>



## Advanced tab


Configure heuristic scanning and scanning of compressed files and Microsoft Outlook e-mail message bodies.

Option or Button	Description
Settings for	Select <b>Workstation</b> (default) or <b>Server</b> from the drop-down list.
Inherit	Deselect this option to configure the policy.
Find unknown program viruses 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.   <b>Notes and Tips</b>  This option is not the same as <b>Also scan for macro viruses in all attachments</b> on the <b>Detection</b> 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.
Find attachments with multiple extensions	Treat attachments with multiple extensions as a threat.   <b>Notes and Tips</b>  When you select this option, an <b>E-mail Scan Warning</b> dialog box appears. Click <b>OK</b> to confirm your selection.
Scan inside archives	Examine archive (compressed) files and their contents.   <b>Notes and Tips</b>  Although it provides better protection, scanning inside archive 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.   <b>Notes and Tips</b>  This option is supported for Microsoft Outlook only.

## Actions tab



Configure which actions to take when an e-mail threat is detected.

Option or Button	Description
Settings for	Select <b>Workstation</b> (default) or <b>Server</b> from the drop-down list.
Inherit	Deselect this option to configure the policy.
Primary Action	<p>Select the first action that you want the scanner to take when a threat is detected.</p> <ul style="list-style-type: none"> <li>■ <b>Clean attachments</b> — The scanner tries to remove the threat from the attachment.</li> <li>■ <b>Prompt for action</b> — Prompt the user for action when a threat is detected. Select this option, then specify which actions users can take under <b>Allowed action in Prompt dialog box</b>. No secondary action is allowed for this option.</li> <li>■ <b>Continue scanning</b> — Continue scanning when an attachment with a threat is detected. No secondary action is allowed for this option.</li> <li>■ <b>Move attachments to a folder</b> — The scanner moves attachments with potential threats to the designated folder.</li> <li>■ <b>Delete attachments</b> — 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.</li> <li>■ <b>Delete mail (for Outlook Scan only)</b> — The scanner deletes mail with potential threats. If you select this option as the primary action, no secondary action is allowed.</li> </ul> <p> <b>Notes and Tips</b></p> <ul style="list-style-type: none"> <li>■ <i>Default = Clean attachments.</i></li> <li>■ 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.</li> </ul>
Secondary Action	<p>Select the next action you want the scanner to take if the first action fails.</p> <ul style="list-style-type: none"> <li>■ <b>Prompt for action</b> — Prompt the user for action when a threat is detected. Select this option, then specify which actions users can take under <b>Allowed action in Prompt dialog box</b>.</li> <li>■ <b>Continue scanning</b> — Continue scanning when an attachment with a threat is detected.</li> <li>■ <b>Move attachments to a folder</b> — The scanner moves attachments with potential threats to the designated folder.</li> <li>■ <b>Delete attachments</b> — 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.</li> <li>■ <b>Delete mail (for Outlook Scan only)</b> — The scanner deletes mail with potential threats.</li> </ul> <p> <b>Notes and Tips</b></p> <p><i>Default = Move attachments to a folder.</i></p>

Option or Button	Description
Move To Folder	<p>Specify the location and name of the quarantine folder.</p> <p> <b>Notes and Tips</b></p> <p>The quarantine folder must be located on a hard drive. It should not be located on a floppy drive or CD drive.</p> <p>The default location for the quarantine folder varies depending on whether you are using Microsoft Outlook or Lotus Notes.</p> <ul style="list-style-type: none"> <li>■ For Microsoft Outlook the quarantine folder is located in the Microsoft Outlook mailbox.</li> <li>■ For Lotus Notes, the quarantine folder is located in the file system.</li> </ul>
Allowed actions in Prompt dialog box	<p>Select the actions that are allowed when the user is prompted for action.</p> <ul style="list-style-type: none"> <li>■ Clean attachment</li> <li>■ Delete attachment</li> <li>■ Move attachment</li> <li>■ Delete mail (for Outlook Scan only)</li> </ul>

## Alerts tab




Configure which actions to take when a threat is detected.

Option or Button	Description
Settings for	Select <b>Workstation</b> (default) or <b>Server</b> from the drop-down list.
Inherit	Deselect this option to configure the policy.
Send alert mail to user	<p>Notify another user when a threatened e-mail message is detected.</p> <p> <b>Notes and Tips</b></p> <p>Select the option and type information in the <b>To</b>, <b>Cc</b>, <b>Subject</b>, and <b>Message</b> text boxes.</p>
Display custom message	<p>If the <b>Prompt for Action</b> option is selected on the <b>Actions</b> tab, you can also display a custom message when a threatened e-mail message is detected.</p> <p>Accept the default message or specify a new one.</p> <p> <b>Notes and Tips</b></p> <p><i>Default message = McAfee VirusScan Enterprise E-mail Scanner Alert!</i></p>







## Unwanted Programs tab


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

Option or Button	Description
Settings for	Select <b>Workstation</b> (default) or <b>Server</b> from the drop-down list.
Inherit	Deselect this option to configure the policy.
Detect unwanted programs	<p>Enables the e-mail scanner to detect potentially unwanted programs.</p> <p> <b>Notes and Tips</b></p> <p>The e-mail scanner uses the settings you configured in the <b>Unwanted Programs Policy</b> to detect potentially unwanted programs. See <a href="#">Unwanted Programs Policies on page 45</a>.</p>
Primary Action	<p>Select the first action that you want the scanner to take when a threat is detected.</p> <ul style="list-style-type: none"> <li>■ <b>Clean attachments</b> — The scanner tries to remove the threat from the attachment.</li> <li>■ <b>Prompt for action</b> — Prompt the user for action when a threat is detected. Select this option, then specify which actions users can take under <b>Allowed action in Prompt dialog box</b>. No secondary action is allowed for this option.</li> <li>■ <b>Continue scanning</b> — Continue scanning when an attachment with a threat is detected. No secondary action is allowed for this option.</li> <li>■ <b>Move attachments to a folder</b> — The scanner moves attachments with potential threats to the designated folder.</li> <li>■ <b>Delete attachments</b> — 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.</li> </ul> <p> <b>Notes and Tips</b></p> <p><i>Default = Clean attachments.</i></p>
Secondary Action	<p>Select the next action you want the scanner to take if the first action fails.</p> <ul style="list-style-type: none"> <li>■ <b>Prompt for action</b> — Prompt the user for action when a threat is detected. Select this option, then specify which actions users can take under <b>Allowed action in Prompt dialog box</b>. No secondary action is allowed for this option.</li> <li>■ <b>Continue scanning</b> — Continue scanning when an attachment with a threat is detected. No secondary action is allowed for this option.</li> <li>■ <b>Move attachments to a folder</b> — The scanner moves attachments with potential threats to the designated folder.</li> <li>■ <b>Delete attachments</b> — 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.</li> </ul> <p> <b>Notes and Tips</b></p> <p><i>Default = Move attachments to a folder.</i></p>

## Reports tab



Configure activity log information.

Option or Button	Description
Settings for	Select <b>Workstation</b> (default) or <b>Server</b> from the drop-down list.
Inherit	Deselect this option to configure the policy.
Log to file	<p>Record e-mail scanning activity in a log file.</p> <p>Accept the default location for the file or select a new location.</p> <p>The default log name is EMAILONDELIVERYLOG.TXT.</p> <p>The default location is</p> <pre>&lt;drive&gt;:\Documents and Settings\All Users\Application Data\McAfee\DesktopProtection\</pre> <p> <b>Notes and Tips</b></p> <ul style="list-style-type: none"> <li>■ 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. You can also use the restore task to restore quarantined items.</li> <li>■ The default location depends on which operating system you are using.</li> </ul>
Limit size of log file	<p>Restrict the log file to the size you specify.</p> <p> <b>Notes and Tips</b></p> <p>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.</p>
Maximum log file size	<p>Specify the maximum size for the log file.</p> <p> <b>Notes and Tips</b></p> <p>Accept the default size (1MB) or set a size from 1MB to 999MB.</p>
Format	<p>Select the format of the log file:</p> <ul style="list-style-type: none"> <li>■ Unicode (UTF8)</li> <li>■ Unicode (UTF16)</li> <li>■ ANSI</li> </ul> <p> <b>Notes and Tips</b></p> <ul style="list-style-type: none"> <li>■ <i>Default = Unicode (UTF8).</i></li> <li>■ The format you choose depends on the information you are storing.</li> </ul> <p>If you are storing western text (every character is one byte), we recommend using the ANSI format.</p> <p>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.</p>
Session settings	Record the properties for each scanning session in the log file.

