



# McAfee VirusScan Enterprise 8.8 software

## Installation Guide

## **COPYRIGHT**

Copyright © 2010 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**

AVERT, EPO, EPOLICY ORCHESTRATOR, FOUNDSTONE, GROUPSHIELD, INTRUSHIELD, LINUXSHIELD, MAX (MCAFFEE SECURITYALLIANCE EXCHANGE), MCAFFEE, NETSHIELD, PORTALSHIELD, PREVENTSYS, SECURITYALLIANCE, SITEADVISOR, TOTAL PROTECTION, VIRUSSCAN, WEBSHIELD are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee 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 ACCOMPANY 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 WEBSITE 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.

# Contents

- Introducing VirusScan Enterprise..... 5**
  - Audience..... 5
  - Conventions..... 5
  - Finding product documentation..... 6
- Pre-Installation Tasks..... 7**
  - Preparation for installing the software..... 7
  - System requirements..... 8
  - Product upgrade and preserving settings..... 10
  - Options for preconfiguring, deploying, updating, and managing VirusScan Enterprise..... 11
  - Product license and performing an upgrade..... 12
- Installing VirusScan Enterprise..... 13**
  - Using the Setup utility to install the software..... 13
  - Using the command line to install the software..... 15
    - Installation scenarios..... 16
    - Installation options and properties..... 17
    - Installing using an Administrative Installation Point..... 20
  - Placing the product under ePolicy Orchestrator management..... 20
  - Migrating the ePolicy Orchestrator policies..... 21
- Post-Installation Tasks..... 23**
  - Testing your installation..... 23
    - Testing for malware detection..... 23
    - Testing for potentially unwanted programs detection..... 24
  - Location of installed files..... 24
    - Location of 32-bit operating system installed files..... 24
    - Location of 64-bit operating system installed files..... 26
- Maintenance Tasks..... 28**
  - Modifying installed features..... 28
    - Using the Setup utility to modify installed features..... 28
    - Using the command line to modify installed features..... 29
  - Reinstalling or repairing program files..... 29
    - Using the Setup utility to reinstall or repair program files..... 29

Using the console to reinstall or repair program files. . . . .	30
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. . . . .	32
Using the Add/Remove Programs utility to remove program files. . . . .	32

# Introducing VirusScan Enterprise

---

McAfee® VirusScan® Enterprise software protects your system from viruses, worms, Trojan horses, and potentially unwanted code and programs.

This guide provides system requirements for VirusScan Enterprise software, and information about installing it as a standalone and as a managed product, as well as modifying, repairing, removing, and reinstalling the software.

## Contents

- ▶ [Audience](#)
- ▶ [Conventions](#)
- ▶ [Finding product documentation](#)

## Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.
- **Users** — People who are responsible for configuring the product options on their system, or for updating the product on their systems.

## Conventions

This guide uses the following typographical conventions.

<i>Book title or Emphasis</i>	Title of a book, chapter, or topic; introduction of a new term; emphasis.
<b>Bold</b>	Text that is strongly emphasized.
User input or Path	Commands and other text that the user types; the path of a folder or program.
Code	A code sample.
<b>User interface</b>	Words in the user interface including options, menus, buttons, and dialog boxes.
Hypertext blue	A live link to a topic or to a website.
<b>Note</b>	Additional information, like an alternate method of accessing an option.
<b>Tip</b>	Suggestions and recommendations.
<b>Important/ Caution</b>	Valuable advice to protect your computer system, software installation, network, business, or data.
<b>Warning</b>	Critical advice to prevent bodily harm when using a hardware product.

## Finding product documentation

McAfee provides the information you need during each phase of product implementation, from installing to using and troubleshooting. After a product is released, information about the product is entered into the McAfee online KnowledgeBase.

- 1 Go to the McAfee Technical Support ServicePortal at <http://mysupport.mcafee.com>.
- 2 Under **Self Service**, access the type of information you need:

To access...	Do this...
User Documentation	<ol style="list-style-type: none"><li>1 Click <b>Product Documentation</b>.</li><li>2 Select a <b>Product</b>, then select a <b>Version</b>.</li><li>3 Select a product document.</li></ol>
KnowledgeBase	<ul style="list-style-type: none"><li>• Click <b>Search the KnowledgeBase</b> for answers to your product questions.</li><li>• Click <b>Browse the KnowledgeBase</b> for articles listed by product and version.</li></ul>

# Pre-Installation Tasks

---

Before installing the VirusScan Enterprise software, you need to make sure your system is ready. This section presents a high-level process of tasks to complete before installing the software, and information that can help you prepare for the installation.

## Contents

- ▶ Preparation for installing the software
- ▶ System requirements
- ▶ Product upgrade and preserving settings
- ▶ Options for preconfiguring, deploying, updating, and managing VirusScan Enterprise
- ▶ Product license and performing an upgrade

## Preparation for installing the software

Complete these tasks before installing the VirusScan Enterprise software.

- 1** Get the VirusScan Enterprise software and documentation from one of these locations:
  - The product CD
  - The McAfee download site:  
<https://secure.nai.com/us/forms/downloads/upgrades/login.asp>
- 2** Review the release notes to identify last minute changes or known issues.
- 3** Verify that you have local administrator rights for the computer where you plan to install VirusScan Enterprise.
- 4** Verify that your server or workstation meets the system requirements before you start the installation process. Refer to *System requirements* for details.
- 5** Decide if you want to preconfigure the installation package, and how you want to update and deploy the product. The installation procedure varies if you use supporting tools to preconfigure, deploy, update, or manage VirusScan Enterprise. Refer to *Options for preconfiguring, deploying, updating, and managing VirusScan Enterprise* for details.
- 6** If you are installing a licensed version over an evaluation version of VirusScan Enterprise, you must upgrade the license. The license is not automatically upgraded from an evaluation version. Refer to *Product license and performing an upgrade* for details.

# System requirements

Verify that your server or workstation meets these system requirements before you start the installation process.

**NOTE:** These are minimum requirements and are not optimal for performance. They apply only to VirusScan Enterprise. You must also consider system requirements for any other products you are installing, such as ePolicy Orchestrator.

