



# USER GUIDE

Quick Heal Total Security 2010

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

<http://www.quickheal.com>

Copyright © 1993-2009 Quick Heal®

## **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, Wakdewadi, 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 cannot:

- 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 SUBJECTED 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.

The following are the list of conventions used in this document:

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. ....	Actions that must be performed
<b>Switch</b>	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.

## **Anti-Phishing**

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. It also 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 lightning speed to thoroughly detect and clean Spywares, Adwares, Roguewares, Dialers, Riskwares and lots of other potential threats in your system.

## **Autorun Protection**

Autorun malwares gain access to your system using Autorun feature of the Operating system, and autorun feature of removable drives such as CDs, DVDs or USB drives. This tool secures your PC against such malwares by disabling the autorun feature of your PC or USB drives

## **AntiSpam Plugins**

AntiSpam plugin feature in Quick Heal Total Security minimizes the effort for the user by providing options in MS Outlook or Eudora mail client. This plugin is user-friendly and will help the user to add email address to the Black List or White List just by a single click.

## **PCTuner**

Quick Heal PCTuner improves the performance of your PC or Notebooks by cleaning out system clutter. It also protects your privacy by washing away online activities that are traced through your Internet browser history, cache and cookies. It removes traces from many popular applications like Adobe Acrobat Reader, Microsoft Office, and also cleans invalid registry entries of your operating system.

## TABLE OF CONTENTS

<b>INSTALLING QUICK HEAL TOTAL SECURITY .....</b>	<b>10</b>
GETTING STARTED.....	10
SYSTEM REQUIREMENTS.....	11
HOW TO INSTALL QUICK HEAL TOTAL SECURITY.....	16
UNINSTALLING QUICK HEAL TOTAL SECURITY.....	17
<b>REGISTERING QUICK HEAL TOTAL SECURITY .....</b>	<b>18</b>
REGISTERING ONLINE WITH INTERNET CONNECTION ON THE SAME PC .....	18
REGISTERING OFFLINE WITH INTERNET CONNECTION ON SOME OTHER PC .....	19
IMPORTANT INFORMATION ABOUT MULTI-USER PACK REGISTRATION.....	20
REACTIVATION .....	20
RENEWAL .....	21
RENEWING ONLINE USING INTERNET ACCESS ON THE SAME PC .....	21
RENEWING OFFLINE USING INTERNET ACCESS ON SOME OTHER PC .....	22
CAN I INSTALL QUICK HEAL ON ANOTHER COMPUTER? .....	23
WHAT TO DO IF MY PRODUCT KEY IS LOST?.....	23
<b>USING QUICK HEAL TOTAL SECURITY .....</b>	<b>24</b>
ABOUT QUICK HEAL MAIN WINDOW .....	24
RIGHT SHELL MENU OPTIONS .....	26
USING HELP.....	26
PERFORMING MANUAL SCANS .....	27
SCHEDULING QUICK HEAL TOTAL SECURITY SCANNER .....	31
USING ONLINE PROTECTION .....	32
USING EMAIL PROTECTION.....	34
KNOWING ABOUT TRUSTED EMAIL CLIENTS .....	35
USING DATA PROTECTION .....	35
USING STARTUP SCAN .....	36
USING MESSENGER .....	37
VIEWING REPORTS .....	38
STATISTICS.....	39
VIEWING VIRUS LIST .....	41
QUARANTINE.....	41
AUTORUN PROTECTION .....	42
SYSTEM INFORMATION .....	45
CREATING EMERGENCY CD OR COMMAND LINE SCANNER .....	46
OVERVIEW OF NATIVE BOOT SCAN.....	47
USING QUICK HEAL ANTIMALWARE.....	47
WHEN QUICK HEAL ANTIMALWARE SHOULD BE USED? .....	49
USING QUICK HEAL ANTI-PHISHING.....	50
USING EXTRA TOOLS.....	51
HIJACK RESTORE.....	52
WINDOWS SPY .....	53
TRACK CLEANER.....	53
ADVANCED SYSTEM EXPLORER.....	53
ABOUT SECTION .....	54
<b>USING PC2MOBILE SCAN.....</b>	<b>55</b>
IMPORTANT REQUIREMENTS FOR PC2MOBILE SCAN .....	57



CONFIGURING WINDOWS MOBILE PHONE BEFORE SCAN .....	57
SCANNING WINDOWS MOBILE.....	58
CONFIGURING OTHER MOBILE PHONE BEFORE SCAN.....	58
CONNECTION THROUGH BLUETOOTH .....	59
SCANNING OTHER MOBILE PHONE THROUGH BLUETOOTH .....	59
CONNECTION THROUGH USB CABLE .....	60
SCANNING OTHER MOBILE PHONE THROUGH CABLE .....	60
<b>USING ANTI-ROOTKIT .....</b>	<b>61</b>
SCANNING RESULTS AND CLEANING ROOTKITS .....	63
CLEANING ROOTKITS THROUGH QUICK HEAL EMERGENCY CD .....	64
<b>USING QUICK HEAL PCTUNER.....</b>	<b>65</b>
ABOUT QUICK HEAL PCTUNER MAIN WINDOW .....	65
DASHBOARD .....	67
CLEANUP .....	68
TOOLS.....	73
USING PCTUNER REPORTS .....	78
OTHER FEATURES .....	81
<b>CUSTOMIZING QUICK HEAL TOTAL SECURITY .....</b>	<b>83</b>
SCANNER - SCAN OPTIONS.....	84
SCANNER – MEMORY SCAN .....	88
SCANNER – DNASCAN .....	88
SCANNER – REGISTRY RESTORE .....	89
SCANNER – PC2MOBILE SCAN.....	90
PROTECTION – ONLINE PROTECTION .....	90
PROTECTION - EMAIL PROTECTION .....	93
PROTECTION – ANTISPAM .....	95
ANTISPAM FILTER FOLDER.....	97
PROTECTION – INTERNET SECURITY.....	97
PROTECTION – DATA PROTECTION.....	99
PROTECTION – PACKER IDENTIFICATION .....	99
UPDATES - AUTOMATIC UPDATES .....	100
UPDATES - MESSENGER .....	101
GETTING MESSAGES FROM LOCAL FOLDER OR NETWORK PATH .....	102
UPDATES - INTERNET SETTINGS.....	102
MISCELLANEOUS - EXCLUSIONS .....	103
MISCELLANEOUS - GENERAL .....	104
<b>CLEANING VIRUSES .....</b>	<b>106</b>
CLEANING VIRUSES ENCOUNTERED DURING SCANS .....	106
CLEANING VIRUS ENCOUNTERED IN MEMORY .....	107
CLEANING BACKDOOR, TROJAN, WORM AND MALWARES ENCOUNTERED IN MEMORY .....	107
<b>USING EMERGENCY CD AND COMMAND LINE SCANNER .....</b>	<b>108</b>
USING EMERGENCY CD .....	108
USING COMMAND LINE SCANNER .....	108
<b>UPDATING QUICK HEAL TOTAL SECURITY .....</b>	<b>110</b>
UPDATING QUICK HEAL TOTAL SECURITY FROM INTERNET .....	110
UPDATING QUICK HEAL TOTAL SECURITY WITH DEFINITION FILES.....	110
UPDATE GUIDELINES FOR NETWORK ENVIRONMENT.....	111
<b>TECHNICAL SUPPORT .....</b>	<b>112</b>
CONTACT US .....	113

## INSTALLING QUICK HEAL TOTAL SECURITY

Quick Heal has a simple installation procedure. During installation, read each installation screen, follow the instructions, and then click Next to continue.

Quick Heal 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. If you are not sure whether your computer is infected by viruses, continue with the installation. Quick Heal setup will scan your computer's critical area for viruses as a part of its installation process.

### GETTING STARTED

Before installing Quick Heal remember the following guidelines:

- If you have any other anti-virus software/hardware loaded, uninstall it before proceeding with Quick Heal installation. Two anti-virus software's co-existing on the same computer at the same time could be hazardous for your computer.
- Quick Heal requires approximately 1 GB of free disk space.
- Close all open programs before proceeding with Quick Heal installation.
- You must install with administrative rights.

## SYSTEM REQUIREMENTS

To use Quick Heal, your computer must meet the following minimum hardware requirements:

Operating System	Minimum Requirements
Windows 2000	<ul style="list-style-type: none"><li>• 300 MHz Pentium Processor (or compatible) or higher</li><li>• 256 MB of RAM</li><li>• 1 GB 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>• 256 MB of RAM</li><li>• 1 GB of free hard disk space</li><li>• DVD or CD-ROM drive</li><li>• Service Pack 2 or above</li></ul>
Windows Vista	<ul style="list-style-type: none"><li>• 1 GHz Processor (or compatible) or higher</li><li>• 512 MB of RAM</li><li>• 1 GB of free hard disk space</li><li>• DVD or CD-ROM drive</li></ul>
Windows 7	<ul style="list-style-type: none"><li>• 1 GHz Pentium Processor (or compatible) or higher</li><li>• For 32-bit 512 MB or higher RAM; for 64-bit 1 GB or higher RAM</li><li>• 1 GB of free hard disk space</li><li>• DVD-ROM / CD-ROM drive</li></ul>

### **Clients supporting Email scan**

Email scanning is supported for any of the following POP3 email clients:

- Microsoft Outlook Express 5.5 and above
- Microsoft Outlook 2000 and above
- Netscape Messenger 4 and above
- Eudora 5 and above
- IncrediMail
- Windows Mail

### **Clients not supporting Email scan**

Email scanning is not supported for the following protocol and email clients:

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

### **SSL connections not supported**

Email Protection does not support encrypted email connections that use Secure Sockets Layer (SSL). If you are using SSL connections then your emails are not protected by Email Protection.



To send email through SSL connections, turn off Email Protection.

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

- Quick Heal Anti-Rootkit is not supported 64-bit Operating Systems.
- It requires minimum 256 MB RAM installed on system.

### **Quick Heal Browsing Protection**

- This feature is only supported for Microsoft Internet Explorer 5.5 and above version.

### **Quick Heal Self-Protection**

- This feature is not supported for Microsoft Windows 2000 Operating System.
- For Microsoft Windows XP Operating System this feature is supported if Service Pack 2 or higher is installed.
- For Microsoft Windows Server 2003 Operating System this feature is supported if Service Pack 1 or higher is installed.

**Quick Heal Anti-Phishing**

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






























**Quick Heal PC2Mobile Scan**




- Quick Heal PC2Mobile feature is supported on Windows XP/Vista/Windows 7 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 PCTuner**

- This feature is not supported for Microsoft Windows 2000 and Windows Server operating systems.

This table gives a comparison of the features available in different flavors of Quick Heal:

		QUICK HEAL ANTIVIRUS	QUICK HEAL INTERNET SECURITY	QUICK HEAL TOTAL SECURITY
<b>PROTECTION</b>				
<b>Anti-Virus</b>	Protects your computer from all types of viruses.			
<b>AntiSpyware</b>	Detects and cleans Spywares, Trojans and keyloggers, and protects against identity theft.			
<b>AntiMalware</b>	Scans system registry and folders to detect and clean Adwares, Roguewares and other potentially harmful software.			
<b>AntiRootkit</b>	Performs deep scan of your computer and removes all hidden rootkits.			
<b>Autorun Protection</b>	Prevents execution of autorun from infected pen drive. Vaccinates pen drive to prevent from malware autorun infections.			
<b>Firewall</b>	Protects your computer from hacker attacks.			
<b>AntiSpam</b>	Blocks junk/spam mails from entering your mailbox.			
<b>INTERNET PROTECTION</b>				
<b>Browsing Protection</b>	Protects against infected websites.			
<b>Anti-Phishing</b>	Blocks access to phishing websites and other online fraudulent websites.			
<b>PRIVACY PROTECTION</b>				
<b>Track Cleaner</b>	Removes computer usage traces of various applications.			
<b>Data Theft Protection</b>	Blocks access to pen drive and other USB storage devices and prevents unauthorized copying of data.			
<b>Secure Delete</b>	Securely removes sensitive and confidential data from the hard disk permanently.			

PC OPTIMIZATION				
<b>Registry Cleanup</b>	Cleans invalid and junk entries from system registry and optimizes system speed.			
<b>Disk Cleanup</b>	Cleans all the unwanted junk files and temporary files.			
MOBILE PROTECTION				
<b>PC2Mobile Scan</b>	Scans and cleans your mobile phones, smart phones and PDA using your computer.			

