



# USER'S GUIDE

Quick Heal™ Total Security 2009

Quick Heal Technologies (P) Ltd.  
<http://www.quickheal.com>

Copyright (c) 1993-2008 Quick Heal™ Total Security

## **ALL RIGHTS RESERVED.**

All rights are reserved by Quick Heal Technologies (P) Ltd.

No part of this software may be reproduced, duplicated or modified in any form or incorporated into any information retrieval system, electronic or any other or transmitted in any form without prior permission of Quick Heal Technologies (P) Ltd, 603 Mayfair Towers II, Wakdevadi, Shivajinagar, Pune-411005, India.

Marketing, distribution or use by anyone barring the people authorized by Quick Heal Technologies (P) Ltd. is liable to legal prosecution.

## **Trademarks**

Quick Heal, Quick Heal Total Security and DNAScan are registered trademarks of Quick Heal Technologies (P) Ltd.

Microsoft, MSN, Windows and Windows Logo are trademarks of Microsoft Corporation. Vade Retro is registered trademark of Goto Software, France. All brand names and product names used in this manual may be trademarks, registered trademarks or trade names of their respective companies.

## LICENSE AGREEMENT

### IMPORTANT:

Read this License Agreement carefully before using this software.

BY USING THIS SOFTWARE IN ANY WAY YOU ACKNOWLEDGE THAT YOU HAVE READ, UNDERSTAND AND AGREE TO THE TERMS OF THIS USER LICENSE AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS BELOW, DO NOT USE THIS SOFTWARE IN ANY WAY AND PROMPTLY RETURN IT OR DELETE ALL THE COPIES OF THIS SOFTWARE IN YOUR POSSESSION.

### Quick Heal License Agreement

This License is a legal agreement between you, the licensee, and Quick Heal Technologies Pvt. Ltd. In consideration of payment of the License Fee, which is a part of the price evidenced by the Receipt, Quick Heal Technologies Pvt. Ltd. grants to the Licensee a nonexclusive right. Quick Heal Technologies Pvt. 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. Copying of the Software or the written materials is expressly forbidden.

You can:

- use one copy of the software on a single computer. In case of multi-user copy which will be appropriately mentioned on the packaging and or the receipt, use the software only on the said number of systems as mentioned on the packaging.
- make one copy of the software solely for backup purpose.
- install the software on a network, provided you have a licensed copy of the software for each computer that can access the software over that network.

You can not:

- sublicense, rent or lease any portion of the software.
- debug, decompile, disassemble, modify, translate, reverse engineer the software

### MANDATORY ACTIVATION

The license rights granted under this Agreement are limited to the first twenty (20) days after you first install the Product unless you supply registration information required to activate your licensed copy as described in Activation Wizard of the Product. You can activate the Product through the use of the Internet or telephone; toll charges may apply. You may also need to reactivate the Product if you happen to re-install the product due to reasons. There are technological measures in this Product that are designed to prevent unlicensed or illegal use of the Product. You agree that we may use those measures.

As the only warranty under this Agreement, and in the absence of accident, abuse or misapplication, Quick Heal Technologies Pvt. Ltd. warrants, to the original Licensee only, that the disk(s) on which the software is recorded is free from 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. Quick Heal Technologies Pvt. Ltd.' only obligation under this Agreement is, at Quick Heal Technologies Pvt. Ltd.' option, to either (a) return payment as evidenced by a copy of the Receipt or (b) replace the disk that does not meet Quick Heal Technologies Pvt. Ltd.' limited warranty and which is returned to Quick Heal Technologies Pvt. Ltd. with the copy of the Receipt.

### THIRD PARTY WEBSITE LINKS

At some points the software product includes links to third party sites, you may link to such third party websites through the user of this software. The third party sites are not under the control of Quick Heal Technologies and Quick Heal Technologies is not responsible for the contents of any third party website, any links contained in the third party websites. Quick Heal Technologies is providing these links to third party websites to you only as a convenience

### EMAIL/ELECTRONIC COMMUNICATION

Once you register the software by activating the software product, Quick Heal Technologies Pvt. Ltd. may communicate with you on the contact information submitted during the registration process through email or other electronic communication device like telephone or a cell phone. The communication can be for the purpose of product renewal or product verification for your convenience.

### QUICK HEAL STATUS UPDATE

Upon every update of licensed copy, Quick Heal Update module will send current product status information to Quick Heal Internet Center. The information that will be sent to the Internet Center includes the Quick Heal protection health status like which monitoring service is in what state in the system. The information collected does not contain any files or personal data. The information will be used to provide quick and better technical support for legitimate customers.

### Disclaimers:

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 Quick Heal Technologies Pvt. Ltd. or its suppliers 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 or inability to use this software package ever.


The disclaimers and limitations set forth above will apply regardless of whether you accept the software.

ALL MATTERS SUBJECT TO PUNE (INDIA) JURISDICTION

## ABOUT THIS DOCUMENT

This user guide contains all the information you need to install and use Quick Heal Total Security on Windows. Once familiar you can also use it for future reference. Full care has been taken to incorporate all details with the latest developments in the shipping.

### Conventions

Convention	Meaning
<b>Bold font</b>	Menu titles, commands, window titles, dialog elements, etc.
	Additional Information, Important Information, Notes etc.
<b>To do this: ...</b> 1. Step 1. 2. ...	Action that must be followed.
<b>[switch]</b> —function of the switch.	Command line switches.

## ABOUT QUICK HEAL TOTAL SECURITY

Quick Heal Total Security gives your desktop needed protection from various Internet threats. It gives Internet Security by automatically removing viruses and spyware, fighting spam, blocking access to hackers, preventing access to unwanted and malicious websites and blocking pop-up banner advertisements.

### Complete Virus Protection

Quick Heal's powerful virus detection engine provides protection from new and more complex virus threats that are appearing. It automatically protects you from viruses, worms, Trojans and backdoors. It continuously scans the system in background and prevents virus infection from files coming in through email attachments, instant messenger, Internet downloads and through vulnerability exploits. It also scans for certain non-virus threats like spyware, adware, riskware and other attack tools.

### Quick Heal Total Security Anti-Virus Features

- Scans and cleans already infected PC before installation
- Cleans worms, backdoors and Trojans by cleaning registry and dropped files.
- Cleans virus-infected files automatically.
- Scans email messages and attachments before they reach to your inbox
- Downloads new updates automatically.
- Messenger service informs you about new Viruses, Hoaxes, general messages and Updates etc.
- Quick Heal Anti Rootkit has been introduced. It detects and removes Rootkits from the system safely.

### Powerful email protection and AntiSpam filter

- Quick Heal's unique on-line email protection scans email messages before they reach your inbox, no matter which email client you use.
- Powerful AntiSpam filter engine that identifies and filters junk emails by tagging them as spam.
- Facility to provide black list and whit list for email filter in combination of spam filter.
- Prevents worms, Trojans and backdoors from sending infected emails.
- Attachment control for better protection from new and unknown worms.
- Remove email containing vulnerability e.g. IFRAME, MIME etc.

### Complete Internet Protection

Quick Heal Personal Firewall protects your PC and valuable data when you are on-line. Firewall will block any application that will try to connect to Internet except those configured by you as trusted. This prevents Trojans, backdoors and spywares from using your Internet bandwidth to spread and or send personal data over the Internet.

### Internet protection features

- Blocks spam mails including credit card phishing scams and email fraud.
- Website filter that will block visits to unwanted websites.
- Blocks pop-up web advertisements that slows down your surfing or tracks your browsing habits.

### Data Protection

Data Theft Protection prevents unauthorized copy of confidential/sensitive data from your PC. Block access to pen drive/CD writer or other USB storage devices from your PC. Using this feature your system's data cannot be copied to the removable drives. Neither can the data from outside (removable drives) be copied to your system. This way it protects your system and data. This helps to protect infection and data theft.

### AntiPhishing

Quick Heal Anti-Phishing toolbar has been introduced. This automatically scans all accessed web pages for fraudulent activity protecting you against any phishing attack as you surf the internet. Prevents identity theft by blocking phishing websites. So you can do online shopping, banking and website surfing safely

### PC2Mobile Scan

PC2Mobile Scan has been introduced under scan. Now scan and clean viruses and spywares from your cell phones, PDAs and smart phones by just connecting it to your PC. Please refer to <http://www.quickheal.co.in/pc2mobile.asp> to check which cell phone modes are supported.

### AntiMalware

A new advanced malware scanning engine scans registry, files and folders at lightening speed to thoroughly detect and clean Spywares, Adwares, Roguewares, Dialers, Riskwares and lots of other potential threats in your system.

## TABLE OF CONTENTS

<b>INSTALLING QUICK HEAL TOTAL SECURITY.....</b>	<b>8</b>
GETTING PREPARED .....	8
SYSTEM REQUIREMENTS .....	8
INSTALLING QUICK HEAL TOTAL SECURITY .....	10
UNINSTALLING QUICK HEAL TOTAL SECURITY .....	10
<b>REGISTERING QUICK HEAL TOTAL SECURITY.....</b>	<b>11</b>
REGISTERING ON-LINE WITH INTERNET CONNECTION ON SAME PC.....	11
REGISTERING OFF-LINE USING INTERNET CONNECTION ON SOME OTHER PC .....	12
REGISTERING THROUGH PHONE .....	13
REACTIVATION .....	14
CAN I INSTALL QUICK HEAL TOTAL SECURITY ON ANOTHER COMPUTER? .....	14
WHAT TO DO IF I LOST MY SERIAL NUMBER OR ACTIVATION NUMBER?.....	14
<b>USING QUICK HEAL .....</b>	<b>15</b>
ABOUT QUICK HEAL MAIN WINDOW.....	15
RIGHT SHELL MENU OPTIONS.....	16
USING HELP .....	17
PERFORMING MANUAL SCANS.....	18
SCHEDULING QUICK HEAL TOTAL SECURITY SCANNER.....	21
USING ONLINE PROTECTION .....	22
USING E-MAIL PROTECTION.....	23
KNOWING ABOUT TRUSTED E-MAIL CLIENTS.....	23
USING DATA PROTECTION .....	24
USING STARTUP SCAN.....	24
USING MESSENGER.....	25
VIEWING REPORTS.....	26
STATISTICS.....	27
VIEWING VIRUS LIST.....	28
QUARANTINE .....	28
SYSTEM INFORMATION.....	29
CREATING EMERGENCY CD OR COMMAND LINE SCANNER .....	30
OVERVIEW OF NATIVE BOOT SCAN .....	31
USING QUICK HEAL ANTIMALWARE .....	32
WHEN QUICK HEAL ANTIMALWARE SHOULD BE USED?.....	33
USING QUICK HEAL ANTI-PHISHING .....	34
USING EXTRA TOOLS.....	36
HIJACK RESTORE .....	36
WINDOWS SPY .....	37
TRACK CLEANER .....	37
ADVANCED SYSTEM EXPLORER .....	37
ABOUT SECTION .....	38
<b>USING PC2MOBILE SCAN .....</b>	<b>39</b>
IMPORTANT REQUIREMENTS FOR PC2MOBILE SCAN .....	41
CONFIGURING WINDOWS MOBILE PHONE BEFORE SCAN.....	41
SCANNING WINDOWS MOBILE .....	41
CONFIGURING OTHER MOBILE PHONE BEFORE SCAN .....	41
CONNECTION THROUGH BLUETOOTH .....	42
SCANNING OTHER MOBILE PHONE THROUGH BLUETOOTH .....	42
CONNECTION THROUGH USB CABLE.....	42
SCANNING OTHER MOBILE PHONE THROUGH CABLE .....	42
<b>USING QUICK HEAL ANTI-ROOTKIT.....</b>	<b>43</b>
CONFIGURING QUICK HEAL ANTI-ROOTKIT.....	44
SCANNING RESULTS AND CLEANING ROOTKITS.....	45
CLEANING ROOTKITS THROUGH QUICK HEAL EMERGENCY CD .....	46
<b>CUSTOMIZING QUICK HEAL TOTAL SECURITY .....</b>	<b>47</b>
SCANNER - SCAN OPTIONS .....	48
SCANNER – MEMORY SCAN .....	51
SCANNER – DNASCAN.....	51
SCANNER – REGISTRY RESTORE .....	52
SCANNER – PC2MOBILE SCAN.....	52
PROTECTION – ONLINE PROTECTION .....	53
PROTECTION - E-MAIL PROTECTION .....	55
PROTECTION – ANTISPAM .....	57
ANTI SPAM FILTER FOLDER .....	58
PROTECTION – INTERNET SECURITY .....	58
PROTECTION – DATA PROTECTION .....	59
UPDATES - AUTOMATIC UPDATES.....	60

UPDATES - MESSENGER .....	61
GETTING MESSAGES FROM LOCAL FOLDER OR NETWORK PATH.....	62
UPDATES - INTERNET SETTINGS .....	62
MISCELLANEOUS - EXCLUSIONS .....	63
MISCELLANEOUS - GENERAL .....	64
<b>CLEANING VIRUSES .....</b>	<b>65</b>
CLEANING VIRUSES ENCOUNTERED DURING SCANS .....	65
CLEANING VIRUS ENCOUNTERED IN MEMORY .....	66
CLEANING BACKDOOR, TROJAN, WORM AND MALWARES ENCOUNTERED IN MEMORY .....	66
<b>USING EMERGENCY CD AND COMMAND LINE SCANNER .....</b>	<b>67</b>
USING EMERGENCY CD .....	67
USING COMMAND LINE SCANNER .....	68
<b>UPDATING QUICK HEAL TOTAL SECURITY .....</b>	<b>69</b>
UPDATING QUICK HEAL TOTAL SECURITY FROM INTERNET .....	69
UPDATING QUICK HEAL TOTAL SECURITY WITH DEFINITION FILES .....	69
UPDATE GUIDELINES FOR NETWORK ENVIRONMENT .....	70
<b>FAQ – FREQUENTLY ASKED QUESTIONS .....</b>	<b>71</b>
GENERAL QUERIES .....	71
REGISTRATION AND RE-ACTIVATION: .....	74
RENEWING QUICK HEAL TOTAL SECURITY .....	76
UPDATING QUICK HEAL TOTAL SECURITY .....	77
<b>GLOSSARY .....</b>	<b>78</b>
<b>TECHNICAL SUPPORT .....</b>	<b>80</b>
<b>CONTACT US .....</b>	<b>81</b>

## INSTALLING QUICK HEAL TOTAL SECURITY

Quick Heal Total Security has a very simple installation procedure. While you are installing, simply read each installation screen, follow the instructions, and then click Next to continue.

Quick Heal Total Security should be installed on a virus-free machine. If you are sure that your computer is infected by a virus, use the Emergency CD to remove the viruses before installing Quick Heal Total Security. If you are not sure whether your computer is already infected by a virus, continue with the installation. Quick Heal Total Security setup will scan your computer's critical area for viruses as a part of its installation process.

## GETTING PREPARED

Before installing Quick Heal Total Security remember following important guidelines:

- If you have any other anti-virus software/hardware loaded, uninstall it before proceeding with Quick Heal Total Security installation. Two anti-virus software's co-existing on the same computer at the same time could be hazardous for your computer.
- Quick Heal Total Security requires approximately 300 MB of free disk space.
- Close all open programs before proceeding with Quick Heal Total Security installation.
- Administrative privilege is required to install Quick Heal Total Security.

## SYSTEM REQUIREMENTS

To use Quick Heal Total Security, your computer must also meet following minimum requirements:

Operating Systems	Minimum Requirements
Windows 2000	<ul style="list-style-type: none"><li>• 300 MHz Pentium Processor (or compatible) or higher</li><li>• 128 MB of RAM</li><li>• 300 MB of free hard disk space</li><li>• DVD or CD-ROM drive</li><li>• Service Pack 3 or above</li><li>• Internet Explorer 6 or higher</li></ul>
Windows XP	<ul style="list-style-type: none"><li>• 300 MHz Pentium Processor (or compatible) or higher</li><li>• 128 MB of RAM</li><li>• 300 MB of free hard disk space</li><li>• DVD or CD-ROM drive</li><li>• Service Pack 1 or above</li></ul>
Windows 2003	<ul style="list-style-type: none"><li>• 300 MHz Pentium Processor (or compatible) or higher</li><li>• 256 MB of RAM</li><li>• 300 MB of free hard disk space</li><li>• DVD or CD-ROM drive</li></ul>
Windows Vista	<ul style="list-style-type: none"><li>• 1 GHz Pentium Processor (or compatible) or higher</li><li>• 1 GB of RAM</li><li>• 300 MB of free hard disk space</li><li>• DVD or CD-ROM drive</li></ul>
Windows Server 2008	<ul style="list-style-type: none"><li>• 1 GHz Pentium Processor (or compatible) or higher</li><li>• 512 MB of RAM</li><li>• 300 MB of free hard disk space</li><li>• DVD or CD-ROM drive</li></ul>



### **E-mail scanning supported clients**

E-mail scanning is supported for any POP3 e-mail clients including:

- Microsoft Outlook Express 5.5 and above
- Microsoft Outlook 2000 and above
- Netscape Messenger 4, 6 and 7
- Eudora 5 and above
- IncrediMail

### **E-mail scanning not supported clients**

E-mail scanning is not supported for following e-mail clients:

- IMAP
- AOL
- POP3s with Secure Sockets Layer (SSL)
- Web based email such as Hotmail and Yahoo! Mail
- Lotus Notes

### **SSL Connections are not supported**

E-mail protection does not support encrypted e-mail connections that use Secure Sockets Layer (SSL). If you are using SSL connections then your e-mails are not protected by Quick Heal mail protection.



To send e-mail through SSL connections, turn off E-mail protection.

### **Quick Heal Anti-Rootkit Requirements**

- Quick Heal Anti-Rootkit is supported on 32-bit operating systems.
- It requires minimum 256 MB RAM installed on system.

### **Quick Heal PC2Mobile Scan**

- Quick Heal PC2Mobile feature is supported on Windows XP/Vista having 32-bit operating systems.
- For Windows Mobile, Microsoft Active Sync 4.0 or above software must be installed.
- For the list of Mobile phones supported please check <http://www.quickheal.co.in/pc2mobile.asp>

### **Quick Heal AntiPhising**

This feature is supported for Internet Explorer 6 or above version.

## INSTALLING QUICK HEAL TOTAL SECURITY

To start with installation, insert the Quick Heal Total Security CD in the CD-Drive. CD being enabled with auto-run feature; will automatically prompt you with a list of available options.

1. Click on **Install Total Security** to initiate the Installation procedure.
2. Installation program will first perform Pre-Install Virus Scan on your system to scan system memory, master boot record and system files for known viruses.
3. During Pre-install virus scan if a virus is found active in memory then follow below given procedures:
  - a. Total Security Installer automatically sets native scanner to scan and disinfect the system on next boot.
  - b. After disinfection restart your system and continue with installation. For more detail refer to **Native Scan** in **User Guide**.
4. If during the Pre-install virus scan, no viruses are found in the critical system areas then installation would proceed further.
5. Click **Next**.
6. Read the License Agreement carefully; if you agree then choose **I Agree**. If you disagree then you cannot continue with the installation.
7. Click **Next**.
8. Click **Browse** to change the installation path if you want to install Quick Heal Total Security in different folder.
9. Click **Next**.
10. Select the Total Security Protection options.
11. Click **Next**.
12. Read the important information relating to **Quick Heal Total Security**.
13. Click **Next**.
14. On **Finish**, **Registration/Re-activation**, **Updating** and **Install Quick Heal Firewall** activities will be performed. In case if you wish to perform these activities later on then unselect the above options and click **Finish**

### If the CD auto-run menu does not appear

In some systems, CD-Rom drive does not automatically start a CD when it is inserted. In such cases, to start the installation from Quick Heal Total security CD follow the steps as mentioned below:

1. Double click on **My Computer** from your Desktop.
2. Right click on CD-Rom drive and select **Explore** option.
3. Double click on **Autorun.exe** to start the installation.

## UNINSTALLING QUICK HEAL TOTAL SECURITY

If due to any reason you wish to uninstall Quick Heal Total Security, follow the steps as mentioned below:

1. Go to **Start Menu->Programs->Quick Heal Total Security** group and click **Uninstall Quick Heal Total Security**.
2. Quick Heal Uninstaller will prompt for the deletion of Reports, Quarantine and Backup files. If you wish to reinstall Quick Heal after some time then you can uncheck **Remove Report Files** and **Remove Quarantine/Backup Files**. Otherwise proceed by pressing **Ok**.
3. To uninstall Quick Heal Firewall Pro select **Uninstall Quick Heal Firewall Pro** and click **Ok**. Quick Heal Firewall Pro un-installation will start. Please go through the screen wise instructions.
4. If you are a registered user, a dialog will be displayed showing Serial Number and Activation Number of your copy. You are requested to note down your serial number and activation number as it will be needed in case you want to reinstall and reactivate Quick Heal.
5. Uninstaller will finally prompt you to **restart** your system for changes to take effect.



