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

All Rights Reserved

Trademarks

End-User License Agreement

IMPORTANT

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

BY USING THIS SOFTWARE OR BY CLICKING THE "I AGREE" BUTTON OR LOADING THE QUICK HEAL'S SOFTWARE, IN ANY WAY, YOU ACKNOWLEDGE AND ADMIT THAT YOU HAVE READ, UNDERSTOOD AND AGREED TO ALL THE TERMS AND CONDITIONS OF THIS USER LICENSE AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS BELOW, DO NOT USE THIS SOFTWARE IN ANY WAY AND PROMPTLY RETURN IT OR DELETE ALL THE COPIES OF THIS SOFTWARE IN YOUR POSSESSION.

This License is a legally enforceable contract between you as an individual (assuming you are above 18 years), or the Company or any legal entity 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 Ltd (hereinafter referred as "Quick Heal" for the sake of brevity). 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 the rights not expressly granted, and retains the 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.

DO'S & DON'TS

You can:

- use one copy of the software on a single computer. In case of multi-users pack, 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.

MANDATORY ACTIVATION

Quick Heal warns you that in the process of installation of the software, the other security products/software applications installed on your computer may uninstall or disable if they are not compatible with Quick Heal's 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 the 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 Quick Heal's software may use the measures that can control and prevent piracy of software applications.

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.

THIRD PARTY WEBSITE LINKS

At some point the software product includes 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 content of any third party website, any links contained in the third party websites. Quick Heal is providing these links to third party websites to you only as a convenience and is not responsible for any kind of loss/damage arising out of it.

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 the computer access remotely. The availing of this support will be solely at your discretion and you are solely responsible to take the backup of the existing data/software/programs in your computer before availing such a support. 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.

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.

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.

COLLECTION OF INFORMATION

Quick Heal's software may collect the following information which may or 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 and risks. This information will not be correlated with any personally identifiable information and shall include, but is not limited to:

- Any type of Executable files which the Quick Heal's 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 the websites visited that the Quick Heal software deems inherently and potentially fraudulent.
- Any type of information that Quick Heal's software deems potentially fraudulent, posing security risks and 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.

DISCLAIMERS

This software package is provided as such without warranty of any kind, expressed or implied, including but not limited to the implied warranties of merchantability and fitness of the package. In no event will Quick Heal or its suppliers will be liable to you or anyone else for any damages arising directly/indirectly or consequential, including loss of data, lost profits or any other damages of the data/property arising out of the use or inability to use this software package ever.

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

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

ALL MATTERS SUBJECTED TO PUNE (INDIA) JURISDICTION.

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
Bold Font	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 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
Core Protection • Anti-virus • AntiSpyware • AntiMalware • Anti-Rootkit • Silent Firewall • Intrusion Detection • Intrusion Prevention	✓	✓	✓	✓	✓
Mail Protection • Spam protection		✓	✓	✓	✓
Internet Protection • Browser Sandbox	✓	✓		✓	✓
• Phishing Protection • Web Security • Parental Control				✓	✓
Privacy Protection • Data Theft Protection			✓		✓
• Secure Delete					✓
PC Optimization • Registry Cleanup • Disk Cleanup • Traces Cleanup • Registry Defragmenter • Duplicate File Finder					✓
Mobile Phone Protection • PC2Mobile Scan					✓

Contents

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 anti-virus software products installed on a single system may result in system malfunction. If any other anti-virus 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 should meet the following minimum requirements.

- Internet connection to receive updates
- CD/DVD Drive

Operating System Compatibility

Operating Systems	Minimum Requirements
Windows 2000	• 300 MHz Pentium (or compatible) processor • 256 MB of RAM • DVD or CD-ROM drive • Service Pack 4 • Internet Explorer 6
Windows 2000 Server*	• 300 MHz Pentium (or compatible) processor • 256 MB of RAM • DVD or CD-ROM drive • Service Pack 4 • Internet Explorer 6
Windows XP	• 300 MHz Pentium (or compatible) processor • 256 MB of RAM • DVD or CD-ROM drive • Service Pack 2 and later
Windows Server 2003*	• 300 MHz Pentium (or compatible) processor • 256 MB of RAM • DVD or CD-ROM drive
Windows Vista	• 1 GHz Pentium (or compatible) processor • 512 MB of RAM • DVD or CD-ROM drive
Windows Server 2008*	• 1 GHz Pentium (or compatible) processor • 512 MB of RAM • DVD or CD-ROM drive
Windows Server 2008 R2*	• 1 GHz Pentium (or compatible) processor • 512 MB of RAM • DVD or CD-ROM drive
Windows 7	• 1 GHz Pentium (or compatible) processor • For 32-bit: 512 MB of RAM; For 64-bit: 1 GB of RAM • DVD or CD-ROM drive
Windows 8	• 1 GHz Pentium (or compatible) processor • For 32-bit: 512 MB of RAM; For 64-bit: 1 GB of RAM • DVD or CD-ROM drive For latest compatibility information on Windows 8, visit http://www.quickheal.com/win8
Windows Server 2012*	• 1 GHz Pentium (or compatible) processor • 512 MB of RAM • DVD or CD-ROM drive For latest compatibility information on Windows 8, visit: http://www.quickheal.com/win8

Free disk space requirement

During installation, the free disk space required for Quick Heal products is as follows.

Products	Free Disk Space
Quick Heal AntiVirus Pro	1.30 GB
Quick Heal Internet Security Essentials	1.30 GB
Quick Heal Internet Security	1.30 GB
Quick Heal Total Security	1.46 GB
Quick Heal AntiVirus Server Edition	1.30 GB

- * Indicates that the operating systems are supported only on Quick Heal AntiVirus Server Edition.
- The requirement is applicable to both 32-bit and 64-bit operating systems unless specifically mentioned.
- The requirement is applicable to all flavors of the operating system.
- 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.
- The requirements provided are minimum system requirements. Quick Heal recommends that your system maintains a higher configuration than the minimum requirements to obtain best results.
- To check for the latest system requirements, visit at www.quickheal.com.

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 256 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.

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.
- For the list of Mobile phones supported, please check at: http://www.quickheal.co.in/pc2mobile.asp.

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, and Microsoft Windows 8 operating systems.

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.

   In case 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, wherein the system memory is scanned. During the pre-install scan, 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-20.

   During the pre-install virus scan if no virus is found in the system memory, the installation proceeds further.

   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 mentioned 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 during 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 ways:

1. To uninstall, select **Start > Programs > Quick Heal AntiVirus**[#] **> Uninstall Quick Heal AntiVirus**.

   A prompt with the 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* ***Remove Report Files***, ***Remove Quarantine/Backup Files*** *and* ***Remove list of black-list & white-list email senders***[†] *options 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 helps us to 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.

Chapter 2

Registration, Re-activation and Renewal

Quick Heal AntiVirus must be immediately registered upon installation to activate the copy. Only the activated copy will receive the database updates regularly and you can get technical support whenever required. 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

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**.

   The Registration Wizard opens.

2. 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 and complete the registration form. Upon completion, 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 ways.

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 ways.

- **Product Key**: Is printed on the User Guide and/or can be found inside the box. If the product is purchased online, then the product key can be obtained from the email confirming the order.
- **Installation Number**: Can be obtained from the Activation Wizard in the following ways:

  i. Select **Start > Programs > Quick Heal AntiVirus > Activate Quick Heal AntiVirus**.