- **Operating system and platform** — This version of VirusScan Enterprise is compatible with any of the following minimum workstation and server Microsoft Windows operating systems and hardware platforms:

**Table 1: Minimum workstation requirements**

Operating system	SP	32-bit	64-bit	Processor	RAM	Minimum hard disk space
Microsoft Windows 2000 Professional, with Update Rollup 1*	SP4	X		133 MHz or greater Pentium. Up to two processors on a single computer	64 MB minimum and 4 GB maximum	450 MB
Microsoft Windows XP Home and Professional Editions	SP2 or SP3	X		233 MHz or greater (single or dual processor system), Intel Pentium/Celeron family, or AMD K6/Athlon/Duron family, or compatible	256 MB	450 MB
Microsoft Windows XP Professional	SP2 or SP3		X	733 MHz or greater	1 GB	500 MB
Microsoft Windows XP Tablet PC Edition	SP3			233 MHz or greater	256 MB**	450 MB
Microsoft Windows XP Embedded (2003)		X		233 MHz or greater	256 MB**	450 MB
Microsoft Windows Embedded Standard 2009		X		233 MHz or greater	256 MB**	450 MB
Microsoft Windows POS 1.1	SP3			233 MHz or greater	256 MB**	450 MB
Microsoft Windows Point of Service (POS) Ready 2009				233 MHz or greater	256 MB**	450 MB
Microsoft Windows Vista Home Basic, Home Premium, Business, Enterprise, and Ultimate		X		1 GHz or greater	1 GB	450 MB
Microsoft Windows Vista Home Basic, Home Premium, Business, Enterprise, and Ultimate			X	1 GHz or greater	1 GB	500 MB
Microsoft Windows 7 Home Premium, Professional, and Ultimate		X		1 GHz or greater	1 GB	450 MB



Operating system	SP	32-bit	64-bit	Processor	RAM	Minimum hard disk space
Microsoft Windows 7 Home Premium, Professional, and Ultimate			X	1 GHz or greater	2 GB	500 MB
<p>* You must install McAfee Agent version 4.0 before installing this version of VirusScan Enterprise on Microsoft Windows 2000 Professional SP4 systems.</p> <p>** At least 250 MB of free memory space must be available to update DAT and engine files. Windows virtual memory can also be used to create additional memory space.</p>						

**Table 2: Minimum server requirements**

Operating system	SP	32-bit	64-bit	Processor	RAM	Hard disk space
Microsoft Windows 2000 Server, Advanced Server, and DataCenter Server editions, with Update Rollup 1*	SP4	X		133 MHz or higher Pentium. Maximum four processors on a single computer.	256 MB minimum and 4 GB maximum	450 MB
Microsoft Windows Server 2003 R2 Standard, Enterprise, Storage, and DataCenter Editions	SP1 or SP2	X		133 MHz or greater. One or more processors on a single computer.	256 MB minimum and 32 GB maximum	450 MB
Microsoft Windows Server 2003 R2 Standard, Enterprise, Storage, and DataCenter Editions	SP1 or SP2		X	1.4 GHz or greater. One to eight processors on a single computer.	1 GB minimum and 1024 GB (1 Terabyte) maximum	500 MB
Microsoft Windows Server 2008 Standard, Enterprise and DataCenter editions**		X		1 GHz (x86 processor) or 1.4 GHz (x64 processor)	512 MB or greater. 4 GB (Standard) or 64 GB (Enterprise and DataCenter)	450 MB
Microsoft Windows Server 2008 Standard, Enterprise and DataCenter editions, with Hyper-V and non-Hyper-V versions**			X	1.4 GHz	32 GB (Standard) or 2 TB (Enterprise, DataCenter)	500 MB
Microsoft Windows Server 2008 Standard, Enterprise, and DataCenter versions R2, with Hyper-V and non-Hyper-V versions**			X	1.4 GHz	512 MB minimum and maximum 8 GB (Foundation) or 32 GB (Standard) or 2 TB (Enterprise, DataCenter)	500 MB
<p>* You must install McAfee Agent version 4.0 before installing this version of VirusScan Enterprise on Microsoft Windows 2000 Professional SP4 systems.</p> <p>** Includes support for Server Core installation.</p>						

- **Microsoft Outlook** — Microsoft Outlook client versions Microsoft Outlook 2003, Microsoft Outlook 2007, and Microsoft Outlook 2010 (both 32-bit and 64-bit).
- **Lotus Notes** — Lotus Notes version 7.0x, and 8.0x through 8.5.1.
- **Browsers** — The following browsers are supported with VirusScan Enterprise ScriptScan:  
**NOTE:** For ePolicy Orchestrator browsers supported refer to the ePolicy Orchestrator documentation.
  - Microsoft Internet Explorer version 6 or later.
  - Firefox 3.x or later.
- **Windows Installer** — Microsoft Windows Installer (MSI) version 3.1 or later.
- **Other** — A CD-ROM drive or Internet connection from which you can install or download software.

**CAUTION:** You must uninstall any other anti-malware products before installing VirusScan Enterprise. McAfee does not support installation with other third-party anti-virus solutions.

**NOTE:** The VirusScan Enterprise installer automatically identifies and removes most incompatible software during VirusScan Enterprise installation. See KB Article <https://kc.mcafee.com/corporate/index?page=content&id=KB60252> for a complete list of automatically removed third-party software.

## Product upgrade and preserving settings

If you are installing VirusScan Enterprise on a computer with an earlier version of the product, you can preserve settings from the earlier version. These settings are preserved during the product upgrade:

- Configuration settings for saved tasks.
- User-specified extensions.
- Exclusion settings.
- Access protection rules.
- Detection definition (DAT) file version and scanning engine version, if either previous version is later than the version in the installation package.
- Log file names and locations.

**NOTE:** 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.

### How access protection rules are preserved

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 8.8 default rules.
- 3** If no exact match is found when comparing local rules to the default rules, 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, the rule is placed in a separate list of rules to be merged with the equivalent VirusScan Enterprise 8.8 rules.
- 5 The whitelist for each of the port rules from Step 4 is merged with the whitelist of the equivalent VirusScan Enterprise 8.7i rule. A newly formed rule is written to the registry for use by VirusScan Enterprise 8.8.
- 6 From Step 3, the modified default rules are converted to the new VirusScan Enterprise 8.8 rule format and written to the registry. These preserved rules are included in the user-defined rules.

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

## Options for preconfiguring, deploying, updating, and managing VirusScan Enterprise

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

### Preconfigure the installation package

Use McAfee Installation Designer 8.8 to preconfigure or customize the installation options for VirusScan Enterprise 8.8. When preconfiguring the installation package, McAfee recommends that you include the following information:

- 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 8.8 Product Guide* for more information.

### Deploy the installation package

Use ePolicy Orchestrator version 4.0, 4.5, or 4.6 to push the software to client computers.

**TIP:** Before pushing the software to client computers, use McAfee Installation Designer 8.8 to replace or update the DAT and engine files included in the installation package. This ensures that the client computer has the most current protection at installation time, and saves network bandwidth.

### Install and configure 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 might 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 prompts you to install the program files using the Windows Add/Remove Programs utility.

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

## Product license and performing an upgrade

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

**CAUTION:** Perform the license upgrade before the evaluation period expires. Otherwise, the scanning function for the on-demand and on-delivery email scanners and the updating function 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 8.8 (*recommended*). Refer to the *McAfee Installation Designer 8.8 Product Guide* for details.
- Remove the evaluation version of the product and install the licensed version.

**NOTE:** Removing the evaluation version causes you to lose all of the configured settings from that installation. Use this method only if you cannot use McAfee Installation Designer 8.8 to upgrade the license.

# Installing VirusScan Enterprise

---

You can install the standalone and ePolicy Orchestrator managed versions of the VirusScan Enterprise software using the Setup utility or the command line.

