Quick Heal™ for Windows 95/98/NT

User's Guide

Cat Computer Services (P) Ltd.

Quick Heal License Agreement

This document is a legal agreement between you, the licensee, and Cat Computer Services (P) Ltd.. By using this program, you are agreeing to become bound by the terms of the agreement. If you do not agree to the terms of this agreement, promptly return the disk package and the other items that are part of this product in their original package, with your payment receipt.

In consideration of payment of the License Fee, which is a part of the price evidenced by the Receipt, Cat Computer Services (P) Ltd. grants to the Licensee a nonexclusive right, without right to sublicense, to use this copy of this anti-virus software on a single Computer at a time. Cat Computer Services (P) Ltd. reserves all rights not expressly granted, and retains title and ownership of the Software, including all subsequent copies in any media. This Software and the accompanying written materials are copyrighted. You may copy the Software solely for backup purposes; all other copying of the Software or the written materials is expressly forbidden.

As the only warranty under this Agreement, and in the absence of accident, abuse or misapplication, Cat Computer Services (P) Ltd. warrants, to the original Licensee only, that the disk(s) on which the software is recorded is free form defects in the materials and workmanship under normal use and service for a period of thirty(30) days from the date of payment as evidenced by a copy of the Receipt. Cat Computer Services (P) Ltd.' only obligation under this Agreement is, at Cat Computer Services (P) Ltd.' option, to either (a) return payment as evidenced by a copy of the Receipt or (b) replace the disk that does not meet Cat Computer Services (P) Ltd.' limited warranty and which is returned to Cat Computer Services (P) Ltd. with the copy of the Receipt.

Disclaimer

This software package is provided as such without warranty of any kind, either expressed or implied, including but not limited to the implied warranties of merchantability and fitness of the package. In no event will Cat Computer Services (P) Ltd. be liable to you or anyone else for any damages including loss of data, lost profits or any other damages arising out of the use of this software package ever.

Printed in Pune at Super Cartons.

Contents

Introduction **7**

About this document **8**

About Quick Heal **9**

Components of Quick Heal **12**

Chapter 1 Installing Quick Heal for Windows 95/98/NT **15**

Getting Prepared 15
Installing Quick Heal 16

Chapter 2 Using Quick Heal **17**

Loading Quick Heal 17
Using Help 18
Using Integrated Scanner 18
Performing virus scans 19
Viewing Activity Log 21
Scheduling Quick Heal Scanner 22
Enabling and disabling On-line Protection 26
Creating Rescue Disk On Windows 95/98 28
Creating Rescue Disk On Windows NT 29
Viewing the Virus List 29
Using Quick Heal Toolbar 31

Chapter 3 Customizing Quick Heal **33**

Customizing Scan Options 33
Customizing Startup Options 38
Customizing On-line Protection 41
Specifying when to scan a file On-line 42
Specifying which files to scan On-line 43
Specifying how to respond when a virus is found On-line 43
Monitoring for boot viruses 44
Checking for virus-like activities (for Windows 95/98 only) 45

Chapter 4 Cleaning Viruses **47**

Cleaning viruses encountered during scans: 47
Cleaning virus encountered in memory 48
Cleaning the virus encountered by macro-virus protection 49
Cleaning viruses encountered in startup scan 49
Responding to Startup scan virus in memory alert 50

Responding to Partition table/Boot record changes 50
Responding to virus found alerts from On-line Protection: 51
On-line Protection Virus found alert 52
On-line protection virus-like activity alerts 53

Chapter 5 Using Quick Heal Emergency and Rescue disk 55
Using Quick Heal Emergency Disk 55
Using Quick Heal Rescue Disk On Windows 95/98 57
Command-line parameters for QHRESCUE.EXE 59
Using Emergency Repair Disk On Windows NT` 59

Chapter 6 Updating Quick Heal 61
Automatically updating Quick Heal 61
Manually updating Quick Heal 61

Appendix A Virus Fundamentals 63
What is a computer virus? 63
Activation of a virus 64
The challenge from modern techniques used by viruses 64
How can you recognize a virus activity? 65

Appendix B Messages in Quick Heal 67

Glossary 73

Introduction

Congratulations for choosing **Quick Heal**™ as the correct anti-virus protection for your computer. This new updated version is a result of customer confidence in our anti-virus product. It is specially designed to combat the latest and deadliest computer viruses.

Quick Heal from Cat Computer Services (P) Ltd.

In Dec 1993, a young wizard had a tough time against a virus. He fought against it and killed it. The idea of developing an anti-virus was established. A small office, a computer and Sanjay Katkar - the starting assets of a product. Early 1994 - a menu driven anti-virus software was ready. It also had a fair number of viruses. The name Quick Heal was coined and a simple but powerful package was born. The product received a wide acceptance. Cat Computer Services was born.

After further deliberations, it was found that the existing anti-virus products were either not effective enough or there was hardly any technical support available. Mean while, the development team was increased in order to cope with the demand for the Quality Product. Quick Heal version 3.0 was launched in 1995 with multi-platform support (DOS, Windows, NetWare..). This version received a very positive response from all over India. It included features that would meet the extensive and critical needs of a wide variety of users, from SOHOS to networking, LAN etc.

Cat Computer Services (P) Ltd. now introduces Quick Heal for Windows 95/98/NT. This version makes use of the most advanced GUI facilities provided by Windows 95/98/NT to provide you with the best of the user interface. This version is backed by Quick Heals most reliable virus detection engine (which was there with Quick Heal for DOS and Windows) taking full advantage of 32-bit platform. We also have web site http://www.quickheal.com for online sales/updates, new virus news and alerts etc. It is one of the select few Indian anti-virus software to be on par with the international standards.

About this document

This user's guide contains all the information you need to install, use and troubleshoot Quick Heal for Windows 95/98/NT. Once familiar you can also use it for reference. Each topic has been dealt separately so as to maximize ease of use and troubleshooting. Full care has been taken to incorporate all details with the latest developments in the shipping.

About Quick Heal

The tremendous upheaval of the IT industry in this decade is making desktops vulnerable to the inundation of viruses owing to the exposure of machines to external data interfaces like modem, internet BBS, E-mail and various online services etc. To rescue you from this situation here comes - Quick Heal virus buster.

Quick Heal for Windows 95/98/NT is one of the most powerful anti-virus software available to rescue you from the onslaught of the viruses. It safeguards your computer from virus infection, no matter what the source. Every feature in Quick Heal is a result of intense study of viruses and the growing needs of users. The underlying objective is to offer thorough user friendly virus protection. The main features that contribute to the strength of the software include

- Powerful Integrated Scanner
- On-line Protection and Automatic Virus Removal
- Detects unknown viruses
- Scans recursively inside compressed files (ZIP & ARJ) and EXEs (LZEXE).
- Uses anti-stealth methodology.
- Saves Rescue Information. Trusted to save you in times of trouble.
- System Integrity Check during Startup
- Scheduler

When you install Quick Heal with default settings, it is already pre-configured so as to provide balanced efficiency and protection.

Once installed, if the default options are not changed, Quick Heal will perform following checks to keep the viruses away from your computer:

- Check system areas for viruses at startup (on Windows 95/98 only).
- Check program files for viruses as soon as the files are accessed for execution or copying.
- Check floppy disks for boot viruses when you use them.
- Monitors your computer for virus-like activities i.e. those activities that might indicate presence of a virus. (on Windows 95/98 only)

How Quick Heal protects your system?

Every component in Quick Heal is designed so as to ease the use of the software. Every feature included in the software is a result of intense research about viruses those are present today as well as those which might come in the future.

Determining the risk level

The probability that a virus infects your system is directly related to the amount of its exposure to the external environment. The more your system is exposed to the external environment (by means of floppies, modem, network etc.), the more is the chance of a virus infecting your system. Depending on the degree to which your system is exposed to such media, you should decide your risk level.

The Quick Heal answer

Quick Heal is equipped with several technologies to keep your computer virus-free. Each technology has specific strengths, which can be configured depending upon the risk level and how much protection do you require.

Of all the components the scanner is the most basic component of any anti-virus software. Quick Heal's integrated scanner is equipped with three different engines along with the capability to scan compressed files and EXEs. The engines that work together to form a versatile scanner include:

- Conventional pattern matching engine: It is the most basic method of scanning that searches known viruses using signatures.
- Integrity checker: This engine keeps vital details of all the executable files. When an unknown virus infects a file, it makes particular changes in the file. The engine detects such changes to determine infection by an unknown virus. It also keeps sufficient information of every file to recover the file from such infections. The only prerequisite for this engine to detect a new virus is that information about the file should have been taken before the virus infects the file.
- Heuristic engine: This engine is intelligent enough to scan unknown viruses in files or partition / boot sectors. For detecting whether a file is infected by an unknown virus, it disassembles the file looking for suspicious characteristics. It is even capable of detecting unknown polymorphic viruses.

Quick Heal's Online Protection module continuously scans your system for viruses and monitors for virus-like activities. It has also got the facility to remove the viruses on-line. You will be totally unaware about the viruses trying to infect your system and getting killed while the on-line protection is working in the background.

Quick Heal also includes a DOS based device driver (CATEYE.SYS). It scans programs that loads before Windows loads, preventing viruses from getting into the system before the On-line Protection system gets loaded.

Scheduled scans and Startup scans supplement other automatic protection features to ensure that your system is free of viruses. All the above mentioned components along with other components such as Tool Bar, DOS based scanner etc. make sure that no virus, whether known or unknown, infect your system.

All the components and their functions are described in the next chapter “Components of Quick Heal”.

Components of Quick Heal

Quick Heal is one of the most reliable anti-virus software that you can use. As you go on learning about various components of Quick Heal, you will know its potentials. Each component has its own role in protecting your machine against viruses.

Quick Heal Integrated Scanner

This is the main component of Quick Heal anti-virus that is fully integrated, with most of the components of Quick Heal. Through its main window you can:

- Initiate manual scan.
- Configure Quick Heal.
- View virus database.
- Create rescue disk.
- View activity log.

Quick Heal Scheduler

Use this component to schedule the scanner to run automatically at predetermined time. This will supplement other automatic protection features to ensure that your computer is virus-free.

Quick Heal Online Protection

Quick Heal's Online Protection component scans your systems program files for viruses whenever they are accessed, executed or copied. It also monitors your system for virus-like activities and warns you, so you can stop them from occurring.

Quick Heal Startup Scan

This is the first level of protection that scans your system each time your computer starts and detects viruses that infect your computers boot record or startup files. This assures you that your system is virus-free each time you start it.

Quick Heal Tool Bar

This component provides you easy access to most of the components of Quick Heal without switching from your current application. This reduces the chance of using unscanned floppies that may contain viruses.

Quick Heal DOS based Scanner

DOS based scanner is one of the important components of Quick Heal which come into picture when removing viruses from a shutdown computer. When your system is already infected by some virus (before installation) or when Quick Heal detects a virus in memory, you are recommended to shutdown your system, boot the system using Rescue Disk (a clean DOS bootable disk in case of Windows NT) or clean bootable and then use Quick Heal DOS scanner from Emergency Disk to remove viruses.

QHRESCUE.EXE Utility

This component of Quick Heal runs from the DOS prompt. Using this you can save, compare and restore your hard disk's partition table, boot records and CMOS settings using Rescue Disk. **This utility cannot be used on Windows NT**.

Live Update

This component easily updates your copy of Quick Heal to latest available version with a click of a button. You will need to have access to Internet to use this utility, as it updates your copy by downloading the latest upgrade definition file from Quick Heal's web site.

Chapter One

Installing Quick Heal for Windows 95/98/NT

Quick Heal for Windows 95 / 98 / NT has a very simple installation procedure. While you are installing, simply read each installation screen, follow the instructions, then click Next to continue. By selecting the preset options, Quick Heal is configured so that you are automatically protected against viruses.

Quick Heal should be installed on a virus-free machine. If you are sure your computer is infected by a virus, use the Emergency Disk to remove the viruses before installing Quick Heal (see "To remove viruses using Quick Heal Emergency Disk" on page 55). If you are not sure whether your computer is already infected by a virus, continue with the installation. Quick Heal setup will scan your computer for viruses as a part of its installation process.

If you are installing Quick Heal for the first time

- ☞ Read this manual carefully atleast once to understand the capabilities and working of the software.
- ☞ Remember to submit the registration form.

Getting Prepared

Installing Quick Heal on a stand-alone machine requires following tips to be remembered:

- ☞ If you have any anti-virus software / hardware loaded, unload it temporarily.
- ☞ Quick Heal for Windows 95 / 98 / NT requires approximately 8 MB of disk space. You can install Quick Heal on any drive partitions like C, D, E, F, etc.
- ☞ On LAN workstations, installation shall be done on local drives. Installation of Quick Heal on network drives is not recommended.

Installing Quick Heal

To start with installation, insert Setup Disk 1 in drive A:, click Start on Windows taskbar and choose Run… from the Start Menu. Give the following command in the text box and click OK.

```
A:\>SETUP
```

Installation program will first perform Pre-Install Virus Scan on your system to scan system memory and system files for known viruses and then start with the installation. Follow the instructions in each succeeding window until the installation is completed, then click Finish.