  The Registration Wizard opens.

  ii. 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 ways:

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**.

   A registration form appears.

4. Enter the relevant information in the registration form. Click **Submit**.

   All asterisk fields are mandatory to fill.

5. A new key is generated. Save this personally.

   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

Once 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 ways:

1. Select **Start > Programs > Quick Heal AntiVirus > Activate Quick Heal AntiVirus**.

   The Registration Wizard opens.

2. 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 as provided in the Quick Heal Registration wizard.

Currently Registration through SMS facility is available only in India.

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

1. Select **Start > Programs > Quick Heal AntiVirus > Activate Quick Heal AntiVirus**.

   The Registration Wizard opens.

2. Click **SMS Registration**.

   A screen with 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. On successful registration at the Quick Heal Registration Center, you will receive an SMS on your mobile which contains an alpha-numeric 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, all 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 full period until 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, then you have to fill all the user information once 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 is protected without any interruption. You can get a 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

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

1. Select **Start > Programs > Quick Heal AntiVirus > Activate Quick Heal AntiVirus**.
2. If your copy of Quick Heal has expired then click **Renew Now** on the Quick Heal Dashboard. If your copy of Quick Heal has not expired, then click **About** in the Help menu and click **Renew Now**.

   The Registration Wizard appears.
3. Select the **I want to renew with renewal code. I already have renewal code with me** option 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 **I do not have renewal code with me. I want to purchase renewal code online** option and click Buy Now.
- In case you renewed your license but its expiration date has not extended, select the **I have already renewed my license. Please update my license from server** option and click **Next**.
- If you have purchased an additional renewal code, then 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 www.quickheal.co.in/offline-renewal.asp and complete the registration form. Upon completion of the offline renewal process, 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 ways:

Getting the details of Quick Heal AntiVirus

Before visiting the offline renewal page, you should 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 steps:

  i. Select **Start > Programs > Quick Heal AntiVirus > Quick Heal AntiVirus**.

  ii. If your copy of Quick Heal has expired, then click **Renew Now** on the Quick Heal Dashboard. If your copy of Quick Heal has not expired, then click **Help > About** and click **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 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 ways:

1. Visit the offline activation page at http://www.quickheal.co.in/offline-renewal.asp.

   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 following screen displays the user name, registered email address, and contact number. If your email address and contact number have changed, then 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

Once 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 then click **Renew Now** on the Quick Heal Dashboard. If your copy of Quick Heal has not expired, then click **About** in the Help menu and click **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 renewed 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.

Can Quick Heal be installed on another PC?

Once a product key of Quick Heal is activated on a PC it cannot be re-used. If you try to re-use the Product Key to activate another copy of Quick Heal, it is considered as a pirated copy and will be blocked.

One product key can be used only for one computer.

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.

Chapter 3 Quick Heal AntiVirus Dashboard

The Quick Heal Main Dashboard serves as the key interface to all the features of Quick Heal AntiVirus. You can also access the Dashboard and certain features of Quick Heal AntiVirus from the taskbar of your system. Quick Heal protects the entire system even with the default settings. You can start Quick Heal to check the status of Quick Heal protection, to manually scan, 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.

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 has the product menus, the middle section has the protection options and the bottom section has the most frequently accessed features of Quick Heal AntiVirus.

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

Files & Folders	Helps you protect files and folders against malicious threats. With Files & Folders, you can configure Scan Settings, Virus Protection, DNAScan, Block Packed Files, Automatic Rogueware Scan, Scan Schedule, Exclude Files & Folders, and Quarantine & Backup.
Emails	Helps you configure Email Protection, Trusted Email Clients Protection and Spam Protection.
Internet & Network	Helps you configure the settings for Internet & Network protection. With this option, you can configure Firewall Protection, Browsing Protection, Malware Protection, Phishing Protection[#], Browser Sandbox[†] and News Alert.
Parental Control[*]	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.

External Drives & Devices	Helps you configure protection for external drives. You can configure protection such as Autorun Protection, Scanning External Drives, Data Theft Protection* and Scanning Windows Mobile†.

This feature is available only in Quick Heal Internet Security and Quick Heal Total Security.

† This feature is not available in Quick Heal AntiVirus Server Edition.

***** This feature is available only in Quick Heal AntiVirus Server Edition and Quick Heal Total Security.

† This feature is available only in Quick Heal Total Security.

The second section includes the product menus that 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 Help and license details.

Settings	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.
Tools	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 roguewares and prevent USB drives against autorun malware infection. You can also exclude files from virus protection.
Reports	Helps you view the activity reports of Scanner, Virus Protection, Email Protection, Scheduler, Quick Update, Memory Scan, Anti-Phishing*, Registry Restore, Boot Time Scanner, AntiMalware Scanner, Browsing Protection, PC2Mobile Scan# , and Firewall Protection.
Help	Helps you access Help for Quick Heal AntiVirus, see details about product version, virus database, validity details, license details and seek Technical Support.

* This feature is available only in Quick Heal Internet Security and Quick Heal Total Security.

This feature is available only in Quick Heal Total Security.

The bottom section includes the following.

News	Displays the latest news from Quick Heal. You can see all the news by clicking **See All**.
PCTuner*	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.

Scan	Provides you with various scan options such as Full System Scan, Custom Scan, Memory Scan, Boot Time Scan and Mobile Scan*.
Support	Helps you get to the support system available in **Support**.
Like	Follow us on Facebook.

***** This feature is available only in Quick Heal Total Security

Right Shell Menu Options

The Quick Heal AntiVirus icon in the taskbar helps you access and use some of the important features that are as follows:

Open Quick Heal AntiVirus	Helps you launch Quick Heal AntiVirus.
Launch AntiMalware	Helps you launch Quick Heal AntiMalware.
Enable / Disable Silent Mode	Helps you enable / disable all Quick Heal prompts and notifications.
Secure Browse	Helps you launch your default browser in Sandbox for secure browsing.
Enable / Disable Virus Protection	Helps you enable / disable Quick Heal Virus Protection.
Remote Support	Helps you launch Remote Support.
Update Now	Helps you update Quick Heal AntiVirus.
Scan Memory	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 data storage drives, folders, or files as per your requirement. Although the default settings for manual scanning are usually adequate, you can adjust the options for manual scanning by selecting **Files & Folders > Scan Settings** from the Dashboard.

Performing Full System Scan

With Full System Scan, you can scan all boot records, drives, folders and files on your computer (excluding mapped network drives) in the following ways:

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

   The scanning begins.

2. After completion of the scanning, you can view the report in the Reports menu.

Performing Custom Scan

With Custom Scan, you can scan specific files or folders in the following ways:

1. On the Quick Heal Dashboard, select **Scan > Custom Scan**.
2. Click **Add** to locate the path of the folder that you want to scan. You can select multiple folders for scanning and then click **Start Scan**.

   The scanning begins.

3. After completion of the scanning, you can view the report in the Reports menu.

Performing Memory Scan

With Memory Scan, you can scan memory in the following ways:

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

   The scanning begins.

