User's Guide

VirusScan for Windows NT

McAfee, Inc.
2710 Walsh Avenue
Santa Clara, CA 95051-0963

Phone: (408) 988-3832
Monday - Friday
6:00 am - 5:00 pm

FAX: (408) 970-9727
BBS: (408) 988-4004

(For international contact information, see the following page.)

TRADEMARK NOTICES

McAfee is a registered trademark of McAfee, Inc. SiteMeter, SiteExpress, ServerStor, and NetRemote are trademarks of McAfee, Inc. All other products or services mentioned in this document are identified by the trademarks or service marks of their respective companies or organizations.

"SABRE" is a trademark of American Airlines, Inc. and is licensed for use to Saber Software Corporation, a wholly owned subsidiary of McAfee. Saber Software is not affiliated with American Airlines, Inc. or SABRE Travel Information Network. All trademarks are the property of their respective owners.

FEEDBACK

A Reader's Comment Form is provided in the back of this publication. McAfee appreciates your comments and reserves the right to use any information you supply in any way it believes appropriate without incurring any obligations whatsoever. If the form has been removed, please address your comments to: McAfee, Inc., Documentation, P.O. Box 9088, Dallas, Texas 75209.

SUPPORT

For fast and accurate help, please have the following ready when you contact McAfee:

- Program name and version number
- Type and brand of your computer, hard drive, and any peripherals
- DOS type and version
- Network name, operating system, and version
- Contents of your AUTOEXEC.BAT, CONFIG.SYS, and system LOGIN script
- Specific steps to reproduce the problem.

INTERNATIONAL CONTACT INFORMATION

McAfee Canada
178 Main Street
Unionville, Ontario
Canada L3R 2G9
Voice: (905) 479-4189
Fax: (905) 479-4540

McAfee Europe B.V.
Orlyplein 81 - Busitel 1
1043 DS Amsterdam
The Netherlands
Voice: (0) 31 20 6815500
Fax: (0) 31 20 6810229

McAfee (UK) Ltd.
Hayley House, London Road
Bracknell, Berkshire
RG12 2TH United Kingdom
Voice: 44 1344 304730
Fax: 44 1344 306902

McAfee France S.A.
50 rue de Londres
75008 Paris
France
Voice: 33 1 44 908733
Fax: 33 1 45 227554

McAfee Deutschland GmbH
Weltenburger Strasse 70
81677 Munich
Germany
Voice: 49 89 92404214
Fax: 49 89 92404211

Issued August 1996

Table of Contents

1 About This Document

Who Should Read This Document

If you are responsible for keeping your Windows NT workstation free from computer viruses, you need to read this book. The tasks in this manual usually belong to the network administrator, but any workstation user with administrator rights to the workstation can perform these duties.

What's in This Book?

Besides this chapter, "About This Document," here's what you'll find in the VirusScan manual:

Chapter 2, "Installing VirusScan." provides a step-by-step procedure for installing VirusScan on your NT workstation.

Chapter 3, "Introducing VirusScan." Is an overview of VirusScan for NT, describing what VirusScan does and how it does it.

Chapter 4, "Setting Up Virus Scanning." Describes how to use VirusScan to set up scanning scenarios, called "tasks," that you can use to scan your NT workstation.

Chapter 5, "Scanning for Viruses." Describes how to scan your workstation using the tasks you set up in the previous chapter. This chapter also descibes how to view scan statistics as the scan is running and how to set up VirusScan's response to any viruses it finds.

Chapter 6, "What to Do When a Virus Is Found." Describes how to configure VirusScan's reactions to discovering viruses.

Chapter 7, "Viewing Scan Results." Tells how to view the run-time scan statistics.

Appendix A, "Using Auto Updating." Explains VirusScan's Auto Update feature, which you can use to obtain updated versions of VirusScan virus data files, patch files, and instructions on a scheduled basis.

Appendix B, "McAfee Support Services." Describes McAfee's various support packages, customer service programs, udpate packages, and training services.

Notations Used in This Book

Understanding Windows terms

As a Windows NT application, the VirusScan workstation console should be used with a mouse. The table below briefly defines several Windows terms regarding the use of the mouse and product windows.

Term	Description
Button 1	The selection or primary mouse button (usually the left button, but can be switched using the Control Panel).
Cancel	Choose Cancel to exit the current dialog box without saving any of the changes you made in the dialog box or without executing a command you chose in the dialog box.
Choose	Click the mouse button (or use a key combination) on an item to initiate an action. For example, “Choose the VirusScan icon” should be interpreted as a click on the VirusScan icon.
Click	Press the mouse button once. To click *on* an object, the mouse pointer must be on that object when you click.
Double-click	Press the mouse button twice in quick succession.
Icon	A graphic representation of an executable or function.
Point	Position the cursor on the screen to rest on the desired item.
Property Page	Windows *tab* metaphor that locates related information in a single dialog box and allows easy navigation from tab to tab.
Scroll	Use the scroll bars and buttons to move through a list of items.

Select	Mark an item by clicking on it or by highlighting it with either key combinations or the mouse. For example, “Select the Include Path option” should be interpreted as click or highlight the Include Path item.
Spin Control	Arrows that increase or decrease the value displayed in the accompanying text box.

✍ *NOTE: The remainder of this manual assumes that you are familiar with Windows NT. Refer to your Microsoft Windows NT documentation for information on the fundamental operating conventions of the Windows environment.*

How to Contact Us

To order or for more information about our products, we invite you to contact our Customer Service department at (408) 988-3832. Or you can contact us at the following address:

McAfee, Inc.
2710 Walsh Avenue
Santa Clara, CA 95051-0963
U.S.A

McAfee's customer and technical support

McAfee is famous for its dedication to customer satisfaction. McAfee's customer support, technical support, and product development departments provide real-time technical support and problem resolutions.

Use the following information to contact McAfee Technical Support.

Phone	(408) 988-3832
FAX	(408) 970-9727
Hours	6 a.m. to 5 p.m. PST
	Monday through Friday
McAfee BBS	(408) 988-4004
	1200 bps to 28,800 bps
	8 bits, no parity, 1 stop bit
	24 hours, 365 days a year
CompuServe	GO MCAFEE
Internet	support@mcafee.com
America On-line	MCAFEE
Microsoft Network (MSN)	GO MCAFEE

To speed the process of helping you use our products, please make note of the following before you call:

- Product name and version
- Computer name and model, and the name of any additional hardware
- Operating system and version
- Network name, operating system, and version
- Contents of your AUTOEXEC.BAT, CONFIG.SYS, and system LOGIN script
- Specific steps to reproduce the problem, if applicable
- The name of any viruses you have found
- Have your computer in front of you when you call.

McAfee training

For more information about scheduling on-site training for any McAfee product, call Customer Service at (800) 338-8754.

2 Installing VirusScan

Before You Start

Before you install VirusScan, be sure you are logged onto the Windows NT network with administrator access. Then review the basic requirements for installing and VirusScan. You need to have:

Installation require-ments

- A workstation running Windows NT version 3.51 or later.
- At least 1.5MB of free disk space to install the program files.
- Since VirusScan is an NT service, no additional memory is required to run the software.

Although VirusScan does not require much memory or hard disk space, the amount of system resources it uses varies. By specifying scanning priority for each task, you determine to what extent the program uses resources.

If you specify a high priority, it uses more resources and scans more quickly. If you specify a low priority, it scans more slowly, but frees up more resources for other crucial applications.

Performing the Installation

You must install SaberTools from a Windows 95 or NT workstation.

1. Start the installation.

   - Logon to your Windows NT workstation. You must have administrator access to the Windows NT system.

2. Do one of the following:

   - If you're installing from the CD or diskettes, insert the CD or the first diskette.

   - If you're installing from files downloaded from the BBS, decompress the zipped files into a directory on the network or your local drive.

3. Double-click the SETUP.EXE program in File Manager or run one of the following commands from the Windows NT command line:

   - If you're installing from the CD or diskettes, enter the following:

     `x:\SETUP`

     where *x* is the drive that contains the CD or diskette.