## Contents

- ▶ Using the Setup utility to install the software
- ▶ Using the command line to install the software
- ▶ Placing the product under ePolicy Orchestrator management
- ▶ Migrating the ePolicy Orchestrator policies

## Using the Setup utility to install the software

Install the standalone version of the VirusScan Enterprise software using the Setup utility.

### Task

- 1 Start the Setup utility using one of these methods:
  - Product CD — When the CD is loaded, the autorun window appears. Select the product you want to install.
  - Windows Explorer — From the location where you extracted the program files, double-click **SetupVSE.exe**.
  - Command line — From the **Start** menu, select **Run**, then type the following and click **OK**: `<X>:\SetupVSE.exe` The `<X>` represents the path of the folder containing the extracted program files.
- 2 In the **McAfee VirusScan Enterprise Setup** dialog box, click **View Readme** to review the release notes for special installation instructions or known issues, then click **Next** to continue.
- 3 In the **McAfee End User License Agreement** dialog box, select and read the product license, click **I accept the terms in the license agreement**, then click **Next** to continue. The license type must match the license type that you purchased. If you don't know which type of license to select, contact the person from whom you purchased the software.
- 4 **Upgrade only.** In the **Previous Version Detected** dialog box, select **Preserve Settings**. See *Product upgrade and preserving settings* for more information.

**NOTE:** When upgrading from VirusScan Enterprise 8.5i or VirusScan Enterprise 8.7i, the DAT files are preserved.
- 5 In the **Select Setup Type** dialog box, choose the installation type and location.

By default, Setup installs the VirusScan Enterprise program files to <drive>:\Program Files\McAfee\VirusScan Enterprise\.

- **Typical** — (*Recommended*) Installs the software with all features.
  - **Custom** — Installs the software with all or selected features and allows you to customize some settings. Use this to install only selected features, import an AutoUpdate repository list, or specify user interface settings during the installation process.
- 6** In the **Select Access Protection Level** dialog box, choose which access protection rules are enabled by default when the feature is installed.
- **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 7.
    - **Typical Installation** — Go to Step 11.
- 7** In the **Feature Selection** dialog box, select specific features to install. For each selected feature you can also select a corresponding action from the list next to the feature name.
- **Console** — Installs the VirusScan Console and all of its features (default = **Console**).
  - **AutoUpdate** — Automatically updates DAT files, scanning engine, and other product upgrades.
  - **Lotus Notes Email Scanner** — Scans Lotus Notes email.
  - **On-Access Scanner** — Protects your system against potential threats from any source as files are read from or written to disk.
  - **Access Protection** — Protects your system access points.
  - **Buffer Overflow Protection** — Protects your system against buffer overflow exploits. Not installed on 64-bit systems, nor if the Host Intrusion Prevention agent or the Cisco Security agent is found on a local system.
  - **Script Scan** — Scans scripts (Java Script and VBScript) before they are executed.
  - **On-Demand Scan** — Allows you to perform immediate or scheduled on-demand scan tasks.
  - **Right-click Scan** — Allows you to perform on-demand right-click scan tasks.
- 8** In the **Install McAfee Products** dialog box, select **Install Alert Manager** to install Alert Manager after the installation is complete. Click **Browse** to navigate to the Alert Manager location.
- 9** In the **Product Configuration** dialog box, import a repository list and/or choose whether to enable the on-access scanner when the installation is complete.
- **Import AutoUpdate repository list** — Import the repository list from a specified location, which must be a local drive.

**NOTE:** This option is selected by default only if a repository list is included in the installation file (.msi) or if the command-line property (cmasourcedir) has been set to a new location to point to the Sitelist.xml file.

If you do not import a repository list at this time, and one resides in the installation folder, it is 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. See the *Updating detection definitions* section of the *VirusScan Enterprise Product Guide* for more information.

- **Enable On-Access Scanner at the end of installation** — *(Recommended)*  
Automatically start the on-access scanner upon completion of the installation process.

- 10** In the **Security Configuration** dialog box, specify password security and which system tray options users can access.

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

- 11** In the **Ready to install** dialog box, click **Install** to begin the installation process.

- 12** In the **McAfee VirusScan Enterprise setup has completed successfully** dialog box, choose whether to perform an update task and an on-demand scan task when the installation is complete.

- **Update Now** — Automatically run an update task when the installation is complete.
- **Scan Now** — Automatically run a **Full Scan** when the installation is complete.

**NOTE:** If you are installing VirusScan Enterprise 8.8 on a system where VirusScan Enterprise has never been installed before, Update Now is selected and grayed out.

If you select both options, the update task runs first before the on-demand scan task runs.

**CAUTION:** On first-time installations of VirusScan Enterprise 8.8, your system does not have virus protection if the DAT update fails. The DAT update fails if either of the following occurs while the McAfee AutoUpdate process is running:

- You click **Cancel** while the Update in Progress process is running.
- The Update in Progress process fails.

**NOTE:** To confirm the DAT update was successful in the VirusScan Console, click **Help | About VirusScan Enterprise** and the About VirusScan Enterprise dialog box appears. Confirm the **DAT Version** is *not* listed as **1111**, which indicates that the DAT update failed. The four "ones" indicated the DAT update failed.

If the automatic DAT update fails, manually update the DAT file. Refer to the *McAfee VirusScan Enterprise 8.8 Product Guide* to run Update Now from the AutoUpdate task, or download a SuperDAT file.

- 13** When the installation is complete, you are prompted to restart the computer to load the network driver.

**CAUTION:** Distributed File Scanning, Port Blocking, Infection Trace, and Infection Trace Blocking are disabled until the computer is restarted.

## Using the command line to install the software

Install the standalone version of the VirusScan Enterprise software using the command line. This method allows you to customize the installation so that it runs the way you want and installs exactly the product features you want.

### Before you begin

You must have local administrator rights to run the SetupVSE.exe executable from the command line.

## Task

- Open the Command Prompt or the Run dialog box and type this command:  
SetupVSE.exe PROPERTY=VALUE[,VALUE] [/option]

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

- **File name** — The name of the executable file, SetupVSE.exe.
- **Options** — Specify options for installing the software, such as perform a silent installation or record installation progress in a log file. See *Installation scenarios* for the available options.

Each option is preceded by a forward slash (/) and is not case-sensitive.

- **Properties** — Specify how the installation runs. Each property consists of:
  - A name in uppercase letters.
  - An equal (=) sign.
  - One or more values, each separated by a comma. Most property values must appear in uppercase but some, such as True and False, must appear in mixed case.

**NOTE:** The Microsoft Installer permits properties that determine how your installation runs. For details, see the Microsoft Installer documentation.

## Installation scenarios

Use these scenarios to customize your installation.