2. After completion of the scanning, you can view the report in the Reports menu.

Performing Boot Time Scan

Boot Time Scan is very useful to disinfect the system in case your system is badly infected by a virus that cannot be cleaned because it is active. However, this scan is performed on next boot using Windows NT Boot Shell. To activate Boot Time Scan, follow these steps:

1. On the Quick Heal Dashboard, select **Scan > Boot Time Scan**.
2. A screen with Boot Time Scan modes appears. Select any one of the modes for Boot Time Scan to proceed further.
3. To scan the system immediately, click **Yes** to restart the system. To scan the system at next boot click **No**.

Performing Mobile Scan*

1. On the Quick Heal Dashboard, select **Scan > Mobile Scan**.
2. Select the Mobile Phone from the list.

   The scanning begins.
3. After completion of the scanning, you can view the scan report in the Reports menu.

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

Chapter 4

Quick Heal Protection Center

Quick Heal Protection Center is your instant interface to vital protection settings that can affect files, folders, emails, and so on. It helps you configure protection rules 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.

Red		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 executed immediately to keep your system protected.
Green		Indicates that Quick Heal AntiVirus is configured with optimal settings and your system is protected.
Yellow		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.

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

Files & Folders

With Files & Folders, you can set the protection rules for files and folders in your system. You can set the protection rules for the following settings.

Scan Settings

With Scan Settings, you can 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**.

   The Files & Folders setting details screen appears.
3. 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): The Automatic scan type is the default scan type , which is recommended as it ensures the optimal protection that your system requires. This setting is an ideal option for novice users as well.

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

Action to be performed when a virus is found

Repair	If a virus is found during a scan, it repairs the file or automatically Quarantines it, if it cannot be repaired. 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.
Delete	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.
Skip	If this option is selected the files are scanned but no action is taken on the infected files and they are skipped. Select this option if you want to take no action even if a virus is found. When the scan is over a summary report appears providing all the scan details.
Backup before taking action	The scanner keeps a backup of the infected files before disinfecting them. The files that are stored in the backup can be restored from the Quarantine menu.

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**.

   The Files & Folders setting details screen appears.
3. 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 execute Scan all files and the scanning process slows your system considerably.

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, RAR files and so on.
    - 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

The Scan archive files help you further set the scan rules for archive files such as ZIP files, RAR files, CHM files, and so on.

To configure the Scan archive files, 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.
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	
Delete	Deletes an archive containing virus-infected file without notifying you.
Quarantine	During scan if a virus is found in an archive file, then the archive will be moved to Quarantine.
Skip	Skips the virus and archive file without taking any action.

Archive Scan level	Set the level to scan inside an archive. The default scan level is set to level 2. However, increasing the default scan level may affect the scanning speed.

Select the type of archive that should be scanned

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

Select All	Helps you select all the archive file types in the list.
Deselect All	Helps you clear all the archive file types in the list.

Scan packed files

With **Scan packed files**, the scanner will scan packers also. Packers are the files that pack together many files, or compress 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 it can cause harm to your computer system. If you want to scan packers, select the **Scan packed files** option.

Scan mailboxes

With **Scan mailboxes**, you can scan the mail box of Outlook Express 5.0 and later versions (inside the **DBX** files). Viruses such as KAK, JS.Flea.B and so on, 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:

Quick scan of mailboxes	Helps you skip all the previously scanned messages and scan only new messages. This option is selected by default.
Thorough scan of mailboxes	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

With Virus Protection, you can continuously keep monitoring your system for viruses that might have tried to infiltrate from various sources such as email attachments, Internet downloads, file transfer, file execution and so on.

It is recommended that you always keep Virus Protection turned on to keep your system clean and protected 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**.

   The Files & Folders setting details screen appears.
3. Turn **Virus Protection** ON.
4. Click **Virus Protection**.

   The Virus Protection details screen appears.
5. Do the following:
   - **Display alert messages** – Select this option if you want to get the alerts about 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 on a file. 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

Repair	During scan if a virus is found, it repairs the file or automatically Quarantines it 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.

The following are the options for turning Virus Protection OFF:

- Turn on after 15 minutes
- Turn on after 30 minutes
- Turn on after 1 hour
- Turn on after next reboot
- Permanently disable

Select an option and click **OK**.

Once you turn off Virus Protection, 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.

DNA Scan

DNA Scan is the indigenous technology of Quick Heal to detect and eliminate new and unknown malicious threats in the system. DNA Scan technology successfully traps suspected files with very less false alarms. Additionally it copies the suspected file in the Quarantine directory before taking any action. The Quarantined-suspicious files can be submitted to our 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.

Whenever DNA Scan detects a new malicious threat in your system, a message about it is sent to you, or prompts you for taking an action during memory scanning if the scanning is set with Prompt settings. One copy of DNA Scan suspected files is also quarantined that you can submit later to the research labs. You can submit the suspicious files either automatically or manually through email. The submission takes place whenever Quick Heal AntiVirus updates itself and finds new DNA Scan suspected files in the Quarantine folder. It sends new DNA Scan suspicious quarantined files in an encrypted file format to the Quick Heal research labs.

To configure DNA Scan, follow these steps:

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

   The Files & Folders setting details screen appears.
3. Turn **DNA Scan** ON.
4. Click **DNA Scan**.

   The DNA Scan details screen appears.
5. Under **Select suspicious files**, select either of the following:
   - **Do not submit files** – Select this option if you do not want to submit files to the Quick Heal research labs.
   - **Submit files** – Select this option if you want to submit the suspicious files. You can also select the **Show notification while submitting files** to get prompts for permission before submitting the files to the Quick Heal Research labs.

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

Manual submission can be done through the Quarantine tool.

Block Suspicious Packed Files

Suspicious Packed Files helps you indentify and block suspiciously packed files. Suspiciously packed files are the files that are packed using pre-defined list of suspicious packers. Such packers are mostly used to pack malicious files, and when unpacked can cause serious harm to the computer. It is recommended that you always keep this option turned on as it prevents spread of threats.

To configure Block Suspicious Packed Files, follow these steps:

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

   The Files & Folders setting details screen appears.
3. Turn **Block Suspicious Packed Files** ON.

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

Automatic Rogueware Scan

The Automatic Rogueware Scan feature in Quick Heal AntiVirus automatically scans and removes rogueware and fake anti-virus software of critical level.

To configure Automatic Rogueware Scan, follow these steps:

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

   The Files & Folders setting details screen appears.
3. Turn **Automatic Rogueware Scan** ON.

   However, Automatic Rogueware Scan is turned on by default.

Scan Schedule

With Scan Schedule, you can define a schedule when to begin scanning of your system automatically. You can define multiple numbers of scan schedules so that the scan is initiated at your convenience. Scanning regularly helps you to keep your system free of virus and other types of threats.

Configuring Scan Schedule

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

   The Files & Folders setting details screen appears.
3. 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 the Daily option if you want to initiate scanning of your system daily. However, this option is selected by default.
  - Weekly: Select the Weekly 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: Select **Start at first boot** to schedule the scanner to begin at the first boot of the day. When you select Start at first boot, you do not have 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 **Start at** if you want to initiate the scanning of your system at a certain time. When you select Start at, the time drop-down list is activated where you can set the time for scanning. However, this option is selected by default.

    You can also define how often the scan should begin in the **Every day(s)** and **Repeat scan after every** options.
- Scan priority.
  - High: Select High if you want to have the scanning priority at high.
  - Low: Select Low if you want to have the scanning priority at low. 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. Provide **User Name** and **Password**.
9. Select **Run task as soon as possible if missed** to initiate scan of the missing tasks.