Option or Button	Description
Session summary	Record a summary of the scanner's actions during each scanning session in the log file.   <b>Notes and Tips</b> 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.

## Notes Scanner Settings tab

Configure Lotus Notes settings for the on-delivery e-mail scanner.

Option or Button	Description
Settings for	Select <b>Workstation</b> (default) or <b>Server</b> from the drop-down list.
Inherit	Deselect this option to configure the policy.
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.   <b>Notes and Tips</b> <i>Default = !!mail\.</i>
Notes Applications to Exclude	Specify which Lotus Notes applications to exclude from scanning.   <b>Notes and Tips</b> <i>Default = MNOTES.</i>

## User Interface Policies




Open the policy pages, then configure security for the VirusScan Enterprise interface.

This section describes:

- [Display Options tab on page 36.](#)
- [Password Options tab on page 37.](#)

## Display Options tab

Specify which system tray options users can access.

Option or Button	Description
Settings for	Select <b>Workstation</b> (default) or <b>Server</b> from the drop-down list.
Inherit	Deselect this option to configure the policy.
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 <b>About VirusScan Enterprise</b> and <b>On-Access Scan Statistics</b> .
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	<p>Connect to remote computers.</p> <p> <b>Notes and Tips</b></p> <ul style="list-style-type: none"> <li>■ You must have administrator rights and the Remote Registry Service must be running.</li> <li>■ See <i>Remote Administration</i> in the <i>VirusScan Enterprise Product Guide</i> for more information.</li> </ul>
Display managed tasks in the client console	Display ePolicy Orchestrator tasks in the VirusScan Console on the client computer.
Disable default AutoUpdate task schedule	<p>Disable the schedule for the default update task.</p> <p> <b>Notes and Tips</b></p> <p>The schedule is disabled when the policy is enforced. The Task Manager service must be running to disable the task's schedule.</p>
Enable splash screen	Display the VirusScan Enterprise splash screen when the VirusScan Console or SHSTAT.EXE is launched.
Preferred language	<p>Specify which language to use for the console text.</p> <p> <b>Notes and Tips</b></p> <ul style="list-style-type: none"> <li>■ The language can be automatically selected or you can select a specific language.</li> <li>■ If you change the preferred language, the change is applied when you restart the computer.</li> </ul>



## Password Options tab

Set password security for the entire system or selected items.

Figure 2-9 User Interface Policies – Password Options tab



Option or Button	Description
Settings for	Select <b>Workstation</b> (default) or <b>Server</b> from the drop-down list.
Inherit	Deselect this option to configure the policy.
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. ⓘ <b>Notes and Tips</b> Setting a password impacts users: <ul style="list-style-type: none"> <li>■ <b>Non-administrators</b> — <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.</li> <li>■ <b>Administrators</b> — <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.</li> </ul>
Password protection for the selected items	Specify one password for selected items in the list. ⓘ <b>Notes and Tips</b> You do not need to enter a password for items that are not locked.

Option or Button	Description
<b>Password protection for conformance to Common Criteria</b>	Secure the interface as required for government agencies that must use only National Information Assurance Partnership (NIAP) Common Criteria validated security products.   <b>Notes and Tips</b> This secures all configuration options from users without administrative credentials except that workstation users can: <ul style="list-style-type: none"> <li>■ Perform an immediate on-demand scan of their own workstation.</li> <li>■ Include or exclude files from an immediate on-demand scan.</li> <li>■ Include or exclude archives, such as a .ZIP file, from an immediate on-demand scan.</li> <li>■ View on-demand scan and on-access scanning activity logs.</li> </ul>
<b>Password</b>	Type the password.
<b>Confirm the password</b>	Type the password again to confirm it.
<b>Items that can be protected by the password</b>	Select the items that you want to protect with the password.   <b>Notes and Tips</b> <ul style="list-style-type: none"> <li>■ A red locked padlock indicates that a password is required for the item.</li> <li>■ A green unlocked padlock indicates that the item is read/write accessible.</li> <li>■ Administrators can lock or unlock the interface through the <b>VirusScan Console</b>.</li> </ul>

## Alert Policies

Open the policy pages, then configure whether to generate alerts and which alerts to generate.

This section describes:

- [Alert Manager Alerts tab on page 39.](#)
- [Additional Alerting Options tab on page 39.](#)

## Alert Manager Alerts tab

Select the components that you want to generate alerts and configure Alert Manager options.

Option or Button	Description
Settings for	Select <b>Workstation</b> (default) or <b>Server</b> from the drop-down list.
Inherit	Deselect this option to configure the policy.
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.
Disable alerting	Do not generate alerts when detections occur.
Enable Centralized alerting	Use centralized alerting to notify you when detections occur.
Enable Alert Manager alerting	Use Alert Manager alerting to notify you when detections occur and specify which Alert Manager server receives alerts.
Specify Alert Manager server to receive alerts	Type the path to the location of the Alert Manager server that receives alerts.
Disable Active Directory Lookup	Do not use Active Directory Lookup.

## Additional Alerting Options tab

Configure filter and local alerting options.

Option or Button	Description
Settings for	Select <b>Workstation</b> (default) or <b>Server</b> from the drop-down list.
Inherit	Deselect this option to configure the policy.
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.

## Access Protection Policies

Open the policy pages, then configure predefined rules or create user-defined rules to protect your computer’s accesses. See the *Access Protection* section of the *VirusScan Enterprise Product Guide* for more information.

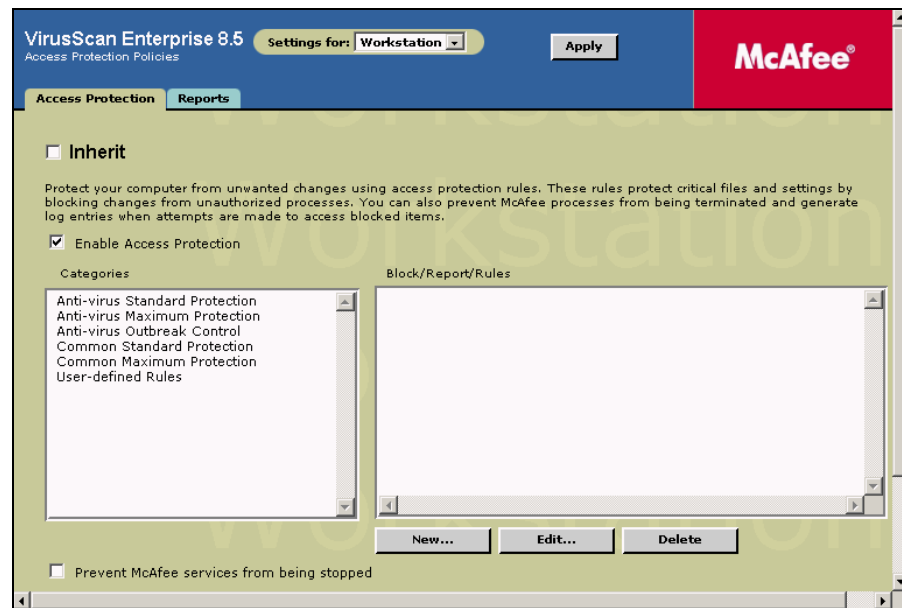
This section describes:


- [Access Protection tab](#).
- [Reports tab on page 42](#).

### Access Protection tab




Configure access protection rules to protect your computer from unwanted changes.

