

VirusScan Enterprise

VERSION 7.0

Beta 1 — Draft 2



COPYRIGHT

© 2002 Networks Associates Technology, 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 Networks Associates Technology, Inc., or its suppliers or affiliate companies. To obtain this permission, write to the attention of the Network Associates legal department at: 3965 Freedom Circle, Santa Clara, California 95054, or call +1-972-308-9960.

TRADEMARK ATTRIBUTIONS

Active Firewall, Active Security, Active Security (in Katakana), ActiveHelp, ActiveShield, AntiVirus Anyware and design, Bomb Shelter, Certified Network Expert, Clean-Up, CleanUp Wizard, CNX, CNX Certification Certified Network Expert and design, Design (stylized N), Disk Minder, Distributed Sniffer System, Distributed Sniffer System (in Katakana), Dr Solomon's, Dr Solomon's label, Enterprise SecureCast, Enterprise SecureCast (in Katakana), Event Orchestrator, EZ SetUp, First Aid, ForceField, GMT, GroupShield, GroupShield (in Katakana), Guard Dog, HelpDesk, HomeGuard, Hunter, LANGuru, LANGuru (in Katakana), M and design, Magic Solutions, Magic Solutions (in Katakana), Magic University, MagicSpy, MagicTree, McAfee, McAfee (in Katakana), McAfee and design, McAfee.com, MultiMedia Cloaking, Net Tools, Net Tools (in Katakana), NetCrypto, NetScan, NetShield, NetStalker, Network Associates, NetXray, NotesGuard, Nuts & Bolts, Oil Change, PC Medic, PCNotary, PGP, PGP (Pretty Good Privacy), Pretty Good Privacy, PrimeSupport, Recoverkey, Recoverkey – International, Registry Wizard, ReportMagic, Router PM, Safe & Sound, SalesMagic, SecureCast, Service Level Manager, ServiceMagic, SmartDesk, Sniffer, Sniffer (in Hangul), Stalker, SupportMagic, TIS, TMEG, Total Network Security, Total Network Visibility, Total Network Visibility (in Katakana), Total Service Desk, Total Virus Defense, Trusted Mail, UnInstaller, Virex, Virus Forum, ViruScan, VirusScan, WebScan, WebShield, WebShield (in Katakana), WebSniffer, WebStalker, WebWall, Who's Watching Your Network, WinGauge, Your E-Business Defender, ZAC 2000, Zip Manager are registered trademarks of Network Associates, Inc. and/or its affiliates in the US and/or other countries. All other registered and unregistered trademarks in this document are the sole property of their respective owners.

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 NETWORK ASSOCIATES OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Contents

Preface	3
Audience	3
Getting more information	4
Contacting McAfee and Network Associates	6
1 Installing the VirusScan Enterprise software	7
Before you begin	7
System requirements	8
Server requirements	8
Workstation requirements	9
Installing the VirusScan Enterprise program files	10
Start the Setup utility	10
Activate the license	12
Start the installation	14
Typical Installation	16
Custom Installation	18
Performing a custom installation on a local computer	18
Installing on a Cluster Server	27
System requirements	27
Creating virtual servers	28
Publishing a VirusScan Enterprise service in Active Directory	29
Command Line Installation	30
Installing silently	31
Logging the installation	32
Installing to a custom directory	33
Selecting specific features to install	33
Setting reboot options	35
Setting security type for Windows NT	35
Removing incompatible software	35
Scanning your system at startup	35
Starting the VShield scanner	36
Preserving on access settings	36

Running Setup from a login script	36
Testing your installation	37
Modifying the VirusScan Enterprise program files	38
Start the Setup utility	38
Modify program features	40
Reinstall or repair program files	42
2 Removing the VirusScan Enterprise software	45
Using the Setup utility to remove the program files	45
Using the command line options to remove the program files	48

Preface

This Installation Guide introduces McAfee VirusScan® Enterprise software version 7.0, and provides the following information:

- *System requirements on page 8.*
- *Installing the VirusScan Enterprise software on page 7.*
- *Testing your installation on page 37.*
- *Modifying the VirusScan Enterprise program files on page 38.*
- *Removing the VirusScan Enterprise software on page 45.*

Audience

This information is intended primarily for:

- Network administrators who are responsible for the company's anti-virus program.

Getting more information

Product Guide	<p>Product introduction and features, detailed instructions for configuring the software, information on deployment, recurring tasks, and operating procedures.</p> <p>Available in an Adobe Acrobat .PDF file from either the product CD or the McAfee download site.</p>
Installation Guide	<p>System requirements and instructions for installing and starting the software.</p> <p>Available as a printed booklet that accompanies the product CD. Also available in an Adobe Acrobat .PDF file from either the product CD or the McAfee download site.</p>
Help	<p>Product information in the Help system that is accessed from within the application.</p> <ul style="list-style-type: none">■ The Help system provides high-level and detailed information. Access from either a Help menu option or Help button in the application.■ Context-sensitive (<i>What's This?</i>) Help provides brief descriptions of the selections in the application. Access by right-clicking on an option, pressing the [F1] control key, or clicking the question icon, then clicking on the option you want help on.
Configuration Guide	<p><i>For use with ePolicy Orchestrator.</i> Procedures for installing, configuring, deploying, and managing your McAfee product through ePolicy Orchestrator management software.</p> <p>Available in an Adobe Acrobat .PDF file from either the product CD or the McAfee download site.</p>

Release Notes

README file. Product information, system requirements, resolved issues, any known issues, and last-minute additions or changes to the product or its documentation.

Available as a .TXT file from either the product CD or the McAfee download site.

Contact

A list of phone numbers, street addresses, web addresses, and fax numbers for Network Associates offices in the United States and around the world. Also provides contact information for services and resources, including:

- Technical Support
- Customer Service
- Download Support
- AVERT Anti-Virus Research Site
- McAfee Beta Site
- On-Site Training
- Network Associates Offices Worldwide

Contacting McAfee and Network Associates

Technical Support <http://knowledge.nai.com>

McAfee Beta Site www.mcafeeb2b.com/beta/

AVERT Anti-Virus
Research Site www.mcafeeb2b.com/naicommon/avert/default.asp

Download Site www.mcafeeb2b.com/naicommon/download/

DAT File Updates www.mcafeeb2b.com/naicommon/download/dats/find.asp

Product Upgrades www.mcafeeb2b.com/naicommon/download/upgrade/login.asp

Valid grant number required.
Contact Network Associates Customer Service.

On-Site Training www.mcafeeb2b.com/services/mcafee-training/default.asp

Network Associates Customer Service:

E-mail services_corporate_division@nai.com

Web www.nai.com

www.mcafeeb2b.com

US, Canada, and Latin America toll-free:

Phone +1-888-VIRUS NO or +1-888-847-8766

Monday – Friday, 8 a.m. – 8 p.m., Central Time

For additional information on contacting Network Associates and McAfee — including toll-free numbers for other geographic areas — see the Contact file that accompanies this product release.

Installing the VirusScan Enterprise software

1

The VirusScan Enterprise 7.0 software supports both servers and workstations. It is a replacement for both the VirusScan version 4.5.1 software for workstations and the NetShield NT version 4.5 software for servers.

Before you begin

McAfee distributes VirusScan Enterprise software in two ways:

- as an archive file that you can download from the Web
- on a product CD

To install VirusScan Enterprise, you must have Administrator privileges for the computer where you plan to install the program.