Scenario	Definition
<b>Silent</b>	<p>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.</p> <p><b>NOTE:</b> When you install the product silently, the default license option of "1 year perpetual" is selected. VirusScan Enterprise does not enforce any license restrictions and no license expiration occurs.</p> <p>Add these options to run a silent or semi-silent installation:</p> <p><b>q</b> or <b>qn</b> — Silent installation. This installs default settings unless you specify otherwise. For example, unless changed the product license default is <b>1 Year Subscription</b>.</p> <p><b>qb</b> — Basic user interface. Use <b>qb!</b> to hide the Cancel button.</p> <p><b>qb+</b> — Basic user interface with a modal dialog box displayed at the end of installation. Use <b>qb+!</b> or <b>qb!+</b> to hide the Cancel button. The modal dialog box is not displayed if the user cancels the installation.</p> <p><b>qb-</b> — Basic user interface with no modal dialog boxes. Use <b>qb-!</b> or <b>qb!-</b> to hide the Cancel button.</p> <p><b>qf</b> — Full user interface and any authored <b>FatalError</b>, <b>UserExit</b>, or <b>Exit</b> modal dialog box displayed at the end of the installation.</p> <p><b>qn+</b> — No user interface except for a modal dialog box displayed at the end of the installation.</p> <p><b>qr</b> — Reduced user interface with no modal dialog box displayed at the end of the installation.</p>
<b>Custom Location</b>	<p>Add the <b>installdir</b> 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:</p> <pre>SetupVSE.exe INSTALLDIR="c:\My AntiVirus Software" /q</pre>



Scenario	Definition
<b>Login Script</b>	Add a <b>Setup</b> command to your login script to install VirusScan Enterprise software when 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.  <b>NOTE:</b> To use a login script for this purpose, you must also copy or push the VirusScan Enterprise installation package to a location on the destination computer.

## Installation options and properties

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

### Command-line installation options

When you run the Setup utility 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. For example:

```
SetupVSE.exe /q ADDLOCAL=Console,OnAccessScanner,AccessProtection,EmailScan
```

Use these feature names as command-line parameters:

Feature	Definition
<b>Console</b>	Installs the VirusScan Console and all of its features (default = <b>Console</b> ).
<b>AutoUpdate</b>	Automatically updates DAT files, scanning engine, and other product upgrades.
<b>LotusNotesScan</b>	Scans Lotus Notes email.
<b>EmailScan</b>	Scans Microsoft Outlook email.
<b>OnAccessScanner</b>	Protects your system against potential threats from any source as files are read from or written to disk.
<b>AccessProtection</b>	Protects your system access points.
<b>BufferOverflow</b>	Protects your system against buffer overflow exploits. Not installed on 64-bit systems, nor if the Host Intrusion Prevention agent or the Cisco Security agent is found on a local system.
<b>ScriptScan</b>	Scans scripts (Java Script and VBScript) before they are executed.
<b>OnDemandScanner</b>	The scanner that allows you to perform either immediate or scheduled on-demand scan tasks.
<b>ShellExtensions</b>	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	Definition
<b>REBOOT=F</b>	Forces a restart if one is required.
<b>REBOOT=R</b>	Prevents a restart.  <b>NOTE:</b> Use this command to run a silent installation and prevent a system restart: SetupVSE.exe REBOOT=R /q
<b>REBOOT=A</b>	Always restarts.

## Installation progress options

To record installation progress in a log file, add this option and parameter to the Setup command line: `/!*v "c:\temp\log.txt"`

Here, `c:\temp\log.txt` is any location and any file name for the log file. This option logs all installer activity including all files copied, all registry keys added, and all `.ini` file changes.

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

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

## Installation properties

Use these properties to customize the command-line installation:

Properties	Definition
<b>ADDLOCAL</b>	Installs specific features to the local computer.
<b>CMASOURCEDIR</b>	Set the source path for the <code>Sitelist.xml</code> file (default = <code>%temp%\naitemp</code> ). The repository list must be located on a local drive and cannot be imported from a mapped or a network drive.
<b>ENABLEONACCESSSCANNER</b>	False = Not valid. True = Enable the on-access scanner when the installation is complete (default). If you do not want to enable the on-access scanner, set the property to "", an empty string. For example, <code>ENABLEONACCESSSCANNER=""</code>
<b>EXTRADATSOURCEDIR</b>	Set the source path for the <code>EXTRA.DAT</code> file. During installation, the <code>EXTRA.DAT</code> file is copied to the location where the engine files reside.
<b>ICONLOCKDOWN</b>	Specifies if the system tray icon appears and the menu options: <code>ICONLOCKDOWN=0</code> — Show the system tray icon with all menu options (default). <code>ICONLOCKDOWN=1</code> — Show the system tray icon with minimal menu options. <code>ICONLOCKDOWN=2</code> — Do not show the system tray icon. The default is to display icon, set the property to "0". For example: <code>ICONLOCKDOWN=0</code>
<b>INSTALLDIR</b>	Specifies the path of the installation folder. The value consists of the installation path.

Properties	Definition
<b>LOCKDOWNSHORTCUTS</b>	<p>False = Not valid.</p> <p>True = Do not display any shortcuts under the Start menu.</p> <p>The default is an empty string. To allow the shortcuts to be installed, set the property to "", an empty string. For example: LOCKDOWNSHORTCUTS=""</p>
<b>PRESERVESETTINGS</b>	<p>False = Not valid.</p> <p>True = Preserve settings (default).</p> <p>Preserves settings when upgrading from an earlier version of VirusScan Enterprise. If you do not want to preserve settings, set the property to "", an empty string. For example: PRESERVESETTINGS=""</p>
<b>PROTECTIONTYPE</b>	<p>Configures VirusScan Enterprise to install with Maximum or Standard security:</p> <ul style="list-style-type: none"> <li>• ProtectionType=Standard</li> <li>• ProtectionType=Maximum</li> </ul>
<b>REBOOT</b>	<p>Restart your computer.</p> <p>You can force the computer to restart if it is required, or prevent it from restarting.</p>
<b>REMOVE</b>	<p>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.</p>
<b>RUNAUTOUPDATE</b>	<p>False = Not valid.</p> <p>True = Run update when the installation is complete (default).</p> <p>Use this command for interactive installations. If you do not want to run an update when the installation is complete, set the property to "", an empty string. For example: RUNAUTOUPDATE=""</p>
<b>RUNAUTOUPDATESILENTLY</b>	<p>False = Not valid.</p> <p>True = Run a silent update when the installation is complete.</p> <p>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 is complete, set the property to "", an empty string. For example: RUNAUTOUPDATESILENTLY=""</p>
<b>RUNONDEMANDSCAN</b>	<p>False = Not valid.</p> <p>True = Run a scan of all local drives when the installation is complete (default).</p> <p>Use this command when performing interactive installations. If you do not want to run the on-demand scanner when the installation is complete, set the property to "", an empty string. For example: RUNONDEMANDSCAN=""</p>
<b>RUNONDEMANDSCANSILENTLY</b>	<p>False = Not valid.</p> <p>True = Run an on-demand scan silently when the installation is complete.</p> <p>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 is complete, set the property to "", an empty string. For example: RUNONDEMANDSCANSILENTLY=""</p>

### Command-line examples

To do this...	Run this command...
<b>Silently install all features</b>	SetupVSE.exe ADDLOCAL=ALL /q

To do this...	Run this command...
<b>Install more than one feature</b>	Use a comma to separate more than one feature. For example, to install the on-access scanner and Script Scan, run SetupVSE.exe ADDLOCAL=OnAccessScanner,ScriptScan /q
<b>Install all features except one</b>	SetupVSE.exe ADDLOCAL=ALL REMOVE=ScriptScan /q
<b>Silently remove all features</b>	SetupVSE.exe REMOVE=ALL /q
<b>Install features using a loud installation</b>	Omit the /q option in any of the command-line examples shown here.