**Figure 2-10 Access Protection Policies — Access Protection tab**







Option or Button	Description
Settings for	Select <b>Workstation</b> (default) or <b>Server</b> from the drop-down list.
Inherit	Deselect this option to configure the policy.
Enable access protection	Enables the access protection feature.   <b>Notes and Tips</b> On-access scanning must also be enabled for access protection to detect access attempts on specified items.



Option or Button	Description
Categories	<p>Click a category to display the list of configured rules for that category. Rules are organized into these categories:</p> <ul style="list-style-type: none"> <li>■ <b>Anti-virus Standard Protection</b> — Anti-virus rules that protect some critical settings and files from being modified, but generally allow you to install and execute legitimate software.</li> <li>■ <b>Anti-virus Maximum Protection</b> — Rules that protect most critical settings and files from modification, but might prevent you from installing legitimate software.</li> <li>■ <b>Anti-virus Outbreak Control</b> — 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.</li> <li>■ <b>Common Standard Protection</b> — Rules that protect some commonly used files and settings from being modified, but generally allow you to install and execute legitimate software.</li> <li>■ <b>Common Maximum Protection</b> — Rules that protect most commonly used files and settings from being modified, but might prevent you from installing legitimate software.</li> <li>■ <b>User-defined Rules</b> — Custom rules defined by the user to supplement the protection provided by the <b>Anti-virus</b> and <b>Common</b> rules.</li> </ul>
Block	<p>Blocks the process that is specified in the <b>Rule Details</b>. Select <b>Block</b> to enable the rule or deselect it to disable the rule.</p> <p> <b>Notes and Tips</b></p> <p>To block access attempts without logging, select <b>Block</b> but do not select <b>Report</b>.</p>
Report	<p>Enables reporting of attempts to violate access protection. When a detection occurs, information is recorded in the activity log.</p> <p> <b>Notes and Tips</b></p> <p>To receive a warning without blocking access attempts, select <b>Report</b>, but do not select <b>Block</b>. 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.</p>
Rules	Use the <b>Anti-virus</b> , <b>Common</b> , and <b>User-defined</b> rules to protect your computer from unwanted changes.
Add	Create a new user-defined rule.
Delete	Remove an existing user-defined rule.
Edit	Change an existing rule.
Prevent McAfee processes from being stopped	<p>Prevent users without debug privileges from terminating McAfee processes.</p> <p> <b>Notes and Tips</b></p> <ul style="list-style-type: none"> <li>■ Users with debug program privileges can still stop McAfee processes even though you select this option.</li> <li>■ 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.</li> </ul>

## Reports tab

Configure activity log information.

Option or Button	Description
Settings for	Select <b>Workstation</b> (default) or <b>Server</b> from the drop-down list.
Inherit	Deselect this option to configure the policy.
Log to file	<p>Record access protection activity in a log file.</p> <p>Accept the default location for the file or select a new location.</p> <p>The default log name is ACCESSPROTECTIONLOG.TXT.</p> <p>The default location is:</p> <pre>&lt;drive&gt;:\Documents and Settings\All Users\Application Data\McAfee\DesktopProtection\</pre> <p> <b>Notes and Tips</b></p> <ul style="list-style-type: none"> <li>■ 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. You can also use the restore task to restore quarantined items.</li> <li>■ The default location depends on which operating system you are using.</li> </ul>
Limit size of log file	<p>Restrict the log file to the size you specify.</p> <p> <b>Notes and Tips</b></p> <p>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.</p>
Maximum log file size	<p>Specify the maximum size for the log file.</p> <p> <b>Notes and Tips</b></p> <p>Accept the default size (1MB) or set a size from 1MB to 999MB.</p>
Format	<p>Select the format of the log file:</p> <ul style="list-style-type: none"> <li>■ Unicode (UTF8)</li> <li>■ Unicode (UTF16)</li> <li>■ ANSI</li> </ul> <p> <b>Notes and Tips</b></p> <ul style="list-style-type: none"> <li>■ <i>Default = Unicode (UTF8).</i></li> <li>■ The format you choose depends on the information you are storing.</li> </ul> <p>If you are storing western text (every character is one byte), we recommend using ANSI format.</p> <p>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.</p>

## Buffer Overflow Protection Policies




Open the policy pages, then configure options to protect your systems from buffer overflow exploits.

This section describes:

- [Buffer Overflow Protection tab on page 43.](#)
- [Reports tab on page 44.](#)





## Buffer Overflow Protection tab

Enable buffer overflow protection, configure the protection mode, and specify processes to exclude from detection.

Option or Button	Description
Settings for	Select <b>Workstation</b> (default) or <b>Server</b> from the drop-down list.
Inherit	Deselect this option to configure the policy.
Enable buffer overflow protection	Enables the buffer overflow protection feature.
Warning mode	<p>Sends a warning when a buffer overflow is detected. No other action is taken.</p> <p> <b>Notes and Tips</b></p> <p>This mode is useful when the full impact of a buffer overflow is not known. Use the feature in <b>Warning Mode</b> for a short while and review the log file during that time to help determine whether to change to <b>Protection Mode</b>.</p>
Protection Mode	<p>Blocks buffer overflows as they are detected and terminates the detected thread.</p> <p> <b>Notes and Tips</b></p> <p>This can also result in termination of the application.</p>
Show the messages dialog box when a buffer overflow is detected	Displays the <b>On-Access Scan Messages</b> dialog box when a detection occurs.
Process	<p>List of process names that are excluded from detection. These can be processes that generate false positives.</p> <p> <b>Notes and Tips</b></p> <ul style="list-style-type: none"> <li>■ Specify the process name that owns the writable memory that is making the call.</li> <li>■ 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.</li> <li>■ Wildcards are not allowed.</li> </ul>
Add	Add a new buffer overflow exclusion.
Edit	Change an existing buffer overflow detection.
Remove	Delete an existing buffer overflow detection.

## Reports tab

Configure activity log information.

Option or Button	Description
Settings for	Select <b>Workstation</b> (default) or <b>Server</b> from the drop-down list.
Inherit	Deselect this option to configure the policy.
Log to file	<p>Record buffer overflow protection activity in a log file.</p> <p>Accept the default location for the file or select a new location.</p> <p>The default log name is BUFFEROVERFLOWPROTECTIONLOG.TXT.</p> <p>The default location is:</p> <pre>&lt;drive&gt;:\Documents and Settings\All Users\Application Data\McAfee\DesktopProtection\</pre> <p> <b>Notes and Tips</b></p> <ul style="list-style-type: none"> <li>■ 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. You can also use the restore task to restore quarantined items.</li> <li>■ The default location depends on which operating system you are using.</li> </ul>
Limit size of log file	<p>Restrict the log file to the size you specify.</p> <p> <b>Notes and Tips</b></p> <p>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.</p>
Maximum log file size	<p>Specify the maximum size for the log file.</p> <p> <b>Notes and Tips</b></p> <p>Accept the default size (1MB) or set a size from 1MB to 999MB.</p>
Format	<p>Select the format of the log file:</p> <ul style="list-style-type: none"> <li>■ Unicode (UTF8)</li> <li>■ Unicode (UTF16)</li> <li>■ ANSI</li> </ul> <p> <b>Notes and Tips</b></p> <ul style="list-style-type: none"> <li>■ <i>Default = Unicode (UTF8).</i></li> <li>■ The format you choose depends on which information you are storing.</li> </ul> <p>If you are storing western text (every character is one byte), we recommend using the ANSI format.</p> <p>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.</p>

## Unwanted Programs Policies

Open the policy pages, then configure options to protect your computer from unwanted programs that are a nuisance or present a security risk.

This section describes:

- [Detection tab](#).
- [User-Defined Detection tab](#).

### Detection tab

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

Option or Button	Description
Settings for	Select <b>Workstation</b> (default) or <b>Server</b> from the drop-down list.
Inherit	Deselect this option to configure the policy.
Detections from DATs	Specify the categories of potentially unwanted programs to detect.
Exclusions	Specify items by detection name to exclude from detection.