   - If you're installing from files you downloaded from the McAfee Web site, enter the following:

     `x:\path\SETUP`

     where *x:path* is the drive and directory where you decompressed the files.

   Response: The VirusScan License Agreement screen is displayed. Read it carefully before proceeding with the installation.

4. Click OK to begin the installation.

   Response: The VirusScan Welcome Screen is displayed.

5. Click Next.

   - The Installer Rights screen is displayed. Read it carefully and make sure you have adequate rights to install VirusScan.
   - Click Next.

6. Select the destination directory for the VirusScan program files. Click Next.

7. Select the Windows Program Group folder where the VirusScan icons will be kept. Click Next.

8. Confirm that the settings are correct, and click Next

9. On the Service Account Information panel, click Next to specify the username and password for administrator access to this workstation's NT system. Click Next

   Response: VirusScan is installed.

After you finish installing, you can choose whether or not to view the VirusScan Readme file. This file contains important last-minute information about the product. It is strongly recommended that you click Yes to read it.

3 Introducing VirusScan

What is VirusScan?

McAfee's VirusScan for Windows NT is the superior anti-virus solution for Windows NT workstation. If you want to protect the files on your Windows NT servers, use McAfee's NetShield for Windows NT.

The VirusScan Console

The Console is the user interface from which you configure VirusScan's scanning and response to found viruses.

You can run the VirusScan Console on either a server or a workstation. If you install it on a server, you are actually scanning that server computer as if it were a workstation. We recommend McAfee's NetShield for Windows NT to protect your server.

How Does VirusScan Scanning Work?

VirusScan offers two methods of scanning: **on-access scanning** to prevent infected files from being copied from and/or to your workstation; and **scheduled scanning** to schedule automatic scanning on specific days and times. If VirusScan detects infected files, it can **delete**, **move**, **deny access** to, **clean**, or **ignore** the files, or **prompt you for action**. The possible actions depend on whether the task is an on-access task or a scheduled task.

For more information about scanning options and infected file actions, refer to "Setting Up Virus Scanning" on page 23.

What types of files does VirusScan scan?

Viruses usually infect executable files, so by default VirusScan scans mostly executable files. However, you can specify any files extensions you want.

The file extensions that VirusScan scans by default are:

- .EXE
- .COM
- .DO?

The DO? extension causes VirusScan to scan all files whose extension begins with DO, such as .DOC files and .DOT files.

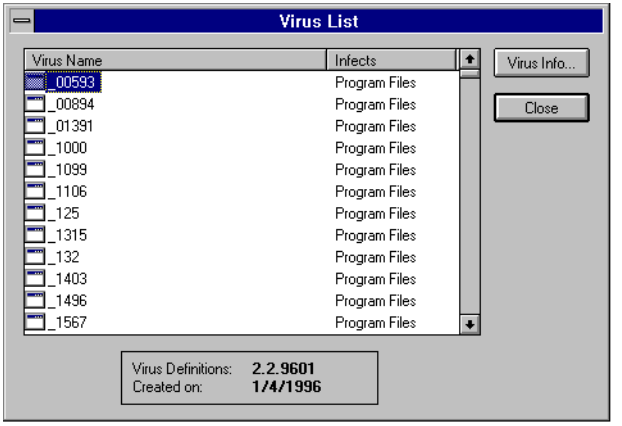
Viewing the virus list

VirusScan uses a virus list, which contains all of the known viruses that VirusScan detects. VirusScan's virus list is viewable, and you can look at the characteristics of each virus. This list is updated when you update your software's virus data files.

To view the VirusScan virus list follow the procedure below.

1. From the VirusScan Console, select **Tools/Virus List**, or Click the  button on the toolbar.

Response: The Virus List is displayed, showing all the viruses VirusScan detects and what types of files each virus infects.



2. Select a virus by clicking once on it, then click the Virus Info button to view specific information about that virus.

   Response: The Virus Information box is displayed. It shows the name of the virus and some of its characteristics.

3. Do one of the following:

   - To look at virus information for the next virus in the list, click Next.
   - To look at information for the previous virus, click Previous.
   - Click Close to return to the virus list.

How are viruses found?

VirusScan is an advanced anti-virus solution designed to protect your Windows NT workstation from viral infection. Employing McAfee's patented Code Trace© and Code Matrix© virus scanning technologies, VirusScan consistently and accurately identifies both known viruses and new viruses, including file, multi-partite, stealth, mutating, polymorphic and encrypted types. VirusScan uses the following methods to detect these viruses:

- Known viruses are detected by searching files for known characteristics (sequences of code) unique to each computer virus and reporting their presence if found. For viruses that encrypt or cipher their codes so that every infection is different, VirusScan uses detection algorithms that work by statistical analysis, heuristics, and code disassembly.

- Strains of known viruses are detected by searching for “generic” or “family” virus strings that have been found repeatedly in different viruses. Since virus writers may use older code or programming techniques when writing new viruses, VirusScan can use these strings to detect viruses that are not yet known.

What are tasks?

A task is an item listed in the Console window that represents predefined scan properties (options). To perform a virus scan, you must select a task. Using a task automates the process of specifying the particular options for running a scan.

VirusScan comes with a default task that is automatically displayed on the Console. It is called VShield NT (although you can change that name), and you can use it to perform on-access scanning. Likewise, you can create tasks to schedule the scanning operation, but you cannot create a new on-access task.

All tasks can be modified. Only scheduled tasks can be created or deleted.

What happens when a virus is found?

If VirusScan discovers infected files on your computer you can specify what actions it takes. You can define the following actions:

- Alerting—This includes various ways of notifying users.

- Virus logging—Scan results can be written to a log file to provide an infection trail for future audits.

- Event logging—This is Windows NT’s Event Log. You can have VirusScan add entries to this log. See your Windows NT documentation for more information about the Event Log.

- Infected file disposal—VirusScan can delete infected files, clean them, or move them to a quarantine directory.

Alerting

In VirusScan alerting, you can configure any of the following:

- Whom to send network messages to
- A VirusScan Console to forward network messages to
- Automatic program execution
- Pager alerts
- Email alerts
- Printer alerts
- SNMP support

Virus logging

VirusScan produces a log of virus activity, called the Activity Log. You can specify the name of the log file to use, and you can specify what types of virus activity are logged in the file. For example, you can include deleted files in the virus log, and not show the files that were cleaned.

For more information on the Activity Log, see "Creating the VirusScan Activity Log" on page 59

Event logging

You can log VirusScan events in the Windows NT Event Log. The Event Log contains a list of events logged by the Windows NT system, events logged by applications, and events that have been selected for auditing in User Manager, File Manager, or Print Manager.

VirusScan events that are logged in the Windows NT Event Log include VirusScan system errors and warnings.

See your Windows NT documentation for more information about NT's Event Log.

Infected file actions

VirusScan can clean the infected files it finds. To clean an infected file is to remove the virus from that file, making the file once again usable.

VirusScan can also move the infect file to a quarantine directory, where there is restricted user access to prevent the spread of infection. Locating the files in this directory also allows you to consolidate cleaning.

Also, VirusScan can simply delete infected files.

Types of scanning

VirusScan offers two types of scanning:

- On-access scanning
- Scheduled scanning

These are described below.

What is on-access scanning?

Using on-access scanning, VirusScan scans the specified files anytime they are saved to or copied from the your computer. Unlike scheduled scanning, on-access scanning does not scan all files in the specified directories, but only those that are accessed.

On-access scanning can scan inbound files, outbound files, or both. The on-access scanning features are encapsulated in the VirusScan default task. This allows you to organize the logging, exclusions, and alerting to help identify where the virus originated and structure the administration logically to your workstation environment.

On-access scanning is either on or off. You cannot specify a schedule for the on-access task.

What is scheduled scanning?

Scheduled scanning allows you to set up a VirusScan task that contains a particular schedule for scanning the selected files. Unlike on-access scanning, this scans all the specified files, according to the schedule, but does not scan files as they are accessed.