If you are upgrading from a previous version of the VirusScan or NetShield software, you can remove the previous version, then load the replacement version. You have the option of preserving settings from the previous version installed.

Review the system requirements to verify that the program can run on your system, then follow the installation steps that start on [page 10](#).

System requirements

Ensure that your computer meets the following system requirements before you start the installation process.

Server requirements

The VirusScan Enterprise software installs and runs on a local or remote server equipped with:

- An Intel processor or compatible architecture. McAfee recommends an Intel Pentium processor or Celeron running a minimum of 166MHz.
- A CD-ROM drive. If you downloaded the software, this is an optional item.
- Any of the following Microsoft Windows platforms:
 - ◆ Windows NT 4.0 Server, Service Pack 4, Service Pack 5, Service Pack 6 / Service Pack 6a
 - ◆ Windows NT 4.0 Enterprise Server, SP4, SP5, SP6/SP6a
 - ◆ Windows 2000 Server, SP1, SP2, SP3
 - ◆ Windows 2000 Advanced Server, SP1, SP2, SP3
 - ◆ Windows 2000 DataCenter Server, SP1, SP2, SP3
 - ◆ Windows .NET Server 2003, Standard Edition
 - ◆ Windows .NET Server 2003, Enterprise Edition
 - ◆ Windows .NET Server 2003, Web Edition
- Microsoft Internet Explorer, version 4.0 or later, if you intend to use the program's AutoUpdate and AutoUpgrade features.
- Adequate hard disk space as follows:
 - ◆ **12MB** — If you perform a complete installation of all the program's features and modules, it occupies about 12MB of disk space on your local server.
 - ◆ **20MB** — The installation process uses an additional 20MB of temporary disk space, which is freed when the installation is complete.

Workstation requirements

The VirusScan Enterprise software installs and runs on a workstation equipped with:

- An Intel processor or compatible architecture. McAfee recommends an Intel Pentium processor or Celeron running a minimum of 166MHz.
- A CD-ROM drive. If you downloaded the software, this is an optional item.
- Any of the following Microsoft Windows platforms:
 - ◆ Windows NT 4.0, SP4, SP5, SP6a
 - ◆ Windows 2000 Professional, SP1, SP2, SP3
 - ◆ Windows XP Home Professional SP1
- Microsoft Internet Explorer, version 4.0 or later, if you intend to use the program's AutoUpdate and AutoUpgrade features.
- Adequate hard disk space as follows:
 - ◆ **12MB** — If you perform a complete installation of all the program's features and modules, it occupies about 12MB of disk space on your local server.
 - ◆ **20MB** — The installation process uses an additional 20MB of temporary disk space, which is freed when the installation is complete.

Installing the VirusScan Enterprise program files

You can install the VirusScan Enterprise program files on either a server or workstation.

The installer distinguishes between the server and workstation by setting the registry key to **McAfee VirusScan Enterprise Server** or **McAfee VirusScan Enterprise Workstation** respectively.

There are several methods of installing the software. You can use any of the following methods:

- The Setup utility that comes with the VirusScan Enterprise software.
- The Command line. See [Command Line Installation on page 30](#).
- McAfee Installation Designer can be used to create a customized installation package and configure product settings. See the McAfee Installation Designer Product Guide for detailed instructions.

Review the [System requirements](#) starting on [page 8](#) before you begin the installation process.

Start the Setup utility

Select the computer that you plan to use to install the program, then proceed as follows:

- 1 Open the **Setup** window using one of the following methods:

If your copy of the software is on the product CD:

- a Insert that CD into the CD-Rom drive.
- b Click **Install** from the **Welcome** window.

or

If you downloaded the software:

- a Create a temporary folder on your hard drive.
- b Use a decompression utility, such as WinZip, to extract the files you downloaded to this folder.
- c Select **Run** from the **Start** menu in the Windows taskbar. The **Run** dialog box appears.

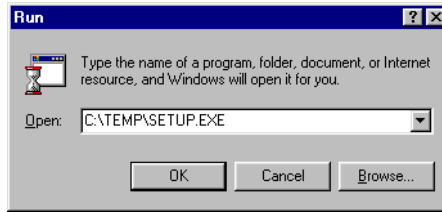


Figure 1-1. Run

- d Type <X>:\SETUP.EXE in the text box, then click **OK**.

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.

The **Setup** window appears.

- 2 Review the product information, then click **Next** to open the **Network Associates Licensing** window.

Activate the license

Network Associates provides 3 types of licenses:

Evaluation copy — The customer can install the product and it is fully functional until the end of the evaluation period.

Subscription license — The customer is entitled to use the product for the license term.

Perpetual license — The customer is entitled to use the product indefinitely.

NOTE

You must enter a *license key* to activate your license. The license key is an alphanumeric string that contains the license details. In most cases, the license key is automatically generated and distributed to the customer along with their grant number.

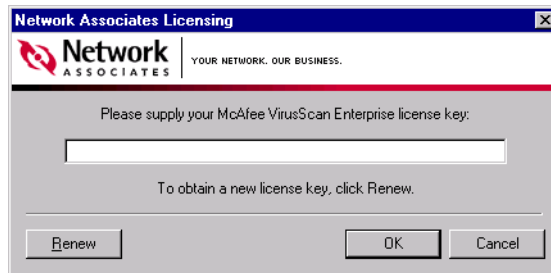


Figure 1-2. License Key

The **Network Associates Licensing** window provides a text box in which you can enter your license key.

- 1 Enter the license key using one of these options:
 - ◆ **If you have a license key:** Enter your license key in the text box.
 - ◆ **If you don't yet have a license key:** Click **Renew** to access the Network Associates web site, where you can renew your product online and obtain a license key. Next, enter the license key in the text box.

NOTE

If you leave the text box for the license key blank, your unregistered software installation is treated like an evaluation copy, which you can use until the evaluation period expires.

- 2 Click **OK** to open the **End User License Agreement**.

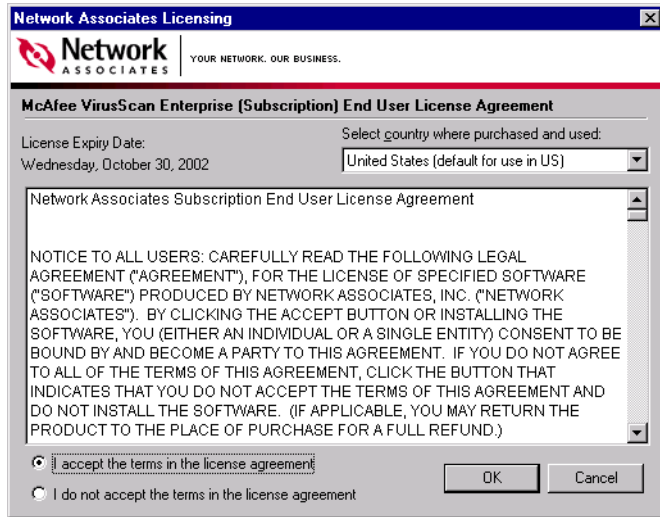


Figure 1-3. License Agreement

- 3 In the **Select country where purchased and used** text box, click  to select the country.

NOTE

If you entered an evaluation license key or left the license key blank in [Step 1](#), the **Select country where purchased and used** text box is not available.

- 4 Read the license agreement carefully, then select one of these options:
 - ♦ If you *agree* to the license terms, select **I accept the terms of the license agreement**.
 - or
 - ♦ If you *do not agree* to the terms, select **I do not accept the terms of the license agreement**.
- 5 Click **OK** to continue.