## HOW TO INSTALL QUICK HEAL TOTAL SECURITY

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

1. Click **Install Quick Heal Total Security** to initiate the installation process.



Figure 1-1: Install Quick Heal Total Security

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. The 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 details refer to **Native Scan** in **User Guide**.
4. During the Pre-install virus scan, if viruses are not 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 in different folder.
9. Click **Next**.
10. You can configure additional protection related to Internet Security to ensure safe browsing. For a novice user, it is recommended to keep the default settings intact as it will provide optimum protection against malwares and various threats.
11. Click **Next**.
12. Read the important information relating to the product.
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 case, to start the installation, please perform the following steps:

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

## UNINSTALLING QUICK HEAL TOTAL SECURITY

If due to any reason you wish to uninstall Quick Heal, please perform the following steps:

1. Click **Start -> Programs -> Quick Heal Total Security -> Uninstall Quick Heal Total Security** to initiate the un-installation process.
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 clicking **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 **Product key** of your copy. You are requested to note down your Product key 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.



- Before proceeding with uninstallation, ensure that all other running programs are closed.
- 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 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 any of the following options:

- [Online with Internet Connection on the same PC](#)
- [Offline with Internet Connection on some other PC](#)

### REGISTERING ONLINE WITH INTERNET CONNECTION ON THE SAME PC

If your PC has Internet connection then you can activate Quick Heal Total Security online. To register Quick Heal online, please perform the following steps:

1. Click **Start** -> **Programs** -> **Quick Heal Total Security** -> **Activate Quick Heal Total Security** to launch the registration wizard.
2. Click **Next** to continue.
3. Select **Yes to I have Internet access on this computer** and click **Next** to continue.
4. Select **Activate the copy** and click **Next** to continue.
5. The **Activation Information** screen appears. Provide the 20-digit Product key and click **Next** to continue.
6. Provide details for **Purchased from** and **Register for** fields. Click **Next**.
7. The Personal Information screen appears. Provide details as requested. The fields marked with \* are mandatory fields. Click **Next** to continue.
8. The **Submit the Information** screen appears. Verify the information displayed. If any modifications are needed click **Back** and make the necessary modifications; else click **Next** to continue.
9. The screen indicating successful activation is displayed. The validity of Quick Heal Total Security is displayed. Click **Finish** to complete the Activation process.



1. You can find the Product key 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 product key in the e-mail confirming your order.
2. Kindly stay connected to the Internet during the Registration process.

## REGISTERING OFFLINE WITH 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://license.quickheal.com/html/off2my\\_act/](http://license.quickheal.com/html/off2my_act/) 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:

- Product key
- Installation Number
- A valid email address.



1. You can find Product key 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 Product key in the email 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 Product key 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 email on the email 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. Click **Start** -> **Programs** -> **Quick Heal Total Security** -> **Activate Quick Heal Total Security** to launch the registration wizard.
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. The validity of Quick Heal Total Security is displayed.
9. Click **Finish** to complete the registration process.

## IMPORTANT INFORMATION ABOUT MULTI-USER PACK REGISTRATION

For Multi-user pack when the first Product key of Quick Heal is registered, registration information of the first Product key is automatically applied for all the other Product keys in the pack. As a result the Product keys that are registered after the registration of first Product key will have same user information and subscription expiry date.

## 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 Product key of your copy and click **Next**.
- Offline Reactivation is similar to the corresponding registration process.

## RENEWAL

To renew your copy of Quick Heal you need to buy renewal code. You can purchase a renewal code from Quick Heal, or from nearest distributor or reseller.

### RENEWING ONLINE USING INTERNET ACCESS ON THE SAME PC

If your PC has Internet connection then you can renew Quick Heal online by performing the following steps:

1. Click **Start** -> **Programs** -> **Quick Heal Total Security** -> **Quick Heal Total Security**.
2. If your subscription to Quick Heal Total Security has expired then **Information** section of the **Status** window will show that the subscription to your copy of Quick Heal has expired. Click **Renew Now** button. If your subscription to Quick Heal has not expired, then click **About** menu and then click **Renew Now** button.
3. The Product key of the product will be displayed in the **Product key** field. Enter the renewal code in **Renewal Code** field. Enter the distributor name or reseller name in the **Purchased from** field.
4. Click **Next** to continue.
5. The subscription information such as **Current Expiry Date** and **New Expiry Date** will be displayed.
6. Click **Renew** to continue.
7. Your copy of Quick Heal will be renewed. Click **OK** to complete the renewal process.



If a user has purchased an additional renewal code, then the renewal can be performed only after 10 days of the current renewal.

## RENEWING OFFLINE USING 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://license.quickheal.com/html/off2renewal/> 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 renewal web form through some other PC having Internet access
- Receiving license.key file through email.
- Renew the Quick Heal Total Security using newly obtained license.key file.

### Detail procedure

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

- Product key
- Installation Number



1. Installation Number and Product key are available in Off-line Renewal section of Quick Heal Total Security Renewal Wizard. Select '**Renew Offline**' and click **Next**. You will find the **Installation Number** along with the **Product key**.

### Obtaining License File

1. Once the Product key, Installation Number and Renewal code are verified, next page will be displayed with **User Name** and **Email Address** field. In case if your email address has been changed then please update the email address in this form.
2. Click the **Submit** button, to get unique License.key file via email on the email address provided by you. You will also get an option to download your License.key file on successful renewal. Take this License.key file to the computer where renewal needs to be done.

### Renewing Offline

Now proceed with the following process to renew your copy:

1. Click **Start -> Programs -> Quick Heal Total Security -> Quick Heal Total Security**.
2. If your subscription to Quick Heal Total Security has expired then **Information** section of the **Status** window will show that the subscription to your copy of Quick Heal has expired. Click **Renew Now** button. If your subscription to Quick Heal Total Security has not expired, then click **About** menu and then click **Renew Now** button.
3. Select **Renew Offline** option on this window.
4. Click **Next**.
5. Click **Browse** and open the **License.Key** file.
6. On completion you will get successful renewal message. The new validity of Quick Heal Total Security is displayed.
7. Click **OK** to complete the renewal process.

## CAN I INSTALL QUICK HEAL 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 Product key. Any previously obtained Product key and License Keys are invalid and will not work on another computer.



One Product key can only be used for one computer.

## WHAT TO DO IF MY PRODUCT KEY IS LOST?

Product key will serve as the users Identity. In case you lose the Product key, you can obtain your Product key by contacting Quick Heal Technical Support by paying nominal charges.

## USING QUICK HEAL TOTAL SECURITY

All the features related to Quick Heal 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 protects your entire system. You do not have to manually start Quick Heal Total Security to protect your system in such cases.

You can manually start Quick Heal by any of the following ways:

- Click **Start -> Programs -> Quick Heal Total Security -> Quick Heal Total Security**.
- In Windows system tray, double click the **Total Security Online Protection** icon or right click **Total Security Online Protection** icon in system tray and select **Open Total Security**.
- At the prompt in DOS window, change the path to the directory where 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.

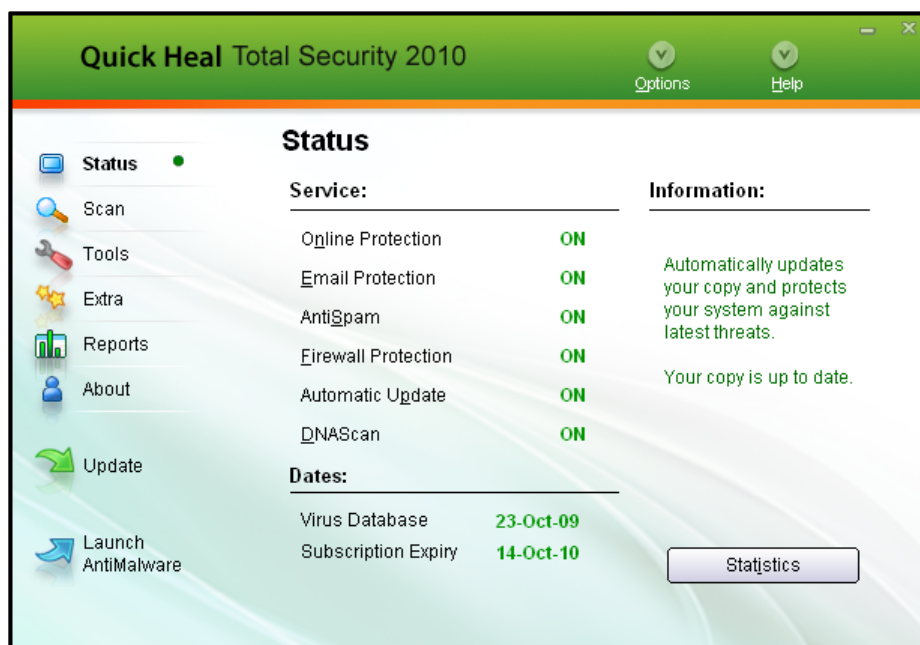


Figure 3-1: Quick Heal Total Security Main Window



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, Autorun Protection 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.

Following are the other options available on the main screen:

<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 softwares (Adwares, Dialers, Pornwares, Potentially unwanted software, Rouge applications, Spyware) and provides cure against them.
<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>Check New Messages</b>	Displays new messages received from Quick Heal.
<b>Enable/Disable Entertainment Mode</b>	Enables/Disables all Quick Heal prompts and notifications.
<b>View Messages</b>	Displays the messages received from Quick Heal.
<b>Enable/Disable Online Protection</b>	Enables/Disables 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 FAQs. Quick Heal provides online help for most of the message windows. You can get help on all the topics by any of the following ways:

1. Launching Help by clicking **Help** button from Scanner or Scanner Options.
2. Pressing **F1** when you need help.
3. Clicking the **Help** button in a dialog box.

The 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 Scanner**.
2. In the Quick Heal Scanner main window, click **Scan** on the left pane.
3. In the Scan pane, click **My Computer**.
4. Click **Scan**.
5. When the scan is complete, scan statistics and report will be provided.
6. After reviewing the statistics and report click **Close**.

### Performing My Documents scan

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

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

### Performing a Windows folder scan

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

1. Start **Quick Heal Scanner**.
2. In the Quick Heal Scanner main window, click **Scan** on the left pane.
3. In the Scan pane, click **Windows Folder**.
4. Click **Scan**.
5. When the scan is complete, scan statistics and report will be provided.
6. After 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 Scanner**.
2. In the Quick Heal Scanner main window, click **Scan** on the left pane.
3. In the Scan pane, double click the **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 **OK** to initiate the scan.
6. When the scan is complete, scan statistics and report will be provided.
7. After 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 Scanner**.
2. In the Quick Heal Scanner main window, click **Scan** on the left pane.
3. In the Scan pane, double click **Scan File**.
4. Select the file(s) you want to scan.
5. Click **OK** to initiate the scan.
6. When the scan is complete, scan statistics and report will be provided.
7. After 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 Scanner**.
2. In the Quick Heal Scanner main window, click **Scan** on the left pane.
3. In the Scan pane, click **Native Boot Scan**.
4. Click **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 Scanner**.
2. In the Quick Heal Scanner main window, click **Scan** on the left pane.
3. In the Scan pane, click **Mailbox Scan**.
4. Click **Scan**. When the scan is complete, scan report will be generated.
5. After reviewing the statistics and 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 **Add Item**.
4. If want to scan a folder or multiple folders then click **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 **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 **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 **Remove Item**.
5. A confirmation prompt will come. Click **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 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 **Tools**.
2. In the **Tools** pane, click **Schedule Scan**. Total Security Scan Scheduler wizard will appear.
3. Select **Create new Schedule Scan** and click **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. By default the **Schedule AntiMalware** option will be checked. This will perform a malware scan along with the virus scan. 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 **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. Click **Next**.
12. Review the summary of your custom scheduled scan.
13. When you are done, click **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 **Tools**.
2. In the Tools pane, click **Schedule Scan**. Total Security Scan Scheduler wizard will appear.
3. Click **Modify Schedule Scan** and select schedule scan created previously.
4. Click **Next**.
5. Change the schedule as desired.
6. When you are done, click **Next**.
7. Change the scan area as desired.
8. Click **Next**.
9. Review the summary of your custom scheduled scan.
10. When you are done, click **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 **Tools**.
2. In the Tools pane, click **Schedule Scan**. Total Security Scan Scheduler wizard will appear.
3. Click **Delete Schedule Scan**.
4. To delete a single schedule scan, select the schedule scan and click **Remove**. To delete all the scheduled scans click **Remove All**.

## USING ONLINE PROTECTION

Online Protection prevents your system from virus attack by continuously monitoring the system and prevents virus infection from email 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 **Total Security Online Protection** icon on the Windows task bar.
2. Click **Disable Online Protection**.
3. A prompt that recommends against turning off Online Protection appears. Select the time period for Online Protection to automatically enable itself or permanently disable using the **Select Action** drop-down box.

