

**Quick Heal®**

*Security Simplified*

# User Guide

Quick Heal Total Security  
Quick Heal AntiVirus Pro  
Quick Heal Internet Security  
Quick Heal AntiVirus Server Edition  
Quick Heal Internet Security Essentials

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

# Copyright Information

Copyright © 2013 Quick Heal Technologies (P) Ltd.

## **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 media 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 is a registered trademark of Quick Heal Technologies (P) Ltd.

# End-User License Agreement

## IMPORTANT

PLEASE READ THIS END-USER LICENSE AGREEMENT CAREFULLY BEFORE USING THIS SOFTWARE.

BY USING THIS SOFTWARE OR BY CLICKING THE "I AGREE" BUTTON OR LOADING OR ATTEMPTING TO LOAD THE QUICK HEAL SOFTWARE, IN ANY WAY (WILL CONSTITUTE A SYMBOL OF YOUR SIGNATURE), YOU ACKNOWLEDGE AND ADMIT THAT YOU HAVE READ, UNDERSTOOD AND AGREED TO ALL THE TERMS AND CONDITIONS OF THIS END-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.

This License is a legally enforceable contract between you as an individual (assuming you are above 18 years and/or eligible to enter into an agreement), or the Company or any legal entity/organization that will be using the software (hereinafter referred to as 'you' or 'your' for the sake of brevity) referred to as the licensee, and Quick Heal Technologies Private Limited, Pune (hereinafter referred as "Quick Heal" for the sake of brevity) and you shall have the right to use the software subject to the terms and conditions mentioned in this agreement or as amended by Quick Heal from time to time.

In consideration of payment of the License Fee, which is a part of the price, evidenced by the Receipt, Quick Heal grants the Licensee, a non-exclusive and non-transferable right. Quick Heal 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 the property of Quick Heal and are copyrighted. Copying of the Software or the written material is expressly forbidden.

### 1. DO'S & DON'TS:

#### **You can:**

- Use one copy of the software on a single computer. In case of multi-users, use the software only on the said number of systems as mentioned on the packaging.
- Make one copy of the software solely for the 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, and reverse engineer the software.
- Try making an attempt to reveal/discover the source code of the software.
- Use for unlicensed and illegal purpose.

## **2. MANDATORY ACTIVATION:**

Quick Heal warns you that in the process of installation of the software, the other security products/software installed on your computer may uninstall or be disabled if the same are not compatible with the Quick Heal software. The license rights granted under this Agreement are limited for 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 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 some reasons. There are technological measures in this Product that is designed to prevent unlicensed or illegal use of the Product. You agree that we may use those measures. You agree that the Quick Heal software may use the measures that can control and prevent piracy of software. As a registered user, you are entitled to receive free (i.e. free of cost) virus database updates and free (i.e. free of cost) version upgrade (whenever Quick Heal releases new version upgrade) during the License period, subject to the terms and conditions mentioned herein.

As the only warranty under this Agreement, and in the absence of accident, abuse or misapplication, Quick Heal 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's only obligation under this Agreement is, at Quick Heal's 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's limited warranty and which is returned to Quick Heal with the copy of the Receipt.

## **3. THIRD PARTY WEBSITE LINKS**

At some point the software product may include links to third party sites; you may link to such third party websites as the user of this software. The third party sites are not under the control of Quick Heal and Quick Heal is not responsible for the contents of any third party website, any links contained in the third party websites. Quick Heal is providing these links to the third party websites to you only as a convenience and is not responsible for any kind of loss/ damage arising out of it.

## **4. SUPPORT**

Quick Heal offers support features during usage of this software i.e., Live Chat with technical support team and/ or the technical support team may, at your discretion, take remote computer access. The availing of this support will be solely at your discretion and you are solely responsible to take the back-up of the existing data/software/programs on your computer before availing such a support and you are liable to bear all the direct, indirect and consequential cost associated to it. Quick Heal will not be held responsible for any loss of data, any kind of direct/ indirect/ consequential loss or damage to data/ property arising during this entire process. If at any point of time the Technical Support team is of the opinion that it is beyond their scope, it will be the sole discretion of Quick Heal to suspend, cease, terminate or refuse such support as Quick Heal does not claim any warranty and/or guarantee of any kind in providing the support feature.

## **5. EMAIL/ELECTRONIC COMMUNICATION**

Once you register the software by activating the software product, Quick Heal 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.

## **6. 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.

All the registered users/subscribers will get the updates free of cost from the date of license activation till the expiry date of the license.

## **7. COLLECTION OF INFORMATION**

Quick Heal's software may collect the following information which may / may not contain any personally identifiable information either with or without your discretion/permission, solely for statistical purpose or enhancing and evaluating the ability, effectiveness and performance of Quick Heal's product in identifying and/or detecting the malicious behavioral pattern, inherently fraudulent websites and other Internet security threats/ risks. This information will not be correlated with any personally identifiable information and shall include, but not limited to:

- Any type of executable files which the Quick Heal software may identify having a potentially malware behavioral pattern.
- Any type of information relating to the status of the software that whether there occurred any error while installing the software or the installation was successful.
- Any type of URLs of websites visited that the Quick Heal software deems inherently and potentially fraudulent.
- Any type of information that the Quick Heal software deems potentially fraudulent, posing security risks/ threats.
- Any type of information for identifying the Media Access Control (MAC) address of the Computer on which the Quick Heal Software has been installed.
- Any type of information for identifying the Internet Protocol (IP) Address and information required for effective license administration and enhancing product functionality and usability.
- You admit that the information/data as collected above can be used for analyzing, preventing and detecting the potential internet security risks, publishing any type of data/ reports/ presentations on the trends collected, sharing the data to create awareness with any organizations, vendors.

## **8. INDEMNIFICATION**

- a. You expressly understand, admit and warrant that in no event shall Quick Heal and/or any of its directors, employees, agents, partners, distributors be liable from any and against all claims, expenses, suits, costs, demands, judgments whatsoever made by you and/ or any third party for any direct, indirect, incidental, special, punitive, consequential and/or exemplary damages including, but not limited to damages for loss of business/profits, damages for loss of confidential/other information, failure to meet any statutory duty/duty of reasonable care/duty in good faith, economic/notional loss, loss for business interruption, goodwill, damage and loss of data or programs, or other intangible losses (even if Quick Heal has been advised of the possibility of such damages), to the fullest extent permissible by law:
  - i. Arising due to your usage of Software;
  - ii. Your negligence or inability of using the Software or support;

- iii. Any dispute between you and third party with respect to availing the Software;
  - iv. Your violation of any rights of any other individual and/or entity;
  - v. Your breach of the Agreement;
  - vi. Your violation of any provisions under any acts in India or abroad;
  - vii. The failure of Quick Heal to provide Support Service or any other service/information.
- b. This limitation will apply to all causes of action whether arise in equity or tort, including but not limited to breach of contract, breach of warranty, negligence, strict liability, misrepresentations and hereby release Quick Heal and/or its directors, employees, agents, distributors from any and all obligations, liabilities in excess of the limitation stated herein.
- c. In the event, Quick Heal and/or its directors, agents, employees, distributors are found liable, You Understand and accept that the liability of Quick Heal and/or its directors, agents, employees, distributors shall be limited only up to and not exceed in any case the License fees incurred by You in acquiring the software from Quick Heal or its distributors/agents. This Clause shall survive the termination of this Agreement.

## **9. LIMITED WARRANTY AND DISCLAIMERS**

The software provided by Quick Heal is “AS IS” and “AS AVAILABLE”

- a. Quick Heal does not warrant, make any representations that the software will work uninterrupted, timely, secure or error-free or shall meet any or all your requirements whether disclosed to Quick Heal or any of its directors, agents, distributors and employees. The entire risks, faults as to performance of the software, the responsibility for selecting the software to achieve your intended results, the results obtained from the Software shall be assumed by You.
- b. The disclaimers and limitations set forth herein will apply regardless of whether you accept the software.
- c. You understand and accept that the Software will substantially perform according to the specifications, descriptions stated in the User Manual, (as updated from time to time), subject to the following and Quick Heal expressly disclaims any and all liabilities arising from the following circumstances:
  - (i) Any actions initiated by You or by third parties which were beyond the reasonable control of Quick Heal;
  - (ii) Any failures, malfunctions, defects resulting from abuse, improper installation, theft, misuse, accident, operation or maintenance, natural calamity, alteration, power failures, casualty, repairs made by any other party than Quick Heal, alterations, neglect, non-permitted modifications, acts of terrorism, vandalism;
  - (iii) The deficiencies, defects in Your computer and related infringements;
  - (iv) Your violations of the terms and conditions described in the User manual or in this Agreement.

## **10. INTELLECTUAL PROPERTY**

The software, source code, activation code, license keys, documentation, systems, ideas, information, content, design and other matters related to the software, trademarks are the sole proprietary and Intellectual Property rights of Quick Heal protected under the Intellectual property Laws and belongs to Quick Heal. Nothing contained in this Agreement grant to You any rights, title, interest to intellectual property, including without limitation any error corrections, enhancements, updates or modifications to the Software whether made by Quick Heal or any third party. You understand and acknowledge that you

are provided with a License to use the software subject to the terms and conditions of this Agreement.

## 11. GENERAL

- a. **Force Majeure.** Quick Heal will not be liable for any delay or failure to fulfill its obligations hereunder that results from any natural calamity (such as earthquake, flood etc.), war, civil disturbance, government policies, or other cause/s beyond its control. Provided that Quick Heal shall endeavour to complete the task within a reasonable period after happening of any event as covered under such force majeure.
- b. **Legal Jurisdiction.** This agreement and any matter relating thereto shall be subject only to jurisdiction of Courts at Pune, India and shall be interpreted as per the terms of the law/s for the time being in force in India. Any dispute which may arise out of this Agreement, breach of terms and conditions under this Agreement, shall be settled by direct negotiations between You and Quick Heal. In the case of failure to resolve the dispute in the manner set out above within 30 days from the date when the dispute arose, the dispute shall be referred to a panel of three arbitrators, with Quick Heal appointing one arbitrator, You appointing one arbitrator and the arbitrators so appointed jointly nominating a third presiding arbitrator. The venue of arbitration shall be Pune. The arbitration proceedings shall be governed by the Arbitration and Conciliation Act, 1996 and Indian Laws and shall be conducted in the English language. The arbitrators shall also decide on the costs of the arbitration proceedings. To the extent possible, after the commencement of any arbitral proceedings the Parties shall continue to perform their respective obligations under this Agreement. The provisions of this Clause shall survive termination of this Agreement. Subject to the provisions of this Clause, the Courts in Pune, India shall have exclusive jurisdiction and the parties may pursue any remedy available to them at law or equity.
- c. **Complete Agreement.** This Agreement comprises the entire agreement between the parties regarding the subject matter, and supersedes any proposals, communications or advertising, oral or written, with respect to the Software or subject matter of this Agreement. You shall be bound by any and all clauses of the Agreement updated and displayed by Quick Heal on [www.quickheal.com](http://www.quickheal.com) (the website) from time to time and the Agreement displayed on the website (from time to time) will be the finally concluded and binding Agreement between You and Quick Heal for all legal purposes which includes your each activation, re-activation and renewal of this Software. In case of any dispute/queries arising out of any translated versions of this Agreement, Quick Heal hereby expressly specifies and confirms that the English version as displayed on the website will be final for interpretation and the terms used, meaning conveyed in the English version will be authoritative and binding. Any waiver by either party of any violation of any provision of this agreement by the other party will not be deemed to waive any other violation of the same or any other provision.
- d. **Severability.** If any of the provisions contained in this Agreement is found by a court of competent jurisdiction to be invalid, illegal or unenforceable in any respect, the validity, legality or enforceability of the remaining provisions contained herein shall not be in any way affected or impaired thereby and the balance of the Agreement will continue in full force and effect to the maximum extent permitted by law or equity while preserving, to the fullest extent possible, its original intent.
- e. **Survival.** The Clauses in this Agreement including but not limited to rights to License fees receivable, “Indemnification”, “Limited Warranties & Disclaimers” and “Intellectual Property” shall survive expiration or termination of this Agreement.
- f. You cannot assign your rights or delegate duties or obligations under this Agreement. The failure to exercise or delay in exercising a right or remedy by Quick Heal under this Agreement shall not constitute a waiver of the right or remedy or a waiver of any prior, concurrent or subsequent right or remedy.
- g. The Section numbers and headings are included merely for the convenience of the parties and are not to be construed in interpreting this Agreement.

- h. Quick Heal reserves the right to co-operate with any legal process and may provide documents, information related to your usage of the Software and your general usage of the Computer.




---

# About the Document

This User Guide covers all the information about how to install and use Quick Heal products on Windows operating systems in the easiest possible ways. We have ensured that the details provided in this guide are up-to-date with the latest developments in the software.

The following list describes the conventions that we have followed to prepare this document.

Convention	Meaning
<b>Bold Font</b>	Anything highlighted in bold indicates that it may be a menu title, window title, check box, drop-down box, dialog, button names, and so on.
	This symbol indicates additional information or important information about the topic being discussed.
<Step 1> <Step 2>	The instruction mentioned in the numbered list indicates actions that you need to perform.
Product Name	The term Quick Heal AntiVirus is used as a generic term in this document. It may refer to any of the following products: Quick Heal AntiVirus Pro, Quick Heal Internet Security Essentials, Quick Heal Internet Security, Quick Heal Total Security, and Quick Heal AntiVirus Server Edition depending on the product you have purchased.

# Quick Heal Products Compared

	Quick Heal AntiVirus Pro	Quick Heal IS Essentials	Quick Heal AntiVirus Server Edition	Quick Heal Internet Security	Quick Heal Total Security
<b>Core Protection</b>					
<ul style="list-style-type: none"> <li>• Anti-virus</li> <li>• AntiSpyware</li> <li>• AntiMalware</li> <li>• Anti-Rootkit</li> </ul> <ul style="list-style-type: none"> <li>• Silent Firewall</li> <li>• Intrusion Detection</li> <li>• Intrusion Prevention</li> </ul>	✓	✓	✓	✓	✓
<b>Mail Protection</b>					
<ul style="list-style-type: none"> <li>• Spam protection</li> </ul>		✓	✓	✓	✓
<b>Internet Protection</b>					
<ul style="list-style-type: none"> <li>• Browser Sandbox</li> </ul>	✓	✓		✓	✓
<ul style="list-style-type: none"> <li>• Phishing Protection</li> </ul>		✓	✓	✓	✓
<ul style="list-style-type: none"> <li>• Web Security</li> <li>• Parental Control</li> </ul>				✓	✓
<b>Privacy Protection</b>					
<ul style="list-style-type: none"> <li>• Data Theft Protection</li> </ul>			✓		✓
<ul style="list-style-type: none"> <li>• Secure Delete</li> </ul>					✓
<b>PC Optimization</b>					
<ul style="list-style-type: none"> <li>• Registry Cleanup</li> <li>• Disk Cleanup</li> <li>• Traces Cleanup</li> </ul> <ul style="list-style-type: none"> <li>• Registry Defragmenter</li> <li>• Duplicate File Finder</li> </ul>					✓
<b>Mobile Phone Protection</b>					
<ul style="list-style-type: none"> <li>• PC2Mobile Scan</li> </ul>					✓

---

# Contents

<b>End-User License Agreement .....</b>	<b>2</b>
<b>About the Document .....</b>	<b>8</b>
<b>Quick Heal Products Compared .....</b>	<b>9</b>
<b>Chapter 1. Getting Started .....</b>	<b>15</b>
Prerequisites .....	15
System Requirements.....	15
Installing Quick Heal AntiVirus.....	19
Uninstalling Quick Heal AntiVirus.....	20
<b>Chapter 2. Registration, Re-activation and Renewal .....</b>	<b>21</b>
Registration.....	21
<i>Registering Online .....</i>	<i>21</i>
<i>Registering Offline .....</i>	<i>22</i>
Obtaining Product Key and Installation Number .....	22
Generating Activation Key for offline activation.....	23
<i>Registering through SMS.....</i>	<i>23</i>
<i>Multi-users Pack Registration .....</i>	<i>24</i>
Re-activation .....	25
Renewal .....	25
<i>Renewing Online .....</i>	<i>25</i>
<i>Renewing Offline .....</i>	<i>26</i>
Getting the details of Quick Heal AntiVirus .....	26
Generating Activation Key for offline activation.....	27
Receiving <license> .key file.....	27
Renewing Quick Heal AntiVirus with <license>.key file .....	27
<i>Multi-users Pack Renewal .....</i>	<i>28</i>
<i>Things to Do if the Product Key is Lost .....</i>	<i>28</i>
<b>Chapter 3. Quick Heal AntiVirus Dashboard .....</b>	<b>29</b>
About Quick Heal AntiVirus Dashboard .....	29
Right Shell Menu Options .....	31
Performing Manual Scans.....	31
<i>Performing Full System Scan.....</i>	<i>32</i>
<i>Performing Custom Scan.....</i>	<i>32</i>
<i>Performing Memory Scan .....</i>	<i>32</i>
<i>Performing Boot Time Scan.....</i>	<i>33</i>
<i>Performing Mobile Scan.....</i>	<i>34</i>

---

<b>Chapter 4. Quick Heal Protection Center .....</b>	<b>35</b>
Files & Folders .....	36
<i>Scan Settings</i> .....	36
Scan archive files.....	38
Select the type of archive that should be scanned.....	38
Scan packed files.....	39
Scan mailboxes .....	39
<i>Virus Protection</i> .....	39
<i>Advanced DNA Scan</i> .....	41
<i>Block Suspicious Packed Files</i> .....	43
<i>Automatic Rogueware Scan</i> .....	43
<i>Scan Schedule</i> .....	43
Configuring Scan Schedule .....	44
<i>Exclude Files &amp; Folders</i> .....	46
Configuring Exclude Files & Folders.....	46
<i>Quarantine &amp; Backup</i> .....	47
Configuring Quarantine & Backup .....	47
Emails .....	48
<i>Email Protection</i> .....	48
Configuring Email Protection .....	48
<i>Trusted Email Clients Protection</i> .....	49
Configuring Trusted Email Clients Protection .....	50
<i>Spam Protection</i> .....	50
Configuring Spam Protection .....	50
Internet & Network .....	52
<i>Firewall Protection</i> .....	53
Configuring Firewall Protection .....	53
<i>Browsing Protection</i> .....	53
Configuring Browsing Protection.....	53
<i>Malware Protection</i> .....	53
Configuring Malware Protection.....	53
<i>Phishing Protection</i> .....	54
Configuring Phishing Protection.....	54
<i>Browser Sandbox</i> .....	54
Configuring Browser Sandbox .....	54
<i>News Alert</i> .....	55
Turning News Alert off .....	56
Parental Control.....	56
Configuring Parental Control.....	57
Restrict access to particular categories of website .....	58
Restrict access to particular website.....	58
Schedule Internet access.....	59
Creating an Administrator account.....	60
Quick Heal Password Protection .....	60

---

Creating restricted user accounts .....	60
<b>External Drives &amp; Devices .....</b>	<b>61</b>
<i>Autorun Protection</i> .....	61
Configuring Autorun Protection.....	61
<i>Scan External Drives</i> .....	61
Configuring Scan External Drives .....	62
<i>Data Theft Protection</i> .....	62
Configuring Data Theft Protection.....	62
<i>Scan Windows Mobile</i> .....	63
Configuring Scan Windows Mobile .....	63
<b>Chapter 5. Quick Access Features.....</b>	<b>64</b>
Scan.....	64
<i>Performing Full System Scan</i> .....	64
<i>Performing Custom Scan</i> .....	64
<i>Performing Memory Scan</i> .....	65
<i>Performing Boot Time Scan</i> .....	66
<i>Performing Mobile Scan</i> .....	66
Quick Heal PCTuner .....	67
News.....	67
<b>Chapter 6. Quick Heal Menus .....</b>	<b>68</b>
Settings.....	68
<i>Import and Export Settings</i> .....	68
<i>Automatic Update</i> .....	69
Configuring Automatic Update .....	69
<i>Internet Settings</i> .....	70
Configuring Internet Settings .....	70
<i>Registry Restore</i> .....	71
Configuring Registry Restore.....	71
<i>Self Protection</i> .....	71
Configuring Self Protection .....	71
<i>Password Protection</i> .....	72
Safe Mode Protection .....	72
Configuring Password Protection.....	72
<i>Report Settings</i> .....	72
Configuring Report Settings.....	73
<i>Report Virus Statistics</i> .....	73
Configuring Report Virus Statistics .....	73
<i>Restore Default Settings</i> .....	73
Restoring Default Settings .....	73
Tools .....	74
<i>Hijack Restore</i> .....	74
Using Hijack Restore .....	74