During the Pre-Install Virus Scan, if a virus is found in memory then restart the system using clean DOS bootable and scan for viruses using Emergency Disk (see “To remove viruses using Quick Heal Emergency Disk” on page xx). If a virus is found in a file, it means that although the virus is not currently active in the system, it has infected your system. Remember to scan entire system for viruses after the installation is over.

During installation, the setup procedure will prompt you to specify the components you would like to add in the startup (components those should be loaded everytime you start Windows). It would also prompt you for installing Word macro virus solution and shell extensions and creating a Rescue Disk.

Quick Heal setup procedure provides online help wherever applicable and necessary. If you still encounter any problems even if you followed the above-mentioned steps, contact your supplier for installation support.

Chapter Two

Using Quick Heal

Using Quick Heal you can scan your system for viruses, view or change the configuration options, save and compare rescue information (only on Windows 95/98), view virus database, view activity log and schedule scans that run automatically.

Loading Quick Heal

You can load Quick Heal in following two ways:

- Click the left most button on Quick Heal Toolbar (see Figure 2-1)
- Click Start on Windows taskbar, choose Programs, choose the Quick Heal group and click Quick Heal from the group items (see Figure 2-2). Quick Heal scanner main window will appear (see Figure 2-3).

Figure 2-1 Quick Heal Toolbar

Figure 2-2 Loading Quick Heal

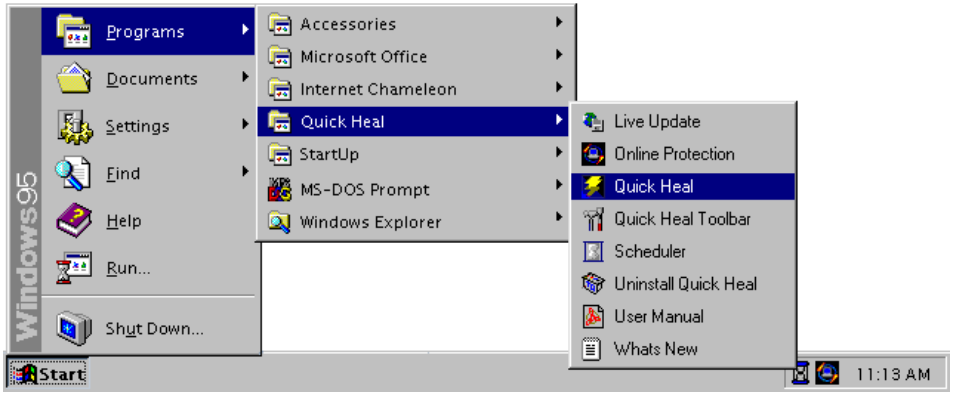
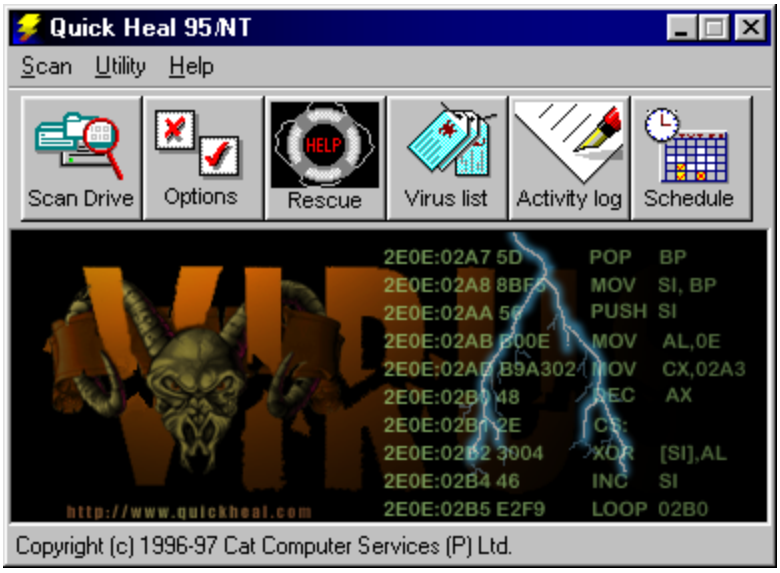


Figure 2-3 Quick Heal Main Window



Using Help

Quick Heal provides On-line help for most of the message windows. You can get help on commands, procedures and definitions by:

- Using commands on the Help menu.
- Pressing F1 when you need help.
- Clicking the Help button in a dialog box.
- Using the “question mark” button in the right corner of the title bar of any dialog box.

Quick Heal’s help system consists of extensive topics index, commands and procedures with general FAQ’s. The help system provides you with easy to use context sensitive help for any option or a feature of Quick Heal.

Using Integrated Scanner

The scanner is obviously the most important component of any anti-virus software. Quick Heal’s integrated scanner can be used to perform virus scans, configure Quick Heal, create Rescue Disk, view virus database and activity log and schedule virus scans.

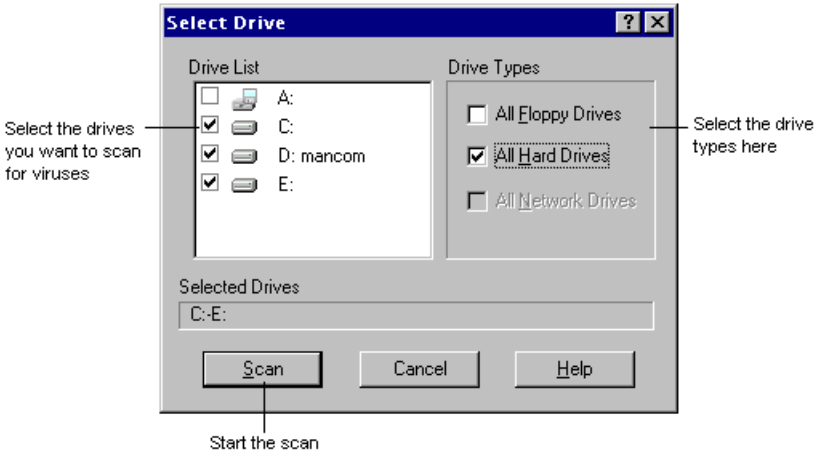
Performing virus scans

You can either scan for viruses manually or schedule a scan to occur automatically. For more details on how to schedule a scan see Scheduling Quick Heal Scanner on page 22. Now we will see how to perform a manual scan.

To scan one or more drives:

1. Start Quick Heal.
2. Click the Scan Drives button on toolbar.
3. In the Select Drive dialog box that appears, check the drives you want to scan from the drives list box. You can check special selection for multiple drives by checking items in the Drive Types group (see Figure 2-4).
4. Now click the Scan button.

Figure 2-4 Drive Selection



To scan a folder:

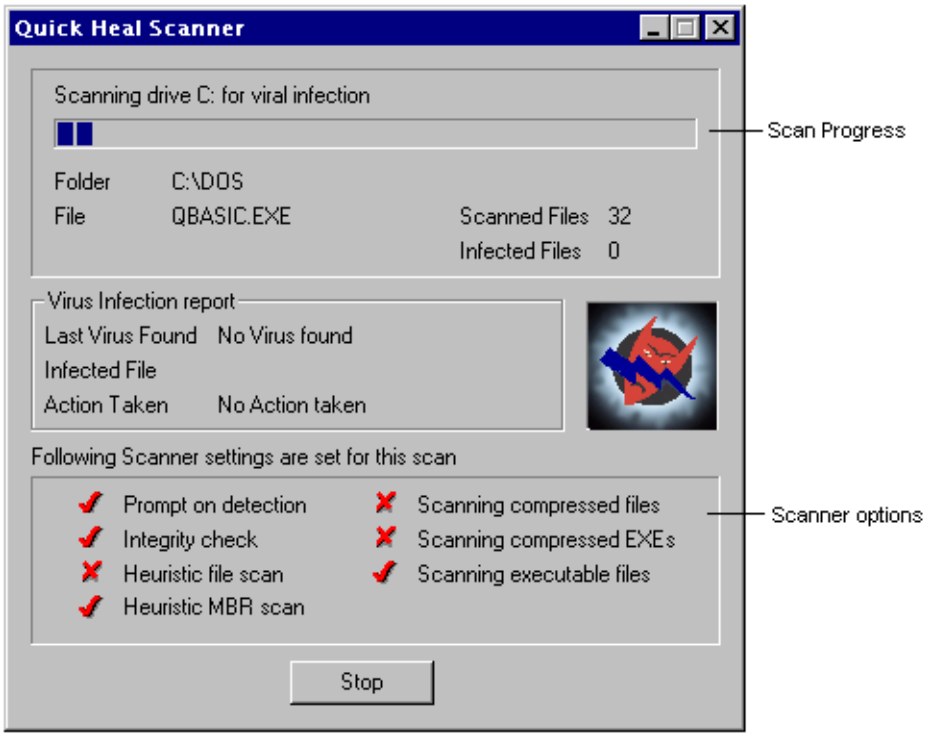
1. In Quick Heal main window, select Folder from Scan menu.
2. In the Scan Folder dialog that appears, select the folder that you want to scan.
3. If you want to skip the sub folders inside the selected folder, deselect the Include Subfolder checkbox.
4. Click Scan.

To scan a file:

1. In Quick Heal main window, select File from Scan menu.
2. Select the file you want to scan.
3. Click Open.

As the scanner scans the selected item, Quick Heal Scanner dialog box displays the scan progress and the current folder being scanned (see Figure 2-5). It also displays scanner configuration and information about last virus found during the scan.

Figure 2-5 Scan Progress



Alternately, you can also scan a single drive, folder or file directly through Explorer if you have enabled shell extensions feature during installation. To scan a drive, folder or file through explorer, simply right-click the item you want to scan and from the menu that appears select Quick Heal Scan.

If a virus is found during the scan, the scanner provides you the option to remove or skip the file (see “Cleaning viruses encountered during scans” on page 47).

At the end of each scan Quick Heal displays the scan summary. For detail scan report, click the Report button. Scan report displays the details about the scan. Quick Heal generates a log entry for each scan. A log entry contains brief information about result of the scan.

By default, Quick Heal scans for only executable files, as these are the only files through which a virus spreads. The executable files include the files with extension .EXE, .COM, .DRV, .DLL, .OVL, .OVR, .SYS, .VXD & .386. But there are few programs that install the executables with extension not from amongst the above-mentioned list. To ensure that these files get scanned as well (if you are scanning the virus infected system) just perform the following steps.

To scan all files:

1. In Quick Heal main window, Click Options button on toolbar.
2. Click the Scanner tab.
3. Select All files option in Scan group.
4. Click OK.
5. Now scan the drive(s) or folder from which you want to scan all files.

For more information on configuring Quick Heal options see “Customizing Scan Options” on page 33.

Viewing Activity Log

Activity log contains the log of all the virus scanning. Quick Heal scanner creates a separate log file for each scan and each log file has an entry in the Activity log viewer.

To view the list of Activity log reports:

- Click Activity Log in Quick Heal main window.

Activity Log dialog box appears. (see Figure 2-6)

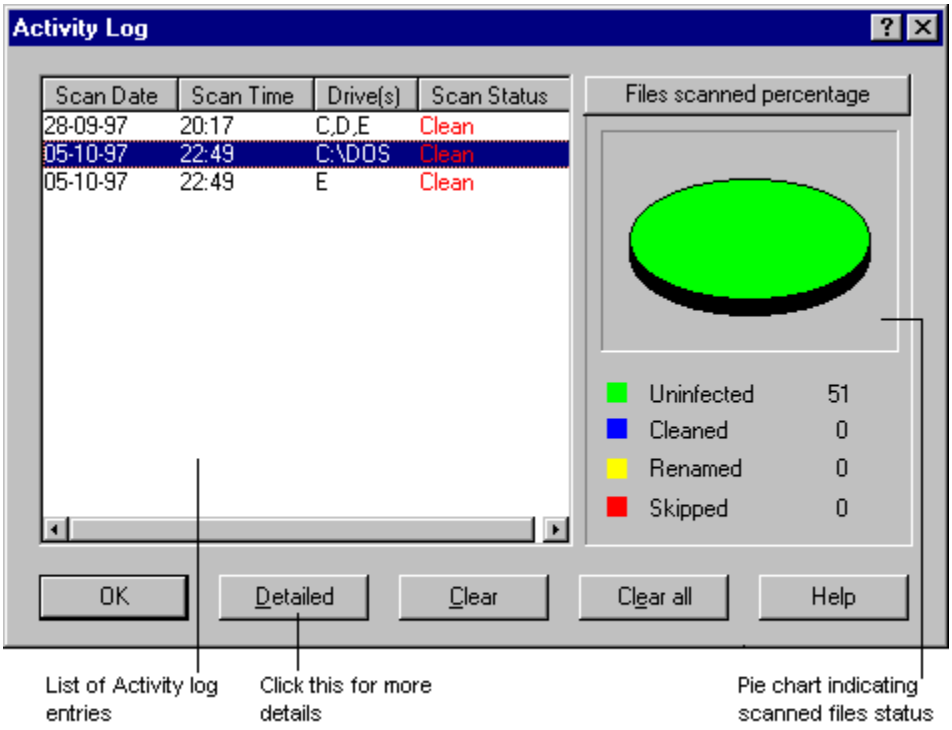
The list box displays a list of activity logs with details such as scan date, scan time, drives scanned and the scan status. A pie chart displaying the percentage of files scanned, with number of viruses found and removed is show to the right side of the list box.

