Installation Guide
revision 1.0

VirusScan® Enterprise

Draft for Beta 1

version 8.7*i*

McAfee®
Proven Security

Industry-leading intrusion prevention solutions

McAfee®

Installation Guide
revision 1.0

VirusScan® Enterprise®™

version 8.7*i*

McAfee®
Proven Security

Industry-leading intrusion prevention solutions

McAfee®

COPYRIGHT

Copyright © 2008 McAfee, Inc. All Rights Reserved.

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

TRADEMARK ATTRIBUTIONS

ACTIVE FIREWALL, ACTIVE SECURITY, ACTIVESECURITY (AND IN KATAKANA), ACTIVESHIELD, CLEAN-UP, DESIGN (STYLIZED E), DESIGN (STYLIZED N), ENTERCEPT, EPOLICY ORCHESTRATOR, FIRST AID, FOUNDSTONE, GROUPSHIELD, GROUPSHIELD (AND IN KATAKANA), INTRUSHIELD, INTRUSION PREVENTION THROUGH INNOVATION, MCAFEE, MCAFEE (AND IN KATAKANA), MCAFEE AND DESIGN, MCAFEE.COM, MCAFEE VIRUSSCAN, NET TOOLS, NET TOOLS (AND IN KATAKANA), NETSCAN, NETSHIELD, NUTS & BOLTS, OIL CHANGE, PRIMESUPPORT, SPAMKILLER, THREATSCAN, TOTAL VIRUS DEFENSE, VIREX, VIRUS FORUM, VIRUSCAN, VIRUSSCAN, VIRUSSCAN (AND IN KATAKANA), 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 MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Attributions

This product includes or may include:

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

PATENT INFORMATION

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

Contents

1 Introducing VirusScan Enterprise 6

Using this guide 6

2 Pre-Installation Information 8

Getting product software and documentation 9
Reviewing release notes 9
Verifying installation rights 9
Preserving settings during product upgrade 9
Meeting system requirements 10
Deploying, updating, and managing options 11
Upgrading the product license 13

3 Installing VirusScan Enterprise 14

Using the Setup utility to install program files 14
Using the command line to install program files 18
Command-line syntax 19
Installation scenarios 20
Installation options and properties 20
Command-line examples 25

4 Modifying, Repairing & Removing VirusScan Enterprise 26

Modifying installed features 26
Using the Setup utility to modify installed features 27
Using the command line to modify installed features 28
Reinstalling or repairing program files 28
Using the Setup utility to reinstall or repair program files 29
Using the command line to reinstall or repair program files 30
Removing program files 31
Using the Setup utility to remove program files 31
Using the command line to remove program files 31
Using the Add/Remove Programs utility to remove program files 31

5 Post-Installation Tasks 32

Testing your installation 32
Locating installed files 33
Product files 33
System files 34

A Getting information 35

Product documentation 35
Contact information 36
. 36

Index 37

1 Introducing VirusScan Enterprise

McAfee® VirusScan Enterprise 8.7*i* offers easily scalable protection, fast performance, and mobile design to protect you from viruses, worms, Trojan horses, as well as potentially unwanted code and programs.

This guide provides information about installing, modifying, and removing VirusScan Enterprise software.

Using this guide

Consider the following when using this guide:

- *Audience*.
- *Conventions* on page 7.

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 installing this product, updating detection definition (DAT) files on their computers, or configuring the software's detection options.

Conventions

This guide uses the following conventions:

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

`Courier`	The path of a folder or program; text that represents something the user types exactly (for example, a command at the system prompt).
	Examples:
	The default location for the program is:
	`C:\Program Files\McAfee\EPO\3.5.0`
	Run this command on the client computer:
	`scan --help`

Italic	For emphasis or when introducing a new term; for names of product documentation and topics (headings) within the material. **Example:** Refer to the *VirusScan Enterprise Product Guide* for more information.
Blue	A web address (URL) and/or a live link. **Example:** Visit the McAfee website at: `http://www.mcafee.com`
<TERM>	Angle brackets enclose a generic term. **Example:** In the console tree, right-click <SERVER>.
	Note: Supplemental information; for example, another method of executing the same command.
	Tip: Suggestions for best practices and recommendations from McAfee for threat prevention, performance and efficiency.
	Caution: Important advice to protect your computer system, enterprise, software installation, or data.

2 Pre-Installation Information

McAfee recommends that you review these topics before installing the VirusScan Enterprise 8.7*i* software:

- *Getting product software and documentation*.
- *Reviewing release notes*.
- *Verifying installation rights*.
- *Preserving settings during product upgrade* on page 9.
- *Meeting system requirements* on page 10.
- *Deploying, updating, and managing options* on page 11.
- *Preconfiguring the installation package* on page 11.
- *Installing and configuring the software for use with other products* on page 11.
- *Upgrading the product license* on page 13.

Getting product software and documentation

Get the VirusScan Enterprise software and documentation from one of these locations:

- The product CD.
- The McAfee download site at:
  https://secure.nai.com/us/forms/downloads/upgrades/login.asp

Logon credentials are required to download products from this website.

Reviewing release notes

Review the release notes, README.TXT, to identify last minute changes or known issues.