---

<i>Track Cleaner</i> .....	75
Using Track Cleaner .....	75
<i>Anti-Rootkit</i> .....	76
Using Quick Heal Anti-Rootkit .....	76
Configuring Quick Heal Anti-Rootkit Settings .....	77
Scanning Results and Cleaning Rootkits .....	78
Cleaning Rootkits through Quick Heal Emergency Disk .....	79
<i>Creating Emergency Disk</i> .....	79
<i>Launch AntiMalware</i> .....	81
Launching Quick Heal AntiMalware .....	81
Using Quick Heal AntiMalware .....	81
<i>View Quarantine Files</i> .....	82
Launching Quarantine Files .....	82
<i>USB Drive Protection</i> .....	82
<i>System Explorer</i> .....	83
<i>Windows Spy</i> .....	83
Using Windows Spy .....	84
<i>Exclude File Extensions</i> .....	84
Creating Exclusion List for Virus Protection .....	84
<b>Reports</b> .....	<b>85</b>
<i>Viewing Reports</i> .....	85
<b>Help</b> .....	<b>86</b>
<b>Chapter 7. Quick Heal PCTuner</b> .....	<b>89</b>
Quick Heal PCTuner Dashboard .....	89
<i>Status</i> .....	90
Tuneup .....	91
<i>Auto Tuneup</i> .....	91
Customizing Auto Tuneup .....	91
Performing Auto Tuneup .....	92
<i>Disk Cleanup</i> .....	92
Performing Disk Cleanup .....	92
<i>Registry Cleanup</i> .....	93
Performing Registry Cleanup .....	93
<i>Traces Cleanup</i> .....	94
Performing Traces Cleanup .....	94
<i>Defragmenter</i> .....	94
Using Defragmenter .....	95
<i>Scheduler</i> .....	95
Customizing Scheduler .....	95
<i>Settings</i> .....	96
Customizing Disk Cleanup .....	96
Customizing Registry Cleanup .....	97
Customizing Traces Cleanup .....	97

---

<i>Tools</i> .....	97
Duplicate File Finder.....	98
Deleting Duplicate Files.....	98
Startup Booster.....	100
Service Optimizer.....	101
<b>Reports</b> .....	<b>102</b>
<i>Auto Tuneup Reports</i> .....	103
<i>Disk Cleanup Reports</i> .....	103
<i>Registry Cleanup Reports</i> .....	103
<i>Traces Cleanup Reports</i> .....	103
<i>Scheduler Reports</i> .....	104
<i>Secure Delete Reports</i> .....	104
<i>Duplicate File Finder Reports</i> .....	104
<i>Startup Booster Reports</i> .....	104
<i>Service Optimizer Reports</i> .....	105
<b>Restore Reports</b> .....	<b>105</b>
<i>Restore</i> .....	105
Restoring Reports.....	106
Deleting Reports.....	106
<b>Chapter 8. Using PC2Mobile Scan</b> .....	<b>107</b>
Configuring Windows Mobile Phone before Scan.....	108
Scanning Windows Mobile.....	108
Configuring Other Mobile Phone before Scan.....	109
<i>Connecting mobile phone through Bluetooth</i> .....	109
<i>Connection through USB Cable</i> .....	110
<b>Chapter 9. Updating Quick Heal AntiVirus &amp; Cleaning Viruses</b> .....	<b>111</b>
Updating Quick Heal AntiVirus from Internet.....	111
Updating Quick Heal AntiVirus with definition files.....	112
Update Guidelines for Network Environment.....	112
Cleaning Viruses.....	113
<i>Cleaning viruses encountered during scanning</i> .....	113
Scanning Options.....	113
<i>Cleaning virus encountered in memory</i> .....	114
<b>Chapter 10. Technical Support</b> .....	<b>115</b>
Support.....	115
Support Contacts.....	116
<i>Contact Quick Heal Technologies</i> .....	117
<b>Index</b> .....	<b>118</b>

## Chapter 1. Getting Started

Quick Heal AntiVirus is simple to install and easy to use. During installation, read each installation screen carefully and follow the instructions.

### Prerequisites

Remember the following guidelines before installing Quick Heal AntiVirus on your system.

- Multiple antivirus software products installed on a single system may result in system malfunction. If any other antivirus software program is installed on your system, you must remove it before proceeding with the Quick Heal AntiVirus installation.
- Close all open programs before proceeding with the Quick Heal AntiVirus installation.
- We recommend you to keep a backup of your data in case your system is infected with viruses.
- Quick Heal AntiVirus must be installed with administrative rights.

### System Requirements

To use Quick Heal AntiVirus, your system must meet the following system requirements.

However, the requirements outlined are minimum system requirements. We recommend that your system should have higher configuration to obtain best results.

- Internet connection to receive updates
- CD/DVD Drive

#### *Operating System Compatibility*

Operating Systems	Minimum Requirements
Windows 2000	<ul style="list-style-type: none"> <li>• 300 MHz Pentium (or compatible) processor</li> <li>• 512 MB of RAM</li> <li>• DVD or CD-ROM drive</li> <li>• Service Pack 4</li> <li>• Internet Explorer 6</li> </ul>



Windows 2000 Server*	<ul style="list-style-type: none"> <li>• 300 MHz Pentium (or compatible) processor</li> <li>• 512 MB of RAM</li> <li>• DVD or CD-ROM drive</li> <li>• Service Pack 4</li> <li>• Internet Explorer 6</li> </ul>
Windows XP	<ul style="list-style-type: none"> <li>• 300 MHz Pentium (or compatible) processor</li> <li>• 512 MB of RAM</li> <li>• DVD or CD-ROM drive</li> <li>• Service Pack 2 and later</li> </ul>
Windows Server 2003*	<ul style="list-style-type: none"> <li>• 300 MHz Pentium (or compatible) processor</li> <li>• 512 MB of RAM</li> <li>• DVD or CD-ROM drive</li> </ul>
Windows Vista	<ul style="list-style-type: none"> <li>• 1 GHz Pentium (or compatible) processor</li> <li>• 512 MB of RAM</li> <li>• DVD or CD-ROM drive</li> </ul>
Windows Server 2008*	<ul style="list-style-type: none"> <li>• 1 GHz Pentium (or compatible) processor</li> <li>• 512 MB of RAM</li> <li>• DVD or CD-ROM drive</li> </ul>
Windows Server 2008 R2*	<ul style="list-style-type: none"> <li>• 1 GHz Pentium (or compatible) processor</li> <li>• 512 MB of RAM</li> <li>• DVD or CD-ROM drive</li> </ul>
Windows 7	<ul style="list-style-type: none"> <li>• 1 GHz Pentium (or compatible) processor</li> <li>• For 32-bit: 512 MB of RAM; For 64-bit: 1 GB of RAM</li> <li>• DVD or CD-ROM drive</li> </ul>
Windows 8	<ul style="list-style-type: none"> <li>• 1 GHz Pentium (or compatible) processor</li> <li>• For 32-bit: 512 MB of RAM; For 64-bit: 1 GB of RAM</li> <li>• DVD or CD-ROM drive</li> </ul>
Windows 8.1	<ul style="list-style-type: none"> <li>• 1 GHz Pentium (or compatible) processor</li> <li>• For 32-bit: 512 MB of RAM; For 64-bit: 1 GB of RAM</li> <li>• DVD or CD-ROM drive</li> </ul>
Windows Server 2012*	<ul style="list-style-type: none"> <li>• 1 GHz Pentium (or compatible) processor</li> <li>• 512 MB of RAM</li> <li>• DVD or CD-ROM drive</li> </ul>
Windows Server 2012 R2*	<ul style="list-style-type: none"> <li>• 1 GHz Pentium (or compatible) processor</li> <li>• 512 MB of RAM</li> <li>• DVD or CD-ROM drive</li> </ul>

- (\*) Indicates that the operating systems are supported only on Quick Heal AntiVirus Server Edition.
- The requirements are applicable to both 32-bit and 64-bit operating systems unless specifically mentioned.
- The requirements are applicable to all flavors of the operating systems.

- Quick Heal AntiVirus Pro, Quick Heal Internet Security Essentials, Quick Heal Internet Security, and Quick Heal Total Security are not supported on Microsoft Windows Server operating systems.
- To check for the latest system requirements, visit at [www.quickheal.com](http://www.quickheal.com).

### ***Free disk space requirement***

The free disk space required for installing the Quick Heal products is as follows.

<b>Products</b>	<b>Free Disk Space</b>
Quick Heal Total Security	1.60 GB
Quick Heal Internet Security	1.50 GB
Quick Heal AntiVirus Pro	1.50 GB
Quick Heal AntiVirus Server Edition	1.50 GB
Quick Heal Internet Security Essentials	1.50 GB

### ***Clients that support email scan***

The POP3 email clients that support the email scanning feature are as follows.

- Microsoft Outlook Express 5.5 and later
- Microsoft Outlook 2000 and later
- Netscape Messenger 4 and later
- Eudora
- Mozilla Thunderbird
- IncrediMail
- Windows Mail

### ***Clients that do not support email scan***

The POP3 email clients and network protocols that do not support the email scanning feature are as follows.

- 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).

**Quick Heal Anti-Rootkit Requirements**

- This feature is not supported on 64-bit operating systems.
- It requires minimum 512 MB RAM installed on your system.

**Quick Heal Self-Protection**

- This feature is not supported on Microsoft Windows 2000 operating system.
- For Microsoft Windows XP operating system, this feature is supported if Service Pack 2 or later is installed.
- For Microsoft Windows Server 2003 operating system, this feature is supported if Service Pack 1 or later is installed.
- Process protection functionality of Self-Protection is supported on Microsoft Windows Vista Service Pack 1 and later.

**Quick Heal PC2Mobile Scan**

- This feature is available only in Quick Heal Total Security.
- This feature is not supported on Microsoft Windows 2000 operating system.
- For Windows Mobile, Microsoft Active Sync 4.0 or later must be installed.
- To check for the list of supported mobile phones, visit [www.quickheal.com/pc2mobile](http://www.quickheal.com/pc2mobile).

**Quick Heal PCTuner**

- This feature is available only in Quick Heal Total Security.
- This feature is not supported on Microsoft Windows 2000 operating system.

**Quick Heal Browser Sandbox**

- This feature is not available in Quick Heal AntiVirus Server Edition.
- This feature is not supported on Microsoft Windows 2000, Microsoft Windows XP 64-bit.

## Installing Quick Heal AntiVirus

To install Quick Heal AntiVirus, follow these steps:

1. Insert the Quick Heal AntiVirus CD in the CD or DVD drive.

*The autorun feature of the CD is enabled and it will automatically open a screen with a list of options.*

*If the CD or DVD drive does not start the CD automatically, follow these steps:*

- i. Double-click **My Computer** or the **Computer** icon on the Desktop.
  - ii. Right-click the CD-ROM drive and select **Explore**.
  - iii. Double-click **Autorun.exe**.
2. Click **Install** to initiate the installation process.

*The installation wizard performs a pre-install virus scan of the system. If a virus is found active in memory, then:*

- The installer automatically sets the boot time scanner to scan and disinfect the system on the next boot.
- After disinfection of the system, the system starts and you need to re-initiate the installation. For more details, refer to [Performing Boot Time Scan](#), in “Chapter 3: Quick Heal AntiVirus Dashboard”, p - 33.

*If no virus is found in the system memory, the installation proceeds.*

*The End-User License Agreement screen appears. Read the license agreement carefully.*

3. At the end of the license agreement, there are two options **Submit suspicious files** and **Submit statistics** which are selected by default. If you do not want to submit the suspicious files or statistics or both, then clear these options.
4. Select **I Agree** if you accept the terms and then click **Next**.

*The Install Location screen appears. The default location where Quick Heal is to be installed is displayed. The disk space required for installation is also mentioned on the screen.*

5. If the default location has insufficient space, or you want to install Quick Heal on another location, click **Browse** to change the location or click **Next** to continue.

*The installation is initiated. When installation is complete, a message appears.*

6. Click **Register Now** to initiate the activation process or click **Register Later** to perform activation later.

## Uninstalling Quick Heal AntiVirus

Removing Quick Heal may expose your system to virus threats. However, you can uninstall Quick Heal in the following way:

1. Select **Start > Programs > Quick Heal AntiVirus<sup>#</sup> > Uninstall Quick Heal AntiVirus**.

*A message **Do you want to Remove Quick Heal AntiVirus completely from your computer?** is displayed.*

2. Click **Yes** to continue with the uninstallation.

*If you have password-protected Quick Heal, an authentication screen appears.*

3. Enter your password and click **OK**.

*Quick Heal maintains a repository of Report Files, Quarantine Files, Backup Files, Black List\* and White List of email addresses\*. You may retain or delete this repository during uninstallation. However, the options **Remove Report Files**, **Remove Quarantine/Backup Files** and **Remove list of black-list & white-list email senders†** are selected by default.*

4. Click **Next** to continue with the uninstallation without saving the repository. If you want to retain the repository, clear the required options and click **Next**.

*The uninstallation process is initiated.*

*When uninstallation is complete, a message appears.*

*You may provide feedback and reasons for uninstalling Quick Heal by clicking **Write to us the reason of un-installing Quick Heal AntiVirus**. Your feedback is valuable to us and it helps us improve the product quality.*

Please note the product key for future reference. You can save your product key information by clicking **Save to file**. Restart is recommended after Quick Heal uninstallation. To restart click **Restart Now**, or click **Restart Later** to continue working on the system and restart after some time.



- **(#)** Quick Heal AntiVirus, here and hereafter, may refer to any of the Quick Heal AntiVirus Pro, Quick Heal Internet Security Essentials, Quick Heal AntiVirus Server Edition, Quick Heal Internet Security or Quick Heal Total Security products that you have installed on your computer.
- **(\*)** Indicates that the feature is configured to be used by Quick Heal AntiSpam feature.
- **(†)** Indicates that the option is displayed only for Quick Heal AntiVirus Server Edition, Quick Heal Internet Security Essentials, Quick Heal Internet Security and Quick Heal Total Security.

# Registration, Re-activation and Renewal

You should register your product immediately after installing it. Unless you register the product, it will be considered as a trial version. Also a subscriber with registered license can use all the features without any interruptions, take the updates regularly, and get technical support whenever required while unregistered users cannot.

If your product is not regularly updated, it cannot protect your system against the latest threats.

## Registration

You can register Quick Heal AntiVirus in any of the following ways.

[Registering Online](#)

[Registering Offline](#)

[Registering through SMS](#)

### Registering Online

If you are connected to the Internet you can register your product online. To register Quick Heal AntiVirus online, follow these steps:

1. Select **Start > Programs > Quick Heal AntiVirus > Activate Quick Heal AntiVirus**.
2. On the Registration Wizard, enter the 20-digit Product Key and click **Next** to continue.

*The Registration Information appears.*

3. Enter relevant information in the **Purchased From** and **Register for** text boxes, and then click **Next**.
4. Provide your **Name, Email Address, Contact Number**. Select your **Country, State, and City**.

*If your State/Province and City are not available in the list, you can type your locations in the respective boxes.*

5. Click **Next** to continue.

*A confirmation screen appears with the details you entered.*

*If any modifications are needed, click **Back** to go to the previous screen and make the required changes.*

6. Click **Next** to continue.

*Your product is activated successfully. The date when your license expires is displayed.*

7. Click **Finish** to close the Registration Wizard.

## Registering Offline

Quick Heal AntiVirus can be registered offline if your system is not connected to the Internet.

You need to visit the offline activation page on the website of Quick Heal at [www.quickheal.com/actinfo.htm](http://www.quickheal.com/actinfo.htm) and complete the registration form. After the registration is complete, a new key will be generated which you have to use to activate your product on your system that is not connected to the Internet.

You can register Quick Heal AntiVirus offline in the following way.

## Obtaining Product Key and Installation Number

Before visiting the offline activation page, ensure that you have the Product Key and the Installation Number with you. You can obtain the key and installation number in the following way.

- **Product Key:** This is printed on the User Guide and/or can be found inside the box. If the product is purchased online, the Product Key can be obtained from the email confirming the order.
- **Installation Number:** This can be obtained from the Activation Wizard in the following way:
  - i. Select **Start > Programs > Quick Heal AntiVirus > Activate Quick Heal AntiVirus**.
  - ii. On the Registration Wizard, click **Register Offline**.

*The offline activation screen appears with the offline activation URL and Installation Number.*

*You can note down the URL for offline activation and 12-digit Installation Number or click **Save to file** to save the details.*

- **A valid email address** – A <license>.key file is generated after successful completion of offline activation. This file is sent to the email address that you provided. You should ensure that you enter the correct email address.

## Generating Activation Key for offline activation

To activate your license offline, you need to generate a key in the following way:

1. Visit the offline activation page at <http://www.quickheal.com/actinfo.htm>.  
*An Off-Line Registration page appears.*
2. Under your product type, click the hyperlink **Click here to proceed to Step 1**.  
*Ensure that you have the Product Key and Installation Number with you.*
3. Provide the Product Key and Installation Number in the relevant fields and click **Submit**.
4. On the registration form, enter the relevant information and then click **Submit**.  
*All asterisk (\*) fields are mandatory to fill.*
5. A new key is generated. Save this key for future reference.  
*Moreover, this key is also sent to your email address provided by you in the registration form.*

## Activating Quick Heal AntiVirus with offline Activation Key

After the offline activation key is generated, you can proceed with activating Quick Heal AntiVirus on your system that is not connected to the Internet in the following way:

1. Select **Start > Programs > Quick Heal AntiVirus > Activate Quick Heal AntiVirus**.
2. On the Registration Wizard, click **Register Offline**.  
*The offline activation screen appears.*
3. Click **Browse** to locate the path where the <license>.key is stored and click **Next**.  
*Your license is activated successfully and the date when your license expires is displayed.*
4. Click **Finish** to close the Registration Wizard.

## Registering through SMS

Quick Heal AntiVirus may also be activated through SMS. If your system is not connected to the Internet, you can register your product through SMS Registration process.



Currently Registration through SMS facility is available to the subscribers based in India only.



Quick Heal AntiVirus can be registered through SMS Registration facility in the following way:

1. Select **Start > Programs > Quick Heal AntiVirus > Activate Quick Heal AntiVirus**.
2. On the Registration Wizard, click **SMS Registration**.  
*A screen with the conditions related to registering through SMS appears.*
3. Click **Next**.
4. Enter the 20-digit **Product Key** and click **Next**.  
*The Registration Information appears.*
5. Enter relevant information in the **Purchased From** and **Register for** text boxes, and then click **Next**.
6. Provide your **Name, Email Address, Contact Number**. Select your **Country, State, and City**.  
*If your State/Province and City are not available in the list, you can type your locations in the respective boxes.*
7. Click **Next** to continue.  
*A confirmation screen appears with the information that you entered.*  
*If any modifications are needed, click **Back** to go to the previous page and make the required changes.*
8. Click **Next** to continue.  
*A unique code along with a mobile number is displayed.*
9. Type the code and send it as an SMS to the number displayed.
10. After successful registration at the Quick Heal Registration Center, you will receive an SMS on your mobile which contains an alphanumeric activation code. Type this activation code in the text box provided and click **Next**.  
*Your product is activated successfully and the date when your license expires is displayed.*
11. Click **Finish** to close the Registration Wizard.

## Multi-users Pack Registration

To activate a multi-users pack, please take note of the following:

- When you register any Product Key in the multi-users pack, the remaining Product Keys in the pack are registered simultaneously.
- The registration information of the first Product Key activated applies to the remaining Product Keys.
- The same license validity applies to all the Product Keys in the pack.

## Re-activation

Re-activation is a facility that ensures that you use the product for the entire period till your license expires. Re-activation is very helpful in case you format your system when all software products are removed, or you want to install Quick Heal AntiVirus on another computer. In such cases, you need to re-install and re-activate Quick Heal AntiVirus on your system.

The re-activation process is similar to the activation process, with the exception that you need not enter the complete personal details again. Upon submitting the Product Key (and Installation Number in case of offline re-activation), the details are displayed. You can just verify the details and complete the process.



If you prefer to re-activate your license through SMS, you have to fill in the user information again.

## Renewal

You can renew your product license as soon as it expires by purchasing a renewal code. However, you are recommended to renew your product before your license expires so that your computer remains protected. You can buy the renewal code from the website of Quick Heal, or from the nearest distributor or reseller.

You can renew Quick Heal AntiVirus in any of the following ways.

[Renewing Online](#)

[Renewing Offline](#)

### Renewing Online

If your computer is connected to the Internet, you can renew Quick Heal AntiVirus online in the following way:

1. Select **Start > Programs > Quick Heal AntiVirus > Activate Quick Heal AntiVirus**.
2. The **Renew Now** button is displayed on the Quick Heal Dashboard. You can renew your license using this button. If your copy of Quick Heal has not expired yet, then go to the Help menu and select **About > Renew Now**.

*The Registration Wizard appears.*

3. Select the option **I want to renew with renewal code. I already have renewal code with me** and click **Next**.

*The Registration Information appears.*

4. Enter relevant information in the **Purchased From, Email Address** and **Contact Number** text boxes, and then click **Next**.