## Installing using an Administrative Installation Point

One method of deploying a customized version of VirusScan Enterprise to a large number of users is to create an Administrative Installation Point (AIP) on a network server. Then you can run the SetupVSE.exe /a command from there. This method allows you to:

- Manage a single set of VirusScan Enterprise files from a central location.
- Create a standard VirusScan Enterprise configuration for a group of users.
- Take advantage of flexible installation options.

To create an AIP complete the following:

### Task

- 1 At the command prompt, type SetupVSE.exe /a. A wizard helps you create the AIP.
- 2 Follow the instruction and create the AIP. When the AIP is created, all of the necessary files in the compressed (.ZIP) file are also copied to the AIP.

If you deploy VirusScan Enterprise using Active Directory group policies, which install using MSIEXEC.EXE, you must remove any existing anti-virus products prior to installing VirusScan Enterprise.

## Placing the product under ePolicy Orchestrator management

You can use ePolicy Orchestrator 4.0, 4.5, or 4.6 to manage the VirusScan Enterprise 8.8 software. To include VirusScan Enterprise 8.8 in the list of products managed by ePolicy Orchestrator, you must install the following VirusScan Enterprise extension .zip files (XXX is the build number of the VirusScan Enterprise 8.8 software.):

- **VIRUSCAN8800(XXX).zip** — Contains the files, components, and information necessary to manage VirusScan Enterprise 8.8 with ePolicy Orchestrator. This extension can co-exist with extensions that manage earlier versions of VirusScan Enterprise.
- **VIRUSCANREPORTS120(XXX).zip** — Contains the queries and reporting functionality VirusScan Enterprise 8.8 uses with ePolicy Orchestrator. This replaces any existing VirusScan Enterprise reports and includes queries and reports for earlier versions of VirusScan Enterprise.

- **epo45\_help\_vse\_880.zip** — Contains the Help files used to describe the VirusScan Enterprise 8.8 features and user interface for ePolicy Orchestrator 4.5 and 4.6.

**NOTE:** This file does not provide ePolicy Orchestrator 4.0 Help files.

### Before you begin

You must have the appropriate permissions to perform this task.

### Task

For option definitions, click **?** in the interface.

- 1 From your version of ePolicy Orchestrator, open the Install Extension dialog box:
  - ePolicy Orchestrator 4.5 or 4.6 — Click **Menu | Software | Extensions | Install Extension**.
  - ePolicy Orchestrator 4.0 — Click **Configuration | Extensions**, then click **Install Extension**.
- 2 Browse to where you saved the VirusScan Enterprise 8.8 installation files (described in *Preparation for installing the software*) and select the extension file **VIRUSCAN8800(XXX).zip**.
- 3 Click **OK**. If prompts to verify the installation version number, click **OK**.
- 4 After the extension installation is complete, confirm that the VirusScan Enterprise 8.8 extension appears in the Extensions list of ePolicy Orchestrator.
- 5 Repeat steps 2-4 to install these extension files:
  - VirusScan Enterprise 8.8 queries and reporting — Select **VIRUSCANREPORTS120(XXX).zip**.
  - VirusScan Enterprise 8.8 Help files — Select **epo45\_help\_vse\_880.zip**.

## Migrating the ePolicy Orchestrator policies

You can use the ePolicy Orchestrator Migration Tool to migrate the existing VirusScan Enterprise 8.7i policies and tasks for use with VirusScan Enterprise 8.8.

**NOTE:** This process is the same for ePolicy Orchestrator 4.0, 4.5, and 4.6. For information about using ePolicy Orchestrator, see that version's product documentation.

### Before you begin

Before using the migration tool you must check the new VirusScan Enterprise 8.8 extension into the ePolicy Orchestrator repository. Refer to *Placing the product under ePolicy Orchestrator management*.

**NOTE:** When the ePolicy Orchestrator Migration Tool migrates the VirusScan Enterprise 8.7i tasks, the migration tool appends "(VSE 8.8)" to the migrated task names. For example, a VirusScan Enterprise 8.7i on-demand scan task named "VSE 8.7i Weekly ODS task" is renamed "VSE 8.7i Weekly ODS task (VSE 8.8)".

## Task

- 1 Browse to where you saved the VirusScan Enterprise 8.8 installation files (described in *Preparation for installing the software*) and double-click the **ePOPolicyMigration.exe** file.

**NOTE:** When upgrading VirusScan Enterprise 8.5i policies and tasks, use the command-line option with the force switch as follows: ePOPolicyMigration.exe /force85

- 2 After the tool has run one of the following ePolicy Orchestrator Migration Tool dialog boxes appears:

Dialog box text	Action
The migration has completed successfully.	Your migration is complete.
The migration tool has already run. To run it again the VirusScan Enterprise extension must be removed from the ePolicy Orchestrator repository and then installed again.	To remove and reinstall the extension, see the ePolicy Orchestrator documentation for details.
The most recent version of the VirusScan Enterprise extension is not checked in. It must be checked in before running the migration tool.	See section, <i>Placing the product under ePolicy Orchestrator management</i> for details.
The migration tool was unable to connect to the ePolicy Orchestrator database. The migration cannot continue.	<p>If you see this error, try the following:</p> <ul style="list-style-type: none"> <li>• Confirm you ran the ePolicy Orchestrator Migration Tool on a server with ePolicy Orchestrator installed. See the ePolicy Orchestrator documentation for details.</li> <li>• The database connection could fail the authentication step caused by a missing password. Try using the ePolicy Orchestrator /PASSWORD switch in the command. For example: epolicymigration.exe /PASSWORD=ePOpassword.</li> <li>• If none of these suggestions solve the problem, go to the McAfee Technical Support ServicePortal at <a href="http://mysupport.mcafee.com">http://mysupport.mcafee.com</a></li> </ul>
The migration script failed. The migration was unsuccessful.	Go to the McAfee Technical Support ServicePortal at <a href="http://mysupport.mcafee.com">http://mysupport.mcafee.com</a> .

- 3 Click **OK**. The ePolicy Orchestrator Migration tool migrates the existing VSE 8.7 policies and tasks to VirusScan Enterprise 8.8.
- 4 After the migration is complete, review the migrated tasks and policies. If needed, rename the migrated tasks and policies.

**NOTE:** To navigate to the list of VirusScan Enterprise 8.8 client tasks and policies, see the *McAfee VirusScan Enterprise 8.8 Product Guide*.