Verifying installation rights

Verify that you have local administrator rights for the computer where you plan to install VirusScan Enterprise.

Preserving settings during product upgrade

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 current VirusScan Enterprise rules are read from the registry.
  2 Each of the local VirusScan Enterprise rules are compared against all of the VirusScan Enterprise 8.0 default rules.
  3 If no exact match is found when comparing local rules to the default rules, then the rule is added to the list of rules to preserve.
  4 For port blocking rules, if the local 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 8.7*i* 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 8.7*i* rule, and a newly formed rule is written to the registry for use by VirusScan Enterprise 8.7*i*.
  6 The modified default rules, if any from Step 3, are converted to the new VirusScan Enterprise 8.7*i* rule format and written to the registry. 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.

If you do not want to preserve settings, you can deselect the option during installation or remove the previous version of the software before installing the current version.

Meeting system requirements

These are preliminary requirements for the Beta 1 release. Verify that your server or workstation meets these system requirements before you start the installation process:

These requirements apply only to VirusScan Enterprise 8.7*i*. You must also consider system requirements for any other products you are installing, such as ePolicy Orchestrator.

- **Processor** — An Intel processor or compatible architecture. McAfee recommends an Intel Pentium or Celeron processor running at a minimum of 166MHz.
- **Operating system** — Any of these Microsoft® Windows® platforms:

Server	Workstation
Windows 2000 Server, with Service Pack 4	Windows 2000 Professional, with Service Pack 4
Windows 2000 Advanced Server, with Service Pack 4	Windows XP Home Edition, with Service Pack 1, 2, or 3
Windows Server 2003, with Service Pack 1 or 2	Windows XP Professional, with Service Pack 1, 2 or 3.
Windows Server 2003 R2	Windows XP Tablet PC Edition, with Service Pack 3.
Windows Storage Server 2003	Windows XP Professional x64 Edition, with Service Pack 1, 2, or 3.
Windows Server 2008	Windows Vista Home Basic
	Windows Vista Home Premium
	Windows Vista Business
	Windows Vista Enterprise
	Windows Vista Ultimate

- **Browser** — Microsoft Internet Explorer, version 5.0 or later.
- **Windows Installer** — Microsoft Windows Installer (MSI), version 3.1 or later.
- **Memory** — <to be determined>MB RAM minimum. For information on optimal operating system performance, review the Microsoft guidelines for minimum RAM configuration.
- **Free disk space** — <to be determined>mb for a complete installation of all the VirusScan Enterprise 8.7*i* features and components, including a copy of the installation MSI file for repair ability.
- **Other** — A CD-ROM drive or an Internet connection from which you can install or download the product software.

Deploying, updating, and managing options

Decide whether you want to preconfigure the installation package and how you want to perform updates and deploy the product. The installation procedure may vary if you use supporting tools to deploy, preconfigure, update, or manage VirusScan Enterprise.

Preconfiguring the installation package

Use McAfee Installation Designer 8.5 to preconfigure or customize the installation options for VirusScan Enterprise. When preconfiguring the installation package, we recommend including:

- Where and how you get updates.
- When you check for updates (the default is daily at 17:00 local time to the computer).
- Which policy settings should be defined.

See the *McAfee Installation Designer 8.5 Product Guide* for more information.

Deploying the installation package

Use ePolicy Orchestrator version 3.5 or later to push the software to client computers.

We recommend that before you push the software to client computers, you use McAfee Installation Designer to replace or update the default detection definition (DAT) and engine files included in the installation package. This ensures that the client computer has the most current protection at installation time. It also saves network bandwidth by not having to retrieve the updated files after installation.

Installing and configuring the software for use with other products

When installing VirusScan Enterprise software where third-party products are installed, or when using it with supporting products, you may need to change the installation procedure or perform additional configuration

For example, if you are using the Setup utility to install the VirusScan Enterprise software where Windows 2003 with Terminal Services is installed, the installation stops and you are notified that you must install the program files using the Windows Add/Remove Programs utility.

This installation method is not required if you are using ePolicy Orchestrator to deploy VirusScan Enterprise.

Upgrading the product license

If you are installing the product for the first time, the product is licensed during the installation process. Skip this section and go to *Installing VirusScan Enterprise* on page 14.

If you are installing a licensed version over an evaluation version of VirusScan Enterprise, you must upgrade the license. The license does not automatically upgrade itself from an evaluation version.

Perform the license upgrade before the evaluation period expires. If you do not, the scanning and updating functions stop until you replace the evaluation version with a licensed version of the product.

Use one of these methods to upgrade an evaluation version of VirusScan Enterprise to a licensed version:

- Use McAfee Installation Designer to upgrade the license. Refer to the *McAfee Installation Designer Product Guide* for specific details.
- Remove the evaluation version of the product and install the licensed version.

Removing the evaluation version causes you to lose all of the configured settings from that installation. This method is only recommended if you cannot use McAfee Installation Designer to upgrade the license.

3 Installing VirusScan Enterprise

VirusScan Enterprise 8.7*i* installs on workstations and servers.

See *Pre-Installation Information* on page 8 for information about preparing for installation.

Install the product software using one of these methods:

- *Using the Setup utility to install program files*.
- *Using the command line to install program files* on page 18.