*The license information such as **Current expiry date** and **New expiry date** is displayed for your confirmation.*

5. Click **Next**.

*The license of Quick Heal AntiVirus is renewed successfully.*

6. Click **Finish** to complete the renewal process.



- In case you do not have the renewal code, select the option **I do not have renewal code with me. I want to purchase renewal code online** and click **Buy Now**.
- In case you renewed your license but its expiration date has not extended, select the option **I have already renewed my license. Please update my license from server** and click **Next**.
- If you have purchased an additional renewal code, the renewal can be performed only after 10 days of the current renewal.

## Renewing Offline

Quick Heal AntiVirus can be renewed offline if your system is not connected to the Internet.

Visit the offline renewal page on the website of Quick Heal at [http://www.quickheal.com/offline\\_renewal](http://www.quickheal.com/offline_renewal) and complete the registration form. After the offline renewal registration is complete, a new key will be generated which you have to use to renew your product on the computer that is not connected to the Internet.

You can renew Quick Heal AntiVirus offline in the following way:

### Getting the details of Quick Heal AntiVirus

Before visiting the offline renewal page, you must have the following details ready with you:

- Product Key and Installation Number – You can get the Product Key and Installation Number by filling in the renewal form in the following way :
  - i. Select **Start > Programs > Quick Heal AntiVirus > Quick Heal AntiVirus**.
  - ii. If your copy of Quick Heal has expired, a button **Renew Now** is displayed on the Quick Heal Dashboard. You can renew your license using this button. If your copy of Quick Heal has not expired yet, then go to the **Help** menu, and select **About > Renew Now**.
  - iii. Click **Renew Offline**.

*The offline renewal details screen appears.*
  - iv. You can either note down the offline renewal URL, Product Key and 12-digit Installation Number or click **Save to file** to save these details.
- A valid email address – A <license>.key file is generated upon successful completion of the offline renewal. This file is sent to the email address that you provided. You should ensure that your email address is correct.

### Generating Activation Key for offline activation

To activate your license offline, you need to generate a key in the following way:

1. Visit the offline activation page at [http://www.quickheal.com/offline\\_renewal](http://www.quickheal.com/offline_renewal).  
*An Off-Line Renewal page appears.*
2. Under your product type, click the hyperlink **Click here to proceed to Step 1**.  
*Ensure that you have the Product Key and Installation Number with you.*
3. Enter the Product Key, Installation Number, Purchased Renewal Code and Purchased From details and click **Submit**.
4. Upon verification of the provided data, the succeeding screen displays the user name, registered email address, and contact number. If your email address and contact number have changed, you can update them or else click **Submit**.

### Receiving <license>.key file

You can download the <license>.key from the Acknowledgement screen after successful completion of the offline renewal. The <license>.key file is also sent as an attachment to the email address. You can download the file and transfer it to the system on which Quick Heal is installed.

### Renewing Quick Heal AntiVirus with <license>.key file

After the <license>.key file is transferred to the system on which Quick Heal AntiVirus is installed, perform the following steps:

1. Select **Start > Programs > Quick Heal AntiVirus > Quick Heal AntiVirus**.
2. If your copy of Quick Heal has expired, a button **Renew Now** is displayed on the Quick Heal Dashboard. You can renew your license using this button. If your copy of Quick Heal has not expired yet, then go to the Help menu and select **About > Renew Now**.
3. Click **Renew Offline**.  
*The offline renewal details screen appears.*
4. Click **Browse** to locate the path where the <license>.key is stored and click **Next** to continue.  
*The copy of Quick Heal is renewed and the license validity is displayed.*
5. Click **Finish** to close the Registration Wizard.

## **Multi-users Pack Renewal**

To renew a multi-users pack, please take note of the following:

- You can either renew a single Product Key of multi-users pack by purchasing a single-user renewal code or renew the multi-users pack by purchasing a multi-users renewal code for all users.
- If you renew a multi-users pack using the multi-users renewal code, the same license validity applies to all the Product Keys in the pack.

## **Things to Do if the Product Key is Lost**

Product Key serves as your identity to Quick Heal. If you lose the Product Key, please contact Quick Heal Technical Support to get the Product Key. A nominal charge is levied for re-issuing the Product Key.

# Quick Heal AntiVirus Dashboard

The Quick Heal Main Dashboard serves as the key interface to all the features of Quick Heal AntiVirus. Quick Heal protects the entire system even with the default settings. You can open Quick Heal to check the status of Quick Heal protection, to manually scan the system, view reports and update the product.

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

- Select **Start > Programs > Quick Heal AntiVirus > Quick Heal AntiVirus**.
- On the taskbar, double-click the **Quick Heal AntiVirus** icon or right-click the **Quick Heal AntiVirus** icon and select **Open Quick Heal AntiVirus**.
- Select **Start > Run**, type **Scanner** and press the **Enter** key.

## About Quick Heal AntiVirus Dashboard

The Quick Heal AntiVirus Dashboard is the main area where you can access all the features. Dashboard is divided into various sections. The top section includes the product menus, the middle section the protection options and the bottom section the latest news from Quick Heal and scan options.

The protection options include Files & Folders, Emails, Internet & Network, Parental Control, and External Drives & Devices. With these options, you can secure your system against malware and viruses.

Options	Description
<b>Files &amp; Folders</b>	Helps you protect files and folders against malicious threats. This feature allows you to configure Scan Settings, Virus Protection, DNAScan, Block Packed Files, Automatic Rogueware Scan, Scan Schedule, Exclude Files & Folders, and Quarantine & Backup.
<b>Emails</b>	Helps you configure Email Protection, Trusted Email Clients Protection, and Spam Protection.
<b>Internet &amp; Network</b>	Helps you configure the settings for Internet & Network protection. With this option, you can configure Firewall Protection, Browsing Protection, Malware Protection, Phishing Protection <sup>#</sup> , Browser Sandbox, and News Alert.
<b>Parental Control</b> *	Helps you control the online activities of your children or other users. You can define the schedule when your children can access and use the Internet.
<b>External Drives &amp; Devices</b>	Helps you configure protection for external drives. You can configure protection such as Autorun Protection, Scanning External Drives, Data Theft Protection <sup>**</sup> and Scanning Windows Mobile <sup>†</sup> .



(#) **Phishing Protection** is not available in Quick Heal AntiVirus Pro.

(\*) **Parental Control** is available only in Quick Heal Total Security and Quick Heal Internet Security.

(\*\*) **Data Theft Protection** is available only in Quick Heal Total Security and Quick Heal AntiVirus Server Edition.

(†) **Scanning Windows Mobile** is available only in Quick Heal Total Security.

The product menus help you configure the general settings of Quick Heal and tools for preventing virus infection. You can diagnose the system and view the reports of various activities of the features and access the Help and license details.

Menus	Description
<b>Settings</b>	Helps you customize features such as Automatic Update, Internet Settings, Registry Restore, Self Protection, Password Protection, Reports Settings, Report Virus Statistics, and Restore Default Settings.
<b>Tools</b>	Helps you diagnose the system in case of virus attacks, clean application and Internet activities, restore the Internet Explorer settings modified by malwares, isolate the infected and suspicious files, remove rogware and prevent USB drives against autorun malware infection. You can also exclude files from virus protection.
<b>Reports</b>	Helps you view the activity reports of Scanner, Virus Protection, Email Protection, Scan Scheduler, Behavior Detection, Quick Update, Memory Scan, Phishing Protection*, Registry Restore, Boot Time Scanner, AntiMalware Scan, Firewall Protection, Parental Control, IDS & IPS, Browsing Protection, and PC2Mobile Scan#.
<b>Help</b>	Helps you access Help for Quick Heal AntiVirus, see details about product version, virus database, validity details, license details and seek Technical Support.



(\*) Report for **Phishing Protection** is not available in Quick Heal AntiVirus Pro.

(#) Report for **PC2Mobile Scan** is available only in Quick Heal Total Security.

The bottom section includes the following:

Miscellanies	Description
<b>News</b>	Displays the latest news from Quick Heal. You can see all the news by clicking <b>See All</b> .
<b>PCTuner*</b>	Helps you optimize and maintain system performance at peak level with features such as Disk Cleanup, Registry Cleanup, Traces Cleanup, Duplicate File Finder, Secure Delete and Registry Defragmenter.
<b>Scan</b>	Provides you with various scan options such as Full System Scan, Custom Scan, Memory Scan, Boot Time Scan, and Mobile Scan#.
<b>Support</b>	Helps you get to various support options available in the <b>Support</b> menu.

<b>Like</b>	<p>With this link, you can follow us on Facebook.</p> <p>Quick Heal's corporate Facebook page has a vibrant community of users and a host of regular posts on cyber security and virus threats and alerts. You can 'Like' the Quick Heal Facebook page through the 'Like' link available on the Dashboard.</p> <p>Alternately, if you are logged in to Facebook but are not a part of the Quick Heal community on Facebook, then you get a prompt to 'Like' the Quick Heal page.</p>
-------------	--



(\*) This feature is available only in Quick Heal Total Security.

(#) **Mobile Scan** is available only in Quick Heal Total Security.

## Right Shell Menu Options

These options provide you quick access to some of the important features of Quick Heal AntiVirus. To access any of these options, right-click the Quick Heal AntiVirus icon in the taskbar and then select an option.

Right Shell Menus	Description
<b>Open Quick Heal AntiVirus</b>	Helps you launch Quick Heal AntiVirus.
<b>Launch AntiMalware</b>	Helps you launch Quick Heal AntiMalware, an integrated tool that helps you scan registry, files, and folders at a very high speed. It helps you to thoroughly detect and clean Spywares, Adware, Rogueware, Dialers, Riskware and a number of other potential threats in your system.
<b>Enable / Disable Silent Mode</b>	Helps you enable / disable all Quick Heal prompts and notifications.
<b>Secure Browse</b>	Helps you launch your default browser in Sandbox for secure browsing.
<b>Enable / Disable Virus Protection</b>	Helps you enable / disable Quick Heal Virus Protection.
<b>Remote Support</b>	Helps you launch Remote Support.
<b>Update Now</b>	Helps you update Quick Heal AntiVirus.
<b>Scan Memory</b>	Helps you scan system memory for viruses.

## Performing Manual Scans

If Virus Protection is enabled with default setting, a manual scan is not required as the system is continuously monitored and protected. However, you can manually scan the entire computer, drives, network drives (mapped drives), USB-based drives, folders, or files as per your requirement. Although the default settings for manual scan are usually adequate, you can adjust the options by selecting **Files & Folders > Scan Settings** from the Dashboard.



## Performing Full System Scan

This option helps you initiate a complete scan of all boot records, drives, folders and files on your computer (excluding mapped network drives).

To initiate a full system scan, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, select **Scan > Full System Scan**.

*The scan starts.*

*After the scan is complete, you can view the scan report in the Reports menu.*

## Performing Custom Scan

This option helps you scan specific records, drives, folders, and files on your system. This is helpful when you want to scan only certain items and not the entire system.

To scan specific files or folders, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, select **Scan > Custom Scan**.
3. On the Custom Scan screen, a list of items is displayed in the Scan Item list if you have added any items to scan. If you have not added any item before or you want to scan some new items, click the **Add** button to add the scan items.

- On the **Browse for Folder** list, select the folders that you want to scan.

*You can add multiple folders for scanning. All the subfolders in the selected folder will also be scanned. You can exclude subfolder from scanning if required. To exclude the subfolder, select the **Exclude Subfolder** option and then click **OK**.*

4. Select an item from the Scan Item list and then click **Start Scan**.

*The scan begins.*

*After the scan is complete, you can view the scan report in the Reports menu.*

## Performing Memory Scan

To perform a memory scan, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, select **Scan > Memory Scan**.

*The scan starts.*

*After the scan is complete, you can view the scan report in the Reports menu.*

The following fields are displayed during a scan:

<b>Files scanned</b>	Displays the total number of files scanned.
<b>Archive/Packed</b>	Displays the number of archive or packed files scanned.
<b>Threats detected</b>	Displays the number of threats detected.
<b>DNAScan warnings</b>	Displays the number of files detected by DNAScan.
<b>Boot/Partition viruses</b>	Displays the number of Boot/Partition viruses.
<b>Files repaired</b>	Displays the number of malicious files that have been repaired.
<b>Files quarantined</b>	Displays the number of malicious files that have been quarantined.
<b>Files deleted</b>	Displays the number of malicious files that have been deleted.
<b>I/O errors</b>	Displays the number of I/O errors occurred during the scan.
<b>Scanning status</b>	Displays the current status of the scan being performed.

## Performing Boot Time Scan

Boot Time Scan is very useful to clean the badly infected systems. Some viruses tend to be active if the system is running and they cannot be cleaned. However, using Boot Time Scan you can clean such viruses. This scan will be performed on next boot using Windows NT Boot Shell.

To set Boot Time Scan, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, select **Scan > Boot Time Scan**.

*Boot Time Scan has the following options:*

- **Quick Scan:** Scans only system pre-defined locations that are at high risk to viruses.
- **Full System Scan:** Scans the entire system. This may be time consuming.

3. Click **Yes**.
4. To scan the system immediately, click **Yes**. To scan the system later, click **No**.

Note: In case Boot Time Scan takes time or it has been initiated by mistake, you can stop it by pressing the ESC key.

## Performing Mobile Scan

This feature helps you can scan mobiles in the following way:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, select **Scan > Mobile Scan**.
3. On the Mobile Scan screen, a list of mobile devices is displayed if you have added any mobile devices. If you have not added any mobile devices before or you want to scan some new mobile device, click the **Add Mobile** button to add new mobile devices in the list.
4. Total Security Mobile Connection Wizard appears with two options.
  - **Windows Mobile Phone:** Select this option if you want to scan Windows-based mobiles, select this option.
  - **Other Mobile Phone:** Select this option if you want to scan other mobiles, select this option.
5. After selecting the mobile model, click **Next**.
6. Select the type of connection that you want to use to connect your mobile phone to computer. The type may be such as Cable Connection (USB/Serial) and so on. Click **Next**.

*Total Security Mobile Connection Wizard checks whether the mobile model that you have selected is connected to the computer. If the mobile model is not found to be connected, no scan can be initiated.*

*If the mobile model is found connected, the Install Connector button is made available. You need to install a connector on the mobile that helps to communicate between the mobile device and the computer. If the connector is already installed on the mobile, ensure that it is running.*

7. Click **Install Connector**.

*A message about installation status appears.*

8. Click **Next**.

*A message that the mobile model is detected appears.*

9. Click **Finish**.

*The selected mobile model is added to the list.*

10. Select a mobile model from the list and click **Start Scan**.

*After the scan is complete, you can view the scan report in the Reports menu.*






The Mobile Scan feature is available only in Quick Heal Total Security.

# Quick Heal Protection Center

Quick Heal Protection Center is your main interface to vital protection settings that can affect files, folders, and emails. It helps you configure protection settings against viruses that try to infiltrate your system through Internet, external drives, and emails.

Quick Heal Protection Center is split into various sections. The top strip of the Protection Center acts as a security status indicator with color coded icons that indicates the security status. Each colored icon has an action associated with it that needs to be executed by the user.

The icons and the description of their status are as follows.

<b>Red</b>		Indicates that Quick Heal AntiVirus is not configured with optimal settings and your immediate attention is needed. The action corresponding to the message needs to be carried out immediately to keep your system protected.
<b>Green</b>		Indicates that Quick Heal AntiVirus is configured with optimal settings and your system is protected.
<b>Yellow</b>		Indicates that a feature of Quick Heal AntiVirus needs your attention at your earliest convenience, but not immediately.

Quick Heal Protection Center also provides you with various categories of protection and customizable settings. These categories are the areas or medium through which malware can gain access and infect your system.

Each of these categories displays vital features that must always be kept turned on. If you turn off any of these features, the corresponding category icons turn to red. The categories and their corresponding features displayed on Dashboard are as follows:

<b>Files &amp; Folders</b>	Scan Settings, Virus Protection, Advanced DNA Scan, Quarantine & Backup
<b>Emails</b>	Email Protection, Spam Protection
<b>Internet &amp; Network</b>	Firewall Protection, Phishing Protection, Browser Sandbox
<b>Parental Control</b>	Permit access to websites, Schedule time for Internet access
<b>External Drives &amp; Devices</b>	Autorun Protection, Scan External Drives, Data Theft Protection

## Files & Folders

This feature allows you to configure the protection settings for files and folders in your system.

The following are the protection settings.

### Scan Settings

This feature helps you define about how to initiate the scan of your system and what action should be taken when a virus is detected. However, the default settings are optimal that ensures the required protection to your system.

To configure Scan Settings, follow these steps:

1. Open **Quick Heal AntiVirus Security**.
2. On the Quick Heal AntiVirus Dashboard, click **Files & Folders**.
3. On the Files & Folders screen, click **Scan Settings**.
4. Under **Select scan mode**, select **Automatic (Recommended)** to initiate the scan automatically, or select **Advanced** for advanced level scanning.
5. Under **Select action to be performed when virus is found**, select an appropriate action.
6. If you want to take a backup of the files and folders before taking an action on them, select **Backup before taking action**.
7. To save your settings, click **Save Changes**.

#### **Select scan mode**

**Automatic (Recommended):** It is the default scan type and is recommended as it ensures the optimal protection to your system. This setting is an ideal option for novice users as well.

**Advanced:** This helps you customize the scan option. This is ideal for experienced users only. When you select the Advanced option, the Configure button is activated and you can configure the Advanced settings for scanning.

#### **Action to be performed when a virus is found**

Action	Description
Repair	<p>If a virus is found during a scan, it repairs the file or it automatically quarantines the infected file, if it cannot be repaired.</p> <p>When the scan is over, a summary window appears providing the details about all the actions taken and other scan details. If the infectious file has a Backdoor, Worm, Trojan, or Malware, then Quick Heal AntiVirus Security automatically deletes the file.</p>

<b>Delete</b>	Deletes a virus-infected file without notifying you. When the scan is over, a summary window appears providing the details about all the actions taken and other scan details. Once the files are deleted, they cannot be recovered.
<b>Skip</b>	Even if an infected file is detected, no action is taken. When the scan is over a summary report appears providing all the scan details.
<b>Backup before taking action</b>	The scanner keeps a backup of the infected files before disinfecting them. The files that are stored in the backup can be restored from Quarantine.

### **Configuring Advanced Scan Mode**

To configure Advanced Scan mode, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Files & Folders**.
3. On the Files & Folders screen, click **Scan Settings**.
4. Under **Select scan mode**, select **Advanced**.  
*The Configure button is activated.*
5. Click **Configure**.  
*The advanced scan setting details screen appears.*
6. Under **Select item to scan**, select **Scan executable files** if you want to scan only the executable files or select **Scan all files** if you want to scan all files.  
*However, the Scan executable files option is selected by default.*  
*It takes time to carry out Scan all files and the process may slow down your system.*
7. Select one of the following items for scanning:
  - **Scan archive files:** Select this option if you want to scan the archive files such as zip files and RAR files.
  - **Scan packed files:** Select this option if you want to scan packed files.
  - **Scan mailboxes:** Select **Quick scan of mailboxes** for a brief scan or else select **Through scan of mailboxes** to scan thoroughly.
8. Click **OK**.
9. Click **Save Changes** to save your settings.

## Scan archive files

This feature helps you further set the scan rules for archive files such as ZIP files, RAR files, and CHM files.

To configure the Scan archive files feature, follow these steps:

1. Select **Scan archive files**.

*The Configure button is activated.*

2. Click the **Configure** button.

*The Scan archive files details screen appears.*

3. Under **Select action to be performed when virus is found**, select any one of the following: Delete, Quarantine, and Skip.

4. In **Archive Scan Level**, select the level till you want to scan the files and folders.

*The default scan level is set to level 2. However, increasing the default scan level may affect the scan speed.*

5. Under **Select the type of archive that should be scanned**, select the archive files types.

6. Click **OK** to save your settings.

### Action to be taken when a virus is found

Action	Description
<b>Delete</b>	Deletes an archive containing virus-infected file without notifying you.
<b>Quarantine</b>	During scan if a virus is found in an archive file, then the archive will be moved to Quarantine.
<b>Skip</b>	Skips the virus and archive file without taking any action.

### Select the type of archive that should be scanned

A list of archive file types that can be scanned during the scanning process is available in this section. Few of the common archive file types are selected by default that you can customize based on your requirement.

<b>Select All</b>	Helps you select all the archive file types in the list.
<b>Deselect All</b>	Helps you clear all the archive file types in the list.

## Scan packed files

This feature helps you scan packers. Packers are the files that group many files, or compress them into a single file to reduce the file size. Moreover, these files do not need a third-party application to get unpacked. They have an inbuilt functionality for packing and unpacking.

Packers can also be used as tools to spread malware by packing a malicious file along with a set of files. When such packers are unpacked they can cause harm to your computer system. If you want to scan packers, select the **Scan packed files** option.

