Quick Heal

Security Simplified

User Guide

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

Quick Heal Technologies Ltd.
www.quickheal.com

Copyright & License Information

Copyright © 2017 Quick Heal Technologies Ltd. All Rights Reserved.

No part of this publication may be reproduced, duplicated, or modified in any form or incorporated into any information retrieval system, electronic or any other media or transmitted in any form without prior permission of Quick Heal Technologies Limited, Reg. Office: Marvel Edge, Office No. 7010 C & D, 7th Floor, Viman Nagar, Pune 411014.

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

Trademarks

Quick Heal and DNAScan are registered trademarks of Quick Heal Technologies Ltd. while Microsoft and Windows are registered trademarks of Microsoft Corporation. Other brands and product titles are trademarks of their respective holders.

License Terms

Installation and usage of Quick Heal Antivirus Security is subject to user's unconditional acceptance of the Quick Heal end-user license terms and conditions.

To read the license terms, visit www.quickheal.com/eula and check the End-User License Agreement for your product.

About This Document

This user guide covers all the information required to install and use Quick Heal antivirus products on Windows operating systems. The following table lists the conventions that we have followed to prepare this guide.

Convention	Meaning
Bold Font	Anything highlighted in bold indicates that it is a menu title, window title, check box, drop-down box, dialog, button names, hyperlinks, and so on.
	This is a symbol used for a note. Note supplements important points or highlights reservation related to the topic being discussed.
	This is a symbol used for a tip. Tip helps users to apply the techniques and procedures to achieve the task related to the topic being discussed.
	This is a symbol used for warning or caution. This is an advice either to avoid loss of data or damage to hardware.
<Step 1> <Step 2>	The instruction mentioned in the numbered list indicates actions that you need to perform.
Product Name	The term Quick Heal antivirus is used as a generic term in this document. It may refer to any of the following products: Quick Heal Total Security, Quick Heal Total Shield, Quick Heal Internet Security, Quick Heal Internet Security Essentials, Quick Heal AntiVirus Pro Advanced, Quick Heal AntiVirus Pro, Quick Heal AntiVirus Server Edition unless specified otherwise.

Quick Heal Products Compared

Features	Quick Heal						
	AntiVirus Pro	**AntiVirus Pro Advanced**	**Internet Security Essentials**	**AntiVirus Server Edition**	**Internet Security**	**Total Shield**	**Total Security**
Advance DNAScan	✔	✔	✔	✔	✔	✔	✔
Core Protection							
• Antivirus • AntiSpyware • AntiMalware • Anti-Rootkit • Firewall • Intrusion Detection • Intrusion Prevention	✔	✔	✔	✔	✔	✔	✔
Mail Protection							
• Spam protection			✔	✔	✔	✔	✔
Internet Protection							
• Browser Sandbox	✔	✔	✔		✔	✔	✔
• Safe Banking			✔		✔	✔	✔
• Phishing Protection			✔	✔	✔	✔	✔
• Web Security • Parental Control					✔	✔	✔
Vulnerability Scan			✔	✔	✔	✔	✔
Virtual Keyboard			✔		✔	✔	✔
Privacy Protection							
• Data Theft Protection		✔		✔		✔	✔
PC Optimization							
• Registry Cleanup • Disk Cleanup • Traces Cleanup • Registry Defragmenter • Duplicate File Finder						✔	✔
Mobile Phone Protection							
• PC2Mobile Scan							✔

Contents

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.

- Remove any other antivirus software program from your computer if you have any. Multiple antivirus software products installed on a single computer may result in system malfunction.
- Close all open applications, browsers, programs, and documents for uninterrupted installation.
- Ensure that you have administrative rights for installing Quick Heal antivirus.

System requirements

To use Quick Heal antivirus, your system must meet the following minimum requirements. However, we recommend that your system should have higher configuration to obtain better results.

Note:

- The requirements are applicable to all flavors of the operating systems.
- The requirements are applicable to the 32-bit and 64-bit operating systems unless specifically mentioned.

General requirements

- CD/DVD Drive
- Internet Explorer 6 or later
- Internet connection to receive updates