1. Before proceeding with uninstallation, ensure that all other running programs are closed.
2. To uninstall Quick Heal Total Security, administrative privilege is required.

## REGISTERING QUICK HEAL TOTAL SECURITY

After installation of Quick Heal Total Security, you will need to register your copy to get it activated. It is strongly recommended that you register and activate your copy immediately after installation; otherwise without activation it cannot be further updated. Registered users can get other benefits like technical support and messenger service. If your copy of Quick Heal Total Security is not registered within 20 days time period from the date of installation, it will expire and its further use will be considered as void.

Registration can be done by either of the following options:

- [On-line with Internet access on same PC](#)
- [Off-line using Internet access on some other PC](#)
- [Phone](#)

## REGISTERING ONLINE WITH INTERNET CONNECTION ON SAME PC

Now proceed with the following process to activate your copy:

1. Launch Registration Wizard, go to **Start Menu->Programs->Quick Heal Total Security** group and click **Activate Quick Heal Total Security** or click **Activate Now** button from the **Scanner's Status** section.
2. Click **Next**.
3. Choose **Yes** to "**I have Internet access on this computer**" and click **Next**.
4. Select **Register the copy for first time** and click **Next**.
5. Provide "**Serial No**", "**Purchased From**" and "**Register for**" details.
6. Click **Next**.
7. Enter your personal details.
8. Click **Next**.
9. Before submitting just go through the details you provided. If you want to modify any details click **Back**. Otherwise click **Next**.
10. It will take few seconds to register and activate your copy. Please stay connected to Internet during this process.
11. On completion you will get successful activation message. This message box will also display **Activation Number** and **License Subscription validity** information for your copy. Activation Number is very important, so please note it down on your User Guide or any other safe place for future reference. You will be asked for this activation number when communicating with Quick Heal Support or during re-activation if need be the case.
12. Click **Finish** to complete the registration process.



1. You can find serial number for your copy pasted on your User Guide and / or inside the box. If you have purchased the software online using credit card then you will find the serial number in the e-mail confirming your order.
2. Kindly stay connected to the Internet during the Registration process.

## REGISTERING OFF-LINE USING INTERNET CONNECTION ON SOME OTHER PC

In case if Internet connection is not available on your computer, you will need to register your copy by filling the registration form on our website. You can visit off-line activation page on our web site at <http://www.quickheal.com/actinfo.htm> with any system having Internet Connection. For example: Cyber cafe.

### This involves following important steps

- Getting details of your Quick Heal Total Security installation
- Visiting and filling off-line registration web form through some other PC having Internet access
- Receiving license.key file through email.
- Activating the Quick Heal Total Security installation using newly obtained license.key file.

### Detail procedure

When filling the registration form on our website you would also need following information of your installed copy:

- Serial Number
- Installation Number
- A Valid E-mail address.



1. You can find serial number for your copy pasted on your User Guide and / or inside the box. If you have purchased the software online using credit card then you will find the serial number in the e-mail confirming your order.
2. Installation Number is available in Off-line Registration section of Quick Heal Total Security Registration Wizard. Choose **No** to '**I have Internet access on this computer**' and click **Next**. Choose **Offline registration through web** and click **Next** to get your **Installation Number**.

### Obtaining License File

Once the Serial Number and Installation Number are verified, you will have access to the Personal Information page wherein you are required to fill the relevant contact details. Once the registration details are submitted successfully you will get your unique License.key file via e-mail on the e-mail address provided by you at the time of registration. You will also get an option to download your License.key file on successful registration/activation. Take this License.key file to the computer where activation needs to be done.

### Activating Offline

Now proceed with the following process to activate your copy:

1. Launch Registration Wizard, go to **Start Menu->Programs->Quick Heal Total Security** group and click **Activate Quick Heal Total Security** or click **Activate Now** button from the **Scanner's Status** section.
2. Click **Next**.
3. Choose **No** to **I have Internet access on this computer**.
4. Click **Next**.
5. Select **Offline Registration through web**.
6. Click **Next**.
7. Click **Browse** and open the **License.Key** file.
8. On completion you will get successful activation message. This message box will also display **Activation Number** and **License Subscription validity** for your copy. Activation Number is very important, so please note it down on your User Guide or any other safe place for future reference. You will be asked for this activation number when communicating with Quick Heal Support or during re-activation.
9. Click **Finish** to complete the registration process.

## REGISTERING THROUGH PHONE

This feature is provided to those users who do not have any access to Internet. Users need to contact Quick Heal Support Team at following nos. +91-20-65223883/ 65223892 to get registered and activate their copy.

Before calling to Quick Heal Support please get the following details of your copy:

- Serial Number
- Installation Number



1. You can find serial number for your copy pasted on your User Guide and / or inside the box. If you have purchased the software online using credit card then you will find the serial number in the e-mail confirming your order.
2. Installation Number is available in Offline Registration section of Quick Heal Total Security Registration Wizard; if you choose **No** to **I have Internet access on this computer** and click **Next**. Choose **Offline registration through phone** and click **Next**.

### Obtaining activation code and activating copy

Now proceed with the following process to activate your copy:

1. Launch Registration Wizard, go to **Start Menu->Programs->Quick Heal Total Security** group and click **Activate Quick Heal Total Security** or click **Activate Now** button from the **Scanner's Status** section.
2. Click **Next**.
3. Choose **No** to **I have Internet access on this computer**.
4. Click **Next**.
5. Choose **Offline Registration through phone**.
6. Click **Next**.
7. Now call to Quick Heal Support Team at following numbers +91-20-65223883/ 65223892.
8. Please provide **Serial Number** and **Installation number** to the support executive. After verifying your purchase details support executive would provide you the phone code for your copy of Quick Heal. Please type the code as it is in the blank square box.
9. Click **Next**.
10. On completion you will get successful activation message. This message box will also display **Activation Code** for your copy. It is very important code, so please note it down on your User Guide or any other safe place for further reference. You will be asked for this activation code when communicating with Quick Heal Support or for re-activation.
11. Click **Finish**.

## REACTIVATION

If due to any reason you need to reinstall your operating system or Quick Heal Total Security, it is necessary to reactivate your copy after reinstallation.

Reactivation is very easy and similar to the registration process. The changes in case of Reactivation are:

- On a PC where you have Internet access, you are required to choose “**Re-activate the copy**” option and provide the **Serial Number** and **Activation Number** of your copy and click **Next**.
- Reactivation through Phone and Off-line is just similar to the corresponding registration process. You only have to remember your **Activation Number** and provide it whenever it is being asked for, during reactivation process.

## CAN I INSTALL QUICK HEAL TOTAL SECURITY ON ANOTHER COMPUTER?

If you install Quick Heal Total Security on another computer, after installation it is necessary to register your software. You must perform the registration procedure by providing new Serial Number. Any previously obtained Serial Number and License Keys are invalid and will not work on another computer.



One Serial number can only be used for one computer.

## WHAT TO DO IF I LOST MY SERIAL NUMBER OR ACTIVATION NUMBER?

**Serial Number** and **Activation Number** will serve as the users Identity. In case you loose Serial Number or Activation Number, you can obtain your Serial Number or Activation Number by contacting Quick Heal Technical Support by paying nominal charges.

# Chapter 3

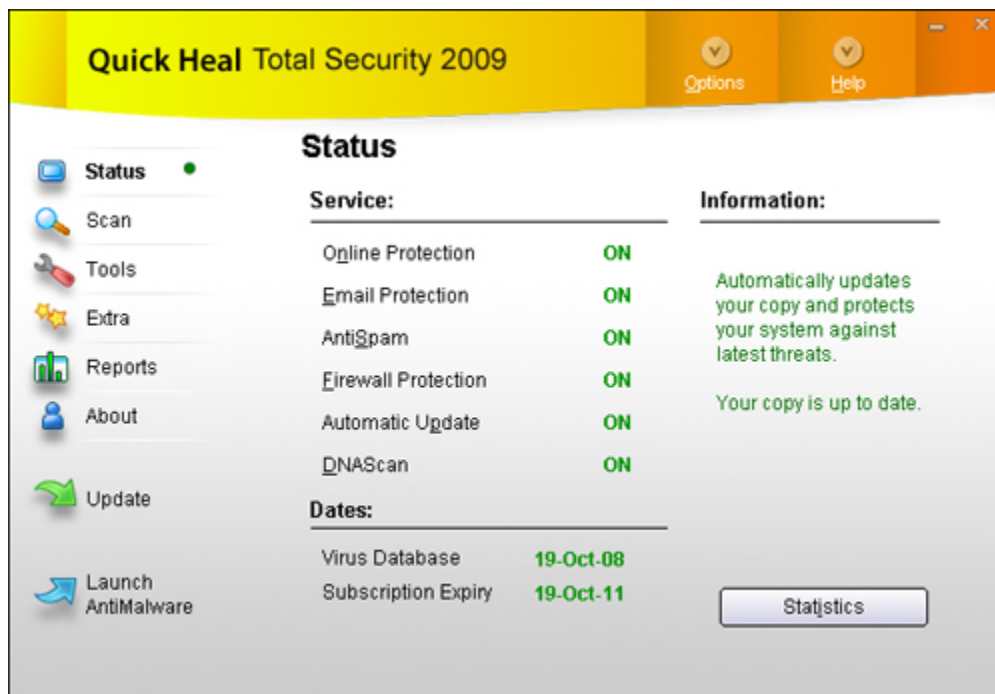
## USING QUICK HEAL

All the features related to Quick Heal Total Security can be accessed from Quick Heal main window. In addition, you can also access Quick Heal main window or the features from Windows system tray. Proceeding by the default installation, Quick Heal Anti-Virus or Total Security protects your entire system. You do not have to manually start Quick Heal Anti-Virus to protect your system in such cases.

You can manually start Quick Heal Total Security by either of the following ways:

- Point to **Start, Programs, Quick Heal Total Security** and **Quick Heal Total Security**.
- In Windows system tray, double click on the **Total Security Online Protection** icon or right click on **Total Security Online Protection** icon in system tray and select **Open Total Security**.
- At the prompt in DOS window, changed to the directory where **Quick Heal Total Security** is located. Type **Scanner** and press **Enter**.

## ABOUT QUICK HEAL MAIN WINDOW



The main window lets you access features, configure the options and access online help. On the left side of the main window select the option that you want. You have following options:

<b>Status</b>	View the status of Quick Heal Total Security. This section provides status of important security scanning.
<b>Scan</b>	Virus scanning is obviously the most important component of any Anti-Virus software. Quick Heal scanner detects viruses in boot records, partition tables, executable files, compressed files, compressed exes, mailboxes, OLE files, script files, scrap etc.
<b>Tools</b>	Important tools can be accessed from this section such as Anti-Rootkit, Quarantine, Virus List, Scheduling Scan, System Information, Emergency CD and Messenger.
<b>Extra</b>	This section provides extra tools for system diagnosis and repair. Advanced tools like Hijack Restore, Windows Spy, Track Cleaner and Advanced System Explorer can be accessed from here.
<b>Reports</b>	View the activity reports of all the important modules.
<b>About</b>	This section provides details about Version, Virus Database, Subscription details and Technical Support. You can also Register/Re-activate or renew your Quick Heal subscription from here.

Other options are:

<b>Options</b>	Customize the general options for Quick Heal Total Security.
<b>Update</b>	Update the virus definition files and Quick Heal Total Security components.
<b>Launch AntiMalware</b>	Scans for malicious software (Adwares, Dialers, Pornwares, Potentially unwanted software, Rogue applications, Spywares) and provides cure against them.
<b>Statistics</b>	Provides statistical information from Online Protection, Email Protection and AntiSpam. This information includes below details: <ul style="list-style-type: none"> <li>➤ Since System Start</li> <li>➤ Since Installation</li> </ul>
<b>Help</b>	Access help for Quick Heal Total Security.

## RIGHT SHELL MENU OPTIONS

<b>Open Total Security</b>	Launch Quick Heal Total Security.
<b>Launch AntiMalware</b>	Launch Quick Heal AntiMalware
<b>View Messages</b>	Check the messages received from Quick Heal.
<b>Disable</b>	Disable Quick Heal Online Protection.
<b>Option</b>	Check or configure various Quick Heal Total Security options.
<b>Statistics</b>	Provides statistical information from Online Protection, Email Protection and AntiSpam Protection.
<b>Update Now</b>	Update Quick Heal Total Security.
<b>Scan Memory</b>	Scan System Memory for viruses.



## USING HELP

Help system consists of extensive topics, index, commands and procedures with general FAQ's. Quick Heal provides online help for most of the message windows. You can get help on all the topics by either of the following ways:

- Launching Help by clicking on Help button from Scanner or Scanner Options.
- Pressing **F1** when you need help.
- Clicking the Help button in a dialog box.
- Latest user guide can be downloaded from <http://www.quickheal.co.in/documentation-manual.asp>

## PERFORMING MANUAL SCANS

If Online Protection is enabled with default setting, you normally would not need to scan manually. However, you can manually scan your entire computer, or individual floppy disks, drives, network drives (mapped drives), USB data storage drives, folders, or files if you wish to. Although the default settings for manual scanning are usually adequate, you can adjust the options for manual scanning in the **Options** of Quick Heal Total Security.

### Performing a full system scan

A full system scan scans all boot records, drives, folders and files on your computer. To perform a full system scan:

1. Start **Quick Heal Total Security Scanner**.
2. In the Quick Heal Total Security Scanner main window, click **Scan** on the left pane.
3. In the **Scan** pane, click on **My Computer**.
4. Click on **Scan**.
5. When the scan is complete, scan statistics and report will be provided.
6. When you are done reviewing the statistics and report, click **Close**.

### Performing a My Documents scan

My Documents scan scans all the documents, spreadsheets, presentation and other files kept in My Documents folder. To perform a My Document Scan:

1. Start **Quick Heal Total Security Scanner**.
2. In the Quick Heal Total Security Scanner main window, click **Scan** on the left pane.
3. In the **Scan** pane, click on **My Documents**.
4. Click on **Scan**.
5. When the scan is complete, scan statistics and report will be provided.
6. When you are done reviewing the statistics and report, click **Close**.

### Performing a System Memory scan

Now you scan System Memory for viruses. To perform a System Memory scan:

1. Start **Quick Heal Total Security Scanner**.
2. In the Quick Heal Total Security Scanner main window, click **Scan** on the left pane.
3. In the **Scan** pane, click on **System Memory**.
4. Click on **Scan**.
5. When the scan is complete, scan statistics and report will be provided.
6. When you are done reviewing the statistics and report, click **Close**.

### Performing a Windows folder scan

Windows folder is the primary folder of the Operating Systems. To perform a Windows folder scan:

1. Start **Quick Heal Total Security Scanner**.
2. In the Quick Heal Total Security Scanner main window, click **Scan** on the left pane.
3. In the **Scan** pane, click on **Windows Folder**.
4. Click on **Scan**.
5. When the scan is complete, scan statistics and report will be provided.
6. When you are done reviewing the statistics and report, click **Close**.

### Performing scan on folder

Occasionally you would also like to scan specific folders. To perform scan on desired folder:

1. Start **Quick Heal Total Security Scanner**.
2. In the Quick Heal Total Security Scanner main window, click **Scan** on the left pane.
3. In the **Scan** pane, double click on **Scan Folder**.
4. Select the folder you want to scan. You can also choose multiple folders for a single scan. Select **Exclude Subfolder** if you do not wish to scan subfolders.
5. Click on **Ok** to initiate the scan.
6. When the scan is complete, scan statistics and report will be provided.
7. When you are done reviewing the statistics and report, click **Close**.

## Performing scan on specific files

Occasionally you would also like to scan specific file(s). To perform scan on desired file(s):

1. Start **Quick Heal Total Security Scanner**.
2. In the Quick Heal Total Security Scanner main window, click **Scan** on the left pane.
3. In the **Scan** pane, double click on **Scan File**.
4. Select the file(s) you want to scan.
5. Click on **Ok** to initiate the scan.
6. When the scan is complete, scan statistics and report will be provided.
7. When you are done reviewing the statistics and report, click **Close**.

## Performing Native Boot Scan

Native Boot Scan is very useful to disinfect the system. In case the system is badly infected by a virus and it cannot be cleaned because the virus is active, use Native Boot Scan. This scan will be performed on next boot using Windows NT Boot Shell.

1. Start **Quick Heal Total Security Scanner**.
2. In the Quick Heal Total Security Scanner main window, click **Scan** on the left pane.
3. In the **Scan** pane, click on **Native Boot Scan**.
4. Click on **Scan**.
5. A confirmation prompt will be displayed to set boot time scanner on next boot. Click **Yes**.
6. If you wish to scan your system immediately then click **Yes** to restart the system. If you wish to scan later when you boot the system next time then click **No**.

## Performing Mailbox Scan

Mailbox scan scans inside Outlook Express and Windows Mail's mailboxes for viruses. It deletes the infected mail ensuring your mailboxes remains clean and virus free.

1. Start **Quick Heal Total Security Scanner**.
2. In the Quick Heal Total Security Scanner main window, click **Scan** on the left pane.
3. In the **Scan** pane, click on **Mailbox Scan**.
4. Click on **Scan**. When the scan is complete, scan report will be generated.
5. When you are done reviewing the report. Click **Close**.

## Adding Item in My Profile for regular scan

You can add a custom scan if you regularly scan a particular area of your computer and don't want to specify that area to be scanned every time. You can delete the scan when it is no longer necessary.

### To create a custom scan

1. Start **Quick Heal Total Security**.
2. In the Quick Heal Total Security main window, click **Scan** on the left pane.
3. In the **Scan** pane, click on **Add Item**.
4. If want to scan a folder or multiple folders then click on **Add Folders** and select the desirable folder(s) and click **Ok**. You can configure **Exclude Subfolder** while scanning of a specific folder. This will ignore scanning inside the subfolders while scanning. e.g. If you select C:\ drive for scan along with selecting Exclude Subfolder option, this will initiate scan for files available at the root of C:\ drive only.
5. You can add your desirable files to scan in a single custom scan. To add specific files, click on Add Files and browse for files and click **Ok**.
6. Click **Next**.
7. Give a name to your custom scan.
8. Click **Finish** to save the custom scan.

### To scan a custom scan item

1. Start **Quick Heal Total Security**.
2. In the Quick Heal Total Security main window, click **Scan** on the left pane.
3. In the **Scan** pane, select the custom scan item and click on **Scan**.
4. When the scan is complete, scan statistics and report will be provided.
5. When you are done reviewing the statistics and report, click **Close**.

### To edit a custom scan

You can edit your custom scan any time to add or remove the scan items. To edit a custom scan:

1. Start **Quick Heal Total Security**.
2. In the Quick Heal Total Security main window, click **Scan** on the left pane.
3. In the **Scan** pane, click on the custom scan which you created previously.
4. Click on **Edit Item**.
5. Make the changes and click **Finish** to save the changes.

### To remove a custom scan

You can remove your custom scan any time. To remove a custom scan:

1. Start **Quick Heal Total Security**.
2. In the Quick Heal Total Security main window, click **Scan** on the left pane.
3. In the **Scan** pane, click on the custom scan item which you want to delete.
4. Click on **Remove Item**.
5. A confirmation prompt will come. Click on **Yes** to delete the custom scan item.

### To scan one or more drives

You can scan all or specific drive(s) available on your system. To scan the drive(s):

1. Start **Quick Heal Total Security**.
2. In the Quick Heal Total Security main window, click **Scan** on the left pane.
3. In the **Scan** pane, click on the **Drives** section.
4. Select **Drive** dialog box appears. Herein 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.
5. Now click **Scan** button.

### Schedule Scan

You can schedule the scanner to scan automatically at predetermined time and intervals. For more details please see [Scheduling Quick Heal Total Security](#).

### Scan initiated by right click handler

You can easily initiate scan by using right click handler. To scan:

1. Right click on the object (Drive, Folder and File) you want to scan.
2. Select **Total Security Scan** from the right click menu.

### Scanning through DOS command line

If you are working in a DOS window, you can easily initiate scan for a specific drive, file or folder, from DOS command line. To scan:

1. In the DOS window prompt, changed to the directory path where you have installed Quick Heal Total Security.
2. At the prompt, type **SCANNER.EXE** and give the path to scan. **For example: Scanner.exe C:\Windows**
3. Press **Enter** to start the scan.