## Scan mailboxes

This feature allows you to scan the mailbox of Outlook Express 5.0 and later versions (inside the **DBX** files). Viruses such as KAK and JS.Flea.B, remain inside the DBX files and can reappear if patches are not applied for Outlook Express. It also scans the email attachments encoded with UUENCODE/MIME/BinHex (Base 64). **Scan mailboxes** is selected by default which activates the following two options:

<b>Quick scan of mailboxes</b>	Helps you skip all the previously scanned messages and scan only new messages. This option is selected by default.
<b>Thorough scan of mailboxes</b>	Helps you scan all the mails in the mailbox all the time. However, this may affect the speed as the size of the mailbox increases.

## Virus Protection

Viruses from various sources such as email attachments, Internet downloads, file transfer, and file execution try to infiltrate your system. This feature helps you to continuously keep monitoring for viruses. Importantly, this feature does not re-scan the files that have not changed since the previous scan. This helps in maintaining lower resource usage.

It is recommended that you always keep Virus Protection turned on to keep your system clean and secure from any potential threats. However, Virus Protection is turned on by default.

To configure Virus Protection, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Files & Folders**.
3. On the Files & Folders screen, turn **Virus Protection ON**.
4. Click **Virus Protection**.

*The Virus Protection details screen appears.*



5. Set the following as per requirement:
  - **Display alert messages** – Select this option if you want to get the alerts on various events such as when malware is detected. However, this option is selected by default.
  - **Select action to be performed when virus is detected** – Select an appropriate action when a virus is detected during the scan.
  - **Backup before taking action** – Select this option if you want to take a backup of a file before taking an action. Files that are stored in the backup can be restored from the Quarantine menu.
  - **Enable sound when threat is detected** – Select this option if you want to be alerted with sound whenever a virus is detected.
6. Click **Save Changes** to save your setting.

#### ***Action to be taken when a virus is detected***

Action	Description
Repair	If a virus is found during a scan, it repairs the file or it automatically quarantines the infected file if it cannot be repaired.
Delete	Deletes a virus-infected file without notifying you.
Deny Access	Restricts access to a virus infected file from use.

#### ***Turning off Virus Protection***

Turning **Virus Protection** off is suggested only when absolutely necessary. Moreover, you can set it off for a certain period of time so that it turns on automatically thereafter. However, when you try to turn off Virus Protection, a message is displayed.

To turn off Virus Protection,

1. Select one of the following options:
  - Turn on after 15 minutes
  - Turn on after 30 minutes
  - Turn on after 1 hour
  - Turn on after next reboot
  - Permanently disable

2. Click **OK** to save your settings.

After you turn Virus Protection off, the icon color of the Files & Folders option on Dashboard changes from green to red and a message “System is not secure” is displayed. If you have selected any of the options for turning off temporarily or after next boot then the icon color changes back from red to green after the certain

time passes or at the next boot. If you have selected to disable permanently, then the icon color remains red until you turn Virus Protection on manually.

## Advanced DNA Scan

DNAScan is an indigenous technology of Quick Heal to detect and eliminate new and unknown malicious threats in the system. Advanced DNAScan technology successfully traps suspected files with very less false alarms. Additionally, it quarantines the suspected file so that malware does not harm your system.

The quarantined suspicious files can be submitted to the Quick Heal research labs for further analysis that helps in tracking new threats and curb them on time. After the analysis, the threat is added in the known threat signature database and the solution is provided in the next updates to the users.

To configure Advanced DNAScan, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Files & Folders**.
3. On the Files & Folders screen, click **Advanced DNAScan**.

*The Advanced DNAScan details screen appears.*

4. Select either of the following as per requirement:
  - **Enable DNAScan:** Select this option to enable DNAScan.
  - **Enable Behavior detection system:** Select this option if you want to enable Behavior detection system. The running applications will be monitored for their behavior. You can also set a security alert level from the **Select Behavior detection level** list either as High, Moderate, or Low.
    - **High:** If you select this security level, Quick Heal will closely monitor the behavior of a running application and will alert you if any unusual application behavior is noticed. You may receive more alerts and sometimes even for genuine files.
    - **Moderate:** If you select this security level, Quick Heal will send alert if any suspicious activity of a running application is noticed.
    - **Low:** If you select this security level, Quick Heal will send alert only if any malicious activity of a running application is noticed.

*Note: If you have selected Moderate or Low security level, **Behavior detection system** will also block many unknown threats in the background without prompting you for any action if it finds the application behavior suspected.*

- **Do not submit files:** Select this option if you do not want to submit suspicious files to the Quick Heal research labs.
- **Submit files:** Select this option if you want to submit the suspicious files to the Quick Heal Research labs for further analysis. You can also select

**Show notification while submitting files** to get prompts for permission before submitting the files.



If the option **Show notification while submitting files** is not selected, Quick Heal will submit the suspicious files without notifying you.

Advanced DNAScan detects files by studying their characteristics and behavior.

### ***Detection by Characteristics***

Thousands of new and polymorphic threats (which change their code/file information) are born daily. Detecting them by their signature requires time. Our Advanced DNAScan technology detects such threats in real time, with zero-time lapses.

Whenever DNAScan detects a new malicious threat in your system, it quarantines the suspicious file and displays a message along with the file name. However if you find that the file is genuine, you can also restore that file from quarantine by using the option provided in the message box.

### ***Detection by Behavior***

If the option **Behavior detection system** is enabled, DNAScan continuously monitors the activities performed by an application in your system. If the application deviates from its normal behavior or carries out any suspicious activity, **Behavior detection system** suspends that application from executing further activities that may cause potential damage to the system.

Upon detecting such an application, it prompts you to take an appropriate action from the following:

- **Allow:** Take this action if you want to allow the application to run. Select this action if you are sure the applications are genuine.
- **Block:** Take this action if you want to block the application from running.

### ***Submitting Suspected Files***

You can submit the suspicious files either automatically or manually. The submission takes place automatically whenever Quick Heal AntiVirus updates itself and finds new quarantined DNAScan-suspected files. This file is sent in an encrypted file format to the Quick Heal research labs.

You can also submit the quarantined files manually if you think they should be submitted immediately. You can submit the files in the following way:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Tools**.

3. Under Cleaning & Restore Tools, click **View Quarantine Files**.  
*The Quarantine dialogue appears.*  
*A list of the files that have been quarantined is displayed.*
4. Select the files that you want to submit to the Quick Heal labs and then click **Send**.
5. Click **Close** to close the Quarantine dialogue.

## Block Suspicious Packed Files

Suspicious packed files are malicious programs that are compressed or packed and encrypted using a variety of methods. These files when unpacked can cause serious harm to the computer systems. This feature helps you identify and block such suspicious packed files.

It is recommended that you always keep this option enabled to ensure that the suspicious files are not accessed and thus prevent infection.

To configure Block Suspicious Packed Files, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Files & Folders**.
3. On the Files & Folders screen, turn **Block Suspicious Packed Files ON**.

*However, Block Suspicious Packed Files is turned on by default.*

## Automatic Rogueware Scan

This feature automatically scans and removes rogueware and fake anti-virus software. If this feature is enabled, all the files are scanned for possible rogueware present in a file.

To configure Automatic Rogueware Scan, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Files & Folders**.
3. On the Files & Folders screen, turn **Automatic Rogueware Scan ON**.

*However, Automatic Rogueware Scan is turned on by default.*

## Scan Schedule

Scanning regularly helps you keep your system free from virus and other types of infections. This feature allows you to define a schedule when to begin scanning of your system automatically. You can define multiple numbers of scan schedules to initiate scan at your convenience.

## Configuring Scan Schedule

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Files & Folders**.
3. On the Files & Folders screen, click **Scan Schedule**.  
*The Scan Schedule details screen appears.*
4. To define a new scan schedule, click **New**.
5. In **Scan Name**, type a scan name.
6. Under Scan Frequency, select the following based on your preferences:
  - Scan Frequency:
    - Daily: Select this option if you want to initiate scanning of your system daily. This option is selected by default.
    - Weekly: Select this option if you want to initiate scanning of your system on a certain day of the week. When you select the Weekly option, the Weekdays drop-down list is activated so you can select a day of the week.
  - Scan time:
    - Start at first boot: This helps you schedule the scanner to begin at the first boot of the day. If you select this option, you do not need to specify the time of the day to start the scan. Scanning takes place only during the first boot regardless what time you start the system.
    - Start at: Select this option to initiate the scanning of your system at a certain time. If you select this option, the time drop-down list is activated where you can set the time for scanning. However, this option is selected by default.

You can further define how often the scan should begin in the **Everyday** and **Repeat scan after every** options.
  - Scan priority.
    - High: Helps you set high scan priority.
    - Low: Helps you set low scan priority . However, this option is selected by default.
7. Under **Scan Settings**, you can specify scan mode, define the advanced options for scanning, action to be performed when virus is found and whether you want a backup of the files before taking any action on them. However, the default setting is adequate for scanning to keep your system clean.
8. In the **Username** text box, enter your user name and your password in the **Password** text box.

9. **Run task as soon as possible if missed:** Select this option if you want to initiate scanning when the scheduled scan is missed. This is helpful in case your system was switched off and the scan schedule passed, later when you switch on the system, the scan schedule will automatically start as soon as possible.

*This option is available only on Microsoft Windows Vista and later operating systems.*

10. Click **Next**.

*The Configure Scan Schedule screen for adding folders to be scanned appears.*

11. Click **Add Folders**.

12. In the Browse for Folder Window, select the drives and folders to be scanned. You can add multiple numbers of drives and folders as per your requirement.

If you want to exclude subfolders from being scanned, you can also select **Exclude Subfolder**. Click **OK**.

13. On the Configure Scan Schedule screen, click **Next**.

14. A summary of your scan schedule appears. Verify and click **Finish** to save and close the Scan Schedule dialogue.

15. Click **Close** to close the Scan Schedule screen.

### ***Editing a scan schedule***

This feature allows you to change the scan schedule if required. To edit a scan schedule, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Files & Folders**.
3. On the Files & Folders screen, click **Scan Schedule**.

*The Scan Schedule details screen appears.*
4. Select the scan schedule that you want to edit and then click **Edit**.
5. Make the required changes in the scan schedule and then click **Next**.
6. On the Configure Scan Schedule screen, you can add or remove the drives and folders as per your preference and then click **Next**.
7. Check the summary of the modification in the scan schedule.
8. Click **Finish** to close the Scan Schedule dialogue.
9. Click **Close** to close the Scan Schedule screen.

### ***Deleting a scan schedule***

You can remove a scan schedule whenever required. To remove a scan schedule, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Files & Folders**.
3. On the Files & Folders screen, click **Scan Schedule**.

*The Scan Schedule details screen appears.*

4. Select the scan schedule that you want to remove and then click **Remove**.

*The confirmation screen appears.*

5. Click **Yes** to remove the selected scan schedule.
6. Click **Close** to close the Scan Schedule screen.

To know about how to configure Scan Schedule, refer to [Scan Settings](#), p - 36.

### **Exclude Files & Folders**

With this feature, you can decide which files and folders should not be included during scanning for known viruses, DNAScan, and Suspicious Packed files. This helps you avoid unnecessarily scanning files which have already been scanned or that you are sure should not be scanned. You can exclude files from being scanned from the following scanning modules:

- Scanner
- Virus Protection
- Memory Scanner
- DNAScan

### **Configuring Exclude Files & Folders**

To configure Exclude Files & Folders, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Files & Folders**.
3. On the Files & Folders screen, click **Exclude Files & Folders**.

*The Exclude Files & Folders details screen appears. Here you see the list of excluded files and folders that have been added.*

4. To add a new file or folder, click **Add**.

*The New Exclude Item screen appears.*

5. In the **Item** text box, provide the path to the file or folder. You can also click the file or folder icon to select the path.

*Ensure that you provide the path to the correct file or folder, else a message appears.*

6. Under Exclude From, select the modules from which you want to exclude the selected file or folder.

*You can select either Known virus detection or any from DNAScan, Suspicious packed files scan, and Behavior Detection options.*

7. Click **OK**.
8. Click **Save Changes** to save your settings.



- If you are getting warning for a known virus in a clean file, 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 from being scanned for DNAScan.

## Quarantine & Backup

This feature allows you to safely isolate the infected or suspected files. The suspected files are quarantined in an encrypted format to prevent from being executed. This helps prevent infection.

If you want a copy of the infected file before it gets repaired, select the option **Backup before taking action** in [Scan Settings](#).

You can also set when the quarantined files should be removed from Quarantine and have a backup of the files if you need.

## Configuring Quarantine & Backup

To configure Quarantine & Backup, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Files & Folders**.
3. On the Files & Folders screen, click **Quarantine & Backup**.

*The Quarantine & Backup details screen appears.*

4. Select **Delete quarantine/backup files after** and set the number of days after which the files should be removed from Quarantine automatically. However, 30 days is set by default.
5. To see which files have been quarantined, click **View Files**. A list of the quarantine files appears. You can take any of the following actions on the quarantined files:



- **Add:** Helps you add new files from the folders and drives to be quarantined manually.
  - **Remove:** Helps you remove any of the quarantine files from the Quarantine list. To remove a file, select the file and then click the **Remove** button.
  - **Restore :** Helps you restore the quarantined files if you require them. To restore a file, select the files and then click the **Restore** button.
  - **Remove All:** Helps you remove all the quarantined files from the Quarantine list. To remove all the files, click the **Remove All** button. On the confirmation message, click **Yes** to remove all the files.
  - **Send:** Helps you send the quarantined files to our research labs. To send a file, select the file and then click the **Send** button.
6. To close the Quarantine dialog, click the **Close** button.

## Emails

With this feature, you can configure the protection rules for all incoming emails. These rules include blocking infected attachment/s (malware, spam and viruses) in the emails. You can also set an action that needs to be taken when malware is detected in the emails.

Email Security includes the following.

### Email Protection

This feature is turned on by default which provides the optimal protection to the mailbox from malicious emails. We recommend that you always keep Email Protection turned on to ensure email protection.

### Configuring Email Protection

To configure Email Protection, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Emails**.
3. On the Emails screen, turn **Email Protection** ON.  
*However, Email Protection is turned on by default.*  
*Protection against malware coming through emails is activated.*
4. To set further protection rules for emails, click **Email Protection**.
5. Select **Display alert message** if you want a message when a virus is detected in an email or attachment.



The message on viruses includes the following information: Virus Name, Sender Email Address, Email Subject, Attachment Name, and Action Taken.

- Under **Select action to be performed when virus is found**, select **Repair** to get your emails or attachment repaired when a virus is found, or select **Delete** to delete the infected emails and attachments.



If the attachment cannot be repaired then it is deleted.

- Select **Backup before taking action** if you want to have a backup of the emails before taking an action on them.
- Under **Attachment control settings**, select an option for blocking certain email types and attachments.
- Click **Save Changes** to save your settings.

### Attachment Control Settings

<b>Block attachments with multiple extensions</b>	Helps you block attachment in emails with multiple extensions. Worms commonly use multiple extensions which you can block using this feature.
<b>Block emails crafted to exploit vulnerability</b>	Helps you block emails whose sole purpose is to exploit vulnerabilities of mail clients. Emails such as MIME, IFRAME contain vulnerability.
<b>Enable attachment control</b>	<p>Helps you block email attachments with specific extensions or all extensions. If you select this option, the following options are activated:</p> <p><b>Block all attachments:</b> Helps you block all types of attachments in emails.</p> <p><b>Block user specified attachments:</b></p> <p>Helps you block email attachments with certain extensions. If you select this option, the <b>Configure</b> button is activated. For further settings, click <b>Configure</b> and set the following:</p> <ul style="list-style-type: none"> <li>Under <b>User specified extensions</b>, select the extensions that you want to retain so that the email attachments with such extensions are blocked and all the remaining extensions are deleted.</li> <li>If certain extensions are not in the list that you want to block, type such extensions in the extension text box and then click <b>Add</b> to add them in the list.</li> <li>Click <b>OK</b> to save changes.</li> </ul>

### Trusted Email Clients Protection

Since email happens to be the most widely used medium of communication, it is used as a convenient mode to deliver malware and other threats. Virus authors always look for new methods to automatically execute their viral codes using the vulnerabilities of popular email clients. Worms also use their own SMTP engine routine to spread their infection.

## Configuring Trusted Email Clients Protection

To configure Trusted Email Clients Protection, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Emails**.
3. On the Emails screen, turn **Trusted Email Clients Protection ON**.
4. To add a new email client, click **Trusted Email Clients Protection**.

*The Trusted Email Clients Protection details screen appears.*

5. Click **Browse** and select a trusted email client
6. Click **Add** to add the email client in the list.
7. Click **Save Changes** to save your settings.

## Spam Protection

Spam Protection allows you to differentiate genuine emails and filter out unwanted emails such as spam, phishing, and adult emails. We recommend you to keep Spam Protection enabled.

## Configuring Spam Protection

To configure Spam Protection, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Emails**.
3. On the Emails screen, turn **Spam Protection ON**.
4. For further settings, click **Spam Protection**.
5. Select the **Tag subject with text (Recommended)**, to tag the subject of an email as SPAM.
6. Under **Spam protection level**, set the protection level:
  - **Soft** - Select this option if you receive only a few spam emails or you want to block only the obvious spam emails. There is little possibility of genuine emails being identified as spam.
  - **Moderate (Recommended)** – Ensures optimum filtering. This is ideal if you receive a good many spam emails. However, there is possibility of some genuine emails being identified as spam. It is recommended that you select moderate filtering which is selected by default also.
  - **Strict** –Enforces strict filtering criteria but is not ideal as the chances are high that some genuine emails may also be blocked. Select strict filtering only when you receive too many spam emails or better select alternative means to stop spam emails.

7. Select **Enable email black list** to create a blacklist of email addresses. The protection rules will be applicable on the blacklisted email addresses.
8. Select **Enable email white list** to create a whitelist of email addresses. The protection rules will be applicable on the whitelisted email addresses.
9. Select **Enable AntiSpam plugin** to implement the protection rules for AntiSpam plug-in.
10. Click **Save Changes** to save your settings.

#### **Setting spam protection rule for blacklist**

Blacklist is the list of unwanted email addresses. Content from the blacklisted email addresses is filtered and will be tagged as "[SPAM] -".

This feature is useful particularly if your server uses an open mail relay, which is used to send and receive emails from unknown senders. This mailer system can be misused by spammers. With blacklist, you can filter incoming emails that you do not want or are from unknown senders both by email addresses and domains.

To add email addresses in the blacklist, follow these steps:

1. On the Spam Protection setting screen, select **Enable email black list**.

*The Customize button is activated.*

2. Click **Customize**.

3. Enter an email address in the blacklist text box and then click **Add**.

*While entering an email address, be careful that you do not enter the same email address in the blacklist that you have entered in the whitelist, or else a message appears.*

*To edit an email address, select the email address in the list and click **Edit**. To remove an email address, select an email address and click **Remove**.*

4. You can import the blacklist by clicking **Import List**.

*This is very helpful if you have exported the list of emails or saved AntiSpam data and want to use such emails.*

5. You can export the blacklist by clicking **Export List**.

*This exports all the email addresses existing in the list. This is helpful when you want to re-install Quick Heal AntiVirus later or on another system and you want to have the same email addresses to be enlisted later.*

6. Click **OK** to save your settings.

#### **Setting spam protection rule for whitelist**

Whitelist is the list of trusted email addresses. Content from the whitelisted email addresses is allowed to skip the spam protection filtering policy and is not tagged as SPAM.

This is helpful if you find that some genuine email addresses get detected as SPAM. Or if you have blacklisted a domain but want to receive emails from certain email addresses from that domain.

To add email addresses in the whitelist, follow these steps:

1. On the Spam Protection setting screen, select **Enable email white list**.

*The Customize button is activated.*

2. Click **Customize**.

3. Enter an email address in the whitelist text box and then click **Add**.

*While entering an email address, be careful that you do not enter the same email address in the whitelist that you have entered in the blacklist, or else a message appears.*

*To edit an email address, select the email address in the list and click **Edit**. To remove an email address, select an email address and click **Remove**.*

4. You can import the whitelist by clicking **Import List**.

*This is very helpful if you have exported the list of emails or saved AntiSpam data and want to use such emails.*

5. You can export the whitelist by clicking **Export List**.

*This exports all the email addresses existing in the list. This is helpful when you want to re-install Quick Heal AntiVirus later or on another system and you want to have the same email addresses to be enlisted later.*

6. Click **OK** to save your settings.

### **Adding Domains to whitelist or blacklist**

To add domain addresses in the whitelist or blacklist, follow these steps:

1. Select either of the options **Enable email white list** or **Enable email black list** and then click **Customize**.

2. Type the domain and click **Add**.

*The domain should be in the format: \*@mytest.com.*

3. Click **OK** to save the changes.

## **Internet & Network**

This feature allows you to set the protection rules to protect your system from malicious files that can sneak into your system during online activities such as banking, shopping, and surfing. You can also set Parental Control to monitor online activities of your children and other users so that you restrict them from accessing any unwanted websites.