Click Details to view details about the selected log entry. The Detail information consists of additional information regarding viruses detected and action taken against those viruses.

Click Clear to delete selected scan log entry.

Click All to delete all scan log entries.

Figure 2-6 Activity Log



Scheduling Quick Heal Scanner

You can schedule the scanner to run automatically at predetermined time and intervals. You can schedule the scan one time, hourly, daily, weekly or monthly. This will supplement other automatic protection features to ensure that your computer remains virus-free.

You can access the scheduler in any one of the following ways:

- Click Scheduler button from Quick Heal toolbar.
- Click Scheduler button from Quick Heal main window.
- Choose Scheduler in Quick Heal group from Start menu.

Once the scheduler is loaded its icon appears on the Windows taskbar (see Figure 2-7). When you double click the taskbar icon of scheduler, Quick Heal Scheduler window appears. Scheduler window contains two tab controls viz. Scheduler Entry Form and Scheduler Report. To schedule Quick Heal you must be in Scheduler Entry Form tab (see Figure 2-8).

Figure 2-7 Windows Taskbar

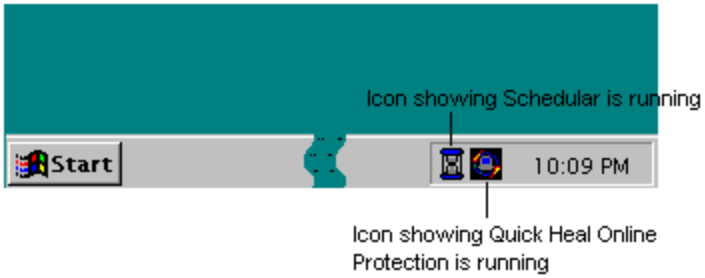
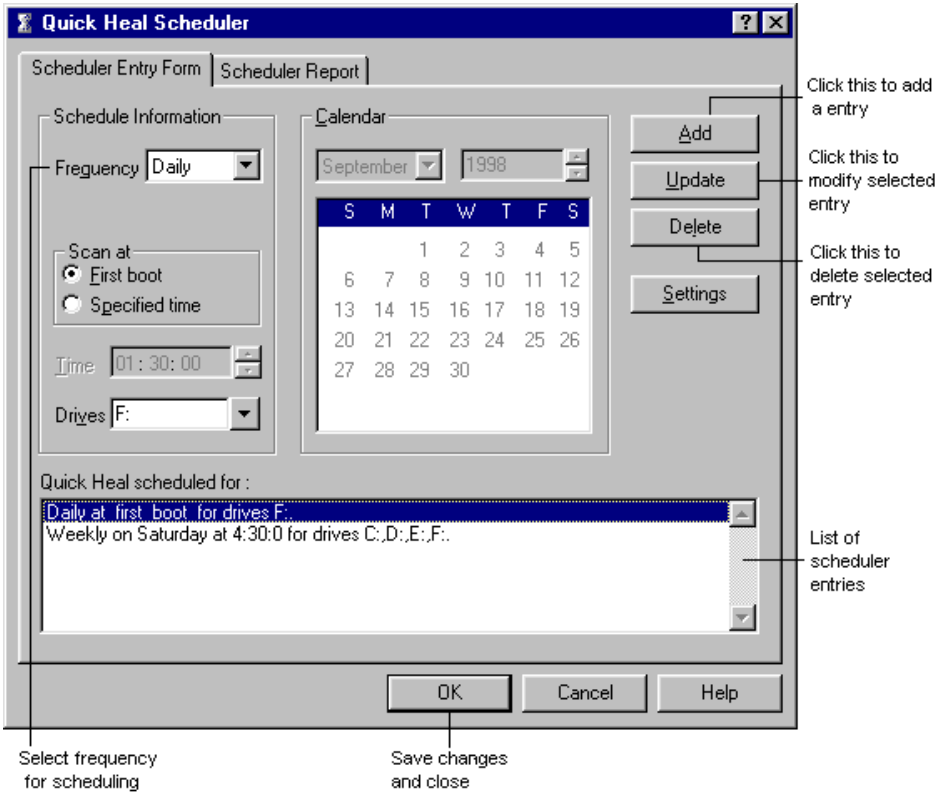


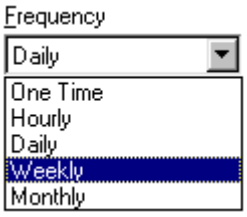
Figure 2-8 Quick Heal Scheduler Entry Form



To schedule virus scans:

- Select how often you want the scan to occur in the frequency drop down list box from Schedule Information group (see Figure 2-9).
- Accordingly enter the correct time, day, or date information, if necessary. You can also select to scan at First Boot instead of Specified time.
- Select drive letters from Drives drop down list box to scan.
- If you need special scanner configuration for this scheduled scan you can change the scanner settings by clicking the Settings button.
- Click Add button to add the schedule scan entry.
- Click OK to confirm.

Figure 2-9 Schedule Frequency



To modify scheduled virus scans:

1. Click the entry you want to modify from the list box.
2. Modify the date, time or other information if necessary.
3. Click Update button.
4. Click OK to confirm.

To delete scheduled virus scans:

1. Click the entry you want to delete from the list box.
2. Click Delete button.
3. Click OK to confirm.

To close scheduler:

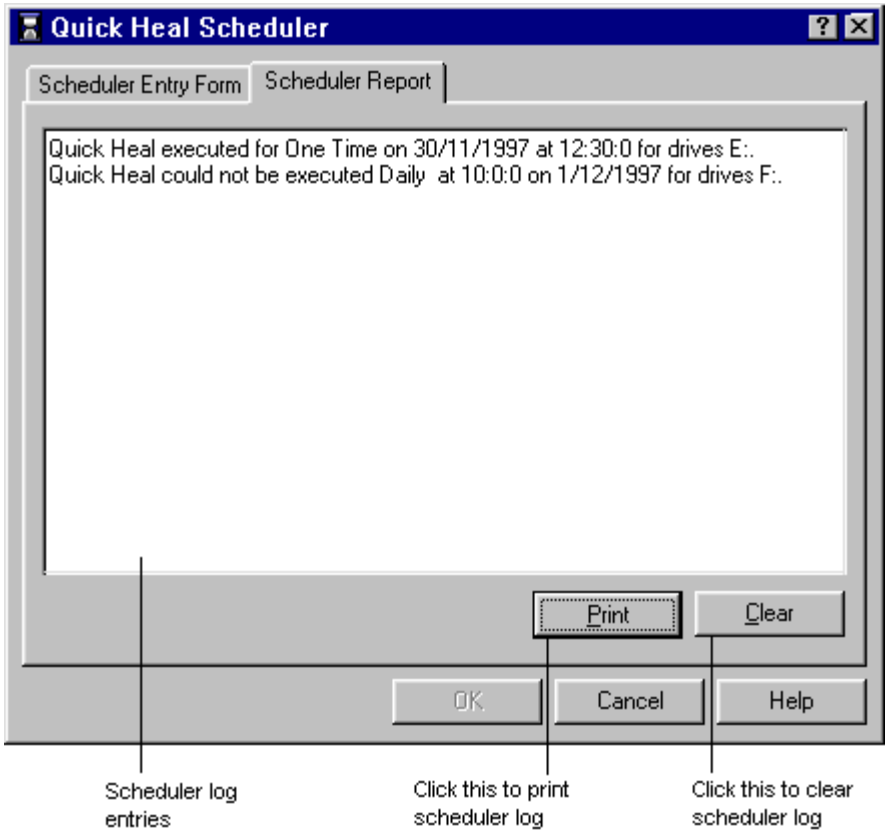
1. Right clicks the scheduler icon on task bar.
2. Click Close.

You can also configure Quick Heal scanner options by right clicking scheduler icon on task bar.

Once you have scheduled the scanner, the scheduler should be loaded for scheduling the scans. For this, you can configure the scheduler to get loaded every time you start Windows so that you are sure it is always loaded (see “Customizing Startup Options” on page 38).

After a scheduled scan is over, the scheduler maintains a log indicating status of the scan. To view scheduled scan report go to Scheduler Report tab in scheduler window (see Figure 2-10).

Figure 2-10 Scheduler Report



Enabling and disabling On-line Protection

Quick Heal On-line protection is configured to load whenever you start your computer. The On-line Protection icon appears on the Windows taskbar (see Figure 2-7). On-line Protection prevents your system from virus attack by continuously monitoring the system for virus like activities and scanning the files before you use them. All this is done in the background and you are notified only when a virus infected file is found or a virus like activity is detected.

Loading On-line Protection

To load On-line Protection every time you start your computer:

1. In Quick Heal main window, Click Options button on toolbar.
2. Click the Startup tab.
3. Check Load On-line Protection System at Startup.
4. Click OK.

On-line Protection is enabled immediately and every time your computer starts-up thereafter.

To load On-line Protection for current Windows session:

You can access the scheduler in any one of the following ways:

- Click On-line Protection button from Quick Heal toolbar.
- Choose On-line Protection in Quick Heal group from Start menu.

Disabling On-line Protection

Generally, we recommend that you never disable Quick Heal On-line Protection.

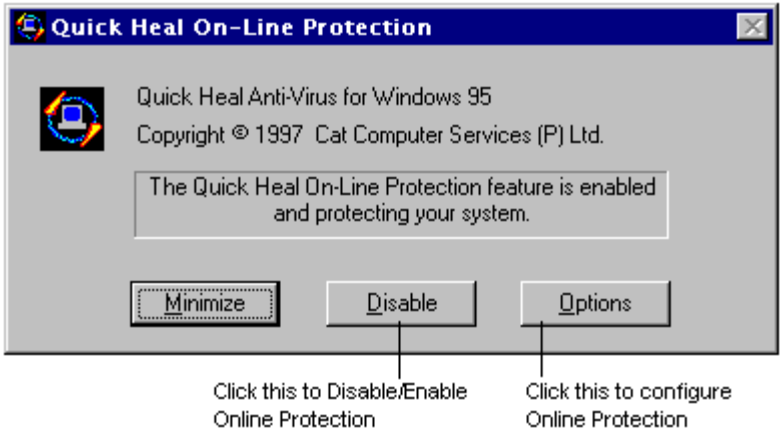
Occasionally, such as when you are installing a program, which warns to disable any anti-virus protection at the time of installation, you can disable On-line Protection.

You can disable On-line Protection temporarily or permanently.

To disable On-line Protection temporarily:

1. Double-click the On-line Protection icon on the Windows task bar.
2. Click Disable button in the On-line Protection windows that appears. (see Figure 2-11). The button changes to Enable and icon also indicates the disable status.
3. Click Minimize to close the On-line Protection dialog box.

Figure 2-11 Quick Heal On-line Protection dialog box



To disable On-line Protection permanently:

1. Double-click the On-line Protection icon on the Windows task bar.
2. Click Options button.
3. Click the Startup tab.
4. Uncheck Load On-line Protection system on startup.
5. Click OK.

On-line Protection will not be loaded, when you start your system next time.

To enable On-line Protection from the disabled state:

1. Double-click the On-line Protection icon on the Windows task bar.
2. Click Enable button in the On-line Protection windows that appears. The button changes to Disable and icon also indicates the enabled state.
3. Click Minimize to close the On-line Protection dialog box.

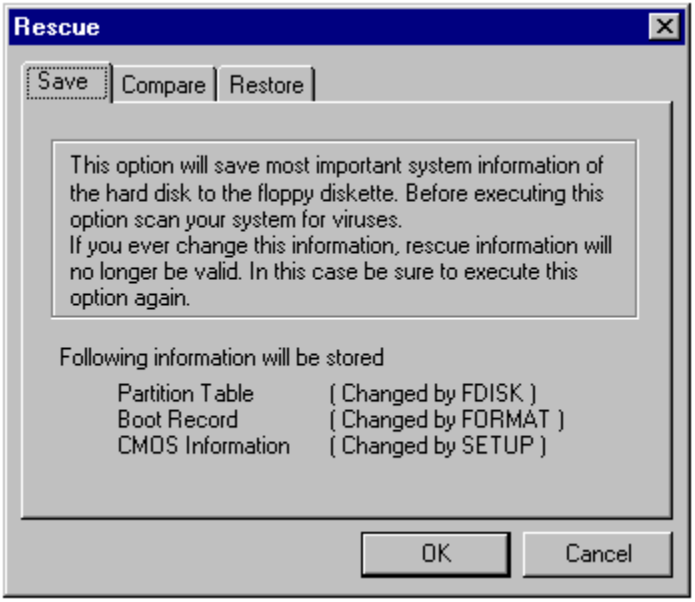
Creating Rescue Disk On Windows 95/98

Rescue Disk plays an important role while recovering from a virus attack, especially boot virus attacks or disk corruption due to bugs in the viruses. Quick Heal Rescue Utility saves most important system information of your hard disk on to the rescue disk. It also saves the programs required to boot your system. Quick Heal prompts you to create the Rescue Disk at the time of installation. If you had opted not to create the rescue disk during installation, create it now. Before creating a rescue disk, you should scan your system for viruses to verify that it is free of viruses.