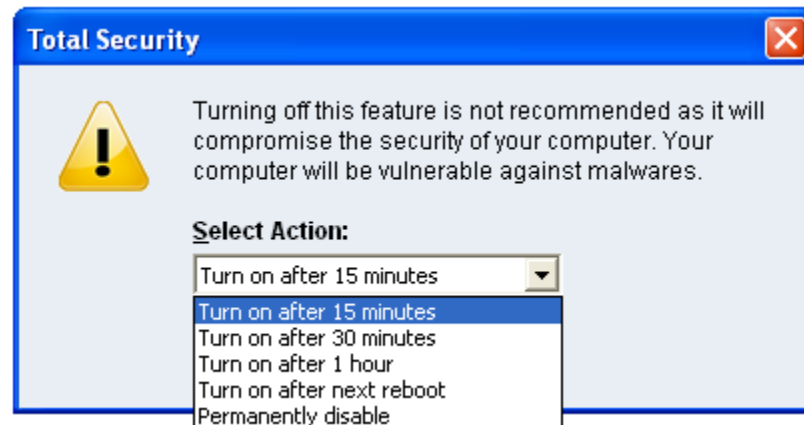


Figure 3-2: Disable Online Protection

4. Click **OK** to disable Online Protection.

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 or permanently based on your selection. If you have selected **Turn on after 15 minutes / 30 minutes / 1 hour** then the icon's color will change back from Red to Green based on the time frame selected, to indicate that Online Protection has been enabled. If you have selected **Turn on after next reboot**, then the icon's color will change back to Green at the next reboot. If you select **Permanently disable** then the icon's color will remain Red until you enable Online Protection manually.

### To disable Online Protection permanently

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

## USING EMAIL PROTECTION

Email is the most common medium for spreading viruses and other malicious programs. Since email is most widely used for communication, newer viruses are using email as a medium to spread. Virus authors are always looking for new methods to automatically execute their viral codes using some vulnerability amongst popular email 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 email protection. It supports all email programs that use POP3 communications protocol. Your email messages are scanned automatically for any malicious code content within, and hence you are assured of virus free safe emails.

Email protection protects you from following threats:

- Viruses received in email and attachments.
- Partial messages.
- Email containing vulnerability such as MIME, IFRAME etc.

The following features are supported in email protection:

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

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

### Disabling Email Protection

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

Email Protection can also be disabled as follows:

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



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

## KNOWING ABOUT TRUSTED EMAIL CLIENTS

Email is the most common medium for spreading viruses and other malicious programs. Since email is most widely used for communication, newer viruses are using email 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 email clients. **Worms** are also using their own SMTP engine routine to spread their infection.

Trusted email client is an advanced option which authenticates email-sending application on the system before they are sending emails. This option will prevent new 'Worms' from further spreading from your system. It contains a default email client list, which is allowed to send emails. Email 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 email but not added in the Trusted email 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 email 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.

### To enable Data Protection

1. Start **Quick Heal Total Security**.
2. Click **Options**, under main windows menu of the Quick Heal Total Security.
3. Click **Data Protection** tab.
4. Select **Data Protection** option.
5. Click **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 / Repair</b>	<p>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.</p> <p>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.</p>
<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, Windows Server 2008 and Windows 7 operating systems.

## 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 the blinking ball to view the message. A detailed log of messages is also maintained.

Color	Indicates
Red	Virus Alert
Amber	Hoax Information
Green	Upgrade
Blue	General

### Viewing Messages

To view the messages, do the following steps:

1. Right click **Quick Heal Total Security** icon from windows system tray.
2. Click **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 **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 **Options**, under main windows menu of the Quick Heal Total Security.
3. Click **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 **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
- Email Protection
- Startup Scan
- Scheduler
- Quick Update
- Memory Scan
- Anti-Phishing
- Registry Restore
- Native Scanner
- AntiMalware Scan
- Browsing Protection
- 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 **Reports**.
3. Now click 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, click **Prev**. To see Next log, click **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	
<b>Number of files scanned</b>	Provides information about total number of files scanned.
<b>Number of infected files</b>	Provides information about total number of infected files found.
<b>Number of suspicious files</b>	Provides information about total number of suspicious files found.
<b>Number of packed files identified</b>	Provides information about the number of packed files found.
<b>Last file scanned</b>	Provides information about the last scanned file.
<b>Last file found infected</b>	Provides information about the last file which was found infected.
<b>Last infection name</b>	Provides information about the Virus or Malware which was recently detected.
<b>Last file found suspicious</b>	Provides information about the file which was found suspicious recently.
<b>Last packed file identified</b>	Provides information about the last packed file that was identified.
<b>Last packer identified</b>	Provides information about the last type of packer that was identified.

Email Protection Statistics	
<b>Number of emails scanned</b>	Provides information about total number of emails scanned for infection.
<b>Number of emails with attachments</b>	Provides information about total number of email received along with attachments.
<b>Number of infected emails</b>	Provides information about total number of emails found infected.
<b>Number of attachments</b>	Provides information about total number of attachments received.
<b>Number of infected attachments</b>	Provides information about total number of attachments found infected.
<b>Number of suspicious attachments</b>	Provides information about total number of attachments found suspicious.
<b>Number of multiple extensions attachments blocked</b>	Provides information about total number of attachments blocked having multiple extensions. e.g. .doc.exe.
<b>Number of vulnerable emails blocked</b>	Provides information about total number of vulnerable emails blocked.
<b>Number of attachments blocked by attachment control</b>	Provides information about total number of attachments blocked as per the Attachment control policy.
<b>Type of attachments received by user mostly</b>	Provides information about attachments which is mostly received by the user. e.g. .doc (Office Document file).
<b>Type of attachments blocked mostly</b>	Provides information about attachments which is being blocked mostly as per the Attachment control policy.
<b>Last application blocked attempting to send mail</b>	Provides information about an un-trusted application which was blocked while sending mails as per Trusted Email Client policy.
<b>Number of attempts to send mail blocked</b>	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	
<b>Number of emails scanned for spam</b>	Provides information about total number of emails scanned for spam.
<b>Number of spam emails</b>	Provides information about total number of spam emails detected by AntiSpam protection.
<b>Since System Start</b>	Under this category, Quick Heal provides statistics since system start. Statistics under this category are purged on every shutdown or restart.
<b>Since Installation</b>	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 **Tools**.
3. Click **Virus List**. For the first time Virus List will take considerable time to load the list.

### Virus List Overview

To find for a virus in the virus list:

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



Click **Print** to take a print-out of 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 **Tools**.
3. Click **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> .

In the Quarantine feature, when a suspicious file is selected and the **Send** button is clicked, a prompt appears requesting permission to obtain your email address. You also need to provide a reason for submitting the files. Select from the following reasons :

<b>Suspicious File</b>	Select this reason if you feel that a particular file in your system has been the cause of suspicious activity in the system.
<b>File is unrepairable</b>	Select this reason if Quick Heal has been able to detect the malicious file on your system during its scans, but has not been able to repair the infection of the file.
<b>False positive</b>	Select this reason if a non malicious data file that you have been using and are aware of its function, has been detected by Quick Heal as a malicious file.

## AUTORUN PROTECTION

Autorun malwares gain access to your system using Autorun feature of the Operating system, and autorun feature of removable drives such as CDs, DVDs or USB drives. This tool secures your PC against such malwares by disabling the autorun feature of your PC or USB drives.

Autorun Protection provides two types of protection:

- Secure PC from autorun malwares.
- Secure removable drives.

### Secure PC from autorun malwares

To safeguard your PC against autorun malwares, please perform the following steps:

1. Click **Tools** -> **Autorun Protection** from the Quick Heal Total Security main window.
2. **Quick Heal Autorun Protection** window opens. In the **Secure PC from autorun malwares** tab, click **Secure my PC from Autorun Malwares** button.
3. Autorun feature is now disabled on your PC protecting it from autorun malwares.

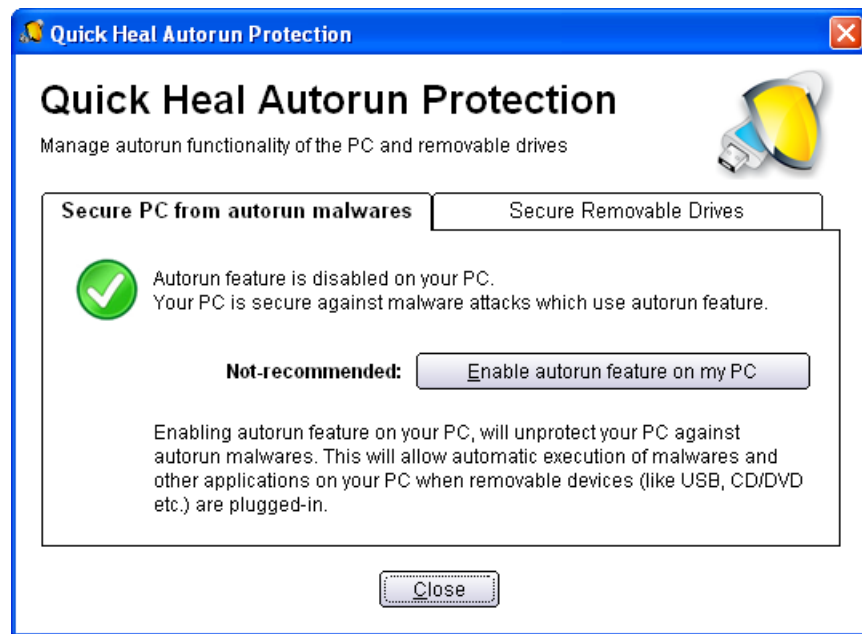


Figure 3-3: Secure PC from autorun malwares



Although Quick Heal recommends that you keep the autorun feature of your PC disabled, but if you wish to enable the Autorun feature of your PC, just follow the steps mentioned earlier, and in Step 2 click the **Enable Autorun feature on my PC** button to enable autorun on your PC.

## Secure Removable Drives

Quick Heal Total Security safeguards your USB devices from autorun malwares. Autorun feature of the removable drive is one of the mediums for malwares to gain access into the system. The **Secure Removable Drives** feature prevents autorun malwares from using your removable device as an infection spreading medium. Securing the removable drive also ensures that the drive, if connected to an infected system, cannot be used for spreading autorun malwares on other system.

To safeguard removable drives please perform the following steps:

1. Click **Tools** -> **Autorun Protection** from the Quick Heal Total Security main window.
2. Click the **Secure Removable Drives** tab.
3. The removable drives plugged into your system will be listed in the **Select a removable drive** drop-down box. Select the drive and click **Secure Removable Drive** button.
4. The drive will be secured against autorun malwares when used in other systems.

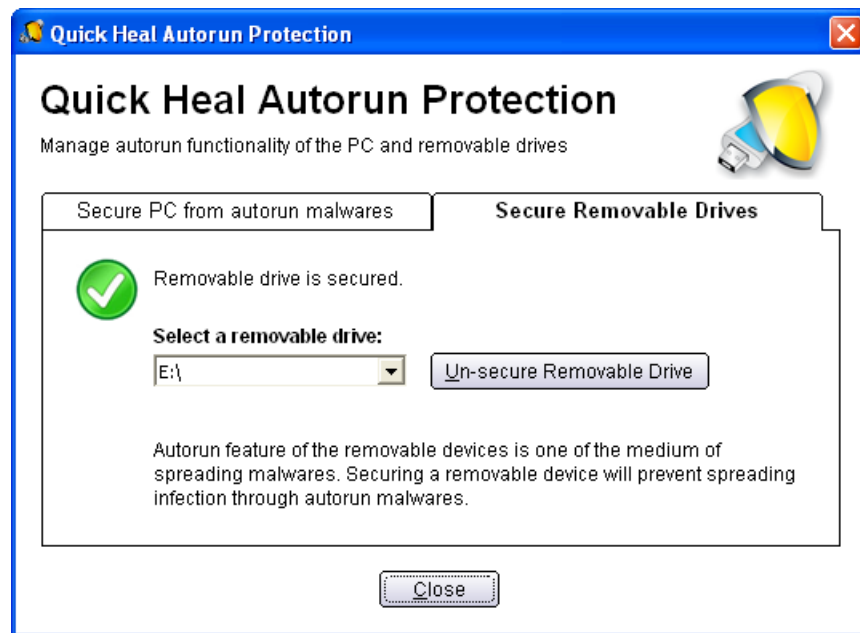


Figure 3-4: Secure Removable Drives



Although Quick Heal recommends that you keep the autorun feature of your USB drive disabled but if you wish to enable the Autorun feature of the USB drive, just follow the steps mentioned earlier and in Step 2 click the **Un-secure Removable Drive** button to enable autorun on your USB drive. Insert the same removable drive for un-secure that has been secured using Quick Heal Total Security.

## SYSTEM INFORMATION

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

<b>To detect new Malwares</b>	This tool gathers information to detect new Malwares from Running processes, Registry, System files like Config.Sys, Autoexec.bat etc.
<b>To get Quick Heal Total Security information</b>	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 submits the same automatically to [sysinfo@quickheal.com](mailto:sysinfo@quickheal.com).



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 **Tools** from the left pane.
3. Click **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.

## 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 **Tools** from the left pane.
3. Click **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 performing the steps that follow:

1. Start **Quick Heal Total Security**.
2. Click **Tools** from the left pane.
3. Click **Emergency CD**.
4. Click **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 **Tools** from the left pane.
3. Click **Emergency CD**.
4. Click **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. Click **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, click **Start -> Programs-> Quick Heal Total Security -> 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 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</b> point 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.