Internet & Network includes the following.

## Firewall Protection

This feature works silently in the background and monitors network activities for any possible malicious behavior. If Firewall Protection detects any malware, it eliminates before the malware can infiltrate into the system.

### Configuring Firewall Protection

To configure Firewall Protection, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Internet & Network**.
3. On the Internet & Network screen, turn **Firewall Protection ON**.

*Firewall Protection is activated.*

## Browsing Protection

While users visit malicious websites, some files may get installed on their systems. These files may spread malware, slow down the system, or corrupt other files. These attacks can cause substantial harm to the system.

Browsing Protection ensures that malicious websites are blocked while the users access the Internet. Once the feature is enabled, any website that is accessed is scanned and blocked if found to be malicious.

### Configuring Browsing Protection

To configure Browsing Protection, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Internet & Network**.
3. On the Internet & Network screen, turn **Browsing Protection ON**.

*Browsing Protection is activated.*

## Malware Protection

This feature helps you protect your system from threats such as spyware, adware, keyloggers, and riskware while you are connected to the Internet.

### Configuring Malware Protection

To configure Malware Protection, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Internet & Network**.

3. On the Internet & Network screen, turn **Malware Protection ON**.

*Malware Protection is activated.*

## Phishing Protection

Phishing is a fraudulent attempt, usually made through email, to steal your personal information. These emails usually appear to have been sent from seemingly well-known organizations and websites such as banks, companies and services seeking your personal information such as credit card number, social security number, account number or password.

Phishing Protection prevents the users from accessing phishing and fraudulent websites. As soon as a website is accessed, it is scanned for any phishing behavior. If found so, it is blocked to prevent any phishing attempts.

## Configuring Phishing Protection

To configure Phishing Protection, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Internet & Network**.
3. On the Internet & Network screen, turn **Phishing Protection ON**.

*Phishing Protection is activated.*



**Phishing Protection** is not available in Quick Heal AntiVirus Pro.

## Browser Sandbox

This feature helps you apply a strict security policy for all untrusted and unverified websites. If you visit a website for the first time and it is not trusted, still you are secure if you have enabled Browser Sandbox. Untrusted websites may be any commercial websites, suppliers, sellers, third-parties, advertisements, and entertainments websites.

Note:

To use Browser Sandbox, you first need to disable the Secure Boot feature of your system. You can disable the Secure Boot feature from BIOS Configuration.

## Configuring Browser Sandbox

To configure Browser Sandbox, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Internet & Network**.

3. On the Internet & Network screen, turn **Browser Sandbox** ON.
4. Click **Browser Sandbox**.
5. Select the Browser security level.

*However, the default setting is optimum and ideal for the novice users.*

6. Do the following:
  - To protect your confidential data (such as bank statements, pictures, important documents etc.) while you are surfing, select **Prevent browser from accessing confidential folders**, and then select the folder that you want to protect.

The data in the confidential folder will not be accessible by the browser and other applications running under Browser Sandbox and hence your data are safe from breaching.

- To protect your data from being manipulated, select **Prevent browser from modifying the protected data**, and then select the folder that you want to protect.

The data in the protected folder will be accessible but they cannot be manipulated, or modified.

- To download content while surfing in a certain folder, select **Allow browser to store all downloads in the specified folder** and then give the path to the folder.

This helps you download content while surfing in a certain folder that you need for future use.

7. Select **Show green border around browser window** to indicate that your browser is running in Sandbox.

*However, this is not a mandatory feature for security and you may not select this feature if you prefer.*

8. To clean Sandbox cache, click the **Delete** button.

*This helps to clean temporary files.*

9. Click **Save Changes** to save your settings.



**Browser Sandbox** is not available in Quick Heal AntiVirus Server Edition.

## News Alert

With this feature, you get the latest news about cyber security, virus threats and alerts and other important information related to Quick Heal. The latest news is also available on the Quick Heal Dashboard. If you do not want to get the news alert, turn News Alert off.



## Turning News Alert off

To turn News Alert off, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Internet & Network**.
3. On the Internet & Network screen, turn **News Alert OFF**.

## Parental Control

This feature allows parents to have full control over the Internet activities of their children and other users. Parents can decide which websites their children should visit and the websites that should be blocked. They can restrict websites by categories or by individual websites. They can also schedule Internet accessibility for their children so that the children do not idle away time on the Internet.

Parental Control in Quick Heal is smart enough to categorize the websites according to their types. If you block a website category, all the websites under the category will be blocked. You can also block individual websites.

Moreover, parents can allow certain websites even from a blocked category. For example, if you have restricted the website category **Streaming Media and Downloads**, you can still allow access to **YouTube** or others. This is perfect for the parents who want to ensure that their kids visit the right kind of websites and are not exposed to the materials unsuitable for them.

### Important things to do before configuring parental control!

To get the maximum benefits from the Parental Control feature, it is recommended that you configure the following:

#### First step

Check if you are logged in as an Administrative user to the computer on which you have installed Quick Heal AntiVirus. In case you are not an administrative user, it is recommended that you [create an Administrator](#) account and configure it.

Do not share the administrative credentials with the users you are creating restricted accounts for.

#### Second step

Create separate [Standard accounts](#) (Restricted user) for your children or other users. This way, they will have only limited access to the system.

This also helps you apply different protection policies to different users. These policies could include website preferences for each restricted user and Internet access timings and schedule.

### Third step

[Password Protect](#) the Parental Control setting e to restrict unauthorized users from removing Quick Heal AntiVirus from the system or modifying the settings.

### Configuring Parental Control

To configure Parental Control, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Parental Control**.  
*The Parental Control setting details screen appears.*
3. Select **Display alert message**, if you want to receive a message when the users visit a blocked website.
4. Under **Select whom to apply the settings**, select one of the following:
  - **Apply to all users**: Select this option if you want to apply the same setting to all users. If you select this option, the **All Users** option is displayed below.
  - **Apply to specific users**: Select this option if you want to apply different settings to different users. If you select the **Apply to specific users** option, a list of all users is displayed below.
5. To restrict users from accessing the websites and configure the Internet schedule, click **All Users** or a single user that appears according to the selection made in the option **Select whom to apply the settings**.  
*The protection rules screen appears.*
6. Configure any or all of the following based on your requirement:
  - [Restrict access to particular categories of website](#): Select this option to restrict access to the websites by category.
  - [Restrict access to particular website](#): Select this option to restrict access to specific websites only.
  - [Schedule Internet access](#): Select this option to schedule Internet accessibility for your children or other users.
7. Click **OK**.
8. Click **Save Changes** to save your settings.



**Parental Control** is available only in Quick Heal Total Security and Quick Heal Internet Security.

## Restrict access to particular categories of website

This feature has a vast range of website categories that you can allow or deny access to as per your preference. Once you restrict a website category, all the websites falling under a category are blocked. This is helpful if you are sure you want to restrict or allow all the websites under a category.

Moreover, if you want to restrict most of the websites in a category but allow certain websites of that category, you can do so by putting such websites in the Exclude list.

To restrict access to the categories of websites, follow these steps:

1. On the protection rules screen that appears upon clicking a user under **Select whom to apply the settings**, select **Restrict access to particular categories of website**.

*The Categories button is activated.*

2. Click **Categories**.

*A list of website categories appears.*

3. Click the **Allow** or **Deny** button available next to each category as per your preference. Moreover, the default settings are optimal and also ideal for novice users.

*If you want to exclude a website that falls in a website category from being blocked, add such a website in the Exclude list. For example, if you have blocked the **Streaming Media and Downloads** category, but you still want to allow access to **YouTube**, you can do so by enlisting YouTube in the Exclude list.*

- On the Web Category dialogue, click **Exclude** for excluding the websites.
- Enter the URL of the website in the **List of URLs (Websites) to exclude from the blocked category** text box that you want to allow users to access and then click **Add**.

*Similarly, if you want to remove a website from the exclusion list, select the URL that you want to remove and click **Remove**. Click **Remove All** to delete all the URLs from the exclusion list.*

4. Click **OK** to save the changes.

## Restrict access to particular website

This feature helps you block specific websites. This is helpful when you are interested in restricting certain websites, or if you have a shorter list of websites.

This is also helpful when a website does not fall in a correct category or you have restricted a website category yet a certain website that you want to block is still accessible.

To restrict access to a particular website, follow these steps:

1. On the protection rules screen that appears upon clicking a user under **Select whom to apply the settings**, select **Restrict access to particular website**.

*The Block List button is activated.*

2. Click **Block List**.
3. Click the **Add** button.
4. Enter the URL of a website in the **Enter website** text box and then click **OK**. If you want to block all subdomains of the website, select **Also block subdomains**.

*For example, if you block **www.abc.com** and its subdomains, then the subdomains such as **mail.abc.com** and **news.abc.com** will also be blocked.*

5. Click **OK** to save your settings.

### **Schedule Internet access**

This feature allows you to schedule Internet accessibility for your children so that you have full control over their browsing time. You can schedule days and times when your children should access the Internet.

To configure Schedule Internet access, follow these steps:

1. On the protection rules screen that appears upon clicking a user under **Select whom to apply the settings**, select **Schedule Internet access**.

*The Configure button is activated.*

2. Click **Configure**.

*The Schedule internet access chart appears.*

3. Under **Specify when the user can access the Internet**, select one of the following:
  - **Always allow access to the Internet:** Select this option if you want no restriction for the Internet accessibility.
  - **Allow access to the Internet as per the schedule:** Select this option if you want to set restriction for accessing the Internet.

*The day and time schedule chart is activated.*

- Select the cells for the days and times during which you want to allow access to the Internet.

*The selected cells are highlighted which indicates the allowed schedule.*

4. Click **OK** to save the settings.

## Creating an Administrator account

This feature allows you to install and remove an application on the system or change any settings, including Parental Control. This ensures that only you as a parent have full control on your system.

To create an Administrators account, follow these steps:

1. Click **Start > Control Panel**.
2. Click **User Accounts**.
3. Your account type is displayed below your user name. Check if your account type is Administrator. If your account type is not Administrator, you need to change it to Administrator Account.

## Quick Heal Password Protection

You can protect the settings of Quick Heal by turning Password Protection on. Password Protection ensures that your settings are protected from modification by any unauthorized users.

To enable Password Protection, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Settings**.  
*The Password Protection feature is turned OFF by default.*
3. Turn **Password Protection ON**.  
*The password setting screen appears.*
4. Type a password in **Enter new password** and re-type the same password in **Confirm new password**.  
*If you are setting the password for the first time, **Enter old password** will be unavailable.*
5. Click **Save Changes**.

## Creating restricted user accounts

The restricted user accounts limit the users only to their account and prevent them from taking full control of the computer. This helps protect your computer by preventing a user from making changes that may affect security privileges.

To create restricted user accounts, follow these steps:

For Microsoft Windows XP operating system:

1. Click **Start > Control Panel > User Accounts**.
2. Under **User Accounts**, click **Create a New User Account**.
3. Fill in **Account Name** and click **Next**.

4. Select **Limited**.
5. Click **Create Account**.

For Microsoft Windows Vista/Windows 7 operating system:

1. Click **Start > Control Panel > User Accounts**.
2. Under **User Accounts**, click **Manage Other Account**.
3. Click **Create a New User Account**.
4. Fill in **Account Name** and select **Standard user**.
5. Click **Create Account**.

## External Drives & Devices

Whenever your system comes in contact with any external devices, your system is at risk that viruses and malwares may infiltrate through them.

This feature allows you to set protection rules for external devices such as CDs, DVDs, and USB-based drives.

### Autorun Protection

The autorun feature of USB-based devices or CDs/DVDs tends to run as soon as such devices are attached to the computer. Autorun malware may also start with the devices and spread malware that can cause substantial harm to the computer. This feature helps you protect your computer from autorun malware.

### Configuring Autorun Protection

To configure Autorun Protection, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **External Drives & Devices**.
3. On the External Drives & Devices screen, turn **Autorun Protection ON**.

*Autorun Protection is activated.*

### Scan External Drives

The USB-based drives are external devices that can transfer malware to the system. With this feature, you can scan the USB-based drives as soon as they are attached to your system.

## Configuring Scan External Drives

To configure Scan External Drives, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **External Drives & Devices**.
3. On the External Drives & Devices screen, turn **Scan External Drives ON**.  
*Scan External Drives is activated.*
4. For further settings, click **Scan External Drives**.
5. Select one of the following:
  - **Scan files on the root of the drive only:** Select this option if you want to scan the files on the root of the drive only. The files within the folders on the root drive are skipped. This scan takes little time but is less safe. However, this option is selected by default.
  - **Scan full drive:** Select this option if you want to scan all the files on the USB-based drive. This scan takes time but is safer.
6. Click **Save Changes** to save you settings.



Scan External Drives does not work if **Data Theft Protection** is turned on, and its option **Block complete access to external drives** is selected.

## Data Theft Protection

This feature allows you to block transfer of the data between the system and external devices such as USB drives and CD/DVD devices. Data Theft Protection ensures no files or data can be copied from your system to any external devices or vice versa. It ensures data security and also eliminates the possibility of transfer of any harmful files.

## Configuring Data Theft Protection

To configure Data Theft Protection, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **External Drives & Devices**.
3. On the External Drives & Devices screen, turn **Data Theft Protection ON**.  
*Data Theft Protection is activated.*
4. Click **Data Theft Protection** and do any of the following:
  - **Read only and no write access to external drives:** Allows transfer of data from the USB drives and CD/DVD devices to the system but not vice versa . However, this option is selected by default.

- **Block complete access to external drives:** Blocks transfer of data between the system and all external devices.
- **Authorize USB drive:** Select this option if you want to allow access only to the authorized USB drives and CD/DVD devices. If this option is selected, and you connect an external device to your system, you are prompted for password to access the external device. Hence access is granted only to the authorized external devices.

This option is available only if Quick Heal Password Protection in Settings is turned on.

5. Click **Save Changes** to save your settings.



**Data Theft Protection** is available only in Quick Heal Total Security and Quick Heal AntiVirus Server Edition.

## Scan Windows Mobile

This feature helps you set the rules to get notification whenever a Windows Mobile phone using a USB cable is connected for scanning purposes.

### Configuring Scan Windows Mobile

To configure Scan Windows Mobile, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **External Drives & Devices**.
3. On the External Drives & Devices screen, turn **Scan Windows Mobile ON**.

*Scan Windows Mobile is activated.*



**Scan Windows Mobile** is available only in Quick Heal Total Security.



## Chapter 5. Quick Access Features

Quick Access Features provides quick access to some of the important features such as Scan options and PCTuner. It also displays latest news about Quick Heal.

The Quick Heal Secure Browse shortcut icon on your desktop helps you launch your default browser in Sandbox for secure browsing. This helps you browse securely even if you have kept Browser Sandbox turned off.

### Scan

The Scan options available on the Quick Heal AntiVirus Dashboard provide you with various options of scanning your system based on your requirements.

You can initiate scanning of your entire system, drives, network drives, USB drives, folders or files, certain locations and drives, memory scan, and boot time scan. Although the default settings for manual scan are usually adequate, you can adjust the options for manual scan as you prefer.

#### Performing Full System Scan

This feature helps you initiate a complete scan of all boot records, drives, folders and files on your computer (excluding mapped network drives).

To initiate a full system scan, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, select **Scan > Full System Scan**.

*The scan starts.*

*On completion of the scan, you can view the scan report under **Reports**.*

#### Performing Custom Scan

This feature helps you scan specific records, drives, folders, and files on your system. This is helpful when you want to scan only certain items and not the entire system.

To scan specific files or folders, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, select **Scan > Custom Scan**.
3. On the Custom Scan screen, a list of items is displayed in the Scan Item list if you have added any items to scan. If you have not added any item before or you want to scan some new items, click **Add** to add the scan items.

- On the **Browse for Folder** list, select the folders that you want to scan.

*You can add multiple folders for scanning. All the subfolders in the selected folder will also be scanned. You can exclude subfolder from scanning if required. To exclude the subfolder, select the **Exclude Subfolder** option and then click **OK**.*

4. Select an item from the Scan Item list and then click **Start Scan**.

*The scan begins.*

*Upon completion of the scanning, you can view the scan report in the Reports menu.*

## Performing Memory Scan

To perform a memory scan, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, select **Scan > Memory Scan**.

*The scan starts.*

*On completion of the scan, you can view the scan report under **Reports**.*

The following fields are displayed during a scan:

<b>Files scanned</b>	Displays the total number of files scanned.
<b>Archive/Packed</b>	Displays the number of archive or packed files scanned.
<b>Threats detected</b>	Displays the number of threats detected.
<b>DNAScan warnings</b>	Displays the number of files detected by DNAScan.
<b>Boot/Partition viruses</b>	Displays the number of Boot/Partition viruses.
<b>Files repaired</b>	Displays the number of malicious files that have been repaired.
<b>Files quarantined</b>	Displays the number of malicious files that have been quarantined.
<b>Files deleted</b>	Displays the number of malicious files that have been deleted.
<b>I/O errors</b>	Displays the number of I/O errors occurred during the scan.
<b>Scanning status</b>	Displays the current status of the scan being performed.

## Performing Boot Time Scan

Boot Time Scan is very useful to clean the badly infected systems. Some viruses tend to be active if the system is running and they cannot be cleaned. However, using Boot Time Scan you can clean such viruses. This scan will be performed on next boot using Windows NT Boot Shell.

To set Boot Time Scan, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, select **Scan > Boot Time Scan**.

*Boot Time Scan has the following options:*

- **Quick Scan:** Scans only system pre-defined locations that are at high risk to viruses.
  - **Full System Scan:** Scans the entire system. This may be time consuming.
3. Click **Yes**.
  4. To restart the system for scanning immediately, click **Yes**. To scan the system later, click **No**.

Note: In case Boot Time Scan takes time or it has been initiated by mistake, you can stop it by pressing the **ESC** key.

## Performing Mobile Scan

With Quick Heal AntiVirus, you can scan mobiles in the following way:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, select **Scan > Mobile Scan**.
3. On the Mobile Scan screen, a list of mobile devices is displayed if you have added any mobile devices. If you have not added any mobile devices before or you want to scan some new mobile device, click **Add Mobile** to add new mobile devices in the list.
4. Total Security Mobile Connection Wizard appears with two options.
  - **Windows Mobile Phone:** If you want to scan Windows-based mobiles, select this option.
  - **Other Mobile Phone:** If you want to scan other mobiles, select this option.
5. After selecting the mobile model, click **Next**.

6. Select the type of connection that you want to use to connect your mobile phone to computer. The type may be Cable Connection (USB/Serial) and so on. Click **Next**.

*Total Security Mobile Connection Wizard checks whether the mobile model that you have selected is connected to the computer. If the mobile model is not found to be connected, no scan can be initiated.*

*If the mobile model is found connected, the Install Connector button is made available. You need to install a connector on the mobile that helps to communicate between the mobile device and the computer. If the connector is already installed on the mobile, ensure that it is running.*

7. Click **Install Connector**.

*A message about installation status appears.*

8. Click **Next**.

*A message that the mobile model is detected appears.*

9. Click **Finish**.

*The selected mobile model is added to the list.*

10. Select a mobile model from the list and click **Start Scan**.

*Upon completion of the scanning, you can view the scan report in the Reports menu.*



The Mobile Scan feature is available only in Quick Heal Total Security.

## Quick Heal PCTuner

Quick Heal PCTuner is a system cleaning tool that is integrated with Quick Heal AntiVirus. It helps in improving the performance of your computer and protects your privacy by eliminating the Internet traces. Regular usage of PCTuner ensures optimal performance of the system.

To know more about PCTuner, refer to [Quick Heal PCTuner Dashboard](#), p - 89.

## News

The News section displays the latest news about cyber security, virus threats and alerts and other important information related to Quick Heal. However, to get the latest information, you must own a licensed version of the product.

# Quick Heal Menus

These menus help you configure the general settings for taking the updates automatically, and password-protect your Quick Heal AntiVirus settings so that unauthorized persons cannot change them. It also provides settings for proxy support and for setting rules for automatic removal of reports from the list.

## Settings

This feature allows you to apply various protection rules such as receiving updates from Quick Heal as and when released, and password-protect your settings. It also allows you to set the rule when the reports generated on all the incidents should be removed. However, the default settings are optimum and can provide complete security to your system. We recommend that you change the settings only when absolutely necessary.

Settings includes the following.

### Import and Export Settings

This feature allows you to import and export the settings of Quick Heal AntiVirus features. If you need re-installation or have multiple computers and want the same settings, you can simply export the settings configured on your current computer and easily import them on the computer(s). Both the default settings and the settings made by you can be exported.