   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 number of drives and folders as per your requirement.

    You can also select **Exclude Subfolder** to exclude subfolders from being scanned. Click **OK**.
13. On the Configure Scan Schedule screen, click **Next**.
14. Check the summary of your scan schedule.
15. Click **Finish** to close the Scan Schedule dialogue.
16. Click **Close** to close the Scan Schedule screen.

Editing a scan schedule

You can change the scan schedule if required. To edit a scheduled scan, follow these steps:

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

   The Files & Folders setting details screen appears.
3. 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**.

   The Files & Folders setting details screen appears.
3. 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.

For more details about Scan Schedule, refer to Scan Settings, p- 22.

Exclude Files & Folders

With Exclude Files & Folders, you can decide which files and folders should not be included during scanning for known viruses or issues, DNA Scan, and packers. This helps you avoid unnecessary repetition of the scanning of 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**.

   The Files & Folders setting details screen appears.
3. Click **Exclude Files & Folders**.

   The Exclude Files & Folders details screen appears. Here you see a list of files and folders to be excluded from scanning, if you have added any.
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 and Suspicious packed files scan 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

With Quarantine & Backup, you can safely isolate the infected or suspected files. When a file is added to Quarantine, Quick Heal AntiVirus encrypts the file and keeps it inside the Quarantine folder. Being kept in an encrypted form, these files cannot be executed and hence are safe. Quarantine also keeps a copy of the infected file before repairing if you have selected **Backup before repairing** in the Scanner Settings.

With Quarantine & Backup, you can configure the rules for the files to be removed after a certain period of time and have a backup of the files.

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**.

   The Files & Folders setting details screen appears.
3. 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 the Quarantine folder automatically. However 30 days is set by default.
5. Click **View Files** to see the quarantined files. In the list of Quarantine files, you can take any of the following actions on the quarantined files:
   - Add: You can add files from folders and drives to be quarantined manually.
   - Remove: You can remove the Quarantine files from the Quarantine list.
   - Restore Selected: You can restore the selected files manually if required so.
   - Remove All: You can remove all the Quarantined files from the Quarantine list.
   - Send: You can send the selected files to our research labs.
   - Close: Helps you close the quarantine dialogue.

Emails

With Email Security, you can customize the protection rules for receiving emails from various sources. You can set rules for blocking emails which are suspicious of spam or malware.

Email Security includes the following.

Email Protection

With Email Protection, you can set the protection rules for all incoming emails. You can block the infected attachment in the emails that may be suspicious of malware, spams, and viruses. You can also customize the action that needs to be taken when malware is detected in the emails.

However, Email Protection is turned on by default and the default settings provide the required 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**.

   The Emails setting details screen appears.
3. Turn **Email Protection** ON.

   However, Email Projection 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.
6. 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.

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

Attachment Control Settings

Block attachments with multiple extensions	Helps you block attachment in emails with multiple extensions. Worms commonly use multiple extensions which you can block using this feature.
Block emails crafted to exploit vulnerability	Helps you block emails whose sole purpose is to exploit vulnerabilities of mail clients. Emails such as MIME, IFRAME contain vulnerability.
Enable attachment control	Helps you block email attachments with specific extensions or all extensions. However, this option is not selected by default. If you select this option, the following are available: **Block all attachments**: Helps you block all types of attachments in emails. **Block user specified attachments:** Helps you block email attachments with certain extensions. If you select this option, the **Configure** button is activated. For further settings, click **Configure** and set the following: • Under **User specified extensions**, select the extensions that you want to retain so as to block the email attachments with such extensions and delete all the remaining extensions. • If certain extensions are not in the list that you want to block, type such extensions in the extension text box and then click **Add** to add them in the list. • Click **OK** to save changes.

Trusted Email Clients Protection

Trusted Email Clients Protection supports most of the commonly used email clients such as Eudora and others. If your email client is different from the ones provided in the list, you can add such email clients in the trusted email client list.

Configuring Trusted Email Clients Protection

To configure Trusted Email Clients, follow these steps:

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

   The Emails setting details screen appears.

3. 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

With Spam Protection, you can block all unwanted emails such as spam, phishing and porn emails from reaching into your mailbox. Spam Protection is turned on by default and we recommend you always keep the feature turned on.

Configuring Spam Protection

To configure Spam Protection, follow these steps:

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

   The Emails setting details screen appears.
3. 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:
   - Moderate – Ensures optimum filtering. It is recommended to select moderate filtering that is selected by default also.
   - Strict – Enforces strict filtering criteria but is not ideal as the chances are that some genuine emails may also be blocked. Select strict filtering only when you receive too many junk emails or better select alternative means to stop junk emails.
7. Select **Enable email black list** to implement the protection rules for emails of black list.
8. Select **Enable email white list** to implement the protection rules for emails of white list.
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 Black List

Black List is the list of email addresses from which all emails are filtered irrespective of their content. All the emails from the addresses listed here are tagged as "[SPAM] -". This feature should be specifically evoked in case some server has an Open Relay which is being misused by Mass Mailers and viruses.

To add email addresses in the Black List, 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 Black List text box and then click **Add**.

   While entering an email address, be careful that you do not enter the same email address in the black list that you have entered in the white list, 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 Black List 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 Black List 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 White List

White List is the list of email addresses from which all emails are allowed to skip from spam protection filter irrespective of their content. No emails from the addresses listed here are passed through the SPAM filter. It is suggested that you configure only those email addresses that you trust on fully.

To add email addresses in the White List, 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 White List text box and then click **Add**.

   While entering an email address, be careful that you do not enter the same email address in the white list that you have entered in the black list, 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 White List 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 White List 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 White/Black List

To add domain addresses in the White or Black List, follow these steps:

1. Select either of **Enable email white list** or **Enable email black list** options 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

With Internet & Network, you can set the protection rules to save your system from malicious files that can sneak into your system during online activities such as banking, shopping, surfing and so on. 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

Firewall Protection works silently in the background and monitors network activity for malicious behavior. Firewall Protection first detects any malware and if found 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**.

   The Internet & Network setting details screen appears.
3. Turn **Firewall Protection** ON.

   Firewall Protection is activated.

Browsing Protection

With Browsing Protection, you can block malicious websites while browsing so that you are prevented from coming in contact with malicious websites and you are secure. However, Browsing Protection is turned on by default.

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**.

   The Internet & Network setting details screen appears.
3. Turn **Browsing Protection** ON.

   Browsing Protection is activated.

Malware Protection

With Malware Protection, you can protect your system from threats such as spywares, adwares, keyloggers, and riskwares 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**.

   The Internet & Network setting details screen appears.
3. Turn **Malware Protection** ON.

Malware Protection is activated.

Phishing Protection

With Phishing Protection, you can prevent access to phishing and fraudulent websites. Phishing is a fraudulent attempt, usually made through email, to steal your personal information. It usually appears to have come from well-known organizations and sites such as banks, companies and services with which you do not even have an account and, ask you to visit their sites telling you to provide your personal information such as credit card number, social security number, account number or password.

Phishing Protection automatically scans all accessed web pages for fraudulent activity protecting you against any phishing attack as you surf the Internet. It also prevents identity theft by blocking phishing websites, so you can do online shopping, banking and website surfing safely.