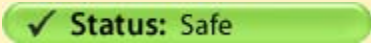
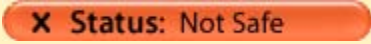
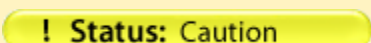
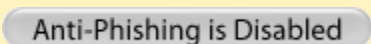
## USING QUICK HEAL ANTI-PHISHING

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 Anti-Phishing automatically scans all accessed web pages for fraudulent activity protecting you against any phishing attack as you surf the internet. It also 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 6 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 Report a Phishing 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 Report an Incorrectly Blocked 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 and higher version's Anti-Phishing

Microsoft's Internet Explorer 7.0 and higher version has its own 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 **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 Default Host file 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 Add. To edit the existing entry select the entry and click Edit. To delete select the entry and click Delete.
<b>Restore important system settings</b>	Critical system settings can be restored using this option. This setings 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 **Extra**.
3. Click **Windows Spy**.
4. Click **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 **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>Update License Details: 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 Product key and Renewal Code.</p> <p>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>	If Quick Heal Total Security is not activated then Activate Now button is available in About section. Activate Now helps you to activate your copy.
<b>Renew Now</b>	Renew Now helps you to renew your existing subscription.
<b>Support</b>	Support section provides information about Technical Support guidelines and Quick Heal Support's contact details. You can locate the nearest Quick Heal Support team.
<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>

## 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:

### Apple

Apple-iPhone

### Kyocera

Kyocera-SE44

### LG

LG-HB620T, LG-KE970, LG-KF310, LG-KF600, LG-KF700, LG-KG130, LG-KG225, LG-KG290, LG-KG320, LG-KG800, LG-KP130, LG-KP202, LG-KP202i, LG-KP230, LG-KU250, LG-KU311, LG-KU380, LG-KU990, LG-L343i, LG-LX1200, LG-M6100, LG-VI5225, LG-VX4400, LG-VX6000, LG-VX6100, LG-VX7000, LG-B2100, LG-KG328

### Mivvy

Mivvy-Chat, Mivvy-Dual

### Motorola

Motorola-A1000, Motorola-A1200, Motorola-A835, Motorola-C385, Motorola-C650, Motorola-E1, Motorola-E770v, Motorola-E8, Motorola-E1000, Motorola-E1070, Motorola-E398, Motorola-E550, Motorola-E770, Motorola-K1, Motorola-K1v, Motorola-K3, Motorola-L2, Motorola-L6, Motorola-L7, Motorola-L7e, Motorola-L7v, Motorola-L9, Motorola-U6, Motorola-U9, Motorola-V1075, Motorola-V180, Motorola-V186, Motorola-V220, Motorola-V235, Motorola-V3, Motorola-V300, Motorola-V3xxv, Motorola-V360, Motorola-V360v, Motorola-V3i, Motorola-V3iv, Motorola-V3x, Motorola-V3xv, Motorola-V3xx, Motorola-V500, Motorola-V505, Motorola-V525, Motorola-V525M, Motorola-V535, Motorola-V547, Motorola-V551, Motorola-V6, Motorola-V600, Motorola-V620, Motorola-V635, Motorola-V8, Motorola-V80, Motorola-V9, Motorola-V975, Motorola-W490, Motorola-W510, Motorola-Z3, Motorola-Z6

## **Nokia**

Nokia-2610, Nokia-3100, Nokia-3105, Nokia-3109 Classic, Nokia-3120, Nokia-3200, Nokia-3220, Nokia-3500 Classic, Nokia-3510, Nokia-3510i, Nokia-3650, Nokia-3660, Nokia-5070, Nokia-5140, Nokia-5140i, Nokia-5200, Nokia-5300 XpressMusic, Nokia-5310 XpressMusic, Nokia-6020, Nokia-6021, Nokia-6030, Nokia-6060, Nokia-6070, Nokia-6080, Nokia-6085, Nokia-6100, Nokia-6101, Nokia-6103, Nokia-6110 Navigator, Nokia-6111, Nokia-6120 Classic, Nokia-6124 Classic, Nokia-6125, Nokia-6131, Nokia-6151, Nokia-6170, Nokia-6220, Nokia-6220 Classic, Nokia-6225, Nokia-6230, Nokia-6230i, Nokia-6233, Nokia-6234, Nokia-6260, Nokia-6267, Nokia-6280, Nokia-6288, Nokia-6300, Nokia-6500 Classic, Nokia-6500 Slide, Nokia-6555, 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-7370, Nokia-7373, Nokia-7380, Nokia-7390, Nokia-7500 Prism, Nokia-7600, Nokia-7610, Nokia-7650, Nokia-7710, Nokia-8800, Nokia-8910i, Nokia-9300, Nokia-9300i, Nokia-9500, Nokia-E50, Nokia-E51, Nokia-E61, Nokia-E65, Nokia-E66, Nokia-N70, Nokia-E71, Nokia-E90, Nokia-N72, Nokia-N73, Nokia-N80, Nokia-N90, Nokia-N95, Nokia-N95 8GB, 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-Armani, Samsung-GT-S7330, Samsung-SCH-U420, Samsung-SGH-D500, Samsung-SGH-D500E, Samsung-SGH-D600, Samsung-SGH-D600E, Samsung-SGH-D820, Samsung-SGH-D830, Samsung-SGH-D880, Samsung-SGH-D900, Samsung-SGH-E100, Samsung-SGH-E250, Samsung-SGH-E251, Samsung-SGH-E330, Samsung-SGH-E330N, Samsung-SGH-E335, Samsung-SGH-E340, Samsung-SGH-E360, Samsung-SGH-E390, Samsung-SGH-S400i, Samsung-SGH-S401i, Samsung-SGH-E530, Samsung-SGH-E570, Samsung-SGH-E570V, Samsung-SGH-E590, Samsung-SGH-E630, Samsung-SGH-E700, Samsung-SGH-E720, Samsung-SGH-E760, Samsung-SGH-E770, Samsung-SGH-E780, Samsung-SGH-E800, Samsung-SGH-E820, Samsung-SGH-E840, Samsung-SGH-E900, Samsung-SGH-E950, Samsung-SGH-F200, Samsung-SGH-F210, Samsung-SGH-F250, Samsung-SGH-F300, Samsung-SGH-F480, Samsung-SGH-F490, Samsung-SGH-F490V, Samsung-SGH-G400, Samsung-SGH-G600, Samsung-SGH-G800, Samsung-SGH-G810, Samsung-SGH-J700, Samsung-SGH-J700V, Samsung-SGH-M150, Samsung-SGH-M310, Samsung-SGH-M310V, Samsung-SGH-P300, Samsung-SGH-P730, Samsung-SGH-U100, Samsung-SGH-U300, Samsung-SGH-U600, Samsung-SGH-U700, Samsung-SGH-U800, Samsung-SGH-U900, Samsung-SGH-U900V, Samsung-SGH-X100, Samsung-SGH-X210, Samsung-SGH-X460, Samsung-SGH-X510, Samsung-SGH-X520, Samsung-SGH-X600, Samsung-SGH-X650, Samsung-SGH-X660, Samsung-SGH-X660V, Samsung-SGH-X680V, Samsung-SGH-X700, Samsung-SGH-X820, Samsung-SGH-X830, Samsung-SGH-Z300, Samsung-SGH-Z320i, Samsung-SGH-Z400, Samsung-SGH-Z400V, Samsung-SGH-Z500V, Samsung-SGH-Z540, Samsung-SGH-Z540V, Samsung-SGH-Z560, Samsung-SGH-Z560V, Samsung-SGH-Z650i, Samsung-SGH-Z720, Samsung-SGH-ZV10, Samsung-SGH-ZV30, Samsung-SGH-ZV40, Samsung-SPH-A660,

## **Sagem**

Sagem-my411V, Sagem-myC-3b, Sagem-myC-4, Sagem-myC5-2, Sagem-myV-65, Sagem-myX-7, Sagem-myZ-55

## **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-C702, Sony Ericsson-C902, Sony Ericsson-D750i, Sony Ericsson-G502, Sony Ericsson-J300i, Sony Ericsson-K300i, Sony Ericsson-K310i, Sony Ericsson-K320i, Sony Ericsson-K500i, Sony Ericsson-K510i, Sony Ericsson-K530i, Sony Ericsson-K600i, Sony Ericsson-K610i, Sony Ericsson-K610im, Sony Ericsson-K660i, Sony Ericsson-K700i, Sony Ericsson-K750i, Sony Ericsson-K770i, Sony Ericsson-K790i, Sony Ericsson-K800i, Sony Ericsson-P800, Sony Ericsson-P900, Sony Ericsson-P910i, Sony Ericsson-S500i, Sony Ericsson-S700i, Sony Ericsson-T610, Sony Ericsson-T630, Sony Ericsson-V630i, Sony Ericsson-T650i, Sony Ericsson-V640i, Sony Ericsson-W200i, Sony Ericsson-W300i, Sony Ericsson-W350i, Sony Ericsson-W550i, Sony Ericsson-W580i, Sony Ericsson-W610i, Sony Ericsson-W660i, Sony Ericsson-W700i, Sony Ericsson-W710i, Sony Ericsson-W760i, Sony Ericsson-W800i, Sony Ericsson-W810i, Sony Ericsson-W850i, Sony Ericsson-W880i, Sony Ericsson-W890i, Sony Ericsson-W900i, Sony Ericsson-W910i, Sony Ericsson-W980i, Sony Ericsson-Z1010, Sony Ericsson-Z310i, Sony Ericsson-Z520i, Sony Ericsson-Z530i, Sony Ericsson-Z550i, Sony Ericsson-Z555i, Sony Ericsson-Z600, Sony Ericsson-Z610i, Sony Ericsson-Z710i, Sony Ericsson-Z770i, Sony Ericsson-K550i, Sony Ericsson-K810i, Sony Ericsson-K850i

## ZTC

ZTC-TE558



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, Windows Vista and Windows 7.
- For Windows Mobile based devices you should have Microsoft Active Sync 4.0 or above installed on PC.
- For Apple iPhone, [iTunes software from Apple](#) is compulsory to be 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.

## 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 **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 your 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 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 **Tools**.
3. Click **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 **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.

<b>Stop Scanning</b>	During scan you can select Stop Scan to stop the scan, Quick Heal Anti-Rootkit will prompt before stopping the scan.
<b>Close</b>	Click Close 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.
<b>Error Report Submission</b>	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.

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>	<p>By selecting Custom Scan radio button, you can configure following options:</p>
<b>Detect Hidden Process</b>	<p>To scan for running hidden processes in the system.</p>
<b>Detect Hidden Registry Items</b>	<p>To scan for hidden items in Windows Registry.</p>
<b>Detect Hidden files and folders</b>	<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>
<b>Scan drive on which operating system is installed</b>	<p>Will scan for hidden files and folders on the drive on which operating system is installed.</p>
<b>Scan all fixed drives</b>	<p>Will scan for hidden files and folders on all the fixed drives of the system.</p>
<b>Alternate Data Streams (ADS)</b>	<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> <p>Quick Heal Anti-Rootkit also displays summary of process scanning as total number of Processes scanned and number of hidden Processes detected.</p>
<b>Terminating Hidden Process</b>	<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> <p>Quick Heal Anti-Rootkit also displays summary of Registry scanning as total number of items scanned and number of hidden items detected.</p>
<b>Renaming Hidden Registry Key</b>	<p>After selecting list of key's for renaming click on Rename button. Renaming operation requires reboot hence Key name will be prefixed by Rename Queued.</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> <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>
<b>Renaming Hidden Files and Folders</b>	<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 Rename Queued.</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 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.



## USING QUICK HEAL PCTUNER

To open Quick Heal PCTuner application click **Start -> Programs -> Quick Heal Total Security -> Quick Heal PCTuner**. This opens the Quick Heal PCTuner Main Window. All the features of Quick Heal PCTuner are accessible from this main window.