# Post-Installation Tasks

---

After installing the VirusScan Enterprise program files, it is important to test your installation to make sure your system can detect malware and potentially unwanted programs (PUPs). You can also check the location on your system where the program files were installed.

## Contents

- ▶ [Testing your installation](#)
- ▶ [Location of installed files](#)

## Testing your installation

You can use test files created by the European Institute for Computer Anti-Virus Research (EICAR) to confirm your installation is installed correctly and can properly scan for malware and potentially unwanted programs (PUPs). Running these EICAR test files also shows you what happens when VirusScan Enterprise detects a virus.

**NOTE:** The EICAR test files are safe and do not contain a virus or any fragments of viral code.

## Tasks

- ▶ [Testing for malware detection](#)
- ▶ [Testing for potentially unwanted programs detection](#)

## Testing for malware detection

The EICAR test file is used to confirm VirusScan Enterprise is installed correctly and can properly scan and find malware and viruses.

**NOTE:** 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.

## Task

- 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.

## Testing for potentially unwanted programs detection

The EICAR-PUO test file is used to confirm VirusScan Enterprise is installed correctly and can properly scan and find potentially unwanted programs.

**NOTE:** 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.

### Before you begin

To successfully detect the EICAR-PUO test file, the Potentially Unwanted Program detection feature must be enabled. See *Configuring the unwanted programs policy* in the *VirusScan Enterprise Product Guide* for additional information.

### Task

- 1 Using a standard Windows text editor such as Notepad, type the following string, on a single line with no spaces or line breaks:  
X5]+)D:)D<5N\*PZ5[/EICAR-POTENTIALLY-UNWANTED-OBJECT-TEST!\$\*M\*L
- 2 Save the file with the name EICAR-PUO.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-access scanner, confirm that Potentially Unwanted Program (PUP) is configured to find unwanted spyware programs.
- 5 Locate the EICAR-PUO.COM file and try to copy or move it to another location. The scanner reports finding the EICAR-PUO test file when it examines the file.

## Location of installed files

During installation, product and system files are installed in various locations. If you have a 32- or 64-bit operating system, the files and their locations vary.

### Tasks

- ▶ [Location of 32-bit operating system installed files](#)
- ▶ [Location of 64-bit operating system installed files](#)

## Location of 32-bit operating system installed files

If you have a 32-bit operating system, during installation the product and system files are installed in the locations listed in this section.

### Product files

Product files for 32-bit operating systems are installed in the installation folder, which is determined during installation. The default location is: <drive>:\Program Files\McAfee\VirusScan Enterprise

### VirusScan Enterprise 32-bit operating system folder

aslicense.bin	McShieldPerfData.ini	pireg.exe
BBCpl.dll	McShieldPerfData.reg	QuarCpl.dll



condl.dll	mcupdate.exe	readme.html
consl.dll	MERTool.url	restartvse.exe
coptcpl.dll	mfeann.exe	scan32.exe
csscan.exe	mfeapconfig.dll	ScnCf32.Exe
Emabout.dll	midutil.dll	shcfg32.exe
EmCf32.dll	mytilus3.dll	shext.dll
EmHelp.dll	mytilus3_server.dll	shstat.dll
ftcfg.dll	mytilus3_worker.dll	shstat.exe
ftl.dll	NaEvent.Dll	shutil.dll
graphics.dll	naiaann.dll	vscan.bof
license.bin	nailite.dll	VsEvtUI.DLL
lockdown.dll	NCDaemon.exe	vsodscpl.dll
logparser.exe	NCExtMgr.dll	vsplugin.dll
mcadmin.exe	NCInstall.exe	VsTskMgr.exe
McAVDetect.DLL	NCMenu.dll	vsupdcpl.dll
McAVSCV.DLL	NCMenu.dll	wmain.dll
mcconsol.exe	NCTrace.dll	WscAv.dll
McShieldPerfData.dll	nvpcpl.dll	wscavexe.exe
McShieldPerfData.h	OASCpl.dll	

### SystemCore 32-bit operating system folder

For 32-bit operating systems the default location for the SystemCore files is: <System drive>:\Program Files\Common Files\McAfee\SystemCore

adslokuu.dll	mfebopa.dll	mytilus3_worker.dll
entvutil.exe	mfehida.dll	naevent.dll
ftl.dll	mfehidin.exe	naievent.dll
lockdown.dll	mfehdk_messages.dll	OtlkScan.dll
mcshield.dll	MfeOtlk.dll	OtlkUI.yyyymmddhhmmss.dll
mcshield.exe	MfeOtlkAddin.dll	scriptff.dll
mcvssnmp.dll	mferkda.dll	ScriptSn.yyyymmddhhmmss.dll
mfeann.exe	mfevtpa.dll	scriptsn.dll
mfeapconfig.dll	mfevtps.exe	strings.bin
mfeapfa.dll	mytilus3.dll	vscan.bof
mfeavfa.dll	mytilus3_server.dll	

### Resources folder

The Resources folder name for 32-bit operating systems depends on the language being installed. For example, the default location for the English folder is: <drive>:\Program Files\McAfee\VirusScan Enterprise\Res0900

mcshield.dll  
strings.bin

### 32-bit operating system engine folder

The engine folder contains common files and those required to scan 32-bit operating systems. These files are installed in the engine folder in the installation path. The default location is: <drive>:\Program Files\Common Files\McAfee\Engine

avclean.dat	avvnames.dat	avvscan.dat	config.dat
license.dat	mcscan32.dll	messages.dat	signlic.txt

### 32-bit operating system files

The system files for 32-bit operating systems are installed in the System32 folder. The default location for system files is: <drive>:\Windows\System32

mfeOtlk.dll  
mfeOtlkAddin.dll

The default location for 32-bit operating system drivers is: <drive>:\Windows\System32\drivers

Mfeapfk.sys	Mfebopk.sys	Mfehidk.sys	Mfetdi2k.sys
Mfeavfk.sys	MfeInk.sys	Mferkdet.sys	

## Location of 64-bit operating system installed files

If you have a 64-bit operating system, during installation the product and system files are installed in the locations listed in this section.