System requirements for various Microsoft Windows OS

Operating Systems (OS)	System Requirements
Windows 10	Processor: 1 gigahertz (GHz) or faster RAM: 1 gigabyte (GB) for 32-bit or 2 GB for 64-bit
Windows 8.1 / Windows 8	Processor: 1 GHz or faster RAM: 1 GB for 32-bit or 2 GB for 64-bit
Windows 7	Processor: 1 GHz or faster RAM: 1 GB for 32-bit or 2 GB for 64-bit
Windows Vista	Processor: 1 GHz or faster RAM: 1 GB
Windows XP (Service Pack 2 and later)	Processor: 300 Megahertz (MHz) Pentium or faster RAM: 512 MB
Windows Server 2016*	Processor: 1.4 GHz Pentium or faster RAM: 2 GB
Windows Server 2012 R2* / Windows Server 2012*	Processor: 1.4 GHz Pentium or faster RAM: 2 GB
Windows Server 2008 R2* / Windows Server 2008*	Processor: 1GHz for 32-bit or 1.4 GHz for 64-bit RAM: Minimum 512 MB (Recommended 2 GB)
Windows Server 2003*	Processor: 550 MHz for 32-bit or 1.4 GHz for 64-bit RAM: 256 MB for 32-bit or 512 MB for 64-bit
Windows 2000 / Windows 2000 Server* (Service Pack 4)	Processor: 300 MHz Pentium or faster RAM: 512 MB

Hard disk space requirements

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

Products	Free Disk Space
Quick Heal Total Security	1.9 GB
Quick Heal Total Shield	1.9 GB
Quick Heal Internet Security	1.5 GB
Quick Heal AntiVirus Pro	1.5 GB
Quick Heal AntiVirus Pro Advanced	1.5 GB
Quick Heal AntiVirus Server Edition	1.9 GB
Quick Heal Internet Security Essentials	1.7 GB

Note:

- (*) Indicates that Quick Heal AntiVirus Server Edition is supported only on the server operating systems as mentioned in the Operating System Compatibility table.
- Quick Heal AntiVirus Pro, Quick Heal AntiVirus Pro Advanced, Quick Heal Internet Security Essentials, Quick Heal Internet Security, Quick Heal Total Shield, and Quick Heal Total Security are not supported on Microsoft Windows Server operating systems.

To check for the latest system requirements, visit the website of Quick Heal at www.quickheal.com.

POP3 email clients compatibility

Quick Heal antivirus supports	Quick Heal antivirus does not support
- Microsoft Outlook Express 5.5 and later - Microsoft Outlook 2000 and later - Netscape Messenger 4 and later - Eudora - Mozilla Thunderbird - IncrediMail - Windows Mail	- IMAP - AOL - POP3s with Secure Sockets Layer (SSL) - Web-based email such as Hotmail and Yahoo! Mail - Lotus Notes

Note: The Email Protection feature of Quick Heal antivirus is not supported on encrypted email connections that use Secure Sockets Layer (SSL).

The following features of Quick Heal antivirus follow specific compatibility

Features	Conditions
Application Control	- Is not supported on Microsoft Windows 2000 with Service Pack 4. - For Microsoft Windows XP, this feature is supported only if Service Pack 1 or later is installed.
Anti-Keylogger	- Is not supported on Microsoft Windows 2000, Windows XP 32-bit with Service Pack 1 or previous, and Windows XP 64-bit. - Is not supported on Windows 2003 Server 32 bit Service Pack 0 and Service Pack 1 and Windows 2003 Server 64 bit.
Browser Sandbox	- Is not supported on Microsoft Windows 2000 and Microsoft Windows XP 64-bit. - This feature supports Internet Explorer, Google Chrome, and Mozilla Firefox browsers only. - This feature does not support Microsoft Edge browser of

	Windows 10 operating system.
Emergency Disk	• Creating Emergency Disk using CD/DVD is not supported on Microsoft Windows 2003 and earlier versions. However, you can create Emergency Disk on USB drives.
Firewall	• The Monitor Wi-Fi Networks feature is not supported on Microsoft Windows 2000 and Windows XP 64-bit.
Safe Banking	• Is not supported on Microsoft Windows 2000 and Microsoft Windows XP 64-bit. • This feature supports Internet Explorer, Google Chrome, and Mozilla Firefox browsers only. • This feature does not support Microsoft Edge browser of Windows 10 operating system.
Self-Protection	• Is not supported on Microsoft Windows 2000 OS. • For Microsoft Windows XP operating system, this feature is supported only if Service Pack 2 or later is installed. • For Microsoft Windows Server 2003 operating system, this feature is supported only if Service Pack 1 or later is installed. • Process protection functionality of Self-Protection is supported on Microsoft Windows Vista Service Pack 1 and later.

Mobile Scan (PC2Mobile Scan)	• Is not supported on Microsoft Windows 2000 OS.
	• For Windows Mobile devices,
	  o Microsoft Active Sync 4.0 or later must be installed on Windows XP or previous OS.
	  o Windows Mobile Device Center must be installed on Windows Vista or later OS.

PCTuner	• Is not supported on Microsoft Windows 2000 OS.
Anti-Rootkit	• Is supported on 32-bit OS only.
Remotely Manage Quick Heal	• Is not supported on Microsoft Windows 2000 OS. • Supports Internet Explorer 9 and later.