### User-Defined Detection tab

Specify individual files or programs to treat as unwanted programs.

Option or Button	Description
Settings for	Select <b>Workstation</b> (default) or <b>Server</b> from the drop-down list.
Inherit	Deselect this option to configure the policy.
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.

## Quarantine Manager Policies

Open the policy page, then specify the location of the quarantine directory and configure the policy to automatically delete quarantined items after a specified number of days.

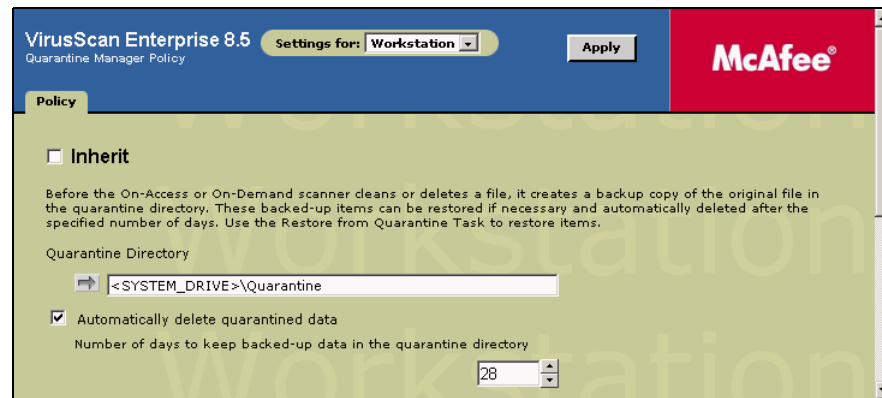


Use the **Restore Task** to restore quarantined items.

### Policy tab

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

**Figure 2-11 Quarantine Manager Policies – Policy tab**



Option or Button	Description
Settings for	Select <b>Workstation</b> (default) or <b>Server</b> from the drop-down list.
Inherit	Deselect this option to configure the policy.
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. <b>Notes and Tips</b> Choose from 1 to 999 days.

## Enforcing policies

After configuring policies, they must be enforced to make them available for the ePolicy Orchestrator agent. Policies are automatically enforced at the next Agent to Server Connection Interval (ASCI), or you can perform an **Agent Wakeup** to apply changes immediately.

The **Enforce Policies** option is set to **Yes** by default to ensure policies are enforced on a regular basis. We do not recommend that you change the default policy configuration.

# 3

## Tasks

Create, configure, and schedule tasks to perform on-demand scans, update the DAT file or scanning engine, mirror sites, restore items from quarantine, and deploy the product or product updates.

This section describes:

- [About tasks.](#)
- [Creating and configuring tasks.](#)
- [Scheduling tasks on page 61.](#)

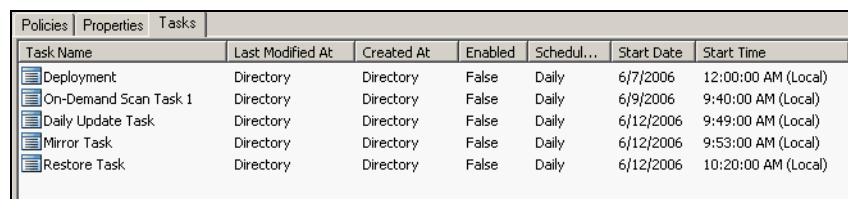
---

### About tasks

Access tasks from the ePolicy Orchestrator console:

- 1 In the console tree under ePolicy Orchestrator, select **Directory**, a site, a group, or a single computer.
- 2 Select the **Tasks** tab to display the current tasks.

**Figure 3-1 Tasks**



Task Name	Last Modified At	Created At	Enabled	Schedul...	Start Date	Start Time
Deployment	Directory	Directory	False	Daily	6/7/2006	12:00:00 AM (Local)
On-Demand Scan Task 1	Directory	Directory	False	Daily	6/9/2006	9:40:00 AM (Local)
Daily Update Task	Directory	Directory	False	Daily	6/12/2006	9:49:00 AM (Local)
Mirror Task	Directory	Directory	False	Daily	6/12/2006	9:53:00 AM (Local)
Restore Task	Directory	Directory	False	Daily	6/12/2006	10:20:00 AM (Local)

- 3 If you created tasks at different levels of the directory tree, select the node to display its tasks.

## Creating and configuring tasks

This section describes:

- [On-demand scan tasks.](#)
- [Update tasks on page 55.](#)
- [Restore from quarantine task on page 57.](#)
- [Deployment task on page 59.](#)

### On-demand scan tasks

This section describes:

- [Creating on-demand scan tasks on page 48.](#)
- [Configuring on-demand scan task settings on page 49.](#)

### Creating on-demand scan tasks

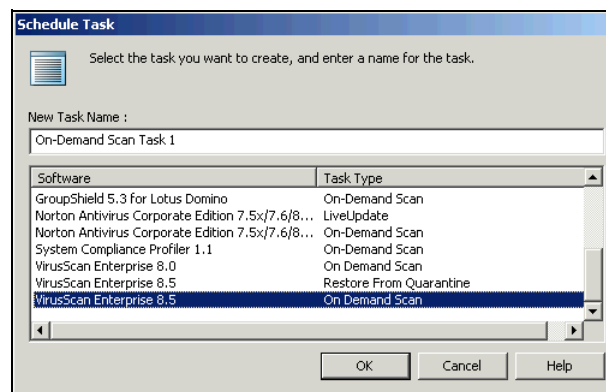
Create and configure as many on-demand scan tasks as you require.



The on-demand scan task you create is by default equivalent to the **Full Scan** task in the VirusScan Enterprise console.

- 1 In the console tree under ePolicy Orchestrator, right-click **Directory** or the desired site, group, or computer, then select **Schedule Task**.

**Figure 3-2 New On-Demand Scan Task**



- 2 Type a New Task Name.
- 3 Select **VirusScan Enterprise 8.5 — On-Demand Scan** from the **Software/Task Type** list.
- 4 Click **OK** to create the task.

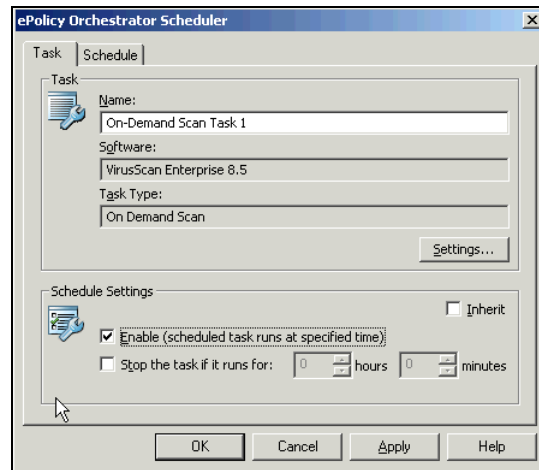


## Configuring on-demand scan task settings

On the Tasks tab in the details pane, right-click the task, then select **Edit Task**.

The ePolicy Orchestrator Scheduler dialog box appears.

**Figure 3-3 ePolicy Orchestrator Scheduler**




Click **Settings** to open the Task Settings dialog box.

This section describes:

- [Where tab on page 50.](#)
- [Detection tab on page 51.](#)
- [Advanced tab on page 52.](#)
- [Actions tab on page 52.](#)
- [Reports tab on page 53.](#)
- [Task tab on page 54.](#)




## Where tab

Configure the item types and locations to scan.