### Product files

Product files for a 64-bit operating system are installed in the installation folder, which is determined during installation. The default location is: <drive>:\Program Files (x86)\McAfee\VirusScan Enterprise

### VirusScan Enterprise 64-bit operating system folder

aslicense.bin	BBCpl.dll	condl.dll
consl.dll	coptcpl.dll	csscan.exe
Emabout.dll	EmCfgCpl.dll	EmHelp.dll
ftcfg.dll	ftl.dll	graphics.dll
license.bin	lockdown.dll	logparser.exe
mcadmin.exe	McAVDetect.DLL	McAVSCV.DLL
mcconsol.exe	McShieldPerfData.dll	McShieldPerfData.h
McShieldPerfData.ini	McShieldPerfData.reg	mcupdate.exe
MERTool.url	mfeann.exe	mfeapconfig.dll
midutil.dll	mytilus3.dll	mytilus3_server.dll
mytilus3_worker.dll	NaEvent.Dll	naiann.dll
nailite.dll	NCInstall.exe	nvpcl.dll
OASCpl.dll	pireg.exe	QuarCpl.dll
readme.html	restartvse.exe	scan32.exe
ScnCfg32.Exe	shcfg32.exe	shext.dll
shstat.dll	shstat.exe	shutil.dll
vscan.bof	VsEvtUI.DLL	vsodscpl.dll
vsplugin.dll	VsTskMgr.exe	vsupdate.dll
vsupdcpl.dll	wmain.dll	WscAv.dll
wscavexe.exe		

## SystemCore 64-bit operating system folder

For 64-bit operating systems the default location of the SystemCore files is: <System drive>:\Program Files (x86)\Common Files\McAfee\SystemCore

lockdown.dll	mytilus3_worker.dll	ScriptSn.yyyymmddhhmmss.dll
mcshield.dll	OtlkScan.dll	scriptsn.dll
MfeOtlk.dll	OtlkUI.yyyymmddhhmmss.dll	Strings.bin
MfeOtlkAddin.dll	OtlkUI.dll	
mytilus3.dll	scriptff.dll	

## Resources folder

The Resources folder name depends on the language being installed. For example, the default location for the English folder is: <drive>:\Program Files\McAfee\VirusScan Enterprise\Res0900

mcshield.dll  
strings.bin

## 64-bit operating system engine folder

The engine folder contains common files and those required to scan 64-bit operating systems. These files are installed in the engine folder in the installation path. The default location is: <drive>:\Program Files\Common Files\McAfee\Engine

avvclean.dat	avvnames.dat	avvscan.dat	config.dat	signlic.txt
license.dat	mcsan32.dll	messages.dat	mferuntime.dat	

## Engine folder\x64

The 64-bit operating system folder, x64, contains files required to scan 64-bit operating systems. These files are installed in the engine folder in the installation path. The default location is: <drive>:\Program Files (x86)\McAfee\VirusScan Enterprise\x64

csscan.exe	FTL.Dll	mytilus3_server.dll	Scan64.Exe	vsodscpl.dll
emabout.dll	lockdown.dll	mytilus3_worker.dll	shext.dll	wmain.dll
EmCfgCpl.dll	mfeann.exe	NaEvent.Dll	shstat.exe	
EmHelp.dll	mfeapconfig.dll	naiann.dll	ShUtil.Dll	
FtCfg.DLL	mytilus3.dll	nailite.dll	VsEvtUI.DLL	

## 64-bit operating system files

The system files for 64-bit operating systems are installed to the SysWOW64 folder. The default location for system files is: <drive>:\Windows\SysWOW64

mfeOtlk.dll  
mfeOtlkAddin.dll

The default location for 64-bit operating system drivers is: <drive>:\Windows\SysWOW64\drivers

Mfeapfk.sys	MfeWfpk.dll	Mfehdk.sys
Mfeavfk.sys	Mfeclnk.sys	Mferkdet.sys

# Maintenance Tasks

---

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

## Contents

- ▶ [Modifying installed features](#)
- ▶ [Reinstalling or repairing program files](#)
- ▶ [Removing program files](#)

## Modifying installed features

As the requirements for your installation change, use the **Program Maintenance** feature to change which VirusScan Enterprise features are installed.

## Using the Setup utility to modify installed features

Change which features are installed in VirusScan Enterprise 8.8 using the Setup utility.

### Task

- 1 Start the Setup utility using one of these methods:
  - Product CD — When the CD is loaded, the autorun window appears. Select the product you want to install.
  - Windows Explorer — From the location where you extracted the program files, double-click **SetupVSE.exe**.
  - Command line — From the **Start** menu, select **Run**, then type the following and click **OK**: <X>:\SetupVSE.exe The <X> represents the path of the folder containing the extracted program files.
- 2 In the **Program Maintenance** dialog box, select **Modify**.
- 3 In the **Feature Selection** dialog box, select specific features for installation.

**NOTE:** For each selected feature, you can also select a corresponding action from the list next to the feature name.
- 4 In the **Ready to install** dialog box, click **Install** to start the installation process.
- 5 In the **McAfee VirusScan Enterprise setup has completed successfully** dialog box, choose whether to perform an update task and an on-demand scan when the installation is complete and to finish the installation.

**NOTE:** If you select both options, the update task runs first, then the on-demand scan task runs.

## Using the command line to modify installed features

You can use the command line to change which features are installed in VirusScan Enterprise 8.8.

### Task

- 1 To access the Windows command-line component, refer to *Using the command line to install the software*.
- 2 Install or remove features individually using a comma-separated list, or you can specify the all property.
  - **Add a feature** — SetupVSE.exe ADDLOCAL=OnAccessScanner,ScriptScan /q
  - **Remove a feature** — SetupVSE.exe REMOVE=ScriptScan,ShellExtentions/q
  - **Install features using a loud installation** — Omit the /q option in any of the previous command-line examples.

## Reinstalling or repairing program files

Use the **Program Maintenance** feature to reinstall or repair VirusScan Enterprise program files that might have been damaged or deleted.

## Using the Setup utility to reinstall or repair program files

To reinstall or repair program files use the Setup utility.

**NOTE:** If you manually remove or rename any of the program files, the repair feature might fail. See *Troubleshooting* in the *VirusScan Enterprise Product Guide* for detailed instructions about repairing files after they have been removed or renamed.

### Task

- 1 Start the Setup utility using one of these methods:
  - Product CD — When the CD is loaded, the autorun window appears. Select the product you want to install.
  - Windows Explorer — From the location where you extracted the program files, double-click **SetupVSE.exe**.
  - Command line — From the **Start** menu, select **Run**, then type the following and click **OK**: <X>:\SetupVSE.exe The <X> represents the path of the folder containing the extracted program files.
- 2 In the **Program Maintenance** dialog box, select **Repair**.
- 3 In the **Reinstall or Repair the Product** dialog box, choose whether to reinstall or repair VirusScan Enterprise program files and to rewrite registry keys as needed.
  - **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.  
**NOTE:** 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.
  - **Rewrite registry keys** — Rewrites registry keys as necessary during the repair process (available only for **Detect and repair missing or corrupt files**).
- 4** In the **McAfee VirusScan Enterprise setup has completed successfully** dialog box, choose whether to perform an update task and an on-demand scan when the installation is complete.
- NOTE:** If you select both options, the update task runs first, then the on-demand scan task runs.

## Using the console to reinstall or repair program files

To restore the program's default installation settings and reinstall all program files, use the VirusScan Console repair installation utility.

### Task

For option definitions, click **Help** in the interface.

- 1** Click **Help | Repair Installation** to access the **Repair Installation** utility from the VirusScan Console.  
**NOTE:** This feature is not available from the ePolicy Orchestrator console.
- 2** From the Repair Installation dialog box, click either of the following and click **OK**:
  - **Restore all settings to installation defaults** — Restores the VirusScan Enterprise default installation settings.  
**CAUTION:** Customized settings might be lost.
  - **Reinstall all program files** — Reinstalls the VirusScan Enterprise program files.  
**CAUTION:** Hotfixes, Patches, and Service Packs might be overwritten.