### Scan using DUMB mode

If you are working in a DOS window, you can easily initiate scan for a specific drive, file or folder, from DOS command line. To scan:

1. In the DOS window prompt, changed to the directory path where you have installed Quick Heal Total Security.
2. At the prompt, type **SCANNER.EXE /DUMB**. **For example: Scanner.exe /DUMB**
3. Press **Enter**. Quick Heal Total Security will start in dumb mode.
4. Now select the item you wish to scan.

### Scanning through DOS command line using DUMB mode

Using DOS command line you can scan in dumb mode. To scan using dumb mode:

1. In the DOS window prompt, changed to the directory path where you have installed Quick Heal Total Security.
2. At the prompt, type **SCANNER.EXE /DUMB** and give the path to scan. **For example: Scanner.exe /DUMB C:\Windows**
3. Press **Enter** to start the scan.

### Overview of DUMB mode scanning

Dumb mode scanning is recommended if no virus was detected during an ordinary scanning procedure but the system is still behaving strangely (for example, slow performance of applications, and so on). Otherwise, we do not recommend dumb scanning mode as it noticeably slows down the scanning speed of Quick Heal Total Security.

## SCHEDULING QUICK HEAL TOTAL SECURITY SCANNER

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

You can easily schedule custom scan. Frequency can be set for daily and weekly scans, which additionally can refine your request to schedule it to occur every two days or every three days instead. Further you can also schedule the task to repeat at specific intervals.

### To create a new schedule scan:

1. On the left pane of the main window, under Quick Heal Total Security, click on **Tools**.
2. In the **Tools** pane, click on Schedule Scan. Total Security Scan Scheduler wizard will appear.
3. Select **Create new Schedule Scan** and press **Next**.
4. Name your custom schedule scan under **Name of the Schedule Scan /Task**. For example: My Scan.
5. Select **First Boot** to schedule the scanner to scan at first boot of the day. When you select First Boot in this case you don't have to specify the time of the day to start the scan. Scan will take place only during the first boot no matter at what time you start the system. Otherwise set the frequency and time at which you want to scan the system. Most of the frequency options include additional options (Every day (s) and Repeat Task) that let you further refine your schedule scan. You can also configure the scanner to scan silently (without any user intervention) by selecting **Silent Scan** option. Select the schedule scan priority from **High**, **Normal** and **Low**. Set the additional options as necessary.
6. Provide **User Name** and **Password**.
7. Under **Setting**, you can specify specific items to be scanned, action required to be taken if a virus is found and use of advance options while scanning. By default, setting has been set for adequate options for scanning.
8. When you are done, press **Next**.
9. Click on **Add Folders**.
10. Select the Drives, folder or multiple folders to be scanned and press **Ok**. You can configure **Exclude Subfolder** while scanning of a specific folder. This will ignore scanning inside the subfolders while scanning. e.g. If you select C:\ drive for scan along with selecting Exclude Subfolder option, this will initiate scan for files available at the root of C:\ drive only.
11. Press **Next**.
12. Review the summary of your custom scheduled scan.
13. When you are done, press **Finish**.

### To edit a scheduled scan

You can change the schedule of any scheduled scan. To edit a scheduled scan:

1. On the left pane of the main window, under Quick Heal Total Security, click on **Tools**.
2. In the **Tools** pane, click on Schedule Scan. Total Security Scan Scheduler wizard will appear.
3. Click on **Modify Schedule Scan** and select schedule scan created previously.
4. Press **Next**.
5. Change the schedule as desired.
6. When you are done, press **Next**.
7. Change the scan area as desired.
8. Press **Next**.
9. Review the summary of your custom scheduled scan.
10. When you are done, press **Finish**.

### To delete a scan schedule

You can delete any scan schedule. To delete a scan schedule:

1. On the left pane of the main window, under Quick Heal Total Security, click on **Tools**.
2. In the **Tools** pane, click on Schedule Scan. Total Security Scan Scheduler wizard will appear.
3. Click on **Delete Schedule Scan**.
4. To delete a single schedule scan, select the schedule scan and press **Remove**. To delete all the scheduled scans press **Remove All**.

## USING ONLINE PROTECTION

Online Protection prevents your system from virus attack by continuously monitoring the system and prevents virus infection from e-mail attachments, Internet Downloads, network, ftp, floppy, Data storage devices, CD-DVD ROM file executables and during suspected file copying. 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.

Quick Heal Total Security Online protection is configured to load automatically whenever you start your computer. Online Protection icon appears on the Windows taskbar.

### Disabling Online Protection

It is not recommended to disable Quick Heal Total Security Online Protection. It could be hazardous for your computer and data. But if you wish to do so, it can be done as follows:

#### To disable Online Protection temporarily

1. Right-click on **Total Security Online Protection** icon on the Windows task bar.
2. Click on **Disable**.

You can now see that Online Protection icon's color is changed from Green to Red in Windows System Tray. It means that Online Protection has been disabled temporarily.

#### To disable Online Protection permanently

1. Start **Quick Heal Total Security**.
2. Click on **Options**, under main windows menu of the Quick Heal Total Security.
3. Click on **Online Protection** tab.
4. Uncheck the **Load Online Protection at Windows Startup** option.
5. Press **OK** to apply the changes.



Online Protection will not be loaded when you start your system thereafter.

## USING E-MAIL PROTECTION

E-mail is the most common medium for spreading viruses and other malicious programs. Since e-mail is most widely used for communication, newer viruses are using e-mail as a medium to spread. Virus authors are always looking for new methods to automatically execute their viral codes using some vulnerability amongst popular e-mail clients. Hence, for every user it is very important to have robust mail protection, which will block viruses or malicious programs at transferring level itself. Total Security Mail Protection has been redesigned to provide utmost & best protection to its users. Total Security provides reliable and robust e-mail protection. It supports all e-mail programs that use POP3 communications protocol. Your e-mail messages are scanned automatically for any malicious code content within, and hence you are assured of virus free safe e-mails.

E-mail protection protects you from following threats:

- Viruses received in e-mail and attachments.
- Partial messages.
- E-mail containing vulnerability such as MIME, IFRAME etc.

Below are the following features supported in e-mail protection:

- Scanning of Incoming Mail.
- Silent mode (does not prompt) scanning.
- Remove multiple extension attachment(s).
- Remove Message/Partial type of mails.
- Actions if virus found are "Delete automatically" and "Repair automatically, delete if unsuccessful".
- Backup before cleaning action.
- Scanning of ZIP attachments.
- Attachments Control.
- Trusted e-mail clients allow only trusted email clients to send mails. This prevents new worms from further spreading to a greater extent.
- AntiSpam.

See [Customizing E-mail Protection](#) for further set-up options.

### Disabling E-mail Protection

It is not recommended that you disable Quick Heal E-mail Protection. Your e-mail communication may not remain safe any further, and your system shall be open for vulnerable virus infection through e-mail.

E-mail Protection can also be disabled as follows:

1. Start **Quick Heal Total Security**.
2. Click on **Options**, under main windows menu of the Quick Heal Total Security.
3. Click on **Mail Protection** tab.
4. Uncheck the **Enable E-mail Protection** option.
5. Press **OK** to apply the changes.

## KNOWING ABOUT TRUSTED E-MAIL CLIENTS

E-mail is the most common medium for spreading viruses and other malicious programs. Since e-mail is most widely used for communication, newer viruses are using e-mail as a very easy medium to spread. Virus authors are always looking for new methods to automatically execute their viral codes using some vulnerability amongst popular e-mail clients. **Worms** are also using their own SMTP engine routine to spread their infection.

Trusted e-mail client is an advanced option which authenticates e-mail-sending application on the system before they are sending e-mails. This option will prevent new 'Worms' from further spreading from your system. It contains a default e-mail client list, which is allowed to send e-mails. E-mail client in the default list are Microsoft Outlook Express, Microsoft Outlook, Eudora and Netscape Navigator.



1. In case if the prompt comes for an application, which is known to you for sending e-mail but not added in the Trusted e-mail client list, click **Yes** to add the same.
2. In case if the prompt comes for an application, which is not known to you for sending e-mail then select **No** as it could be a new **Worm**. We also request you to send the same file to [analyze@quickheal.com](mailto:analyze@quickheal.com) for further analysis of the same.

## USING DATA PROTECTION

Data protection can be used to block access to removable drives (viz USB drives, Pen Drives, Memory cards, etc.). This will protect your confidential information in the system from being copied using these drives. Using this feature your system's data cannot be copied to the removable drives. Neither can the data from outside (removable drives) be copied to your system. This way it protects your system and data. This helps to protect infection and data theft.



1. This protection does not imply on floppy drives.

### To enable Data Protection

1. Start **Quick Heal Total Security**.
2. Click on **Options**, under main windows menu of the Quick Heal Total Security.
3. Click on **Data Protection** tab.
4. Select **Data Protection** option.
5. Press **OK** to apply the changes.

## USING STARTUP SCAN

Total Security Startup Scan keeps a watch on the programs trying to get automatic execution control. It also keeps a watch on some of the system files, which are commonly patched (or replaced) by certain worms/backdoors/trojans.

By default it is configured to check these on every boot operation. When a program takes an automatic execution control it can be:

- A program installed by you.
- A program installed without your knowledge, which in case might be a malicious program.

Total Security Startup Scan warns you in both the cases.

### It provides you three options:

<b>Accept</b>	This registers the program or changes with Startup Scan and does not warn from the next boot. If you have installed a program or upgraded an existing program you shall get the warning, which should be registered, once with the Startup Scan. Press A to accept.
<b>Delete</b> <b>OR</b> <b>Repair</b>	If it discovers a new entry in the system, it gives the option to delete. If selected to Delete, it removes the entry of the particular program and sends the file to Quarantine.  If it discovers that some old entry or system file has been modified it gives the option to repair. If Repair is selected it restores the old settings and sends the new file to Quarantine.
<b>Help</b>	It shows in detail what the alarm means. This will help you in deciding the course of action.

### General guideline for choosing the response is:

If you have installed some program and you receive a Startup Scan warning for that program select "**Accept**". If you have not installed any application knowingly and you get a Startup Scan warning choose "**Repair**" / "**Delete**" as this may be a new Trojan/Worm/Backdoor.



This feature is not supported on Windows Vista and Windows Server 2008 Operating system.



## USING MESSENGER

Quick Heal Total Security Messenger provides the trusted link for message delivery between Quick Heal Team and you (the User). It automatically gathers information from our web site and informs you about New Viruses, Hoaxes, Upgrade availabilities and other information. It can be also used from Local Folder or Network path.

Quick Heal Total Security Messenger icon on the tray indicates that the messenger is running. By default Quick Heal Total Security Messenger is configured to load automatically.

The messenger starts blinking along with an Audio Alarm whenever there is a new message. Click on the blinking ball to view the message. A detailed log of messages is also maintained.

Colour	Indicates
Red Colour	Virus Alert.
Amber Colour	Hoax Information.
Green Colour	Upgrade.
Blue Colour	General.

### Viewing Messages

To view the messages, do the following steps:

1. Right click on **Quick Heal Total Security** icon from windows system tray.
2. Click on **View Messages** to open the Newsletter Viewer containing the list of all the messages with date, type and subject.
3. Select the message you want to view.
4. Click on **View** to see the particular message. The message is displayed instantly. You can use **Prev** and **Next** buttons to browse through the other messages. Click **Close** to move back to the Newsletter Viewer.
5. Click **Close** Newsletter Viewer.
6. Click **Minimize** to minimize the Messenger.

### Disabling Messenger

If you turn off Quick Heal Total Security Messenger then you are going to miss the important information related to new threats, updates and other information about Quick Heal Total Security.

**Quick Heal Messenger can also be disabled as follows:**

1. Start **Quick Heal Total Security**.
2. Click on **Options**, under main windows menu of the Quick Heal Total Security.
3. Click on **Messenger** tab.
4. Uncheck the **Enable Messenger** option.
5. Press **Ok** to apply the changes.

### To check the Message Instantly:

By default the messenger is configured to check for the message automatically from Internet. See [Customizing Quick Heal Total Security Messenger](#). You can also check the message any time instantly. To check the message instantly:

1. Right Click on Quick Heal Total Security icon from windows system tray.
2. Select **Check New Messages**

This checks the new message if available on Quick Heal website instantly (subject to the availability of internet). You can also see the status of the messenger, configure Messenger and view message log from here.

## VIEWING REPORTS

Quick Heal Total Security Reports provide detailed information about the different module's functioning & virus scans sessions. Activity Log generates log for the following module:

- Scanner
- Online Protection
- E-mail Protection
- Startup Scan
- Scheduler
- Quick Update
- Memory Scan
- AntiPhishing
- Registry Scan
- Native Scanner
- AntiMalware Scan
- PC2Mobile Scan

### To view reports

1. Start **Quick Heal Total Security**.
2. In the left pane of the Quick Heal Total Security main window, click on **Reports**.
3. Now click on the desirable report section which you want to see.

**Reports** contain a list of activity logs for each module with details such as scan date, scan time & report for different scan session.

- 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. To see previous log, press **Prev**. To see Next log, press **Next**.
- Click **Delete** to delete selected scan log entry.
- Click **Delete All** to delete all scan log entries for that particular module.



**Print** and **Save As** add-ons are provided in Reports.

## STATISTICS

Quick Heal now provides statistics for Online Protection, Email Protection and AntiSpam Protection. Following are the statistics provided by Quick Heal:

Online Protection Statistics	
Number of files scanned	Provides information about total number of files scanned.
Number of infected files	Provides information about total number of infected files found.
Number of suspicious files	Provides information about total number of suspicious files found.
Last file scanned	Provides information about the last scanned file.
Last file found infected	Provides information about the last file which was found infected.
Last infection name	Provides information about the Virus or Malware which was recently detected.
Last file found suspicious	Provides information about the file which was found suspicious recently.

Email Protection Statistics	
Number of emails scanned	Provides information about total number of emails scanned for infection.
Number of emails with attachments	Provides information about total number of email received along with attachments.
Number of infected emails	Provides information about total number of emails found infected.
Number of attachments	Provides information about total number of attachments received.
Number of infected attachments	Provides information about total number of attachments found infected.
Number of suspicious attachments:	Provides information about total number of attachments found suspicious.
Number of multiple extensions attachments blocked	Provides information about total number of attachments blocked having multiple extensions. e.g. .doc.exe.
Number of vulnerable emails blocked	Provides information about total number of vulnerable emails blocked.
Number of attachments blocked by attachment control	Provides information about total number of attachments blocked as per the Attachment control policy.
Type of attachments received by user mostly	Provides information about attachments which is mostly received by the user. e.g. .doc (Office Document file).
Type of attachments blocked mostly	Provides information about attachments which is being blocked mostly as per the Attachment control policy.
Last application blocked attempting to send mail	Provides information about an un-trusted application which was blocked while sending mails as per Trusted Email Client policy.
Number of attempts to send mail blocked	Provides information about total number of attempts of sending mails by un-trusted email clients that were blocked as per Trusted Email Client policy.

AntiSpam Protection Statistics	
Number of emails scanned for spam	Provides information about total number of emails scanned for spam.
Number of spam emails	Provides information about total number of spam emails detected by AntiSpam protection.

Since System Start	Under this category, Quick Heal provides statistics since system start. Statistics under this category are purged on every shutdown or restart.
Since Installation	Under this category, Quick Heal provides statistics since installation.

## VIEWING VIRUS LIST

Quick Heal Total Security Virus List provides an exhaustive database of respective virus names along with their category.

### Viewing Virus List

1. Start **Quick Heal Total Security**.
2. In the left pane of the Quick Heal Total Security main window, click on **Tools**.
3. Click on **Virus List**. For the first time Virus List will take considerable time to load the list.

### Virus List Overview

<b>All Categories</b>	All Categories contains all type of viruses and their specific category in the right pane.
<b>DOS (16 Bit)</b>	DOS (16 Bit) viruses are mentioned in this category.
<b>Linux</b>	Linux viruses are mentioned in this category.
<b>Macro</b>	Macro viruses which infect Office documents, spreadsheets, presentation etc. are mentioned in this category.
<b>Mobile</b>	Mobile threats are mentioned in this category.
<b>Script</b>	Script based viruses are mentioned in this category.
<b>Windows (32 Bit)</b>	Windows (32 bit) viruses are mentioned in this category.

### To find for a virus in the virus list:

1. Click on **Find**.
2. Type the name of virus you want to find.
3. Click on **Find**.



Click **Print** to print the virus list.

<b>Latest</b>	Latest section contains the threats, added in the daily updates.
---------------	--

## QUARANTINE

Quarantine helps in safely isolating the infected or suspected files. When a file is added to Quarantine, Quick Heal Total Security encrypts the file and keeps it inside the Quarantine directory. Being kept in an encrypted form, these files cannot be executed and hence are safe. Quarantine also keeps a copy of infected file before repairing. Backup functionality is available by selecting **Backup before repairing** option under Scanner's settings.

### To launch Quarantine

1. Start **Quick Heal Total Security**.
2. In the left pane of the Quick Heal Total Security main window, click on **Tools**.
3. Click on **Quarantine**.

### You can perform the following tasks with the Quarantine feature:

<b>Add</b>	Add a file to the Quarantine module.
<b>Remove (Delete)</b>	Delete a quarantine file.
<b>Remove All</b>	Delete all the Quarantine files.
<b>Restore</b>	Restore a file from Quarantine to its original location.
<b>Send</b>	You can send the quarantined file to our research lab for further analysis. Select the file which you wish to submit and click <b>Send</b> . A mail will be generated containing the suspected file. A confirmation will be requested before sending the mail.

## SYSTEM INFORMATION

Quick Heal Total Security System Information is an essential tool to gather critical information of a Windows based system for following cases:

To detect new Malwares	This tool gathers information to detect new Malwares from Running processes, Registry, System files like Config.Sys, Autoexec.bat etc.
To get Quick Heal Total Security information	It gathers information of the installed version of Quick Heal Total Security, its configuration settings and Quarantined file(s), if any.

### Submitting System Information file

This tool generates an INFO.QHC file at C:\ and sends the same using default e-mail client to [sysinfo@quickheal.com](mailto:sysinfo@quickheal.com). If there is no default e-mail client, INFO.QHC file will be created at C:\ and you will be asked to send the same at the above mentioned e-mail address, for analyzing the problem of your system.



INFO.QHC file contains information in text and binary format. It contains critical system details and installed Quick Heal Total Security version details. Information contains automatic execution of files (through Registry, Autoexec.bat, System.ini and Win.ini) and Running processes along with their supported library details. These details are used to analyze the system for new Malwares and proper functioning of Quick Heal Total Security. The above information is used to provide better and adequate services to customers. This tool doesn't collect any other personally identifiable information, passwords etc. We respect your privacy; rest assured this information will not be shared or disclosed.

### Generating System Information

To generate system information follow the below given steps:

1. Start **Quick Heal Total Security**.
2. Click on **Tools** from the left pane.
3. Click on **System Information**.
4. Select the system information generating reason. If you are suspecting new Malwares in your system then select **I suspect my system is infected by new Malwares** or if you are facing problem while using Quick Heal Total Security then select **I am having problem while using Quick Heal**. Click **Finish**.
5. System Information (INFO.QHC) will be generated and sent to Quick Heal Technical Support by using default e-mail client settings, or you shall be manually prompted to do so.

## CREATING EMERGENCY CD OR COMMAND LINE SCANNER

You can create your own emergency bootable CD that will help you to boot your Windows PC and scan and clean all the drives including NTFS partitions. This helps in cleaning badly infected PC from file infecting viruses which cannot be cleaned from inside Windows. This feature works on Windows 2000 and above operating system.

You can create an emergency CD or command line scanner from Quick Heal Total Security at any time. This will be created with the latest virus signature pattern file used by Quick Heal Total Security on your system.

### To create an Emergency CD

To create Quick Heal Emergency CD, your system should fulfill following requirements:

- Licensed copy of Microsoft Windows Operating System. (Windows 2000/XP/2003 or above).
- Microsoft Windows Installation CD. (Windows XP/2003)
- A blank writable CD and a CD-Writer drive.
- Emergency CD can only be used to scan and clean drives of the same system for which you have licensed Microsoft Windows operating system.

### Creating Emergency CD:

1. Start **Quick Heal Total Security**.
2. Click on **Tools** from the left pane.
3. Click on **Emergency CD**.
4. Click **Next**.
5. Select **Create Emergency CD**, click **Next**.
6. Bootable files required to make the CD bootable. Select **Operating System Installation CD** option and insert the Operating CD (Windows XP and Windows 2003 operating system CD only). Select the CD-Rom drive.
7. Click **Next**.
8. System files will be fetched from the installation CD.
9. Remove the Operating System Installation CD and insert a blank writable CD.
10. Select the CD-Rom drive.
11. Click **Next**.
12. Emergency CD will be created.