4 Setting Up Virus Scanning

This chapter describes how to set up VirusScan to scan for viruses. VirusScan uses *tasks* to store settings for various scanning scenarios. These tasks allow you to set up different scanning configurations with different properties, and access each one when you want without having to redefine properties each time.

You can also copy and paste a task to simplify the creation of your scanning environment.

✍ *Many of the task-related procedures given in this chapter can be performed from a pop-up menu that you get by right-clicking on the task.*

Using the Scan Wizard for Scheduled Scanning

Most of this chapter deals with configuring VirusScan's many scanning features. It is recommended that you read the whole chapter, but the McAfee Scan Wizard offers you a quick, easy way to create a scheduled scanning task.

The Scan Wizard simplifies configuring a scanning task by walking you through the process and prompting you for information. This is different from Creating a new scanning task and configuring it step-by-step, because the Scan Wizard asks you simple questions and then configures the task for you.

To use the Scan Wizard, follow the procedure below.

Step	Action
1.	Select **Scan/Scan Wizard**, or click the  button.
2.	Follow the instructions on the Scan Wizard windows.
3.	To use the Scan Wizard to launch a one-time scan without saving a task to the Console, select 'Do not save this as a scan task' from the Wizard's last panel before finishing.

Using the VirusScan Console

The VirusScan Console is your user interface to the VirusScan scanning software. VirusScan performs its virus scanning based on the configurations you created in the Console. .

Starting the Console

Follow the procedure below to start the Console.

- From Windows NT Program Manager, open the McAfee VirusScan NT group and double-click on the VirusScan NT Console icon.

  Response: The VirusScan Console is displayed on your screen.

The main Console window contains these components:

- menu bar
- toolbar
- task display area
- status bar.

The menu bar

The menu bar contains the following menus and menu commands:

Scan menu	Edit menu	View menu	Tools menu	Help menu
New Task	Copy	Toolbar	Virus List	Help Topics
Scan Wizard	Paste	Statusbar	Auto Update	About VirusScan
Enable/ Disable/Start	Export	Refresh	Alerts	
Rename	Import	Options	Event Viewer	
Delete				
Statistics				
Activity log				
Properties				
Exit				

The toolbar

The toolbar contains the following buttons:

Tool	Description (Corresponding Menu/Command)
	Start the Scan Wizard (**Scan/Scan Wizard**).
	Create a new task (**Scan/New Task**).
	Edit a task's properties (**Scan/Properties**).
	Copy a task (**Edit/Copy**).
	Paste a task (**Edit/Paste**).
	Remove a task from the Console (**Edit/Delete**).

Tool	Description (Corresponding Menu/Command)
	Start a scheduled task (**Scan/Start** and **Scan/Enable**).
	Stop a scheduled task.(**Scan/Stop** and **Scan/Disable**)
	View the VirusScan virus list (**Tools/Virus list**).
	View the Windows NT Event Log (**Tools/Event Log**).

The status bar displays an explanation of each menu command when the cursor is on that menu command.

The task display area

The task display area, the main part of the Console windows, contains a list of all the tasks defined for this installation of VirusScan. The VirusScan default task is always shown at the top of the display area.

Other tasks appear as you create them. To create a task, see “Creating new tasks” on page 30.

If you double-click on a task, that task’s scan statistics are displayed. This is the same as selecting a task and then selecting **Scan/Statistics**.

The status bar

As you look at the menus on the Console and move from menu item to menu item, the status bar contains information about the currently highlighted menu item.

Refreshing the Console view

The Console shows all tasks currently defined for this installation of VirusScan. If any changes are made, such as adding a task, you must refresh the view so that the changes are shown in the Console window. However, you can set up the Console to automatically refesh the window at whatever interval you want by selecting **View/Options**.

To refresh the Console view at any time:

- Select **View/Refresh** or press F5.

  Response: The Console screen is updated to show any recent changes.

Getting help

To get Help on a specific object on the Console, click the ? button, and then click that object. Or use the right mouse button to click the object, and then click What's This? on the menu that appears.

To get general help on using VirusScan, Select **Help/Help Topics**.

Types of Tasks

Tasks are VirusScan's way of allowing you to set up many scanning configurations which you can start and stop without disturbing other scanning configurations or currently running tasks.

There are two types of tasks:

- On-access
- Scheduled

These types are described in the sections that follow.

The on-access (default) task

There is only one on-access task allowed in the Console, and that task is created during installation. It is the VirusScan default task, called McAfee VirusScan for Windows NT. This task performs all on-access scanning for VirusScan.

With on-access scanning, VirusScan scans files when they are accessed (opened or copied). You can specify which file types to scan and in what directories to scan.

For example, if you configure the on-access scanning task to scan all files on your C: drive that have .EXE extensions, all .EXE files on that drive are scanned for viruses whenever they are written to or copied from the drive.

✍ *See "Changing the On-Access Scan Configuration" on page 38 for information about the default task's scanning options.*

You cannot delete the default (on-access) task from the Console, nor can you copy it to make other on-access tasks. You can, however, change the specific configuration of the default task. You can also deactivate it so that on-access scanning does not occur. See "Changing the On-Access Scan Configuration" on page 38 for instructions on changing the default task properties.

Scheduled tasks

With scheduled scanning, you set the schedule and tell VirusScan which file types, drives, and directories to scan.

For example, if you configure a scheduled task to scan your C: drive once a month, on the 15th, and then start the task, VirusScan scans those directories on the 15th of each month until you stop the task.

Unlike the on-access task, you can create as many scheduled tasks as you want. Each of these tasks is configured to scan the drives and directories you want, according to a schedule you define when you configure each task.

You have complete control over scheduled scanning tasks; you can delete them, copy them to create other scheduled tasks, and configure each one to suit your needs.

Manipulating tasks on the Console

Creating new tasks

Any time you want to define a new scanning scenario, you can do so by creating a new VirusScan task.

To create a new task, follow the procedure below.

Step	Action
1.	Select **Scan/New Task** or click the  button on the toolbar. **Response**: The new task is displayed on the Console. It has the default name, “New VirusScan Task.” You can change this name by selecting the task and then selecting **Scan/Rename**.
2.	Configure the task’s scanning properties as described in “Setting Up a Scheduled Scan” on page 32.

An alternative to this process is to use the Scan Wizard. See “Using the Scan Wizard for Scheduled Scanning” on page 24.

Copying tasks

You can copy an existing VirusScan task and paste it on the Console to create a new task with the same scanning properties as the original. You can then edit the properties of the new task so that you'll have a unique task.

To copy a task, following the procedure below.

Step	Action
1.	Select the task you want to copy by clicking once on its name in the Console window.
2.	Select **Edit/Copy**, or click the  button.
	Response: The task is stored in the clipboard.
3.	Select **Edit/Paste**, or click the  button.
	Response: The new task is pasted into the clipboard.

See "Creating new tasks" on page 30 for a description of how to change a task's name. See "Setting Up a Scheduled Scan" on page 32 for a description of how to reconfigure the new task's properties.

Removing tasks from the Console

To remove a task from the Console, follow the procedure below.

Step	Action
1.	Select the task you want to copy by clicking once on its name in the Console window.
2.	Select **Edit/Delete** or click the  button.
	or
	You can press the DELETE key.
	Response: The task is deleted from the Console.

Setting Up a Scheduled Scan

This section describes how to configure a scheduled scanning task. Each procedure in this section is performed from the Scan Configuration dialog. To get to this dialog:

Step	Action
1.	Select a task by clicking once on its name in the Console. You can also perform this procedure when creating a new task using the Task Wizard. See "Using the Scan Wizard for Scheduled Scanning" on page 24.
2.	Select **Scan/Properties** or click the  button on the toolbar.

Specifying the files to scan

When you configure a scanning task, you tell VirusScan what to scan. Here's what you can specify:

- The devices to scan
- The directories to scan
- The types of files to scan (for example, .EXE files, .DLL files, etc.).

To specify what files VirusScan scans, follow the procedure below.