To Create a Rescue Disk:

1. In Quick Heal main window, click Rescue button on toolbar.
2. Click the Save tab (see Figure 2-12).
3. Click OK.
4. Insert the Quick Heal Rescue Disk in any of the floppy drive(s).
5. Select the drive in which you have inserted the Rescue Disk and click OK.

Figure 2-12 Rescue Information dialog box



The rescue utility will format the rescue disk, transfer the system and copy information regarding partition table, boot records and CMOS settings along with few other important files on to the disk.

NOTE: If you ever change this important information of your hard disk, the information on your rescue disk will no longer be valid. In this case be sure to save the rescue information again.

Creating Rescue Disk On Windows NT

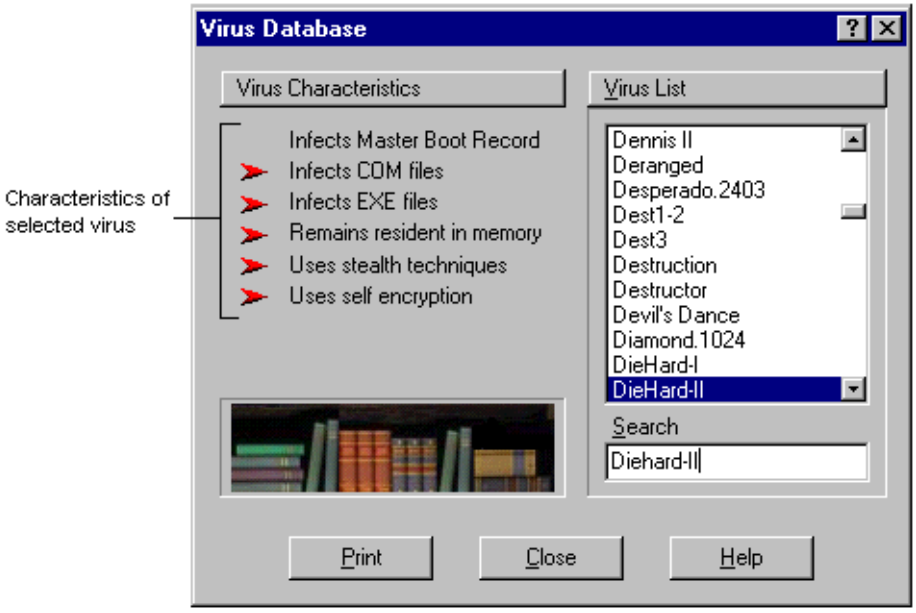
To create Rescue Disk on Windows NT use the Repair Disk utility which is provided with Windows NT. This utility is used to make an Emergency Repair Disk for Windows NT and is located in SYSTEM32 directory of Windows NT system. The Repair Disk utility saves all of your current system settings to an Emergency Repair Disk (ERD). You can then use this disk to restore your computer if files become damaged. It is strongly recommended that you create and update an ERD every time you make significant changes to your hardware or software setup.

The repair information on Emergency Repair Disk can be used to reconstruct your Windows NT system files, system configuration and startup environment variables if they become damaged.

Viewing the Virus List

Quick Heal Virus List provides you with the overview of the characteristics of each virus. (see Figure 2-13)

Figure 2-13 Quick Heal Virus List



To view the virus list:

- Click Virus List in Quick Heal main window.

The dialog box displaying the virus list will appear.

List of most important characteristics of viruses appears to the left in the dialog box. A red marker before the characteristic indicates that the selected virus is having that characteristic.

To search for a virus in the virus list:

1. Activate the search edit control box by clicking inside the edit box below the list box or by pressing Alt+S.
2. Start typing the name of virus you want to find.
3. The virus that you are searching for will get highlighted and its characteristics will be marked in the Virus Characteristics group.

Click Print to print the virus list to a printer or to a file.

Using Quick Heal Toolbar

You can use Quick Heal Toolbar for single-click access to the procedures you use most often. You can drag the Toolbar to any location on screen. If the Toolbar is docked you can hide it until you need it by clicking Auto Hide on the menu that appears when right clicked on it. When you want to use the Toolbar again, point to the side of the screen where it is docked.

If the Toolbar is not already loaded, you can load it from the Quick Heal group. You can also customize the Toolbar to run automatically when you start Windows (see “Customizing Startup Options” on page 38).

Toolbar provides following buttons that help you use Quick Heal more easily:


This is used to activate Quick Heal scanner.

This will scan the diskette in Drive A.

This will scan the diskette in Drive B.


This is used to load Quick Heal Online Protection.


This is used to load Quick Heal Scheduler.


This is to exit from Quick Bar.

Chapter Three

Customizing Quick Heal

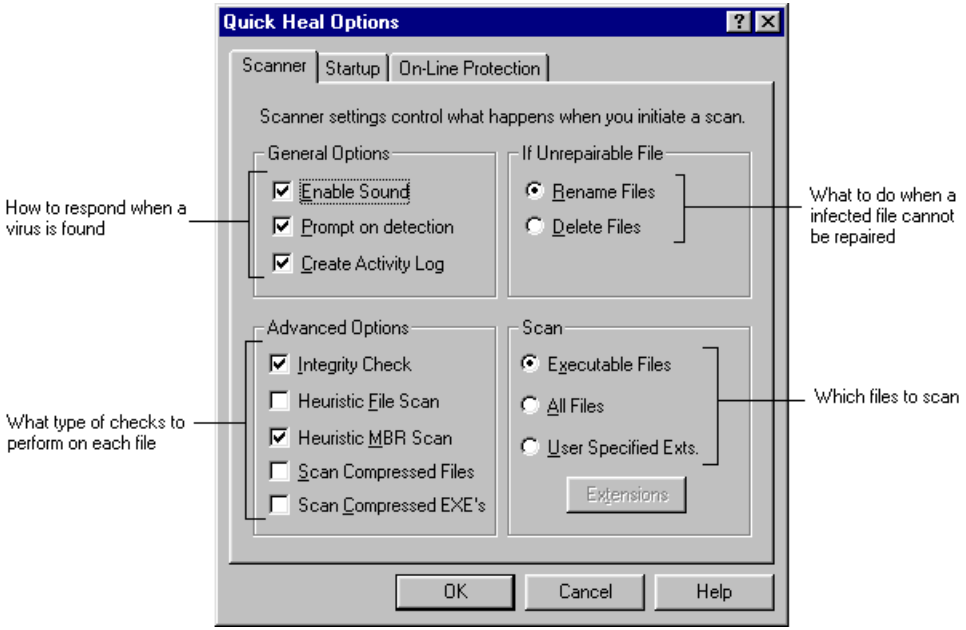
Quick Heal is provided with various options for customizing as per your protection requirements. By default, Quick Heal is configured to provide the idle protection for most of the computing environments. We recommend you not to change these preset options unless specifically required.

Customizing Scan Options

The Scanner settings will affect the scanning done during manual scans or when scheduled scans occur. For configuring the scanner you need to be in the scanner options window. To bring the scanner options window:

1. Load Quick Heal
2. Click Options in Quick Heal's main window.
3. Click Scanner tab (see Figure 3-1)

Figure 3-1 Scanner Settings



Customizing how to respond when a virus is found

Following settings can be seen in General Options group.

Enable Sound: When selected, gives an audio alarm on detection of a virus or occurrence of an error.

Prompt on detection: When selected, informs you when a virus is found and allows you to select what to do with the virus.

Create Activity Log: When selected, the scanner creates a log entry for each scan. Each entry consists of a summary about the scan. Details about each scan and virus-found events are also maintained in separate files. You can view the activity log entries later. (see "Viewing Activity Log" on page 21)

Customizing how to handle unrepairable files

Quick Heal is designed with in-built intelligence to analyze if the file can be disinfected safely or not. A file may not be recoverable due to following reasons

- The virus has destroyed file by overwriting certain areas of the file.
- It is a new variant of the virus.

In such cases, virus removal may finally result into a non-working executable file. You can configure Quick Heal to either rename or delete the unrepairable files.

If you have selected to rename the unrepairable files, the first character of the extension is changed to V. Thus, EXE becomes VXE, COM becomes VOM and so on. This helps the user in identifying the files later and sending them for further research. It also prevents the accidental use of such files.

If you have selected to delete the unrepairable files, Quick Heal goes on deleting all such files.

Customizing Advanced Options

The Advanced options determine how to perform a scan. You can set following options as per your requirements.

- **Integrity Check**: Quick Heal offers an extra level of protection against unknown viruses using Integrity Check. When this option is selected Quick Heal stores critical information within the file for later reference. Quick Heal then monitors for any changes in the file integrity by using this stored data.

- **Heuristic File Scan**: When this option is selected Quick Heal searches for virus-like code in the file. This helps you detect possible infection by an unknown virus. As it searches for virus-like code, it may give false alarms. Here are some possible reasons when you may get false alarms.

  1. Files belonging to the anti-virus programs.
  2. Files containing some TSR code, etc.

  In case you get a warning, check if the virus is spreading to other files. If not, ignore the warning for that particular file.

  As far as possible, heuristic scanning should be performed on new files only. This will provide you with an ideal mix of security and convenience.

- **Heuristic MBR Scan**: When this option is selected Quick Heal scans for infection by an unknown Boot / Partition virus, by searching virus like code in the Master Boot Record.

- **Scan Compressed Files**: When this option is selected Quick Heal scans files inside the compressed files. Quick Heal can scan files compressed using popular compression utilities like ZIP and ARJ. Compressed files within compressed files are also scanned. Scanning inside compressed files increases scanning time. Quick Heal can detect the virus (if any) inside compressed file, however it cannot remove the virus from these files. You are advised to decompress such files, remove the viruses from them and compress the same again. This will ensure that the compressed copy is also virus free.

- **Scan Compressed EXE's**: When this option is selected Quick Heal scans internal EXE's compressed using popular executable file compressor LZEXE.

Customizing which files to scan

You can specify which files to scan by specifying their extensions. By default Quick Heal scans for the executable extensions. Scanning executable files is adequate in most of the situations as viruses only infect and spread from these types of files.

- Executables only: It covers the most common executable extensions only. They include .COM, .EXE, .SYS, .OVL, .OVR, .DRV, .386, .DLL.

- All files: Certain programs do not store the executable files by their normal extensions. This option would scan all the files irrespective of their extension or type (executable or data file). This may reduce the scanning speed and hence is recommended only after a virus attack is discovered.

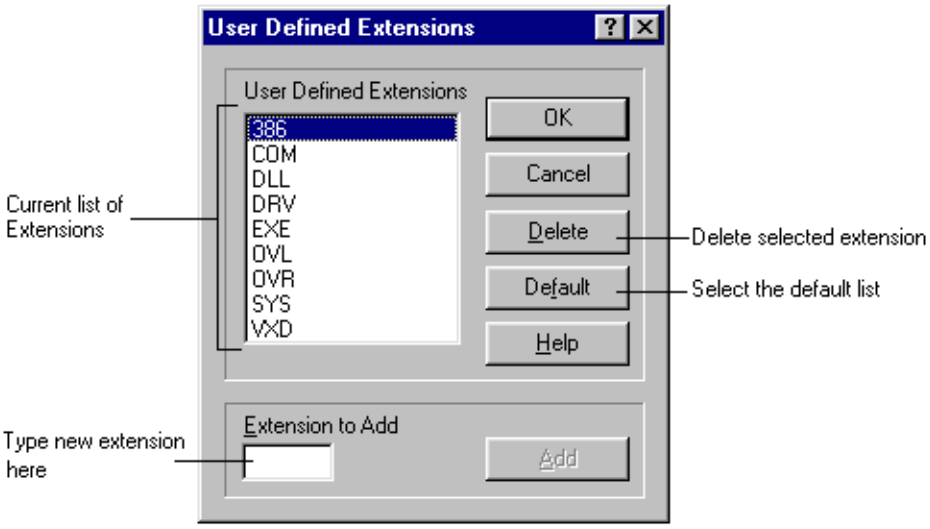
- User Specified: This choice allows you to specify extensions of the files to be scanned. On selecting this option you can enter the executable file extensions of your choice. From the next scan, the scanner will scan all the files with these extensions.

Specifying file extensions

1. elect User Specified Extensions in Scan group box.
2. Click Extensions in the Scanner Settings Tab. The User Specified Extensions dialog box appears (see Figure 3-2).

The default list includes most of the program file extensions. In case some of your applications use some other extensions add them to the list.

Figure 3-2 User Specified Extensions dialog box



To add a program file extension:

1. Click in the Extension To Add text box.
2. Type the extension.
3. Click Add.

To Remove a program file extensions:

1. Select the file extensions in the User Defined Extensions list box.
2. Click Delete.

To reintroduce the original list:

1. Click on Default.

Default list of extensions include COM, EXE, SYS, OVL, OVR, DLL, 386, DRV and VXD.