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**.

   The Internet & Network setting details screen appears.
3. Turn **Phishing Protection** ON.

   Phishing Protection is activated.

Browser Sandbox

With Browser Sandbox, you can apply a strict security mechanism to prevent access to all untrusted and unverified sites whether they are commercial sites, suppliers, sellers, third-parties, advertisements, entertainments sites.

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**.

   The Internet & Network setting details screen appears.
3. Turn **Browser Sandbox** ON.
4. Click **Browser Sandbox**.

4. Select the Browser security level.

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

5. 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 against confidential breach.
   - 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.

6. 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.

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

   This helps to clean temporary files.

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

News Alert

With News Alert, you get the latest news alert about the cyber security, important information related to Quick Heal etc. the latest news is also available on 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**.

   The Internet & Network setting details screen appears.
3. Turn **News Alert** OFF.

Parental Control

With Parental Control, parents can have full control over the Internet activity of their children and/or other users. Parents can decide which websites their children should visit and which they should not. Using the Parental Control feature, the parents can restrict categories of websites or block specific websites. The parents can also schedule Internet accessibility for their children.

Parental Control is smart enough to categorize all the sites accessed. It has a list of categories of sites that you can allow or deny based on your preferences. This is perfect for parents, who want to ensure that their kids visit the right kind of websites and are not exposed to materials unsuitable for the kids.

Important things to do before configuring parental control!

To get the best benefits from the parental control feature, we recommend you follow these steps though they are not mandatory:

First step

Check if you are logged in as an Administrative user. In case you are not an administrative user, it is recommended that you create an Administrator account and configure it. Do not reveal the administrative credentials to anyone.

Second step

Create Standard accounts (Restricted user) for your children. This way, the children will have only restricted access on the system.

Third step

The Password Protect in Parental Control ensures that Quick Heal AntiVirus settings are protected from modification by any unauthorized users. Then set the protection rules for users as who can access the Internet and when. You can assign different rules to different users based on you preferences.

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. Under **Select whom to apply the settings**, select:
   - **Apply to all users** if you want to apply the same setting to all the users.
   - **Apply to specific users** to apply different settings to different users. If you have selected the Apply to specific users, the list of all users appears.
4. To configure the setting, click **All Users** if you want apply the same setting to all the users, or click a single user in the list to apply different setting to a specific user.

   The protection rules screen appears.
5. Configure the following based on your preferences:
   - Restrict access to particular categories of website: Helps you restrict access to all websites under a category.
   - Restrict access to particular website: Helps you restrict access to specific websites only.
   - Schedule Internet access: Helps you schedule Internet accessibility for your children or other users.
6. Click **OK**.
7. Click **Save Changes** to save your settings.

Restrict access to particular categories of website

The **Restrict access to particular categories of website** feature in Parental Control has a vast range of website categories to allow or deny access to them based on your preferences. Once you restrict or allow a website category, all the websites falling under a category are blocked or allowed. This is helpful if you are sure you would like 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, which are a priority to you, you can do so by excluding such websites in the Exclude list.

To restrict access to particular categories of website, follow these steps:

1. On the protection rules screen for Parental Control, select **Restrict access to particular categories of website**.

   The Categories button is activated.

2. Click **Categories**.

   A list of website categories whose access can be allowed or denied appears.

3. Click the **Allow** or **Deny** button available next to each category that you want to allow or restrict 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 Social Networking and Chat category, but you still want to provide access to **Facebook**, you can do so by enlisting the website in the Exclude list.*

   i. On the Web Category list, click **Exclude** for excluding the websites.
   ii. Enter the URL of the website in the website 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.*

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

4. Click **OK** to save your settings for access restriction.

Restrict access to particular website

The **Restrict access to particular website** feature in Parental Control helps you block specific websites. This is helpful when you are interested in restricting certain websites, and when you have a shorter list in the website category. 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 is accessible that you want to block.

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

1. On the protection rules screen for Parental Control, 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 and then click **OK**. If you want to block all subdomains of the website, select **Also block subdomains**.

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

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

Schedule Internet access

The Schedule Internet access feature in Parental Control helps you schedule Internet accessibility for your children so you have full control over their browsing time. You can allow your children access to the Internet without any restriction or you can schedule the Internet accessibility. 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 for Parental Control, select **Schedule Internet access**.

   The Configure button is activated.

2. Click **Configure**.

   The Schedule internet access chart appears.

3. Select **Always allow access to the Internet**, if you want no restriction for the Internet accessibility.

4. Select **Allow access to the Internet as per the schedule** if you want to set restriction for accessing the Internet.

   The day and time schedule chart is activated.

5. Select the days and times for the days during which you want to allow access to the Internet for your children and other users.

   The selected cells are highlighted which indicates the allowed schedule.

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

Check if you have logged in as an Administrator

Administrators User Account allows you to change any settings or install an application on the system, 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 the **Start > Control Panel**.
2. Click **User Accounts**.
3. Your account type is displayed below your user name. If your account type is Administrator, then you are currently logged on as an Administrator. If your account type is not Administrator, then you need to change it to Administrator Account.

Quick Heal Password Protection

You can protect the settings and configurations 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. Click **Settings** on the Quick Heal AntiVirus Dashboard.
3. The Password Protection feature is set to **OFF** by default.
4. Click **OFF** to open Password Protection window.
5. If you are setting the password for the first time, then **Enter old password** will appear dimmed.
6. Type a password in **Enter new password** and re-type the same password in **Confirm new password**.
7. Click **Save Changes**.

Creating restricted user accounts

The restricted user accounts restrict the users only to their account and prevent them from taking full control of the computer system. This helps you 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

With External Drives & Devices, you can set protection rules for all external devices and drives such as CDs, DVDs, USB-based drives and so on. Whenever your system comes in contact with any external devices or drives, your system is at risk that malware may infiltrate.

Autorun Protection

Autorun Protection protects your system from autorun malware that tries to sneak into your system from USB-based devices or CDs/DVDs using the autorun feature of the installed operating system.

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**.

   The External Drives & Devices setting details screen appears.
3. Turn **External Drives & Devices** ON.

   Autorun Protection is activated.

Scan External Drives

With Scan External Drives, you can scan the USB-based drives as soon as they are attached to your system. The USB-based drives should always be scanned for viruses before accessing it from your system, as these devices have become the medium for quick transfer of malware from one system to another.

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**.

   The External Drives & Devices setting details screen appears.
3. Turn **Scan External Drives** ON.

   Scan External Drives is activated.
4. For further settings, click **Scan External Drives**.

5. Select **Scan files on the root of the drive only**, 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.
6. Select Scan full drive, if you want to scan all the files on the USB-based drive. This scan takes time but is safe.
7. 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

With Data Theft Protection, you can block transfer of the data between the system and USB drives and CD/DVD devices. Data Theft Protection ensures no files or data can be copied from your system to any external drives or devices. Similarly no files or data can be transferred from the USB drives or CD/DVD devices to your system. Hence neither your information can be theft nor can any harmful files be implanted in your system.

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**.

   The External Drives & Devices setting details screen appears.
3. Turn **Data Theft Protection** ON.