Installing Quick Heal antivirus

To install Quick Heal antivirus, follow these steps:

1. Insert the Quick Heal antivirus CD/DVD in the DVD drive.

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

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

   i.   Go to the folder where you can access the CD/DVD.

   ii. Right-click the DVD drive and select **Explore**.

   iii. Double-click **Autorun.exe**.

2. Click **Install** to initiate the installation process.

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

   - The installer automatically sets the boot time scanner to scan and disinfect the system on the next boot.

   - After disinfection of your computer, the computer restarts and you need to re-initiate the installation. For more details, see Performing Boot Time Scan.

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

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

3. At the end of the license agreement, there are two options **Submit suspicious files** and **Submit statistics** which are selected by default. If you do not want to submit the suspicious files or statistics or both, clear these options.

4. Select **I Agree** if you accept the terms and then click **Next**.

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

5. If the default location has insufficient space, or if you want to install Quick Heal antivirus 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 antivirus may expose your system to virus threats. However, you can uninstall Quick Heal antivirus in the following way:

1. Select **Start > Programs > Quick Heal antivirus# > Uninstall Quick Heal antivirus**.

    ▪ **Remove Quick Heal and keep update definitions files** - If you select this option, Quick Heal will save license information, all downloaded update definitions, reports, quarantined files, anti-spam whitelist/blacklist in a repository on your computer, so that these can be used during reinstallation.

    ▪ **Remove Quick Heal completely** - If you select this option, Quick Heal will be completely removed from your computer.

2. Select one of the options and click **Next** to continue with the uninstallation.

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

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

    The uninstallation process is initiated.

    When uninstallation is complete, a message appears.

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

    Please note down the product key for future reference. You can save your product key information by clicking **Save to file**. Restart of your computer is recommended after Quick Heal antivirus 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 following products: Quick Heal Total Security, Quick Heal Total Shield, Quick Heal Internet Security, Quick Heal Internet Security Essentials, Quick Heal AntiVirus Pro Advanced, Quick Heal AntiVirus Pro, Quick Heal AntiVirus Server Edition , products that you have installed on your computer.

Registration, reactivation, and renewal

You should register your product immediately after installing it. Unless you register the product, it will be considered as a trial version. Also, a subscriber with registered license can use all the features without any interruptions, take the updates regularly, and get technical support whenever required. If your product is not regularly updated, it cannot protect your system against the latest threats.

Registration

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

Registering online

Registering offline

Registering through SMS

Registering online

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

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

2. On the Registration Wizard, enter the 20-digit Product Key and click **Next**.

   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**, and **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 expiry date of your license is displayed.

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

> **i** Once you register Quick Heal antivirus, you are asked to create an account with Quick Heal RDM, which allows you to manage your device remotely. To know about how to create an account with Quick Heal RDM, see Remotely Manage Quick Heal.

Registering offline

You can register Quick Heal antivirus offline also 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. After the registration is complete, a new key is generated which you have to use to activate your product on your system that is not connected to the Internet.

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

Obtaining Product Key and Installation Number

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

- **Product Key**: The Product Key is found in your product packaging. The Product Key is sent to your email address if you have purchased it online.

- **Installation Number**: You can obtain the Installation Number from the Activation Wizard in the following way:

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

    ii. On the Registration Wizard, click **Register Offline**.

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

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

Generating Activation Key for offline activation

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

1. Visit the offline activation page at 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 (as described in the preceding section) with you.

3. Provide the Product Key and Installation Number in the relevant fields and click **Submit**.

4. On the registration form, enter the relevant information and then click **Submit**.

   All asterisk (*) fields are mandatory to fill.

5. A new key is generated. Save this key for future reference.

   This key is also sent to your email address that you provided during registration of the product.

Activating Quick Heal with offline Activation Key

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

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

2. On the Registration Wizard, click **Register Offline**.

   The offline activation screen appears.

3. Click **Browse** to locate the path where the **<license>.key** is stored and click **Next**.

   Your license is activated successfully and the expiry date of your license 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.

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

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

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

2. On the Registration Wizard, click **SMS Registration**.

A screen with the conditions related to registering through SMS appears. Read the conditions carefully.

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**, and **Contact Number**. Select your **Country**, **State**, and **City**.

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

7. Click **Next** to continue.

   A confirmation screen appears with the information that you entered.

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

8. Click **Next** to continue.

   A unique code along with a mobile number is displayed.

9. Type the code and send it as an SMS to the number displayed.

10. After successful registration at the Quick Heal Registration Center, you will receive an SMS on your registered mobile which contains an alphanumeric activation code. Type this activation code in the text box provided and click **Next**.

    Your product is activated successfully and the expiry date of your license is displayed.