### Creating Emergency CD using system files

If you have created emergency CD earlier by providing Microsoft Windows Installation CD using Emergency CD Creation Wizard. Then you can quickly burn the emergency CD again by following below given steps:

1. Start **Quick Heal Total Security**.
2. Click on **Tools** from the left pane.
3. Click on **Emergency CD**.
4. Press **Next**.
5. Select **System files used earlier while creating emergency CD**.
6. Click **Next**.
7. System files used earlier for CD creation will be fetched automatically.
8. Remove the Operating System Installation CD and insert a blank writable CD.
9. Select the CD-Rom drive.
10. Click **Next**.
11. Emergency CD will be created.

### To create Command line scanner

You can create DOS Command line scanner using Emergency CD wizard.

1. Start **Quick Heal Total Security**.
2. Click on **Tools** from the left pane.
3. Click on **Emergency CD**.
4. Press **Next**.
5. Select **Save Command line scanner** at option provided.
6. Browse the folder or type the path where you wish to create command line scanner.
7. Press **Next**.
8. Command line scanner will be created.

In case if you wish to disinfect the badly infected system it is recommended that write a CD by copying Command line Scanner folder.



See [Using Emergency CD or Command line scanner](#).

## OVERVIEW OF NATIVE BOOT SCAN

Native Boot Scan is an advance administration tools. In short it schedules the system to boot in Windows NT boot shell on next boot. On next start Native Boot scan will start before the desktop is loaded. It scans all drives and detect/clean virus infections on your computer. This activity is quite fast and reliable, without the risk of spreading the infection any further. This will help you in detecting and cleaning even the most cunning Rootkits, spywares, special purpose Trojans and loggers. Additionally Native Boot Scan cleans the registry entries created/modified by malwares.

Native Boot Scan works with **all Windows-supported file systems**, i.e. **FAT32**, **NTFS**, as well as less common storage devices, such as SCSI/RAID. See [Performing Native Boot Scan](#).

## USING QUICK HEAL ANTIMALWARE

Quick Heal AntiMalware is a new advanced malware scanning engine. It scans registry, files and folders at lightening speed to thoroughly detect and clean Spywares, Adwares, Roguewares, Dialers, Riskwares and lots of other potential threats in your system.

### Start Quick Heal AntiMalware

Quick Heal AntiMalware Scan can be started from:

#### Start Quick Heal AntiMalware from Quick Heal Total Security Program Group

To launch Quick Heal AntiMalware, go to **Start Menu->Programs->Quick Heal Total Security** group and click **Quick Heal AntiMalware**.

#### Start Quick Heal AntiMalware from Quick Heal Total Security

1. Start **Quick Heal Total Security**
2. Click **Launch AntiMalware**.
3. Quick Heal AntiMalware program will start.
4. Click **Scan Now** to initiate AntiMalware Scanning.


#### Start Quick Heal AntiMalware from Quick Heal Total Security system tray icon

1. Right click on Quick Heal Total Security system tray icon.
2. Click **Launch AntiMalware**.
3. Click **Scan Now** to initiate AntiMalware Scanning.

### Quick Heal AntiMalware Action on Malware found

While scanning for malwares Quick Heal AntiMalware displays malicious files, folders and registry entries related to various malwares. Once the scanning is complete, a list will be displayed for detected malwares containing malicious files, folders and registry. You can un-check specific file, folder or registry entries within displayed list, but be ensured that all un-checked items are not malicious and belongs to a genuine application.

You can take following action once the scanning is complete:

<b>Clean</b>	Selecting this action will clean the malwares and its remnants from the system. If you have un-checked specific file, folder or registry entry then you will be prompted whether you wish to exclude those items in future scan. If you wish to permanently exclude those items then click <b>Yes</b> , otherwise click <b>No</b> for temporary exclusion.
<b>Skip</b>	Selecting this will not take any action against malwares in your system.
<b>Set System Restore point before cleaning</b>	Selecting this option will create System Restore point before the cleaning process starts in your system. This enables you to revert the cleaning done by Quick Heal AntiMalware by using Windows System Restore facility.  <b>Set System Restore point</b> feature is not available on Windows 2000 and Server Operating system.
<b>Malware Details</b>	Malware details are available at <a href="http://www.quickheal.co.in">http://www.quickheal.co.in</a> website.

### Quick Heal AntiMalware Report

To view detailed AntiMalware scanning report, please refer [Quick Heal Total Security Reports](#) section.



## Quick Heal AntiMalware Settings

<b>Scan for suspicious items</b>	<p>A signature free scanning to detect malware traces based on heuristic. To enable Scan for Suspicious items please follow the below given steps:</p> <ol style="list-style-type: none"><li>1. Start <b>Quick Heal AntiMalware</b>.</li><li>2. Click <b>Settings</b>.</li><li>3. Select <b>Scan for Suspicious items</b></li><li>4. Click <b>OK</b> to save the changes.</li></ol>
<b>Exclusion</b>	<p>You can configure Quick Heal AntiMalware to skip scanning of certain files and folders.</p> <p><b>To exclude a file from AntiMalware scanning:</b></p> <ol style="list-style-type: none"><li>1. Start <b>Quick Heal AntiMalware</b>.</li><li>2. Click <b>Settings</b>.</li><li>3. Click <b>Add File</b>.</li><li>4. Select the file to be excluded and click <b>Open</b>.</li><li>5. Click <b>OK</b> to save the changes.</li></ol> <p><b>To exclude a folder from AntiMalware scanning:</b></p> <ol style="list-style-type: none"><li>1. Start <b>Quick Heal AntiMalware</b>.</li><li>2. Click <b>Settings</b>.</li><li>3. Click <b>Add Folder</b>.</li><li>4. Select the folder to be excluded and click <b>OK</b>.</li><li>5. Click <b>OK</b> to save the changes.</li></ol>

## WHEN QUICK HEAL ANTIMALWARE SHOULD BE USED?

Quick Heal AntiMalware should be used in following cases:

- Quick Heal Online Protection has detected a malware and recommending you to scan your system using Quick Heal AntiMalware.
- Quick Heal Total Security Scanner has detected a malware during scan and recommending you to scan your system using Quick Heal AntiMalware.
- In case of visible changes in your system. e.g. Desktop wallpaper changed, Internet Explorer functionalities changed such as default website and search page are changed, Rougeware applications are installed etc.

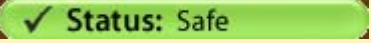
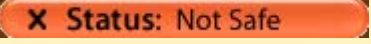
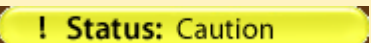
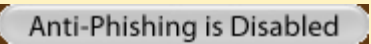
## USING QUICK HEAL ANTI-PHISHING

Quick Heal Total Security prevents you from accessing phishing and fraudulent websites. Phishing is a fraudulent attempt, usually made through email, to steal your personal information. Quick Heal AntiPhishing automatically scans all accessed web pages for fraudulent activity protecting you against any phishing attack as you surf the internet. Prevents identity theft by blocking phishing websites. So you can do online shopping, banking and website surfing safely.

Phishing is generally attempted through emails. It usually appear to come from a well-known organization and ask for your personal information — such as credit card number, social security number, account number or password. Many times phishing attempts appear to come from sites, banks, services and companies with which you do not even have an account. In order for Internet criminals to successfully "phish" your personal information, they must get you to go from an email to a website. Phishing emails will almost always tell you to click a link that takes you to a site where your personal information is requested. Legitimate organizations would never request this information of you via email.

Quick Heal Anti-Phishing is only supported for Microsoft Internet Explorer 5.5 and above. To use Quick Heal Anti-Phishing you need to enable this feature. To enable Quick Heal Anti-Phishing please see [Enable Quick Heal Anti-Phishing](#). Quick Heal Anti-Phishing toolbar is visible in Internet Explorer once it is enabled.

Quick Heal Anti-Phishing shows following tags for websites you are visiting:

Status	Information
 <b>Status: Safe</b>	This tag informs that the website you are visiting is safe.
 <b>Status: Not Safe</b>	This tag informs that the website you are visiting is not safe. Phishing attempts appear to come from this site.
 <b>Status: Caution</b>	This tag informs that you must be cautious while browsing this website. If Quick Heal Anti-Phishing Server is down due to some technical reason all the websites will have Caution tag.
 <b>Anti-Phishing is Disabled</b>	This tag informs that Quick Heal Anti-Phishing is disabled.

While browsing you can use following option in Quick Heal Anti-Phishing toolbar:

<b>Report a Phishing site</b>	Select this option if you wish to report a website which you think is suspicious or doing fraudulent activities. Selecting this option will lend you to <b>Report a Phishing</b> web page on Quick Heal website . Please fill the appropriate information in all the fields. Providing specific information will help our team to analyze the website and take necessary action.
<b>Report an Incorrectly Blocked Phishing site</b>	Select this option if you wish to report a website which you think is incorrectly blocked by Quick Heal Anti-Phishing. Selecting this option will lend you to <b>Report an Incorrectly Blocked</b> web page on Quick Heal website. Please fill the appropriate information in all the fields. Providing specific information will help our team to analyze the website and take necessary action.
<b>Disable Quick Heal Anti-Phishing Toolbar</b>	Select this option to disable Quick Heal Anti-Phishing. Selecting this option will stop automatic scanning of websites for fraudulent activities.
<b>Enable Quick Heal Anti-Phishing Toolbar</b>	Select this option to enable Quick Heal Anti-Phishing. Selecting this option will start automatic scanning of websites for fraudulent activities.
<b>Help</b>	Select this option to get the help related to Quick Heal Anti-Phishing.

### Incompatibility with Internet Explorer 7's Anti-Phishing

Microsoft's Internet Explorer 7.0 also has Anti-Phishing toolbar feature. It has been observed that if two anti-phishing toolbars are installed and used simultaneously you may experience inconsistent results or your browsing speed may slow down. It is not recommended to run Quick Heal Anti-Phishing toolbar along with Internet Explorer's own anti-phishing toolbar. Running two or more anti-phishing toolbar could affect your browsing experience. You will be prompted accordingly when you try to enable Quick Heal Anti-Phishing toolbar along with Microsoft's Anti-Phishing toolbar.

<b>Disable Internet Explorer's Anti-Phishing, Enable Quick Heal Anti-Phishing</b>	Select this option if you wish to use Quick Heal Anti-Phishing.
<b>Keep Internet Explorer's Anti-Phishing enabled.</b>	Select this option if you wish to use Internet Explorer's Anti-Phishing

## USING EXTRA TOOLS

Quick Heal Total Security consists of advanced tools which can help user by performing following activities:

- Restore the default Internet Explorer settings.
- Restore the important system settings.
- Remove all known lists that can expose your privacy.
- Provide important information of an application.
- Provide all important information related to your computer such as running process, installed BHO's, toolbars installed in Internet Explorer, installed ActiveX, Hosts, LSPs, Startup Programs, Internet Explorer settings and Active network connection.

## HIJACK RESTORE

Hijack Restores, restores the important Internet Explorer settings to default settings. Internet Explorer settings modified by Malwares, Spywares, Genuine applications and even by you can be easily restored to default setting using Hijack restore. This tool also restores certain other critical operating system settings like registry editor and task manager.

### Using Hijack Restore

1. Start **Quick Heal Total Security**.
2. In the left pane of the Quick Heal Total Security main window, click on **Extra**.
3. Click **Hijack Restore**.

Restoring Internet Explorer Browser Settings	
<b>Settings</b>	This section displays the important Internet Explorer settings which can be restored using Hijack Restore.
<b>Current Settings</b>	This section displays the current Internet Explorer settings.
<b>Previous/Default Settings</b>	This sections displays the last or default Internet Explorer settings.
<b>Check All</b>	Select all Internet Explorer to restore previous or default settings.
<b>Restore default Host file</b>	Select this option to restore default Host file. Click <b>Default Host file</b> to configure your own Host file so that during restore of the host file your settings are well preserved. Type the IP address and Host name and click <b>Add</b> . To edit the existing entry select the entry and click <b>Edit</b> . To delete select the entry and click <b>Delete</b> .
<b>Restore important system settings</b>	Critical system settings can be restored using this option. This settings generally modified by the Malware/Spywares to disable specific and important feature of the Operating System such as Registry Editor, Task Manager etc.
<b>Restore Now</b>	Restores the Internet Explorer settings to its default or at previous stage. You can restore specific settings by selecting specific settings and click <b>Restore Now</b> . To restore all the settings select <b>Check All</b> and click <b>Restore Now</b> .
<b>Undo</b>	This feature revert the last restoration and giving a chance to user to undone the changes.

## WINDOWS SPY

This tool can be used to find out more information about an application or process whenever required. At times it happens that we keep on getting dialog boxes or messages that are shown by spyware or some malware and we are not able to locate the malware. In such situation this tool can be used to find out more information about the application by dragging the target on to the dialog or window that appears on the screen. This tool will provide following information about the dialog or a window.

- Application Name
- Original File Name
- Company Name
- File Description
- File Version
- Internal Name
- Product Name
- Product Version
- Copyrights Information
- Comments

### Using Windows Spy

1. Start **Quick Heal Total Security**.
2. In the left pane of the Quick Heal Total Security main window, click on **Extra**.
3. Click **Windows Spy**.
4. Click at Drag and move the mouse pointer on the application.
5. A window will be opened displaying above mentioned information.
6. If you wish to terminate that application or window then click **Kill Process**.

## TRACK CLEANER

Track Cleaner removes the entire list that expose your privacy. Many applications store the list of recently opened files in their internal format to help you open them again for easy of use purpose. This feature of Windows is good but at the same time on the systems which is used by more than one user it may happen that the users privacy is compromised. Track Cleaner helps delete all the tracks of such applications and prevent privacy.

### Using Track Cleaner

1. Start **Quick Heal Total Security**.
2. In the left pane of the Quick Heal Total Security main window, click on **Extra**.
3. Click **Track Cleaner**.
4. To clear the privacy item, select the application and item that should be cleaned and click **Start Cleaning**.
5. The selected items will be cleaned.
6. To clear all the privacy item, select **Check All** and click **Start Cleaning**.
7. All items will be cleaned.

## ADVANCED SYSTEM EXPLORER

This tool provides all important information related to your computer such as running process, installed BHO's, toolbars installed in Internet Explorer, installed ActiveX, Hosts, LSPs, Startup Programs, Internet Explorer settings and Active network connection. This will help diagnose the system for tracing existence of any new malware or riskware.

## ABOUT SECTION

Quick Heal Total Security About section provides following information:

- Quick Heal Total Security Version
- Quick Heal Total Security Virus Database
- License Information

Following options are also available in About Section:

<b>License Details</b>	<p>License Information and End User License Agreement (EULA) are available under this section.</p> <p><b>Update License Details:</b> This feature is pretty useful to synchronize your existing License information with Quick Heal Activation Server. e.g. Suppose you wish to renew your existing subscription and you do not know how to renew it or facing problem during renewal. You can call Quick Heal Support team; provide your Serial Number, Activation Number and Renewal Code. Quick Heal Support team will renew your copy. You just need to follow the below given steps:</p> <ol style="list-style-type: none"><li>1. Be connected to Internet.</li><li>2. Click <b>Update License Details</b></li><li>3. Click <b>Continue</b> to update your existing subscription.</li></ol> <p><b>Print License Details:</b> Click <b>Print License Details</b> to print the existing subscription information.</p>
<b>Activate Now</b>	<p>If Quick Heal Total Security is not activated then <b>Activate Now</b> button is available in About section. Activate Now helps you to activate your copy.</p>
<b>Renew Now</b>	<p>Renew Now helps you to renew your existing subscription.</p>
<b>Support</b>	<p>Support section provides information about Technical Support guidelines and Quick Heal Support's contact details. You can locate the nearest Quick Heal Support team.</p>
<b>Remote Support</b>	<p>Quick Heal Technical Support Team also provides Remote Support in some cases. Quick Heal Remote Support module helps us to easily connect to your PC through the Internet and provide remote support. This helps us to give you efficient remote support as if our technical executives are there in front of your PC. No installation is required. Please follow the below given to use Remote Support:</p> <ol style="list-style-type: none"><li>1. You just need to click <b>Remote Support</b> to activate the Remote Support Agent on your system.</li><li>2. Contact Quick Heal Support team</li><li>3. Provide the <b>ID</b> available in Quick Heal Remote Support Agent to Quick Heal Support executive.</li><li>4. Quick Heal Support executive will remotely access your system to fix the issue.</li></ol>

# Chapter 4

## USING PC2MOBILE SCAN

**Quick Heal PC2Mobile Scan** feature is available in **Quick Heal Total Security**. This feature scans for viruses, spywares and other malwares in mobile phone. To scan your mobile device you need to connect it to PC using any of the following methods:

- USB Cable or
- Bluetooth

List of all the PC2Mobile Scan supported mobile is given below. Some mobile phones can be connected to PC by both the methods USB cable as well as Bluetooth. In such case we recommend using USB Cable instead of Bluetooth as it gives better results when using PC2Mobile Scan feature. Quick Heal PC2Mobile Scan supports following mobile:

### Kyocera

Kyocera-SE44

### LG

LG-KE970, LG-KG320, LG-LX1200, LG-VI5225, LG-VX4400, LG-VX6000, LG-VX6100, LG-VX7000, LG-B2100, LG-KG328

### Motorola

Motorola-A1000, Motorola-A835, Motorola-C385, Motorola-C650, Motorola-E1, Motorola-E1000, Motorola-E1070, Motorola-E398, Motorola-E550, Motorola-K1, Motorola-K1v, Motorola-L2, Motorola-L6, Motorola-L7, Motorola-L7e, Motorola-L7v, Motorola-L9, Motorola-U6, Motorola-V1075, Motorola-V180, Motorola-V186, Motorola-V220, Motorola-V235, Motorola-V3, Motorola-V300, Motorola-V360, Motorola-V3i, Motorola-V3iv, Motorola-V3x, Motorola-V3xv, Motorola-V3xx, Motorola-V500, Motorola-V505, Motorola-V525, Motorola-V547, Motorola-V551, Motorola-V6, Motorola-V600, Motorola-V620, Motorola-V635, Motorola-V80, Motorola-V975, Motorola-E770, Motorola-K3, Motorola-V3xxv, Motorola-W490, Motorola-Z3

### Nokia

Nokia-3100, Nokia-3105, Nokia-3120, Nokia-3200, Nokia-3220, Nokia-3510i, Nokia-3650, Nokia-3660, Nokia-5140, Nokia-5140i, Nokia-5200, Nokia-5300 XpressMusic, Nokia-6020, Nokia-6021, Nokia-6070, Nokia-6080, Nokia-6085, Nokia-6100, Nokia-6101, Nokia-6103, Nokia-6111, Nokia-6125, Nokia-6131, Nokia-6151, Nokia-6170, Nokia-6220, Nokia-6225, Nokia-6230, Nokia-6230i, Nokia-6233, Nokia-6234, Nokia-6260, Nokia-6280, Nokia-6288, Nokia-6300, Nokia-6600, Nokia-6610, Nokia-6610i, Nokia-6630, Nokia-6681, Nokia-6800, Nokia-6810, Nokia-6820, Nokia-6822, Nokia-7200, Nokia-7210, Nokia-7250, Nokia-7250i, Nokia-7260, Nokia-7270, Nokia-7280, Nokia-7360, Nokia-7373, Nokia-7380, Nokia-7390, Nokia-7600, Nokia-7610, Nokia-7650, Nokia-7710, Nokia-8800, Nokia-8910i, Nokia-9300, Nokia-9300i, Nokia-9500, Nokia-E50, Nokia-E61, Nokia-E65, Nokia-N70, Nokia-N73, Nokia-N80, Nokia-N90, Nokia-N95, Nokia-N-Gage, Nokia-N-Gage QD, Nokia-3110Classic, Nokia-3230, Nokia-6101b, Nokia-6102, Nokia-6270, Nokia-6500, Nokia-E61i