## Using the command line to reinstall or repair program files

Use this task to change which features are installed, using the command line.

### Task

- 1** Open the Windows command-line component. See *Using the command line to install the software* for more information.
- 2** Install or remove features individually using a comma-separated list, or you can specify the ALL property.
  - **Reinstall the product** — `msiexec /I{product code} REINSTALL=[feature] REINSTALLMODE=[option]`
  - **Remove a feature** — `msiexec /f[option] {product code} REMOVELOCAL=[feature]`

- **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

You can remove the VirusScan Enterprise program files to reinstall another version of the program or to completely remove the program.

**NOTE:** McAfee strongly recommends that you restart your computer after you remove files and before you reinstall the software.

When you remove files using Setup or the command line, some files or stopped services might not be removed. For example, if you remove VirusScan Enterprise 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.

## Using the Setup utility to remove program files

To remove program files, use the Setup utility.

### Task

- 1 Start the Setup utility using one of these methods:
  - Product CD — When the CD is loaded, the autorun window appears. Select the product you want to install.
  - Windows Explorer — From the location where you extracted the program files, double-click **SetupVSE.exe**.
  - Command line — From the **Start** menu, select **Run**, then type the following and click **OK**: <X>:\SetupVSE.exe The <X> represents the path of the folder containing the extracted program files.
- 2 In the **Program Maintenance** dialog box, select **Remove**.
- 3 Select **Remove** again, then click **Finish**.

**NOTE:** After the program files are removed, you might be prompted to remove remaining files or folders. These are files or folders that 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.

- 4 *(Recommended)* Restart your computer before reinstalling the software.

## Using the command line to remove program files

To remove program files, use the command line.

### Task

- 1 Type this syntax at the command prompt:  
<X>:\SetupVSE.exe /x  
where <X>: represents the path of the location of the extracted program files.
- 2 *(Recommended)* Restart your computer before reinstalling the software.

## Using the Add/Remove Programs utility to remove program files

To remove program files, use the Add/Remove Programs utility.

### Task

- 1 Click **Start**, then select **Settings | Control Panel | Add/Remove Programs**.
- 2 Select the VirusScan Enterprise program from the list of installed programs, then click **Remove**.
- 3 *(Recommended)* Restart your computer before reinstalling the software.



# Index

## A

- Access Protection feature
  - default levels of protection [13](#)
  - installing from the command line [17](#)
  - installing with Setup [13](#)
- Add/Remove Programs, removing program files [32](#)
- administrator rights
  - silent installation [16](#)
  - system requirements [7](#)
- Alert Manager, installing [13](#)
- audience for this guide [5](#)
- AutoUpdate feature
  - installing from the command line [17](#)
  - installing with Setup [13](#)

## B

- Buffer Overflow Protection
  - installing from the command line [17](#)
  - installing with Setup [13](#)

## C

- command line
  - command examples [19](#)
  - installation options [16](#)
  - modifying installed features [29](#)
  - progress options, installation [18](#)
  - properties, installation [18](#)
  - removing program files [32](#)
  - restart options [17](#)
  - scenarios for installation [16](#)
  - selecting features, installation [17](#)
- Console feature
  - installing from the command line [17](#)
  - installing with Setup [13](#)
- conventions used in this guide [5](#)
- Custom installation, selecting a type [13](#)

## D

- documentation
  - product-specific, finding [6](#)
  - typographical conventions [5](#)

## E

- EICAR test for your installation [23, 24](#)
- ePolicy Orchestrator
  - installing VirusScan Enterprise [20](#)
  - version requirements [20](#)

## F

- features
  - modifying [28](#)

- features (*continued*)
  - selecting and installing [13, 17](#)

## I

- installation
  - Alert Manager [13](#)
  - license type, selecting [13](#)
  - loading network driver [13](#)
  - modifying installed features [28](#)
  - post-installation tasks [23, 24](#)
  - preserving settings from a previous version [10, 13](#)
  - requirements [8](#)
  - selecting features [13, 17](#)
  - Setup utility, installing with [13](#)
  - testing [23, 24](#)
  - Typical or Custom setup type, selecting [13](#)
  - upgrading an evaluation version [10](#)
  - user interface security [13](#)

## L

- license agreement, selecting correct license type [13](#)
- login script, command-line options [16](#)
- Lotus Notes Email Scanner
  - installing from the command line [17](#)
  - installing with Setup [13](#)

## M

- Maximum protection level, selecting [13](#)
- McAfee ServicePortal, accessing [6](#)
- Microsoft Outlook Email Scanner
  - installing from the command line [17](#)
  - installing with Setup [13](#)

## N

- network driver, restarting computer to load [13](#)

## O

- On-Access Scanner
  - installing from the command line [17](#)
  - installing with Setup [13](#)
- On-Demand Scan feature
  - installing from the command line [17](#)
  - installing with Setup [13](#)

## P

- post-installation tasks [23, 24](#)
- pre-installation information [10](#)
- pre-installation tasks [7](#)
- program files
  - reinstalling or repairing [28](#)
  - installing [13](#)
  - location of [24](#)

Program Maintenance feature  
  modifying installed features [28](#)  
  reinstalling or repairing [29](#)

## R

release notes, viewing [13](#)  
removal of program files [31](#)  
repository list, importing [13](#)  
requirements for installation [8](#)  
restart  
  after installation [13](#)  
  after removing program files [31, 32](#)  
  command-line options [17](#)  
Right-click Scan feature  
  installing from the command line [17](#)  
  installing with Setup [13](#)

## S

scanners, selecting features [13, 17](#)  
Script Scan feature  
  installing from the command line [17](#)  
  installing with Setup [13](#)  
security, user interface options [13](#)  
ServicePortal, finding product documentation [6](#)  
settings, preserving from previous version [10, 13](#)  
setup type, choosing Typical or Custom [13](#)  
Setup utility  
  installing the product [13](#)

Setup utility (*continued*)  
  modifying installed features [28](#)  
  reinstalling or repairing program files [29](#)  
  removing program files [31](#)  
silent installation  
  and reboot options [17](#)  
  command-line examples [19](#)  
  command-line options [16](#)  
Sitelist.xml, importing a repository list [13](#)  
Standard protection level, selecting [13](#)  
system requirements [8](#)

## T

tasks  
  pre-installation [7](#)  
  installation, Setup utility [13](#)  
  modifying installed features [28, 29](#)  
  post-installation, running a test scan [23, 24](#)  
  reinstalling or repairing program files [29](#)  
  removing program files [31, 32](#)  
test file, verifying the installation [23, 24](#)  
Typical installation, selecting a type [13](#)

## U

user interface, selecting security options [13, 16](#)

## V

version requirements, ePolicy Orchestrator [20](#)