Option or Button	Description
Inherit	Deselect this option to configure the policy.
Item Name	<p>Select the items to scan. Click <b>Add</b>, <b>Edit</b>, or <b>Remove</b> to change the items in the list.</p> <ul style="list-style-type: none"> <li>■ <b>Memory for rootkits.</b> 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.</li> <li>■ <b>Running processes.</b> Scans the memory of all running processes. Actions other than <b>Clean</b> are treated as <b>Continue scanning</b>.</li> <li>■ <b>Registered Files.</b> 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.</li> <li>■ <b>My computer.</b> Scans all drives physically attached to your computer or logically mapped to a drive letter on your computer.</li> <li>■ <b>All local drives.</b> Scans all drives and their subfolders on your computer.</li> <li>■ <b>All fixed drives.</b> Scans all drives physically connected to your computer.</li> <li>■ <b>All removable drives.</b> Scans all removable drives or other storage devices connected to your computer.</li> <li>■ <b>All mapped drives.</b> Scans network drives logically mapped to a network drive on your computer.</li> <li>■ <b>Home folder.</b> Scans the home folder of the user who starts the scan.</li> <li>■ <b>User Profile folder.</b> Scans the profile of the user who starts the scan, including the user's <b>My Documents</b> folder.</li> <li>■ <b>Windows folder.</b> Scans the contents of the Windows folder.</li> <li>■ <b>Program Files folder.</b> Scans the contents of the Program Files folder.</li> <li>■ <b>Temp folder.</b> Scans the contents of the Temp folder.</li> <li>■ <b>Recycle bin.</b> Scans the contents of the recycle bin.</li> <li>■ <b>Drive or folder.</b> Scans the specified drive or folder.</li> <li>■ <b>File.</b> Scans the specified file.</li> </ul> <p> <b>Notes and Tips</b></p> <ul style="list-style-type: none"> <li>■ <i>Default = Memory for rootkits, running processes, and all local drives.</i></li> <li>■ 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.</li> </ul>
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.


**Detection tab**

Configure detection options.

Option or Button	Description
Inherit	Deselect this option to configure the policy.
All files	Scan all files, regardless of extension.
Default + additional file types	<p>Scan the default list of extensions plus any additions you specify. The default list is defined by the current DAT file.</p> <ul style="list-style-type: none"> <li>■ Select <b>Default + additional file types</b>.</li> <li>■ Click <b>Additions</b> to open the <b>Additional File Types</b> dialog box.</li> </ul> <p> <b>Notes and Tips</b></p> <p>You cannot delete file types from the <b>Scanned by default</b> list. To exclude file types from this list, use the <b>Exclusions</b> feature.</p>
Specified file types	<p>Create a list of user-specified extensions to be scanned. You can also remove any extensions you added previously.</p> <ul style="list-style-type: none"> <li>■ Select <b>Specified file types</b>.</li> <li>■ Click <b>Specified</b> to open the <b>Specified File Types</b> dialog box.</li> </ul>
Overwrite client exclusions	<p>Use only exclusions that are specified in this policy.</p> <p> <b>Notes and Tips</b></p> <p>If this option is not selected, the client computer uses exclusions that were specified locally and the exclusions specified in this policy.</p>
Exclude disks, files, and folders	<p>Create a list of files, folders, and drives to exclude from scanning. You can also remove exclusions that you previously specified.</p> <p>Click <b>Exclusions</b> to open the <b>Set Exclusions</b> dialog box.</p>
Scan inside archives	<p>Examine archive (compressed) files and their contents.</p> <p> <b>Notes and Tips</b></p> <ul style="list-style-type: none"> <li>■ Although it provides better protection, scanning inside archive files can increase the amount of time required to perform a scanning activity.</li> <li>■ If archive scanning is disabled, the on-access scanner still scans the files within the archive if they are extracted and written to disk.</li> </ul>
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.

Option or Button	Description
Inherit	Deselect this option to configure the policy.
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.
System utilization	Use the slider to set the utilization level for the scan. Each task runs independently; unaware of the limits for other tasks.   <b>Notes and Tips</b> <i>Default = 30%.</i>



### Actions tab

Configure which actions to take when a threat is detected.

Option or Button	Description
Inherit	Deselect this option to configure the policy.
Primary Action	Select the first action that you want the scanner to take when a threat is detected. <ul style="list-style-type: none"> <li>■ <b>Clean</b> — The scanner tries to remove the threat from the detected file.</li> <li>■ <b>Continue scanning</b> — Continue scanning when a file is detected. No secondary action is allowed for this option.</li> <li>■ <b>Delete</b> — The scanner deletes the entire file, document, or archive.</li> </ul>  <b>Notes and Tips</b> <ul style="list-style-type: none"> <li>■ <i>Default = Clean.</i></li> <li>■ 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.</li> <li>■ If the action is set to delete and a file within an archive is detected, the entire archive file is deleted.</li> </ul>
Secondary Action	Select the next action you want the scanner to take if the first action fails. <ul style="list-style-type: none"> <li>■ <b>Continue scanning</b> — Continue scanning when a file is detected.</li> <li>■ <b>Delete</b> — The scanner deletes the entire file, document, or archive.</li> </ul>  <b>Notes and Tips</b> <i>Default = Delete.</i>




## Unwanted Programs tab



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

Option or Button	Description
Inherit	Deselect this option to configure the policy.
Primary Action	<p>Select the first action that you want the scanner to take when a threat is detected.</p> <ul style="list-style-type: none"> <li>■ <b>Clean</b> — The scanner tries to remove the threat from the detected file.</li> <li>■ <b>Continue scanning</b> — Continue scanning when a file is detected. No secondary action is allowed for this option.</li> <li>■ <b>Delete</b> — The scanner deletes the entire file, document, or archive.</li> </ul> <p> <b>Notes and Tips</b> <i>Default = Clean.</i></p>
Secondary Action	<p>Select the next action you want the scanner to take if the first action fails.</p> <ul style="list-style-type: none"> <li>■ <b>Continue scanning</b> — Continue scanning when a file is detected.</li> <li>■ <b>Delete</b> — The scanner deletes the entire file, document, or archive.</li> </ul> <p> <b>Notes and Tips</b> <i>Default = Delete.</i></p>

## Reports tab


Configure activity log information.

Option or Button	Description
Log to file	<p>Record on-demand scanning activity in a log file.</p> <p>Accept the default location for the file or select a new location.</p> <p>The default log name is ONDEMANDSCANLOG.TXT.</p> <p>The default location is</p> <pre>&lt;drive&gt;:\Documents and Settings\All Users\Application Data\McAfee\DesktopProtection\</pre> <p> <b>Notes and Tips</b></p> <ul style="list-style-type: none"> <li>■ 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. You can also use the restore task to restore quarantined items.</li> <li>■ The default location depends on which operating system you are using.</li> </ul>
Limit size of log file	<p>Restrict the log file to the size you specify.</p> <p> <b>Notes and Tips</b></p> <p>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.</p>
Maximum log file size	<p>Specify the maximum size for the log file.</p> <p> <b>Notes and Tips</b></p> <p>Accept the default size (1MB) or set a size from 1MB to 999MB.</p>

Option or Button	Description
Format	<p>Select the format of the log file:</p> <ul style="list-style-type: none"> <li>■ Unicode (UTF8)</li> <li>■ Unicode (UTF16)</li> <li>■ ANSI</li> </ul> <p> <b>Notes and Tips</b></p> <ul style="list-style-type: none"> <li>■ <i>Default = Unicode (UTF8).</i></li> <li>■ The format you choose depends on the information you are storing.</li> </ul> <p>If you are storing western text (every character is one byte), we recommend using the ANSI format.</p> <p>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.</p>
Session settings	Record the properties for each scanning session in the log file.
Session summary	<p>Record a summary of the scanner's actions during each scanning session in the log file.</p> <p> <b>Notes and Tips</b></p> <p>Summary information includes the number of files scanned, the number and type of detections, the number of files cleaned or deleted, and other information.</p>
Failure to scan encrypted files	Record the name of encrypted files that the scanner failed to scan.
User name	Name of the logged on user when the detection occurred.

### Task tab

Specify the platforms where this on-demand task runs.

Option or Button	Description
Run this task on workstations and servers	Run this on-demand scan task on both workstations and servers.
Only run this task on servers	Run this on-demand scan task on servers.
Only run this task on workstations	Run this on-demand scan task on workstations.
User	<p>Specify the user's account name.</p> <p> <b>Notes and Tips</b></p> <p>If no account information is entered, the task runs under the system account.</p>
Password	Type the password.
Domain	Type the domain.