NOTE

If you do not accept the terms of the license you will not be able to continue with the product installation.

Start the installation

After you have selected a license type and accepted the terms of the license, follow these steps to continue the installation.

- If you are installing VirusScan Enterprise software over a previous version of NetShield or VirusScan software, the **Preserve Settings** window appears. Go to [Step 1](#)
- If this is a first time installation of the product (if Setup does not detect a previously installed version of either NetShield or VirusScan), go to [Step 2](#).

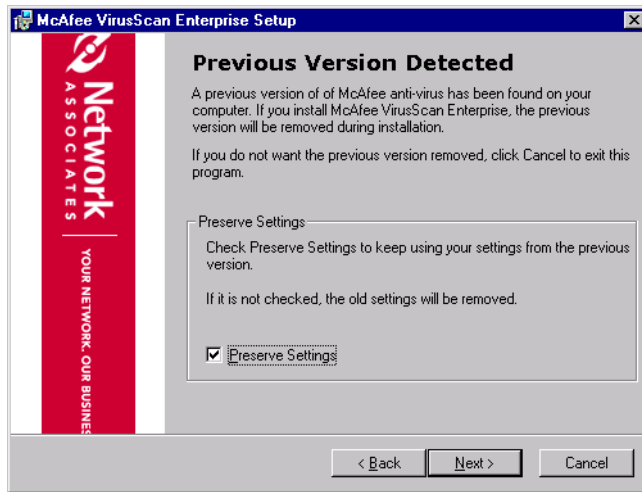


Figure 1-4. Preserve Settings

WARNING

If you do not select the **Preserve Settings** option, the old settings are removed.

- 1 Select the **Preserve Settings** option if you want to continue using the settings from the previous version of the McAfee anti-virus software, then click **Next** to continue.

The **McAfee VirusScan Enterprise Setup** window appears.

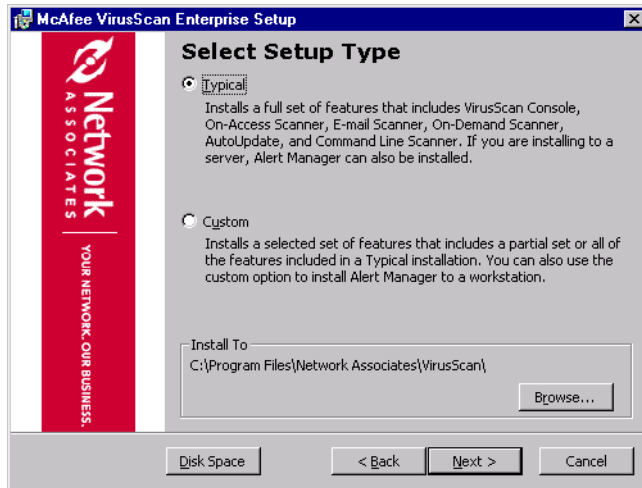


Figure 1-5. Setup Type

2 You have two Setup Type choices:

- ◆ **Typical.** Select this option to install the client and server software, together with all utilities. A typical installation provides the functionality to perform virus scanning, updating of virus definition files, and sending of alert messages. McAfee recommends this installation for most environments. See [Typical Installation on page 16](#).

WARNING

Typical installation does not give you the capability of customizing your site list or setting a user interface password. You must use Custom installation if you want to customize these features.

- ◆ **Custom.** Select this option to choose the specific features you want to install. You can also use the custom installation to customize your auto configuration file, setup a user interface password, and install the alerting function as a cluster resource. See [Custom Installation on page 18](#).

Typical Installation

Complete [Steps 1 to 2](#) in *Start the Setup utility*, then continue as follows:

- 1 Select **Typical** in the **McAfee VirusScan Enterprise Setup** window.
- 2 Select the installation path. By default, Setup installs the VirusScan Enterprise program files in this path:

C:\Program Files\Network Associates\VirusScan

Accept the default path or click **Browse** to select another path.

NOTE

Click **Disk Space** to view the disk space requirements, then click **OK** to return to the **McAfee VirusScan Enterprise Setup** window.

- 3 Click **Next** to continue.

The **Ready to install** window appears.

NOTE

Click **Back** to review or change any of the settings, then return to the **Ready to install** window and click **Install**.

If you are satisfied with all of the installation settings you selected, click **Install** to begin the installation process.

- 4 Review the installation details in the **McAfee Common Framework Installation** window, then click **OK** to continue the installation process.
- 5 When the setup has completed successfully, select the update options you want. You can **Update Now** and/or **Run On-Demand Scan** upon completion of installation.

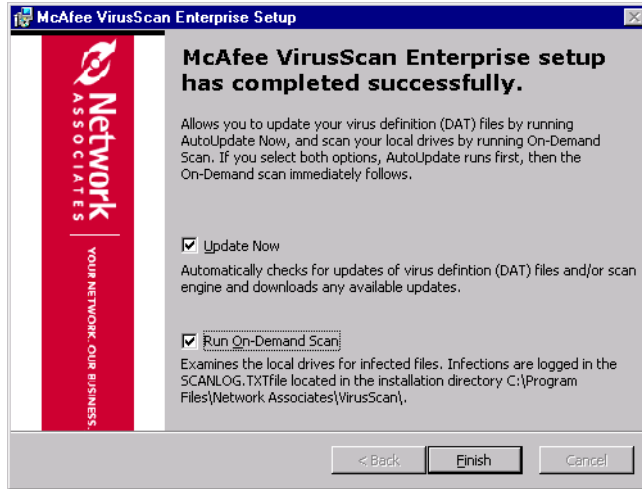


Figure 1-6. Setup completed successfully — Update and scan options

- 6 Click **Finish** to continue.

NOTE

Depending on the options you selected above, the program may run auto-update or an on-demand scan at this time.

- 7 You must reboot your machine before VirusScan Enterprise Setup can continue. Click **Yes** if you would like to reboot now.

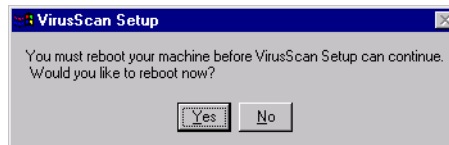


Figure 1-7. Reboot your machine

NOTE

To start the AntiVirus Console, select **Programs** from the **Start** menu. Next, select **VirusScan** then **VirusScan Console**.

Custom Installation

You can use the custom installation to select specific features for installation.

Performing a custom installation on a local computer

Complete [Steps 1 to 2](#) in *Start the Setup utility*, then continue as follows:

- 1 Select **Custom** in the **McAfee VirusScan Enterprise Setup** window.
- 2 Select the installation path. By default, Setup installs the VirusScan Enterprise program files in this path:

C:\Program Files\Network Associates\VirusScan

Accept the default path or click **Browse** to select another path.

NOTE

Click **Disk Space** to view the disk space requirements, then click **OK** to return to the **McAfee VirusScan Enterprise Setup** window.

- 3 Click **Next** to continue.

The **Feature Selection** window appears.