   Data Theft Protection is activated.
4. Click **Data Theft Protection**.
5. Do any of the following:
   - Select **Read only and no write access to external drives** to allow 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.
   - Select **Block complete access to external drives** to block transfer of data between the system and all external devices.
   - Select **Authorize USB drive** if you want to restrict accessing the 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. Only when you authorize, the

external device can be accessed. This option is available only if Quick Heal Password Protection in Settings is turned on.

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

Scan Windows Mobile

With Scan Windows Mobile, you can apply 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**.

   The External Drives & Devices setting details screen appears.
3. Turn **Scan Windows Mobile** ON.

   Scan Windows Mobile is activated.

Chapter 5 Quick Access Features

Quick Access Features provides you with quick access to important features such as Scan and PCTuner and so on. It also provides latest news about Quick Heal.

Secure Browse icon

The Quick Heal Secure Browse 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 option available on Dashboard provides you with various options of scanning your system to suit 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

With Full System Scan, you can 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

With Custom Scan, you can scan specific records, drives, folders, and files on your system that you require. This is helpful when you want to scan only certain items and not the entire system.

To initiate Custom Scan, follow these steps:

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

   The custom scan preference screen appears.
3. Click **Add** and then locate the path to the files and folders that you want to scan. You can select multiple folders for scanning.
4. After setting your scan preference, click **Start Scan**.

   The scan starts.

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

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:

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

Performing Boot Time Scan

Boot Time Scan is very useful to disinfect the system. In case the system is badly infected by a virus and it cannot be cleaned because the virus is active, use Boot Time Scan. 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 your entire system which though may take time. .
3. Click **Yes**.
4. To restart the system for scanning immediately, click **Yes**. To scan the system later, click **No**.

Performing Mobile Scan

1. Open **Quick Heal AntiVirus**.
2. On the Quick Heal AntiVirus Dashboard, select **Scan > Mobile Scan**.
3. Select the Mobile Phone from the list.

   In case your mobile is not available in the list, you need to add it. To add mobile to your system, refer to *Scan Windows Mobile, p-49.*

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

Quick Heal PCTuner

Quick Heal PCTuner is a tool that is integrated with Quick Heal AntiVirus that 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.

To know more about PCTuner, refer to Using Quick Heal PCTuner, p-76.

News

The News section displays the latest updates of information and developments from the Quick Heal Labs. Whenever there is any new information about the computer protection, security alerts, or other important issues, news about such things are displayed here. However to get the latest information, you must own licensed version of the product.

Chapter 6 Quick Heal Menus

With the Quick Heal AntiVirus menus, you can configure the general settings for taking updates automatically, password-protect your Quick Heal AntiVirus so that no unauthorized person can change your settings, provide settings for proxy support and set rules for the reports to be removed from the list automatically.

Settings

With Settings, you can apply various protection rules such as you can get the updates from Quick Heal when released, password-protect your settings and set the rule for the reports to be removed and so on. 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.

Automatic Update

With Automatic Update, you can get the updates automatically to keep your software updated with the latest virus signatures to protect your system from the latest malware. To get updates regularly, your system on which Quick Heal AntiVirus is installed needs to be connected to the Internet. 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**.

   The Settings details screen appears.
3. Turn **Automatic Update** ON.

   Automatic Update is activated.
4. Click **Automatic Update**.

5. 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.
6. Select the update mode from:
   - **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.
   - **Download from Admin Console Sever** – Helps you download the updates to your system from Quick Heal server.
   - **Copy update files to specified location** – Helps you save a copy of the updates to your local folder or network folder.
7. Click **Save Changes** to save your settings.

Internet Settings

With Internet Settings, you can 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 using 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**.

   The Settings details screen appears.
3. 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

The Registry is a database used to store settings and options of Microsoft Windows operating systems. It contains information and settings for all the hardware, software, users, and preferences of the system.

Whenever a user makes changes to 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.

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**.

   The Settings details screen appears.

3. 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

With Self Protection, you can apply protection to your application Quick Heal AntiVirus so that its files, folders, configurations and registry entries configured against malware are not altered or tampered in any way.

Configuring Self Protection

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

   The Settings details screen appears.
3. Turn **Self Protection** ON.

   However Self Protection is turned on by default.

Password Protection

With Password Protection, you can restrict all other users from accessing Quick Heal AntiVirus so that no unauthorized users can make any changes in the settings. You are recommended to always keep Password Protection turned on.

Configuring Password Protection

To configure Password Protection, follow these steps:

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

   The Settings details screen appears.
3. Turn **Password Protection** ON.

   Password Protection setting 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

With Report Settings, you can set rules for the reports to be removed generated on all activities. You can specify the number of days after which the reports should be removed from the list automatically. You may also retain the reports if you need them. However, the default setting for deleting reports is 30 days.

Configuring Report Settings

To configure Report Settings, follow these steps:

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

   The Settings details screen appears.
3. Click **Password Protection**.

   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.

   *However, 30 days is by default. If you clear **Delete reports after**, no reports will be removed.*
5. Click **Save Changes** to apply the settings.

Report Virus Statistics

Report Virus Statistics submits the virus detection statistics report, generated during scans, to Quick Heal Research Center.

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**.

   The Settings details screen appears.
3. Turn **Report Virus Statistics** ON.

   The Report Virus Statistics is activated.

Restore Default Settings

With Restore Default Settings, you can restore your customized settings to the system default settings. This is very helpful when you configure the settings but you are not satisfied with the protection settings or you are doubtful about the protection or you feel your protection is being compromised, you can restore the system default settings. However, you can set any of the settings as you prefer later.

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 set to default settings.

Tools

With Tools, you can carry out various activities such as you can clean and restore settings, prevent access to drives, diagnose system and so on.

Tools includes the following.

Hijack Restore

With Hijack Restore, you can restore the modified settings of Internet Explorer browser to default settings. 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 of Internet Explorer browser by using the Hijack Restore feature. This feature also helps to restore 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**.

   The Hijack Restore screen appears.
4. Select **Check All** to select all the browser settings in the list.
5. Select **Restore default host file**, to restore 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:

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

Restore important system settings

The restore important system settings option includes the following.

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

The buttons on the Hijack Restore function and their feature are as follows:

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

Track Cleaner

With Track Cleaner, you can remove the most recently used (MRU) applications to ensure that your privacy is not breached. Most of the applications store the list of recently opened files in their internal format to help you open them again for quick access. However, in the case that a system is used by more than one user the user's privacy may be compromised. Track Cleaner helps remove all the tracks of such applications 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.
4. Select the applications whose traces you want to remove or select **Check All** to select all the applications in the list.
5. To initiate cleaning, click **Start Cleaning**.
6. Upon completion click **Close** to exit.

Anti-Rootkit

With Anti-Rootkit, you can 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 certain knowledge of the operating system or with the help of Quick Heal Technical Support engineer. Improper usage of this program could result in unstable system.

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 pop-up appears that recommends closing 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 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.

Stop Scanning	Helps you stop the scan while the scan is under way.
Close	Helps you close the Anti-Rootkit. If you choose to close the Anti-Rootkit while scanning is in progress, it will prompt to stop the scan.
Error Report Submission	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 select what item to scan during scan process.

Configuring Quick Heal Anti-Rootkit Settings

1. Open **Quick Heal Anti-Rootkit**.
2. On the Quick Heal Anti-Rootkit screen, click **Tools**.

   The Tools dialog appears.
3. Quick Heal Anti-Rootkit is configured for Auto Scan by default where it scans the required system areas.