### Panasonic

Panasonic-X700

## **Samsung**

Samsung-SCH-U420, Samsung-SGH-D500, Samsung-SGH-D500E, Samsung-SGH-D600E, Samsung-SGH-D820, Samsung-SGH-D830, Samsung-SGH-D900, Samsung-SGH-E100, Samsung-SGH-E250, Samsung-SGH-E330, Samsung-SGH-E330N, Samsung-SGH-E335, Samsung-SGH-E360, Samsung-SGH-E530, Samsung-SGH-E570V, Samsung-SGH-E630, Samsung-SGH-E700, Samsung-SGH-E720, Samsung-SGH-E760, Samsung-SGH-E770, Samsung-SGH-E800, Samsung-SGH-E900, Samsung-SGH-P300, Samsung-SGH-X100, Samsung-SGH-X210, Samsung-SGH-X460, Samsung-SGH-X600, Samsung-SGH-X650, Samsung-SGH-X660, Samsung-SGH-X820, Samsung-SGH-Z300, Samsung-SGH-Z400V, Samsung-SGH-Z540V, Samsung-SGH-ZV10, Samsung-SGH-ZV40, Samsung-SPH-A660, Samsung-SGH-D600, Samsung-SGH-E340, Samsung-SGH-E390, Samsung-SGH-S400i, Samsung-SGH-S401i, Samsung-SGH-U600, Samsung-SGH-X510, Samsung-SGH-X660V, Samsung-SGH-X830, Samsung-SGH-Z320i, Samsung-SGH-Z400, Samsung-SGH-Z500V, Samsung-SGH-Z560V, Samsung-SGH-Z650i, Samsung-SGH-Z720

## **Sharp**

Sharp-550SH, Sharp-703SH, Sharp-770SH, Sharp-GX17, Sharp-GX29, Sharp-GX33, Sharp-GX40

## **Siemens**

Siemens-A65, Siemens-A75, Siemens-AX75, Siemens-C55, Siemens-C60, Siemens-C65, Siemens-C72, Siemens-C75, Siemens-CF62, Siemens-CF75, Siemens-CX65, Siemens-CX70, Siemens-CX75, Siemens-CXT65, Siemens-M50, Siemens-M55, Siemens-M65, Siemens-M75, Siemens-MC60, Siemens-ME45, Siemens-ME75, Siemens-MT50, Siemens-S35i, Siemens-S45, Siemens-S45i, Siemens-S55, Siemens-S65, Siemens-SK65, Siemens-SL45, Siemens-SL45i, Siemens-SL55, Siemens-SL65, Siemens-SX1

## **Sony Ericsson**

Sony Ericsson-D750i, Sony Ericsson-J300i, Sony Ericsson-K300i, Sony Ericsson-K310i, Sony Ericsson-K320i, Sony Ericsson-K500i, Sony Ericsson-K510i, Sony Ericsson-K600i, Sony Ericsson-K610i, Sony Ericsson-K700i, Sony Ericsson-K750i, Sony Ericsson-K790i, Sony Ericsson-K800i, Sony Ericsson-P800, Sony Ericsson-P900, Sony Ericsson-P910i, Sony Ericsson-S700i, Sony Ericsson-T610, Sony Ericsson-T630, Sony Ericsson-V630i, Sony Ericsson-W200i, Sony Ericsson-W300i, Sony Ericsson-W550i, Sony Ericsson-W610i, Sony Ericsson-W700i, Sony Ericsson-W710i, Sony Ericsson-W800i, Sony Ericsson-W810i, Sony Ericsson-W850i, Sony Ericsson-W880i, Sony Ericsson-W900i, Sony Ericsson-Z1010, Sony Ericsson-Z310i, Sony Ericsson-Z520i, Sony Ericsson-Z530i, Sony Ericsson-Z550i, Sony Ericsson-Z600, Sony Ericsson-Z610i, Sony Ericsson-Z710i, Sony Ericsson-K550i, Sony Ericsson-K810i, Sony Ericsson-K850i

We regularly keep on adding support for new models. For latest updated list of supported mobile devices please visit <http://www.quickheal.co.in/pc2mobile.asp>



We regularly keep on adding support for new models. For latest updated list of supported mobile devices please keep watch on <http://www.quickheal.co.in/pc2mobile.asp>



## IMPORTANT REQUIREMENTS FOR PC2MOBILE SCAN

- This feature is only supported on 32-bit Operating Systems of Microsoft Windows XP and Vista.
- For Windows Mobile based devices you should have Microsoft Active Sync 4.0 or above installed on PC.
- For Nokia Phones, Nokia PC Suite software is recommended to be installed on the PC. For all other mobile phones it is recommended to have respective vendor software drivers installed on the PC.
- For Bluetooth connection PC should have Bluetooth device with appropriate drivers properly installed.
- For Bluetooth device only Microsoft, Broadcom and Widcomm drivers are supported. For better results we recommended to install Microsoft drivers for Bluetooth device.
- For Bluetooth connection between mobile device and PC some of the phone models need to have Quick Heal Connector installed on the mobile device. Quick Heal Mobile connection wizard will help you install Quick Heal Connector in your mobile device. Mobile phones that needs to have Quick Heal connector installed for scanning are: Nokia 3650, Nokia 3660, Nokia 7650, Nokia N-Gage, Nokia N-Gage QD, Panasonic X700, Siemens SX1, Nokia 3230, Nokia 6260, Nokia 6600, Nokia 6630, Nokia 6670, Nokia 6680, Nokia 6681, Nokia 7610, Nokia N70, Nokia N90, Nokia E50, Nokia E61, Nokia E65, Nokia N73, Nokia N80, Nokia N95, Nokia 9300, Nokia 9500, Nokia 7710, Motorola A1000, Sony Ericsson P800, Sony Ericsson P900 and Sony Ericsson P910i.
- **Windows Mobile** - All Windows SmartPhones having Operating System Windows Mobile version 3.0 and above are supported. e.g. O2, HP, HTC, i-mate, Motorola, Samsung, Siemens, T-Mobile.

## CONFIGURING WINDOWS MOBILE PHONE BEFORE SCAN

To configure your Windows Mobile Phone, please follow the below given steps:

1. Connect your Window SmartPhone to PC or Laptop through USB Cable.
2. Ensure that Microsoft Active Sync 4.0 or above is installed and running.
3. Start **Quick Heal Total Security**.
4. In the Quick Heal Total Security main window, click **Scan** on the left pane.
5. In the **Scan** pane, select **Mobile** tab.
6. Click **Add Mobile**.
7. Select **Windows Mobile Phone** and click **Next**.
8. Total Security Mobile Connection Wizard will search for Windows Mobile attached to your computer.
9. Upon successful detection of Windows Mobile, click **Finish** to complete the mobile configuration.

Once Windows Mobile is successfully configured, it will be added in the Mobile List.

## SCANNING WINDOWS MOBILE

To scan a Windows Mobile, follow the below given steps:

1. Start **Quick Heal Total Security**.
2. In the Quick Heal Total Security main window, click **Scan** on the left pane.
3. In the **Scan** pane, select **Mobile** tab.
4. Select the Mobile Phone from the list.
5. Click on **Scan** to start scanning.

### Scanning Notification for Windows Mobile Phone when connected to PC

When you connect your Windows Mobile Phone to PC using USB cable, Quick Heal Total Security PC2Mobile automatically detects and prompt you for Scan.

## CONFIGURING OTHER MOBILE PHONE BEFORE SCAN

Other Mobile Phones can be configured to your PC by following methods:

[Connection through Bluetooth](#)  
[Connection through USB Cable](#)

## CONNECTION THROUGH BLUETOOTH

To configure your mobile phone via Bluetooth, please follow the below given steps:

1. Connect your Mobile phone to PC or Laptop through Bluetooth.
2. Ensure that you are able to connect your mobile phone through your PC via Bluetooth.
3. Start **Quick Heal Total Security**.
4. In the Quick Heal Total Security main window, click **Scan** on the left pane.
5. In the **Scan** pane, select **Mobile** tab.
6. Click **Add Mobile**.
7. Select **Other Mobile Phone**.
8. Select your Mobile phone from Mobile phone List and click **Next**.
9. Mobile Connection Wizard will search your mobile phone and displays available Bluetooth connections to your computer.
10. Select your mobile phone from the list of Bluetooth connection and click **Next**.
11. If your mobile phone requires Quick Heal Connector to be installed on your Mobile, you will be prompted to Install Connector on your mobile phone. Follow below given steps to install Quick Heal Connector in your mobile phone.
  - a. Click **Install Connector**
  - b. Total Security Mobile Connection wizard will send **Quick Heal Connector** installer to your mobile phone.
  - c. You will receive a message on your mobile phone. View the message to install Quick Heal Connector on your mobile phone. After installation **Start Quick Heal Connector** from mobile.
  - d. Click **Next**.
12. Click **Finish** to complete the configuration.

Once Bluetooth Mobile is successfully configured, it will be added in Quick Heal Total Security Mobile List.

## SCANNING OTHER MOBILE PHONE THROUGH BLUETOOTH

To scan Other Mobile Phone via Bluetooth, please follow the below given steps:

1. Connect your Mobile phone to PC or Laptop through Bluetooth.
2. Ensure that you are able to connect your mobile phone through your PC via Bluetooth.
3. Start **Quick Heal Total Security**.
4. In the Quick Heal Total Security main window, click **Scan** on the left pane.
5. In the **Scan** pane, select **Mobile** tab.
6. Select the Mobile Phone from the list.
7. Click **Scan** to start scanning.

## CONNECTION THROUGH USB CABLE

To configure your mobile phone via Cable, please follow the below given steps:

1. Connect your Mobile phone to PC or Laptop through Cable.
2. Ensure that you are able to connect your mobile phone through your PC via Cable.
3. Start **Quick Heal Total Security**.
4. In the Quick Heal Total Security main window, click **Scan** on the left pane.
5. In the **Scan** pane, select **Mobile** tab.
6. Click **Add Mobile**.
7. Select **Other Mobile Phone**.
8. Select you Mobile phone from Mobile phone List and click **Next**.
9. Click on **Finish** to complete mobile phone configuration.

Once Cable Mobile is successfully configured, it will be added in Mobile List.

## SCANNING OTHER MOBILE PHONE THROUGH CABLE

To scan Other Mobile Phone via Cable, please follow the below given steps:

1. Connect your Mobile phone to PC or Laptop through Cable.
2. Ensure that you are able to connect your mobile phone through your PC via Cable.
3. Start **Quick Heal Total Security**.
4. In the Quick Heal Total Security main window, click **Scan** on the left pane.
5. In the **Scan** pane, select **Mobile** tab.
6. Select the Mobile Phone from the list.
7. Click **Scan** to start scanning.

## USING QUICK HEAL ANTI-ROOTKIT

Quick Heal Anti-Rootkit is a program that proactively detects and cleans rootkits that are active in the system. This program scans objects like running Processes, Windows Registry and Files and Folders for any suspicious activity and detects the rootkits without any signatures. It detects most of the existing rootkits and is designed to detect the upcoming rootkits and also provides the option to clean them.

It is recommended that Quick Heal Anti-Rootkit should be used by person having certain knowledge of the operating system or with the help of Quick Heal Technical Support engineer. Improper usage of this program could result in unstable system.

### To Start Quick Heal Anti-Rootkit from Quick Heal Total Security

1. Start **Quick Heal Total Security**
2. In the left pane of main window click on **Tools**.
3. Click on **Quick Heal Anti-Rootkit** (icon with R on the shield).
4. **Quick Heal Anti-Rootkit** program will start.

### Using Quick Heal Anti-Rootkit

1. Start **Quick Heal Anti-Rootkit**
2. In the left side of the main window click on **Start Scan**
3. **Quick Heal Anti-Rootkit** will start scanning your system for suspicious rootkit activity in running Processes, windows registry and Files and Folders.
4. After completing the scan result is displayed in three different tabs that will display hidden items in running Processes, Windows Registry, Files and Folders.
5. You can now select and take appropriate action against each displayed threat. Like you can terminate the rootkit Process, rename the rootkit Registry entry/Files and Folders.
6. After taking the appropriate action you need to restart your system so that rootkit cleaning take place.

<p><b>Stop Scanning</b></p> <p><b>Close</b></p>	<p>During scan you can select <b>Stop Scan</b> to stop the scan, Quick Heal Anti-Rootkit will prompt before stopping the scan.</p> <p>Click <b>Close</b> to quit Quick Heal Anti-Rootkit. If you choose to close the application while scanning is in progress, it will prompt to stop the scan.</p>
<p><b>Error Report Submission</b></p>	<p>Due to infection or some unexpected conditions in system, scanning of Quick Heal Anti-Rootkit may fail. On failure you will be asked to re-scan your system and submit error report to Quick Heal Team for further analysis.</p>

## CONFIGURING QUICK HEAL ANTI-ROOTKIT

With the help of Scan Settings you can select what item to scan during scan process.

### Configuring Quick Heal Anti-Rootkit for Scan

1. Start **Quick Heal Anti-Rootkit**
2. Click on the **Settings** button on top bar of Quick Heal Anti-Rootkit
3. **Settings** dialog box will appear.
4. By default Quick Heal Anti-Rootkit is configured for **Auto Scan** where it scans appropriate predefined system areas.

<b>Auto Scan</b>	<p>Auto Scan is default scan option provided by Quick Heal Anti-Rootkit. Under Auto Scan Quick Heal Anti-Rootkit scans appropriate predefined system areas. During Auto Scan, scanning is performed for:</p> <ul style="list-style-type: none"><li>• Hidden Processes.</li><li>• Hidden Registry entries.</li><li>• Hidden Files and Folders.</li><li>• Executable ADS.</li></ul>
<b>Custom Scan</b>  <b>Detect Hidden Process</b> <b>Detect Hidden Registry Items</b> <b>Detect Hidden files and folders</b>  <b>Scan drive on which operating system is installed.</b> <b>Scan all fixed drives</b>  <b>Alternate Data Streams (ADS)</b>	<p>By selecting <b>Custom Scan</b> radio button, you can configure following options:</p> <p>To scan for running hidden processes in the system.</p> <p>To scan for hidden items in Windows Registry.</p> <p>To scan for hidden files and folders in the system and executable ADS (Alternate Data Streams). You can choose option:</p> <ol style="list-style-type: none"><li>1. Scan drive on which Operating System is installed.</li><li>2. Scan All Drives to perform scanning in all fixed drives.</li><li>3. Alternate Data Streams (ADS) to scan for executable ADS.</li></ol> <p>Will scan for hidden files and folders on the drive on which operating system is installed.</p> <p>Will scan for hidden files and folders on all the fixed drives of the system.</p> <p>To scan for suspicious items in Alternate Data Streams of NTFS File system.</p>
<b>Report File Path</b>	<p>Quick Heal Anti-Rootkit creates a scan report file at the location from which it is executed. You can specify different location by specifying report file path.</p>

### Overview of Alternate Data Streams - ADS

ADS allows data to be stored in hidden files that are linked to a normal visible file. Streams are not limited in size and there can be more than one stream linked to a normal file. The primary reason why ADS is a security risk is because streams are almost completely hidden and represent possibly the closest thing to a perfect hiding spot on a file system - something trojans can and will take advantage of. Streams can easily be created/written to/read from, allowing any trojan or virus author to take advantage of a hidden file area.

## SCANNING RESULTS AND CLEANING ROOTKITS

### Quick Heal Anti-Rootkit Scanning

1. Start **Quick Heal Anti-Rootkit**
2. In the left side of the main window click on **Start Scan**
3. **Quick Heal Anti-Rootkit** will start scanning your system for suspicious rootkit activity in running Processes, Windows Registry and Files and Folders.
4. After completing the scan result is displayed in three different tabs that will display hidden items in running Processes, Windows Registry and Files and Folders.
5. You can now select and take appropriate action against each displayed threat. Like you can terminate the rootkit Process or rename the rootkit Registry entry or Files.
6. After taking the appropriate action you need to restart your system so that rootkit cleaning take place.

### Action to be taken on Scan Results

<b>Process</b>	<p>After scanning Quick Heal Anti-Rootkit will detect and display a list of hidden Processes. You can select process or process for termination, but make sure that list of Processes for termination doesn't include any know trusted process.</p>
<b>Terminating Hidden Process</b>	<p>Quick Heal Anti-Rootkit also displays summary of process scanning as total number of Processes scanned and number of hidden Processes detected.</p> <p>After selecting list of Processes for termination click on Terminate button. If a process is successfully terminated then its PID (Process Identifier) field will show <b>n/a</b> and process name will be appended by <b>Terminated</b>. All terminated Processes will be renamed after a restart.</p>
<b>Registry</b>	<p>Similar to process scan Quick Heal Anti-Rootkit will display a list of hidden Registry key's. You can select keys for renaming, but make sure that list of key's for renaming doesn't include any known trusted registry key.</p>
<b>Renaming Hidden Registry Key</b>	<p>Quick Heal Anti-Rootkit also displays summary of Registry scanning as total number of items scanned and number of hidden items detected.</p> <p>After selecting list of key's for renaming click on Rename button. Renaming operation requires reboot hence Key name will be prefixed by <b>Rename Queued</b>.</p>
<b>Files and Folders</b>	<p>Similar to process and Registry Quick Heal Anti-Rootkit will display a list of hidden Files and Folders. You can select Files and Folders for renaming, but make sure that list of Files and Folders for renaming doesn't include any know trusted file.</p>
<b>Renaming Hidden Files and Folders</b>	<p>Quick Heal Anti-Rootkit also displays list of executable Alternate Data Streams.</p> <p>Quick Heal Anti-Rootkit also displays summary of File scanning as total number of files scanned and number of hidden files detected.</p> <p>After selecting list of Files and Folders for renaming click on Rename button. Renaming operation requires reboot hence Files and Folders name will be prefixed by <b>Rename Queued</b>.</p>

## CLEANING ROOTKITS THROUGH QUICK HEAL EMERGENCY CD

In some cases it may happen that rootkits are not being cleaned. They are reappearing during Quick Heal Anti-Rootkit scan. In such case you can also use Quick Heal AntiVirus Emergency CD for proper cleaning. All you have to do is create a Quick Heal Emergency CD and boot your system through it. To create a Quick Heal Emergency CD and clean your system through it please follow the below given steps:

### Steps 1

#### To create an Emergency CD

To create Quick Heal Emergency CD, your system should fulfill following requirements:

- Licensed copy of Microsoft Windows Operating System. (Windows 2000/XP/2003 or above).
- Microsoft Windows Installation CD. (Windows XP/2003 or above)
- A blank writable CD and a CD-Writer drive.
- Emergency CD can only be used to scan and clean drives of the same system for which you have licensed Microsoft Windows operating system.

#### Creating Emergency CD:

1. Start **Quick Heal Total Security**.
2. Click on **Tools** from the left pane.
3. Click on **Emergency CD**.
4. Click **Next**.
5. Select **Create Emergency CD**, click **Next**.
6. Bootable files required to make the CD bootable. Select **Operating System Installation CD** option and insert the Operating CD (Windows XP and Windows 2003 operating system CD only). Select the CD-Rom drive.
7. Click **Next**.
8. System files will be fetched from the installation CD.
9. Remove the Operating System Installation CD and insert a blank writable CD.
10. Select the CD-Rom drive.
11. Click **Next**.
12. Emergency CD will be created.

### Steps 2

1. Start **Quick Heal Anti-Rootkit**
2. In the left side of the main window click on **Start Scan**
3. **Quick Heal Anti-Rootkit** will start scanning your system for suspicious rootkit activity in running Processes, Windows Registry and Files and Folders.
4. After completing the scan result is displayed in three different tabs that will display hidden items in running Processes, Windows Registry and Files and Folders.
5. You can now select and take appropriate action against each displayed threat. Like you can terminate the rootkit process or rename the rootkit registry entry or files.

### Steps 3

1. Boot your system using **Quick Heal Emergency CD**.
2. **Quick Heal Emergency CD** will automatically scan and clean the rootkits from your system during native scan.

## CUSTOMIZING QUICK HEAL TOTAL SECURITY

Quick Heal Total Security is provided with various options for customizing. You can easily configure Quick Heal Total Security as per your requirements. By default, Quick Heal Total Security is configured to provide the ideal protection for most of the computing environments.



We recommend you not to change the preset options unless they are specifically required.

### To configure options

All the options related to the customization are available under **Options**, in the main window menu of Quick Heal Total Security. To configure the options do following:

1. Start **Quick Heal Total Security**.
2. Click on **Options**, under the top menu of the Quick Heal Total Security.

### To restore default settings of Quick Heal

You can change any or all of the options provided under the **Options** tab. Also, you can restore the default settings at any point of time.

To restore default settings on the Options page	On the page for which you want to restore default settings, click <b>Default</b> .
To restore default settings for all options	On any page in the Options window, click <b>Default All</b> .



If you have set password protection for **Options**, Quick Heal Total Security will promptly ask you for the password before you can view or change the settings.

## SCANNER - SCAN OPTIONS

The Scanner settings will affect the scanning during manual scans. Scanner primarily contains the following options:

### What items to scan?

You can specify which files to scan by specifying their extensions. By default, Quick Heal Total Security 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.