Step	Action
1.	Select the Detection tab. If this is an existing task that has previously been configured, the names of items that it scans are displayed.
2.	Click the Add button to add items to the list. Items include folders, files, and drives. All of these will be on drives attached to your workstation.

3. Select the type of item in the Item to Scan box, and type its name in the Description box. Click OK.

   Response: The item is added to the list, and the Detection property page reappears.

   You can do this as many times as you want until you have chosen all of the items you want to scan.

4. Do one of the following:

   - If you want to scan inside compressed files, select that checkbox.
   - If you want to scan the subfolders of all the items in this list, select that checkbox.

5. Select whether VirusScan scans all files or program files only.

   If you select program files only, you can define what file extensions apply to program files. Click the Program Files button to do so.

6. Click the Advanced button to specify advanced scanning settings:

   - Set the Scan Priority slider to determine how much of your system's resources you want the task to take. A lower the setting leaves more resources free for other applications but results in a slower scan.
   - Click the 'Skip Boot Record Scanning' checkbox to telll VirusScan not to scan your your disk's boot sector,.

7. Click OK to finish setting the task's priorities, or continue with the sections below to set other scanning options.

Specifying how VirusScan responds to viruses

When VirusScan finds a virus, it can perform many responses. VirusScan can:

- Send you, or another user, a message that a virus was found
- Forward messages to other users

- Execute a specified program when a virus event occurs
- Send an alert to a pager
- Send alerts via email
- Send an alert to a printer
- Clean the infect file or files
- Delete the infected files
- Deny access to the infected files
- Prompt you for more action
- Move the infected files to a quarantine directory.

VirusScan can also report virus activity using the activity log and the Windows NT Event Log. See “Specifying virus reporting options” on page 35.

To choose among the above options, use the Actions tab on the Scan Configuration dialog.

To configure a task’s virus response actions, follow the procedure below.

Step	Action
1.	Select the Actions tab from the Scan Configuration dialog.
2.	Click the arrow on the When a Virus is Found box to choose among the following options: ▪ Prompt for further action ▪ Continue scanning ▪ Clean the infected file ▪ Delete the infected file.
3.	If you want to sound an alert or display a message on the workstation running the Console, check the appropriate boxes. Enter the text of the message in the box provided.
4.	Click OK to accept the virus response configuration.

Specifying virus reporting options

In addition to sending you an alert message when it finds a virus, VirusScan can log virus information to the VirusScan activity log and to the Windows NT Event Log.

To specify VirusScan activity reporting options, follow the procedure below.

Step	Action
1.	Select the Reports tab from the Scan Configuration dialog.
2.	If you want to log virus activity in the activity log, click the Log To File checkbox and enter the path and name of the log file you want to use, or browse for the log file. When you select Browse to find a log file, you can select the Network button to specify another Windows NT computer. You can then update that computer's Event Log.
3.	If you want to limit the size of the log file, click the appropriate box and enter the maximum size, in kilobytes, in the place provided.
4.	Select the checkbox corresponding to each piece of information you want to include in the log file.
5.	Click OK to accept the virus reporting configuration.

Setting up the scanning schedule

All VirusScan tasks (except for the default task, which is for on-access scanning only) can be set to run according to a schedule that you specify. You can schedule a task to scan monthly, weekly, daily, or just once.

To set up the scanning schedule for a task:

Step	Action
1.	Select the Schedule tab.

- Select the Enable Schedule checkbox.
- Choose, from among the options provided, which type of schedule you want to apply to this scanning task. If you choose a daily schedule, click Which Days to specify on which days of the week to scan.
- Enter the specifics of the schedule, such as at what time to start or on what day of the month.

2. If you are finished configuring this task, click OK.

Specifying what to exclude from scanning

VirusScan scans the file types you choose, on the drives you choose, in the folders you choose. But you can exclude from scanning any files within the scanned area.

To exclude files from scanning, follow the procedure below.

Step	Action

1. Select the task from which you want to exclude files.

   Response: A list of *items* appears.

2. Click the Add button to add items to the list.

   Items include folders, files, and drives. All of these will be on drives attached to your workstation.

3. Enter the name of the file or folder to exlclude, or browse for it.

4. Specify whether to exclude the item's subfolders, and whether to exclude from file scanning or boot record scanning. Click OK

   Response: The item is added to the list, and the Exclusions property page reappears.

You can do this as many times as you want until you have chosen all of the items you want to exclude.

Changing the On-Access Scan Configuration

On-access scanning is the scanning of inbound or outbound (or both) files whenever they are accessed. If you select inbound files for scanning, any file that is written to the workstation is scanned for viruses. If you select outbound files for scanning, any file that is copied from the workstation is scanned.

Not necessarily all accessed files are scanned. Only those files with certain extensions are scanned. You can configure on-access scanning to scan the file types you want. The default file types are:

- .EXE
- .COM
- .DO?

Although you cannot delete or copy the VirusScan default task (which is the only on-access scanning task), you can customize it to suit your needs. You can change any of the following:

- What files to scan
- Whether VirusScan services are loaded at startup
- Whether VirusScan can be disabled
- How VirusScan responds when a virus is detected
- What not to scan.

Specifying the files to scan

To tell VirusScan what files to scan, follow the procedure below.

Step	Action
1.	Select the on-access scanning task by clicking once on the task called, “McAfee VirusScan NT” in the Console window.
2.	Select **Scan/Properties** or click the  button. The VirusScan Properties dialog is displayed.

3. Select the Detection tab.

4. Select the appropriate options on the Detection page:

   - Select the ‘Inbound Files’ checkbox, the ‘Outbound Files’ checkbox, or both. ‘Inbound Files’ scan all files being save to the workstation. ‘Outbound Files’ scans any files being copied from the workstation.

   - Select either the ‘All Files’ option or the Program Files Only option.

   - If you select ‘Program Files Only’, click the Program Files button to specify which file types to scan. For example, you can specify to scan only files that have .EXE extensions.

   - Select the ‘Compress Files’ checkbox if you want to scan inside compressed files such as .ZIP files.

   - Specify whether or not you want to load VirusScan at startup and whether or not VirusScan can be disabled from Windows NT Services by checking the appropriate checkboxes.

     If you specify that VirusScan cannot be disabled, then the on-access task cannot be disabled using the Scan/Disable command.

5. Click OK to finish setting the task’s priorities, or continue with the sections below to set other scanning options.

Specifying how VirusScan responds to viruses

When VirusScan finds a virus, it can perform many responses. VirusScan can:

- Send you, or another user, a message that a virus was found
- Forward messages to other users
- Execute a specified program when a virus event occurs
- Send an alert to a pager
- Send alerts via email
- Send an alert to a printer
- Clean the infect file or files

- Delete the infected files
- Deny access to the infected files
- Prompt you for more action
- Move the infected files to a quarantine directory.

To specify VirusScan's response when it finds a virus, follow the procedure below.

Step	Action

1. Select the task called, "McAfee VirusScan NT" in the Console window, and select **Scan/Properties**.

2. Select the Actions tab on the VirusScan Properties dialog.

3. Choose one of the following options:

   - Deny access to infected files and continue.

     If VirusScan finds a virus in a file, users are prevented from accessing that file.

   - Move infected files to a folder.

     If VirusScan finds an infected file, the file is moved to a quarantine directory. When you select this option, you are given an opportunity to specify the path of the quarantine directory.

   - Clean infected files automatically.

     If VirusScan finds an infected file, the file is cleaned without further intervention from you. The cleaning information is logged in the activity log if you have specified that information for inclusion. (See "Specifying how VirusScan responds to viruses" on page 33.)

   - Delete infected files automatically.

     If VirusScan finds an infected file, the file is deleted without further intervention from you. The deletion is logged in the activity log if you have specified that information for inclusion. (See "Specifying how VirusScan responds to viruses" on page 33.)

4. Click OK to save the on-access task's virus options.

5. Select Tools/Alerts

6. On the System Alerts tab:

   - Select 'Log event in application log' to include VirusScan virus events in the Windows NT Event Log. You can log these in the local computer's Event Log, or in another NT Computer's Event Log.