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

Multiuser Pack registration

To activate a multiuser pack, please take note of the following:

- When you register any Product Key in the multiuser pack, all the remaining Product Keys in the pack are registered simultaneously.

- The registration information of the first Product Key activated applies to all the remaining Product Keys.

- The same license validity applies to all the Product Keys in the pack.

Reactivation

Reactivation is a facility that ensures that you use the product for the entire period until your license expires. Reactivation is 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 reactivate Quick Heal antivirus on your system.

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

If you have saved the license backup using the [Remove Quick Heal and keep update definitions files](#) option during uninstallation on your computer, and initiate reactivation, the Product Key is displayed on the Quick Heal registration dialog box. You can proceed with the found Product Key and the updates you saved. Moreover, you can also use another Product Key if you prefer.

Upon submitting the Product Key (and Installation Number in case of offline reactivation), the user details are displayed. You can verify the details and complete the process.

> **i** If you prefer to reactivate your license through SMS, you have to fill in the user information again.

Renewal

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

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

[Renewing online](#)

[Renewing offline](#)

Renewing online

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

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

2. Click the **Help** menu and then select **About > Renew Now**.

    If your product license has expired, the **Renew Now** button is displayed on the Quick Heal Dashboard. To renew your license, click **Renew Now**.

    The Registration Wizard appears.

3. Select **I have renewal code or new product key with me** if you have already bought the renewal code and click **Next**.

The Registration Information appears.

Note: If you do not have a renewal key and want to renew your license, select I **do not have renewal code with me** and then make the purchase*.

4. Relevant information in the **Purchased From**, **Email Address**, and **Contact Number** text boxes appears pre-filled. However, you can modify your contact details if required 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.

    - (*) You cannot renew Quick Heal Total Shield and Quick Heal AntiVirus Pro Advanced from the website of Quick Heal.
    - If you have purchased an additional renewal code, the renewal can be performed only after 10 days of the current renewal.

Renewing offline

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

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

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

Getting the details of Quick Heal

Before visiting the offline renewal page, keep the following details ready:

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

        The offline renewal details screen appears.

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.

Generating Activation Key for offline activation

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

1. Visit the offline renewal page at http://www.quickheal.com/offline_renewal.

   An Off-Line Renewal page appears.

2. Under your product type, click the hyperlink **Click here to proceed to Step 1**.

   Ensure that you have the Product Key and Installation Number (as described in the preceding section), and renewal code with you.

3. Enter the Product Key, Installation Number, Purchased Renewal Code and Purchased From details and click **Submit**.

4. Upon verification of the provided data, the succeeding screen displays the user name, registered email address, and contact number. If your email address and contact number have changed, you can update them or else click **Submit**.

5. A new key is generated. Save this key for future reference.

   This key is also sent to your email address that you provided during registration of the product.

Renewing Quick Heal with <license>.key file

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

1. Select **Start > Programs > Quick Heal antivirus > Quick Heal antivirus**.

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

3. Click **Renew Offline**.

   The offline renewal details screen appears.

4. Click **Browse** to locate the path where the <license>.key is stored and click **Next** to continue.

   The copy of Quick Heal antivirus is renewed and the license validity is displayed.

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

Multiuser Pack renewal

To renew a multiuser pack, please take note of the following conditions:

- You can renew either a single Product Key of multiuser pack by purchasing a single-user renewal code, or renew the multiuser pack by purchasing a multiuser renewal code for all users. You can also buy renewal codes for the other licenses separately.
- If you renew a multiuser pack using the multiuser renewal code, all the licenses are simultaneously renewed and the same license validity applies to all the Product Keys in the pack.

Quick Heal Dashboard

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

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

- Select **Start > Programs > Quick Heal antivirus > Quick Heal antivirus**.

- On the taskbar, double-click the **Quick Heal antivirus** icon or right-click the **Quick Heal antivirus** icon and select **Open Quick Heal antivirus**.

- Select **Start > Run**, type Scanner and press the **Enter** key.

About Quick Heal Dashboard

The Quick Heal Dashboard is divided into various sections. The top section includes the product menus, the middle section the protection options, and the bottom section the latest news from Quick Heal and scan options.

Top section

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

The following table describes the menus and their usage.

Menus	Description
Settings	Helps you customize features such as Automatic Update, Internet Settings, Registry Restore, Self Protection, Password Protection, Reports Settings, Report Virus Statistics, Remotely Manage Quick Heal, 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 rogueware 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, Scan Scheduler, Behavior Detection[1], Quick Update, Memory Scan, Phishing Protection[2], Registry Restore, Boot Time Scanner, AntiMalware Scan, Firewall Protection, Parental Control[3], IDS & IPS, Browsing Protection, PC2Mobile Scan[4], Vulnerability Scan[5], Safe Banking[6], and Anti-Keylogger.
Help	Helps you access the Help tool for Quick Heal antivirus, see details about product version, virus database, validity details, license details, and seek technical support.