### ABOUT QUICK HEAL PCTUNER MAIN WINDOW

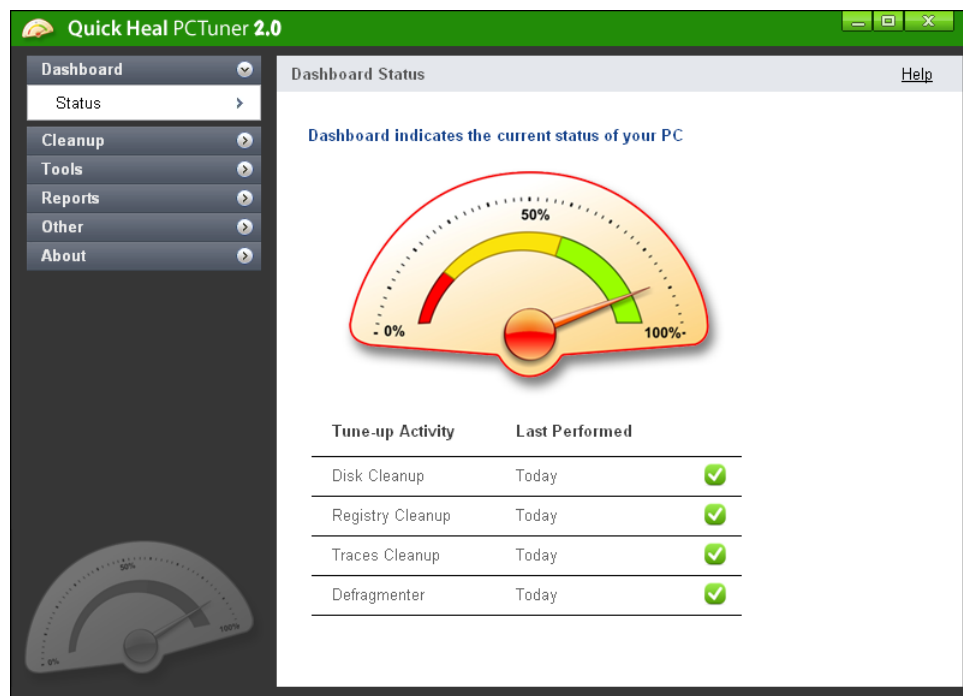


Figure 6-1: Quick Heal PCTuner Main Window

This main window of Quick Heal PCTuner lets you access and execute all the features of Quick Heal PCTuner. The features are divided under six menus. These menus are available on the left side of the window. The menus available in Quick Heal PCTuner are as follows:

Menu	Feature
<b>Dashboard</b>	Provides an indication of the current status of the system.
<b>Cleanup</b>	Cleans up system clutter such as junk files, invalid registry entries, browsing history, etc.
<b>Tools</b>	Contains tools to securely delete duplicate files and defragment the hard disk drive.
<b>Reports</b>	Provides reports for the various tune-up activities performed.
<b>Other</b>	Restores the items deleted during Cleanup.
<b>About</b>	Provides information about the software and support information.

Clicking the menu expands the list to reveal menu items. Each menu item will perform a specific feature of PCTuner. The menus and their corresponding menu items are as follows:

Menu	Menu Items
<b>Dashboard</b>	Status
<b>Cleanup</b>	Auto Cleanup Disk Cleanup Registry Cleanup Traces Cleanup
<b>Tools</b>	Duplicate File Finder Secure Delete Defragmenter
<b>Reports</b>	Auto Cleanup Reports Disk Cleanup Reports Registry Cleanup Reports Traces Cleanup Reports Secure Delete Reports Duplicate File Finder Reports Restore Reports
<b>Other</b>	Restore
<b>About</b>	Information

## DASHBOARD

The **Dashboard** menu is the default feature that is visible on opening the PCTuner application. The Dashboard menu organizes information making it easy to read and interpret. The information is presented in a manner to provide an indication about the actions that have been taken and the actions that are pending.

## STATUS



The Status feature provides up-to-date status information about the key performance indicators of Quick Heal PCTuner. It also presents a visual representation of the status information with the help of a Status Meter.

The Status Meter displays the status of the PC based on the execution of certain tune-up activities of PCTuner. The tune-up activities on which the Status Meter is dependant, for displaying the system status, are as follows:

- Disk Cleanup
- Registry Cleanup
- Traces Cleanup
- Defragmenter

The pointer of Status Meter will point to the green region only if you perform all the mentioned tune-up activities periodically.

The Status feature also provides the status of tune-up activities in the following format:

<b>Tune-up Activity</b>	The name of the Tune-up activity (Disk Cleanup, Registry Cleanup, Traces Cleanup and Defragmenter).
<b>Last Performed</b>	<p>The last execution date of each of the tune-up activities. If the concerned tune-up activity has never been executed, then the result will be <b>NEVER</b>.</p> <p>This third column will contain a symbol against each tune-up activity. If the symbol is  then it means that the corresponding tune-up activity has never been performed, or it means that the corresponding tune-up activity has not been performed in the past 30 days. If the symbol in the third column is  then it means that the corresponding activity has been performed in the past 30 days.</p>

## CLEANUP

Cleanup menu cleans up system clutter such as invalid and unwanted junk files, invalid registry entries, traces of your Internet history, etc. The Cleanup menu consists of four menu items. They are:

- Auto Cleanup
- Disk Cleanup
- Registry Cleanup
- Traces Cleanup

## AUTO CLEANUP

Auto Cleanup is a tune-up activity that performs **Disk Cleanup**, **Registry Cleanup** and **Traces Cleanup** at the click of a single button. It is ideal for novice users, and for users who do not want to waste time by performing individual Cleanup activity. Only the items deleted by Disk Cleanup and Registry Cleanup can be recovered.

### Customizing Auto Cleanup

Before you execute Auto Cleanup, it can be customized to perform as per your needs. To customize Auto Cleanup, please perform the following steps:

1. Click **Cleanup** -> **Auto Cleanup**.
2. Click **Options** button.
3. The **Auto Cleanup Options** screen opens. This screen has three tabs: **Disk Settings**, **Registry Settings** and **Traces Settings**. Each tab has a list of items preceded by a checkbox. By default all items are checked in each of the tabs.
4. Uncheck the items in each of the tabs that need to be skipped by Auto Cleanup feature. For a novice user we recommend to keep all the items in all the tabs checked.
5. By default **Take backup before deleting the items** is checked. If this feature is unchecked, Auto Cleanup will delete all the items without backup. We recommend that you keep it checked.
6. Click **Apply** to save the new settings; click **Close** to exit without saving the settings.

## How to Perform Auto Cleanup

To execute Auto Cleanup, please perform the following steps:

1. Click **Cleanup** -> **Auto Cleanup**.
2. Click **Options** if you wish to customize Auto Cleanup as mentioned earlier.
3. Click **Start** to begin Auto Cleanup.
4. Click **Stop** if you want to halt the Auto Cleanup; else click **Close** after completion of Auto Cleanup.

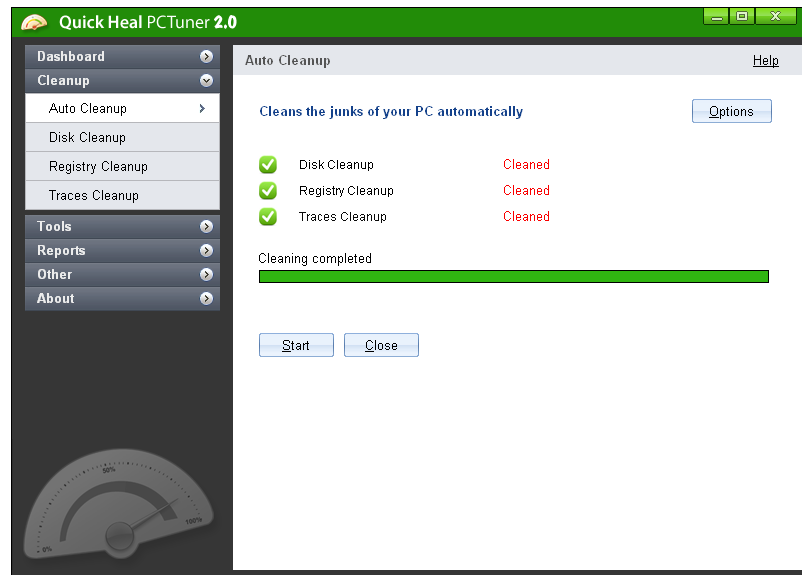


Figure 6-2: Performing Auto Cleanup

## DISK CLEANUP

The Disk Cleanup feature is a tune-up activity that finds and removes invalid and unwanted junk files from the hard disk drive. Disk Cleanup deletes these files freeing up space that can be used for other applications and helps improving system performance. The Disk Cleanup feature also deletes temporary files, Internet cache files, improper shortcut files, garbage name files & empty folders.

### Customizing Disk Cleanup

Before you execute Disk Cleanup, it can be customized to perform as per your needs. To customize Disk Cleanup, please perform the following steps:

1. Click **Cleanup** -> **Disk Cleanup**.
2. Click **Options** button.
3. The **Disk Cleanup Options** screen opens. Each item in the list is preceded by a checkbox. By default all items are checked in the list.
4. Uncheck the items that need to be skipped by Disk Cleanup feature.
5. Click **Apply** to save the new settings; click **Close** to exit without saving the settings.

### How to Perform Disk Cleanup

To execute Disk Cleanup, please perform the following steps:

1. Click **Cleanup** -> **Disk Cleanup**.
2. Click **Options** if you wish to customize Disk Cleanup as mentioned earlier.
3. Click **Start** to populate the list with file locations and its junk category.
4. You can click **Stop** to halt the entries being added to the list.
5. Each file location will be preceded by a checkbox. By default all file locations are checked. Uncheck the locations that need to be skipped by Disk Cleanup.

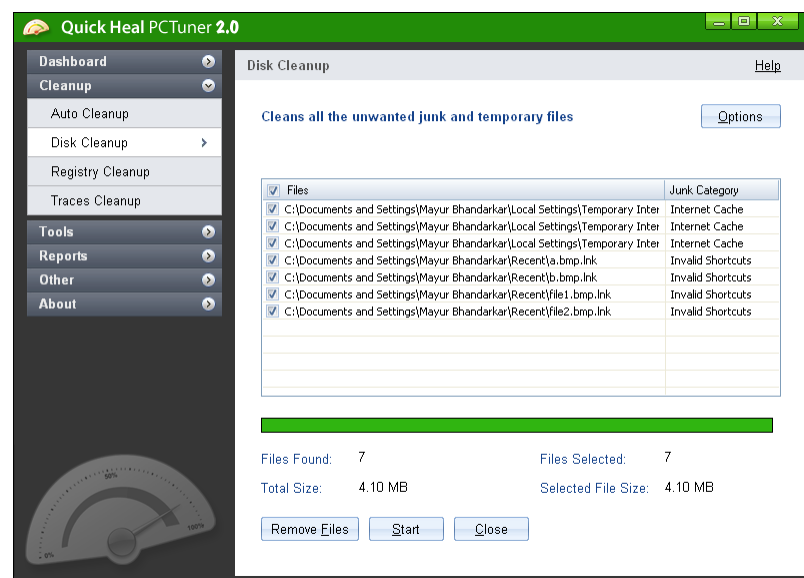


Figure 6-3: Performing Disk Clean Up

6. There are four other fields which display the following information:
  - **Files Found:** The total number of files found by Disk Cleanup.
  - **Total Size:** The size of the total number of files found by Disk Cleanup.
  - **Files Selected:** The number of files selected for deletion.
  - **Selected File Size:** The size of the number of files selected for deletion.
7. Click **Remove Files** to remove the files. Click **Close** to exit Disk Cleanup.

## REGISTRY CLEANUP

The Registry Cleanup feature is a tune-up activity that removes invalid registry entries from the system that have appeared due to improper uninstall, non-existent fonts, etc. Sometimes during installation, the registry entries are not deleted. This leads to slower performance of the system memory. The Registry Cleanup removes such invalid registry entries to boost the performance of system memory.

### Customizing Registry Cleanup

Before you execute Registry Cleanup, it can be customized to perform as per your needs. To customize Registry Cleanup, please perform the following steps:

1. Click **Cleanup** -> **Registry Cleanup**.
2. Click **Options** button.
3. The **Registry Cleanup Options** screen opens. Each item in the list is preceded by a checkbox. By default all items are checked in the list.
4. Uncheck the items that need to be skipped by Registry Cleanup feature.
5. Click **Apply** to save the new settings; click **Close** to exit without saving the settings.

### How to Perform Registry Cleanup

To execute Registry Cleanup, please perform the following steps:

1. Click **Cleanup** -> **Registry Cleanup**.
2. Click **Options** if you wish to customize Registry Cleanup as mentioned earlier.
3. Click **Start** to populate the list with registry entries and their path.
4. You can click **Stop** to halt the entries being added to the list.
5. Each registry entry will be preceded by a checkbox. By default all registry entries are checked. Uncheck the registry entries that need to be skipped by Registry Cleanup.