#### Importing and Exporting the Quick Heal AntiVirus Settings

To import or export the Quick Heal AntiVirus settings, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Settings**.
3. On the Settings screen, click the **Import/Export** tab.
4. On the Import/Export Settings dialog, select either of the following options.
  - **Export settings to a file:** Helps you export the current settings to a .dat file.
  - **Import settings from a file:** Helps you import the settings from a .dat file.

While you import the settings, a caution **This will overwrite all settings that you have configured.** appears. To confirm importing, click **Yes**.

5. Upon successful export or import, a message appears. Click **OK** to close the Import/Export dialogue.

Notes:

- The settings can be imported from the same product flavor and the same version only. For example, the settings of Quick Heal AntiVirus Pro 2014 can be imported to Quick Heal AntiVirus Pro 2014 only.
- The settings of the following features cannot be exported or imported:
  - Scheduled Scans
  - Browser Sandbox
  - Password Protection

## Automatic Update

This feature helps you take automatic updates of latest virus signatures. This protects your system from the latest malware. To take the updates regularly it is recommended that you always keep Automatic Update turned on. However, Automatic Update is turned off by default.

### Configuring Automatic Update

To configure Automatic Update, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Settings**.  
*On the Settings screen, turn **Automatic Update ON**.*  
*Automatic Update is activated.*
3. Click **Automatic Update**.
4. Select **Show update notification window**, if you want to get notified about the update of Quick Heal AntiVirus. However, this option is turned on by default.
5. Select the update mode from the following:
  - **Download from Internet** – Helps you download the updates to your system from the Internet.
  - **Pick update files from the specified path** – Helps you pick the updates from a local folder or a network folder.
  - **Copy update files to specified location** – Helps you save a copy of the updates to your local folder or network folder.

- Check for the latest version of Quick Heal
  - **Notify me when upgrade is available:** Select this option if you want to be notified when there is a new upgrade available.
  - **Automatically download the upgrade:** Select this option if you want a new upgrade when available get downloaded automatically on your system. Then you need to install it to upgrade your current version.

6. Click **Save Changes** to save your settings.

## Internet Settings

This feature helps you turn proxy support on, set proxy type, configure IP address, and port of the proxy for using Internet connection. If you are using a proxy server on your network, or Socks Version 4 & 5 network, you need to enter the IP address (or domain name) and port of the proxy, SOCKS V4 & SOCKS V5 server in the Internet settings. However, if you configure Internet Settings, you have to enter your user name and password credentials.

The following Quick Heal modules require these changes.

- Registration Wizard
- Quick Update
- Messenger

## Configuring Internet Settings

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Settings**.
3. On the Settings screen, click **Internet Settings**.
4. Select **Enable proxy settings**.

*The proxy type, server, port, and user credentials text boxes are activated.*

5. In **Type** list, select the proxy type from HTTP, SOCKS V4, SOCKS V5 based on your preference.
6. In the **Server** text box, enter the IP address of the proxy server or domain.
7. In the **Port** text box, enter the port number of the proxy server.

*Port number is set as 80 for HTTP and 1080 for SOCKS V4, SOCKS V5 by default.*

8. Enter your user name and password credentials.
9. Click **Save Changes** to save your settings.

## Registry Restore

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 the Control Panel settings, or File Associations, System Policies, or install new software, the changes are reflected and stored in the Registry. Malware usually targets the system Registry to restrict specific features of the operating systems or other applications. It may modify the system registry so that it behaves in a manner beneficial to malware creating problem to the system.

The Quick Heal Registry Restore feature restores the critical system registry area and other areas from the changes made by malware. It also repairs the system registry.

### Configuring Registry Restore

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Settings**.
3. On the Settings screen, click **Registry Restore**.
4. Select **Restore critical system registry areas** to restore the critical system registry during the scan. Critical System Registry areas are generally changed by malware to perform certain task automatically or to avoid detection or modification by system applications such as Disabling Task Manager, and Disabling Registry Editor.
5. Select **Repair malicious registry entries** to scan system registry for malware related entries. Malware and its remains are repaired automatically during the scan.

## Self Protection

This feature helps you protect Quick Heal AntiVirus so that its files, folders, configurations and registry entries configured against malware are not altered or tampered in any way. It also protects the processes and services of Quick Heal AntiVirus. It is recommended that you always keep Self Protection on. However this option is turned on by default.

### Configuring Self Protection

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Settings**.
3. On the Settings screen, turn **Self Protection ON**.

*However Self Protection is turned on by default.*



## Password Protection

This feature allows you to restrict unauthorized people from modifying the Quick Heal AntiVirus settings so that your security is not compromised. It is recommended that you always keep Password Protection turned on.

## Safe Mode Protection

If you run Windows in Safe Mode, your computer starts with only basic files and drivers and the security features of Quick Heal are disabled by default. In such a situation, unauthorized users may take advantage and steal data or modify the settings of the Quick Heal features.

To prevent access to your system by any unauthorized users, you can configure Safe Mode Protection. Once you configure it, you need to provide a password to work in Safe Mode.

## Configuring Password Protection

To configure Password Protection, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Settings**.
3. On the Settings screen, turn **Password Protection ON**.

*The Password Protection settings screen appears.*

4. In **Enter new password**, enter a new password if you are setting the password for the first time, and then enter the same password in **Confirm new password**.

*If you are setting the password for the first time, then **Enter old password** will not be available.*

5. Click **Save Changes**.

## Report Settings

Reports on all activities of the Quick Heal product are generated. You can use these reports to verify what all activities are going on such as whether your computer has been scanned, any malware has been detected, or any blocked website has been visited.

Such reports keep on adding up in the report list. You can set the rule when these reports should be removed automatically. The default setting for deleting reports is 30 days. You can also retain the reports if you need them.

## Configuring Report Settings

To configure Report Settings, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Settings**.
3. On the Settings screen, click **Report Settings**.

*The Report Settings screen appears.*

4. Select **Delete reports after**, and then select the number of days after which the reports should be removed automatically.

*If you clear **Delete reports after**, no reports will be removed.*

5. Click **Save Changes** to apply the settings.

## Report Virus Statistics

This feature helps you submit the virus detection statistics report generated during scans to the Quick Heal Research Center automatically.

### Configuring Report Virus Statistics

To configure Report Virus Statistics, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Settings**.
3. On the Settings screen, turn **Report Virus Statistics ON**.

*The Report Virus Statistics is activated.*

## Restore Default Settings

This feature allows you to revert the settings customized by you to the default settings. This is very helpful when you change the default settings but you are not satisfied with the protection or you feel your protection is being compromised. You can restore the system default settings.

### Restoring Default Settings

To restore default settings, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Settings**.  
*The Settings details screen appears.*
3. On the Restore Default Settings, click the **Default All** button.

*Your Quick Heal AntiVirus is reverted to the default settings.*

## Tools

This feature allows you to carry out various activities such as you can clean and restore your system to its original settings, prevent access to certain drives, and diagnose the system.

Tools includes the following.

### Hijack Restore

If you have modified the default settings of Internet Explorer or if the settings have been modified by malwares, spywares, and sometimes genuine applications, you can restore the default settings.

This feature helps you restore the settings of Internet Explorer browser, and also of critical operating system settings such as Registry Editor and Task Manager.

### Using Hijack Restore

To use Hijack Restore, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Tools**.  
*The Tools details screen appears.*
3. Under Cleaning & Restore Tools, click **Hijack Restore**.
4. On the Hijack Restore screen, select **Check All** to select all the browser settings in the list.
5. Select **Restore default host file** to restore the default host file.
6. Select **Restore important system settings** to restore important system settings.
7. To initiate restoring your settings, click **Restore Now**.

### Restore Default Host File

The default host file includes the following:

<b>IP Address</b>	Enter the IP Address of the host.
<b>Host Name</b>	Enter the host name.
<b>Add</b>	Click <b>Add</b> to add the host details in the list.
<b>Edit</b>	Select the host in the list and click <b>Edit</b> to make the changes.
<b>Delete</b>	Select the host in the list and click <b>Delete</b> to remove the host.
<b>OK</b>	Click <b>OK</b> to save your setting for the host files and exit from the Host Specification window.
<b>Close</b>	Click <b>Close</b> to exit without saving your settings from the Host Specification window.

## Restore Important System Settings

This feature includes the following.

<b>Check All</b>	Helps you restore all the system settings in the list.
<b>OK</b>	Helps you save all the modified settings and exit from the Important System Settings window.
<b>Close</b>	Helps you exit without saving the settings, from the Important System Settings window.

The buttons on the Hijack Restore screen are as follows:

<b>Restore Now</b>	Helps you initiate restoring the settings that you selected.
<b>Undo</b>	Helps you undo your settings done on the current screen. If you click the Undo button, it opens a window <b>Undo Operations</b> . The settings which have been restored to default settings will be listed. Select your settings or <b>Check All</b> to select all the settings. Click <b>OK</b> to revert to the existing settings.
<b>Close</b>	Helps you exit from the Hijack Restore window without saving your settings.

## Track Cleaner

Most of the programs store the list of recently opened files in their internal format to help you open them again for quick access. However, if a system is used by more than one user, the user's privacy may be compromised. Track Cleaner helps you remove all the tracks of such most recently used (MRU) programs and prevent privacy breach.

### Using Track Cleaner

To use Track Cleaner, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Tools**.  
*The Tools details screen appears.*
3. Under Cleaning & Restore Tools, click **Track Cleaner**.  
*The Track Cleaner screen appears. This displays a list of all the programs opened recently.*
4. Select the programs whose traces you want to remove or select **Check All** to select all the programs in the list.
5. To initiate cleaning, click **Start Cleaning**.
6. To close the Track Cleaner window, click **Close**.

## Anti-Rootkit

This feature helps you proactively detect and clean rootkits that are active in the system. This program scans objects such as running Processes, Windows Registry, and Files and Folders for any suspicious activity and detects the rootkits without any signatures. Anti-Rootkit detects most of the existing rootkits and is designed to detect the upcoming rootkits and also to provide the option to clean them.

However, it is recommended that Quick Heal Anti-Rootkit should be used by a person who has good 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.

### Using Quick Heal Anti-Rootkit

To use Anti-Rootkit, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Tools**.  
*The Tools details screen appears.*
3. Under Cleaning & Restore Tools, click **Anti-Rootkit**.  
*A message appears that recommends you to close all other applications before launching Anti-Rootkit.*
4. In the left pane on the Anti-Rootkit screen, click the **Start Scan** button.  
*Quick Heal Anti-Rootkit starts scanning your system for suspicious rootkit activity in the running Processes, Windows Registry and Files and Folders.*  
*After completion of the scan, the result is displayed in three tabs.*
5. Select the appropriate action against each threat displayed. For example, you can terminate the rootkit Process, rename the rootkit Registry entry/Files and Folders.  
*After taking the action, you should restart your system so that rootkit cleaning takes place.*

<b>Stop Scanning</b>	Helps you stop the scan while the scan is under way.
<b>Close</b>	Helps you close the Anti-Rootkit window. If you choose to close the Anti-Rootkit window while scanning is in progress, it will prompt you to stop the scan first.
<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 the Settings feature available on the Anti-Rootkit screen, you can configure what items to scan.

## Configuring Quick Heal Anti-Rootkit Settings

1. Open **Quick Heal Anti-Rootkit**.
2. On the Quick Heal Anti-Rootkit screen, click **Tools**.  
*The Tools details screen appears.*
3. Quick Heal Anti-Rootkit is configured for Auto Scan by default where it scans the required system areas.

<b>Auto Scan</b>	Auto Scan is the default scan setting for Anti-Rootkit. Under Auto Scan, the Quick Heal Anti-Rootkit scans the predefined system areas such as: <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>	Helps you customize the scan setting for Anti-Rootkit for the following: <p><b>Detect Hidden Process</b> – scans the hidden processes running in the system.</p> <p><b>Detect Hidden Registry Items</b> – scans the hidden items in Windows Registry.</p> <p><b>Detect Hidden files and folders</b> – scans the hidden files and folders in the system and executable ADS (Alternate Data Streams). You can further choose from the following options:</p> <ul style="list-style-type: none"> <li>• Scan drive on which Operating System is installed</li> <li>• Scan all fixed drives</li> <li>• ADS (Alternate Data Streams) to scan for executable ADS.</li> </ul>
<b>Report File Path</b>	Quick Heal Anti-Rootkit creates a scan report file at the location from which it is executed. However, you can specify different location.

## Overview of Alternate Data Streams – ADS

Alternate Data Streams or ADS allows the data to be stored in hidden formats 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. ADS is a security risk because streams are almost completely hidden.

Trojan or virus author can take advantage of streams to spread malware so to hide the source of viruses.

## Scanning Results and Cleaning Rootkits

1. Open **Quick Heal Anti-Rootkit**.
2. In the left pane on the Quick Heal Anti-Rootkit screen, click the **Start Scan** button.
3. Quick Heal Anti-Rootkit starts scanning your system for suspicious rootkit activity in the running Processes, Windows Registry and Files and Folders.

*After completion of the scan, the result is displayed in three different tabs.*

*Take the appropriate action. You need to restart your system so that rootkit cleaning takes place.*

### Tabs that appear on the Scan Results screen

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

## Cleaning Rootkits through Quick Heal Emergency Disk

Sometimes rootkits are not cleaned properly and they reappear even after Quick Heal Anti-Rootkit scan. In such a case you can also use Quick Heal Emergency Disk for complete cleaning. For cleaning this way, create Quick Heal Emergency Disk and boot your system through it.

To create Quick Heal Emergency Disk and clean your system through it, follow these steps:

### Step 1

To create Quick Heal Emergency Disk, follow the link [Create Emergency Disk](#), p - 79.

### Step 2

1. Open **Quick Heal Anti-Rootkit**.
2. In the left pane on the Quick Heal Anti-Rootkit screen, click the **Start Scan** button.

*Quick Heal Anti-Rootkit starts scanning your system for suspicious rootkit activity in the running Processes, Windows Registry, and Files and Folders.*

*After the scan is complete, the scan result is displayed in three different tabs.*

3. Take the appropriate action against each threat displayed. For example, you can terminate the rootkit process or rename the rootkit registry entry or files.

### Step 3

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

## Creating Emergency Disk

You can create your own emergency bootable Disk that will help you boot your Windows computer system and scan and clean all the drives including NTFS partitions. This Disk helps in cleaning badly infected system from the files infecting viruses that cannot be cleaned from inside Windows.

The Emergency Disk will be created with the latest virus signature pattern file used by Quick Heal AntiVirus on your system.



To create an Emergency Disk, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Tools**.  
*The Tools details screen appears.*
3. Under Cleaning & Restore Tools, click **Create Emergency Disk**.
4. On the Create Emergency Disk screen, click the link and download the required package for emergency tool.
5. Extract the downloaded package on your system. For example: **c:\my documents\qhemgpkg**.
6. Provide the extracted package path, and click **Next**.
7. To create Emergency Disk, select any one of the options that are displayed on the screen. For example, select either **Create Emergency USB disk** or **Create Emergency CD/DVD**.
8. Select the disk drive to be converted to an Emergency Disk and click **Next**.  
*On successful creation of an Emergency Disk, a message is displayed.*

### **Things to remember while creating an Emergency Disk**

- It is recommended that you retain a copy of the extracted package on your system.
- On Windows XP and Windows 2003 operating systems, you need to install **Imaging API version 2.0 patch**.
- While using an USB device, rewritable CD/DVD, take a backup as the device will be formatted.
- To boot the system from either USB or CD/DVD, you have to set Boot sequence in BIOS.
- Once the scan is complete, you must remove the Emergency USB disk or CD/DVD before restarting the computer, otherwise it will again boot in the boot shell.

### **Using Emergency Disk**

1. Insert **Emergency Disk** in your CD/DVD/USB drive.
2. Restart your system.
3. Emergency Disk starts scanning all the drives automatically. It will disinfect the infection, if found.
4. Restart your system.

## Launch AntiMalware

Quick Heal AntiMalware, with its improved malware scanning engine, scans registry, files and folders at a very high speed to thoroughly detect and clean spyware, adware, rogware, dialers, riskware and lots of other potential threats in your system.

## Launching Quick Heal AntiMalware

Quick Heal AntiMalware can be launched in any of the following ways:


- Select **Start > Programs > Quick Heal AntiVirus > Quick Heal AntiMalware**.
- Right-click the **Virus Protection** icon on the Windows system tray and select **Launch AntiMalware**.
- Click **Tools > Launch AntiMalware** from the Quick Heal Dashboard.

## Using Quick Heal AntiMalware

On the Quick Heal AntiMalware screen, click **Scan Now** to initiate the malware scan process. During scanning, Quick Heal AntiMalware displays the files, folders, and registry entries infected by malwares. Once the scan is complete, a list will be displayed with all the detected malwares contained in malicious files, folders, and registry entries.

You can clear specific file, folder, or registry entries from the displayed list, but ensure that all cleared items are genuine applications and not malicious ones.

In a case a malware is detected, you can take any of the following actions:

<b>Clean</b>	Helps you clean the malwares and its remains from the system. If you clear the specific file, folder or registry entry, you are prompted whether you want to exclude those items in future scan. If you want to permanently exclude those items, click <b>Yes</b> , otherwise click <b>No</b> for temporary exclusion.
<b>Skip</b>	Helps you to skip taking any action against malwares in your system.
<b>Stop Scan</b>	Helps you stop the scan.
<b>Set System Restore point before cleaning</b>	Helps you create System Restore point before the cleaning process starts in your system. This helps you revert to the cleaning done by Quick Heal AntiMalware by using Windows System Restore facility.  The feature <b>Set System Restore point before cleaning</b> is not available in Windows 2000 operating system.
<b>Details</b>	Helps you redirect to the Web site of <a href="#">Quick Heal</a> .

## View Quarantine Files

This feature helps you safely isolate the infected or suspected files. When a file is quarantined, Quick Heal AntiVirus encrypts the file and keeps it inside the Quarantine directory. Being kept in an encrypted format, these files cannot be executed and hence are safe. Quarantine also keeps a copy of the infected file before repairing. However, you can take a backup of the files also before taking an action.

## Launching Quarantine Files

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Tools**.  
*The Tools details screen appears.*
3. Under Cleaning & Restore Tools, click **View Quarantine**.  
*A list of all quarantined files is displayed.*

You can perform the following tasks on the Quarantine dialog:

<b>Add</b>	Helps you quarantine a file manually.
<b>Remove</b>	Helps you remove a quarantined file.
<b>Restore</b>	Helps you restore a quarantined file to its original location.
<b>Remove All</b>	Helps you remove all the quarantined files.
<b>Send</b>	Helps you send the quarantined file to our research labs for further analysis. Select the file that you want to submit and click <b>Send</b> .

When you send a quarantined file to the Quick Heal research labs, you are prompted to provide your email address and a reason for submitting the file. The reasons include the following:

<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 un-repairable</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.

## USB Drive Protection

Whenever any external drives are connected to your system, the autorun feature starts automatically and all programs in the drive may also start. The autorun malware may also be written in the drives so that it starts as soon as the drive is connected and spreads malware to your system. This feature helps you safeguard your USB devices from autorun malware.

To configure USB Drive Protection, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Tools**.  
*The Tools details screen appears.*
3. Under Preventive Tools, click **USB Drive Protection**.
4. In the **Select a removable drive** list, all the removable drives plugged into your system are listed. Select the drive and click the **Secure Removable Drive** button.

*The drive will be secured against autorun malwares when used in other systems.*



Quick Heal recommends that you keep the autorun feature of your USB drive turned off, however, if you may turn on the Autorun feature of the USB drive following the same process as mentioned in here.

## System Explorer

This tool provides you all the important information related to your computer such as running process, installed BHOs, toolbars installed in Internet Explorer, installed ActiveX, Hosts, LSPs, Startup Programs, Internet Explorer settings and Active network connection. This helps you diagnose the system for any new malware or riskware.

To use system explorer, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Tools**.  
*The Tools details screen appears.*
3. Under Diagnostic Tools, click **System Explorer**.

## Windows Spy

This feature helps you find more information about an application or process. Sometimes we keep getting dialog boxes or messages that are actually shown by spyware or some malware that we are unable to locate. In such a case, 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. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Tools**.  
*The Tools details screen appears.*
3. Under Diagnostic Tools, click **Windows Spy**.
4. Drag the mouse pointer on the application.  
*A window will be opened displaying the above mentioned information.*
5. If you want to terminate that application or window, click **Kill Process**.

### Exclude File Extensions

This feature helps you create an exclusion list of file types or extensions for Virus Protection. This helps Virus Protection concentrate only on those files that are prone to malicious behavior.

### Creating Exclusion List for Virus Protection

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Tools**.  
*The Tools details screen appears.*
3. Under Diagnostic Tools, click **Exclude File Extensions**.
4. Enter the file extension that needs to be excluded from the Virus Protection scan and click **Add**.
5. If the added extension is incorrect, then select the extension added in the list and click **Remove** to delete it.
6. Click **OK** to save the list.

## Reports

Quick Heal AntiVirus creates and maintains a detailed report of all important activities such as virus scan, updates details, changes in settings of the features, and so on.