> (1) Report for Behavior Detection is not available in Quick Heal AntiVirus Server Edition.
>
> (2) Report for Phishing Protection is not available in Quick Heal AntiVirus Pro and Quick Heal AntiVirus Pro Advanced.
>
> (3) Report for Parental Control is available only in Quick Heal Total Security, Quick Heal Total Shield, and Quick Heal Internet Security.
>
> (4) Report for PC2Mobile Scan is available only in Quick Heal Total Security.
>
> (5) Vulnerability Scan is not available in Quick Heal AntiVirus Pro and Quick Heal AntiVirus Pro Advanced.
>
> (6) Report for Safe Banking is not available in Quick Heal AntiVirus Pro, Quick Heal AntiVirus Pro Advanced, and Quick Heal AntiVirus Server Edition.

To know more about this section, see [Quick Heal Menus](#).

Middle section

The middle section includes the protection options that help you configure various features for the security that your computer needs.

The following table describes the options and their usage.

Options	Description
Files & Folders	Helps you protect files and folders against malicious threats. With this option, you can configure Scan Settings, Virus Protection, Advance DNAScan, Block Suspicious Packed Files, Automatic Rogueware Scan, Anti-Keylogger, Screen Locker Protection[1], Scan Schedule, Exclude Files & Folders, and Quarantine & Backup.
Emails	Helps you configure Email Protection, Trusted Email Clients Protection, and Spam Protection[2].
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[3], Browser Sandbox[4], Safe Banking[5], News Alert, and IDS/IPS.
Parental Control[6]	Helps you control the Internet access, application access, and computer access for the children and other users.
External Drives & Devices	Helps you configure protection for external drives. With this option, you can configure Autorun Protection, Scan External Drives, Data Theft Protection[7] and Scan Windows Mobile[8].

i (1) Screen Locker Protection is not available in Quick Heal AntiVirus Server Edition.

(2) Spam Protection is not available in Quick Heal AntiVirus Pro and Quick Heal AntiVirus Pro Advanced.

(3) Phishing Protection is not available in Quick Heal AntiVirus Pro and Quick Heal AntiVirus Pro Advanced.

(4) Browser Sandbox is not available in Quick Heal AntiVirus Server Edition.

(5) Safe Banking is not available in Quick Heal AntiVirus Pro, Quick Heal AntiVirus Pro Advanced, and Quick Heal AntiVirus Server Edition.

(6) Parental Control is available only in Quick Heal Total Security, Quick Heal Total Shield, and Quick Heal Internet Security.

(7) Data Theft Protection is available only in Quick Heal Total Security, Quick Heal Total Shield, Quick Heal AntiVirus Pro Advanced, and Quick Heal AntiVirus Server Edition.

(8) Scan Windows Mobile is available only in Quick Heal Total Security.

To know more about this section, see Quick Heal Protection Center.

Bottom section

The following table describes the options and their usage.

Miscellanies	**Description**
News	Displays the latest news from Quick Heal. You can see all the news by clicking ***See All***.
PCTuner[1]	Helps you improve system performance by cleaning your system 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, Mobile Scan[2], and Vulnerability Scan[3].
My Account	With this link, you can go to the web portal of Quick Heal Remote Device Management (Quick Heal RDM). You can add your product to Quick Heal RDM to monitor the product remotely through the portal.
Virtual Keyboard[4]	Virtual Keyboard helps you enter the required information without pressing any keys on the physical keyboard. It reduces the risk of getting your information recorded by a possible keystroke logger malware. When

	you launch Safe Banking, you should prefer virtual keyboard.
	Hovering: Helps you enter the information by hovering over the keys than actually clicking the mouse. Using this feature, you can reduce the risk of being tracked by the malwares that record click of the mouse.
	Shuffling: Helps you shuffle the alphabets and characters on the virtual keyboard each time you click the mouse. This reduces the risk of eavesdropping about what information you type with the virtual keyboard.
Support	Helps you get to various support options available in the Support menu.
Facebook Like	With this link, you can like the Quick Heal page on Facebook.
	Quick Heal's corporate Facebook page has a vibrant community of users and a host of regular posts on cyber security and virus threats and alerts. You can follow the Quick Heal Facebook page by clicking the 'Facebook Like' link available on Dashboard.
	Alternately, if you are logged on to Facebook but you are not a part of the Quick Heal community on Facebook, you will get a prompt to like and follow the Quick Heal page.

i (1) PCTuner is available only in Quick Heal Total Shield and Quick Heal Total Security.
(2) Mobile Scan is available only in Quick Heal Total Security.
(3) Vulnerability Scan is not available in Quick Heal AntiVirus Pro and Quick Heal AntiVirus Pro Advanced.
(4) Virtual Keyboard is not available in Quick Heal AntiVirus Pro, Quick Heal AntiVirus Pro Advanced, and Quick Heal AntiVirus Server Edition.