Customizing Startup Options

It is very important to check for viruses when you start (boot) your system. This prevents viruses from getting in memory and there by preventing further spreading of the virus. Also it is important that various components of Quick Heal get loaded automatically every time you start your system.

To customize system startup protection:

1. Click Options in Quick Heal's main window.
2. Click the Startup tab.

   (see Figure 3-3)

Figure 3-3a Startup Settings for Windows 95/98

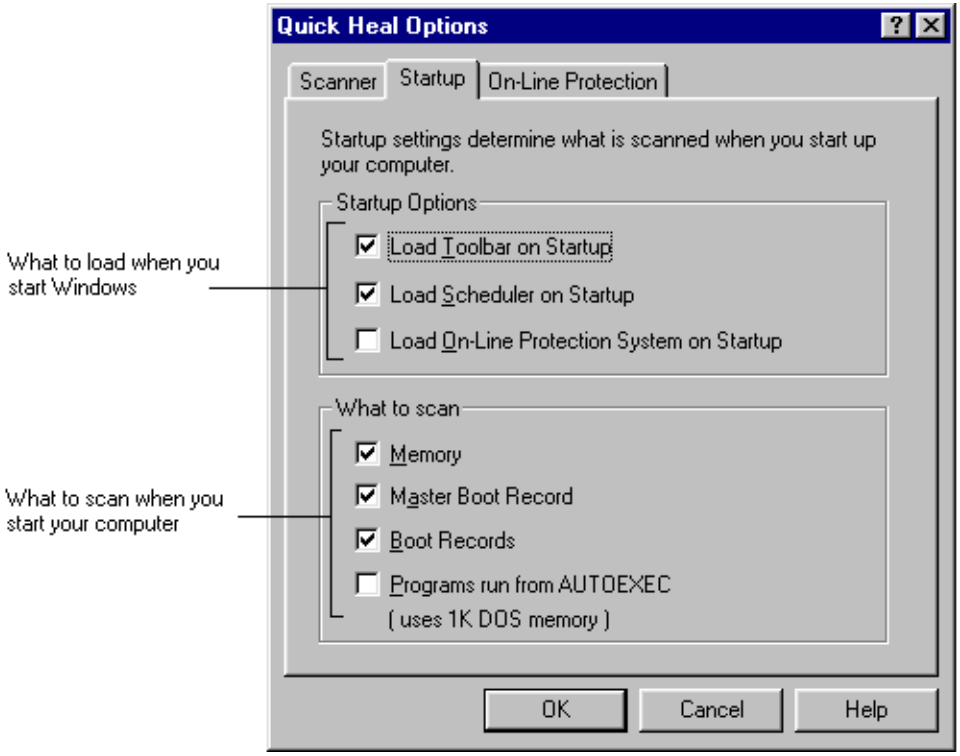
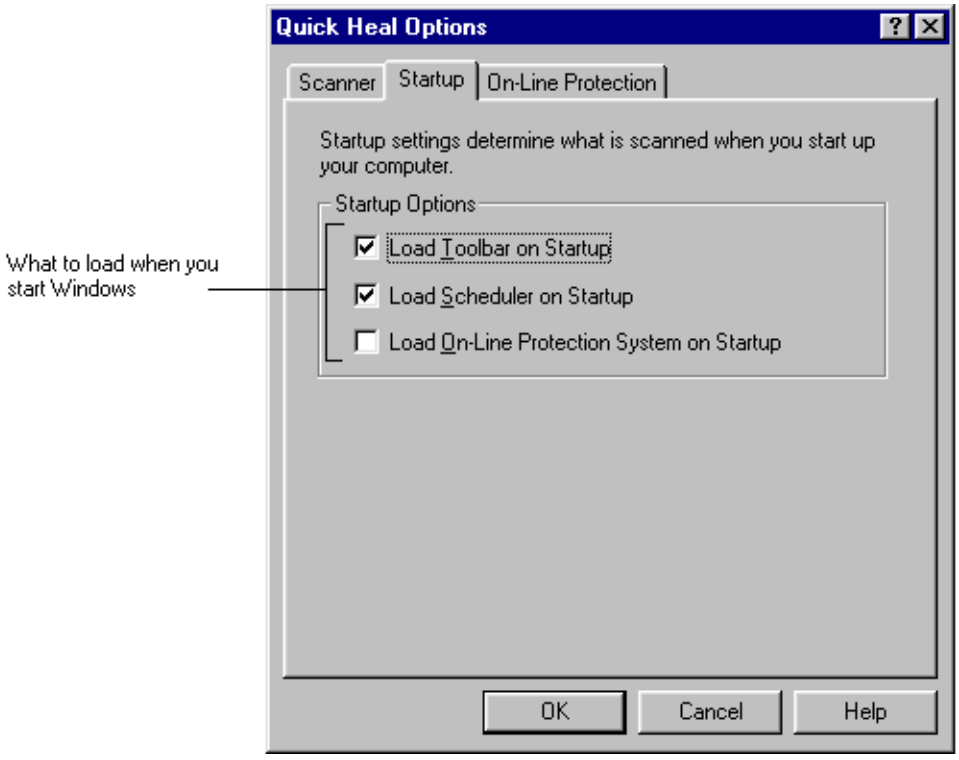


Figure 3-3b Startup Settings for Windows NT



Specifying what components to load at the startup

The components that can be loaded at the time of startup are:

- Toolbar: Always on top shortcut bar, which gives easy access for Quick Heal components.
- Scheduler: Quick Heal scheduler for scheduling virus scan.
- On-line Protection: This will provide continuous protection in background.

Specifying what to scan at startup (for Windows 95/98 only)

On Windows 95/98, Quick Heal provides additional facilities to scan the system when it starts. In What to Scan group box specify the areas that you want Quick Heal to scan each time you start your computer.

- **Memory**: Scans for viruses resident in your computer's memory. Viruses in memory can spread to other files you access.
- **Master Boot Record**: Scans for boot viruses in the master boot record.
- **Boot Records**: Scans for boot viruses in the boot records on your hard disk.
- **Programs run from AUTOEXEC**: Scans programs that load before Windows 95 loads preventing viruses from getting into the system before the On-line Protection system gets loaded. This will load a DOS based device driver through CONFIG.SYS.

Customizing On-line Protection

Quick Heal's On-line Protection continuously scans the system and prevents virus infection from:

- Email Attachments
- Internet Download
- Network
- File Execution and Copying
- Use of infected floppy disks

To Customize On-line Protection:

1. Click Options in Quick Heal's main window.
2. Click the On-line Protection tab (see Figure 3-4).

Figure 3-4a On-line Protection Settings for Windows 95/98

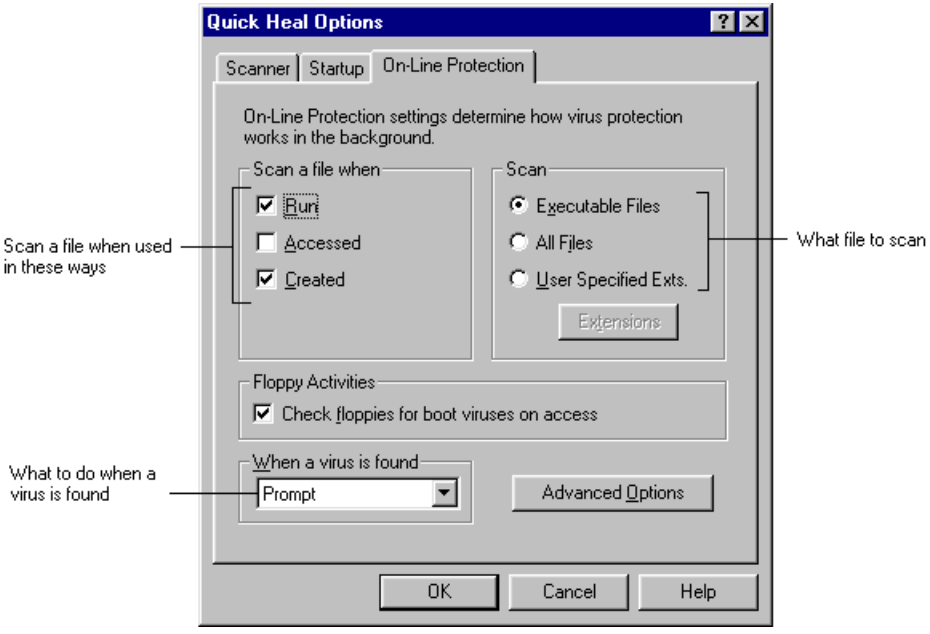
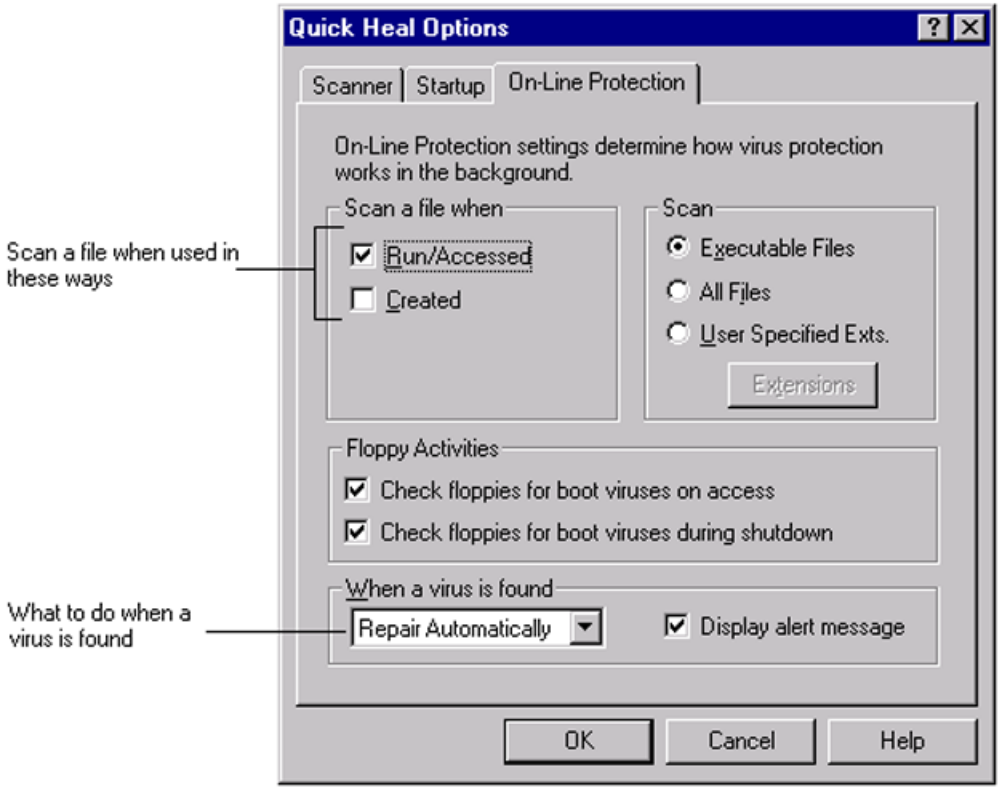


Figure 3-4b On-line Protection Settings for Windows NT



Specifying when to scan a file On-line

In 'Scan a file when' group box you can select amongst the following options:

- Run: Scans a program file each time you execute it.
- Accessed: Scans files when they are accessed. For example, a file is scanned while copying.
- Created: Scans files when they are created on your drive by an installation program, by decompressing files or by downloading files from an internet site.

Specifying which files to scan On-line

In Scan group box you can select amongst the following options:

- Executable Files: Scans files that are most likely to get infected by a virus.
- All files: Scans all files including executable files as well as data files.
- User Specified Extensions: Scans the files with the extension that are listed in the User Specified Extensions list box. You can invoke the User Specified Extensions dialog box by selecting User Specified Extensions and clicking on the Extensions button. Here you can view and modify the extensions in the list. For more information on how to add new extension to Extensions list refer to “Specifying file extensions” on page 36.

Specifying how to respond when a virus is found On-line

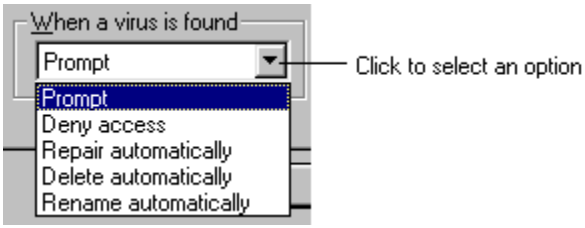
In When A Virus Is Found drop down list box you can select one of the following options (see Figure 3-5):

- Prompt: Informs you when a virus is found and allows you to choose how to respond. When prompted you can select to :
  - Remove the virus and continue with the file activity.
  - Delete the file and stop the file activity.
  - Keep the virus and continue the file activity.
  - Stop the particular file activity.

  This option is not available on Windows NT.
- Deny Access: Prevents you from using a virus-infected file.
- Repair Automatically: Removes a virus from infected file without notifying you. Before repairing a virus infected file, Quick Heal makes a backup copy of that file with .VIR extension.
- Delete Automatically: Deletes a virus-infected file without notifying you. Once deleted these files cannot be recovered.
- Rename Automatically: Renames a virus-infected file without notifying you.