Using the Setup utility to install program files

Use the Setup utility that comes with the product to install the product software.

1 Start the Setup utility using one of these methods:

Method	Description
Product CD	1 Insert the CD into the CD-ROM drive. 2 In the autorun window, select the product that you want to install. 3 Follow the instructions in the installation wizard to install the product.
Command line	1 Click **Start**, then select **Run**. 2 Type <X>:\SETUP.EXE in the **Run** dialog box, then click **OK**. Notes and Tips Here, <X>: represents the drive letter for your CD-ROM, or the path of the folder that contains the extracted program files. If your copy of the software came on a product suite CD, you must also specify which folder contains the specific software package.
Windows Explorer	1 Browse to the location where you extracted the program files. 2 Double-click SETUP.EXE. 3 Follow the instructions in the installation wizard to install the product.

2 McAfee VirusScan Enterprise Setup — Review the release notes.

Option or Button	Description
View Readme	Display the release notes for this product. Notes and Tips Identify special installation instructions or known issues before you continue with the installation process.

3 McAfee Licensing — Choose and read the product license.

Option or Button	Description
License expiry type	Specify the type of license. Notes and Tips The license type must match the type of license that you purchased. If you are unsure of which type of license to select, contact the person from whom you purchased the software.
Select location where purchased and used	Select the country in which you are using the software.
I accept the terms in the license agreement	Accept the license agreement and continue the installation.
I do not accept the terms in the license agreement	Do not accept the license agreement and terminate the installation. Select I do not accept the terms in the license agreement, then: ■ Click Cancel twice. ■ Click Yes to confirm that you want to cancel. ■ Click Finish to exit the Setup wizard.

4 Select Setup Type — Choose the installation type and location.

Option or Button	Description
Typical	Installs the software with all features. Notes and Tips We recommend a typical installation for most environments.
Custom	Installs the software with all or selected features and allows you to customize some settings. Notes and Tips Use custom installation to install only selected features, import an AutoUpdate repository list, or specify user interface settings during the installation process.
Install To	Accept the default installation location or specify a new location. Notes and Tips By default, Setup installs the VirusScan Enterprise program files to this path: `<drive>:\Program Files\McAfee\VirusScan Enterprise\`
Disk Space	View the disk space requirements for this installation.

5 Select Access Protection Level — Choose which access protection rules are enabled by default when this feature is installed.

Option or Button	Description
Standard Protection	Anti-virus and common rules that protect some critical settings and files from being modified, but generally allow you to install and execute legitimate software.
Maximum Protection	Anti-virus and common rules that protect most critical settings and files from being modified, but might prevent you from installing legitimate software.

Go to the next step that applies to the installation type you selected:

- Custom Installation — Go to Step 6.
- Typical Installation — Go to Step 10 on page 18.

6 Feature Selection — Select specific features for installation.

Feature	Description
Console	Installs the VirusScan Console and all of its features. Notes and Tips *Default = Console*.
AutoUpdate	Installs the feature that automatically updates DAT files, scanning engine, and other product upgrades.
Lotus Notes E-mail Scanner	Installs the feature that scans Lotus Notes e-mail.
Microsoft Outlook E-mail Scanner	Installs the feature that scans Microsoft Outlook e-mail.
On-Access Scan	Installs the scanner that protects your computer from potential threats that arrive on disks, from your network, or from various sources on the network.
Access Protection	Installs the feature that protects your computer's accesses.
Buffer Overflow Protection	■ Installs the feature that protects your computer from buffer overflow exploits. ■ Notes and Tips ■ This feature will not be installed on 64-bit systems. ■ This feature will not be installed if either the Host Intrusion Prevention (Entercept) agent or the Cisco Security agent are found on the local computer.
Script Scan	Installs the feature that scans Java Script and VBScript scripts before they are executed.
On-Demand Scan	Installs the scanner that allows you to perform either immediate or scheduled on-demand scan tasks.
Right-click Scan	Installs the feature that allows you to perform on-demand right-click scan tasks.

7 Feature action options — For each selected feature, you can also select a corresponding action from the drop-list next to the feature name:

- This feature will be installed on local hard drive.
- This feature, and all subfeatures, will be installed on local hard drive.
- This feature will not be available.

8 Product Configuration — Import a repository list and/or choose whether to enable the on-access scanner when the installation completes.

Option	Description
Import AutoUpdate repository list	Import the repository list from the location you specify. Notes and Tips 1 The repository list must be located on a local drive; it cannot be imported from a mapped drive or a network drive. 2 This option is selected by default only if a repository list is included in the installation file (.MSI) or the command-line property (cmasourcedir) has been set to a new location to point to the SITELIST.XML file. 3 If you do not import a repository list at this time, and one resides in the installation folder, it will be imported even though you do not select this option. If a repository list is not imported, AutoUpdate performs updates using the default McAfee site as its repository list. 4 See the *AutoUpdate* section in the *VirusScan Enterprise Product*
Enable On-Access Scanner at the end of installation	Automatically start the on-access scanner upon completion of the installation process. Notes and Tips We recommend that you select this option to provide maximum security.