Auto Scan	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: • Hidden Processes. • Hidden Registry entries. • Hidden Files and Folders. • Executable ADS.

Custom Scan	Helps you customize the scan setting for Anti-Rootkit for the following: **Detect Hidden Process** – scans for the hidden processes running in the system. **Detect Hidden Registry Items** – scans for the hidden items in Windows Registry. **Detect Hidden files and folders** – scans for the hidden files and folders in the system and executable ADS (Alternate Data Streams). You can choose option: • Scan drive on which Operating System is installed • Scan all fixed drives • ADS (Alternate Data Streams) to scan for executable ADS.
Report File Path	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

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

Scanning Results and Cleaning Rootkits

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 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.

Action to be taken on Scan Results

Process	After the scan is complete, Quick Heal Anti-Rootkit will detect and display a list of hidden Processes. You can select process for termination, but make sure that the list of Processes for termination does not include any known trusted process. Quick Heal Anti-Rootkit also displays a summary of process scanning about total number of Processes scanned and number of hidden Processes detected.
Terminating Hidden Process	After selecting list of Processes for termination, 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.

Registry	Similar to the Process scan, Quick Heal Anti-Rootkit displays a list of hidden Registry keys. You can select keys for renaming, but make sure that the list of keys for renaming does not include any known trusted registry key. Quick Heal Anti-Rootkit also displays a summary of Registry scanning about total number of items scanned and number of hidden items detected.
Renaming Hidden Registry Key	After selecting list of keys for renaming, click the Rename button. Renaming operation requires reboot hence Key name will be prefixed by Rename Queued.

Files and Folders	Similarly, Quick Heal Anti-Rootkit displays a list of hidden Files and Folders. You can select Files and Folders for renaming, but make sure that the list of Files and Folders for renaming does not include any known trusted file. Quick Heal Anti-Rootkit also displays a list of executable Alternate Data Streams. Quick Heal Anti-Rootkit also displays a summary of File scanning about total number of files scanned and number of hidden files detected.
Renaming Hidden Files and Folders	After selecting list of Files and Folders for renaming, click the Rename button. Renaming operation requires reboot hence Files and Folders name will be prefixed by Rename Queued.

Cleaning Rootkits through Quick Heal Emergency Disk

At times, rootkits are not cleaned and they reappear during Quick Heal Anti-Rootkit scan. In such a case you can also use Quick Heal Emergency Disk for proper 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-65.

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 running Processes, Windows Registry and Files and Folders.

   After completing 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 file 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.
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 scanning 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** into 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 Spywares, Adwares, Roguewares, Dialers, Riskwares 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:

1. Select **Start > Programs > Quick Heal AntiVirus > Quick Heal AntiMalware**.
2. Right-click the Virus Protection icon on the Windows system tray and select **Launch AntiMalware**.
3. 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. While scanning for malwares Quick Heal AntiMalware displays malicious files, folders and registry entries related to various malwares. Once the scanning is complete and in case a malware is found, a list will be displayed for detected malwares contained in malicious files, folders and registry.

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

In a case any malware is detected, the following actions can be taken:

Clean	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 **Yes**, otherwise click **No** for temporary exclusion.
Skip	Helps you skip taking any action against malwares in your system.
Stop Scan	Helps you stop the scan.
Set System Restore point before cleaning	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.  **Set System Restore point before cleaning** feature is not available on Windows 2000 operating system.
Details	Helps you redirect to Quick Heal Website.

View Quarantine Files

With Quarantine, you can safely isolate the infected or suspected files. When a file is added to Quarantine, Quick Heal AntiVirus encrypts the file and keeps it inside the Quarantine directory. Being kept in an encrypted form, these files cannot be executed and hence are safe. Quarantine also keeps a copy of 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 with the Quarantine feature:

Add	Helps you add a file to Quarantine manually.
Remove	Helps you remove a quarantined file.
Restore	Helps you restore a file from Quarantine to its original location.
Remove All	Helps you remove all the quarantined files.
Send	Helps you send the quarantined file to our research labs for further analysis. Select the file that you want to submit and click **Send**.

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

Suspicious File	Select this reason if you feel that a particular file in your system has been the cause of suspicious activity in the system.
File is un-repairable	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.
False positive	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

With Quick Heal AntiVirus, you can safeguard your USB devices from autorun malware. The Autorun feature of the removable drive is one of the mediums for malware to infiltrate your system. The USB Drive Protection feature prevents autorun malware from using your removable device as an infection spreading medium. Securing the removable drive also ensures that the drive, if connected to an infected system, cannot be used for spreading autorun malware to other system.

To safeguard removable drives, 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 BHO's, 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 tracing existence of 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

With Windows Spy, you can find out more information about an application or process whenever required. Sometimes, we keep on getting dialog boxes or messages that are actually shown by spyware or some malware and we are not able to locate the malware. 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 above mentioned information.
5. If you want to terminate that application or window, click **Kill Process**.

Exclude File Extensions

With Exclude File Extensions, you can 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
- Quick Update
- Memory Scan
- Phishing Protection
- Registry Restore
- Boot Time Scanner
- AntiMalware Scanner
- 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 the feature to view 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
Details	Helps you display a detailed report of the selected record in the list.
Delete All	Helps you delete all the records in the list.
Delete	Helps you delete the selected record in the list.
Close	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
Prev	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.
Next	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.
Print	Helps you take the print of the detailed report.
Save As	Helps you save the detailed report in .txt format in a location of your system.
Close	Helps you exit from the report details screen.

For more details about Reports, refer to Reports, p-89.

Help

With the Help feature, you can 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 Quick Heal Technologies Pvt. Ltd., 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 irrespective whether you are connected to the Internet or not. 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 about how to submit System Information, refer to System Information, p-74.
- **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 about Support, refer to Support, p-102.
- **About**: The About section of Quick Heal AntiVirus includes the following information – .

  Quick Heal AntiVirus Version

  License details

  License validity

  Update Now option

Following buttons are also available in the About section:

Renew Now	Renew Now helps you renew your existing subscription.
License Details	License Information and End-User License Agreement (EULA) are available under this section. **Update License Details**: 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. Quick Heal Support team will renew your copy. However, you need to follow these steps: 1. Be connected to the Internet. 2. Click **Update License Details**. 3. Click **Continue** to update your existing subscription. **Print License Details**: Click Print License Details to take the print of the existing subscription information.
Update Now	Update Now 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:

To detect new Malwares	This tool gathers information to detect new Malwares from Running processes, Registry, System files like Config.Sys, Autoexec.bat etc.
To get Quick Heal AntiVirus information	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 the same automatically to 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 In**formation wiza**rd open**s.***

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 Using Quick Heal PCTuner

Quick Heal PCTuner is a tool that is integrated with Quick Heal AntiVirus that 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.

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

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

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

Status

The Status 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.

Tune-up Activity	The name of the Tuneup activity (Disk Cleanup, Registry Cleanup, Traces Cleanup, and Defragmenter).
Last Performed	The last execution date of each of the Tuneup activities. If the concerned Tuneup activity has never been executed, then the result will be **NEVER**. 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.
Tuneup Now button	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

The Tuneup 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 is a tuneup activity that 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

The Disk Cleanup feature is a tune-up activity that 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 that can be used for other applications 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

The Registry Cleanup feature is a tune-up activity that removes invalid and obsolete registry entries from the system that have appeared due to improper un-install, non-existent fonts, and so on. Sometimes during uninstallation, the registry entries are not deleted. This results in slower performance of the system. The Registry Cleanup 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

The Traces Cleanup feature is a tune-up activity that 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 have 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, Saved Passwords and so on.