To know more about this section, see Quick Access Features.

Right-click Menu Options

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

Right-click Menus	Description
Open Quick Heal antivirus	Helps you launch Quick Heal antivirus.
Launch AntiMalware	Helps you launch Quick Heal AntiMalware, an integrated tool that helps you scan registry, files, and folders at a very high speed. It helps you to thoroughly detect and clean Spywares, Adware, Rogueware, Dialers, Riskware and a number of other potential threats in your system.
Enable / Disable Silent Mode	Helps you enable / disable all Quick Heal antivirus prompts and notifications.
Safe Banking[1]	Helps you launch Safe Banking. In Safe Banking, you can do banking

	transactions safely.
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 where technical experts from Quick Heal will access your system to resolve your issues.
Update Now	Helps you update Quick Heal virus database.
Scan Memory	Helps you scan system memory for viruses.
Virtual Keyboard[2]	Helps you use virtual keyboard in place of physical keyboard.

To know more about this section, see Quick Heal Protection Center.

$\boxed{i}$ (1) Safe Banking is not available in Quick Heal AntiVirus Pro, Quick Heal AntiVirus Pro Advanced, and Quick Heal AntiVirus Server Edition.
(2) Virtual Keyboard is not available in Quick Heal AntiVirus Pro, Quick Heal AntiVirus Pro Advanced, and Quick Heal AntiVirus Server Edition.

Quick Heal Protection Center

While working with computer system, you are connected to the Internet, external drives, and send and receive email communications. This makes your system exposed to viruses that try to infiltrate into your system. Quick Heal Protection Center includes those features that allow you to secure your systems, folders, files, and data against any possible threats of malware, viruses, worms, and data theft.

Just above the features current status about your Quick Heal antivirus product is displayed. If the antivirus detects any threat in your system, it is indicated through color coded icons.

The following table describes the icons and their meanings.

Green	🟢	Indicates that Quick Heal antivirus is configured with optimal settings and your system is protected.
Orange	🟠	Indicates that a feature of Quick Heal antivirus needs your attention at your earliest convenience, but not immediately.
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 carried out immediately to keep your system protected.

Quick Heal Protection Center includes the following features.

Features	Description
Files & Folders	Includes Scan Settings, Virus Protection, Advance DNAScan, Block Suspicious Packed Files, Automatic Rogueware Scan, Anti-Keylogger, Screen Locker Protection[1], Scan Schedule, Exclude Files & Folders, and Quarantine & Backup.
Emails	Includes Email Protection, Trusted Email Clients Protection, and Spam Protection[2].
Internet & Network	Includes Firewall Protection, Browsing Protection, Malware Protection, Phishing Protection[3], Browser Sandbox[4], Safe Banking[5], News Alert, and IDS/IPS.
Parental Control[6]	Allows parents to control the Internet access, application access, and

	computer access for the children and other users.
External Drives & Devices	Includes Autorun Protection, Scan External Drives, Data Theft Protection[7], and Scan Windows Mobile.

> [i] (1) Screen Locker Protection is not available in Quick Heal AntiVirus Server Edition.
> (2) Spam Protection is not available in Quick Heal AntiVirus Pro and Quick Heal AntiVirus Pro Advanced.
> (3) Phishing Protection is not available in Quick Heal AntiVirus Pro and Quick Heal AntiVirus Pro Advanced.
> (4) Browser Sandbox is not available in Quick Heal AntiVirus Server Edition.
> (5) Safe Banking is not available in Quick Heal AntiVirus Pro, Quick Heal AntiVirus Pro Advanced, and Quick Heal AntiVirus Server Edition.
> (6) Parental Control is available only in Quick Heal Total Security, Quick Heal Total Shield, and Quick Heal Internet Security.
> (7) Data Theft Protection is available only in Quick Heal Total Security, Quick Heal Total Shield, Quick Heal AntiVirus Pro Advanced, and Quick Heal AntiVirus Server Edition.

Files & Folders

With this feature, you can configure the protection settings for files and folders in your system.

Files & Folders includes the following protection settings.

Scan Settings

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

To configure Scan Settings, follow these steps:

1. Open **Quick Heal antivirus**.

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

3. On the Files & Folders screen, click **Scan Settings**.

4. Under **Select scan mode**, select **Automatic (Recommended)** to initiate the scan automatically, or select **Advanced** for advanced level scanning.