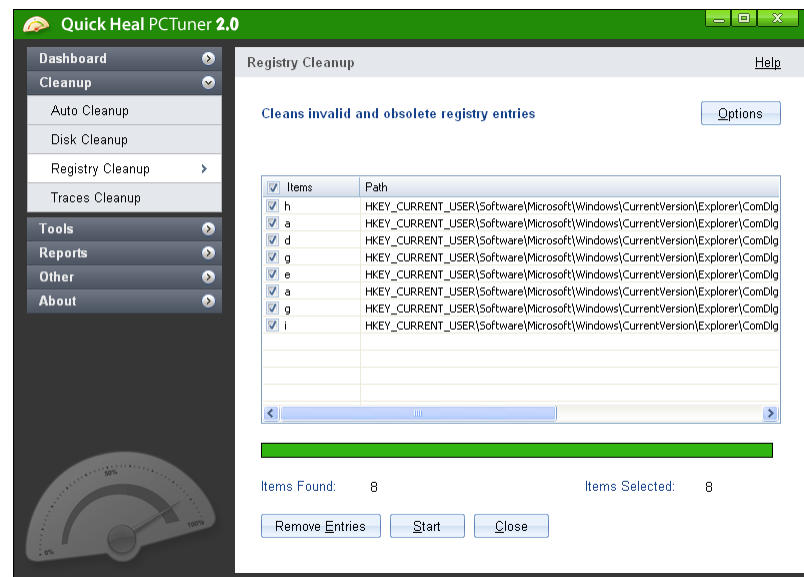


Figure 6-4: Performing Registry Cleanup

6. There are two other fields which display the following information:
  - **Items Found:** The total number of registry entries found by Registry Cleanup.
  - **Items Selected:** The total number of registry entries selected for removal.
7. Click **Remove Entries** to remove the files. Click **Close** to exit Registry Cleanup.

## TRACES CLEANUP

The Traces Cleanup feature is a tune-up activity that removes traces from Internet history and MRU List (Most Recently Used) of various applications. It safely deletes history, cleans the cookies, cache, auto-complete forms and passwords. Removing traces like auto complete entries and saved passwords have to be deleted to ensure that user privacy is not breached. It also erases the traces from popular application programs such as MS Office Applications, Adobe Acrobat Reader, Media Player, WinZip, WinRAR and traces such as Browser Cookies, Saved Passwords and so on.

### Customizing Registry Cleanup

Before you execute Traces Cleanup, it can be customized to perform as per your needs. To customize Traces Cleanup, please perform the following steps:

1. Click **Cleanup** -> **Traces Cleanup**.
2. Click **Options** button.
3. The **Traces Cleanup Options** screen opens. Each item in the list is preceded by a checkbox. By default all items are checked in the list.
4. Uncheck the items that need to be skipped by Traces Cleanup feature.
5. Click **Apply** to save the new settings; click **Close** to exit without saving the settings.

### How to Perform Traces Cleanup

To execute Traces Cleanup, please perform the following steps:

1. Click **Cleanup** -> **Traces Cleanup**.
2. Click **Options** if you wish to customize Traces Cleanup as mentioned earlier.
3. Click **Start** to populate the list with applications containing traces.
4. You can click **Stop** to halt the entries being added to the list.
5. Each application containing traces will be preceded by a checkbox. By default all application containing traces are checked. Uncheck the applications that need to be skipped by Traces Cleanup.

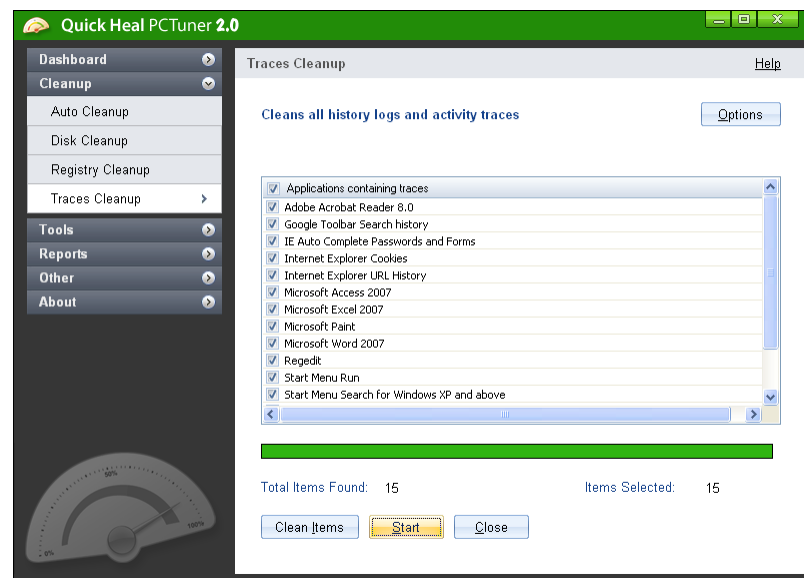


Figure 6-5: Performing Traces Cleanup

6. There are two other fields which display the following information:
  - a. **Total Items Found**: The total number of applications containing traces found by Traces Cleanup.
  - b. **Items Selected**: The total number of application containing traces selected for removal.
7. Click **Clean Items** button to remove traces from the applications listed. Click **Close** to exit Traces Cleanup.



## TOOLS

The Tools menu provides features which deletes duplicate files from the system. It also performs system defragmentation to improve system performance. It offers secure deletion where files will be deleted permanently and will not be recovered even if recovery software is used.

### DUPLICATE FILE FINDER

The Duplicate File Finder feature will delete duplicate files of various pre-defined file categories. It will search for duplicate files on different locations as per user input. The user can also provide a folder exclusion list, to be omitted from the scan of duplicate files. Duplicate files will be deleted using One Pass, Two Pass or DoD deletion method as per the user's choice. The default deletion method is One Pass.

The pre-defined file categories that will be scanned during the execution of Duplicate File Finder feature are as follows:

File Category	Extensions
<b>Application Executables</b>	.exe, .dll, .scr, .ocx, .sys
<b>Image / Photo Files</b>	.pcx, .tiff, .wpg, .bmp, .gif, .jpg, .jpeg, .wmp, .png, .tif
<b>Creative Artwork Files</b>	.ai, .eps, .pcx, .psd, .tiff, .wpg, .bmp, .gif, .jpg, .jpeg, .wmp, .png, .cdr, .pdf, .tif
<b>Movie Files</b>	.avi, .rm, .vob, .mov, .qt, .mpeg, .mpg, .mpe, .mpa, .dat
<b>Sound Files</b>	.wmv, .wma, .mp4, .mp3
<b>Text Files</b>	.txt, .asci
<b>Document Files</b>	.pdf, .doc, .rtf, .wri, .sam, .dox, .xls, .ppt, .docx, .xlsx, .pptx, .wk3, .wk4, .vsd, .vsdx, .wg, .123, .wpd
<b>Email Files</b>	.eml

## How to Delete Duplicate Files

To delete Duplicate Files using Duplicate File Finder, please perform the following steps:

1. Click **Tools** -> **Duplicate File Finder**.
2. Click **Options** if you want to modify Duplicate File Finder settings.
3. The **Quick Heal Duplicate File Finder Options** window opens. In the **Please select a duplicate category type** frame; uncheck the categories that need to be skipped by the Duplicate File Finder.
4. In the **Exclude folder(s)** frame, you can add exclusion lists for Duplicate File Finder to skip. Click **Add Folder** button to add the locations for exclusions. Highlight a location and click **Clear**, if the added location is incorrect. Click **Clear All** to remove all exclusion locations added.
5. The **Use Secure Delete** option will be activated by default, and **One Pass Random – Quick Data Destruction** deletion method is selected by default. You can select any deletion method or deactivate **Use Secure Delete** option by unchecking it. See [Deletion Methods](#) to know about different deletion methods.
6. Click **Apply** button to save the modification of settings; else click **Close** button to exit without saving any modified settings.
7. Click **Add Path** to add the path for Duplicate File Finder to search for duplicate files. This opens the **Browse for folder** window. Browse for the required folder. Check **Exclude sub-folder** if you want to exclude the sub-folders within the folder in the scan. By default **Exclude sub-folder** option will be unchecked. Click **OK** after selecting the required path. If the added path is incorrect, highlight that path and click **Clear** to delete the path. Click **Clear All** to delete all the added paths from the list.
8. Click **Start Search**.
9. A list of file locations collapsed with duplicate file locations will be displayed. The information of the scan will be provided in the following fields:
  - **Search Progress**: Displays the progress of the search.
  - **Folders Scanned**: Displays the number of folders scanned.
  - **Files Scanned**: Displays the number of files scanned.
  - **Duplicates Found**: Displays the number of files with duplicates found.
  - **Space Wasted**: Displays the space that was consumed by the duplicate files.

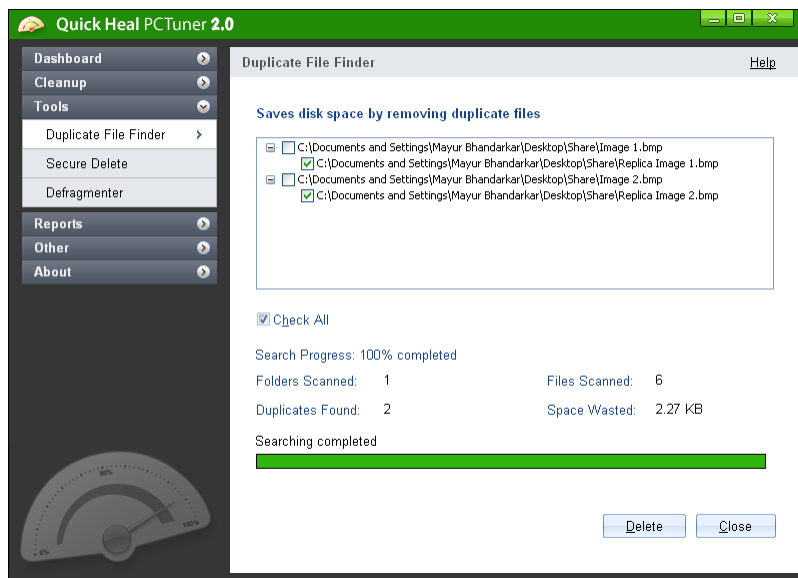


Figure 6-6: Using Duplicate File Finder

10. Check the option **Check All** to select all the duplicate files within the collapsed originals.
11. Click **Delete** button to delete all the duplicate files
12. Click **Close** to exit from the Tools menu.

## SECURE DELETE

The Secure Delete feature is used to for deleting unwanted files or folders completely from the system. Data deleted using the Delete function of Windows can be recovered using Recovery Softwares as the link to such data remains in the cluster of hard drives. The Secure Delete feature of Quick Heal PCTuner deletes the file or folders directly from the hard drive making it unrecoverable even if Recovery Softwares are used.

### Deletion Methods

There are three file deletion methods available in Quick Heal PCTuner. They are:

<b>One Pass Random – Quick Data Destruction</b>	One Pass Random deletion method uses random letters to overwrite the data. This method of deletion is quick and quite secure. Data once deleted cannot be recovered. This is the best choice for most users. This is also the default file deletion method.
<b>Two Pass – More Secure Destruction</b>	Two Pass deletion method uses twice the number of random letters to overwrite the data. This method of deletion provides additional layer of security. Data once deleted cannot be recovered by any recovery software.
<b>DoD – Standard Data Destruction</b>	DoD deletion uses the encryption method of using random letters to overwrite data as per the Department of Defense Memo. Data once deleted cannot be recovered by any recovery software.

## How to use Secure Delete

To delete files or folders using Secure Delete, please perform the following steps

1. Click **Tools** -> **Secure Delete**.
2. Click **Options** button. The **Select Secure Delete Method** window opens. Select the deletion method and click **Accept** button.
3. Click **Add File** button to locate the file you want to delete.
4. Click **Add Folder** button to locate the folder and its sub folders you want to delete.

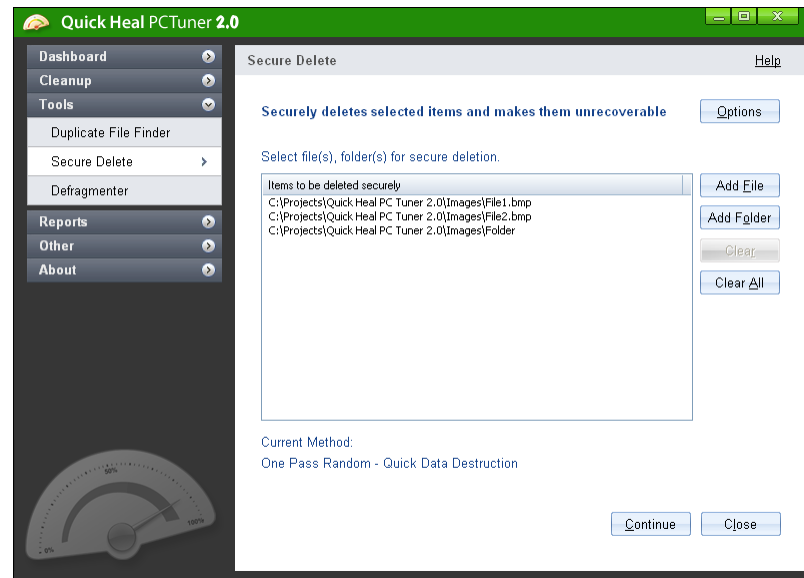


Figure 6-7: Using Secure Delete

5. If the selection for file deletion is incorrect, highlight the file and click **Clear**. Click **Clear All** to delete all the selections.
6. Click **Continue**.
7. A window appears saying that the deletion is unrecoverable. It also allows you to change the deletion method. If you want to change the deletion method at this stage, click **Options**. Click **Yes** to proceed with the deletion process.
8. The selected files will be deleted and a **Deletion Summary** screen appears. Click **View Report** button to view the report of the deletion process else click **Close** to exit from Tools Menu.