   - Select 'Execute program on event' to launch a program when VirusScan finds a virus. Specify the name of the program in the box provided, of click Browse to find it. You can run that program every time a virus is found, or only the first time by selecting the corresponding checkbox.

   - Select 'Send events to Alert Manager' to use VirusScan's Alert Manager. The next section, "Configuring the Alert Manager", describes how to confiugre the Alert Manager.

7. On the Messages tab:

   - Select each message you want to include by activating its check-box.

   - To edit the text of any message, click on that message and click the Edit button. You can edit the messages text and select the pri-ority for each messsage. Click OK.

8. Click OK to save the Alert list, or click Configure from the System Alerts tab to confgure the Alert Manager.

Configuring the Alert Manager

The Alert Manger allows you to specify the following:

- Pager alerts
- Printer alerts
- Email alerts

- Computers to forward alerts to
- SNMP configuration

To configure the Alert Manager:

Step	Action
1.	Select Configure from the Alert List.
2.	On the Pager tab: ▪ Click Add to set up one pager's properties. ▪ Enter the pager's type (alphanumeric or numeric), its phone number, its ID number, and its password in the spaces provided. ▪ Select whether to use a standard alert message or a custom message. ▪ Click Modem Settings to specify the type of modem to use. Click OK. ▪ Click Priority Level to specify whether the pager responds to low-, medium-, or high-priority alerts. Click OK. ▪ Click OK to save this pager's alert properties.
3.	On the Forward tab: ▪ Click Add to select computers to forward alerts to. ▪ Type in the name of the computer, or browse for it. ▪ Click Priority Level to specify whether this forwarding responds to low-, medium-, or high-priority alerts. Click OK. ▪ Click Test to send a test message to that computer. ▪ Click OK.

4. On the Printer tab:

   - Click Add to add the name of a printer to the Alert list.
   - Select a printer and click Remove to remove a printer's name from the list.
   - Select a printer and click Properties to re-specify the name of the printer or the priority level.
   - Click OK.

5. On the Network Message tab:

   - Click Add to select a computer to send messages to.
   - Enter the computer's name or browse for it.
   - Click Priority Level to specify whether the message is sent for low-medium- or high-priority alerts. Click OK.
   - Click Test to send a test message to that computer.
   - Click OK.
   - Select a computer from the list and click Remove to remove that computer's name from the list.
   - Select a computer from the list and click Properties to re-specify the name of the computer or its priority level.
   - Click OK.

6. On the SNMP tab, click Enable SNMP to send an alert to a third-party SNMP manager.

7. On the E-mail tab:

   - Click Add to select an email address and header information.

- Click SMTP Settings to specfiy mail server and account information. Click OK.
- Click Priority Level to specify whether the email is sent for low-medium- or high-priority alerts.
- Click Test to test the email setup.
- Click OK.
- Select an email receiver from the list and click Remove to remove it from the list.
- Select an email receiver from the list and click Properties to re-specify the this email receiver's setup.
- Click OK.

8. On the SNMP tab:
   - Select the 'Enable SNMP' checkbox if you want SNMP enabled.
   - If you enabled SNMP, click Configure SNMP to specify the network settings.
   - Click OK.
9. The summary tab displays all the alerts devices you have set up. Click OK to accept the configuration.

Specifying what to exclude from scanning

To exclude files from on-access scanning:

Step	Action
1.	If you do not already have the VirusScan Properties dialog open, select the task called, "McAfee VirusScan NT" in the Console window, and select **Scan/Properties**.

2. Select the Exclusions tab.

3. Click the Add button to add items to the list.

   Items include folders, files, and drives. All of these will be on drives attached to your workstation.

4. Enter the name of the file or folder to exlclude, or browse for it.

5. Specify whether to exclude the item's subfolders, and whether to exclude from file scanning or boot record scanning. Click OK

   Response: The item is added to the list, and the Exclusions property page reappears.

   You can do this as many times as you want until you have chosen all of the items you want to exclude.

5 Scanning for Viruses

This chapter describes how to run VirusScan tasks from the VirusScan console. See "Types of Tasks" on page 26 for an explanation of what a task is and how to create one.

To scan for viruses, you simply start, or enable, a task that you previously configured to do the type of scanning you want. See "Setting Up Virus Scanning" on page 20 for more information about configuring tasks.

There are two types of scanning in VirusScan: on-access scanning and scheduled scanning. These are described in the following sections.

✍ *Many of the task-related procedures given in this chapter can be performed from a pop-up menu that you get by right-clicking on the task.*

On-Access Scanning

VirusScan has only one on-access scanning task. It is the VirusScan default task. Anytime you want to perform on-access scanning of files on your workstation, configure this task to scan the types of files you want. See "Changing the On-Access Scan Configuration" on page 35 for more information on setting up the on-access task.

The name of the default task, when VirusScan is first installed, is McAfee VirusScan NT. But you can change the name to whatever you want. See "Changing the name of the default task" on page 49 for more information.

Enabling the default task

The VirusScan default task is enabled automatically when you install VirusScan, but if it is disabled, it remains disabled until it is restarted, even if you exit and restart the VirusScan Console.

You can prevent the default task from being disabled by deselecting the 'Users are allowed to disable VirusScan' checkbox in the Detections tab of the VirusScan Properties dialog.

To enable the VirusScan default task, follow the procedure below.

Step	Action
1.	Select the default task by clicking once on its name in the Console Window. The default task is always the first task on the task list.
2.	Select **Scan/Enable**. **Response**: The default task is restarted.

Disabling the default task

The VirusScan default task is enabled automatically when you install VirusScan. To disable it.

✍ *You can prevent the default task from being disabled by deselecting the 'Users are allowed to disable VirusScan' checkbox in the Detections tab of the VirusScan Properties dialog.*

To disable the default task, follow the procedure below.

Step	Action
1.	Select the default task by clicking once on its name in the Console Window.
2.	Select **Scan/Disable**. **Response**: The default task is disabled.

Changing the name of the default task

When VirusScan is installed, the default task is called McAfee VirusScan NT. You can change this name to anything you want, up to 27 characters. (You can use more than 27 characters, but if you do, the name overlaps other information on the Console.)

To change the name of the default task, follow the procedure below.

Step	Action
1.	Right-click on the default task. It's the first task listed in the Console. **Response**: A pop-up menu is displayed.
2.	Select **Rename** from the drop-down menu. **Response**: The name of the task is highlighted.

3. Type the new name you want. You can use the arrow keys and the HOME and END keys to edit the name.

Scheduled Scanning

To scan your workstation for viruses using VirusScan, you start predefined tasks. This section describes how to start and stop these tasks. "Setting Up Virus Scanning" on page 20 explains how to create them.

Choosing a Scheduled task

The VirusScan console displays all tasks that you have created on that console. To select a task, follow the procedure below.

1. If you do not already have the VirusScan Console running, start it now.
2. Select the task you want to run by clicking on it once.

   If the task you want is not visible, scroll down until it is visible.

✍ *For scheduled scanning, do not choose the default task, which is always the first task on the list. The default task is for on-access scanning only.*

Once you have selected a task, you can make sure it's the one you want by viewing its properties. To view a task's properties, follow the procedure below.

1. Select a task as shown above.
2. Select **Edit/Properties.**

Starting a scheduled task

Once you have configured the task to scan what and when you want, follow the procedure below.

Step	Action
1.	Select the task by clicking once on its name in the Console.
2.	Select **Scan/Start**, or click the  button.

Response: The task is activated, but it won't begin actual scanning until it is scheduled to do so.

✍ *The task must be started in order for its scheduled scans to take place.*

If the task is configured for a one time only scan, the task stops running when the scan is complete. If it is a regularly scheduled scan, the task keeps running, waiting for the next scheduled scan, until you either stop it or exit the Console. See "Stopping a scheduled task" on page 52 for instructions on disabling a task that is running.

Stopping a scheduled task

You can stop any task currently running in the VirusScan Console. To stop a scheduled scan, follow the procedure below.

Step	Action
1.	Select the task you want to halt by clicking once on its name in the Console.
2.	Click the  button on the toolbar.