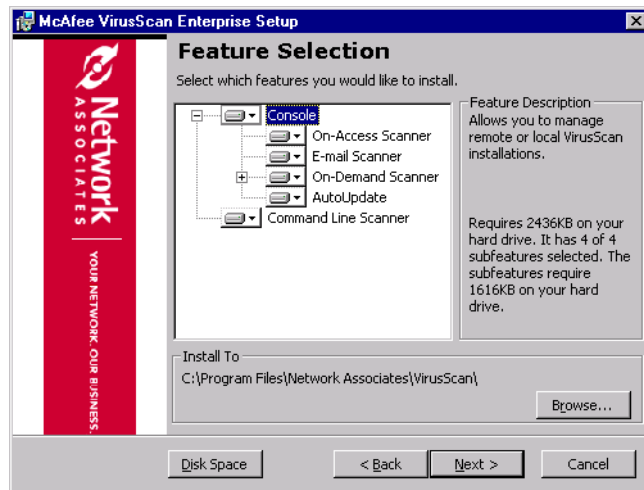



Figure 1-8. Feature Selection

- 4 Select the features you want to install. When you select a feature, a brief description of its function appears. Click  next to the feature you want to install, to display the action options available for that feature.

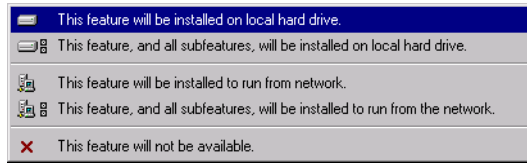


Figure 1-9. Feature action options

You have these action options:

- ◆ **This feature will be installed on local hard drive.** Select this option if you want to install the selected program component on the current server. This action is available for all features.
 - ◆ **This feature, and all subfeatures, will be installed on local hard drive.** If you select the icon adjacent to Console, then select this option to install all of the components that are subordinate to Console. For example, On-Access Scanner, On-Demand Scanner, and AutoUpdate. This action is available for all features.
 - ◆ **This feature will be installed to run from the network.** Select this option if you want to install the Command Line to run from the network. This action is available for Command Line installation only.
 - ◆ **This feature, and all subfeatures, will be installed to run from the network.** Select this option if you want to install the Command Line and all components that are subordinate to the Command Line to run from the network. This action is available for Command Line installation only.
 - ◆ **This feature will not be available.** Select this option if you do not want to install the selected program component. This action is available for all features.
- 5 After selecting the features you want to install, select the installation path. Accept the default or click **Browse** to select a new installation path.
 - 6 Click **Next** to continue.

NOTE

If Setup detects that you are installing the VirusScan Enterprise software on a Cluster Server, and that you included Alert Manager as an installed service on your custom installation, the **Alert Manager Cluster Installation** window appears.

You have the option of installing Alert Manager as a cluster service, allowing it to take advantage of the fault-tolerance features of clustering technology. See *Installing on a Cluster Server* on page 27 for additional information. For information about Alert Manager, refer to the VirusScan Enterprise Product Guide.

Reviewers — This screen capture to be replaced.



Figure 1-10. Alert Manager Cluster Installation

- 7 If you are not installing the VirusScan Enterprise software on a Cluster Server go to [Step 15 on page 23](#).

or

If you want Alert Manager to be a clustered resource, select the **Install Alert Manager as a Cluster Resource** option.

WARNING

To use Alert Manager as a cluster resource, the VirusScan Enterprise software, including Alert Manager must be installed on both server nodes that make up the cluster. For information on configuring Alert Manager, refer to the VirusScan Enterprise Product Guide.

- 8 In the boxes provided, enter a *static IP Address* and a **Subnet Mask** for the McAfee virtual server. You cannot use Dynamic Host Configuration Protocol (DHCP) to dynamically allocate an IP address to the virtual server.

- 9 Enter a name for the McAfee virtual server for Alert Manager. This must be a valid NetBIOS name, containing no more than 14 characters. By default, the name of the virtual server is ALERTMGR.

NOTE

If you do not accept ALRTMGR as the name of the virtual server, and have substituted another name that exceeds fourteen characters, or is otherwise incorrect, you will be unable to bring the service online.

You will be asked to provide this information only while installing the VirusScan Enterprise software to the first of the two server nodes. Setup stores this information for use during installation to the second node.

The **IP address**, **Subnet Mask**, and **Virtual Server Name** boxes will be filled in with the information you provided while configuring the first node. However, during installation to the second node, you have the option of activating Alert Manager immediately. To do so, select the **Bring the Alert Manager Server Online** option.

- 10 When finished with the Alert Manager Cluster Installation panel, click **Next**. If you are installing the VirusScan Enterprise program on a Windows 2000 Server with Active Directory installed, the **Alert Manager Active Directory** panel appears. For additional information, see [Publishing a VirusScan Enterprise service in Active Directory on page 29](#).

Reviewers — This screen capture to be replaced.



Figure 1-11. Alert Manager Active Directory

- 11 Select the **Publish Alert Manager in the Active Directory** option if you want the Alert Manager included in the current installation to appear in Active Directory. Any McAfee anti-virus product that has access to Active Directory can select the published listing and be routed automatically to this copy of Alert Manager.

NOTE

If you want to publish the Alert Manager that you installed as a cluster resource, select the **Publish Alert Manager in the Active Directory** option only while installing the software on the first node in the cluster. Do not select this option when installing the software on the second node.

- 12 Enter a unique name for the Alert Manager to distinguish it from other Alert Managers that you may install on other servers.
- 13 Select the **Set as the Default Alert Manager** option if you want this copy of Alert Manager to serve as the default copy.

WARNING

You can designate only one Alert Manager as the default in an Active Directory tree. To change the default, you must uninstall the VirusScan Enterprise program and reinstall it, designating a different default Alert Manager.

If you enter a name that is already in use in the current Active Directory tree, or if you set a second Alert Manager as default, the second Alert Manager will not appear in Active Directory.

- 14 Click **Next** to continue.

The **Product Configuration** window appears.

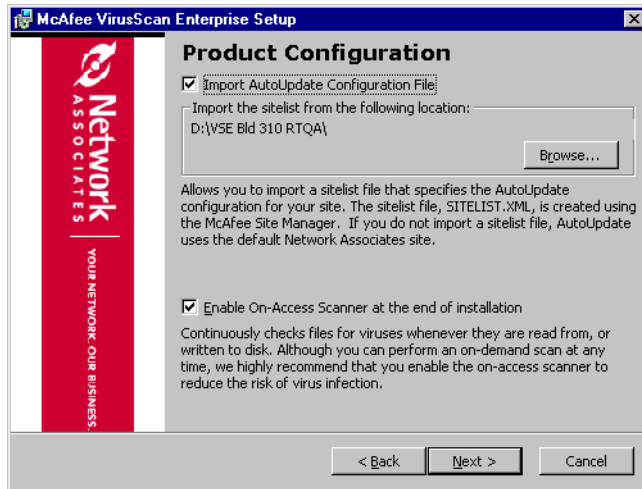


Figure 1-12. Product Configuration

- 15 Select the **Import AutoUpdate Configuration File** option if you want to import a sitelist file that specifies the AutoUpdate configuration for your site.

NOTE

The **AutoUpdate Configuration File**, also referred to as sitelist, is required to perform updating of Virus Definition (DAT) files or the engine. If you do not import a sitelist, AutoUpdate uses the default Network Associates site.

If you select this option, also select the directory where your SITELIST.XML file is located. Accept the default site or click **Browse** to select a new location.

- 16 Click **Next** to continue.

The **Install Alert Manager** window appears.



Figure 1-13. Install Alert Manager

- 17 Select **Install Alert Manager Server** if you want to install the Alert Manager Server after this installation process completes. If you select this option the Alert Manager files must be in the directory shown. Click **Browse** to select a different location.
- 18 Click **Next** to continue.

The **Security Configuration** window appears.