5. Under **Select action to be performed when virus is found**, select an appropriate action.

6. If you want to take a backup of the files before taking an action on them, select **Backup before taking action**.

7. To save your settings, click **Save Changes**.

Select scan mode

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

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

Action to be performed when a virus is found

Various actions and their description are as follows:

Action	Description
Repair	Select this option if you want to repair an infected file.
	If a virus is found during a scan in a file, it repairs the file. If the file cannot be repaired, it is quarantined automatically.
	If the infectious file has a Backdoor, Worm, Trojan, or Malware, Quick Heal antivirus automatically deletes the file.
Delete	Select this option if you want to delete an infected file. The-infected file is deleted without notifying you. Once the files are deleted, they cannot be recovered.
Skip	Select this option if you want to take no action on an infected file.
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 Quarantine.

Configuring Advanced Scan Mode

To configure Advanced Scan mode, follow these steps:

1. Open **Quick Heal antivirus**.

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

3. On the Files & Folders screen, click **Scan Settings**.

4. Under Select scan mode, select **Advanced**.

   The Configure button is activated.

5. Click **Configure**.

   The advanced scan setting details screen appears.

6. Under **Select item to scan**, select **Scan executable files** if you want to scan only the executable files or select **Scan all files** if you want to scan all files.

   However, the Scan executable files option is selected by default.

   It takes time to carry out **Scan all files** and the process may slow down your system.

7. Select one of the following items for scanning:

- **Scan archive files**: Select this option if you want to scan the archive files such as zip files and RAR files.

- **Scan packed files**: Select this option if you want to scan packed files.

- **Scan mailboxes**: Select **Quick scan of mailboxes** for a brief scan or else select **Through scan of mailboxes** to scan thoroughly.

8. Click **OK**.

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

Scan archive files

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

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

1. On the advanced scan setting screen, 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 one of the following options: Delete, Quarantine, and Skip.

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

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

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

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

Action to be taken when a virus is found

The following table describes various actions and their description.

Action	Description
Delete	Select this option if you want to delete an infected file. The-infected file is deleted without notifying you.
Quarantine	Select this option if you want to quarantine an infected archive if a virus is found in it.
Skip	Select this option if you want to take no action on an infected file.

Select the type of archive that should be scanned

A list of archives that can be included for scan during the scanning process is available in this section. Few of the common archives are selected by default that you can customize based on your requirement.

The following table describes the archive types.

Buttons	Description
Select All	Helps you select all the archives in the list.
Deselect All	Helps you clear all the archives in the list.

Scan packed files

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

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

Scan mailboxes

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

Options	Description
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

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

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

To configure Virus Protection, follow these steps:

1. Open **Quick Heal antivirus**.

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

3. On the Files & Folders screen, turn **Virus Protection** on.

4. Click **Virus Protection**.

    The Virus Protection details screen appears.

5. Set the following options as per requirement:

    - **Display alert message** – Select this option if you want to get the alerts on various events such as when malware is detected. However, this option is selected by default.

    - **Select action to be performed when virus is detected** – Select an appropriate action when a virus is detected during the scan.

    - **Backup before taking action** – Select this option if you want to take a backup of a file before taking an action. Files that are stored in the backup can be restored from Quarantine.

    - **Enable sound when threat is detected** – Select this option if you want to be alerted with sound whenever a virus is detected.

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

Action to be taken when a virus is detected

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

Turning off Virus Protection

It is recommended that you always keep Virus Protection turned on to keep your system clean and secure from any potential threats. However, you can turn Virus Protection off when absolutely necessary. While you turn Virus Protection off, you have a number of options to turn the feature only temporarily, so that it turns on automatically after the select time interval passes.

To turn off Virus Protection,

1. Open **Quick Heal antivirus**.

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

3. On the Files & Folders screen, turn **Virus Protection** off.

4. Select one of the following options:

- Turn on after 15 minutes

- Turn on after 30 minutes

- Turn on after 1 hour

- Turn on after next reboot

- Permanently disable

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

   After you turn Virus Protection off, the icon color of the Files & Folders option on Dashboard changes from green to red and a message "System is not secure" is displayed.

Advance DNAScan

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

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

To configure Advance DNAScan, follow these steps:

1. Open **Quick Heal antivirus**.

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

3. On the Files & Folders screen, click **Advance DNAScan**.

   The Advance DNAScan details screen appears.

4. Select either of the following options as per requirement:

- **Enable DNAScan**: Select this option to enable DNAScan.

- **Enable Behavior detection system***: Select this option if you want to enable Behavior detection system. The running applications will be monitored for their behavior. You can also set a security alert level from the **Select Behavior detection level** list either as High, Moderate, or Low.

  o High: If you select this security level, Quick Heal antivirus will closely monitor the behavior of a running application and will alert you if any unusual application behavior is noticed. You may receive more alerts and sometimes even for genuine files.

  o Moderate: If you select this security level, Quick Heal antivirus will send alert if any suspicious activity of a running application is noticed.

  o Low: If you select this security level, Quick Heal antivirus will send alert only if any malicious activity of a running application is noticed.