A record is maintained for each activity and corresponding action taken against the virus.

Figure 3-5 What to do When A Virus Is Found list box



Monitoring for boot viruses

If the Check Floppies for Boot viruses option is selected Quick Heal's On-line protection will check for boot viruses in every floppy you use. This will prevent spreading of boot viruses through floppy disks.

To monitor floppy disk activities:

1. Click Options in Quick Heal main window.
2. Click the On-line protection tab.
3. In the Floppy Activities group box select the Check Floppies for Boot viruses option.
4. Click OK to close the dialog box.

On Windows NT, Quick Heal scans for boot viruses in all the floppy disk drives during shut down.

To check floppy disk during Shut Down:

1. Click Options in Quick Heal main window.
2. Click the On-line protection tab.
3. In the Floppy Activities group box select the Check Floppies for Boot viruses during Shut Down option.
4. Click OK to close the dialog box.

Checking for virus-like activities (for Windows 95/98 only)

On Windows 95, Quick Heals On-line protection constantly monitors your system for suspicious activities. On detection of any suspicious activity it displays a warning message, telling you exactly what is going on. A virus-like activity is an action that viruses typically perform when damaging your files or spreading through your system. Although some applications perform these actions for valid reasons, we can keep check on such activities to prevent them from being performed by an unknown virus.

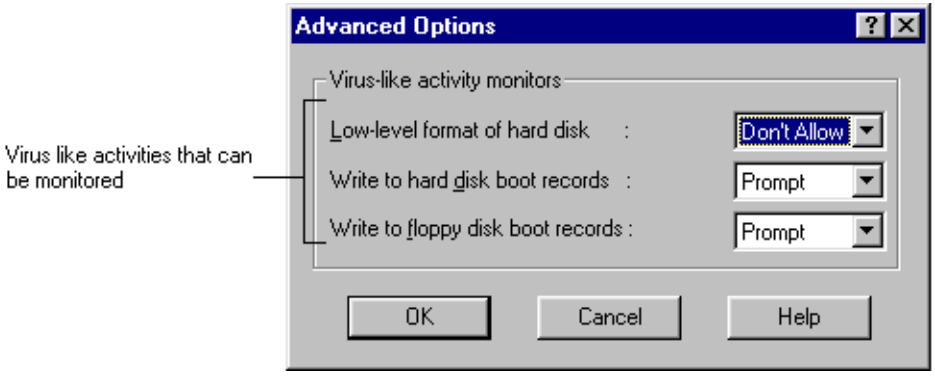
Quick Heals On-line protection monitors for following virus-like activities

- Low-level Format of hard disk: All information on the disk is erased and cannot be recovered. This activity certainly indicates presence of an unknown virus.
- Write to Hard Disk boot records: There are very few programs that write to hard disk boot record. Unless you are specifically using the program that writes to the hard disk boot records, such as FORMAT, this activity probably indicates a virus.
- Write to Floppy Disk boot records: There are very few programs that write to floppy disk boot record. Unless you are specifically using the program that writes to the floppy disk boot records, such as FORMAT, SYS this activity probably indicates a virus.

To monitor for virus-like activities:

1. Click Options in Quick Heal's main window.
2. Click the On-line protection tab.
3. Click Advanced Options in On-line protection tab (see Figure 3-4).
4. The Advanced Options dialog box appears (see Figure 3-6).
5. Select monitoring options in each drop down list box to specify what to do when a virus like activity is detected.

Figure 3-6 On-line Protection Advanced Options



You can customize what should the On-line Protection do if it detects some application performing such activities. For each virus-like, you can select amongst following options:

- **Allow**: Allows the activity to continue every time without informing you. Selecting this option will not provide any protection against an unknown virus performing the activity.
- **Prompt**: Warns you when a program tries to perform the activity and prompts you to take appropriate action. (see “On-line Protection virus-like activity alerts” on page 53.)
- **Don’t Allow**: Prevents the activity from occurring every time it is detected.

Chapter Four

Cleaning Viruses

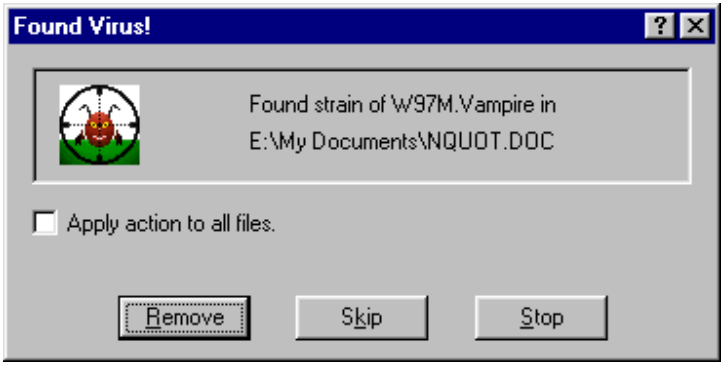
Quick Heal warns you for a virus infection when:

- A virus encountered during a manual or scheduled scan.
- A virus encountered in the memory.
- A virus encountered by Quick Heal On-line Protection.
- A virus detected through Start-up Scan.

Cleaning viruses encountered during scans:

If a virus is detected during a scan, Quick Heal pops up for you to select the right option. For known viruses the window is (see Figure 4-1).

Figure 4-1 Virus found alert from integrated scanner

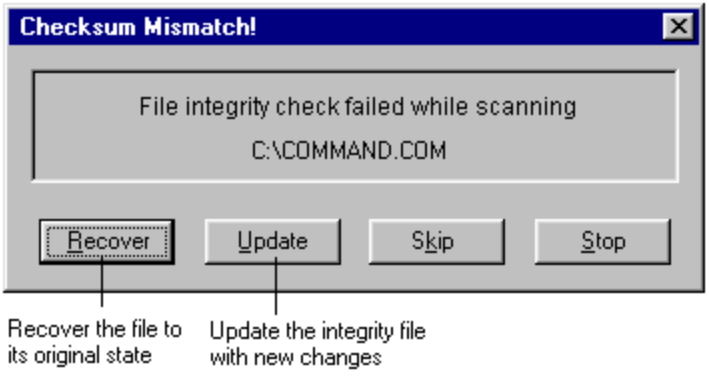


Button	Action
Remove	Removes the virus and returns the infected file or Boot record to its original state. Choose this button if you wish to remove the viruses manually one at a time.
Skip	Does not remove the virus and continue scanning.
Stop	Stop scanning and return to the main window.

If Apply Action to All Files check box is selected then scanner will go in auto mode and will automatically remove viruses without prompting for action to be taken.

During the scan if Quick Heal's integrity checker detects any change in the file integrity it will warn for possible unknown virus. It displays following alert message:

Figure 4-2 Checksum mismatch alert from integrated scanner.



Button	Action
Recover	Tries to recover the file using the integrity information saved previously.
Update	Updates the integrity data file with the new file information and leaves the file as it is
Skip	To skip this warning and keep the file as it is. Integrity checker will again warn you next time you scan the file while integrity check option in on.
Stop	To stop the scan.

Cleaning virus encountered in memory

A virus in memory means that the virus is active, spreading to other files, and doing its damaging activities. When Quick Heal detects a virus in memory, it warns in the following way:

Figure 4-3 Virus active in memory alert from integrated scanner

At this stage shut down and restart the machine. Try to scan once again. If you still get the same message, it means that the virus is getting activated from the startup files. Use Emergency Diskette for virus removal (Refer to chapter 5 - Using Quick Heal Emergency and Rescue Disk)

Cleaning the virus encountered by macro-virus protection

When Quick Heal macro-virus protection detects a virus in the document, it automatically removes the virus from the document by deleting all the macros related with the virus.

Cleaning viruses encountered in startup scan

Startup scan scans your computer system areas like Partition/Boot sectors and system files. It also detects any changes done to these areas and thus catches any unknown/new virus. Startup scan verifies the Partition Table and the Boot Sector by comparing it with the original image stored at the time of installation.

Startup scan will warn you when:

- A virus is found in memory.
- A change is detected in Partition Table or Boot Record.
- A change is detected in system files (IO.SYS, COMMAND.COM..).

When a Startup scan warning message is flashed, we request you to read the message in the dialog box to understand the type of problem and respond accordingly.

Responding to Startup scan virus in memory alert

When a virus is detected in memory at the time of Startup scan following warning is flashed.

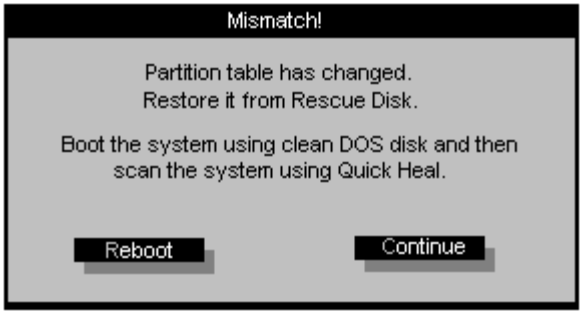
Figure 4-4 Virus in memory alert from the Startup scan

At this stage shut down the computer and use Emergency Disk for removing virus from the system. (Refer to chapter 5 - Using Quick Heal Emergency and Rescue Disk)

Responding to Partition table/Boot record changes

When a change is detected in Partition table following warning is flashed.

Figure 4-5 Partition table changed alert from the Startup scan



When a change is detected in Boot record following warning is flashed.

Figure 4-6 Boot record changed alert from the Startup scan

Your systems boot record may change if :

- You upgrade or reinstall your operating system. For example, you run a Windows 95 upgrade patch program.
- You install new operating system.
- You are using a program that makes changes to system files.

It may be either a new virus or the area might have been damaged due to some other reasons. In both the cases use rescue diskette to restore the original information.

(Refer to chapter 5 - Using Quick Heal Emergency and Rescue Disk)

Responding to virus found alerts from On-line Protection:

Quick Heal On-line Protection continuously scans your system for viruses in the background as you work. It will display a warning screen whenever it comes across a virus or a virus like activity. This screen will appear in character mode and will stop your system until you respond to the warning.

On-line protection will warn you when:

- A virus is found in a program you are trying to execute or a program file you are trying to copy (depending on the On-line protection settings. See “Specifying how to respond when a virus is found On-line” on page 43).
- A virus-like activity is detected (depending on the On-line protection settings. See “Checking for virus-like activities” on page 45).

On-line Protection Virus found alert

If a virus is found in a program you are trying to execute or trying to copy a following warning message is flashed.

Figure 4-7 Virus found alert from the On-line protection

Button	Action
Stop	Stops the execution or copying process of the infected file.
Remove	Removes the virus from infected file.
Delete	Deletes the infected file.
Continue	Continues with the execution or copying process of the infected file. This will let the virus go and spread in your system.

We recommend you to select the Remove button to prevent the spreading of the virus to other files or disks. This verifies that the virus is not present, in other files or disks.

Virus found on file creation

If a virus is found in a program you have just extracted or downloaded from the internet or being created by any other program (e.g. installation programs, compression utilities, etc.) a warning message is flashed (see Figure 4-7).

Button	Action
Stop	This will not allow you to create the infected file for which the warning was flashed.

Remove	To remove the virus from the infected file
Delete	This will delete the newly created infected file for which the warning was flashed.
Continue	This will allow creating the file without any action. You can leave the specified file as it is to remove the virus later by using Quick Heal scanner (see “To scan a file” on page 20).

Boot virus found in a floppy disk

If a boot virus is found in a floppy disk boot record a following warning message is flashed.

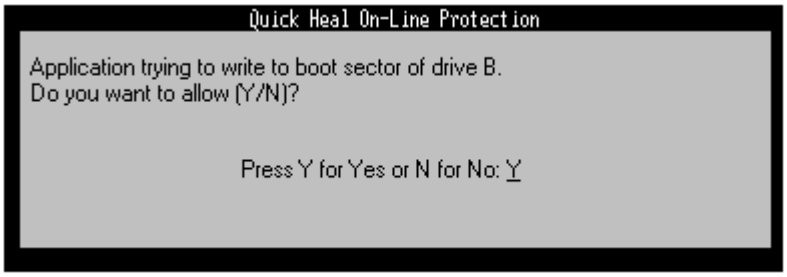
Figure 4-8 Boot virus found alert from the On-line protection

When such a alert message is flashed it means the floppy disk you just inserted in the drive is infected by a boot virus. Remove the disk and press Enter. To remove the virus, run Quick Heal and scan the infected floppy disk.

On-line protection virus-like activity alerts

If a virus-like activity is detected by Quick Heal On-line protection, it displays a warning screen depending upon the options set for that particular virus like activity (see “Customizing On-line protection” on page 41). If On-line protection is configured to prompt for virus-like activity, a warning screen will appear when any such activity is detected and will stop your system until you respond to the warning.

Figure 4.9 Virus-like activity alert from the On-line protection



A virus-like activity warning does not necessarily mean your computer has a virus. It is simply an indication. We recommend you to decide whether the operation is valid in the context in which it occurred.