The reports on the following features of Quick Heal AntiVirus can be viewed:

- Scanner
- Virus Protection
- Email Protection
- Scan Scheduler
- Behavior Detection
- Quick Update
- Memory Scan
- Phishing Protection
- Registry Restore
- Boot Time Scanner
- AntiMalware Scan
- Firewall Protection
- Parental Control
- IDS & IPS
- Browsing Protection
- PC2Mobile Scan

### Viewing Reports

To view reports and statistics of different features, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, click **Reports**.  
*A Reports list appears.*
3. In the **Reports for** list, click a feature to view its report.

*The report details list appears in the right pane. The report statistics on each feature includes Date and Time when the report was created and the reason for which the report was created.*

Button	Action
<b>Details</b>	Helps you display a detailed report of the selected record in the list.
<b>Delete All</b>	Helps you delete all the records in the list.
<b>Delete</b>	Helps you delete the selected record in the list.
<b>Close</b>	Helps you close the Reports screen.

You can view further details of a report of a feature. In the right pane, click the report to view the details. The report details screen appears that includes the following:

Button	Action
<b>Prev</b>	Helps you display the detailed report of the previous record in the list.  This button is not available if the selected record is the first record in the list.
<b>Next</b>	Helps you display the detailed report of the next record in the list. This button is not available if the selected record is the last record in the list.
<b>Print</b>	Helps you take the print of the detailed report.
<b>Save As</b>	Helps you save the detailed report in .txt format in a location of your system.
<b>Close</b>	Helps you exit from the report details screen.

For more details about Reports, refer to [Reports](#), p - 102.

## Help

This feature helps you access the Help topics whenever you want to know about how to use and configure the Quick Heal Mobile Security features, how to seek support from the Quick Heal Technical Support team, how to update the product, and see the license details of the product.

The Help feature includes the following.

- **Help:** Helps you access the in-built Help topics. On the Quick Heal AntiVirus Dashboard, select **Help > Help**, you are redirected to the Help page where you can find topics that describe the features of the product and how to use them. (Alternatively, press **F1** key, or click the **Help** button in a dialog to get to the Help page.)
- **Submit System Information:** Helps you submit information of your system to Quick Heal for analysis.

For details on how to submit System Information, refer to [System Information](#), p - 87.

- **Support:** Helps you seek support from the Customer Care of Quick Heal Technologies Pvt. Ltd. whenever you face issues regarding the product or its features. Support has the options: Web Support (Visit FAQ), Email Support, Phone Support, and Live Chat Support. You can also submit your system information and ask the Quick Heal technical executives to remotely access your system for solving an issue.

For more details on Support, refer to [Support](#), p - 115.

- **About:** The About section of Quick Heal AntiVirus includes the following information – .

Quick Heal AntiVirus Version

License details

License validity

Update Now option

The following buttons are also available in the About section:

<b>Renew Now</b>	Helps you renew your existing subscription.
<b>License Details</b>	<p>License Information and End-User License Agreement (EULA) are available under this section.</p> <p><b>Update License Details:</b> This feature is useful to synchronize your existing License information with Quick Heal Activation Server. If you want to renew your existing subscription and you do not know how to renew it or you face the problem during renewal, you can call Quick Heal Support team and provide your Product Key and Renewal Code.</p> <p>Quick Heal Support team will renew your copy. However, you need to follow these steps:</p> <ol style="list-style-type: none"> <li>1. Be connected to the 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 Print License Details to take the print of the existing subscription information.</p>
<b>Update Now</b>	Helps you update virus database of Quick Heal AntiVirus.

### **System Information**

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

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



### **Submitting System Information file**

This tool generates an INFO.QHC file at C:\ and submits it automatically to [sysinfo@quickheal.com](mailto:sysinfo@quickheal.com).



INFO.QHC file contains the critical system details and version details of Quick Heal AntiVirus installed on your system in the text and binary format. The 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 AntiVirus. The above information is used to provide better and adequate services to customers. This tool does not collect any other personally identifiable information such as passwords, nor do we share or disclose this information with anyone. We respect your privacy.

### **Generating System Information**

To generate system information, follow these steps:

1. On the Quick Heal AntiVirus Dashboard, select **Help > Submit System Information**.  
*The System Information wizard opens.*
2. Click **Next** to continue.
3. Select a reason for submitting the system information. If you are suspecting new malwares in your system, select **I suspect my system is infected by new Malwares** or if you are facing issues while using Quick Heal AntiVirus, select **I am having problem while using Quick Heal**. Provide comments in the **Comments** text box and also enter your email address.
4. Click **Finish**.
5. System Information (INFO.QHC) will be generated and sent to Quick Heal Technical Support.

## Chapter 7. Quick Heal PCTuner

Quick Heal PCTuner is a tool that is integrated with Quick Heal AntiVirus. It helps you maintain peak performance of your computer and protects your privacy by eliminating the Internet traces. Regular usage of PCTuner ensures optimal performance from the system.



**PCTuner** is available only in Quick Heal Total Security.

### Quick Heal PCTuner Dashboard

The Quick Heal PCTuner Dashboard is the default interface when you open the PCTuner application. Dashboard displays the information about the actions that have been taken and those that are pending.

To access PCTuner, follow these steps:

- Select **Start > Programs > Quick Heal AntiVirus > Quick Heal PCTuner**.

*The main window of Quick Heal PCTuner appears.*

The following features of Quick Heal PCTuner are available:

Menu	Feature
<b>Dashboard</b>	Displays the current status of the system.
<b>Tuneup</b>	Helps you clean up system clutter such as junk files, invalid registry entries, and browsing history.
<b>Tools</b>	Contains tools to securely delete files from the hard drive.
<b>Reports</b>	Provides reports for various tune-up activities performed.
<b>Restore</b>	Restores the items deleted during Tuneup.
<b>About</b>	Provides information about the software and support information.
<b>Help</b>	Includes Help topics. Alternatively, you may press <b>F1</b> to view the Help topics.

Each feature has a list of items that are as follows.



Menu	Menu Items
<b>Dashboard</b>	Status
<b>Tuneup</b>	Auto Tuneup Disk Cleanup Registry Cleanup Traces Cleanup Defragmenter Scheduler Settings
<b>Tools</b>	Duplicate File Finder Secure Delete Startup Booster Service Optimizer
<b>Reports</b>	Auto Tuneup Disk Cleanup Registry Cleanup Traces Cleanup Scheduler Secure Delete Duplicate File Finder Startup Booster Service Optimizer Restore
<b>Restore</b>	Disc/Registry Startup Booster
<b>About</b>	Information

## Status

This feature provides the current status of your system about certain tuneup activities of PCTuner with the help of a status meter. The tune-up activities include the following:

- Disk Cleanup
- Registry Cleanup
- Traces Cleanup
- Defragmenter

The pointer of status meter points to the dark green region only if you perform all the 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 Tuneup activity (Disk Cleanup, Registry Cleanup, Traces Cleanup, and Defragmenter).
<b>Last Performed</b>	The last execution date of each of the Tuneup activities. If the concerned Tuneup activity has never been executed, then the result will be <b>NEVER</b> .  The third column includes a symbol against each Tuneup activity. If the symbol is  then it means that the corresponding tuneup activity has never been performed, or it means that the corresponding tuneup activity has not been performed in the past 15 days. If the symbol in the third column is  , it means that the corresponding activity has been performed in the past 15 days.
<b>Tuneup Now button</b>	Select Advanced mode if you want to customize the scanning behavior. This is ideal for experienced users only. If you select this option, the Configure button is activated.



When you schedule Defragmenter, the message **Defragmenter has been set to run on next boot** is displayed.

## Tuneup

This feature cleans up system clutter such as invalid and unwanted junk files, invalid registry entries, traces of the Internet history, and so on. Tuneup includes the following.

### Auto Tuneup

Auto Tuneup performs **Disk Cleanup**, **Registry Cleanup**, **Traces Cleanup**, and **Defragmenter**. 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 Tuneup

Before executing, you should customize Auto Tuneup to perform as per your requirements. To customize Auto Tuneup, follow these steps:

1. Select **Tuneup > Settings**.

*The Tuneup Settings screen appears. This screen has three tabs: Disk Settings, Registry Settings, and Traces Settings. Each tab has a list of items preceded by a check box. All the items are selected in each of the tabs by default.*

2. Clear the items that need to be skipped by Auto Tuneup. For a novice user, we recommend to keep all the items selected.

*Take backup before deleting is selected by default. If this option is not selected, Auto Tuneup will delete all the items without taking the backup. We recommend that you keep it selected.*

3. Click **Apply** to save the new settings.
4. Click **Close** to exit without saving the settings.

### **Performing Auto Tuneup**

To execute Auto Tuneup, follow these steps:

1. Select **Tuneup > Auto Tuneup**.
2. Click **Settings** if you want to customize Auto Tuneup as mentioned in the previous section.
3. Click **Start** to begin Auto Tuneup.
4. Click **Stop** if you want to halt the Auto Tuneup; else click **Close** after completion of Auto Tuneup.

### **Disk Cleanup**

Disk Cleanup finds and removes invalid and unwanted junk files from the hard disk drive. These files consume hard disk space and also slow down the system considerably. Disk Cleanup deletes these files freeing up space and helps in improving system performance. The Disk Cleanup feature also deletes temporary files, Internet cache files, improper shortcut files, garbage name files, and empty folders.

### **Performing Disk Cleanup**

To execute Disk Cleanup, follow these steps:

1. Select **Tuneup > Disk Cleanup**.
2. Click **Settings** if you want to [Customize Disk Cleanup](#).
3. Click **Start**.

*A list with file locations and its junk category appears.*

4. You may click **Stop** to halt the entries being added to the list.

*Each file location will be preceded by a check box. All file locations are selected by default.*

5. Clear the locations that need to be skipped by Disk Cleanup.  
There are four other fields that 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.
6. Click **Remove Files** to remove the files.
7. Click **Close** to exit Disk Cleanup.

## Registry Cleanup

This feature removes invalid and obsolete registry entries from the system that appear due to improper un-install or non-existent fonts. Sometimes during uninstallation, the registry entries are not deleted. This results in slower performance of the system. This feature removes such invalid registry entries to boost the performance of system.

### Performing Registry Cleanup

To execute Registry Cleanup, follow these steps:

1. Select **Tuneup > Registry Cleanup**.
2. Click **Settings** if you want to [Customize Registry Cleanup](#) as mentioned in the previous section.
3. Click **Start**.  
*A list with registry entries and their path appears.*
4. You may click **Stop** to halt the entries being added to the list.  
*Each registry entry will be preceded by a check box. All registry entries are selected by default.*
5. Clear the registry entries that need to be skipped by Registry Cleanup.  
There are two other fields that 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.
6. Click **Remove Entries** to remove the files.
7. Click **Close** to exit Registry Cleanup.

## Traces Cleanup

This feature removes traces from the Internet history and MRU (Most Recently Used) list of various applications. It safely deletes history, cleans the cookies, cache, auto-complete forms and passwords. Traces such as auto complete entries and saved passwords need to be deleted to ensure that user privacy is not breached. It also erases the traces from popular application programs such as Microsoft Office applications, Adobe Acrobat Reader, Media Player, WinZip, WinRAR and traces such as Browser Cookies, and Saved Passwords.

### Performing Traces Cleanup

To execute Traces Cleanup, follow these steps:

1. Select **Tuneup > Traces Cleanup**.
2. Click **Settings** if you want to [Customize Traces Cleanup](#) as mentioned in the previous section.
3. Click **Start**.

*A list with applications containing traces appears.*

4. You may click **Stop** to halt the entries being added to the list.

*Each application containing traces will be preceded by a check box. All applications containing traces are selected by default.*

5. Clear the applications that need to be skipped by Traces Cleanup.

There are two other fields that display the following information:

- **Total Items Found:** The total number of applications containing traces found by Traces Cleanup.
- **Items Selected:** The total number of application containing traces selected for removal.

6. Click **Clean Items** to remove traces from the applications listed.
7. Click **Close** to exit Traces Cleanup.

## Defragmenter

This 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 that slow down system performance. Defragmenter reduces the number of fragments and clubs all the fragments into one contiguous chunk to improve system performance.

## Using Defragmenter

To defragment page files and registry hives, follow these steps:

1. Select **Tuneup > Defragmenter**.

*Two options for defragment appear: **Enable defragmentation** and **Cancel defragmentation**. **Cancel defragmentation** is selected by default.*

2. 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.
3. **Defragment system paging file (Virtual Memory)** and **Defragment Windows Registry** are not selected by default. You can select any of these two or both for the Defragmenter to perform. We recommend that you keep these options selected.
4. Click the **Apply** button to save these settings, or else click **Close** to exit without saving.

## Scheduler

This feature helps you schedule the Tuneup activity periodically as per your requirements. You can configure the Tuneup schedule to perform Disc Cleanup, Registry Cleanup, Traces Cleanup, and Defragmenter. You can create a task and schedule it. The task is performed in the background at the time you specify when you created the task. You can see the details of the tasks performed in the Scheduler Reports.

### Customizing Scheduler

You can customize Scheduler to perform at your convenient time. However, Defragmenter can be scheduled only at next boot. To customize Scheduler, follow these steps:

1. Select **Tuneup > Scheduler**.

*A list of tasks is displayed along with details such as Task Name, Frequency, Activity, Backup, and Delete oldest backup.*

There are three options that you can select while you schedule tuneup activity:

- i. **New** – to configure any new task
  - ii. **Edit** – to edit any existing task
  - iii. **Remove** – to remove the already scheduled task
2. To schedule a new tuneup activity, click **New**.  
*The Configure Tuneup Schedule screen appears.*



3. Enter **Task Name**, **Frequency**, and **Start At** details.  
*Each Tuneup activity in the screen is preceded by a check box. All items are selected in the list by default.*
4. Clear the items that need to be skipped by Scheduler feature.
5. **Take backup before cleaning** is selected by default. If this option is not selected, cleaning will be done without taking the backup. We recommend that you keep it selected. **Delete oldest backup if maximum backup limit exceeds** will delete the oldest backup when the limit of backup is surpassed.
6. Enter **User Name** and **Password**.
7. Click **Apply** to save the new settings or else click **Close** to exit without saving the settings.



In case you keep Delete oldest backup if maximum backup limit exceeds not selected, Scheduler will not perform when the backup limit is surpassed.

## Settings

This feature helps you customize Disk Settings, Registry Settings, and Traces Settings as per your requirements.

### Customizing Disk Cleanup

You can customize Disk Cleanup to perform as per your requirements before you execute it. To customize Disk Cleanup, follow these steps:

1. Select **Tuneup > Settings**.  
*The Tuneup Settings screen appears.*
2. Click **Disk Settings**.  
*Each item in the list is preceded by a check box. All items are selected in the list by default.*
3. Clear the items that need to be skipped by Disk Cleanup feature.
4. **Take backup before deleting the items** is selected by default. If this option is not selected, Disk Cleanup will delete all the items without taking the backup. We recommend that you keep it selected.
5. Click **Apply** to save the new settings or else click **Close** to exit without saving the settings.

## Customizing Registry Cleanup

You can customize Registry Cleanup to perform as per your requirements before you execute it. To customize Registry Cleanup, follow these steps:

1. Select **Tuneup >Settings**.

*The Tuneup Settings screen appears.*

2. Click **Registry Settings**.

*Each item in the list is preceded by a check box. All items are selected in the list by default.*

3. Clear the items that need to be skipped by Registry Cleanup feature.
4. **Take backup before deleting the items** is selected by default. If this option is not selected, Registry Cleanup will delete all the items without taking the backup. We recommend that you keep it selected.
5. Click **Apply** to save the new settings or else click **Close** to exit without saving the settings.

## Customizing Traces Cleanup

You can customize Traces Cleanup to perform as per your requirements before you execute it. To customize Traces Cleanup, follow these steps:

1. Select **Tuneup > Settings**.

*The Tuneup Settings screen appears.*

2. Click **Traces Settings**.

*Each item in the list is preceded by a check box. All items are selected in the list by default.*

3. Clear the items that need to be skipped by Traces Cleanup feature.
4. **Take backup before deleting the items** is selected. If this option is not selected, Registry Cleanup will delete all the items without taking the backup. We recommend that you keep it selected.
5. Click **Apply** to save the new settings or else click **Close** to exit without saving the settings.

## Tools

This feature helps you delete duplicate files from the system. It offers secure deletion where files are deleted permanently and will not be recovered even if recovery software is used. The Tools menu includes the following.

## Duplicate File Finder

This feature removes duplicate files of various pre-defined file categories. It searches for duplicate files on user-specific locations. 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 your preference. 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
Image / Photo Files	.pcx, .tiff, .wpg, .bmp, .gif, .jpg, .jpeg, .wmp, .png, .tif
Creative Artwork Files	.ai, .eps, .pcx, .psd, .tiff, .wpg, .bmp, .gif, .jpg, .jpeg, .wmp, .png, .cdr, .pdf, .tif
Movie Files	.avi, .rm, .vob, .mov, .qt, .mpeg, .mpg, .mpe, .mpa, .dat
Sound Files	.wmv, .wma, .mp4, .mp3
Text Files	.txt, .asci, .xml
Document Files	.pdf, .doc, .rtf, .wri, .sam, .dox, .xls, .ppt, .docx, .xlsx, .pptx, .wk3, .wk4, .vsd, .vsdx, .wg, .123, .wpd
Email Files	.eml

## Deleting Duplicate Files

To delete duplicate files, follow these steps:

1. Select **Tools > Duplicate File Finder**.
2. To modify Duplicate File Finder settings, click **Options**.  
*The Quick Heal Duplicate File Finder Options window appears.*
3. In the **Please select a duplicate category type** list; clear the categories that need to be skipped by the Duplicate File Finder.  
*In the Exclude folder(s) list, you can add exclusion lists for Duplicate File Finder to skip.*
4. Click the **Add Folder** button to add the locations for exclusions. Select a location and click **Clear** if the added location is incorrect. Click **Clear All** to remove all exclusion locations added.  
*The Use Secure Delete option is activated and One Pass Random – Quick Data Destruction deletion method is selected by default. You can select any deletion method. See Deletion Methods to know about different deletion methods.*
5. Click the **Apply** button to save the modification of settings or else click the **Close** button to exit without saving any modified settings.
6. Click **Add Path** to add the path for Duplicate File Finder to search for duplicate files.

*The Browse for folder window appears.*

7. Browse for the required folder. Select **Exclude sub-folder** if you want to exclude the sub-folders within the folder in the scan. **Exclude sub-folder** option is not selected by default.
8. Click **OK** after selecting the required path. If the added path is incorrect, select that path and click **Clear** to delete the path. Click **Clear All** to delete all the added paths from the list.
9. Click **Start Search**.

A list of the file locations with duplicate file locations is displayed. The information of the scan is 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.

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

### ***Secure Delete***

This feature is used for deleting unwanted files or folders completely from the system. In case you want to delete any confidential data, Secure Delete helps you delete the data making it absolutely impossible to recover by any means. Data deleted using the Delete function of Windows can be recovered using a Recovery Software 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 a Recovery Software is used.

### ***Deletion Methods***

The following are the three file deletion methods available in Quick Heal PCTuner.

<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 option 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 method 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.

### **Using Secure Delete**

To delete files or folders using Secure Delete, follow these steps:

1. Select **Tools > Secure Delete**.
2. Click the **Options** button.  
*The Select Secure Delete Method window appears.*
3. Select the deletion method and click the **Accept** button. Select **Enable Right Click Secure Delete (Context Menu)** to facilitate deleting any data by just right-clicking Secure Delete.
4. Click the **Add File** button to locate the file you want to delete.
5. Click the **Add Folder** button to locate the folder and its sub-folders you want to delete.
6. If the selection for file deletion is incorrect, select the file and click **Clear**. Click **Clear All** to delete all the selections.
7. Click **Continue**.
8. A window appears with the message that the deletion is unrecoverable. It also helps 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.  
*The selected files are deleted and a Deletion Summary screen appears.*
9. Click the **View Report** button to view the report of the deletion process or else click **Close** to exit from Tools Menu.

### **Startup Booster**

This tool removes unwanted startup programs from the system. It removes all the unnecessary applications from the Registry Run and Startup, and enhances the startup speed of the system.

### ***Using Startup Booster***

To use Startup Booster, follow these steps:

1. Select **Tools > Startup Booster**.
2. Click **Start Search**.

*The applications that automatically load themselves during startup are displayed in a list. Each application is preceded by a check box. No applications are selected by default.*

3. Select the applications that need to be removed from loading every time your system starts.
4. Click **Remove** to remove the application from the list or else click **Close** to exit.

### **Service Optimizer**

Your computer may have many unwanted services that run at startup, consuming CPU and memory that can potentially slow down your system performance. Service Optimizer analyzes your system and suggests services that can be safely disabled to run at startup based on your answers to the related services.