<b>Executable Files</b>	It covers the most common executable extensions. Quick Heal Total Security looks at the file and finds if it contains executable code or not and scans only the files having executable codes.
<b>All files</b>	It scans for all the files irrespective of whether it contains executable code or not. This reduces the scanning speed and hence is recommended only after a virus attack is discovered.
<b>User Specified Extensions</b>	<p>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.</p> <p><b>Customizing User Specified Extensions</b></p> <ol style="list-style-type: none"><li>1. Select <b>User Specified Extensions</b></li><li>2. Press <b>Customize</b> button.</li><li>3. The default list includes most of the program file extensions. In case some of your applications use some other extensions, add them to this list to include it for scanning.</li></ol> <p><b>To add an extension</b></p> <ol style="list-style-type: none"><li>1. Feed the extension <b>Add</b> box.</li><li>2. Click <b>Add</b>.</li></ol> <p><b>To remove a program file extension</b></p> <ol style="list-style-type: none"><li>1. Select the file extensions in the <b>User Defined Extensions</b> list box.</li><li>2. Click <b>Delete</b>.</li></ol> <p>To reintroduce the original list, click on <b>Default</b>.</p>



## How to respond when a virus is found

This option allows the user to configure following activities when a virus is found during a scan:

<b>Repair Automatically, Delete if unsuccessful</b>	During a scan if a virus is found, then it will repair the virus without any interaction with you. If the file cannot be repaired it will be automatically deleted from your computer. When the scan is over, a summary window appears providing details about all the actions taken and other scan details. If the infectious file is a Backdoor, Worm, Trojan, or Malware then Quick Heal Total Security automatically deletes the file.
<b>Repair Automatically, Quarantine if unsuccessful</b>	During a scan if a virus is found, then it will repair the file or automatically quarantine it, if it cannot be repaired. When the scan is over, a summary window appears providing details about all the actions taken and other scan details. If the infectious file is a Backdoor, Worm, Trojan, or Malware then Quick Heal Total Security automatically deletes the file.
<b>Delete Automatically</b>	Deletes a virus-infected file without notifying you. When the scan is over, a summary window appears providing details about all the actions taken and other scan details. Files deleted in such a manner cannot be recovered.
<b>Prompt</b>	<p>Informs you when a virus is found and allows you to choose how to respond. When the scan is over, a summary window appears providing details about all the actions taken and other scan details. Herein following options are provided, to act upon the infected file:</p> <ul style="list-style-type: none"><li>• Repair, delete if unsuccessful</li><li>• Repair, quarantine if unsuccessful</li><li>• Skip</li><li>• Delete</li><li>• Quarantine</li></ul> <p><b>Apply action to all:</b> This option automates the action for all the infections found during the same scan.</p>
<b>Report Only</b>	In this mode the scanner scans for viruses, skips them, when the scan is over a summary window (report) appears providing all the scan details.
<b>Backup before repairing</b>	Scanner will keep a copy of infected file before disinfecting it. (Files that are stored in backup can be restored from Quarantine menu.)

## Using Advanced Options while scanning

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

<b>Scan Archive Files</b>	When this option is selected Quick Heal Total Security scans files inside the archive files. Quick Heal Total Security can scan archive files like ARJ, CAB, CHM, GZ, MSeXpand, RAR, SIS, TAR, TNEF and ZIP. Scanning inside compressed files increases scanning time. Quick Heal Total Security can detect viruses inside the 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.
<b>Scan Packed files</b>	When this option is selected Quick Heal Total Security scans packed executable files (.exe's) packed by popular packages like COM2EXE and LZex.
<b>Show Packed/Archive info</b>	This feature provides packed and archive information in the scan report about packed files and archive scanned files during the scan.
<b>DNAScan</b>	DNAScan technology is used to detect new and unknown malicious threats.
<b>List files while scanning</b>	All files will be listed in the Report section during scanning along with their status i.e. Clean or Infected.
<b>Scan Mailboxes</b>	<p>Quick Heal Total Security can scan Outlook Express 5.x Mail Box (inside .DBX files). Viruses like KAK, JS.Flea.B etc. remain inside DBX files and can reappear from there, if patches are not applied for OE. It also scans for e-mail attachments with Outlook Express 5.0. It scans e-mail attachments encoded with UUENCODE/MIME/BinHex (Base 64).</p> <p><b>Quick Scan</b> : If this option is selected then Quick Heal scans new mails and does not scan previously scanned emails. By default this option is selected.</p> <p><b>Thorough Scan</b> : If this option is selected then Quick Heal always scans all mails every time. This scan takes a long time.</p>

## Configuring Archive Settings

Archive scan settings are different from the normal scan. You can set which archives to be scanned and action to be taken if a virus is found in an archive. This option allows the user to configure following activities when a virus is found during scan:

<b>Delete Automatically</b>	Deletes an archive containing virus-infected file without notifying you.
<b>Prompt</b>	<p>Informs you when a virus is found in an archive and allows you to choose how to respond. When the scan is over, a summary window appears providing details about all the actions taken and other scan details. It provides you with the following options for an infected file:</p> <ul style="list-style-type: none"><li>• Skip</li><li>• Delete</li><li>• Quarantine</li></ul> <p><b>Apply action to all:</b> This option automates the action for all the infections found during the same scan.</p>
<b>Report Only</b>	In this mode the scanner scans for viruses under archive, skips the virus and archive file without taking any action.
<b>Quarantine</b>	During scan if a virus is found in an archive file, then the archive will be moved to Quarantine.
<b>Archive Scan level</b>	Set the level to scan inside an archive. By default it is set to level 2. Increasing the default Archive Scan Level may affect the scanning speed.

## SCANNER — MEMORY SCAN

Quick Heal Total Security scans the system memory every time it is started. It ensures that any infectious object is not running in the memory. Quick Heal Total Security Memory scan is smart enough to scan executable processes and additionally their supporting dynamic link libraries (.DLL).

### Memory scanning mode

<b>Quick Scan</b>	Scans memory for running executable processes only.
<b>Thorough Scan</b>	Scans memory for running executable processes along with their supporting dynamic link libraries. This scan will take considerable time.
<b>DNAScan</b>	This feature scans for new malicious threats in the memory using Quick Heal's indigenous DNAScan technology. When a new threat is found running in the memory it will clean the same. You will also have the option to send the suspicious file to our research lab for further analysis of that file. If that file is behaving like a malware then it will be added in the known threat signature database.

## SCANNER — DNASCAN

### Objective

DNAScan is Quick Heal's indigenous technology to detect and eliminate new and unknown malicious threats in the system. Additionally it copies the suspected file in the Quarantine directory before taking any action. Quarantined suspicious files can be submitted to our research lab for further analysis. This submission is important to curb the wild spread of new malicious threats. Suspicious file submission ensures the detailed analysis of the file in our research lab. After the detailed analysis it can be added in the known threat signature database which will be provided in updates to all the users. This can be only possible if they are detected and eliminated before their wild spread. DNAScan technology successfully traps suspected files with very less false alarms.

### Process

Whenever DNAScan detects a new malicious threat in your system it informs you, or asks for your action during memory scanning if the scanning is set with Prompt settings. One copy of DNAScan suspected files will always be quarantined which can later be submitted to research lab for further detailed analysis. The submission can be done automatically or manually through e-mail. The submission takes place whenever Quick Heal Total Security updates itself and finds new DNAScan suspected files in the Quarantine folder. It sends new DNAScan suspicious quarantined files in an encrypted file format to Quick Heal research lab.

### Setting the submission settings

DNAScan suspected files can be submitted to research lab of Quick Heal through e-mail. Submission of the suspected files is at your liberty. Submission of the DNAScan suspected files depend on the below mentioned settings:

<b>Do not submit files</b>	This option does not let DNAScan submit the suspected files to Quick Heal research lab.
<b>Submit suspicious files</b>	DNAScan suspected files can be submitted to Quick Heal research lab. Submission mail will be generated containing the suspected files. A confirmation will be requested from you to send the mail.



Manual submission can be done through the Quarantine tool.

## SCANNER — REGISTRY RESTORE

The Registry is a database used to store settings and options of Microsoft Windows Operating Systems. It contains information and settings for all the hardware, software, users, and preferences of the system. Whenever a user makes changes to a Control Panel settings, or File Associations, System Policies, or installed new software, the changes are reflected and stored in the Registry. Malwares usually target the system Registry to restrict specific features of the Operating Systems or other applications. They may modify the system registry so that it behaves according to the benefit for their activities. Most of the time it creates problem for the system.

**Quick Heal Registry Restore** - restores the critical system registry area and other areas for the changes made by malwares and repair the system registry.

### Registry Restore settings

<b>Critical System Registry Restore</b>	Selecting this option allows Quick Heal Total Security to restore the critical system registry during scan. Critical System Registry areas are generally changed by malwares to perform certain task automatically or to avoid detection or modification by system applications. e.g. Disabling Task Manager, Disabling Registry Editor etc.
<b>Repair malicious registry entries</b>	Selecting this option allows Quick Heal Total Security to scan system registry for malware related entries. Malwares and their remnants will be repaired automatically during scan.

## SCANNER — PC2MOBILE SCAN

### To customize PC2Mobile Scan for Microsoft Windows SmartPhones

1. Start **Quick Heal Total Security**.
2. Click on **Options**, under the top menu of the Quick Heal Total Security.
3. Select **PC2Mobile Scan** under Protection tab.
4. Select **Notify Windows Mobile when connected**. Selecting this option will notify you when ever a Windows Mobile phone is connected through USB cable to PC.

## PROTECTION – ONLINE PROTECTION

Quick Heal Total Security Online Protection continuously scans the system and prevents virus infection from E-mail Attachments, Internet Downloads, Network, File Execution and Copying.

### To Customize Online Protection

1. Start **Quick Heal Total Security**.
2. Click on **Options**, under the top menu of the Quick Heal Total Security.
3. Select **Online Protection** under Protection tab.

### General Settings

<b>Load Online Protection at Windows Startup</b>	By default this option is enabled and starts protecting your system, right from the time it is started.
<b>Display Alert Message</b>	Alert message will be displayed whenever a virus is found.
<b>DNAScan</b>	This feature detects and eliminates new malicious threats and protects your system from the latest threats. When a new malicious threat is detected it will be quarantined. You will also have the option to restore the file back to the same location if you are sure that the file is not a malicious threat.

### Specifying which files to scan Online

<b>Executable Files</b>	Scans files that are most likely to get infected by a virus.
<b>User Specified Extensions</b>	<p>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.</p> <p><b>Customizing User Specified Extensions</b></p> <ol style="list-style-type: none"><li>1. Select <b>User Specified Extensions</b>.</li><li>2. Press <b>Customize</b> button.</li><li>3. The default list includes most of the program file extensions. In case some of your applications use some other extensions, add them to this list to include it for scanning.</li></ol> <p><b>To add an extension</b></p> <ol style="list-style-type: none"><li>1. Feed the extension in <b>Add</b> box.</li><li>2. Click <b>Add</b>.</li></ol> <p><b>To remove a program file extension</b></p> <ol style="list-style-type: none"><li>1. Select the file extensions in the <b>User Defined Extensions</b> list box.</li><li>2. Click <b>Delete</b>.</li></ol> <p>To reintroduce the original list, click on <b>Default</b>.</p>

## How to respond when a virus is found

<b>Deny Access</b>	Prevents you from using a virus-infected file.
<b>Repair Automatically, delete if unsuccessful</b>	Attempts to repair the file from virus infection, in case if the file cannot be repaired, it will be deleted.
<b>Delete Automatically</b>	Deletes a virus-infected file without notifying you. Files deleted in such a manner cannot be recovered.
<b>Repair Automatically, Quarantine if unsuccessful</b>	Attempts to repair the file and quarantines it automatically in case if it cannot be repaired.
<b>Backup before repairing</b>	Online Protection will keep a copy of infected file before disinfecting it. (Files that are stored in backup can be restored from Quarantine menu.)

## Floppy Activities

<b>Check Floppy for Boot viruses on Access</b>	Boot sector of floppy will be scanned whenever a floppy is accessed.
<b>Check Floppy for Boot viruses during Shutdown</b>	Boot sector of floppy will be scanned if a floppy exists in the floppy drive during shutdown.

## PROTECTION - E-MAIL PROTECTION

1. Start **Quick Heal Total Security**.
2. Click on **Options**, under the top menu of the Quick Heal Total Security.
3. Select **E-mail Protection** under Protection tab.

### General Settings

<b>Enable Protection</b>	This option enables scanning of e-mails while downloading.
<b>Display Alert Message</b>	<p>Virus found alert will be shown in case a virus is found in an e-mail or attachment. Display Alert Message will contain following information:</p> <ul style="list-style-type: none"><li>• Virus Name</li><li>• Sender E-mail Address</li><li>• Recipient E-mail Address</li><li>• E-mail Subject</li><li>• Attachment Name</li><li>• Action Taken</li></ul>

### How to respond when a virus is found

You can specify how to respond when a virus is found in an e-mail attachment. You will get a prompt from Total Security E-mail protection about the action taken if the Display Alert option is enabled. Action taken details are also logged into the Activity Log.

<b>Delete infected attachments</b>	Selecting this option will delete the infected attachment while downloading mails.
<b>Repair automatically, Delete if unsuccessful</b>	Attempts to repair the virus without interacting with you. If the attachment cannot be repaired then it will be deleted.
<b>Backup before repairing</b>	Email Protection will keep a copy of infected email before disinfecting it. (Files that are stored in backup can be restored from Quarantine menu.)

### Control attachments to your incoming e-mail

<b>Block attachments with multiple extensions</b>	Worms commonly use multiple extensions. Enabling this option will block multiple extension attachments in incoming e-mails. It prevents infection from new worms, and thus protects your system. Common multiple extensions are .exe, .scr, .mpg, etc.
<b>Block emails crafted to exploit vulnerability</b>	Enabling this option will block e-mails, which contain vulnerability like MIME, IFRAME, etc. Sending an e-mail into broken parts is known as partial mail. Microsoft Outlook Express and Microsoft Outlook have an option of breaking message into separate parts.
<b>Enable Attachment Control – Enable attachment blocking in incoming e-mail.</b>	
<b>All attachments</b>	Selecting this option will delete all the attachments in incoming e-mails. This option is only recommended for users who require high security or prefer text based e-mails only.
<b>User specified extensions</b>	<p>This choice allows you to specify extensions of the files (attachments) to be blocked. On selecting this option you can either use provided default extension list or enter the file extensions of your choice.</p> <p>To add your own extension follow the below given steps:</p> <ol style="list-style-type: none"><li>1. Select User specified extensions.</li><li>2. Press Customize.</li><li>3. Type the extension name. For example: 'mpg'.</li><li>4. Click Add to add the extension in the list.</li><li>5. Click Ok to save the settings.</li></ol>

## Prevent new worm infection filtering e-mail clients

<b>E-mail clients allowed to send mails</b>	<p>Total Security E-mail protection is by default configured to support most of the popularly used e-mail clients like Eudora. If your e-mail client is different from the ones provided in the list, then you can simply add the same in the trusted e-mail client list. To add e-mail client follow the below given steps:</p> <ol style="list-style-type: none"><li>1. Select <b>Enable trusted e-mail clients</b>.</li><li>2. Press <b>Configure</b> button.</li><li>3. Click <b>Add</b> to add the e-mail client into trusted e-mail client list.</li><li>4. Click <b>Ok</b> to save the changes.</li><li>5. Press <b>Default</b> to load the default e-mail client list.</li></ol>
---	--



## PROTECTION – ANTI SPAM

Quick Heal AntiSpam has been integrated with Quick Heal E-mail Protection. It will block unwanted mails coming to your inbox. Choose from these options to customize email scanning.

1. Start **Quick Heal Total Security**.
2. Click on **Options**, under the top menu of the Quick Heal Total Security.
3. Select **AntiSpam** under Protection tab.

AntiSpam	
<b>Enable AntiSpam</b>	Scans email for Spam.
<b>Threshold Spam Score</b>	Higher the Threshold Score, weaker the SPAM control. To increase protection against SPAM shifts the Threshold Score towards lower point.
<b>Add Tag to Subject</b>	Using this option Spam mail's subject will be tagged with <b>[SPAM]</b> – and directly moved to <b>SpamMails</b> folder.
<b>Add score to mail header</b>	Spam mail's header will be appended with SPAM score. Header will be: <ul style="list-style-type: none"> <li>• X-QHSPAM:</li> <li>• X-QHSPAM-SCORE:</li> </ul>
<b>Enable White List</b>	<p>White List is the list of email addresses/domains whose mails are to be seen irrespective of their contents. Thus, mails from the addresses/domains listed here will not be passed through the SPAM filter.</p> <p>Please configure such email address and domain for your regular contacts.</p> <p>To add specific email address in the white list, follow the below given steps:</p> <ol style="list-style-type: none"> <li>1. Select White List and click <b>Customize</b> button.</li> <li>2. To add the email address click <b>Add</b>. For editing an existing entry click <b>Edit</b>.</li> <li>3. Click <b>OK</b> to save the changes.</li> </ol> <p>To add specific domain in the white list, follow the below given steps:</p> <ol style="list-style-type: none"> <li>1. Select White List and click <b>Customize</b> button.</li> <li>2. Type the domain and click Add. e.g. <b>*@mytest.com</b>. For editing an existing entry click <b>Edit</b>.</li> <li>3. Click <b>OK</b> to save the changes.</li> </ol>
<b>Enable Black List</b>	<p>Black List is the list of mail addresses/domains whose mails have to be blocked and moved to SPAM folder irrespective of their contents. Thus, mails from the addresses/domains listed here will be tagged as SPAM and moved to SPAM folder.</p> <p>This feature may be specifically evoked in case some server has an Open Relay which is being misused by Mass Mailers and viruses.</p> <p>To add specific email address in the black list, follow the below given steps:</p> <ol style="list-style-type: none"> <li>1. Select Black List and click <b>Customize</b> button.</li> <li>2. To add the email address click <b>Add</b>. For editing an existing entry click <b>Edit</b>.</li> <li>3. Click <b>OK</b> to save the changes.</li> </ol> <p>To add specific domain in the black list, follow the below given steps:</p> <ol style="list-style-type: none"> <li>1. Select Black List and click <b>Customize</b> button.</li> <li>2. Type the domain and click <b>Add</b>. e.g. <b>*@mytest.com</b>. For editing an existing entry click <b>Edit</b>.</li> <li>3. Click <b>OK</b> to save the changes.</li> </ol>
<b>Import List</b>	If you have exported or saved anti spam data and wish to use the same. You can import the existing list using this feature.
<b>Export List</b>	If you are having anti spam data configured in Anti Spam and planning to uninstall Quick Heal Total Security. It is recommended that you export/save your existing anti spam configuration using this feature. You can reuse the same data after re-installation of Quick Heal Total Security.

## ANTI SPAM FILTER FOLDER

Quick Heal Anti Spam scans the mail while scanning it will append the subject of the Spam mail with **[SPAM]** -. A SpamMails folder in the e-mail client gets created automatically and all SPAM mails will be directly moved to that folder. Automatic SPAM filter rules creation is supported for Microsoft Outlook Express, Microsoft Windows Mail, Eudora and Mozilla Thunderbird. For Microsoft Outlook, you can create SPAM filter manually by following below given steps:

### Configuring MS Outlook:

1. Launch MS Outlook
2. Point at **File, New, Folder**.
3. Name the folder name as **SPAM** and click **OK**.
4. Point Tools, Rules Wizard, **New**.
5. Select **Move message based on content** from "Which type of rule do you want to create?"
6. In Rule Description window click on **specific words**.
7. Type the following line, as it is **[SPAM] -** and click **ADD, OK** to apply the setting.
8. Then select **move it to the specified folder** and select the **SPAM** folder. Click **OK**.
9. Click on **Finish** to save the rule.

### Remember simple steps to create filters

To configure all e-mail clients you have to remember following simple steps:

1. You've to create a mailbox/folder name as **SPAM**.
2. Create the rules for subject.
3. For subject rule you need to write **[SPAM] -**
4. Move incoming messages containing above body or subject to SPAM folder.

## PROTECTION — INTERNET SECURITY

Quick Heal Total Security gives your desktop needed protection from various Internet threats. It gives Internet Security by automatically removing viruses and spyware, fighting spam, blocking access to hackers, preventing access to unwanted and malicious websites and blocking pop-up banner advertisements. Quick Heal Total Security takes care of the latest threats while surfing Internet.

1. Start **Quick Heal Total Security**.
2. Click on **Options**, under the top menu of the Quick Heal Total Security.
3. Select **Internet Security** under Protection tab.

### Enable Anti-Popup

Quick Heal Anti-Popup prevents annoying ads popup while surfing Internet. This feature is support to Internet Explorer 5.5 and above version only.