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

The Defragmenter feature defragments vital files, such as page files and registry hives for improving the performance of the system. Files are often stored in different locations 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

The Scheduler 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 the time you specify. 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

The Settings 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

With Tools, you can 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

The Duplicate File Finder 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 using Duplicate File Finder, follow these steps:

1. Select **Tools > Duplicate File Finder**.
2. Click **Options** if you want to modify Duplicate File Finder settings.

   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 C**lose** to exit from the Tools menu.

Secure Delete

The Secure Delete 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.

One Pass Random – Quick Data Destruction	One Pass Random deletion 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.
Two Pass – More Secure Destruction	Two Pass deletion 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.
DoD – Standard Data Destruction	DoD deletion uses the encryption method of using random letters to overwrite data as per the Department of Defense Memo. Data once deleted cannot be recovered by any recovery software.

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 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

The Startup Booster feature is a tool that removes unwanted startup programs from the system. The Startup Booster 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 four types of 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, that is when 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

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

Click the Details button in any menu item to open a window called Report that 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

Auto Tuneup Reports includes a list of records distinguished by **Date** and **Time**. Each record includes a detailed report of 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

Disk Cleanup Reports includes a list of records distinguished by **Date** and **Time**. Each record includes a detailed report of 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

Registry Cleanup Reports includes a list of records distinguished by **Date** and **Time**. Each record includes a detailed report of 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

Traces Cleanup Reports includes a list of records distinguished by **Date** and **Time**. Each record includes a detailed report of 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

Scheduler Reports includes a list of records distinguished by **Date** and **Time**. Each record includes a detailed report of 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

Secure Delete Reports includes a list of records distinguished by **Date** and **Time**. Each record includes a detailed report of 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

Duplicate File Finder Reports includes a list of records distinguished by **Date** and **Time**. Each record includes a detailed report of 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

Startup Booster Reports includes a list of records distinguished by **Date** and **Time**. Each record includes a detailed report of 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

Service Optimizer Reports includes a list of records distinguished by **Date** and **Time**. Each record includes a detailed report of 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

Restore Reports includes a list of records distinguished by **Date** and **Time**. Each record includes a detailed report of 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

The Restore 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 the Auto Tuneup feature is executed, the Restore feature will restore only the items deleted by the Disk Cleanup and Registry Cleanup feature and skip the items deleted by the Traces Cleanup feature.

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 pops up 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 clicked **Yes** in the previous step, the backup is restored and a message box will pop-up saying **The selected backup was restored successfully**. 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 box will pop-up 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.

Chapter 8 Using PC2Mobiles Scan

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

- USB Cable
- Bluetooth

We regularly keep on adding support for new models. For latest list of supported mobile devices, please check at www.quickheal.co.in/pc2mobile.asp.

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 PC.
- For Nokia Phones, Nokia PC Suite software is recommended to be installed on your system. 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 PC 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 PC 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 Total Security 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 **Scan** to start scanning.

Scanning Notification for Windows Mobile Phone when connected to PC

When you connect your Windows Mobile Phone to PC using USB cable, Quick Heal 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 ways.

Connection through Bluetooth

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

1. Connect your Mobile phone to PC or Laptop through Bluetooth.

   Ensure that you are able to connect your mobile phone through your system via 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 Total Security 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 Other Mobile Phone through Bluetooth

To scan Other Mobile Phone via Bluetooth, follow these steps:

1. Connect your Mobile phone to PC or Laptop through Bluetooth.

   Ensure that you are able to connect your mobile phone through your system via 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 **Scan** to start scanning.

Connection through USB Cable

To configure your mobile phone via Cable, follow these steps:

1. Connect your Mobile phone to PC or Laptop through Cable.

   Ensure that you are able to connect your mobile phone through your PC via 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 via Cable, follow these steps:

1. Connect your Mobile phone to PC or Laptop through Cable.

   Ensure that you are able to connect your mobile phone through your PC via 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 **Scan** to start scanning.

Chapter 9

Updating Quick Heal AntiVirus & Cleaning Viruses

Updates for Quick Heal AntiVirus are released regularly on the website of Quick Heal which contains information pertaining to the detection and removal of newly discovered viruses. To prevent your system from new viruses, you should have the updated copy of Quick Heal AntiVirus. 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. Automatic updates can also be applied from a local or a network path, but that path should have the latest set of definitions.

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.

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).

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

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 www.quickheal.com.

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 any .bin 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. Go to the **Automatic Update** page under **Settings**.
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 files of the viruses, such files are quarantined. In case you have customized the default scanner settings, then take an appropriate action when a virus is found.

Scanning Options

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

Action Tab	Displays the action taken on the files.
Skip Folder	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.
Skip File	Helps you avoid scanning the current file. This option is useful while scanning an archive of a large number of files.
Stop	Helps you stop the scanning process.
Close	Helps you exit from the scanning process.
Shut down PC when finished	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 computer (if connected to network) and doing malicious activity as per its payload.

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 at boot time before the desktop is completely loaded. It will detect and clean even the most cunning Rootkits, spywares, special purpose Trojans, and loggers.

Restart required during cleaning for some malwares

Some malwares drop and inject their dynamic link libraries into system's running processes such as explorer.exe, 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

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

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.

Chapter 10 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

The Support 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

With Web Support, you can submit your queries, and see FAQ (Frequently Asked Questions) where you can find answers to the most 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 as 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**.

   Check for the answer to your queries in FAQ. If you do not find the appropriate answer, submit your queries to us.

Email Support

With Email Support, you can 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.
4. You may also email Support at support@quickheal.com.

Phone Support

With Phone Support, you can call us for instant support from the Quick Heal technical experts.

The following is the contact number for phone support: 1800 2333 733.

Remote Support

Quick Heal Technical Support Team also provides Remote Support in some cases. Quick Heal Remote Support module helps us easily connect to your computer system through the Internet and provide technical support remotely. This helps us 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 menu bar, select **Help > Support**.
3. Click **Remote Support**.

   The Remote Support terms agreements screen appears.
4. Click **I Agree**.
5. Provide the **ID** available in Quick Heal Remote Support agent to Quick Heal Support executive.

The details for remote access such as IP address and remote access ID are displayed. Provide these details to the remote support engineers who will connect to your system. The Quick Heal Support executive will remotely access your system to fix the issue.

Live Chat Support

With Live Chat Support, you can chat with Quick Heal technical executives.

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 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 (Indian Standard time).

Which number to call?

Quick Heal users in India can call **+91 - 927 22 33 000**.

Quick Heal users in India can also call us at the Toll Free support number: **1800 233 3733**.

For support in other Countries

Email : support@quickheal.com

Online chat available at www.quickheal.com (24/7)

For support in specific countries, log on to:
http://www.quickheal.com/locatedistributor.asp

Details that are necessary during the call

- Product Key, that is included inside the box of your product. If the product is purchased online, then 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

For more details, please visit: www.quickheal.com

Index