Response: The task stops until you start it again. To restart it, see "Starting a scheduled task" on page 51.

6 What to Do When a Virus Is Found

You can set up VirusScan to respond to viruses in the following ways:

- Send you, or another user, a message that a virus was found
- Forward messages to other users
- Execute a specified program when a virus event occurs
- Send an alert to a pager
- Send alerts via email
- Send an alert to a printer
- Clean the infect file or files
- Delete the infected files
- Deny access to the infected files
- Move the infected files to a quarantine directory.

VirusScan can also report virus activity using the activity log and the Windows NT Event Log.

Some of the actions are set up on a task- by-task basis, using the Scan Configuration dialog. See "Setting Up a Scheduled Scan" on page 29 and "Changing the On-Access Scan Configuration" on page 35.

The rest of configured using the Alert List and the Alert Manager, which you access using the **Tools/Alerts** command. This chapter tells you how to set up the virus alerting the Alert List and Alert Manager.

✍ *Many of the task-related procedures given in this chapter can be performed from a pop-up menu that you get by right-clicking on a task name in the Console window.*

Deleting, Cleaning, and Moving Infected Files

When VirusScan finds a file that is infected with a computer virus, it can clean that file immediately, delete it, or move it to a quarantine directory for you to take care of later. You can also set it up to prompt you for further action.

Deleting infected files

You can configure a VirusScan task to delete any infected files as soon as it finds them.

To set up a task to delete infected files, follow the procedure below.

Step	Action
1.	Select the task you want to configure by clicking once on its name in the Console.
2.	Select **Scan/Properties**.
3.	Select the Actions tab on the Scan Configuration dialog.
4.	Select Delete Infected File from the drop list.
5.	Click OK.

Response: The task is now configured to delete any infected files it finds. The deleted files are logged in the Activity Log and are represented in the Scan Statistics dialog, which you can view by double-clicking on a scheduled task, and in the VirusScan Status dialog, which you can view by double-clicking on the deafult task.

Cleaning infected files

You can configure a VirusScan task to remove the viruses from any infected files as soon as it finds them.

To set up a task to clean infected files, follow the procedure below.

Step	Action

1. Select the task you want to configure by clicking once on its name in the Console.
2. Select **Scan/Properties**.
3. Select the Actions tab on the Scan Configuration dialog.
4. Select Clean Infected File from the drop list.
5. Click OK.

   Response: The task is now configured to remove the viruses from any infected files it finds, leaving the files intact. Any viruses found but not cleaned are logged in the Activity Log.

Moving infected files to a quarantine area

You can configure the VirusScan default (on-access) task to move any infected files it finds to a *quarantine directory*. You can designate any directory you want as a qarantine directory, including one on another computer.

The purpose of the quarantine directory is to isolate infected files to an inaccessible area.

To set up a task to move infected files to a quarantine directory, follow the procedure below.

Step	Action

1. Select the VirusScan default task by clicking once on its name in the Console.
2. Select **Scan/Properties**.
3. Select the Actions tab on the Scan Configuration dialog.
4. Select Move Infected Files to a Folder from the drop list.

Response: A text box labeled ‘Folder’ appears on the dialog.

5. Enter the path to the folder you want to use as a quarantine directory.

   You can also browse for the folder by clicking the Browse button and you can click the Network button to select another computer to receive the files.

6. Click OK to save these settings.

The task is now configured so that any infected files are moved to the quarantine folder you specified.

Denying access to infected files

You can configure the VirusScan default scanning task so that it denies user access to any infected files it finds.

With denied access, infected files cannot be copied, moved, or executed. Infected files can, however, be cleaned or deleted, as appropriate.

To set up the default task to deny access to infected files, follow the procedure below.

Step	Action

1. Select the VirusScan default task by clicking once on its name in the Console.

2. Select **Scan/Properties**.

3. Select the Actions tab on the Scan Configuration dialog.

4. Select Deny Access to Infected Files an Continue from the drop list.

5. Click OK.

   Response: The task is now configured to deny access to any infected files it finds. This option does not clean or delete the files.

Taking no action with infected files

You can configure a VirusScan task to log infected files into the VirusScan activity log without taking any other action on the files.

To set up a task to leave infected files alone, follow the procedure below.

Step	Action
1.	Select the task you want to configure by clicking once on its name in the Console.
2.	Select **Scan/Properties**.
3.	Select the Actions tab on the Scan Configuration dialog.
4.	Select Continue Scanning from the drop list.
5.	Click OK. **Response**: The task is now configured to leave alone any infected files it finds. The file is entered in the VirusScan activity log.

Choosing a virus response on the fly

You can configure a VirusScan task to prompt you for action each time it finds an infected file.

To set up a task to prompt you for action, follow the procedure below.

Step	Action
1.	Select the task you want to configure by clicking once on its name in the Console.
2.	Select **Scan/Properties**.
3.	Select the Actions tab on the Scan Configuration dialog.

4. Select Prompt for Action from the drop list.

5. Click OK.

Response: The task is now configured to prompt you for action. When VirusScan finds an infected file, it prompts you to decide whether the infected file is cleaned, deleted, or ignored.

Creating the VirusScan Activity Log

The VirusScan activity log contains the results of scanning tasks. The specific information it contains depends on what you decide to put into it. See "Specifying what to put in the activity log" on page 59 for a list of what you can include in the activity log and instructions for doing it.

You can specify a different activity log for each task, or use the same log for all tasks. You can name any file as the activity log, but it must be a text file

To name an activity log:

Step	Action

1. Select the task for which you are setting up virus reporting.
2. Select **Scan/Properties**.
3. Choose the Reports tab.
4. Do one of the following:
   - In the Log to File text box, enter the path and name of the file you want to use as a log file.

   or

   - Click Browse to find the file.
5. Select the types of information to put into the log file. See "Specifying what to put in the activity log" on page 59 for more information.

See "Viewing the VirusScan Activity Log" on page 67 for more information.

Specifying what to put in the activity log

The following information can be included in the activity log:

- Discovery of infected files

- Files that are cleaned
- Files that are deleted
- Files that are moved
- The VirusScan settings at the time of the virus discovery
- A summary of the VirusScan scanning session
- The date and time the virus is discovered
- The name of the user running VirusScan.

To specify what to put in the activity log, follow the procedure below.

Step	Action
1.	Select the task for which you are setting up virus reporting.
2.	Select **Scan/Properties**.
3.	Choose the Reports tab.
4.	Select, from among the checkboxes, which information you want to include in the log file.

Sending Virus Alerts

In addition to telling VirusScan what virus reporting actions to take, and what to do with infected files, you can use the Alert Manager to configure VirusScan's alerting actions.

✍ *These options are specified independently of any task; your settings apply to all scanning tasks configured for the Console.*

Listed below are the possible actions VirusScan can take:

- Send you, or another user, a message that a virus was found
- Forward messages to other users
- Execute a specified program when a virus event occurs
- Send an alert to a pager
- Send alerts via email
- Send an alert to a printer.

To set virus alerting actions:

1. Select Tools/Alerts

2. On the System Alerts tab:

   - Select 'Log event in application log' to include VirusScan virus events in the Windows NT Event Log. You can log these in the local computer's Event Log, or in another NT Computer's Event Log.

   - Select 'Execute program on event' to launch a program when VirusScan finds a virus. Specify the name of the program in the box provided, of click Browse to find it. You can run that program every time a virus is found, or only the first time by selecting the corresponding checkbox.

   - Select 'Send events to Alert Manager' to use VirusScan's Alert Manager. The next section, "Configuring the Alert Manager", describes how to confiugre the Alert Manager.

3. On the Messages tab:

   - Select each message you want to include by activating its check-box.
   - To edit the text of any message, click on that message and click the Edit button. You can edit the messages text and select the priority for each messsage, which VirusScan uses to filter the messages.
   - Click OK.

4. Click OK to save the Alert list, or click Configure from the System Alerts tab to confgure the Alert Manager.

Configuring the Alert Manager

The Alert Manger allows you to specify the following:

- Pager alerts
- Printer alerts
- Email alerts
- Computers to forward alerts to
- SNMP configuration.