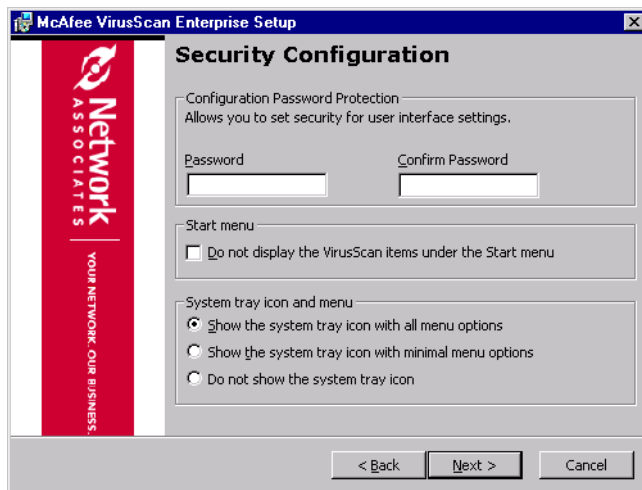


Figure 1-14. Security Configuration

You can set a user interface password and determine what the parts of the product the user can see.

- a Enter and confirm the user interface password if you want to place password security on the interface.
 - b Select the user interface options for the **Start Menu**
 - c Select the user interface options for the **System tray icon**.
- 19 Click **Next** to continue.

The **Ready to install** window appears.

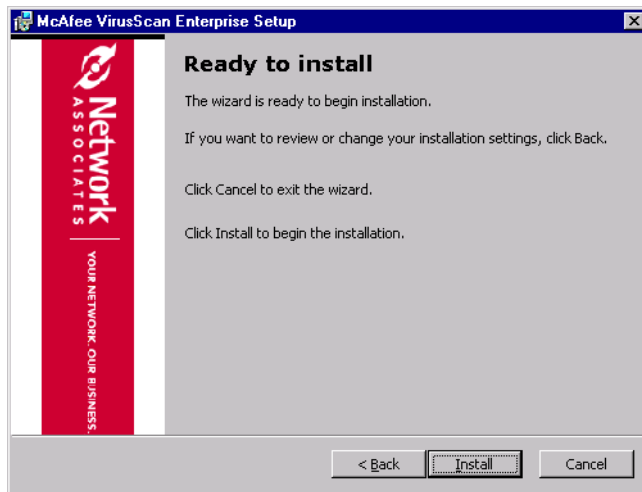


Figure 1-15. Ready to install

NOTE

Click **Back** to review or change any of the settings, then return to the **Ready to install** window and click **Install**.

If you are satisfied with all of the installation settings you selected, click **Install** to begin the installation process.

- 20 Review the installation details in the **McAfee Common Framework Installation** window, then click **OK** to continue the installation process.
- 21 When the setup has completed successfully, select the update options you want. You can **Update Now** and/or **Run On-Demand Scan** upon completion of installation.



Figure 1-16. Setup completed successfully — Update and scan options

- d Click **Finish** to continue.

NOTE

Depending on the options you selected above, the program may run auto-update or an on-demand scan at this time.

- e You must reboot your machine before VirusScan Enterprise Setup can continue. Click **Yes** if you would like to reboot now.

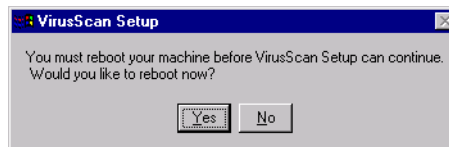


Figure 1-17. Reboot your machine

NOTE

To start the AntiVirus Console, select **Programs** from the **Start** menu. Next, select **VirusScan** then **VirusScan Console**.

Installing on a Cluster Server

The Alert Manager component of the VirusScan Enterprise software can run as a cluster resource on a Microsoft Cluster Server (MSCS). As a cluster service, Alert Manager takes advantage of the fault-tolerance provided by clustering technology. By creating a virtual server to host Alert Manager, messaging services can continue functioning even if the currently-running server goes down.

System requirements

This section provides an overview of the requirements for MSCS. See Microsoft's documentation for details.

MSCS requires:

- ◆ two servers, each with its own system disk.
- ◆ a dedicated network connection on each server. Consequently, each server requires two Network Interface Cards (NIC)—one connected to the network and one connected directly to the other server in the cluster.
- ◆ a shared SCSI disk, that both servers are properly configured to access.
- ◆ Windows NT Server, Enterprise Edition in Windows NT 4.0 environments,

or

Windows 2000 Server.

In addition, the VirusScan Enterprise software must be installed on both servers.

Creating virtual servers

When you install Windows NT Server, Enterprise Edition, MCSC creates a virtual server that can be used for general cluster administration, including administration of the virtual servers that host clustered resources, such as McAfee Alert Manager, Sequel Server, or MS Exchange.

WARNING

It is possible for a virtual server to host multiple resources. However, if one of those resources fails, then all of the resources on that virtual server will go down as well.

When you install the software, Setup creates a virtual server consisting of:

- ◆ a group named **NETWORK ASSOCIATES**.
- ◆ an IP address resource, called **NAI IP ADDRESS**. This resource must include a static IP address and a subnet mask, which you will be asked to provide during Setup.
- ◆ a network name resource. This is the name of the virtual server on which Alert Manager resides. When you configure the on-access and on-demand scanning tasks to notify Alert Manager when a virus is detected, you will be required to provide this name.
- ◆ a generic service resource called **ALERT MANAGER**. This is the McAfee Alert Manager service.

When Setup is complete, the administrative virtual server that was created by MSCS displays the McAfee Alert Manager virtual server tree.

McAfee recommends that you bear in mind the following additional considerations.

- ◆ Although the VirusScan Enterprise program supports use of Alert Manager as a cluster resource, it does not require this arrangement. The benefit you derive from the fault-protection that a cluster server provides may be outweighed by other factors.
- ◆ The default installation of Alert Manager as cluster resource on a Cluster Server requires you to create a network name resource for the Virtual Server on which Alert Manager resides.
- ◆ Any McAfee application running on the nodes in the cluster server, such as the VirusScan Enterprise anti-virus program, will be unable to detect a local Alert Manager. These applications must be configured to use the Virtual Alert Manager located on the cluster.

Publishing a VirusScan Enterprise service in Active Directory

The Alert Manager component of the VirusScan Enterprise software can publish its existence as an object in Active Directory on servers that are running Windows 2000. If you install multiple Alert Managers on your network, you can publish the existence of each one as an object in Active Directory. Because the object contains all the information required to connect to Alert Manager, the user does not need to know the Alert Manager's current location on the network in order to relocate it, administer it, or make it accessible to the scanner for distribution of alert messages.

Electing to publish Alert Manager in Active Directory takes place during a custom installation of the VirusScan Enterprise software (see [Step 11 on page 22](#) for details). If you did not perform a custom installation, or if you did not include publication of Alert Manager in Active Directory, but now want to do so, you must remove the VirusScan Enterprise software and reinstall it. Similarly, if, after publishing a particular Alert Manager in Server A, you now wish to substitute the Alert Manager located on Server B as the published service, you must:

- a** remove the Alert Manager module from Server A.
- b** reinstall the Alert Manager module on Server A, if desired, but do not specify that you want to publish Alert Manager in Active Directory.
- c** install the VirusScan Enterprise software on Server B, and specify that you want to publish Alert Manager in Active Directory.

Depending on the options you selected above, the program may run auto-update or an on-demand scan at this time.