The following are the services available for Service Optimizer in Quick Heal PCTuner.

- Network related Services
- System related Services
- Performance related Services
- Security related Services

### ***Using Service Optimizer***

To use Service Optimizer, follow these steps:

1. Select **Tools > Service Optimizer**.

*The services are categorized in four sections represented by four Tabs: **Network, System, Performance, and Security**.*

2. Select the service and select the relevant answer to the questions in each section.

*Every time you open Service Optimizer, the Apply button appears dimmed. However, on changing any of the answers, like if you select either **YES** or **NO**, the Apply button is activated.*

3. Click the **Apply** button to optimize the service or else click **Close** to exit without saving.

4. You get a **Service Optimization Summary** if you have optimized any service. Click **View Report** to view the detailed report or else click **Close** to exit.



- If the answers related to the services do not require any change, a message appears.
- If you click the Default button, all the optimized services are reverted to their original status.

## Reports

This menu contains reports for various activities performed by Quick Heal PCTuner. It includes several menu items. Each menu item corresponds to the report of a particular activity.

The menu items in the Reports menu are as follows.

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

Button	Action
Details	Helps you display a detailed report of the selected record in the list.
Delete All	Helps you delete all the reports in the list.
Delete	Helps you delete the selected record in the list.
Close	Helps you exit from the Reports menu.

If you click the Details button in any menu item, a window titled Report opens. This includes five more buttons whose actions are common to all the menu items that are as follows:

Button	Action
Prev	Helps you display the detailed report of the previous record in the list.
Next	Helps you display the detailed report of the next record in the list.
Print	Helps you take out the print of the detailed report.

Save As	Helps you save the detailed report in text format on your system.
Close	Helps you exit from the Report window.

## Auto Tuneup Reports

This feature includes a list of records with a detailed report on the **Auto Tuneup** feature performed on the system. To view Auto Tuneup Reports, follow these steps:

1. Select **Reports > Auto Tuneup**.
2. Select the required record in the list.
3. Click the **Details** button.

*The Report window appears that includes the detailed report for the selected record.*

## Disk Cleanup Reports

This feature includes a list of records with a detailed report on the **Disk Cleanup** feature performed on the system. To view Disk Cleanup Reports, follow these steps:

1. Select **Reports > Disk Cleanup**.
2. Select the required record in the list.
3. Click the **Details** button.

*The Report window appears that includes the detailed report for the selected record.*

## Registry Cleanup Reports

This feature includes a list of records with a detailed report on the **Registry Cleanup** feature performed on the system. To view Registry Cleanup Reports, follow these steps:

1. Select **Reports > Registry Cleanup**.
2. Select the required record in the list.
3. Click the **Details** button.

*The Report window appears that includes the detailed report for the selected record.*

## Traces Cleanup Reports

This feature includes a list of records with a detailed report on the **Traces Cleanup** feature performed on the system. To view Traces Cleanup Reports, follow these steps:

1. Select **Reports > Traces Cleanup**.
2. Select the required record in the list.



3. Click the **Details** button.

*The Report window appears that includes the detailed report for the selected record.*

## Scheduler Reports

This feature includes a list of records with a detailed report on all the **Scheduled tasks** performed on the system. To view Scheduler Reports, follow these steps:

1. Select **Reports > Scheduler**.
2. Select the required record in the list.
3. Click the **Details** button.

*The Report window appears that includes the detailed report for the selected record.*

## Secure Delete Reports

This feature includes a list of records with a detailed report on the **Secure Delete** feature performed on the system. To view Secure Delete Reports, follow these steps:

1. Select **Reports > Secure Delete**.
2. Select the required record in the list.
3. Click the **Details** button.

*The Report window appears that includes the detailed report for the selected record.*

## Duplicate File Finder Reports

This feature includes a list of records with a detailed report on the **Duplicate File Finder** feature performed on the system. To view Duplicate File Finder Reports, follow these steps:

1. Select **Reports > Duplicate File Finder**.
2. Select the required record in the list.
3. Click the **Details** button.

*The Report window appears that includes the detailed report for the selected record.*

## Startup Booster Reports

This feature includes a list of records with a detailed report on the **Startup Booster** feature performed on the system. To view Startup Booster Reports, follow these steps:

1. Select **Reports > Startup Booster**.
2. Select the required record in the list.
3. Click the **Details** button.

*The Report window appears that includes the detailed report for the selected record.*

## Service Optimizer Reports

This feature includes a list of records with a detailed report on the **Service Optimizer** feature performed on the system. To view Service Optimizer Reports, follow these steps:

1. Select **Reports > Service Optimizer**.
2. Select the required record in the list.
3. Click the **Details** button.

*The Report window appears that includes the detailed report for the selected record.*

## Restore Reports

This feature includes a list of records (with a detailed report on the **Restore** feature performed on the system. To view Restore Reports, follow these steps:

1. Select **Reports > Restore**.
2. Select the required record in the list.
3. Click the **Details** button.

*The Report window appears that includes the detailed report for the selected record.*

## Restore

This feature restores the items to its original locations that were deleted by any of the Disk Cleanup, Registry Cleanup, and Startup Booster features. However, it does not restore the items deleted by Traces Cleanup.



If **Delete items without taking backup** is not selected during Disk Cleanup or Registry Cleanup, backup will not be taken. In case of Auto Tuneup, **Take backup before deleting the Files** should be selected to take the backup and restore the files when needed.

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

### Restoring Reports

To restore, follow these steps:

1. Select the required restore point.
2. Click the **Restore** button.
3. A message box appears with the following prompt: **Are you sure you want to restore the backup?** Click **Yes** if you want to restore the backup or else click **No** if you do not want to restore the backup.
4. If you have clicked **Yes** in the previous step, the backup is restored and a message **The selected backup was restored successfully** appears. Click **OK** to complete the restore process.

### Deleting Reports

To delete any of the restore points in the list, follow these steps:

1. Select the required restore point.
2. Click the **Delete** button.
3. A message appears with the following prompt: **Are you sure you want to delete it?** Click **OK** if you want to delete the restore point or else click **Cancel** to exit without deleting.

# Using PC2Mobile Scan

This feature is available in Quick Heal AntiVirus. This helps you scan mobile devices for viruses, spywares, and malwares. To scan your mobile device, you need to connect it to your computer using any of the following methods:

- USB Cable
- Bluetooth



- **PC2Mobile Scan** is available only in Quick Heal Total Security.
- We regularly keep on adding support for new mobile device models. For latest list of supported mobile devices, please check at [www.quickheal.com/pc2mobile](http://www.quickheal.com/pc2mobile).

### ***Important Requirements for PC2Mobile Scan***

- This feature is only supported on Microsoft Windows XP, Windows Vista, and Windows 7 operating systems.
- For Windows Mobile based devices, you should have Microsoft Active Sync 4.5 or later installed on your computer.
- For Nokia Phones, Nokia PC Suite software is recommended to be installed on your computer. For all other mobile phones, it is recommended to have relevant vendor software drivers installed on your system.
- For Bluetooth connection, your system 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 computer some of the phone models need to have Quick Heal Connector installed on the mobile device. Quick Heal Mobile connection wizard helps you install Quick Heal Connector in your mobile device.

## Configuring Windows Mobile Phone before Scan

To configure your Windows Mobile Phone, follow these steps:

1. Connect your Window SmartPhone to the computer or Laptop through USB Cable.

*In case of Windows XP, ensure that **Microsoft Active Sync 4.5** or later is installed and running. For Windows Vista and Windows 7, **Windows Mobile Device Center** is installed and running.*

2. Start **Quick Heal AntiVirus**.
3. On the Quick Heal AntiVirus Dashboard, select **Scan > Mobile Scan**.
4. On the Mobile Scan Wizard, click **Add Mobile**.
5. Select **Windows Mobile Phone** and click **Next**.

*The Mobile Connection Wizard will search for Windows Mobile attached to your computer.*

6. Upon successful detection of Windows Mobile, click **Finish** to complete the mobile configuration.

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

## Scanning Windows Mobile

To scan a Windows Mobile, follow these steps:

1. Start **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, select **Scan > Mobile Scan**.
3. Select the mobile phone from the list.
4. Click **Start Scan** to start scanning.

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

When you connect your Windows Mobile Phone to the computer using USB cable, Quick Heal AntiVirus PC2Mobile automatically detects and prompt you for Scan.

## Configuring Other Mobile Phone before Scan

Other Mobile Phones can be configured to your system in the following way.

### Connecting mobile phone through Bluetooth

To configure your mobile phone through Bluetooth, follow these steps:

1. Connect your mobile phone to the computer or Laptop through Bluetooth.
2. Start **Quick Heal AntiVirus**.
3. On the Quick Heal AntiVirus Dashboard, select **Scan > Mobile Scan**.
4. In the Mobile Scan Wizard, click **Add Mobile**.
5. Select **Other Mobile Phone**.
6. Select your mobile phone from the mobile phone list and click **Next**.

*The Mobile Connection Wizard searches your mobile phone and displays available Bluetooth connections to your computer.*

7. Select your mobile phone from the list of Bluetooth connection and click **Next**.
8. If your mobile phone requires Quick Heal Connector to be installed on your Mobile, you are prompted to Install Connector on your mobile phone. Follow these steps to install Quick Heal Connector in your mobile phone.

- i. Click **Install Connector**.

*The Mobile Connection wizard will send **Quick Heal Connector** installer to your mobile phone.*

*You will receive a message on your mobile phone. Follow the message to install Quick Heal Connector on your mobile phone.*

- ii. After installation **Start Quick Heal Connector** from mobile.
  - iii. Click **Next**.
9. Click **Finish** to complete the configuration.

*Once Bluetooth Mobile is successfully configured, it is added in Quick Heal AntiVirus Mobile List.*

### Scanning mobile phones through Bluetooth

To scan other mobile phones through Bluetooth, follow these steps:

1. Connect your mobile phone to the computer or Laptop through Bluetooth.
2. Start **Quick Heal AntiVirus**.
3. On the Quick Heal AntiVirus Dashboard, select **Scan > Mobile Scan**.
4. Select the mobile phone from the list.
5. Click **Start Scan** to start scanning.

### Connection through USB Cable

To configure your mobile phone through cable, follow these steps:

1. Connect your mobile phone to the computer or Laptop through cable.
2. Start **Quick Heal AntiVirus**.
3. On the Quick Heal AntiVirus Dashboard, select **Scan > Mobile Scan**.
4. Click **Add Mobile**.
5. Select **Other Mobile Phone**.
6. Select you mobile phone from the mobile phone list and click **Next**.
7. Click **Finish** to complete mobile phone configuration.

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

### Scanning Other Mobile Phone through Cable

To scan Other Mobile Phone through cable, follow these steps:

1. Connect your mobile phone to the computer or Laptop through cable.
2. Start **Quick Heal AntiVirus**.
3. On the Quick Heal AntiVirus Dashboard, select **Scan > Mobile Scan**.
4. Select the mobile phone from the list.
5. Click **Start Scan** to start scanning.

# Updating Quick Heal AntiVirus & Cleaning Viruses

Updates for Quick Heal AntiVirus are released regularly on the website of Quick Heal. The updates include information pertaining to the detection and removal of newly discovered viruses. To prevent your system from new viruses, Quick Heal AntiVirus must be updated regularly.

The default setting of Quick Heal AntiVirus is configured to take the updates automatically from the Internet, without the intervention of the user. However, your system must be connected to the Internet to get the updates regularly.

The updates can also be taken from a local or a network path, but that path should have the latest set of definitions. This is helpful if your computer on which Quick Heal AntiVirus is installed is not connected to the Internet.

## Some important facts about the Quick Heal AntiVirus updates are:

- All the Quick Heal AntiVirus updates are complete updates including Definition File Update and Engine Updates.
- All the Quick Heal AntiVirus Security updates also upgrade your version whenever required, thus making the new features and technology available for your protection.
- Quick Heal AntiVirus Update is a single step upgrade process.

You can update Quick Heal AntiVirus manually whenever necessary in any of the followings ways:

## Updating Quick Heal AntiVirus from Internet

With Update Now, you may update Quick Heal AntiVirus manually whenever you prefer. However, the default setting of Quick Heal AntiVirus is configured to take the updates automatically through the Internet. Your system must be connected to the Internet to get updates regularly. This feature works for all types of Internet connections (Dialup, ISDN, Cable, etc.).

To update Quick Heal AntiVirus, follow these steps:

1. Select **Start > Programs > Quick Heal AntiVirus > Quick Update**.
2. Follow the instructions and click the **Next** button.
3. Select **Download from Quick Heal AntiVirus 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 Quick Heal 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 AntiVirus with definition files

If you have the update definition file with you, you can update Quick Heal AntiVirus without connecting to the Internet. It is useful for Network environments with more than one system. You are not required to download the update file on all the computers within the network using Quick Heal. You can download the latest definition files from the website of Quick Heal from <http://www.quickheal.com/update>.

To update Quick Heal AntiVirus through definition file, follow these steps:

1. Select **Start > Programs > Quick Heal AntiVirus > Quick Update**.
2. Follow the instructions and click the **Next** button.
3. Select **Pick from specified path**.
4. Click **File** to locate the definition file. Select the update file.
5. 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 AntiVirus accordingly.

## Update Guidelines for Network Environment

Quick Heal AntiVirus 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. Make **QHUPD** folder in any location. For example: **C:\QHUPD**.
3. Assign Read-Only sharing rights to this folder.
4. Select **Start > Programs > Quick Heal AntiVirus > Quick Heal AntiVirus** to open **Quick Heal AntiVirus**.
5. Select **Settings > Automatic Update** from Dashboard.
6. Select **Copy update files to specified location**.
7. Click **Browse** and locate the **QHUPD** folder. Click **OK**.
8. Click **Save Changes** to save this setting.

9. On all user computers within the network launch **Quick Heal AntiVirus**.
10. Under **Settings**, go to the **Automatic Update** page.
11. Select **Pick update files from specified path**.
12. Click **Browse**.
13. Locate the **SERVER\QHUPD** folder from Network Neighborhood.  
Alternatively you can type the path as **\\SERVER\QHUPD**.
14. Click **Save Changes** to save the settings.

## Cleaning Viruses

Quick Heal warns you of a virus infection when:

- A virus is encountered during a manual scan.
- A virus is encountered by Quick Heal AntiVirus Virus Protection/Email Protection.

### Cleaning viruses encountered during scanning

The default settings of Quick Heal AntiVirus are adequately configured and are optimum to protect your system. If a virus is detected during scanning, Quick Heal AntiVirus tries to repair the virus. However, if it fails in repairing the infected files, such files are quarantined. In case you have customized the default scanner settings, take an appropriate action when a virus is found.

### Scanning Options

During scan , you can take any of the following actions as per requirement.

<b>Action Tab</b>	Displays the action taken on the files.
<b>Skip Folder</b>	Helps you avoid scanning the current folder. Scanning moves to other location. This option is useful while scanning a folder which contains non-suspicious items.
<b>Skip File</b>	Helps you avoid scanning the current file. This option is useful while scanning an archive of a large number of files.
<b>Stop</b>	Helps you stop the scanning process.
<b>Close</b>	Helps you exit from the scanning process.
<b>Shut down PC when finished</b>	Helps you shut down your system after finishing the scan. This feature will work only when the scan is complete.

## **Cleaning virus encountered in memory**

“Virus Active in memory” means that a virus is active, and is spreading to other files or computers (if connected to a network) and doing malicious activity.

Whenever a virus is detected during memory scan, a Boot Time Scan is automatically scheduled to run the next time you boot your system. Boot Time Scan will scan and clean all drives including NTFS partitions before the desktop is completely loaded. It will detect and clean even the most typical Rootkits, spywares, special purpose Trojans, and loggers.

### ***Restart required during cleaning for some malwares***

Some malwares drop and inject their dynamic link libraries in the running processes of the system such as explorer.exe, Iexplore.exe, svchost.exe, etc. which cannot be disabled or cleaned. During memory scan when they are detected, they will be set for deletion in the next boot automatically. Quick Heal AntiVirus memory scan will provide details or action recommendation for you in such cases.

### ***Cleaning of Boot/Partition viruses***

If Quick Heal AntiVirus memory scanner detects a boot or partition virus in your system, it will recommend you to boot your system using a clean bootable disk. It will scan and clean the virus using the Quick Heal Emergency disk.

### ***Responding to virus found alerts from Virus Protection***

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

# Technical Support

Quick Heal provides extensive technical support for the registered users. It is recommended that you have all the necessary details with you during the email or call to receive efficient support from the Quick Heal support executives.

## Support

This option provides you with a comprehensive online support where you can find answers to your queries in a wide variety of ways. The Support option includes FAQ (Frequently Asked Questions) where you can find answers to the most frequently asked questions, submit your queries, send emails about your queries or call us directly.

Support includes the following.

### **Web Support**

This feature helps you submit your queries and see FAQ (Frequently Asked Questions). However, it is advisable that you check with your queries in FAQ at least once before you resort to other means of support. It is possible that you may get an answer to your question in FAQ itself.

To use Web Support, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus menu bar, select **Help > Support**.
3. On the Support screen, click **Visit FAQ** to view FAQ or submit your queries through **Visit Forums**.

### **Email Support**

This feature helps you send us an email about your queries so that the experts at Quick Heal can reply you with an appropriate answer.

To use Email Support, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus menu bar, select **Help > Support**.
3. On the Support screen, click **Submit Ticket** under **Email Support** to submit your queries.

*When you click the Submit Ticket button, you are redirected to our Support webpage where you can submit your queries.*

### **Phone Support**

This feature helps you to call for instant support from the Quick Heal technical experts.

The following is the contact number for phone support: +91 92722 33000.

### **Remote Support**

Quick Heal Technical Support Team also provides Remote Support in some cases. This support module helps us easily connect to your computer system through the Internet and provide technical support remotely. This helps Quick Heal give you efficient support as our technical executives solve the issue for you.

To use Remote Support, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, select **Help > Support**.
3. Click the **Remote Support** button.

*The Remote Support terms agreements screen appears. Read the agreement carefully.*

4. Click **I Agree**.
5. Provide the **ID** available in the Quick Heal Remote Support agent to the Quick Heal Support executive.

*The Quick Heal Support executive will remotely access your system to fix the issue.*

### **Live Chat Support**

This feature helps you to chat with Quick Heal technical executives live to get your issues resolved.

## **Support Contacts**

Quick Heal provides extensive technical support for the registered users. It is recommended that you have all the necessary details with you during the call to receive efficient support from the Quick Heal support executives.

### **When is the best time to call?**

Quick Heal Technologies (P) Ltd. provides technical support between 9:30 AM and 9:30 PM IST (India Standard time).

### **Which number to call?**

Quick Heal users in India can call at +91 92722 33000.

Regional support for South India is available at +91 90431 21212 (Malayalam, Tamil, Telugu, and Kannada)

**For support in other countries**

To submit online queries and avail of the online chat facility, visit [http://www.quickheal.com/contact\\_support](http://www.quickheal.com/contact_support) (24/7)

To check for the phone numbers in specific countries, visit [http://www.quickheal.com/int\\_techsupp](http://www.quickheal.com/int_techsupp)

To check for the dealers in your country, visit <http://www.quickheal.com/locate-dealer>.

**Details that are necessary during the call**

- Product Key is included inside the box of your product. If the product is purchased online, the Product Key can be obtained from the email confirming the order.
- Information about your computer system: brand, processor type, RAM capacity, the size of the hard drive and free space on it, as well as information about other peripherals.
- The operating system: name, version number, language.
- Version of the installed anti-virus and the virus database.
- Software installed on your system.
- Is your system connected to a network? If yes, contact the system administrators first. If the administrators cannot solve the problem they should contact the Quick Heal technical support.
- Details: When did the problem first appear? What were you doing when the problem appeared?

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

You need to be as specific as possible and provide maximum details as the support executive will provide solution based on your inputs.

**Contact Quick Heal Technologies****Head Office**

Quick Heal Technologies (P) Ltd.

603, Mayfair Towers II,

Wakdewadi, Shivajinagar,

Pune 411005, Maharashtra

Email: [info@quickheal.com](mailto:info@quickheal.com)

For more details, please visit: [www.quickheal.com](http://www.quickheal.com).

---

# Index

---

**B**

Browser Sandbox, 50  
Browsing Protection, 49

**C**

Cleaning Viruses, 109

**D**

Data Theft Protection, 58  
DNA Scan, 38

**E**

Email Protection, 44

**P**

Parental Control, 52  
Password Protection, 68  
Phishing Protection, 50

**Q**

Quarantine & Backup, 43

**R**

Registration

Multi-users pack, 21

Offline, 19

Online, 18

Product Key, 19  
through SMS, 20

**Renewal**

Multi-users pack, 25

Offline, 23

Online, 22

**S****Scan**

External Drives, 57

Scan Schedule, 39

Scan Settings, 33

Spam Protection, 46

**V**

Virus Protection, 36