To enable Quick Heal Anti-Popup:

1. Select **Enable Anti-Popup**.
2. Click **Ok** to save the changes.

### Enable Anti-Malware

Quick Heal Total Security provides complete protection against Internet malwares like Riskware, Pornware, Hacktool, Spyware, Joke/Prank, etc.

To enable Quick Heal Anti-Malware:

1. Select **Enable Anti-Malware**.
2. Click **Ok** to save the changes.

### Enable Anti-Phishing

Quick Heal Total Security prevents you from accessing phishing and fraudulent websites. Phishing is a fraudulent attempt, usually made through email, to steal your personal information.

To enable Quick Heal Anti-Phishing:

1. Select **Enable Anti-Phishing**.
2. Click **Ok** to save the changes.

To run Quick Heal Anti-Phishing under Windows 2003 Operating System, following settings are required:

1. Open **Internet Explorer**.
2. Go for **Tools, Internet Option**.
3. Go to **Security** tab, click **Custom Level**.
4. Go to **Scripting** section, and enable **Active Scripting**
5. Click **Ok**.
6. Now go to **Advanced** tab, under **Browsing** section select **Enable third-party browser extensions (requires restart)**.

## PROTECTION — DATA PROTECTION

1. Start **Quick Heal Total Security**.
2. Click on **Options**, under main windows menu of the Quick Heal Total Security.
3. Click on **Data Protection** tab.
4. Select **Data Protection** option.
5. Press **Ok** to apply the changes.

<b>Block write access to removable drives</b>	Selecting this option will block data copying/modification/transfer on all the removable drives.
<b>Block complete access to removable drives</b>	Selecting this option will block complete access to the removable drives on your system. It will not allow access to the removable drives hence copying/modification/transfer activities can not be performed.



1. This protection does not imply on floppy drives.

## UPDATES - AUTOMATIC UPDATES

1. Start **Quick Heal Total Security**.
2. Click on **Option**, under the top menu of Quick Heal Total Security.
3. Select **Automatic Update** under Updates tab.

### General Settings

<b>Enable Automatic Update</b>	Automates the Quick Heal Total Security update process.
<b>Silent Update</b>	Enabling this option sets Quick Heal Total Security to update in non-interactive mode.
<b>Show Update Notification</b>	This option lets Quick Heal Total Security show the update notification after the successful updates.

### Select the updating mode

<b>Download from Internet Centre</b>	Download and update through Internet.
<b>Pick from specified path</b>	Download and update through local or network folder.

### Backup update files

<b>Keep a backup of update files</b>	This option allows saving the definition files while updating through Internet. Saved definition files can be used to deploy the updates to all other computers within a network.
--------------------------------------	---

## UPDATES - MESSENGER

1. Start **Quick Heal Total Security**.
2. Click on **Options**, under the top menu of Quick Heal Total Security.
3. Select **Messenger** under Updates tab.

### General Settings

<b>Enable Messenger</b>	This option enables Quick Heal Total Security Messenger service which provides important information about latest threats, updates and other information related to Quick Heal Total Security.
<b>Show Messenger icon in system tray</b>	This option shows Quick Heal Total Security Messenger icon in the system tray. If this option is unchecked then the Quick Heal Total Security Messenger icon will not be visible in the system tray but you will still receive messages and notifications.

### Select the mode to get message

<b>Download from Internet Centre</b>	Download and notify the messages through Internet.
<b>Pick from specified path</b>	Download and notify the messages through local or network folder.

### Keep a backup of message

<b>Keep a backup of message</b>	This option allows saving the message while notifying through Internet. Saved message can be used to deploy the notification message to all other computers within a network.
---------------------------------	---

<b>Customize messages settings</b>	<p>You can customize audio alarm for the various message notifications of Quick Heal Total Security Messenger. To customize sound:</p> <ol style="list-style-type: none"><li>1. Select <b>Customize messages settings</b>.</li><li>2. Click on <b>Settings</b> button.</li><li>3. Select the sound file (any WAV file) to be played with the event. Click on the icon on the right of the dialog box and select the file.</li><li>4. After finishing the configuration click <b>Ok</b> to save the changes and exit.</li></ol>
<b>Delete messages if older then</b>	<p>You can delete message at scheduled intervals or just after viewing. To manage messages:</p> <ol style="list-style-type: none"><li>1. Select <b>Delete messages if older then</b>.</li><li>2. Choose the desired intervals for deleting the viewed messages.</li><li>3. Press <b>Ok</b> to save the changes.</li></ol>

## GETTING MESSAGES FROM LOCAL FOLDER OR NETWORK PATH

Quick Heal Total Security Messenger can be configured to gather messages from a Local Folder or the Network Path. This feature enables Quick Heal Total Security Messenger's full functioning on systems where Internet connection is not available but systems are connected to LAN.

To get messages from local folder/network path please follow the below given steps:

1. Take a system, which is connected, to the Internet. This system will download messages from Total security Internet centre.
2. Create a folder on that system. For example: **C:\QHMSGGR**
3. Share this folder with Read access rights on the network.
4. Now click on **Start** & point to **Programs, Quick Heal Total Security** and **Quick Heal Total Security**.
5. Click on **Options**.
6. Select **Messenger** from the Updates tab.
7. Select **Keep a backup of message**.
8. Specify the folder where you want to keep a backup of messages. For example: **C:\QHMSGGR**
9. Click **OK** to save the changes.
10. On workstations go to **Messenger** settings under Updates option tree.
11. Select **"Pick from specified path"** and specify the shared backup messages folder path. For example: **\\SERVER\QHMSGGR**
12. Click **OK** to save the changes.

## UPDATES-INTERNET SETTINGS

1. Start **Quick Heal Total Security**.
2. Click on **Options**, under the top menu of Quick Heal Total Security.
3. Select **Internet Settings** under the Updates tab.

Your Internet Connection will be automatically detected. Change the settings only if you have trouble with the default connection settings.

### Enabling and configuring proxy settings

If you are "using a proxy server on your network" or "using Socks Version 4 & 5 network" then you need to enter the IP address (or domain name) and port of the proxy, SOCKS V4 & SOCKS V5 server in the Connection settings. Username & password are mandatory for the logon credential. Following Quick Heal modules require these changes:

- **Registration Wizard**
- **Quick Update**
- **Messenger**

### To enable and configure HTTP proxy settings

1. On the Internet Settings, select **Enable proxy settings**.
2. Choose **HTTP Proxy, Socks V 4** or **SOCKS V 5** as per your settings and then do the following:
  - In **Server**, type IP address of the proxy server or domain name (For example: proxy.yourcompany.com).
  - In **Port**, type the port number of the proxy server (For example: 80).
  - In **User name** and **Password**, type your server logon credentials, when required.
3. Click **Ok** to save the settings.

## MISCELLANEOUS - EXCLUSIONS

You can configure Quick Heal Total Security to skip scanning of certain files or folders. Scanning can be excluded in both cases, of known virus detection as well as DNAScan.

### Following scanning modules can be excluded

- Scanner
- Online Protection
- Memory Scanner
- DNAScan

### To exclude Files or Folders from scanning

1. Start **Quick Heal Total Security**.
2. Click on **Options**, under the top menu of Quick Heal Total Security.
3. Select **Exclusion** under the Miscellaneous tab.
4. Click **New**.
5. Click on File Icon or Folder icon for the exclusion.
6. Select the options of **Exclude** from.
7. Click **OK** to complete the process.

For selecting "Exclude from" follow these guidelines:

- If you are getting a warning for a known virus in a clean file and Quick Heal Total Security still gives you warning, you can exclude it for scanning of "Known Virus Detection".
- If you are getting a DNAScan warning in a clean file, you can exclude it for scanning of "DNAScan".

## MISCELLANEOUS - GENERAL

### Quickly scan system at Windows startup

<b>Enable Startup Scan</b>	This option lets Quick Heal Total security to scan the starting area of the system from wherein the programs are trying to get automatic execution control to trap new and unknown virus. It also keeps a watch on some of the system files, which are commonly patched (or replaced) by certain worms/backdoors/trojans.
----------------------------	---



This feature is not supported on Windows Vista and Windows Server 2008 Operating system.

### Get the status of a file by checking its Property

<b>Enable Property Sheet Scanner</b>	This option registers Quick Heal Total Security Scan tab in every file's properties tab. It provides information about the file status (Clean or Infected). You will also get the Quick Heal Total Security version and virus database information here.
--------------------------------------	--

### Schedule for deleting Reports and Quarantine file

<b>Delete Reports after</b>	You can delete the reports of Quick Heal Total Security at specific intervals.
<b>Delete Quarantine/Backup files after</b>	You can delete the quarantine files (including backup of the infected files) at specific intervals.

### Prevent unauthorized access to option settings of Quick Heal

To protect Quick Heal Total Security options from being changed without your permission, you can choose to protect it by enabling password protection for the same. If you specify a password, you are asked to enter a password every time when you wish to view or change the Options.

<b>Enable password protection</b>	<b>To specify a password:</b> <ol style="list-style-type: none"><li>1. At the top of the main window, click <b>Options</b>.</li><li>2. In the Options window, under the Miscellaneous tab, click <b>General</b>.</li><li>3. Select <b>Enable password protection</b> and press <b>Change Password</b>.</li><li>4. In the password dialog box, type a password.</li><li>5. Click <b>OK</b>.</li></ol>
-----------------------------------	--

### Application Status

<b>Show application icon at system tray</b>	If this option is enabled, Quick Heal Total Security icon will be visible at the system tray. User can easily access Quick Heal Total Security from this icon directly.
---	---



## CLEANING VIRUSES

Quick Heal warns you for a virus infection when:

- A virus is encountered during a manual or scheduled scan.
- A virus is encountered in the memory.
- A virus is encountered by Quick Heal Total Security Online Protection/E-mail Protection.
- A virus is detected through Start-up Scan.

## CLEANING VIRUSES ENCOUNTERED DURING SCANS

Quick Heal Total Security is adequately configured with the default installation to protect your system. If a virus is detected during scanning with default settings, Quick Heal Total Security tries to repair the virus and if it fails in doing so, it will delete the file. If you have changed the default scanner settings, then action will be taken accordingly when a virus is found. See [How to respond when a virus is found](#).

### Scanning Options

During scanning you are provided with the following options for your ease of operation:

<b>Statistics</b>	Scan statistics of a scan provided under this section.
<b>Skip Folder</b>	During the scan if you want to avoid scanning the current folder, just press on <b>Skip folder</b> . Scanning will be moved to other location. This option can be used while scanning a folder which contains non-suspicious items.
<b>Skip File</b>	During the scan if you want to avoid scanning the current file, just press on <b>Skip file</b> . Scanning of the current file will be skipped. This option can be used while scanning a big archive of files.
<b>Stop</b>	To stop the scanning process.
<b>Close</b>	To stop and terminate the scanning process.
<b>Shut down PC when finished</b>	Check this option when you to shut down your system after finishing the scan. This feature will work only if the scanning is completed.
<b>Reports</b>	During the scan you can also check the reports of the scan simultaneously. While scanning just press <b>Reports</b> window tab. By default setting, reports will be having infection event only. If you want to have the list of entire scan including clean files, select <b>List files while scanning</b> in the <b>Scanner's</b> option page.
<b>Settings</b>	You can check the settings used during the scan. To view these settings, just press Settings window tab.

## CLEANING VIRUS ENCOUNTERED IN MEMORY

"Virus Active in memory" means that virus is active, spreading to other files, computer (if connected to network) and doing malicious activity as per its payload. When Quick Heal Total Security detects a virus in memory, it warns in the following manner:

You can schedule Native Scanning of your PC at next boot which will scan and clean all drives including NTFS partitions at boot time before desktop is completely loaded. This will help you in detecting and cleaning even the most cunning Rootkits, spywares, special purpose Trojans and loggers. After disinfection restart your system and continue with installation. See [Performing Native Boot Scan](#) for more detail.

## CLEANING BACKDOOR, TROJAN, WORM AND MALWARES ENCOUNTERED IN MEMORY

During memory scanning if backdoor, trojan, worm, and other malwares are found, then Quick Heal Total Security will try to disable them and will ask you to scan the system for complete disinfection.

### Restart required during cleaning for some malwares

Some malwares drop and inject their dynamic link libraries into system's running processes such as explorer.exe, iexplorer.exe, svchost.exe, etc. which cannot be disabled or cleaned. During memory scan when they will be detected, they will be set for deletion in the next boot automatically. Quick Heal Total Security memory scan will provide complete detail or action recommendation for you in such cases.

### Cleaning of Boot/Partition viruses

In case if Quick Heal Total Security memory scanner detects a boot or partition virus in your system then it will recommend you to boot your system using a clean bootable disk and scan it using Quick Heal Emergency disk to clean the virus. See Using Emergency disk for more details.

### Responding to virus found alerts from Online Protection

Quick Heal Total Security Online Protection continuously scans your system for viruses in the background as you work. By default, Online Protection repairs the infected files automatically. You will also get a prompt after the action is taken by Quick Heal Total Security Online protection.

## USING EMERGENCY CD AND COMMAND LINE SCANNER

Quick Heal Total Security Emergency CD, create your own emergency bootable CD that will help you to clean boot your Windows PC and scan and clean all the drives including NTFS partitions. This helps in cleaning badly infected PC from file infecting viruses which cannot be cleaned from inside windows.

If your computer is badly infected by a virus in such a case while installing Quick Heal Total Security, Pre-install scan of Quick Heal Total Security installer will detect the active virus resident in memory. Hence you are unable to proceed with Quick Heal Total Security Installation. You are required to remove the virus from memory and other critical system areas before proceeding with Quick Heal Total Security Installation. To create Quick Heal Total Security Emergency CD, your system should fulfill following requirements:

- Licensed copy of Microsoft Windows Operating System. (Windows 2000/XP/2003 or above).
- Microsoft Windows Installation CD. (Windows XP/2003 or above)
- A blank writable CD and a CD-Writer drive.
- Emergency CD can only be used to scan and clean drives of the same system for which you have licensed Microsoft Windows operating system.

### How to make Emergency CD

Emergency CD and Command line scanner can be created using installed Quick Heal Total Security software. See [Creating Emergency CD or Command line scanner](#).

## USING EMERGENCY CD

1. Insert **Emergency CD** into your CD-Rom/DVD-Rom drive.
2. Restart your system.
3. Emergency CD will be automatically start and starts scanning all the drives. It will automatically disinfect the infection if found.
4. Once the scanning is over remove the Emergency CD from CD-Rom/DVD-Rom drive.
5. Restart your system.

## USING COMMAND LINE SCANNER

Command line Scanner is executed using **EMGSCAN.EXE** command at the DOS command prompt. EMGSCAN.EXE usage is:

Emgscan.exe [drive/path] [options]

### Emgscan Options

/DELETE	Delete infected files.
/REPAIR	Disinfect whenever possible.
/DUMB	Do a "dumb" scan of all files.
/WARE	Scan for Adware/Spyware.
/MIME	Scan for eml files.
/HELP or /?	Display this help.
/LIST	List all files checked.
/NOSUB	Do not scan subdirectories.
/ARCHIVE[-]	Scan inside archive files.
/PACKED[-]	Unpack compressed executables.
/REPORT=FileName	Create a report file.
/TEMPDIR=DirPath	Temporary Directory name.

For specified options '-' inverts the default meaning.

### To remove viruses using Emergency Disk:

1. Shutdown your computer.
2. Switch on the computer.
3. Insert Windows 95/98 Startup Disk or a clean DOS bootable disk. This will boot your system in A:\ Dos Shell.
4. Insert the Quick Heal Emergency disk.
5. Type "**EMGSCAN C: /REPAIR**" at the DOS command prompt and press Enter.
6. Quick Heal will scan entire C drive of your system and will try to disinfect the boot sectors or files if found infected during the scan.
7. When Quick Heal removes all the viruses and completes the scan, it will provide you with the respective scan summary.

## UPDATING QUICK HEAL TOTAL SECURITY

Updates for Quick Heal Total Security are posted regularly on its website containing detection and removal of newly discovered viruses. To prevent newly discovered viruses from infecting your computer, your system should have latest updated copy of Quick Heal Total Security. By default Quick Heal Total Security is set to update automatically from the Internet. This is done without user's intervention. Only basic requirement in this case, is the availability of a valid Internet connection for availing automatic updates. Automatic updates can also be applied from local or network path, but that path should have the latest set of definitions.

### Some important facts about Quick Heal Total Security Updates

- All Quick Heal Total Security Updates are complete updates including Definition File Update and Engine Updates.
- All Quick Heal Total Security updates also provide you version up gradation, thus making available the new features and technology for your protection.
- Quick Heal Quick Update is a single step upgrade.

## UPDATING QUICK HEAL TOTAL SECURITY FROM INTERNET

Quick Update by default automatically updates your copy of Quick Heal Total Security through the Internet. For this, you only need to have a valid Internet Connection. This feature works for all types of Internet connections (Dialup, ISDN, Cable, etc.)

### To update Quick Heal Total Security manually through Internet

1. Click **Quick Update** from **Start, Programs, Quick Heal Total Security**.
2. Follow the instructions and click **Next** button.
3. Check **Download from Total Security Internet Centre**.
4. Ensure that the Internet connection is active, and then click **Next** to initiate the update procedure.
5. Quick Update connects to the Total Security site, downloads the appropriate upgrade files for your copy of Quick Heal, and applies it thereafter to your copy, thus updating it to the latest available update file.

## UPDATING QUICK HEAL TOTAL SECURITY WITH DEFINITION FILES

If you already have the upgraded definition file with you, you can upgrade Quick Heal Total Security without connecting to the Internet. It is specifically useful for Network environments with more than one PC. You are not required to download the upgrade file from the internet on all the PCs within the network using Quick Heal.

To update Quick Heal Total Security through definition file:

1. Click **Quick Update** from **Start, Programs, Quick Heal Total Security**.
2. Follow the instructions and click **Next** button.
3. Click **Pick from specified path**.
4. Click **File** to locate the definition file.
5. Provide the index file for the definition i.e. **Index.dat**.
6. Click **Next**.

Quick Update picks up the definition file from the designated path, verifies its applicability on the installed version and upgrades your copy of Quick Heal Total Security accordingly.

## UPDATE GUIDELINES FOR NETWORK ENVIRONMENT

Quick Heal Total Security can be configured to provide hassle free updates across the network. You are suggested to follow these guidelines for best results:

1. Setup one computer (may be the server) as the master update machine. Suppose server name is **SERVER**.
2. Configure Quick Heal Total Security on this computer to upgrade automatically from the Internet as per your desired schedule.
3. Make **QHUPD** folder in any location. For example: **C:\QHUPD**
4. Assign Read-Only sharing rights to this folder.
5. Start Quick Heal Total Security and press the **Option** button.
6. Go to **Automatic Update** page under Updates section.
7. Select **Keep a backup of definition files**.
8. Click on **Folder** and locate the **QHUPD** folder. Click **Open**.
9. Click **Ok** to save this setting.
10. On all user computers within the network launch **Quick Heal Total Security**.
11. Go to **Automatic Update** page under Updates section.
12. Select **Pick from Specified path**.
13. Click on **Folder**.
14. Locate the **SERVER\QHUPD** folder from Network Neighborhood. Alternatively you can type the path as **\\SERVER\QHUPD**.
15. Click **Ok** to save the settings.

With the above steps all the machines will be upgraded automatically without user intervention at all. Following the steps as mentioned below can further extend the functionality:

1. In case of major out breaks, Quick Heal Total Security also provides intermediate upgrades. Messenger flashes the notice about the same, on your machine.
2. On receipt of the message, circulate a network notice requesting other Quick Heal Total Security users to click on **Update Now** button by right clicking on Quick Heal Total Security icon in the system tray.

## FAQ—FREQUENTLY ASKED QUESTIONS

### GENERAL QUERIES

#### **What is a Virus?**

Virus is a malicious piece of software or code, which is written intentionally for the destruction of data or malfunctioning on computers. It doesn't have its own entity. It has two prominent features i.e. execution and replication.

#### **What is a Worm?**

A computer WORM is a self-contained program or set of programs able of spreading itself to other computer systems (usually via network connections). Worms unlike viruses don't patch themselves to the executables files. They work independently.

#### **What is a Trojan Horse?**

A Trojan Horse is a fake file that pretends to do something desirable but infects. It does malicious activity without the user's knowledge.

#### **What is a Backdoor?**

Backdoor is an independent program. It has two components i.e. Server and Remote. Server component is installed on the victim system and remote component is the tool to control the victim system remotely. This is basically used for hacking.