9 Security Configuration — Specify password security and which system tray options users can access.

Option or Button	Description
Password	Specify a password for user interface security.
Confirm Password	Type the password again to confirm it.
Do not display the VirusScan items under the Start menu.	Do not display the Start menu shortcuts for VirusScan Enterprise.
Show the system tray icon with all menu options	Allow users to see all menu items on the system tray icon menu.
Show the system tray icon with minimal menu options	Hide all options on the system tray menu except About VirusScan Enterprise and On-Access Scan Statistics.
Do not show the system tray icon	Hide the system tray icon from all users.

You can also configure these security options after installation. See the *VirusScan Enterprise Product Guide* for details.

10 Ready to install — Start the installation process.

Option or Button	Description
Install	Begin installing the product software. Notes and Tips If you are not satisfied with all of the installation settings, click **Back** to review or change any of the settings. When ready, return to the **Ready to install** dialog box and click **Install**.

11 McAfee VirusScan Enterprise setup has completed successfully — Choose whether to perform an update task and/or an on-demand scan when the installation completes.

Option or Button	Description
Update Now	Automatically run an update task when the installation completes.
Run On-Demand Scan	Automatically run a **Full Scan** when the installation completes.
Finish	Complete the installation.

If you select both the **Update Now** and **Run On-Demand Scan** options, the update task runs first, then the on-demand scan task runs.

Using the command line to install program files

Installing VirusScan Enterprise from the command line allows you to customize the installation so that it runs the way you want and installs exactly the product features you want.

Review *Meeting system requirements* on page 10 before you begin the installation process.

You can run Setup from the command line to install the VirusScan Enterprise software to your *local* computer, but only if you have local administrator rights.

This section describes:

- *Command-line syntax* on page 19.
- *Installation scenarios* on page 20.
- *Installation options and properties* on page 20.
- *Restart options* on page 22.

Command-line syntax

To install the product from the command line:

1 Open the Windows command-line component using one of these methods:

- Select **Command Prompt** from the **Start** menu.
- Select **Run** from the **Start** menu.

2 Type the command line at the command prompt or in the **Run** dialog box.

```
setup.exe PROPERTY=VALUE[,VALUE] [/option]
```

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

Item	Description
File name	The name of the executable file, setup.exe.
Options	Specify options for installing the software. For example, perform a silent installation and/or record installation progress in a log file. Each option is preceded by a forward slash (/) and is not case-sensitive. Notes and Tips The installation scenarios that appear later in this guide discuss some of the available options.
Properties	Specify how the installation runs. Each property consists of: ■ A name, which must appear in uppercase letters. ■ An equal (=) sign. ■ One or more values, each separated by commas. Most property values must appear in uppercase letters, but some, such as **True** and **False**, must appear in mixed case. Notes and Tips The Microsoft Installer permits a variety of properties that determine how your installation runs. To learn about those properties, see the Microsoft Installer documentation.

Installation scenarios

Use these scenarios to customize your installation:

Scenario	Description
Silent	A silent installation does not display the installation wizard or offer the user any configuration options. Instead, you preconfigure those choices and run Setup in the background on each destination computer. You can install VirusScan Enterprise software on any unattended computer with or without the user's knowledge, provided you have the necessary administrator rights. Add these options to run a silent or semi-silent installation: ■ **q or qn** Silent installation. This installs default settings unless you specify otherwise. For example, the product license default is a 1 Year Subscription. ■ **qb** Basic user interface. Use qb! to hide the Cancel button. ■ **qb+** Basic user interface with a modal dialog box displayed at the end of installation. Use qb+! or qb!+ to hide the Cancel button.The modal dialog box is not displayed if the user cancels the installation. ■ **qb-** Basic user interface with no modal dialog boxes. Use qb-! or qb!- to hide the Cancel button. ■ **qf** Full user interface and any authored FatalError, UserExit, or Exit modal dialog box displayed at the end of installation. ■ **qn+** No user interface except for a modal dialog box displayed at the end of installation. ■ **qr** Reduced user interface with no modal dialog displayed at the end of installation
Custom Location	Add the **`installdir`** property to specify the location. For example, to silently install VirusScan Enterprise software to C:\My AntiVirus Software, type this text at the command prompt: `setup.exe INSTALLDIR="c:\My AntiVirus Software" /q`
Login Script	Add a **`Setup`** command to your login script to install VirusScan Enterprise software at the time each of your destination computers starts. Include all of the options and properties for governing how Setup runs. For example, you can add a property to look for the VirusScan Enterprise default program location. Notes and Tips To use a login script for this purpose, you must also copy or push the VirusScan Enterprise installation package to a local location on the destination computer.

Installation options and properties

Use a combination of options and properties to customize the software installation.

This section describes:

■ *Selecting features* on page 21.
■ *Restart options* on page 22.
■ *Installation progress options* on page 22.
■ *Installation properties* on page 23.
■ *Command-line examples* on page 25.

Selecting features

When you run Setup from the command line to install specific program features, the utility installs those features according to a pre-existing hierarchy. For example, if you specify **ScriptScan**, Setup knows that you must have the on-access scanner installed to use those features. It therefore installs any required files.