## DEFRAGMENTER

The Defragmenter feature defragments vital files, such as page-files and registry hives for improving the performance of the system. Files are often stored in different locations slowing down system performance. Defragmenter reduces the number of file fragments and clubs all the file fragments into one contiguous chunk on the disk to improve system performance.

### How to use Defragmenter

To defragment the hard drive, please perform the following steps:

1. Click **Tools** -> **Defragmenter**.
2. There are two options: **Enable defragmentation** and **Cancel defragmentation**. By default, **Cancel defragmentation** is selected. Select **Enable defragmentation**.
3. Select **Defragment at next boot** to perform defragmentation the next time you start the system; else select **Defragment at every boot** to perform defragmentation every time you start the system.
4. By default **Defragment system paging file (Virtual Memory)** and **Defragment Windows Registry** is checked. You can uncheck any of these two for the Defragmenter to skip, although we recommend that you keep these options checked.
5. Click **Apply** button to save these settings; else click **Close** to exit without saving.

## USING PCTUNER REPORTS

The **Reports** menu will contain reports for various tune-up activities performed by Quick Heal PCTuner. The Reports menu consists of seven menu items. Each menu item corresponds to a report of a particular tune-up activity. The menu items of **Reports** menu are as follows:

- Auto Cleanup Reports
- Disk Cleanup Reports
- Registry Cleanup Reports
- Traces Cleanup Reports
- Secure Delete Reports
- Duplicate File Finder Reports
- Restore Reports

There are four buttons in each menu item. Their actions are the same for all menu items. The four buttons and their actions are as follows:

Button	Action
<b>Details</b>	Click this button to display a detailed report of the highlighted record in the list.
<b>Clear</b>	Click this button to delete the highlighted record in the list.
<b>Clear All</b>	Click this button to delete all the reports in the list.
<b>Close</b>	Click this button to exit from the <b>Reports</b> menu.

Click the **Details** button in any menu item to open a window called **Report**, which contains five more buttons whose actions are common to all the menu items. The five buttons are as follows:

Button	Action
<b>Prev</b>	Click this button to display the detailed report of the previous record in the list. This button will be disabled if the record being accessed is the first record in the list.
<b>Next</b>	Click this button to display the detailed report of the next record in the list. This button will be disabled if the record being accessed is the last record in the list.
<b>Save As</b>	Click this button to save the detailed report in <b>.txt</b> format on your system.
<b>Print</b>	Click this button to take a print-out of the detailed report.
<b>Close</b>	Click this button to exit from the <b>Report</b> window

## AUTO CLEANUP REPORTS

Auto Cleanup Reports contains a list of records distinguished by **Date** and **Time**. Each record contains a detailed report of **Auto Cleanup** feature performed on the system. To view Auto Cleanup Reports please perform the following steps:

1. Click **Reports** -> **Auto Cleanup**.
2. Highlight the required record in the list.
3. Click the **Details** button.
4. The **Report** window appears that contains the detailed report for the highlighted record.

## DISK CLEANUP REPORTS

Disk Cleanup Reports contains a list of records distinguished by **Date** and **Time**. Each record contains a detailed report of **Disk Cleanup** feature performed on the system. To view Disk Cleanup Reports please perform the following steps:

1. Click **Reports** -> **Disk Cleanup**.
2. Highlight the required record in the list.
3. Click the **Details** button.
4. The **Report** window appears that contains the detailed report for the highlighted record.

## REGISTRY CLEANUP REPORTS

Registry Cleanup Reports contains a list of records distinguished by **Date** and **Time**. Each record contains a detailed report of **Registry Cleanup** feature performed on the system. To view Registry Cleanup Reports please perform the following steps:

1. Click **Reports** -> **Registry Cleanup**.
2. Highlight the required record in the list.
3. Click the **Details** button.
4. The **Report** window appears that contains the detailed report for the highlighted record.

## TRACES CLEANUP REPORTS

Traces Cleanup Reports contains a list of records distinguished by **Date** and **Time**. Each record contains a detailed report of **Traces Cleanup** feature performed on the system. To view Traces Cleanup Reports please perform the following steps:

1. Click **Reports** -> **Traces Cleanup**.
2. Highlight the required record in the list.
3. Click the **Details** button.
4. The **Report** window appears that contains the detailed report for the highlighted record.

## SECURE DELETE REPORTS

Secure Delete Reports contains a list of records distinguished by **Date** and **Time**. Each record contains a detailed report of **Secure Delete** feature performed on the system. To view Secure Delete Reports please perform the following steps:

1. Click **Reports** -> **Secure Delete**.
2. Highlight the required record in the list.
3. Click the **Details** button.
4. The **Report** window appears that contains the detailed report for the highlighted record.

## DUPLICATE FILE FINDER REPORTS

Duplicate File Finder Reports contains a list of records distinguished by **Date** and **Time**. Each record contains a detailed report of **Duplicate File Finder** feature performed on the system. To view Duplicate File Finder Reports please perform the following steps:

1. Click **Reports** -> **Duplicate File Finder**.
2. Highlight the required record in the list.
3. Click the **Details** button.
4. The **Report** window appears that contains the detailed report for the highlighted record.

## RESTORE REPORTS

Restore Reports contains a list of records distinguished by **Date** and **Time**. Each record contains a detailed report of **Restore** feature performed on the system. To view Restore Reports please perform the following steps:

1. Click **Reports** -> **Restore**.
2. Highlight the required record in the list.
3. Click the **Details** button.
4. The **Report** window appears that contains the detailed report for the highlighted record.



## OTHER FEATURES

This chapter covers information about the two remaining menus of PCTuner: **Other** and **About**.

### OTHER

The **Other** menu contains a menu item called **Restore**. The Restore feature restores the items to its original locations that were deleted by the Disk Cleanup and Registry Cleanup feature. It does not restore the items deleted by Traces Cleanup. If the Auto Cleanup feature is executed, then the Restore feature will restore only the items deleted by the Disk Cleanup and Registry Cleanup feature and skip the items deleted by Traces Cleanup feature.



The **Restore** feature will only work if the **Delete items without taking backup** checkbox is kept unchecked during Disk Cleanup or Registry Clean Up. In case of Auto Cleanup, the option **Take backup before deleting the items** should be checked in the **Quick Heal PCTuner Options** window.

The **Restore Points** area lists out up to five tune-up activities that can be restored. The actions that can be performed on the Restore Points are as follows:

- Restore
- Delete
- Close

#### Restore

To restore any of the five restore points in the list, please perform the following steps:

1. Highlight the required restore point.
2. Click **Restore** button.
3. A message box pops up with the following prompt: **This will restore all the changes done to the system and will restore the deleted item(s). Are you sure you want to restore the backup?** Click **Yes** if you want to restore the backup, else click **No** if you don't want to restore the backup.
4. If you clicked **Yes** in the previous step, the backup will be restored and a message box will pop-up saying **The selected backup was restored successfully**. Click **OK** to complete the restore process.

#### Delete

To delete any of the restore points in the list, please perform the following steps:

1. Highlight the required restore point.
2. Click **Delete** button.
3. A message box will pop-up with the following prompt: **This will permanently delete the backup file. You will lose the changes stored in this backup file. Are you sure you want to delete it?** Click **OK** if you want to delete the restore point, else click **Cancel** to exit without deleting.

#### Close

Click **Close** button to exit from the **Other** menu.

## ABOUT

The **About** menu contains a menu item called **Information**. The Information screen contains the following information:

- Name of the software and version.
- Copyright information
- Whether the software is registered or not
- Legal warning

The Information screen also contains the following buttons:

- Activate/License Details
- Support
- Close

### Activate/License Details

The **Activate** button will only be available if the registration process of the PCTuner has not been completed. If the registration has not been completed, then click **Activate** button to begin the Registration process.

If the registration of Quick Heal PCTuner is complete, then **License Details** button will replace the **Activate button**. Clicking the **License Details** button will open the **PCTuner License Details** window. It will contain the following details:

- Your Name
- Product key
- Installation Number
- Quick Heal PCTuner License Agreement

Click **Print License Details** button to take a print-out of the license details; else click **Close** button to exit from the **PCTuner License Details** window.

### Support

Click the **Support** button to open a window **PCTuner Support Information**. The **PCTuner Support Information** window contains details about Quick Heal Technical Support. It also contains the following buttons:

<b>Save As</b>	Click <b>Save As</b> to save Quick Heal Technical Support information in <b>.txt</b> format.
<b>Print</b>	Click <b>Print</b> to take a print-out of Quick Heal Technical Support information.
<b>Close</b>	Click <b>Close</b> to exit from the <b>PCTuner Support Information</b> window.

### Close

Click **Close** button to exit from the **About** menu.

## 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 **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 Default.
To restore default settings for all options	On any page in the Options window, click Default All.

## 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>	<p>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.</p>
<b>All files</b>	<p>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.</p>
<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 <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, MSeExpand, 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 email attachments with Outlook Express 5.0. It scans email 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 email. 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 email. 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>	<p>DNAScan suspected files can be submitted to Quick Heal research lab.</p> <p>If <b>Show notification while submitting the files</b> option is checked, then Quick Heal prompts for permission before submission of samples to Quick Heal Research Lab.</p> <p>If <b>Show notification while submitting the files</b> option is not checked, then Quick Heal submits the suspicious files without notifying you.</p>



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 **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 whenever 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 Email Attachments, Internet Downloads, Network, File Execution and Copying.

### To Customize Online Protection

1. Start **Quick Heal Total Security**.
2. Click **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> <b>User Specified Extensions</b>	<p>Scans files that are most likely to get infected by a virus.</p> <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 <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 - EMAIL PROTECTION

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

### General Settings

<b>Enable Protection</b> <b>Display Alert Message</b>	<p>This option enables scanning of emails while downloading.</p> <p>Virus found alert will be shown in case a virus is found in an email or attachment. Display Alert Message will contain following information:</p> <ul style="list-style-type: none"><li>• Virus Name</li><li>• Sender Email Address</li><li>• Recipient Email Address</li><li>• Email 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 email attachment. You will get a prompt from Total Security Email 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> <b>Repair automatically, Delete if unsuccessful</b> <b>Backup before repairing</b>	<p>Selecting this option will delete the infected attachment while downloading mails.</p> <p>Attempts to repair the virus without interacting with you. If the attachment cannot be repaired then it will be deleted.</p> <p>Email Protection will keep a copy of infected email before disinfecting it. (Files that are stored in backup can be restored from Quarantine menu.)</p>
---	--

## Control attachments to your incoming email

<b>Block attachments with multiple extensions</b>	Worms commonly use multiple extensions. Enabling this option will block multiple extension attachments in incoming emails. 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 emails, which contain vulnerability like MIME, IFRAME, etc. Sending an email 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</b> – Enable attachment blocking in incoming email.	
<b>All attachments</b>	Selecting this option will delete all the attachments in incoming emails. This option is only recommended for users who require high security or prefer text based emails 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 <b>User specified extensions</b>.</li><li>2. Press <b>Customize</b>.</li><li>3. Type the extension name. For example: 'mpg'.</li><li>4. Click <b>Add</b> to add the extension in the list.</li><li>5. Click <b>Ok</b> to save the settings.</li></ol>

## Prevent new worm infection filtering email clients

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

## PROTECTION — ANTISPAM

Quick Heal AntiSpam has been integrated with Quick Heal Email 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 **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>

<p><b>Enable AntiSpam Plugin</b></p>	<p>In the earlier version of Quick Heal Total Security, adding email addresses, to the Black List or White List was done using the Options Menu of Quick Heal Total Security. To know more about these methods see <a href="#">Enable Black List</a> and <a href="#">Enable White List</a>. Although one can still add email address to the Black List or White List this way, the AntiSpam plugin feature in Quick Heal Total Security minimizes the effort for the user by providing options in MS Outlook or Eudora mail client. This plugin is user-friendly and will help the user to add email address to the Black List or White List just by a single click.</p> <p>To add specific email address in the black list, please perform the following step:</p> <ul style="list-style-type: none"> <li>Highlight the mail and click the <b>Quick Heal Black List</b> button in case of MS Outlook. In case of Eudora, highlight the mail and click <b>Edit -&gt; Message Plug-ins -&gt; Quick Heal Black List</b>.</li> </ul> <p>The sender of the email will be added into Quick Heal Black List.</p> <p>To add specific email address in the white list, please perform the following step:</p> <ul style="list-style-type: none"> <li>Highlight the mail and click the <b>Quick Heal White List</b> button in case of MS Outlook. In case of Eudora, highlight the mail and click <b>Edit -&gt; Message Plug-ins -&gt; Quick Heal White List</b>.</li> </ul> <p>The sender of the email will be added into Quick Heal White List even if the sender's email ID is suspected by Quick Heal as spam.</p> <p>AntiSpam plugin feature will only work with Eudora and MS Outlook email clients. In case of MS Outlook, for 64-bit operating systems, the AntiSpam plugin feature will only work if a 64-bit MS Outlook is installed on your system. Also, <b>Enable Black List</b> and <b>Enable White List</b> have to be checked under <b>Options -&gt; AntiSpam</b>.</p>
<p><b>Import List</b></p>	<p>If you have exported or saved anti spam data and wish to use the same. You can import the existing list using this feature.</p>
<p><b>Export List</b></p>	<p>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.</p>



## ANTI-SPAM FILTER FOLDER

Quick Heal AntiSpam scans the mail while scanning it will append the subject of the Spam mail with **[SPAM]** -. A SpamMails folder in the email 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 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 **Finish** to save the rule.