#### **What is Adware and Joke (Prank) files?**

Adware: Programs that secretly gather personal information through the Internet and relay it back to another computer, generally for advertising purpose. This is often accomplished by tracking information related to Internet browser usage or habits.

Joke (Prank): Programs that change or interrupt the normal behavior of your computer, creating a general distraction or nuisance.

#### **Why Trojan, Worm and Backdoor files are not repaired?**

As they have their own independent programs which replicates its infection from computer to computer unlike viruses that replicates from file to file. They don't patch to executables or any other files. Hence deletions of their files cure the system.

#### **Where can I find technical details about viruses on Quick Heal's website?**

Technical details of latest viruses can be found at [www.quickheal.com](http://www.quickheal.com).

#### **Does Quick Heal detect all the wild viruses?**

Yes, Quick Heal detects and repairs all the wild viruses.

#### **Can I use more than one anti-virus software on my computer?**

Running more than one anti-virus software on your computer is not recommended unless specified specifically by the vendors. Anti-Virus product has some modules like real time scanning of files and real time scanning of mails, which seemingly integrates with OS to provide such services. Such integration can cause problems if there are multiple such services being installed and doing the same task. This way technical issue may arise as such modules are not designed keeping such things in mind. Technical issues may cause your system to freeze repeatedly which may lead to data loss or an unstable system. If the situation of using more than one scanner is unavoidable then one can install more than one anti-virus but make sure you keep real time protection for mails and file active only for one of the product and switch off these features for other products. This way you can have on-line protection active only for one product and can use scanner of multiple products.

### **Why do you recommend not using full share access features on computer?**

Allotting full share access rights to drives and folders could be dangerous for data, system & entire network. Virus threats increase if full sharing rights are assigned to folders or drives. Current new viruses tend to replicate immediately if they find share level access on computers. Avoid using full sharing on your computer but in case if data has to be shared in network then sharing rights should be assigned READ ONLY or PASSWORD PROTECTED.

Steps to share/unshare your folder & drive:

1. Double click My Computer icon on the desktop.
2. Right click on drive or folder to be shared, click on **Sharing** tab.
3. Look at sharing status.
4. If '**not shared**' is checked, Press **OK**.
5. If '**shared as**' is checked, we recommend that you disable this option by checking **Not Shared**.
6. If you have to share this volume, then under **Access Type** check either **Read Only** or Depends on Password.
7. You can create separate passwords for read only and full access. Give the Full Access Password only to those who need it.
8. For all other shared files and folders, make sure Access Type is set appropriately.

### **Does Quick Heal detect corrupt worms?**

Yes, Quick Heal scan engine is built with intelligence to detect corrupt worms.

### **What is a false positive?**

If virus is detected in a clean file it is referred to as false positive.

### **What is denial of service (DOS) attack?**

A Denial of Service (DOS) attack is a method that hackers use to prevent or deny legitimate users access to a computer. DOS attacks are executed using DOS tools like TFN, TFN2K etc. These tools send many request packets to a targeted Internet server (usually Web, FTP, or Mail server), that floods the server's resources, making the system unusable.

### **Why Quick Heal Total Security requires Microsoft Service Pack to be installed on the system?**

Microsoft recommends the latest service pack use to fix the different bugs or vulnerabilities in its Operating System. This recommendation applies to both customers as well as developers who are working in Windows environment. Hence the products are being developed by following Microsoft recommendations. If any system does not have the latest service packs or appropriate patches installed, then it is vulnerable or susceptible to viruses or other troublesome activities while using any of the applications.

Quick Heal has always been developed by following Microsoft recommendations. Hence to use Quick Heal your system should have appropriate service pack installed to get the maximum benefits.

### **For technical support where should I contact?**

For obtaining technical support on Quick Heal Total Security please feel free to contact the Quick Heal Technical support team at the following address:

Quick Heal Technical Support

#### **Quick Heal Technologies (P) Ltd.**

Office No 201, 1<sup>st</sup> Floor, Sunrise Apartment,  
775/3 Ketkar Path, Opposite Kamala Nehru Park,  
Pune – 411 004, India.

Tel: +91-20-65223883/ 65223892

E-mail: [support@quickheal.com](mailto:support@quickheal.com)

Web: <http://www.quickheal.com>



## **How to disable System Restore feature on WIN XP?**

### **Disabling System Restore under Windows XP:**

Point to **Start, Control Panel, Performance and Maintenance**. Double click '**System**', then select the '**System Restore**' tab. Select the '**Turn off System Restore**' on all drives box. Click '**Apply**'. Click '**Yes**'. Restart your system.

### **Do I require a Serial Number to fully evaluate Quick Heal Total Security?**

No, Serial Number is not required for evaluating Quick Heal Total Security.

## REGISTRATION AND RE-ACTIVATION:

### **I have reinstalled Quick Heal Total Security. Should I register it again?**

If due to any reason you need to reinstall your operating system or Quick Heal Total Security, it is necessary to re-activate your copy after reinstallation.

Re-activation is very easy and similar to the registration process. The changes in case of Re-activation are:

- On a PC having Internet access, choose '**Re-activate the copy**' option and provide the '**Serial Number**' and '**Activation Number**' of your copy and click '**Next**'.
- Re-activation through Phone and Off-line method is just similar to the corresponding registration process. Only '**Activation Number**' is what you need to remember and provide whenever it is being asked for, during re-activation process.

### **What to do if I lost my Serial Number or Activation Number?**

Serial Number and Activation Number serve as the users Identity. In case you lose Serial Number or Activation Number, you can obtain your Serial Number or Activation Number by contacting Quick Heal Technical Support by paying nominal charges.

Contact Details:

Quick Heal Technical Support

**Quick Heal Technologies (P) Ltd.**

Office No 201, 1<sup>st</sup> Floor, Sunrise Apartment,  
775/3 Ketkar Path, Opposite Kamala Nehru Park,  
Pune – 411 004, India.

Tel: +91-20-65223883/ 65223892

E-mail: [support@quickheal.com](mailto:support@quickheal.com)

Web: <http://www.quickheal.com>

**How long can I use this registered copy?**

You can use registered copy till the subscription period of your Quick Heal Total Security copy. After the subscription period is over you will need to renew the subscription for your copy of Quick Heal Total Security.

**Are the upgrades free, if yes for how long?**

All updates and upgrades are free for registered users till the subscription period of the copy.

**Where do I get Serial Number and Activation Number in Quick Heal Total Security on my computer?**

Serial Number and Activation Number can be obtained from 'About' section of Quick Heal Total Security. 'About Quick Heal' section also contains Version, Virus Database and Subscription validity information.

**For Off-line Registration I require Installation Number of Quick Heal, where do I get it in Quick Heal?**

Installation Number is available in Off-line Registration section of Quick Heal Total Security Registration Wizard, if you choose 'No' to 'I have Internet access on this computer' and click Next. Choose Off-line registration through web and click 'Next'. Here you will get the installation number of Quick Heal Total Security.

**What is my Customer ID or Customer Reference Number (CRN)?**

Your Serial Number of Quick Heal Total Security is your Customer ID or Customer Reference Number. Please do mention your Serial Number in every communication with Quick Heal Support.

**Whenever I run Quick Heal Total Security, scanner shows a message "Your copy of Quick Heal Total security is not yet activated. Please register your copy to get activated. Do you want to register now?"****At every boot Quick Heal Total Security registration wizard automatically starts?**

After installation of Quick Heal Total Security you will need to register your copy to get updates, online services and other benefits. If Quick Heal Total Security is not registered within 20 days time period from the date of installation, your copy of Quick Heal Total Security will expire and its further usage will be considered as void.

**Why registration wizard does not accept serial number?**

Registration wizard does not accept invalid serial number. To avoid such messages please type serial number as it as provided to you in the registration wizard.

**'License.key file is invalid' message comes during off-line registration?**

This prompt can come if previously obtained License.key file is being used to reactivate Quick Heal Total Security. In case, you have reinstalled Quick Heal Total security then you have to apply new License.Key by re-activating your copy of Quick Heal Total Security.

**'Registration Wizard' prompts I am not connected to Internet, but I am online?**

This problem may arise if you are using a 'proxy server' or 'Socks Version 4 & 5' on your network. In such cases, you have to configure 'Internet Settings' of the registration wizard. For more details please see [Customizing Internet Setting](#). (**Note.** This problem may also arise if you or your ISP is using Firewall. Firewall should be configured to allow Registration Wizard to get Internet access.)

In case the above problem remains as it is even after following the above mentioned steps, then we recommend you to contact [Quick Heal Technical Support](#) Team.

## RENEWING QUICK HEAL TOTAL SECURITY

### How do I renew my copy of Quick Heal?

To renew Quick Heal Total Security you need to buy renewal code. You can buy renewal code from your nearest reseller or Quick Heal directly. For more details about how to obtain renewal code please contact [Quick Heal Technical Support Team](#).

Quick Heal Total Security consists of renewal tool. Renewal tool is used to renew Quick Heal anti virus software. It can renew Quick Heal on PC having Internet connection or without Internet connection.

[Renewing Quick Heal Total Security On-line with PC having Internet connection](#)

[Renewing Quick Heal Total Security Off-line via Internet access on some other PC](#)

### Renewing Quick Heal Total Security On-line with PC having Internet connection

1. Execute **Renew Now** from Quick Heal Total Security's **About** section.
2. In case if Quick Heal Total Security is registered and activated then Serial Number and Activation Number will be detected by Quick Heal renewal tool. If Quick Heal is not activated then you will have to provide '**Serial Number**' and '**Activation Number**'.
3. Provide '**Renewal Code**' and '**Purchase From**' details and click on **OK**.
4. This process may take some time depending on the speed of Internet connection. Please stay connected to Internet.
5. '**Renewed successfully**' message will be shown along with the subscription validity information.

### Renewing Quick Heal Total Security Off-line via Internet access on some other PC

In case if Internet connection is not available on your computer, you will need to renew your copy by filling the renewal form on our website. You can visit off-line renewal page on our web site at <http://www.quickheal.co.in/offline-renewal.asp> with any system having Internet Connection. For example: Cyber cafe.

When filling the renewal form you would also need following information about your installed copy:

- Serial Number
- Activation Number
- Renewal Code
- Installation Number
- A Valid E-mail address.

During renewal on website you will need to provide a valid e-mail address. Upon successful renewal the License.key file will be sent to you on the e-mail address you provided during renewal on the website form. This License.key will be required for renewal of Quick Heal.

Take this License.key file to the computer where renewal has to be done.

1. Execute **RENEW.EXE** from Quick Heal Total Security's About section.
2. Select '**Renew Off-line**' and click on **Next**.
3. Click **Browse** and open the **License.Key** file.
4. '**Renewed successfully**' message will be shown along with the subscription validity information.

### Note:

1. Serial Number is provided in Quick Heal pack.
2. If the copy is activated then you can also find following details by clicking '**Renew Off-line**' in Quick Heal Renewal tool:
  - Serial Number
  - Activation Number and
  - Installation number

During renewal On-line and Off-line if you encounter any problem(s) then please feel free to contact Quick Heal Support Team with error details.

### When I will be informed to renew my subscription of Quick Heal Total Security?

Quick Heal Total Security will inform you to renew your subscription, one month before your copy is about to expire.

## UPDATING QUICK HEAL TOTAL SECURITY

**I am using Quick Heal Total Security on my network. How can I configure Quick Heal Total Security so all systems on network get updated automatically?**

Quick Heal Total Security can be configured to provide hassle free up gradation across the network. You are suggested to follow these guidelines for best results:

1. Setup one computer (may be the server) as the master update machine. Suppose server name is **SERVER**.
2. Configure Quick Heal Total Security on this computer to upgrade automatically from the Internet as per your desired schedule.
3. Make **QHUPD** folder in any location. For example: **C:\QHUPD**
4. Assign Read-Only sharing rights to this folder.
5. Start Quick Heal Total Security and press the **Option** button.
6. Go to **Automatic Update** page under Updates section.
7. Select **Keep a backup of definition files**.
8. Click on **Folder** and locate the **QHUPD** folder. Click **Open**.
9. Click **Ok** to save this setting.
10. On all user computers within the network launch **Quick Heal Total Security**.
11. Go to **Automatic Update** page under Updates section.
12. Select **Pick from Specified path**.
13. Click on **Folder**.
14. Locate the **SERVER\QHUPD** folder from Network Neighborhood. Alternatively you can type the path as **\\SERVER\QHUPD**.
15. Click **Ok** to save the settings.

With the above steps all the machines will be upgraded automatically without user intervention at all. The functionality can be further extended by following the steps as mentioned below:

- In case of major out breaks, Quick Heal Total Security also provides intermediate upgrades. Messenger flashes the notice about the same, on your machine. On receipt of the message, circulate a network notice requesting other Quick Heal users to click on **Update Now** button by right clicking on Quick Heal Total Security icon in the system tray.

## 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 switched on.

**bootable disk** A disk that contains all the necessary programs for the operating system to start or boot the computer.

**boot sector** The first physical sector on a floppy disk or the 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, etc.

**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 loaded.

**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 can select to proceed.

**directory** See folder.

**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** A table in the system area of a disk that identifies the specific (FAT) 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.

**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 detects and identifies by name.

**load** To start or run an application.

**Local Area Network** A group of computers linked together and having 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 into 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.

**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 viruses in memory may still be there when the boot is complete.

## TECHNICAL SUPPORT

If you call Technical Support and have the necessary information on hand we will be able to help you more efficiently.

### Where should I call?

Please call our toll free support number **18002333733**

### When is the best time to call?

Quick Heal Technologies (P) Ltd. provides technical support between 10.00 AM to 18.00 PM (Indian Standard time).

### What should I be ready with, before calling?

- Your Serial Number which is included in the boxed version of the products. If you have purchased our products on-line then you will find the serial number in the mail confirming your order.
- Information about your computer: brand, processor type, RAM capacity, the size of your hard drive and free space on it, as well as information about other peripherals.
- Your operating system: name, version number, language.
- What is the version of installed anti-virus and what is the virus database.
- What software is installed on your computer?
- Is your computer connected to a network? If yes - contact your system administrators first. If they can't solve your problem they should contact technical support themselves.
- Details: when did the problem first appear? What had you been doing before the problem appeared?



Very often this information allows us to resolve your problem quickly.

### What should I say to the technical support personnel?

Please be as specific as possible and provide maximum details. Remember that the specialist is basing on the information that you provide.



## CONTACT US

Head Office	World wide Online support centre
<p>Quick Heal Technologies (P) Ltd. 603 Mayfair Towers II, Wakdewadi, Shivajinagar, Pune 411 005, India. E-mail: <a href="mailto:info@quickheal.com">info@quickheal.com</a> Web: <a href="http://www.quickheal.com">http://www.quickheal.com</a></p>	<p>Quick Heal Technologies (P) Ltd. Office No 201, 1<sup>st</sup> Floor, Sunrise Apartment, 775/3 Ketkar Path, Opposite Kamala Nehru Park, Pune – 411 004, India. E-mail: <a href="mailto:support@quickheal.com">support@quickheal.com</a> Web: <a href="http://www.quickheal.com">http://www.quickheal.com</a></p>

### Distribution Centers and Support Offices in India

<p><b>Ahmedabad</b></p> <p>Quick Heal Technologies (P) Ltd. C/o. Rachaita Inc., C-201, Aalekh Apartment, Near Shailraj Tower, B/h Management Enclave, Vastrapur, Ahmedabad – 380015, Email: <a href="mailto:ahd@quickheal.co.in">ahd@quickheal.co.in</a></p>	<p><b>Bangalore</b></p> <p>Quick Heal Technologies (P) Ltd. #1422, 37<sup>th</sup> 'B'Cross, 11<sup>th</sup> Main, 4<sup>th</sup> 'T' Block, Jayanagar, Bangalore – 560 041 E-mail: <a href="mailto:bangalore@quickheal.co.in">bangalore@quickheal.co.in</a></p>	<p><b>Baroda</b></p> <p>Quick Heal Technologies (P) Ltd. C/o. Rachaita Inc. 215, Race Course Towers, Race Course Circle, Opp City Bank, Near Pasha Bhai Park, Baroda - 390 007 E-mail: <a href="mailto:baroda@quickheal.co.in">baroda@quickheal.co.in</a></p>
<p><b>Chandigarh</b></p> <p>Quick Heal Technologies (P) Ltd. S.C.O. 188-190, Unique Chambers, First Floor, Sector 34-A, Chandigarh -160 022 E-mail: <a href="mailto:chandigarh@quickheal.co.in">chandigarh@quickheal.co.in</a></p>	<p><b>Chennai</b></p> <p>Quick Heal Technologies (P) Ltd. New No. 6/2, Old No. 79/2, 1<sup>st</sup> Floor, 53rd Street, Near Anjanayar temple, Ashok Nagar, Chennai-600 083 E-mail: <a href="mailto:chennai@quickheal.co.in">chennai@quickheal.co.in</a></p>	<p><b>Coimbatore</b></p> <p>Quick Heal Technologies (P) Ltd. Old No. 160, New No. 111, 6<sup>th</sup> Street Extension, 100 Feet Road, Gandhipuram, Coimbatore-641012 E-mail: <a href="mailto:coimbatore@quickheal.co.in">coimbatore@quickheal.co.in</a></p>
<p><b>New Delhi</b></p> <p>Quick Heal Technologies (P) Ltd. 2948/A, 1<sup>st</sup> Floor, Near Shiv Chowk Temple, Ranjeet Nagar, South Patel Nagar, New Delhi -110 008 E-mail: <a href="mailto:delhi@quickheal.co.in">delhi@quickheal.co.in</a></p>	<p><b>Hyderabad</b></p> <p>Quick Heal Technologies (P) Ltd. 1-2-253/7, 1<sup>st</sup> Floor, Laxmi Narsu Mansion, 95, Parklane, Opp. Hotel Parklane Hyderabad-500 003 E-mail: <a href="mailto:hyderabad@quickheal.co.in">hyderabad@quickheal.co.in</a></p>	<p><b>Indore</b></p> <p>Quick Heal Technologies (P) Ltd. C/o. M/S. R T &amp; T Services, UG- 29, Sunrise Tower, 579, M. G. Road, Indore, Madhya Pradesh E-mail: <a href="mailto:indore@quickheal.co.in">indore@quickheal.co.in</a></p>
<p><b>Kochi</b></p> <p>Quick Heal Technologies (P) Ltd. N-38/351, Sy No 2/20, EARA-113, Near Mailalathu Temple, Edappally Junction, Edappally, Kochi - 682024 E-mail: <a href="mailto:cochin@quickheal.co.in">cochin@quickheal.co.in</a></p>	<p><b>Mumbai</b></p> <p>Quick Heal Technologies (P) Ltd. 408, 3rd Floor, 'D' Wing, Mathura Bhuvan, CHS, Dada Saheb Phalke Road, Dadar (E), Mumbai – 400 014 E-mail: <a href="mailto:mumbai@quickheal.co.in">mumbai@quickheal.co.in</a></p>	<p><b>Nagpur</b></p> <p>Quick Heal Technologies (P) Ltd. Flat No.8, Plot No.G.B.27, Ahilya Niwas, 2nd Floor, Jitendra Singh Tomer Road, Giripeth, Nagpur-440 010 E-mail: <a href="mailto:nagpur@quickheal.co.in">nagpur@quickheal.co.in</a></p>
<p><b>Nashik</b></p> <p>Quick Heal Technologies (P) Ltd. 12, Komal Residency, Sadhu Waswani Road, Near MICO Circle, Nashik – 422 005 E-mail: <a href="mailto:nashik@quickheal.co.in">nashik@quickheal.co.in</a></p>	<p><b>Pune</b></p> <p>Quick Heal Technologies (P) Ltd. 775/3, Office No. 201, 1<sup>st</sup> Floor, Sunrise Appts., Opp. Kaml Nehru Park, Bhandarkar Road, Pune-411004 E-mail: <a href="mailto:helpdesk@quickheal.co.in">helpdesk@quickheal.co.in</a></p>	<p><b>Surat</b></p> <p>Quick Heal Technologies (P) Ltd. C/o Amity Software &amp; Solutions, 101, Maher Park –B, Athwa Gate, Ring Road, Surat, Gujarat - 390007 E-mail: <a href="mailto:baroda@quickheal.co.in">baroda@quickheal.co.in</a></p>
<p><b>Visakhapatnam</b></p> <p>Quick Heal Technologies (P) Ltd. 30-9-16, 1st floor, Sarada Street, Centre Point Hotel Lane, Dabagardens, Visakhapatnam – 530020 E-mail: <a href="mailto:vaizag@quickheal.co.in">vaizag@quickheal.co.in</a></p>		

For more details please visit <http://www.quickheal.com>