Use these feature names as command-line parameters:

Feature	Description
Console	Installs the **VirusScan Console** and all of its features. Notes and Tips *Default = Console*.
AutoUpdate	Installs the feature that automatically updates DAT files, scanning engine, and other product upgrades.
LotusNotesScan	Installs the feature that scans Lotus Notes e-mail.
EmailScan	Installs the feature that scans Microsoft Outlook e-mail.
OnAccessScanner	Installs the scanner that protects your computer from potential threats that arrive on disks, from your network, or from various sources on the network.
AccessProtection	Installs the feature that protects your computer's accesses.
BufferOverflow	■ Installs the feature that protects your computer from buffer overflow exploits. ■ Notes and Tips ■ This feature will not be installed on 64-bit systems. ■ This feature will not be installed if either the Host Intrusion Prevention (Entercept) agent or the Cisco Security agent are found on the local computer.
ScriptScan	Installs the feature that scans Java Script and VBScript scripts before they are executed.
OnDemandScanner	Installs the scanner that allows you to perform either immediate or scheduled on-demand scan tasks.
ShellExtensions	Installs the feature that allows you to perform on-demand right-click scan tasks.

Restart options

You can force a restart if one is required, prevent the destination computer from restarting during the installation or always perform a restart. To do this, add the REBOOT property to the command line:

Option	Description
REBOOT=F	Forces a restart if one is required.
REBOOT=R	Prevents a restart. Notes and Tips To run a silent installation and prevent a system restart: `setup.exe REBOOT=R /q`
REBOOT=A	Always restarts.

Installation progress options

To record installation progress in a log file, add this option and parameter to the Setup command line:

```
/l*v "c:\temp\log.txt"
```

Here, `c:\temp\log.txt` can be any location and any file name you want to use to create the log file. This option logs all installer activity, including all files copied, all registry keys added, and all .INI file changes.

Replace the asterisk (*) shown in the command-line example, with one or more of these parameters to limit the type of data that the log file records:

Option	Description
i	status messages
w	non-fatal warnings
e	all error messages
a	action starts
r	action-specific records
u	user requests
c	initial user interface parameters
m	out-of-memory or fatal exit information
o	out-of-disk-space messages
p	terminal properties
+	append to existing file
!	flush each line to the log

Installation properties

Use these properties to customize the command-line installation:

Property	Description
ADDLOCAL	Installs specific features to the local computer.
CMASOURCEDIR	Set the source path for the SITELIST.XML file. The default path is: %TEMP%\NAITemp. Notes and Tips The repository list must be located on a local drive and cannot be imported from a mapped or a network drive.
ENABLEONACCESSSCANNER	False = A False value cannot be set. True = Enable on-access scanner when the installation completes (Default). Notes and Tips If you do not want to enable the on-access scanner, set the property to "", an empty string. For example: `ENABLEONACCESSSCANNER=""`
EXTRADATSOURCEDIR	Set the source path for the EXTRA.DAT file. During installation, the EXTRA.DAT file is copied into the location where the engine files reside.
ICONLOCKDOWN	False = A False value cannot be set. True = Do not display any icons. Notes and Tips ■ The default is an empty string. ■ To display icons, set the property to "", an empty string. For example: `ICONLOCKDOWN=""`
INSTALLDIR	Specifies the installation folder. Notes and Tips The value consists of the installation path.
LOCKDOWNSHORTCUTS	False = A False value cannot be set. True = Do not display any shortcuts under the **Start** menu. Notes and Tips ■ The default is an empty string. ■ To allow the shortcuts to be installed, set the property to "", an empty string. For example: `LOCKDOWNSHORTCUTS=""`.
PRESERVESETTINGS	False = A False value cannot be set. True = Preserve settings (Default). Notes and Tips ■ Preserves settings when upgrading from NetShield®, VirusScan, or an earlier version of VirusScan Enterprise. ■ If you do not want to preserve settings, set the property to "", an empty string. For example: `PRESERVESETTINGS=""`

Property	Description
REBOOT	Restart your computer. Notes and Tips You can force the computer to restart if it is required, or prevent it from restarting.
REMOVE	Removes one or more program features. You can specify a feature, or use the value `ALL` to remove all features. If you combine this property with the `ADDLOCAL` property, you can install all but one or two specific features.
RUNAUTOUPDATE	False = A False value cannot be set. True = Run update when the installation completes (Default). Notes and Tips ■ Use this command when performing interactive installations. ■ If you do not want to run update when the installation completes, set the property to "", an empty string. For example: `RUNAUTOUPDATE=""`
RUNAUTOUPDATESILENTLY	False = A False value cannot be set. True = Run silent update when the installation completes. Notes and Tips ■ The default is an empty string. ■ Use this command when performing silent updates. ■ If you do not want to run a silent update when the installation completes, set the property to "", an empty string. For example: `RUNAUTOUPATESILENTLY=""`
RUNONDEMANDSCAN	False = A False value cannot be set. True = Run a scan of all local drives when the installation completes (Default). Notes and Tips ■ Use this command when performing interactive installations. ■ If you do not want to run the on-demand scanner when the installation completes, set the property to "", an empty string. For example: `RUNONDEMANDSCAN=""`
RUNONDEMANDSCANSILENTLY	False = A False value cannot be set. True = Run on-demand scan silently when the installation completes. Notes and Tips ■ The default is an empty string. ■ Use this command when performing silent installations. ■ If you do not want to run a silent on-demand scan when the installation completes, set the property to "", an empty string. For example: `RUNONDEMANDSCANSILENTLY=""`