To configure the Alert Manager:

Step	Action

1. Select Configure from the Alert List.

2. On the Pager tab:

   - Click Add to set up one pager's properties.
   - Enter the pager's type (alphanumeric or numeric), its phone number, its ID number, and its password in the spaces provided.

- Select whether to use a standard alert message or a custom message.
- Click Modem Settings to specify the type of modem to use. Click OK.
- Click Priority Level to specify whether the pager responds to low-, medium-, or high-priority alerts. Click OK.
- Click OK to save this pager's alert properties.

3. On the Forward tab:

   - Click Add to select computers to forward alerts to.
   - Type in the name of the computer, or browse for it.
   - Click Priority Level to specify whether this forwarding responds to low-, medium-, or high-priority alerts. Click OK.
   - Click Test to send a test message to that computer.
   - Click OK.

4. On the Printer tab:

   - Click Add to add the name of a printer to the Alert list.
   - Select a printer and click Remove to remove a printer's name from the list.
   - Select a printer and click Properties to respecify the name of the printer or the priority level.
   - Click OK.

5. On the Network Message tab:

   - Click Add to select a computer to send messages to.
   - Enter the computer's name or browse for it.

- Click Priority Level to specify whether the message is sent for low-medium- or high-priority alerts. Click OK.
- Click Test to send a test message to that computer.
- Click OK.
- Select a computer from the list and click Remove to remove that computer's name from the list.
- Select a computer from the list and click Properties to re-specify the name of the computer or its priority level.
- Click OK.

6. On the SNMP tab, click Enable SNMP to send an alert to a third-party SNMP manager.

7. On the E-mail tab:

- Click Add to select an email address and header information.
- Click SMTP Settings to specfiy mail server and account information. Click OK.
- Click Priority Level to specify whether the email is sent for low-medium- or high-priority alerts.
- Click Test to test the email setup.
- Click OK.
- Select an email receiver from the list and click Remove to remove it from the list.
- Select an email receiver from the list and click Properties to re-specify the this email receiver's setup.
- Click OK.

8. On the SNMP tab:

- Select the ‘Enable SNMP’ checkbox if you want SNMP enabled.
- If you enabled SNMP, click Configure SNMP to specify the network settings.
- Click OK.

9. The summary tab displays all the alerts devices you have set up. Click OK to accept the configuration.

7 Viewing Scan Results

Viewing Scan Results

VirusScan offers several methods of viewing the results of a scan:

- Run-time statistics
- The VirusScan Activity Log
- The Windows NT Event Log.

Each of these is explained in this chapter.

Viewing Scan statistics

You can view the statistics of scans in progress by double-clicking on the task in the VirusScan console. The statistics displayed in the scan statistics box correspond to the selected task only.

- A list of the files, folders, and drives that get scanned by this task
- The name of the file currently being scanned
- The number of files and boot records that have been scanned, found infected, cleaned, and deleted.

Viewing the VirusScan Activity Log

The VirusScan Activity Log tracks scanning activity for all the tasks on your Console.

Unlike the statistics listed above, the Activity Log contains information for all tasks, but you specify on a task basis what goes in. For example, you can specify that only infected files are logged for task 1, and all information is logged for task 2.

The following are the types of information you can include:

- Each discovery of an infected file
- Each file cleaned
- Each file deleted
- Each file moved
- The VirusScan settings at the time of each virus discovery
- A summary of the VirusScan scanning session
- The date and time each virus is discovered
- The name of the user running VirusScan.

See "Specifying what to put in the activity log" on page 55 to see how to select what goes in to the Activity Log for each task.

To view the Activity Log, select a task, and then select Scan/Activity log. See "Creating the VirusScan Activity Log" on page 55. for more information.

Viewing the Windows NT Event Log

You can look also look at the Windows NT Event Log for information about VirusScan activity. The Event Log is a Microsoft Windows NT product and is not part of VirusScan. However, VirusScan, like other NT applications, can record information in that log.

The Event Log contains significant events and system errors, including those occurring in VirusScan. To view the Windows NT Event Log, follow the procedure below.

Step	Action
1.	From Windows NT Program Manager, open the Administrative Tools program group.
2.	Double-click on the Event Viewer icon.

Response: The Event Log window is displayed.

3. See your Windows NT documentation for more information about Event Viewer.

A

Using Auto Updating

Auto Updating allows you to have VirusScan periodically update its own virus data files or patches.

VirusScan can get those files, along with any installation instructions, from a central location. Alternatively, VirusScan can get them from an external source, such as the McAfee FTP site, using a command script file. Once you have set up which type of updating you want to do, and specified the location or the script name, you can schedule how often to update, or update immediately.

This appendix describes how to specify these options and set up VirusScan's Auto Updating.

Getting Automatic Updates From a Central Location

You can create a central repository to store all of VirusScan's updateable files. By having a central location, you ensure that all computers running the VirusScan scanning can work with the same virus data files.

To specify a central location where VirusScan will obtain updated files:

Step	Action

1. Select **Tools/Auto Update**.
2. On the Update Location tab:
   - Select the ''Copy update module from' option, and enter the path to the update module in the box.

     Enter the path only; do not enter a file name.
   - Select the 'Store Update Module in' option, and enter the directory name in the box.

     Again, do not enter a file name.
3. On the Schedule tab:
   - Select the 'Enable scheduler' option.
   - Choose, from among the options provided, which type of schedule you want to apply to this scanning task. If you choose a daily schedule, click Which Days to specify on which days of the week to scan.
   - Enter the specifics of the schedule, such as at what time to start or on what day of the month.
4. When you are finished configuring Auto Updating, click OK

Response: Auto Updating is configured to get the updated files from the directory you chose according to the schedule you specified.

When obtaining update files, Auto Update looks for a text file called VERSION.DAT. Auto Update compares the information in the file with a Windows NT registry value. If they match properly, Auto Update looks again at VERSION.DAT to get the name of the actual update file, which is then downloaded.

Performing an immediate update from a central location

In addition to scheduling automatic updates, you can initiate an immediate update:

- Set up the central location downloading as described above, but rather than moving on to the Schedule tab, click the Update Now button.

  Response: The virus data files are updated immediately. However, for future updates, you must either set up a schedule for Auto Updating, or else do another one-time update when it's again time to update. (Files should be updated approximately monthly).

Automatically Downloading Updates From an External Souce

You can use a predefined script to download update files automatically. This script can be anything from an FTP download script to a ProcommPlus download script. VirusScan comes with a sample script that you can use, but you will need to update it so that it is specific to your needs. The sample script is shown in “Sample Auto Update script” on page 75.

To specify the name of a script that VirusScan will use obtain updated files from an external source:

Step	Action

1. Select **Tools/Auto Update**.

2. On the Update Location tab:

   - Select the ’Obtain update module using shell script’ option, and enter the path and name of the script in the box.

     VirusScan comes with a sample script, called FTPGET.CMD, which you can change, rename, or use as is. This script is shown in “Sample Auto Update script” on page 75.

   - Select the ‘Store Update Module in’ option, and enter the directory name in the box.

     Again, do not enter a file name.

3. On the Schedule tab:

   - Select the ‘Enable scheduler’ option.

   - Choose, from among the options provided, which type of schedule you want to apply to this scanning task. If you choose a daily schedule, click Which Days to specify on which days of the week to scan.

- Enter the specifics of the schedule, such as at what time to start or on what day of the month.

4. When you are finished configuring Auto Updating, click OK

Response: Auto Update executes the script you specified to download virus data file updates from the Internet.

Performing an immediate update using a script

In addition to scheduling automatic updates, you can initiate an immediate update:

- Set up the external source downloading as described above, but rather than moving on to the Schedule tab, click the Update Now button.

Response: The virus data files are updated immediately. However, for future updates, you must either set up a schedule for Auto Updating, or else do another one-time update when it's again time to update. (Files should be updated approximately monthly).