Responding to virus-like activity alert

In all virus-like activity alert messages, you are prompted to continue with the activity or to stop the activity if you have customize to **Prompt** for the particular virus like activity (see "Checking for virus-like activities" on page 45). In this case you can respond by pressing 'Y' (Yes) to allow the activity to be performed and 'N' (No) to don't let the activity to be performed.

If you have customized the virus-like activity to Don't Allow (see "Checking for virus-like activities" on page 45), a alert message will be given indicating that the particular virus-like activity occurred and was stopped.

Chapter Five

Using Quick Heal Emergency and Rescue disk

Quick Heal Emergency and Rescue disks play a vital role when your computer is badly infected by a virus. In such a case, the startup scan detects a known or unknown virus in your system or the scanner detects the virus in memory. You are unable to start Quick Heal scanner and remove the virus. The worst case is that you are unable to start your system or access your hard disk due to infection by a virus.

Using Quick Heal Emergency Disk

Quick Heal Emergency Disk is used to remove viruses from your system when it is already infected by some virus (before installation) or when Quick Heal detects a virus in memory. You are recommended to shutdown your system, boot the system using Rescue Disk and then use Quick Heal DOS scanner from Emergency Disk to remove viruses.

To remove viruses using Quick Heal Emergency Disk

1. Shutdown your computer by choosing Shutdown from the Start menu on the Windows taskbar.
2. Switch off the computer. This will remove any viruses that might be present in memory.
3. Insert Quick Heal Rescue disk in drive A: and switch on the computer.

In case you have not created the Rescue disk during installation, you can also use the Windows 95/98 Startup Disk that is created during installation of Windows 95/98. In case of Windows NT, use Emergency Repair Disk. If you don't have a Startup Disk or Emergency Repair Disk, you can also use an uninfected, write-protected, bootable floppy disk of DOS version 3.3 or later (Non-DOS partitions will not be accessible in this case).

4. When your system gets booted and comes to the command prompt, insert the Quick Heal Emergency disk.
5. Type QH /a at the DOS prompt and press Enter.

6. Quick Heal will scan all the hard drives of your system and will prompt when the virus is found.

7. Remove the viruses by selecting proper button on the dialog. See “Cleaning viruses encountered during scans” on page 47 for information on how to remove the virus.

8. When Quick Heal removes all the viruses and completes the scan, remove the disk in drive A: and reboot your computer.

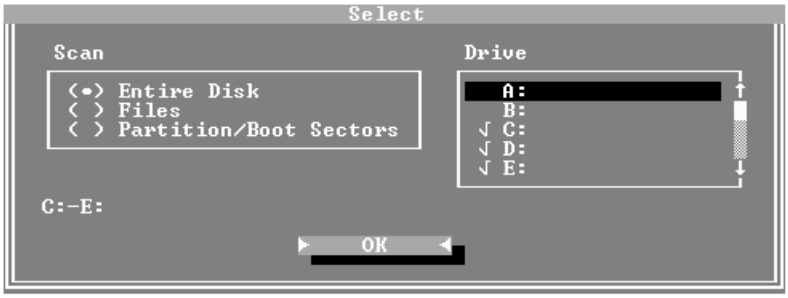
9. After restarting your system, start Quick Heal and scan all hard drives again.

While starting Quick Heal from Emergency disk if you do not specify the ‘/a’ parameter indicating scan all drives, Quick Heal main menu will be displayed.

Figure 6-1 Quick Heal DOS based scanner

On selecting Drives command from Scan menu Select drives dialog box will be displayed. Here select all the hard drives to scan. To select a drive move the highlight bar on the drive letter you want to select and press space bar. After marking all the hard drives to scan just press Enter to select OK for scan.

Figure 6-2 Select Drive dialog box



Using Quick Heal Rescue Disk On Windows 95/98

Quick Heal Rescue disk is very important at the time of recovering from a virus attack or in some other emergencies. It stores most important system information and few important system files that will help you to boot the computer and recover from most of the boot virus infection.

At the time of installation Quick Heal by default creates the rescue disk. If you have not created the Rescue disk, do it now (see "Creating Rescue disk on Windows 95/98" on page 28).

There are few situations when a virus damages critical system information of your computer and it cannot be recovered. You can use Quick Heal Rescue disk to recover from such emergencies.

To restore rescue information, you must have created rescue disk previously. The rescue information consists of following information other than important system files:

Partition Table This includes your systems Master Boot Record and other extended partition tables if any.

Boot Record This includes first logical sector of all the logical drives of your hard disk.

CMOS Information This contains your computer hardware configuration stored in CMOS Setup.

To restore rescue information of your hard disk:

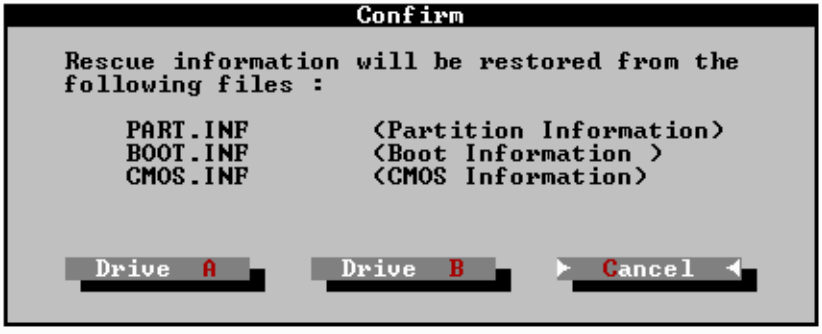
1. Shutdown your computer by choosing Shutdown from the Start menu on the Windows taskbar.
2. Switch off the computer. This will remove any viruses that might be present in memory.
3. Insert the Rescue Disk in drive A: and switch on your computer. Your computer will get booted from the Rescue Disk.
4. Type QHRESCUE /RESTORE at A: prompt and press Enter.

The Restore Rescue information dialog box appears (see Figure 6-3).

Figure 6-3 Restore Rescue dialog box

5. Select continue to proceed. The drive select dialog box appears (see Figure 6-4).

Figure 6-4 Select source drive dialog box



6. Select Drive A button as your Rescue Disk is in A: drive.
7. Check the items you want to restore.
8. Press Enter to proceed.
9. When the process is complete, remove the Rescue Disk from Drive A: and restart your computer.

Command-line parameters for QHRESCUE.EXE

QHRESCUE.EXE saves, compares and restores the rescue information of your system. It runs at DOS prompt of Windows 95/98 and will not work from DOS box with Windows 95/98 active.

Syntax

QHRESCUE Options

Options:

/COMPARE	To compare rescue information.
/RESTORE	To restore rescue information.
/SAVE	To save rescue information.

Using Emergency Repair Disk On Windows NT`

Windows NT Emergency Repair Disk is very important at the time of recovering from a virus attack or in some other emergencies. This can be used to reconstruct your Windows NT system files, system configuration, and startup environment variables if they become damaged.

To restore your Windows NT system using Emergency Repair Disk, you must have created Emergency Repair Disk previously. If you have not created the Rescue disk, do it now (see “Creating Rescue disk on Windows NT” on page 29).

To restore rescue information of your hard disk:

1. Shutdown your computer by choosing Shutdown from the Start menu on the Windows taskbar.
2. Switch off the computer. This will remove any viruses that might be present in memory.
3. Insert the Emergency Repair Disk in drive A: and switch on your computer. Your computer will get booted from the Rescue Disk.
4. Now follow the instructions on screen.

Chapter Six

Updating Quick Heal

Quick Heal is updated monthly as new viruses are discovered daily. To prevent newly discovered viruses from infecting your computer, you should update your copy of Quick Heal regularly. The upgrade definition file is available monthly. It is very easy to update Quick Heal using the Live Update utility given with Quick Heal.

Automatically updating Quick Heal

Using Live Update utility you can automatically update your copy of Quick Heal through Internet. For this you need to have an Internet connection facility.

To update Quick Heal automatically through Internet:

1. From Quick Heal Group select Live Update.
2. Follow the instructions and click Next button.
3. From the Locate Definition File dialog select the option of "Download from web site" (See Figure 6-1).
4. Click Next to start automatic download and update procedure.

   Live Update makes the connections, downloads the appropriate file and upgrades your copy of Quick Heal. You don't have to do anything else.

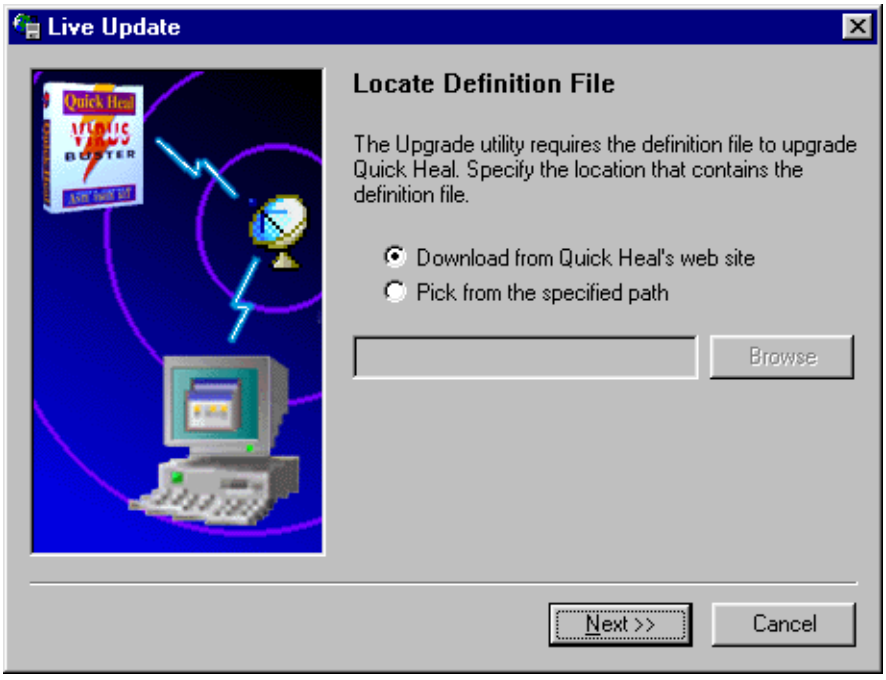
Manually updating Quick Heal

To manually update Quick Heal, you need to download the definition file from Quick Heal's web site or through variety of other sources. Once you have the definition file with you, then you can update it as follows.

To update Quick Heal manually through Internet:

1. From Quick Heal Group select Live Update.
2. Follow the instructions and click Next button.
3. From the Locate Definition File dialog select the option of "Pick from specified path" (See Figure 6-1).
4. Click Next to start update procedure.

Figure 6-1 Updating Quick Heal



Appendix A

Virus Fundamentals

The last decade has been one of tremendous upheaval in the world of computers. As processing powers have increased so have the viruses. They have become far more complex and difficult to detect. Everyday the world is confronted with new damaging viruses. With the opening up of information technology viruses are now finding it easier to spread themselves. Today viruses spread through floppies, CD-ROMS, Internet, E-mail etc.

What is a computer virus?

Computer viruses are, simply, executable computer programs. Just like a biological virus finds and attaches itself to a human host, a computer virus finds and attaches itself to an item, such as an executable file or a computer start-up area. After a computer virus attaches itself to such items, it spreads to its neighbouring items. A computer virus has three basic properties:

- It is a piece of executable code.
- It is a parasite. It never remains as a named piece of software.
- It reproduces itself, and on activation it tries to spread by attaching itself to other executable code.

A computer virus can live in the boot record, partition table, executable files (EXE, COM, OVL etc.) and data files with macro capabilities. Essentially there are three types of viruses:

- Boot sector / Partition table viruses (hereafter referred to as Boot virus): A virus that infects the boot record program on hard disks and floppy disks and / or the master boot record on the hard disks. A boot virus loads into memory before the operating system, takes control of your computer and starts infecting any floppy disks that are accessed.
- File viruses: A virus that infects the files on your hard disk or floppy disks. A File virus can either be a Program virus or a Macro virus. Program viruses are those that infect executable files by inserting instructions into the execution sequence. Macro viruses infect data files with macro capabilities. For example, Microsoft Word document and template files are susceptible to such viruses.
- Multipartite viruses: these can remain in both.

Activation of a virus

A piece of code cannot be effective unless it moves into the memory as an effective executable code. When a virus moves into the memory as an executable code, we say the virus is active in memory.

Activation of a Boot virus: A Boot virus gets itself attached in such a way that it gets activated when you start your system. This is because, while start-up the system always loads the boot / partition areas into memory and gives the control to it. As the virus resides in these areas, it automatically gets the control. After receiving the control, the virus stays resident in memory for further infections and then gives the control to the actual code from the boot / partition areas. Here onwards, the virus attaches itself to the boot sector of the floppies or to the executable files.

NOTE: A Boot virus infects a machine only if the machine is booted with an infected disk. Merely using that floppy will not lead to infection.

Activation of a Program virus: A Program virus gets activated when an infected file is executed. As the operating system loads the infected file into memory, the virus code moves into the memory along with it and gets executed. Most of the recent viruses stay in the memory even after termination of the program. Here onwards, the virus can spread itself to other files or boot / partition areas as per its capabilities and will.