Command Line Installation

The VirusScan Setup utility runs as a Microsoft Installer (MSI) application, which allows a wide array of custom installation options. Running the Setup utility from the command line allows you to shape the installation so that it runs the way you want and installs exactly the product components you want.

NOTE

You can run Setup from the command line to install the VirusScan Enterprise software to only a local computer. If you want to use the command line to install the software over a network, you must use ePolicy Orchestrator. Refer to the VirusScan Enterprise Configuration Guide for information about how to use ePolicy Orchestrator to install the program files.

- 1 Click **Start** in the Windows taskbar, then choose **Run**.
- 2 Enter the command line you want to use in the Run dialog box, then click **OK**.

The Setup command-line syntax looks like this:

```
setup PROPERTY=VALUE[,VALUE] [/option] /i
```

This syntax does not require any particular order in its elements, except that you may not separate a property and its value, and you must terminate the line with the `/i` option so that Setup knows to look for a particular .MSI file it needs for installation. The syntax consists of:

- ◆ the name of the executable file: `setup.exe`.
- ◆ any options you choose to add, each preceded by a `/` character. Options are *not* case sensitive. The installation scenarios that appear later in this guide discuss some of the available options.
- ◆ any properties you want to use to shape how the installation runs.

Each property consists of a name, which must appear all in capitals, an `=` sign, and one or more values, each separated by commas. Most property values must appear in all capitals, too, but some—such as `True` and `False`, must appear in capitals and lower case. The Microsoft Installer permits a large variety of properties, all of which you can use to determine how your installation runs. To learn about those properties, see the Microsoft Installer documentation. To install VirusScan Enterprise software, specifically, you can use these additional properties:

- ◆ `ADDLOCAL`. This property tells Setup to install particular components to the local computer.
- ◆ `INSTALLDIR`. This property specifies which installation directory you want to use. The value consists of the directory path you want to use.

- ◆ PRESERVESETTINGS. This property tells Setup whether it should retain the configuration options you used for previous VShield scanner installations. By default, its value is True.
- ◆ REBOOT. This property tells Setup whether it should restart your computer. You can either force the computer to restart, or prevent it from restarting.
- ◆ REMOVE. This property tells Setup to remove one or more program components. You can specify a particular component, or use the value ALL to remove all components. If you combine this property with the ADDLOCAL property, you can install all but one or two specific components.
- ◆ REMOVEINCOMPATIBLESOFTWARE. This property tells Setup to remove previous VirusScan versions or other anti-virus software that could conflict with this VirusScan Enterprise version. By default, its value is True.
- ◆ STARTONACCESSSCANNER. This property tells Setup to start the VShield scanner after it finishes the installation. By default, its value is True.
- ◆ USEADMINONLYSECURITY. This property tells Setup which security mode you want this VirusScan Enterprise copy to use when it runs. Possible values are 0, which runs the software with standard security, and 1, which runs the software with maximum security.

The following sections describe some common scenarios that use command-line options to run custom installations.

Installing silently

- Use command-line options to set up VirusScan Enterprise software on each network node with little or no interaction from end users. During a silent installation, Setup does not display any of its usual wizard panels or windows, or offer the end user any configuration options. Instead, you pre-configure these choices and run Setup in the background on each target workstation. If you want, you can install VirusScan Enterprise software on any unattended workstation with or without the end user's knowledge, provided you have all the necessary administrative privileges.

setup/q/i

- Use /q to run a silent installation. The /i should always appear last on the command line. It tells Setup to locate the .MSI file that controls the installation.
- Other semi-silent installation methods are:

/qb	shows a small progress bar during installation, with a cancel button
/q+	shows a success/failure installation complete dialog box
/qb+	shows both the progress and completed dialog boxes
/qf	shows the full progress bar screen from the regular installation

Logging the installation

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

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

Installing to a custom directory

To install VirusScan Enterprise software to a custom directory, add the `INSTALLDIR` property to the command line, then follow the property with a value for the directory you want to use. To install VirusScan Enterprise software to `C:\My Anti-Virus Software`, for example, type this line at the command prompt:

```
setup INSTALLDIR= "c:\My Anti-Virus Software" /q/i
```

Use quotes only if the target directory name has spaces. You can add the `/q` switch run the installation silently, if you prefer. The `/i` switch is not optional—Setup needs it to locate the `.MSI` file that has current installation data.

Selecting specific features to install

When you run Setup from the command line to install specific program components, the utility installs those components according to a preexisting hierarchy. This means that if you choose to install only the VirusScan Enterprise shell extensions, for example, Setup knows that you must have `SCAN32.EXE`, the VirusScan Enterprise application, installed in order to use the extensions. It therefore installs both this file and any related files.

To specify the components you want to install, Setup requires you to add particular component names as command-line parameters. The component names you can specify from the command line are:

Table 1-1.

Component Name	Description
AlertManager	The Alert Manager Client configuration utility
CMD	The VirusScan Enterprise Command Line scanners: <code>SCAN.EXE</code> , <code>SCANPM.EXE</code> , <code>SCAN86.EXE</code>
EdiskUtil	The Emergency Disk wizard and archived files
EmailScan	The VShield E-Mail Scan module and the E-Mail Scan extension
InternetScan	The VShield Download Scan and Internet Filter modules
SystemScan	The VShield System Scan module
Scan32	The VirusScan Enterprise application, <code>SCAN32.EXE</code>
Scheduler	The VirusScan Enterprise Console
McUpdate	The AutoUpdate and AutoUpgrade utilities
ShellExtensions	Extensions that add right-click functionality that enables you to scan individual files

Table 1-1.

Component Name	Description
ScreenScan	The ScreenScan utility
SendVirus	An applet that allows you to send virus samples to AVERT Labs for analysis

- To use these component names in a command line, specify the destination and the component name, exactly as it appears in the table.

For example, to add the VirusScan Enterprise application to the local system, type this line at the command prompt:

```
setup.exe ADDLOCAL=Scan32/q/i
```

- Use a comma to separate values in order to install more than one component. To add Scan32 and SystemScan together, for example, type this line at the command prompt:

```
setup.exe ADDLOCAL=SystemScan,Scan32/q/i
```

- To do a complete installation, type this line at the command prompt:

```
setup.exe ADDLOCAL=ALL/q/i
```

- To remove all VirusScan Enterprise components, type this line at the command prompt:

```
setup.exe REMOVE=ALL/q/i
```

- To install all components except for one—the SendVirus component, in this example—type this line at the command prompt:

```
setup.exe ADDLOCAL=ALL REMOVE=SendVirus/q/i
```

- You can also choose different components for an installation that you do not run silently. If, for example, you leave off the /q option in any of the command line examples shown above, the Custom Setup wizard panel (see [Custom Installation on page 18](#)) will show only the components you specify as those available for installation. If you use these same examples to specify a component set for installation, Setup installs only the components you specified during a Typical installation.

Setting reboot options

You can force or prevent the target computer from restarting during the installation. To do this, add the REBOOT property to the command line. REBOOT=F forces the restart, while REBOOT=R prevents the restart. If you must first install the Windows Installer service on a target computer, Setup requires you to restart whether you force or prevent a restart for other reasons. Setup resumes after MSI forces a restart. It then uses the options you set to determine whether to force or prevent a restart after the installation.

```
setup REBOOT=R /q /i
```

This example runs a silent installation and prevents a system restart.

Setting security type for Windows NT

If you install VirusScan Enterprise software on Windows NT Workstation v4.0 or Windows 2000 Professional systems, you can choose to run the software with regular or maximum security. To set this value from the command line, run Setup with the USEADMINONLYSECURITY property and the value you want to use.