## Update tasks

Update tasks can be used to perform immediate or scheduled updates of the detection definition (DAT) files, the scanning engine, Service Packs, Patches, and the EXTRA.DAT file. Create as many update tasks as required.

This section describes:

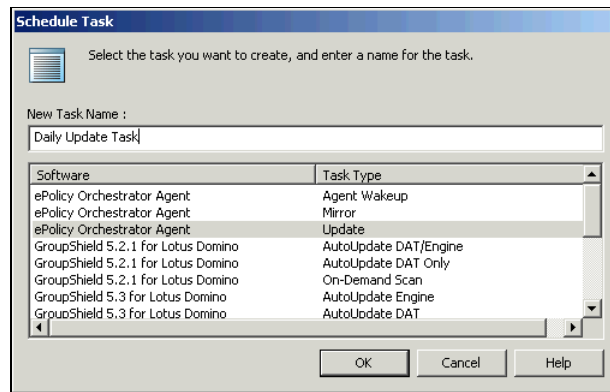
- [Creating an update task.](#)
- [Configuring the update task settings on page 56.](#)

### Creating an update task

- 1 In the console tree under ePolicy Orchestrator, right-click Directory or the desired site, group, or computer, then select Schedule Task.

The Schedule Task dialog box appears.

**Figure 3-4 New Update Task**



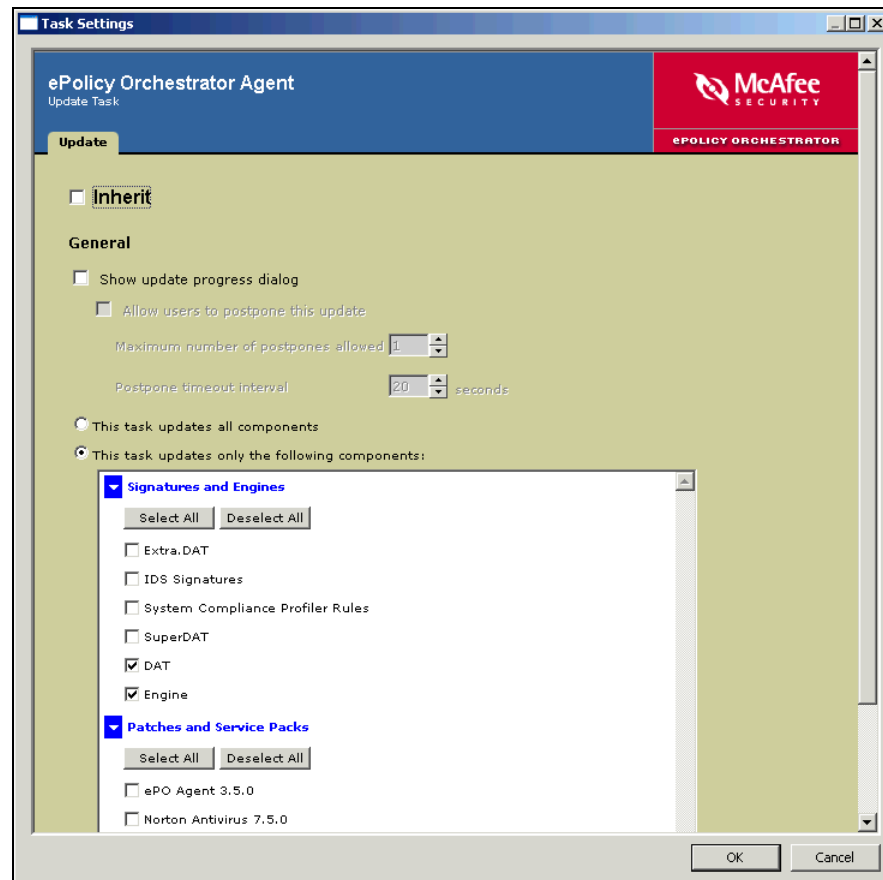
- 2 Type a New Task Name.
- 3 Select ePolicy Orchestrator Agent — Update from the Software/Task Type list.
- 4 Click OK to create the task.

## Configuring the update task settings

Configure and schedule update tasks to meet your needs.

- 1 On the Tasks tab in the details pane, right-click the update task, then select **Edit Task**.
- 2 Click **Settings** to display the Task Settings dialog box.

**Figure 3-5 ePolicy Orchestrator — Update Task**



Option or Button	Description
Inherit	Deselect this option to configure the policy.
Show update progress dialog	Displays the update progress dialog box on the client computer.
Allow users to postpone this update	Gives users the opportunity to delay running this task.
Maximum number of postpones allowed	Specify the number of times a user can postpone this task.
Postpone timeout interval	Specify the length of time before a task runs that a user can postpone the task.
This task updates all components	Update all components.
This task updates only the following components	Update only the selected components.



## Restore from quarantine task

Use the restore task to restore quarantined items.

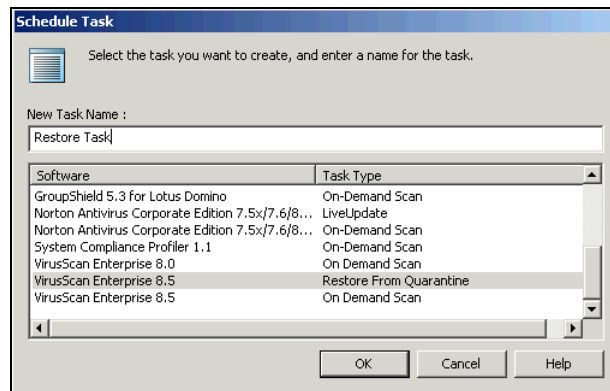
This section describes:

- [Creating a restore task.](#)
- [Configuring the restore task on page 57.](#)

### Creating a restore task

- 1 In the console tree under ePolicy Orchestrator, right-click Directory or the desired site, group, or computer, then select Schedule Task.

**Figure 3-6 Restore From Quarantine Task**



- 2 Type a New Task Name.
- 3 Select VirusScan Enterprise 8.5 — Restore From Quarantine from the Software/Task Type list.
- 4 Click OK to create the task.

### Configuring the restore task

- 1 On the Tasks tab in the details pane, right-click the Restore Task, then select Edit Task.
- 2 Click Settings to display the Task Settings dialog box.

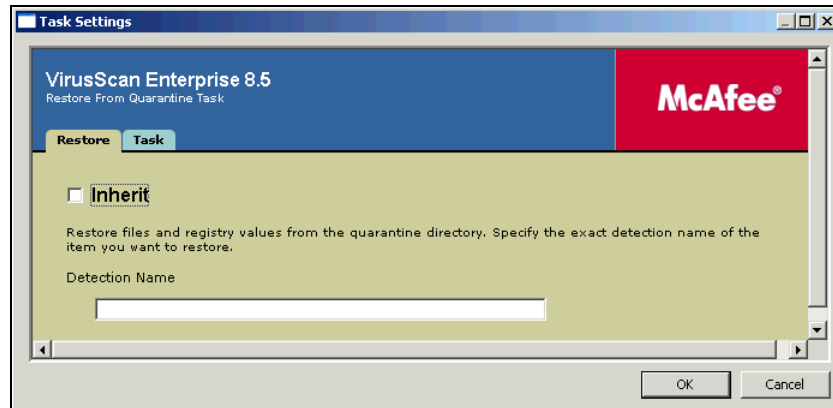
This section describes:

- [Restore tab on page 58.](#)
- [Task tab on page 59.](#)

### Restore tab

Specify the name of the quarantined item to restore.