NOTE: Unless an infected file is executed, the virus residing inside the file is harmless. Copying or accessing infected files do not lead to destruction or further spreading of the virus to other files.

Activation of a Macro virus: Macro viruses are not an exception to the rule that a virus is a piece of executable code. A macro virus gets activated when an infected document is loaded. While loading the document, the application also loads any accompanying macros that are contained in the file. There are some macros that the application loads automatically on meeting certain criteria. Macro viruses use this auto-execution capability of the application to gain the control. Once the virus gets the control, it waits for a new document to be edited and attaches its macros to the new document by the virtue of auto-executing macros.

The challenge from modern techniques used by viruses

Virus authors have always been trying to fool the existing virus scanners. The techniques used by them include:

Polymorphic nature: Most of the scanners detect viruses by a unique signature for each virus. To evade such style, new generation viruses keep on changing their code. This poly (many) morphic (forms) nature makes the virus identification a difficult task.

Stealth methodology: For a normal computer user, one method to detect a virus is to look at file sizes. Since the file size increases after a virus attack, the user can suspect a virus in the file and take corrective measures. Recent viruses are smart enough to hide such information and furnish the ideal information when they are active in the memory.

Anti-debug code: To make the study difficult for the anti-virus persons, many viruses employ anti-debug techniques. By using few techniques, the viruses change themselves the moment somebody tries to study them using debugging tools.

By using combinations of the above techniques, a virus can remain undetected and spread effectively.

How can you recognize a virus activity?

There are some very obvious ways. In many cases your computer starts behaving differently. This primarily happens because the virus often fiddles with the basic computer formats, directories etc. It can format the hard disk, encrypt the hard disk data, corrupt file allocation table, change screen display, hang the system, lock keyboard & floppy drives and much more.

It's imperative that computers are fitted with comprehensive anti-virus software that is also easily upgradable and has the information of the newer types of viruses afloat. The good news is that the anti virus software is catching up with viruses. With some care and the right computer protection, you can keep viruses at bay.

Appendix B

Messages in Quick Heal

This appendix contains an alphabetical list of the error messages and warnings you may see while using Quick Heal.

Convention: Actual filename, filename with full path, drive or virus name in the messages are replaced by <FILENAME>, <FILEPATH>, <DRIVE> or <VIRUS NAME>.

Access denied. Could not recover the file.

The specified file could not be accessed because the file can be in use by some other application. Try to find out which application is using the file. Close the application, and try recovering the file.

Activity log is empty.

The log file of the scanning activities is empty. This message would arrive when you are running Quick Heal for first time or when you have cleared activity log. If this message appears even after you have performed scanning, check 'Create Activity Log' flag in Scanner options.

Application trying to write to boot sector of <DRIVE>.

This activity is sometimes performed by a virus. Quick Heal's Online Protection is configured to display this message when such an activity occurs. See "On-line Protection virus-like activity alert" on page 53 for more information.

Application trying to format hard disk.

This activity is sometimes performed by a virus. Quick Heal's On-line Protection is configured to display this message when such an activity occurs. See "On-line Protection virus-like activity alerts" on page 53 for more information.

Atleast one extension should be present.

Quick Heal requires atleast one extension which should be scanned while scanning files with user specified extensions.

Bad or missing <FILENAME>.

Quick Heal was unable to locate the specified file. Ensure that the file is present in Quick Heal's directory. If the file is not present, you will have to reinstall Quick Heal.

Can not create backup file. Continue with file recovery?

This message appears while recovering the file from infection by an unknown virus. Quick Heal creates a backup of the file while it is recovering the file. Check free space on the drive.

Can not extract. Insufficient disk space.

This message appears when Quick Heal tries to extract a file in a compressed file or expand a compressed executable. Also check if you have write permission to the drive.

Can not read drive <DRIVE> ...

Quick Heal could not access the drive. Verify the drive door is closed and that the disk is formatted and free of errors.

Could not execute Quick Heal scheduled for Daily scan at ...

Scheduler was unable to schedule Quick Heal because either your machine was off during that time or the scheduler was not loaded at the scheduled time. Check if the scheduler entry is present in Startup Options.

Could not execute <MODULE NAME> !

Quick Heal could not load the specified module required to proceed with current task. The file is missing or corrupt. You will have to reinstall Quick Heal.

Could not open <FILENAME> required by Quick Heal. ...

Ensure that the file exists in Quick Heal's directory. If not, you will have to reinstall Quick Heal.

Disk is write protected...

Quick Heal is trying to write to a write protected floppy disk. Remove the write protect tag and retry.

Error writing Boot Record/Partition table.

Quick Heal was unable to write the boot record / partition table while recovering from virus infection or using rescue utility. This message can occur if the drive is write protected or you do not have write access to the drive. It can also occur if you are using a program that locks the boot / partition sector in some way, preventing Quick Heal from writing to it.

Error recovering file. Recovery data not valid.

Quick Heal has detected an unknown virus in the file and is trying to recover the file. The recovery data can mismatch if the infected file was changed after the integrity information was updated. You will have to rename or delete the file.

Found virus (<VIRUS NAME>) in file <FILEPATH>. Access denied to file.

You are trying to access / execute a virus-infected file. Quick Heal's Online Protection is configured to deny access to such files. See "Customising On-line Protection" on page 41 for more information.

Found virus (<VIRUS NAME>) in boot sector of <DRIVE>. Remove the disk from the drive.

The disk you are trying to access is infected by a boot virus. Remove the disk from the drive and use Quick Heal to remove the virus.

Found <VIRUS> active in memory.

A virus was found in the memory. This means that the virus is currently active and possibly spreading to other files. For more information on how to proceed, see "Cleaning virus encountered in memory on page 48".

General failure reading drive information.

This message most probably indicates a hardware problem.

Insufficient memory. Cannot proceed ...

If this message is given by DOS Version of Quick Heal, your computer does not have enough conventional memory to load Quick Heal. Might be some terminate-and-stay-resident programs are taking up conventional memory. Although you would hardly get this message in GUI based version of Quick Heal, this can happen if Windows runs out of virtual memory.

No floppy drive was detected to save rescue information. Setup cannot save rescue information.

Quick Heal saves rescue information of your system on to floppy disks which can be used after the system crash. If a floppy drive is not present, rescue information will not be saved.

Self integrity check failed for <MODULE NAME>.

This message indicates that the specified module is corrupt. You will have to reinstall Quick Heal.

The date or time you entered has already elapsed.

You are trying to schedule Quick Heal for 'One time' at a time which has already elapsed. Check date and time of scheduling in the respective fields.

This disk does not contain any rescue files, unable to proceed.

You would get this message when you are trying to compare or restore rescue information. The disk in the drive you specified for reading rescue information does not contain rescue information. Insert the disk in which you had previously stored the rescue information and retry.

Unable to copy <FILENAME>.

This message occurs while saving rescue information. There can be some problem with the disk you are using to save rescue information. Try using another diskette.

Unable to delete the file. Skipping...

This message occurs when Quick Heal encounters a unrecoverable file infected by a virus. Check the read-write access of the specified file.

Unable to format the disk. Aborting..

Before saving rescue information, Quick Heal quick formats the rescue disk. This problem can arise if the floppy you are using to save rescue information is not pre-formatted or has physical problems.

Unable to read the Boot Sector/Partition table

Quick Heal was unable to access the boot record / partition table while scanning or using rescue utility. This message can occur if you are using a program that locks the boot / partition sector in some way, preventing Quick Heal from accessing it.

Unable to read disk information.

Verify that the disk is properly formatted and free of errors. If the disk is accessible from other applications, there is some internal consistency error. Try re-installing Quick Heal.

Unable to rename the file. Want to delete this file.

This message occurs when Quick Heal encounters a unrecoverable file infected by a virus. If the options is set to Rename unrepairable files, Quick Heal will try to rename the file. Quick Heal is not able to rename the file because a file with the new name already exists.

Unable to save scan details to activity log.

The activity log could not be updated because you don't have read-write access to it.

Unable to start print operation.

The data cannot be printed because the printer is not connected or not online.

Unable to transfer system to drive <DRIVE>...

There can be some problem with the disk used for saving rescue information. Try using another diskette or transferring system from DOS prompt using SYS command.

Unable to write to drive <DRIVE>..

Quick Heal was unable to write to the drive because either the disk is write protected or you don't have read-write access to the drive.

Glossary

activity log	A file in which Quick Heal maintains the log of all the virus detection and removal activities during each scan.
archive file	A collection of files or a single file compressed in a single file to save disk space.
AUTOEXEC.BAT	A batch file that is automatically executed when the computer is started.
bootable disk	A disk that contains all the necessary programs for the operating system to start or boot the computer.
boot sector	A first physical sector on a floppy disk or a first logical sector on a hard disk partition. It contains the information about the disk or partition, such as number of sectors, number of FAT copies, number of root directory entries.
boot virus	A virus that infects the boot sector of the hard disk or floppy disk by replacing the boot sectors executable code by their own code, so that they are loaded into the memory before operating system gets load.
CMOS	An abbreviation for Complimentary Metal Oxide Semiconductor. This is a battery-powered chip in the computer that stores the basic hardware configuration of the system.
cold boot	To start your computer by switching on the power switch.
command line options	An option that is used to control the execution of the program. This option has to be given at the operating system prompt or through the RUN.. command in Windows.
compressed file	A collection of files or a single file compressed in a single file to save disk space.
CONFIG.SYS	A text file containing commands those configure DOS and the system's hardware. DOS automatically executes this file when you start your computer.

conventional memory	The first 640K of your system memory. This is the largest amount of memory that DOS can use without the aid of an extended or expanded memory manager.
data file	A file that is created by or needed by an application and contains no executable code. For example database files, graphics files, configuration files, etc.
device driver	A type of terminate-and-stay-resident program that is loaded from CONFIG.SYS or SYSTEM.INI at startup.
dialog box	A box on the screen containing buttons and options that you an select to proceed.
directory	See folder.
docked	The position the Quick Heal Toolbar takes when you drag it to the edge of the screen. It snaps into place along the length of the screen edge
download	Transfer a file from one computer to another through modem or network.
executable file	A file containing a program that can be run by the operating system. Executable files generally have the following extensions: .COM .EXE, .OVR, .OVL, .DRV, .BIN, .SYS, etc.
extensions	A three-letter suffix of a DOS filename. This is usually used to describe the file type.
File Allocation Table (FAT)	A table in the system area of a disk that identifies the specific place on the disk where each file is physically stored.
file extensions	See extensions
folder	A part of a disk that you reserve to store certain files. This makes it easier to organize files on the disk.
hard disk	A non-removable disk built into your computer and used to store information.
hotkey	A shortcut key which when pressed opens a menu or executes a command associated with the button, or option.
infected file	A file that contains a virus.

integrity check	A check performed to determine presence of unknown virus in the file. This check needs the integrity information file to verify the file's integrity.
known virus	Any virus that Quick Heal detect and identify by name.
load	To start or run an application.
Local Area Network	A group of computers linked together and have access to a shared computer.
macro virus	A virus that infects document files with macro capability. For example, Microsoft Word document and template files are susceptible to such viruses
master Boot Record	This is the first physical sector on a hard disk. It contains information on how a hard disk is partitioned and the master boot record program.
memory resident program	A program that loads itself into memory the first time it runs, and remains there until it is disabled or the computer is restarted.
multipartite virus	A virus that affects both executable files and boot / partition.
network	A series of computers and associated hardware connected together in a work group for the purpose of sharing information and hardware between users.
operating system	Master control program that loads in to the memory when you start your computer. It controls and manages all computer operations and programs
partition table	A table in the master boot record of a hard disk that specifies how the disk is set up, including information such as the size and location of the partitions, which operating system each partition uses, and which partition the computer will boot from.
polymorphic virus	Most of the scanners detect viruses by a unique signature for each virus. To evade such style, new generation viruses keep on changing their code. Such viruses are categorized as polymorphic virus.

polymorphic virus	Most of the scanners detect viruses by a unique signature for each virus. To evade such style, new generation viruses keep on changing their code. Such viruses are categorized as polymorphic virus.
reboot	To restart your computer. See also warm boot
stealth virus	A virus that actively defends itself against attempts to analyze or remove it.
system files	The files that make up operating system.
Taskbar	Desktop component that gives access to the Start menu and currently running programs.
terminate-and-stay-resident	A program that loads itself into memory the first time it runs and remains there until it is disabled or the computer is restarted.
trojan horse	A program that promises to be something useful or interesting, but covertly may damage or erase files on your computer while you are running it. These do not come under virus category.
TSR	See terminate and stay resident program.
virus	Virus is actually a misnomer given to software written with the intention of performing harmful acts like formatting your hard disk, deleting data, damaging other software etc. A virus spreads from one computer to other by copying itself to an existing executable code so that it is executed when the code to which it has attached is run.
virus-like activity	An activity or action caused by other software that Quick Heal perceives as the work of a possible unknown virus.
VXD	Virtual Device driver. It is an operating system extension that manages a computer resource. Quick Heal Online protection is an example of a VXD.
warm boot	To restart your computer by pressing Ctrl+Alt+Del. A warm boot can be detected and emulated by some viruses, so virus in memory may still be there when the boot is complete.