Command-line examples

Option	Command & Description
Complete silent installation	`setup.exe ADDLOCAL=ALL /q` Silently installs all features.
Installing more than one feature.	Use a comma. For example: `setup.exe ADDLOCAL=OnAccessScanner,ScriptScan /q` Silently installs the On-Access Scanner and Script Scan.
Install all features except one	`setup.exe ADDLOCAL=ALL REMOVE=ScriptScan /q` Silently installs all features except for Script Scan.
Remove all features	`setup.exe REMOVE=ALL /q` Silently removes all features.
Installing features using a loud installation	Omit the `/q` option in any of the command-line examples shown here. Installs specified features.

4 Modifying, Repairing & Removing VirusScan Enterprise

Use the **Program Maintenance** feature to modify, repair, or reinstall the VirusScan Enterprise program files.

This section describes:

- *Modifying installed features*.
- *Reinstalling or repairing program files* on page 28.
- *Removing program files* on page 31.

Modifying installed features

Use the **Program Maintenance** to change which features are installed:

- *Using the Setup utility to modify installed features* on page 27.
- *Using the command line to modify installed features* on page 28.

You cannot use this feature to change the specified **Install To** path and/or **Disk Space**. To change the installation path, you must first remove the product, then reinstall the product to the required path.

Using the Setup utility to modify installed features

1 Start the Setup utility. See *Using the Setup utility to install program files* on page 14 for details

2 Program Maintenance — Select **Modify**.

3 Feature Selection — Select specific features for installation. See Step 6 on page 16 for details.

4 **Feature action options** — For each selected feature, you can also select a corresponding action from the drop-list next to the feature name:

- This feature will be installed on local hard drive.
- This feature, and all subfeatures, will be installed on local hard drive.
- This feature will not be available.

5 Ready to install — Start the installation process.

Option or Button	Description
Install	Begin installing the product software. Notes and Tips If you are not satisfied with all of the installation settings, click **Back** to review or change any of the settings. When ready, return to the **Ready to install** dialog box and click **Install**.

6 McAfee VirusScan Enterprise setup has completed successfully — Choose whether to perform an update task and/or an on-demand scan when the installation completes and finish the installation.

Option or Button	Description
Update Now	Automatically run an update task when the installation completes.
Run On-Demand Scan	Automatically run a **Full Scan** when the installation completes.
Finish	Complete the installation.

If you select both the **Update Now** and **Run On-Demand Scan** options, the update task runs first, then the on-demand scan task runs.

Using the command line to modify installed features

Open the Windows command-line component. See *Command-line syntax* on page 19 for details.

Install or remove features individually using a comma-separated list, or you can specify the ALL property. See *Selecting features* on page 21 for a list of feature names.

Option	Command
Add a feature	`setup.exe ADDLOCAL=OnAccessScanner,ScriptScan /q`
Remove a feature	`setup.exe REMOVE=ScriptScan,ShellExtentions/q`
Installing features using a loud installation	Omit the `/q` option in any of the command -line examples shown here.

Reinstalling or repairing program files

Use Program Maintenance to reinstall product features or repair program files.

This section describes:

- *Using the Setup utility to reinstall or repair program files*.
- *Using the command line to reinstall or repair program files* on page 30.

Using the Setup utility to reinstall or repair program files

1 Start the Setup utility. See *Using the Setup utility to install program files* on page 14.

2 Program Maintenance — Select **Repair**.

3 Reinstall or Repair the Product — Choose whether to reinstall or repair VirusScan Enterprise program files.

Option or Button	Description
Reinstall McAfee VirusScan Enterprise	Reinstalls the VirusScan Enterprise program files, registry keys, and shortcuts.
Detect and repair missing or corrupt files	Finds missing or corrupt program files and repairs them. Notes and Tips ■ This feature does not support repairing update components. If an AutoUpdate file is removed or corrupted, you must remove the AutoUpdate component, then reinstall it. ■ If you manually remove or rename any of the program files, the repair feature may fail. See the *Troubleshooting* appendix in the *VirusScan Enterprise Product Guide* for detailed instructions about trying to repair files after they have been removed or renamed.
Re-write registry keys	Re-writes registry keys as necessary during the repair process. Notes and Tips This option is available only for **Detect and repair missing or corrupt files**.
Install	Begin the installation process.

4 McAfee VirusScan Enterprise setup has completed successfully — Choose whether to perform an update task and/or an on-demand scan when the installation completes and finish the installation.

Option or Button	Description
Update Now	Automatically run an update task when the installation completes.
Run On-Demand Scan	Automatically run a **Full Scan** when the installation completes.
Finish	Complete the installation.

If you select both the **Update Now** and **Run On-Demand Scan** options, the update task runs first, then the on-demand scan task runs.

Using the command line to reinstall or repair program files

Open the Windows command-line component.