Sample Auto Update script

The script shown below is exactly the same as the one included with your VirusScan installation. You will need to modify it to suit the needs of your site.

```
@echo off
rem *****  FTPGET.CMD                                    *****
rem *****  Copyright (C) 1996 McAfee Associates Inc.     *****
rem *****  This script will download file specified      *****
rem *****  on the command line from mcafee.com           *****
rem *****  /pub/updates directory                        *****
rem *****  errors and status information will be         *****
rem *****  logged into FTPGET.LOG in the current         *****
rem *****  directory                                     *****
rem Create FTP command file FTPCMD.FTP
echo open>FTPCMD.FTP
echo ftp.mcafee.com>>FTPCMD.FTP
echo ftp>>FTPCMD.FTP
echo %USERNAME%@%USERDOMAIN%>>FTPCMD.FTP
echo bin>>FTPCMD.FTP
```

```
echo get /pub/updates/%1>>FTPCMD.FTP
echo close>>FTPCMD.FTP
echo quit>>FTPCMD.FTP
rem Now launch ftp.exe with the command file FTPCMD.FTP
ftp -s:FTPCMD.FTP >> FTPGET.LOG
rem Now delete FTPCMD.FTP
del FTPCMD.FTP > nul
rem We're done
```

B

McAfee Support Services

McAfee is pleased to offer many different types of technical assistance to customers. These flexible support programs are designed to meet the needs of individuals and businesses at any level. Whether it is our complimentary 90-day introductory technical support program or the optional 1-year personal online maintenance and support program, McAfee wants to ensure that all our customers receive the level of support they require.

In addition, we offer a variety of technical assistance plans designed to meet the needs of business customers, including training, consulting, and enterprise support, as well as a Jump Start program.

Please review each of the different support service plans and benefits listed in this appendix and pick the one best suited for you.

✍ *The term update refers only to the virus definition files (.DATs), and the term upgrade refers to product version revisions, executables, and definition files. McAfee offers free online virus signature file updates (.DATs) for the life of your product. However, we cannot guarantee backward compatibility of the signature files with previous versions' executable files (.EXEs). By upgrading your software to the latest product version and latest .DAT files, you ensure complete virus protection for the term of your software subscription or maintenance plan.*

Customer Service Programs

Free 90-day introductory support program

All registered owners of single-node products are entitled to free online virus updates (new .DAT files) for the life of the product, one free online product upgrade (product version revision) with the newest features and virus protection (if applicable), and the free support services listed below during the first 90 days of software ownership.

- Technical support phone assistance during regular business hours, 6:00A.M.– 5:00P.M. PST, Monday through Friday, from our professionally trained support representatives at (408) 988-3832.
- Electronic and online support available 24 hours a day, seven days a week on each of the forums listed below:
  - Automated voice and fax system: (408) 988-3034
  - McAfee BBS (electronic bulletin board system): (408) 988-4004
  - World Wide Web site: http://www.mcafee.com
  - CompuServe: GO MCAFEE
  - The Microsoft Network: MCAFEE
  - America Online keyword: MCAFEE.

To receive your free one-time online upgrade please contact our Sales Support department at (408) 988-3832. Please supply your proof of purchase when you request the upgrade. You will be given a password to the upgrade area on either the McAfee BBS, FTP site, or World Wide Web site so that you can download a registered version of the latest product. This password is valid for one access only.

Subscription maintenance and support program (free)

McAfee offers all registered owners of licensed multiple-node subscription products the following free support services and maintenance during the two-year term of the software subscription.

- Technical support phone assistance during regular business hours, 6:00A.M.–5:00P.M. PST, Monday through Friday, from our professionally trained support representatives at (408) 988-3832.

- Two years of free online product upgrades with the newest features and virus protection (if applicable). If you upgrade your operating system, you can also upgrade your McAfee product to the new platform (for example, from Windows 3.1 to Windows 95).

- Electronic and online support available 24 hours a day, seven days a week on each of the forums listed below:

  - Automated voice and fax system: (408) 988-3034
  - McAfee BBS (electronic bulletin board system): (408) 988-4004
  - World Wide Web site: http://www.mcafee.com
  - CompuServe: GO MCAFEE
  - The Microsoft Network: MCAFEE
  - America Online keyword: MCAFEE.

Optional support plans

Option 1—one-year personal online maintenance and support program

$49 U.S.

For registered owners of single-node products who want to extend their support coverage, this plan allows you to call in for unlimited technical support, download the latest virus protections updates each month, and periodically download upgrades from any of McAfee's registered online services—all for a full year. If you upgrade your operating system, you can also upgrade your product program to the new platform.

Option 2—one-year quarterly disk/CD maintenance and support programs

$149 U.S.

This plan is for registered owners of either single- or multiple-node subscription products. It offers all the features of option 1, while adding a quarterly mailing of software upgrade diskettes or CDs (depending on the product) and a quarterly update newsletter. With this option, you can update your product to include the latest features and virus updates without having to download files from an online service.

Each optional support plan begins as soon as you purchase the product, and is good for one year, at which time you can renew your support program through McAfee's sales support department at (408) 988-3832.

✍ *McAfee reserves the right to change part or all components of its customer services programs at any time without notice.*

Professional Services Programs

McAfee Professional Services provide a wide range of on-site services. Whether for short-term assistance or long-term strategic planning, a highly qualified consultant can help you achieve positive results. McAfee consultants are trained on NetWare, Microsoft NT Advanced Server, Windows 95, and a multitude of desktop applications.

Before work begins, a project manager discusses the project scope and objective with you and comes to a mutual agreement on the job objective. When the consultant leaves the site, you can be sure that the objective has been achieved.

✍ *McAfee reserves the right to change part of all of its Professional Services Program at any time without notice.*

Training

$190 U.S./hour or $1,200 daily, as well as packaged rates

McAfee's expertise and experience is available to your personnel, allowing an organization to take full advantage of computing resources. McAfee offers on-site training on all McAfee products, network management seminars, anti-virus seminars, customized curriculums for site-specific applications as well as product and personnel certification. McAfee's consultants provide extensive training with curriculum tailored to your organization's needs.

Consulting

$190 U.S./hour or $1,200 daily, as well as packaged rates

McAfee Professional Services offer a number of hourly and daily consulting services including:

- Troubleshooting an existing installation
- Writing PowerScript or SaberBASIC scripts
- Planning and designing networks
- Installation and configuration

- Windows 95 configuration
- One-on-one consulting.

McAfee Professional Services are available on a quotable time and materials basis to perform project management, product research, and a number of other consulting services.

Jump Start program

$7,500 U.S. for a 4-day network management program or $5,500 for a 3-day anti-virus program

This fixed-fee consulting program is designed to get clients up and running on McAfee products as soon as possible. It includes training, installation, and configuration services as needed on a single server. It is designed to demonstrate how to connect various PCs to the LAN, train administrators how to use the program, and master the roll-out process.

Enterprise support

$10,000 U.S. for a one-year subscription

McAfee's Enterprise Support Program provides customers with the highest level of support possible. This fee-based program is designed for those customers who need a higher level of personal service.

The Enterprise Support Program offers the following features:

- Direct pager number to your assigned senior Enterprise Support Program analyst
- Extended support hours: 7:00 A.M. to 7:00 P.M. CST Monday–Friday
- Five designated McAfee contacts
- Proactive support, providing updated company and product information as it becomes available
- On-site services at a 25% discount

- VIP issues review list
- Beta site (if desired).

Each Enterprise Support Representative calls clients each week. This phone call is used to forward any information such as technical notes and application anomalies of which you should be aware. This call also ensures that you have no unresolved problems or complications with the product. Enterprise Support representatives will return your page on the day it is received.

Optional enterprise support features

$5,000 U.S per feature

7 X 24 support

Frequently, customers are responsible for their own LANs, which run 24 hours a day, seven days a week. This feature offers round-the-clock support for clients requiring support outside normal business hourst.

Remote support

This feature provides customers with data connection support using McAfee's NetRemote product. This support option provides services such as remote network administration and management, network troubleshooting, and optimization.

Index

W