### Remember simple steps to create filters

To configure all email 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 **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).

## Enable Browsing Protection

Quick Heal Total Security blocks malicious content from the websites before the user can access them, using the Browsing Protection feature. To enable Browsing Protection, please perform the following steps:

1. Select **Block infecting Web URLs**.
2. Click **OK** to save the changes.

## PROTECTION — DATA PROTECTION

1. Start **Quick Heal Total Security**.
2. Click **Options**, under main windows menu of the Quick Heal Total Security.
3. Click **Protection** tab.
4. Select **Data Protection** option.
5. Click **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 cannot be performed.



This protection is not implied for floppy drives.

## PROTECTION — PACKER IDENTIFICATION

Packers are files that pack together many files, or compress a single file to reduce file size. These files do not need a third party application to get unpacked. They have an inbuilt functionality of packing and unpacking. Packers can also be used as tools to spread malware by packing a malicious file amidst a set of files. There are certain packers that are used specifically to spread malicious files. These packers, when unpacked can cause harm to your PC. By default Quick Heal Packer Identification scans the system for a select list of highly suspicious packers and alerts you if such a packer is found.

You can also customize the list of packers that Quick Heal Packer Identification can scan. To include additional packers in the scan please customize the Packer Identification by performing the following steps:

1. Start **Quick Heal Total Security**.
2. Click **Options** under main windows menu of the Quick Heal Total Security.
3. Double click **Protection** to collapse the Protection menu.
4. Select **Packer Identification**.

### General Settings

<b>Identify packed files</b>	Check this feature to identify packer files during the scan. You can customize the list of packers to be detected by clicking the <b>Customize</b> button. For novice users we recommend not to change the settings as the default settings will provide optimum safety.
------------------------------	--

## How to respond when a packer is found

<b>Action for scanner</b>	Select the action that the scanner needs to take when a suspicious packer is detected while scanning. The following actions can be performed when the scanner detects a suspicious packer file: <ul style="list-style-type: none"><li>• <b>Report only:</b> Leaves the infected packer as it is and generates a report of the infections detected.</li><li>• <b>Quarantine:</b> The infected packer will be moved to the quarantine folder.</li></ul>
<b>Action for scanner in case of archive files</b>	Select the action that the scanner needs to take if an archive is found while scanning. The following actions can be performed by the scanner: <ul style="list-style-type: none"><li>• <b>Report only:</b> Leaves the infected archive file as it is and generates a report of the infections detected.</li><li>• <b>Quarantine:</b> The infected archive file will be moved to the quarantine folder.</li></ul>
<b>Action for Online Protection</b>	The following actions can be performed when Online Protection detects a suspicious packer file: <ul style="list-style-type: none"><li>• <b>Deny access:</b> Completely blocks access to the infected packer.</li><li>• <b>Quarantine:</b> The infected packer file will be moved to the quarantine folder.</li></ul>

## UPDATES - AUTOMATIC UPDATES

1. Start **Quick Heal Total Security**.
2. Click **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 **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>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:\QHMSGR**
3. Share this folder with Read access rights on the network.
4. Now click **Start** and point to **Programs, Quick Heal Total Security** and **Quick Heal Total Security**.
5. Click **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:\QHMSGR**
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\QHMSGR**
12. Click **OK** to save the changes.

## UPDATES - INTERNET SETTINGS

1. Start **Quick Heal Total Security**.
2. Click **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 **Options**, under the top menu of Quick Heal Total Security.
3. Select **Exclusion** under the Miscellaneous tab.
4. Click **New**.
5. Click 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 above 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.
---	---



## Scan removable devices

<b>Scan removable device when plugged into the system</b>	<p>If this option is enabled, then Quick Heal will prompt you to perform a scan of removable device except CDs or DVDs. The user has two options:</p> <ul style="list-style-type: none"><li>• Scan files on root of drive only</li><li>• Scan full drive</li></ul> <p>Select the necessary option and click <b>Scan</b> button. We recommend that you scan any USB removable storage devices before using it, but if you wish to use the device without scanning it first, then click <b>Do Not Scan</b> button to exit from the scanner prompt.</p>
---	--

## Self Protection

<b>Start Self Protection at Windows Startup</b>	<p>If this option is enabled, then Quick Heal Total Security will protect itself by safeguarding Quick Heal files, folders, configurations and registry entries against malwares and also against tamper from other applications.</p>
---	---

## 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/Email 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>	View 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 Skip folder. 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 Skip file. 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 Reports 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 List files while scanning in the Scanner's 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

For specified options '-' inverts the default meaning.

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

### 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 **Start -> Programs -> Quick Heal Total Security -> Quick Update**.
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 **Start -> Programs -> Quick Heal Total Security -> Quick Update**.
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 **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 **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.

## 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?

You can call to 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 and 6:00 PM (Indian Standard time).

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

- Your Product key which is included in the boxed version of the products. If you have purchased our products on-line then you will find the Product key 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 helps 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	Global Support Center
<p>Quick Heal Technologies (P) Ltd. 603, Mayfair Towers II, Wakdewadi, Shivajinagar, Pune 411005, Maharashtra Phone: +91-20-41060400 Fax: +91-20-41060401 Email: <a href="mailto:info@quickheal.com">info@quickheal.com</a></p>	<p>Telephone Support</p> <p>Toll Free Number: 1800-233-3733 (For Indian Users) Additional Help Line for Support: +91-253-3041888 Email: <a href="mailto:support@quickheal.com">support@quickheal.com</a></p>

Distribution Centers and Support Offices in India		
<p><b>Ahmedabad</b></p> <p>Quick Heal Technologies (P) Ltd. 318, Saman Complex, Opposite Satyam Mail, Near Manasi Char Rasta, Satellite, Ahmedabad 380015, Gujrat Phone: +91-79-32524771 Email: <a href="mailto:ahd@quickheal.co.in">ahd@quickheal.co.in</a></p>	<p><b>Aurangabad</b></p> <p>Quick Heal Technologies (P) Ltd. S-2, Chandrakala Arcade, Nirala Bazar Road, Aurangpura, Aurangabad 431001, Maharashtra Phone: +91-240-2336000 Email: <a href="mailto:aurangabad@quickheal.co.in">aurangabad@quickheal.co.in</a></p>	<p><b>Bangalore</b></p> <p>Quick Heal Technologies (P) Ltd. #1422, 37<sup>th</sup> 'B' Corss, 11<sup>th</sup> Main, 4<sup>th</sup> 'T' Block, Jayanagar, Bangalore 560041, Karnataka Phone: +91-80-41304560 Email: <a href="mailto:bangalore@quickheal.co.in">bangalore@quickheal.co.in</a></p>
<p><b>Baroda</b></p> <p>Quick Heal Technologies (P) Ltd. SF-30, Sunner Complex, Hari Nagar Junction, Gotri Road, Baroda 390021, Gujrat Phone: +91-265-2390953 Email: <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. 43, Second Floor, Sector 31-D, Chandigarh 160030 Phone: +91-172-3250233 Email: <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, 53<sup>rd</sup> Street, Near Anjanayar Temple, Ashok Nagar, Chennai – 600083, Tamil Nadu Phone: +91-44-32421551 Telephone: <a href="mailto:chennai@quickheal.co.in">chennai@quickheal.co.in</a></p>
<p><b>Cochin</b></p> <p>Quick Heal Technologies (P) Ltd. N-38/351, Sy No. 2/20, EARA-113, Near Mailalathu Temple, Near Edappally Junction, Edappally, Cochin 682024, Kerala Phone: +91-484-3290908 Email: <a href="mailto:cochin@quickheal.co.in">cochin@quickheal.co.in</a></p>	<p><b>Coimbatore</b></p> <p>Quick Heal Technologies (P) Ltd. C/o A. Ajeema, Old No. 160, New No. 111, 6 Street – Extension, 100 Feet Road, Gandhipuram, Coimbatore 641012, Tamil Nadu Phone: +91-422-3215758 Email: <a href="mailto:coimbatore@quickheal.co.in">coimbatore@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 Narasu Mansion, 95, Parklane, Opposite Hotel Parklane, Secunderabad 500003, Andhra Pradesh Phone: +91-40-27845782 / 66387437 Email: <a href="mailto:hyderabad@quickheal.co.in">hyderabad@quickheal.co.in</a></p>

<b>Indore</b> Quick Heal Technologies (P) Ltd. Flat No. 202, Rani Sati Apartments, C-Block, 60/1/5, New Dewas Road, Ahilya Mata Colony, Indore 452001, Madhya Pradesh Phone: +91-731-4236021 Email: <a href="mailto:indore@quickheal.co.in">indore@quickheal.co.in</a>	<b>Mumbai</b> Quick Heal Technologies (P) Ltd. 408, 3 <sup>rd</sup> Floor, 'D' Wing, Mathura Bhuvan, CHS, Dada Saheb Phalke Road, Dadar (E) Mumbai 400014, Maharashtra Phone: +91-22-42310701/2/3/4 Email: <a href="mailto:mumbai@quickheal.co.in">mumbai@quickheal.co.in</a>	<b>Nagpur</b> Quick Heal Technologies (P) Ltd. Flat No. 8, Plot No. G.B.27, Ahilya Niwas, 2 <sup>nd</sup> Floor, Jitendra Singh Tomer Road, Giripeth, Nagpur 440010, Maharashtra Phone: 91-712-2540750 Email: <a href="mailto:nagpur@quickheal.co.in">nagpur@quickheal.co.in</a>
<b>Nashik</b> Quick Heal Technologies (P) Ltd. 12, Komal Residency, Sadhu Waswani Road, Near MICO Circle, Nashik 422005, Maharashtra Phone: +91-253-2576306 Email: <a href="mailto:nashik@quickheal.com">nashik@quickheal.com</a>	<b>New Delhi</b> Quick Heal Technologies (P) Ltd. 3066/7B, Ground Floor, Near Sarvodaya Kanya Vidyalay, Ranjit Nagar South Patel Nagar, New Delhi 110008 Phone: +91-11-25846645 / 25846646 / 25842974 Email: <a href="mailto:delhi@quickheal.co.in">delhi@quickheal.co.in</a>	<b>Pune</b> Quick Heal Technologies (P) Ltd. Office No. 101, Shree Sai Narayan Apartment, Ganjave Chowk, Navi Peth, Opposite Patrakar Bhavan, LBS Road, Pune 411030, Maharashtra Phone: +91-20-41402901/02/03/04 Email: <a href="mailto:punesales@quickheal.com">punesales@quickheal.com</a> (Sales) Email: <a href="mailto:helpdesk@quickheal.com">helpdesk@quickheal.com</a> (Support)  Quick Heal Technologies (P) Ltd. Office No. 56, Jai Ganesh Vardhast Complex, Opposite Traffic Police Station, Pimpri Chowk, Pune 411018, Maharashtra Phone: +91-20-30687567 Email: <a href="mailto:pcmc@quickheal.com">pcmc@quickheal.com</a>
<b>Rajkot</b> Quick Heal Technologies (P) Ltd. C/o Amity Software and Solutions, 213 Penorama Complex, Opposite SBI Bank, Gondal Road, Rajkot 360001, Gujarat Phone: +91-281-3012580 Email: <a href="mailto:ahd@quickheal.co.in">ahd@quickheal.co.in</a>	<b>Surat</b> Quick Heal Technologies (P) Ltd. C/o Amity Software and Solutions, 101. Maher Park – B Athwa Gate, Ring Road, Surat 390007, Gujarat Phone: +91-261-2464365 Email: <a href="mailto:baroda@quickheal.co.in">baroda@quickheal.co.in</a>	<b>Visakhapatnam</b> Quick Heal Technologies (P) Ltd. D.No. 14-1-40, 1 <sup>st</sup> Floor, Nowroji Road, Maharani Peta, Visakhapatnam 530002, Andhra Pradesh Phone: +91-891-3245454 Email: <a href="mailto:vizag@quickheal.co.in">vizag@quickheal.co.in</a>
For more details, please visit <a href="http://www.quickheal.com">www.quickheal.com</a>		