Topic	Description

Command-line Syntax	Use this syntax to:
	■ Reinstall the product:
	`msiexec /I{product code}REINSTALL=[feature]REINSTALLMODE=[option]`
	■ Remove a feature:
	`msiexec /f[option]{product code}`

Selecting Features	See *Selecting features* on page 21 for details.
Command-line Options	Use any combination of these options: ■ **p** Reinstall only if file is missing. ■ **o** Reinstall if file is missing or if an older version is installed. ■ **e** Reinstall if file is missing or an equal or older version is installed. ■ **d** Reinstall if file is missing or a different version is installed. ■ **c** Reinstall if file is missing, or if the stored checksum does not match the calculated value. Only repairs files that have msidbFileAttributesChecksum in the Attributes column of the File table. ■ **a** Force all files to be reinstalled. ■ **u** Rewrite all required user-specified registry entries. ■ **m** Rewrite all required system-specific registry entries. ■ **s** Overwrite all existing shortcuts. ■ **p** Run from source and re-cache the local package.

Removing program files

Use one of these methods to remove the software.

Using the Setup utility to remove program files

1 Start the Setup utility to open the **Program Maintenance** dialog box:

2 Select **Remove**.

3 Select **Remove** again, then click **Finish**.

After VirusScan Enterprise is removed, you may be prompted to remove remaining files or folders. Click **Yes** or **No**.

These are files or folders which were not installed initially with the VirusScan Enterprise product such as, log files or other files or folders that the user added. For example, the aseinst.log is used for debugging and is left in the %TEMP%\MCAFEELOGS folder.

Using the command line to remove program files

Use this syntax to remove the software:

```
<X>:\SETUP.EXE /x
```

Here, <X>: represents the drive letter for your CD-ROM or the path of the folder that contains the extracted program files. To search for the correct files on your hard disk or CD, click Browse. If your copy of the software came on a product suite CD, you must also specify which folder contains the specific software package.

Using the Add/Remove Programs utility to remove program files

1 Click **Start**, then select **Settings** | **Control Panel** | **Add/Remove Programs** to open the **Add/Remove Programs** utility that is included in the Windows Control Panel

2 Select the VirusScan Enterprise program from the list of installed programs, then click **Remove**.

We strongly recommend that you restart your computer after removing files and before you reinstall the software.

When you remove files using Setup on the command line, some files or stopped services may not be removed. For example, if you remove the VirusScan Enterprise product while the McAfee Task Manager or the McShield services are stopped, these services are not removed. Restarting after removing files ensures that all files and services are removed before reinstalling the software.

5 Post-Installation Tasks

This section describes:

- *Testing your installation*.
- *Locating installed files* on page 33.

Testing your installation

Once installed, the software can scan your system for potentially unwanted files. You can test whether it is installed correctly and can properly scan for potentially unwanted programs by implementing a test developed by the European Institute for Computer Anti-Virus Research (EICAR).

To test your installation:

1 Using a standard Windows text editor such as Notepad, type the following string, *on a single line with no spaces or line breaks*:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

2 Save the file with the name EICAR.COM. The file size is 68 or 70 bytes. Make a note of the folder in which you saved the file.

3 Start the VirusScan Enterprise program.

4 To test the on-demand scanner, create an on-demand scan task that examines the folder where you saved EICAR.COM. When the scanner examines this file, it reports finding the EICAR test file.

5 To test the on-access scanner, confirm that the on-access scanner is configured to scan files written to the computer and files read from the computer. See *Configuring the on-access scanner properties* in the *VirusScan Enterprise Product Guide* for additional information. Locate the EICAR.COM file and try to copy or move it to another location. The scanner reports finding the EICAR test file when it examines the file.

This file is *not a virus* — it cannot spread, infect other files, or harm your system. Delete the file when you have finished testing your installation to avoid alarming other users.

Locating installed files

During installation, files are installed in various locations.

Two types of files are installed:

- *Product files*.
- *System files* on page 34.

Product files

Product files are installed in the installation path, which is determined during installation. The default installation path is:

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

Product files are installed in these folders:

- *VirusScan Enterprise folder*.
- *Resources folders* on page 34.
- *Engine folder* on page 34.
- *Engine folder\x64* on page 34.

VirusScan Enterprise folder

These files are installed to the VirusScan Enterprise folder in the installation path:

AdsLokUU.Dll	mscshield.exe	mfetdik.sys	readme.txt
BBCpl.dll	McShieldPerData.dll	msiutil.dll	scan32.exe
condl.dll	McShieldPerData.h	mytilus.dll	ScanOTLK.dll
consl.dll	McShieldPerData.ini	mytilus2.dll	scncfg32.exe
coptcpl.dll	McShieldPerData.reg	naevent.Dll	scriptproxy.dll
csscan.exe	mcupdate.exe	naiann.dll	shcfg32.exe
EmAbout.dll	Mcvssnmp.dll	naievent.dll	shext.dll
EmCfgCpl.dll	mfeapfa.dll	nailite.dll	shstat.exe
entsrv.dll	mfeapfk.sys	NCDaemon.exe	shutil.dll
EntvUtil.exe	mfeavfa.dll	NCExtMgr.dll	vscan.bof
FtCfg.dll	mfeavfk.sys	NCInstall.dll	VsEvntUI.DLL
Ftl.dll	mfebopa.dll	NCMenu.dll	vsodscpl.dll
graphics.dll	mfebopk.sys	NCScan.dll	vsplugin.dll
lockdown.dll	mfecaka.dll	NCTrace.dll	vstskmgr.exe
logparser.exe	mfecakk.sys	nvpcpl.dll	vsupdate.dll
McAVDetect.DLL	mfehida.dll	OASCpl.dll	vsupdcpl.dll
mcavscv.dll	mfehidin.exe	pireg.exe	vwmain.dll
mcconsol.exe	mfehidk.sys	quarcpl.dll	