- To run the software with standard security, give the property the value 0:

```
USEADMINONLYSECURITY=0
```

- To run the software with maximum security, give the property the value 1:

```
USEADMINONLYSECURITY=1
```

- To use the property from the command line, type a line similar to this:

```
setup USEADMINONLYSECURITY=1 /q /i
```

This runs a silent installation and sets the security level so that only a user with administrative rights can configure or stop the product.

Removing incompatible software

By default, Setup removes incompatible software during a silent installation. To prevent Setup from removing incompatible software, add the property REMOVEINCOMPATIBLESOFTWARE to the command line with the value False:

```
setup REMOVEINCOMPATIBLESOFTWARE=False
```

Scanning your system at startup

By default, Setup adds a line to the AUTOEXEC.BAT file that tells the VirusScan Enterprise application to scan the master boot record (MBR) when your computer starts. To prevent Setup from doing so—during a silent installation, for example—add the property SCANATSTARTUP to the command line with the value False:

```
setup SCANATSTARTUP=False
```

Starting the VShield scanner

By default, Setup starts the VShield System Scan module if the installation does not require you to restart your computer—if you remove earlier VirusScan versions during installation, for example. To keep Setup from starting the VShield scanner, add the STARTONACCESSSCANNER property to the command line with the value False:

```
setup STARTONACCESSSCANNER=False
```

Preserving on access settings

By default, Setup preserves your VShield settings from previous VirusScan installations. To install the new VirusScan Enterprise version without previous settings, add the PRESERVESETTINGS property to the command line with the value False:

```
setup PRESERVESETTINGS = False
```

Running Setup from a login script

To install VirusScan Enterprise software at the time each of your target computers starts, you can add a Setup command line to your login script and include any logic you think necessary to ensure that the installation runs once—checking for the VirusScan Enterprise default program directory, for example. The command line should include all of the options and properties you want to use to govern how Setup runs.

- If you run the login script from a Windows 95 or Windows 98 workstation, you *must* add the option /LSCRIPT to the command line if the target computer has any previous VirusScan version installed, or if it might not have Microsoft Installer (MSI) v1.1 installed. Unlike other options, the /LSCRIPT option is case sensitive and must appear in the command line with all capitals.
- Without the /LSCRIPT option, Setup will run and, if you do not have MSI v1.1 installed or if you have a previous VirusScan version on the target computer, it requires the target computer to restart. Before it does so, however, it places a flag in the Windows RunOnce registry key.
- Because Windows 95 and Windows 98 execute the login script at the same time they act on the contents of the RunOnce key, however, they will try to run another instance of Setup while, at the same time, they try to resume the previous Setup you started. MSI does not permit more than one instance of Setup to run at the same time.
- Adding the /LSCRIPT option to the command line causes Setup to place a flag in the RunServicesOnce registry key, which Windows executes before it runs the login script. If your login script checks for the presence of the default VirusScan program directory before it runs Setup, therefore, Windows will not try to run Setup a second time.

- In order to use a login script for this purpose, you must also copy or “push” the VirusScan Enterprise installation package to a local directory on the target computer. You may *not* use a login script to install VirusScan Enterprise software from elsewhere on your network. To install VirusScan Enterprise software from a remote location on the network, use McAfee ePolicy Orchestrator management software.

NOTE

If you plan to install VirusScan Enterprise software to a Windows NT Workstation v4.0 or a Windows 2000 system via login scripts, you do not need to include the /LSCRIPT option in your command line. Testing your installation

Testing your installation

Once installed, the software can scan your system for infected files. You can test whether it is installed correctly and can properly scan for viruses by implementing a test developed by the European Institute for Computer Anti-Virus Research (EICAR), a coalition of anti-virus vendors, as a method for their customers to test any anti-virus software installation.