**Figure 3-7 Restore Task – Restore tab**

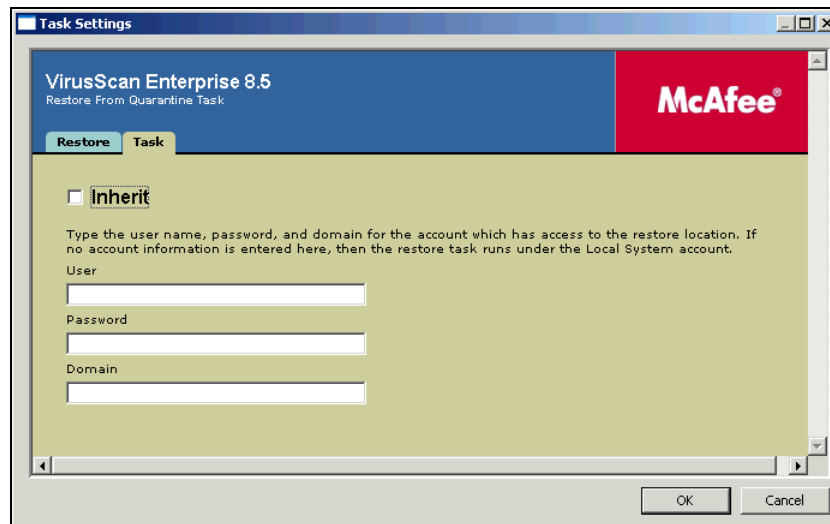


Option or Button	Description
Inherit	Deselect this option to configure the policy.
Detection Name	Specify the exact name of the item to restore from the quarantine directory.

## Task tab

The restore task runs under the system account by default unless you specify a different user name, password, and domain here.

**Figure 3-8 Restore Task – Task tab**



Option or Button	Description
Inherit	Deselect this option to configure the policy.
User	Type the name of the user which has access to the restore location.
Password	Type a password for the specified user.
Domain	Type the domain for the specified user.

## Deployment task

The deployment task deploys the managed product to client computers.

This section describes:

- [Using the default deployment task.](#)
- [Configuring the deployment task settings on page 60.](#)

### Using the default deployment task

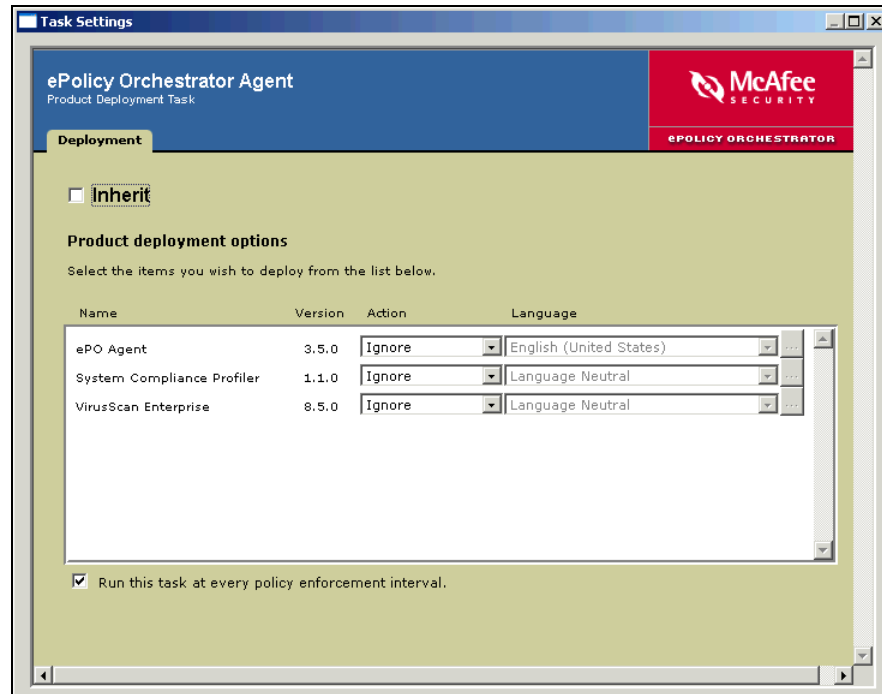
A deployment task is created by default and already exists on the **Tasks** tab in the details pane.



## Configuring the deployment task settings

You can configure and schedule this task to meet your needs

- 1 On the Tasks tab in the details pane, right-click the **Deployment** task, then select **Edit Task**.
- 2 Click **Settings** to display the Task Settings dialog box.

**Figure 3-9 Deployment Task**



Option or Button	Description
Inherit	Deselect this option to configure the policy.
Action	Select <b>Install</b> or <b>Remove</b> for each item.   <b>Notes and Tips</b> This list includes only those products that have been checked into the repository.
Language	Select the language for the product you are deploying.
	Click to specify a command-line option.
Run this task at every policy enforcement interval	Deploy the specified products at every policy enforcement interval.

## Scheduling tasks

Schedule a task to run at specific dates and time, or specific intervals.

Settings can be configured for these tabs:

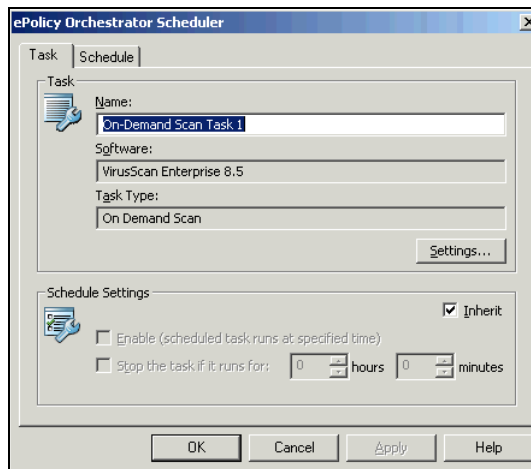
- [Task tab](#).
- [Schedule tab on page 62](#).



## Task tab

Enable the schedule for the selected task.

- 1 On the Tasks tab in the details pane, right-click the task, then select **Edit Task** to open the ePolicy Orchestrator Scheduler dialog box.
- 2 Select the Task tab.

**Figure 3-10 ePolicy Orchestrator Scheduler – Task tab**



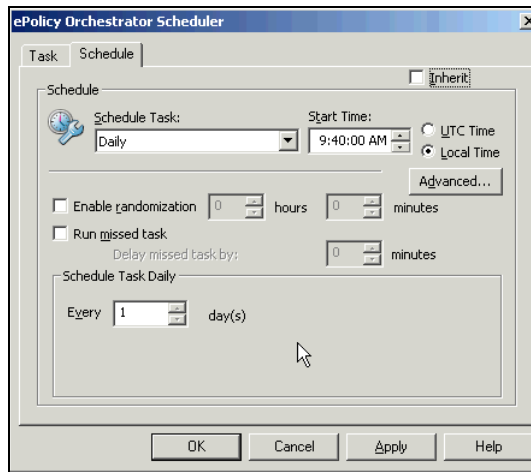
Option or Button	Description
Inherit	Deselect this option to configure the policy.
Enable (scheduled task runs at specified time)	Schedule the task to run at a specified time.  <b>Notes and Tips</b> This option must be selected to schedule the task.
Stop the task if it runs for	Stop the task after the number of hours and/or minutes that you specify.  <b>Notes and Tips</b> If the task is interrupted before it completes, the next time it starts it resumes scanning from where it left off.




## Schedule tab

Specify when the task runs.

From the ePolicy Orchestrator Scheduler dialog box, select the Schedule tab.

**Figure 3-11 ePolicy Orchestrator Scheduler — Schedule tab**



Option or Button	Description
Inherit	Deselect this option to configure the policy.
Schedule Task	Enables the schedule for this task.   <b>Notes and Tips</b> This option must be selected to start the task at the scheduled interval.
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.   <b>Notes and Tips</b> <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.   <b>Notes and Tips</b> <ol style="list-style-type: none"> <li>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.</li> <li>This option is not available when scheduling the task <b>At Startup</b>, <b>At Logon</b>, or <b>When Idle</b>.</li> </ol>

See the Scheduling section of the *VirusScan Enterprise Product Guide* for a complete description of scheduling options.

# 4

## Reports and Queries

View VirusScan Enterprise detections using ePolicy Orchestrator reports and queries.