The default location is: `<drive>:\Program Files\McAfee\VirusScan Enterprise`

Resources folders

The resources folder name depends on the language being installed. For example, the English resources folder is named Res0900. These files are installed to the resources folder in the installation path:

mcshield.DLL	strings.bin

The default location is:

`<drive>:\Program Files\McAfee\VirusScan Enterprise\Res0900`

Engine folder

The engine folder contains common files and those required to scan 32-bit operating systems. These files are installed to the engine folder in the installation path:

avvclean.dat	avvnames.dat	avvscan.dat	config.dat
license.dat	mcscan32.dll	messages.datt	signlic.Txt

The default location is: `<drive>:\Program Files\Common Files\McAfee\Engine`

Engine folder\x64

The x64 folder contains files required to scan 64-bit operating systems. These files are installed to the engine folder in the installation path:

config.dat_x64	licenst.dat_x64	mscan64a.dll	signlic.txt_x64

The default location is: `<drive>:\Program Files\Common Files\McAfee\Engine\x64`

System files

The list of installed system files depends on your operating system. For example, these files are installed to the System32 folder:

msvcrt.dll	psapi.dll

The default location is: `<drive>:\Windows\System32\drivers`

6 Getting information

This section describes:

- *Product documentation* on page 35.
- *Contact information* on page 36.

Product documentation

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

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

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

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

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

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

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

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

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

Contact information

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

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

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

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

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

Product Upgrades *(Valid grant number required)*

Security Updates (DATs, engine)

HotFix and Patch Releases

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

Product Evaluation

McAfee Beta Program

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

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

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

Customer Service

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

Phone — US, Canada, and Latin America toll-free:
+1-888-VIRUS NO or **+1-888-847-8766** Monday – Friday, 8 a.m. – 8 p.m., Central Time

Professional Services

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

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

Index

A

access protection, default levels of protection 16
audience for this guide 6
Avert Labs Threat Center 36
Avert Labs Threat Library 36

B

beta program website 36

C

command line
  installing program files 18
  logging installation progress
    progress installation log 20
  modifying features 28
  properties 23
  properties, installation 23
  reinstalling or repairing program files 28, 30
  restart options, setting 22
  scenarios 20
  selecting specific features 21
  syntax 19
command line, using 18
Custom install 15
custom installation
  enable on-access scanner 17
  feature actions 17, 27
  import repository list 17
customer service, contacting 36

D

DAT files
  Avert Labs notification service for updates 36
  updates, website 36
deployment options 11
documentation, product 35
download website 36

E

ePolicy Orchestrator
  deploy installation package 11
evaluating McAfee products, download website 36

F

features, modifying 26
files, installed
  product 33
  system 34

H

HotFix and Patch releases (for products and security vulnerabilities) 36

I

information, getting 35
installation
  Custom 15
  installed files 33
  post installation 32
  pre-installation 8
  rights 9
  system requirements 10
  testing 32
  type 15
  Typical 15
installation package
  deploy using ePolicy Orchestrator or ProtectionPilot 11
  preconfigure using McAfee Installation Designer 11

K

KnowledgeBase search 36

L

license
  product 15
  upgrade 13
login script, installing program files 20

M

McAfee Installation Designer, preconfigure installation package 11

O

on-access scanner, enable after installation 17
on-demand scan task, run after installation 18
operating systems supported, server and workstation 10

P

privileges, installation 9
processor requirements, server and workstation 10
product documentation, where to find 35
product license
  select during install 15
  upgrading 13
product management options 11
product software, getting 9
product upgrades 36
professional services, McAfee resources 36
program files
  modifying 26
  reinstalling or repairing 28
ProtectionPilot
  deploy installation package 11

R

RAM requirements, server and workstation 11
release notes, reviewing 9
repository, import 17
restarting options via command line 22

S

Security Headquarters (*See* Avert Labs)
security updates, DAT files and engine 36
security vulnerabilities, releases for 36
ServicePortal, technical support 36
setup type, choosing 15
Setup utility
  installing the product 14
  modifying program files 27
  reinstalling or repairing program files 29

submit a sample, Avert Labs WebImmune 36
system requirements, server and workstation 10

T

technical support, contacting 36
Terminal Server, installation recommendations. 11
testing your installation 32
third party products 11
Threat Center (*See* Avert Labs)
threat library 36
training, McAfee resources 36
Typical install 15

U

update task, run after installation 18
updating options 11
upgrade website 36
using this guide 6
  audience 6
  typeface conventions and symbols 7

V

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

W

WebImmune, Avert Labs Threat Center 36