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 carriage returns*:


```
X50!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 will be 69 or 70 bytes. Make a note of the directory in which you saved the file.
- 3 Start the program.
 - ◆ To test the on-demand scanner, create an on-demand scan task that examines the directory where you saved EICAR.COM. See “Creating a task with the Scan Wizard” in the *VirusScan Enterprise Product Guide* for instructions. When the scanner examines this file, it reports finding the EICAR test file.
 - ◆ To test the on-access scanner, confirm that the on-access scanner is configured to scan files written to the server and files read from the server. See “Configuring the on-access task” in the *VirusScan Enterprise Product Guide* for additional information. Next, 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.

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.

Modifying the VirusScan Enterprise program files

You can use the Setup utility to modify, repair, or reinstall the VirusScan Enterprise program files.

Start the Setup utility

- 1 Select **Run** from the **Start** menu in the Windows taskbar. The **Run** dialog box appears.

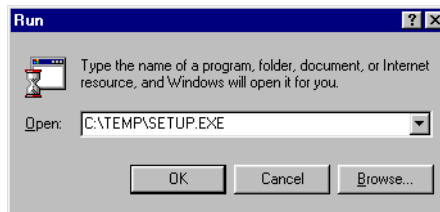


Figure 1-18. Run

- 2 Type <X>:\SETUP.EXE in the text box provided, then click **OK**.

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 Total Virus Defense CD, you must also specify which folder contains the VirusScan Enterprise software.

- 3 The **Setup** window appears.

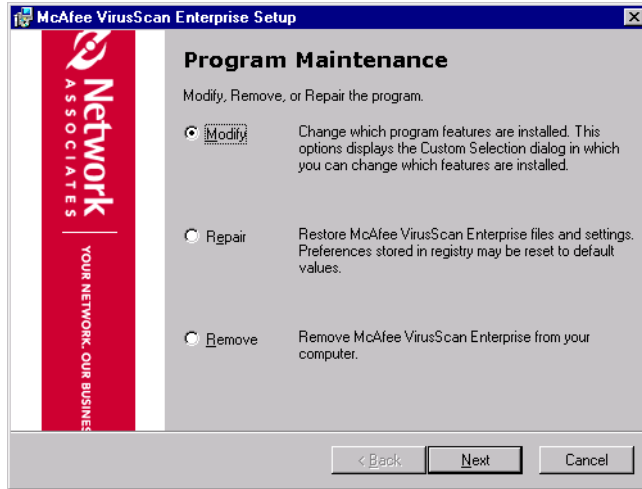


Figure 1-19. Program Maintenance

- 4 Select the program maintenance activity you want to perform. You can choose from the following options:
 - ◆ **Modify.** Select this option to change which program features are installed. This option uses the Custom Selection dialog to change the installed features.

Go to [Modify program features on page 40](#) to complete the modification process.
 - ◆ **Repair.** Select this option to reinstall or repair the program files.

Go to [Reinstall or repair program files on page 42](#) to complete the reinstall or repair process.

Modify program features

- 1 Select **Modify** in the **McAfee VirusScan Enterprise Setup** window, then click **Next**.

The **Feature Selection** window appears.

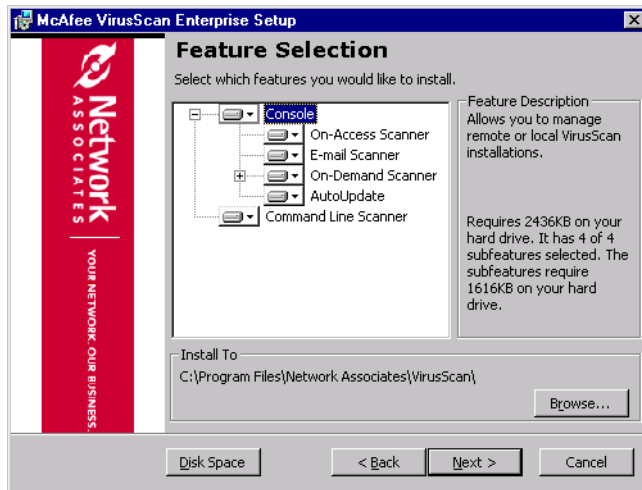


Figure 1-20. Feature Selection

- 2 Select the features you want to install. When you select a feature, a brief description of its function appears. Click next to the feature you want to install, to display the action options available for that feature.

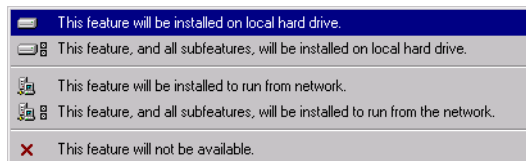


Figure 1-21. Feature action options

You have these action options:

- ◆ **This feature will be installed on local hard drive.** Select this option if you want to install the selected program component on the current server. This action is available for all features.

- ◆ **This feature, and all subfeatures, will be installed on local hard drive.** If you select the icon adjacent to Console, then select this option to install all of the components that are subordinate to Console. For example, On-Access Scanner, On-Demand Scanner, and AutoUpdate. This action is available for all features.
 - ◆ **This feature will be installed to run from the network.** Select this option if you want to install the Command Line to run from the network. This action is available for Command Line installation only.
 - ◆ **This feature, and all subfeatures, will be installed to run from the network.** Select this option if you want to install the Command Line and all components that are subordinate to the Command Line to run from the network. This action is available for Command Line installation only.
 - ◆ **This feature will not be available.** Select this option if you do not want to install the selected program component. This action is available for all features.
- 3 After selecting the features you want to install, select the installation path. Accept the default or click **Browse** to select a new installation path.
 - 4 Click **Next** to continue.

The **Product Configuration** window appears.

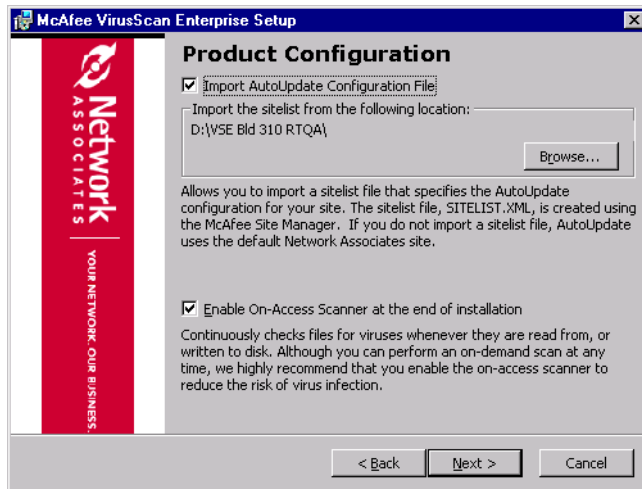


Figure 1-22. Product Configuration

- 5 Select the **Import AutoUpdate Configuration File** option if you want to import a sitelist file that specifies the AutoUpdate configuration for your site.

NOTE

The **AutoUpdate Configuration File**, also referred to as sitelist, is required to perform updating of Virus Definition (DAT) files or the engine. If you do not import a sitelist, AutoUpdate uses the default Network Associates site.

If you select this option, also select the directory where your SITELIST.XML file is located. Accept the default site or click **Browse** to select a new location.

- 6 Click **Next** to continue.

The **Ready to install** window appears.

NOTE

Click **Back** to review or change any of the settings, then return to the **Ready to install** window and click **Install**.

If you are satisfied with all of the installation settings you selected, click **Install** to begin the installation process.

- 7 When the setup has completed successfully, click **Finish**.

Reinstall or repair program files

- 1 Select **Repair** in the **McAfee VirusScan Enterprise Setup** window, then click **Next**.

The **Reinstall or Repair the Product** window appears.



Figure 1-23. Reinstall or repair the product

- 2 Select the maintenance options you want, then click **Install**.

- 3 When the setup has completed successfully, click **Finish**.

Removing the VirusScan Enterprise software

2

You can use the Setup utility or the command line to remove the VirusScan Enterprise program files.

You can also remove the program files using the Add/Remove Programs utility that is included in the Windows Control Panel.

Using the Setup utility to remove the program files

- 1 Open the **Setup** window using one of the following methods:

If your copy of the software is on the product CD:

- a Insert that CD into the CD-Rom drive.
- b Click **Install** from the **Welcome** window.

or

If you downloaded the software:

- a Create a temporary folder on your hard drive.
- b Use a decompression utility, such as WinZip, to extract the files you downloaded to this folder.
- c Select **Run** from the **Start** menu in the Windows taskbar. The **Run** dialog box appears.

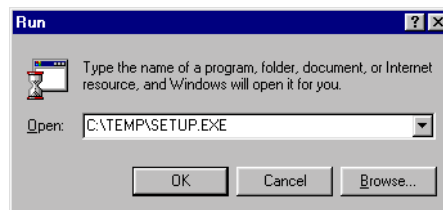


Figure 2-1. Run

- d Type `<X>:\SETUP.EXE` in the text box, then click **OK**.

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.

The **Setup** window appears.

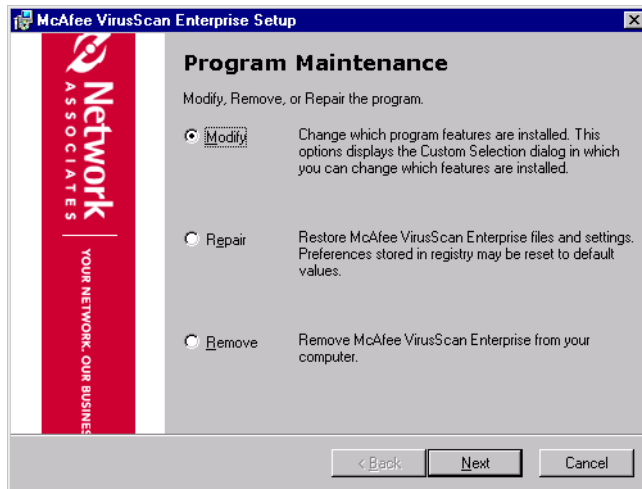


Figure 2-2. Program Maintenance

- 2 Select **Remove** in the **Setup** window, then click **Next**.

The **Remove McAfee VirusScan Enterprise** window appears.



Figure 2-3. Remove McAfee VirusScan Enterprise

- 3 Click **Remove** to start the removal process.
- 4 When the setup completes successfully, click **Finish**.

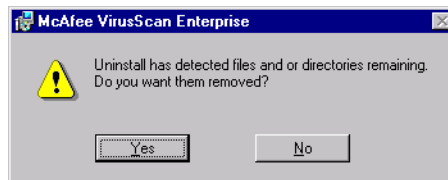


Figure 2-4. Remove remaining files

- 5 Click **Yes** to remove the remaining files, or click **No** if you do not want to remove the remaining files.

Reviewers — A note will be added defining what files are remaining.

Using the command line options to remove the program files

- 1 Open the Windows command-line module.
 - a Select **Command Prompt** from the **Start** menu.
or
 - b Select **Run** from the **Start** menu.
- 2 Type the following at the command prompt or dialog box:

```
<installpath>\setup -s -x
```