This section describes:

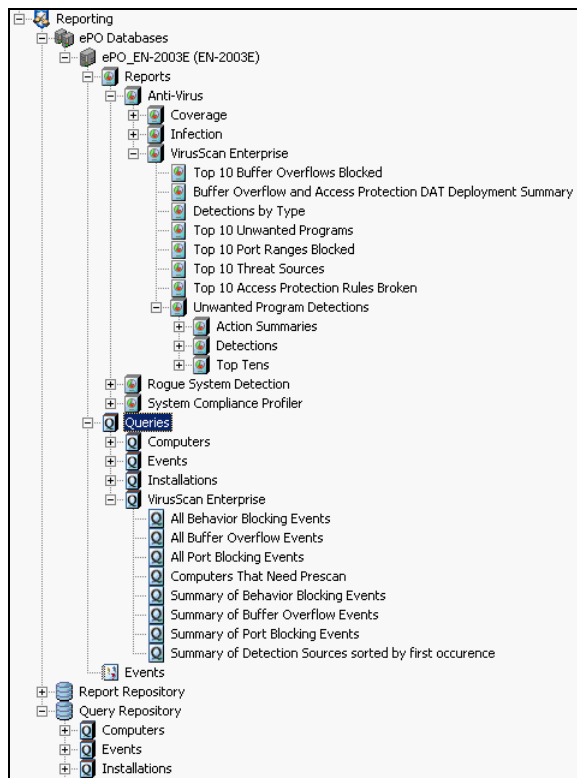
- [Accessing reports and queries on page 64.](#)
- [Filtering reports on page 65.](#)

## Accessing reports and queries

To access ePolicy Orchestrator reports and queries:

- 1 From the ePolicy Orchestrator console, expand Reporting.
- 2 Expand ePO Databases, then select the ePO <server name> and log on with ePO Authentication.
- 3 Expand Reports, then expand Anti-Virus | VirusScan Enterprise to view reports.
- 4 Expand Queries, then expand VirusScan Enterprise to view queries.

Figure 4-1 Reports and queries





## Filtering reports

In addition to using the anti-virus specific reports, you can configure filters for any of the standard anti-virus detection reports to display events specific to unwanted programs or to display only virus or Trojan activity. When you run a report, you can set a data filter for the report. You can also combine multiple filters to perform a more specific search.

Some filter configuration examples follow. Note that some entries are case specific.

### Viruses Detected

This report lists all types of malware and unwanted programs detected in your environment. You can filter out potentially unwanted programs and view only virus related detections.

This example filters out potentially unwanted programs based on the Event ID. Potentially unwanted program detections begin with the number 2.

Filter out potentially unwanted programs:

Data Filter Tab	Condition	Term / Variable
Event ID	Starting with	2



Use this Event ID to filter potentially unwanted programs out of other reports, such as **Infection History** and **Infections Detected Monthly**.

Filter out everything except potentially unwanted programs:

Data Filter Tab	Condition	Term / Variable
Event ID	Not starting with	2

Add an additional filter on the Detection tab to filter cookies out of the potentially unwanted programs:

Data Filter Tab	Condition	Term / Variable
Event ID	Starting with	2
Detection	Not starting with	Cookie

*Cookie* is case sensitive.

### Number of Infections Detected Monthly Showing Viruses

This filter works by inclusion to search on select threat types.

Filter out everything except Trojan horse detections:

Data Filter Tab	Condition	Term / Variable
Type	Equal to	Trojan

Filter out everything except Trojan horse and worm detections:

Data Filter Tab	Condition	Term / Variable
Type	Equal to	Trojan
		Worm

### Infection History

Filter this report to determine when potentially unwanted program detections occurred over time. It begins by displaying **Infections by Year**, then you can drill down to see other time periods such as **Year to Date** and **Quarter to Date**.

Filter using the detection type. All detection types for potentially unwanted programs start with *app\_*:

Data Filter Tab	Condition	Term / Variable
Detection	Starting with	app_

You can also remove all filters from the **Infection History** report to display the relationship of potentially unwanted program detections compared to virus detections.

Remove filters:

Data Filter Tab	Condition	Term / Variable
None		

### Top 10 Detected Viruses

This report lists the top ten malware detections in your environment. This information allows you to determine if potentially unwanted programs constitute a large percentage of your overall detections. You can drill down to see additional details.

Recommended filter configuration:

Data Filter	Tab	Condition	Term / Variable
None			

# A

## Getting More Information

This section describes where to find product and other information:

- [Product documentation.](#)
- [Contact information on page 68.](#)

---

### 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.

**Configuration Guide** — Procedures for configuring VirusScan Enterprise 8.5i for use with ePolicy Orchestrator 3.5 or later 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.

---

## Contact information

**Threat Center: McAfee Avert® Labs** [http://www.mcafee.com/us/threat\\_center/default.asp](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](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](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>

# Index

## A

access protection  
    policies [40](#)  
    reports [42](#)  
    restricting access [40](#)  
alert policies, configuring [38](#)  
audience for this guide [6](#)  
Avert Labs  
    Threat Center [68](#)  
    Threat Library [68](#)

## B

beta program website [68](#)

## C

customer service, contacting [68](#)

## D

DAT files  
    Avert Labs notification service  
    for updates [68](#)  
    updates, website [68](#)  
default processes policies,  
configuring [20](#)  
deployment task [59](#)  
    configuring [60](#)  
    using [59](#)  
display options [36](#)  
documentation, product [67](#)  
download website [68](#)

## E

enforcing policies [46](#)  
evaluating McAfee products,  
download website [68](#)

## F

filtering reports and queries [65](#)

## H

help package file, adding [11](#)  
high-risk processes policies,  
configuring [27](#)  
HotFix and Patch releases (for  
products and security  
vulnerabilities) [68](#)

## I

information, getting [67](#)

## K

KnowledgeBase search [68](#)

## L

low-risk processes policies,  
configuring [25](#)

## O

on-access scanning  
    default processes policies [20](#)  
    general policies [16](#)  
    high-risk processes policies [27](#)  
    low-risk processes policies [25](#)  
on-demand scan task [48](#)  
    configuring [49](#)  
    creating [48](#)

## P

package files  
    online Help [11](#)  
    product [10](#)  
password options [37](#)  
policies  
    about [13](#)  
    configuring [16](#)  
    enforcing [46](#)  
    McAfee defaults [14](#)  
preserving configuration settings [10](#)  
product documentation, where to  
find [67](#)  
product package files, adding [10](#)  
product upgrade  
    preserving settings [10](#)  
product upgrades [68](#)  
professional services, McAfee  
resources [68](#)

## Q

quarantine items, restoring [57](#)  
queries and reports [63](#)  
    accessing [64](#)  
    filtering [65](#)

## R

reports and queries [63](#)  
    accessing [64](#)  
    filtering [65](#)

restore task [57](#)

## S

scheduling tasks [61](#)  
script scanning [17](#)  
security  
    updates, DAT files and engine [68](#)  
    vulnerabilities, releases for [68](#)  
Security Headquarters (*See* Avert  
Labs)  
ServicePortal, technical support [68](#)  
submit a sample, Avert Labs  
WebImmune [68](#)

## T

tasks  
    deployment [59](#)  
    on-demand scan [48](#)  
    restore quarantine items [57](#)  
    scheduling [61](#)  
    update [55](#)  
technical support, contacting [68](#)  
Threat Center (*See* Avert Labs)  
threat library [68](#)  
training, McAfee resources [68](#)

## U

unwanted programs policies [45](#)  
    configuring [45](#)  
update task [55](#)  
    configuring [56](#)  
    creating [55](#)  
upgrade website [68](#)  
user interface policies [35](#)  
    configuring [36](#)  
using this guide  
    audience [6](#)  
    typeface conventions and  
    symbols [7](#)

## V

Virus Information Library (*See* Avert  
Labs Threat Library)

## W

WebImmune, Avert Labs Threat  
Center [68](#)