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

- **Do not submit files**: Select this option if you do not want to submit suspicious files to the Quick Heal research labs.

- **Submit files**: Select this option if you want to submit the suspicious files to the Quick Heal Research labs for further analysis. You can also select **Show notification while submitting files** to get prompts for permission before submitting the files.

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

> (*) Behavior Detection System is not available in Quick Heal AntiVirus Server Edition.

Advance DNAScan detects files by studying their characteristics and behavior.

Detection by Characteristics

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

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

Detection by Behavior

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

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

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

- **Block**: Take this action if you want to block the application from running.

> (*) Behavior Detection System is not available in Quick Heal AntiVirus Server Edition.

Submitting Suspected Files

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

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

1. Open **Quick Heal antivirus**.

2. On the Quick Heal Dashboard, click **Tools**.

3. Under Cleaning & Restore Tools, click **View Quarantine Files**.

   The Quarantine dialogue appears.

   A list of the files that have been quarantined is displayed.

4. Select the files that you want to submit to the Quick Heal labs and then click **Send**.

5. Click **Close** to close the Quarantine dialogue.

Block Suspicious Packed Files

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

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

To configure Block Suspicious Packed Files, follow these steps:

1. Open **Quick Heal antivirus**.

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

3. On the Files & Folders screen, turn **Block Suspicious Packed Files** on.

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

Automatic Rogueware Scan

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

To configure Automatic Rogueware Scan, follow these steps:

1. Open **Quick Heal antivirus**.

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

3. On the Files & Folders screen, turn **Automatic Rogueware Scan** on.

   However, Automatic Rogueware Scan is turned on by default.

Anti-Keylogger

Keyloggers are malicious programs that record all information typed by you on the keyboard of your computer or laptop and share that information with the hackers. You may lose confidential information such as usernames, passwords, or PIN to the hackers. Anti-Keylogger helps you prevent information getting recorded by keystroke logger malware.

Configuring Anti-Keylogger

1. Open **Quick Heal antivirus**.

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

3. On the Files & Folders screen, turn **Anti-Keylogger** on or off as you prefer.

Screen Locker Protection

Malicious programs that lock the screen preventing access to your computer are known as screen lockers. With Screen Locker Protection, you can create a short-cut key combination to initiate a clean-up of your computer and remove such malicious programs. By pressing the short-cut key, you can initiate cleaning up of your computer and remove the malicious program.

Configuring Screen Locker Protection

1. Open **Quick Heal antivirus**.

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

3. On the Files & Folders screen, click **Screen Locker Protection**.

4. To enable Screen Locker Protection, select **Protect from screen lockers**. However, this option is selected by default.

5. Select an alphabet from the drop-down list to create a short-cut combination with **Ctrl+Alt+Shift.** Here **A** is selected by default.

6. Click **Save Changes**.

$\boxed{i}$	• You have to restart your computer at least once after you install the product to activate this feature. • Screen Locker Protection is not available in Quick Heal AntiVirus Server Edition.

Scan Schedule

Scanning regularly helps you keep your system free from virus and other types of infections. This feature allows you to define a schedule when to begin scanning of your system

automatically. You can define multiple numbers of scan schedules to initiate scan at your convenience.

Configuring Scan Schedule

1. Open **Quick Heal antivirus**.

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

3. On the Files & Folders screen, click **Scan Schedule**.

   The Scan Schedule details screen appears.

4. To define a new scan schedule, click **New**.

5. In **Scan Name**, type a scan name.

6. Under Scan Frequency, select the following options based on your preferences:

   - Scan Frequency:

     o Daily: Select this option if you want to initiate scanning of your system daily. This option is selected by default.

     o Weekly: Select this option if you want to initiate scanning of your system on a certain day of the week. When you select the Weekly option, the Weekdays drop-down list is activated so you can select a day of the week.

   - Scan time:

     o Start at first boot: This helps you schedule the scanner to begin at the first boot of the day. If you select this option, you do not need to specify the time of the day to start the scan. Scanning takes place only during the first boot regardless what time you start the system.

     o Start at: Select this option to initiate the scanning of your system at a certain time. If you select this option, the time drop-down list is activated where you can set the time for scanning. However, this option is selected by default.

       You can further define how often the scan should begin in the **Everyday** and **Repeat scan after every** options.

   - Scan priority.

     o High: Helps you set high scan priority.

     o Low: Helps you set low scan priority . However, this option is selected by default.

7. Under **Scan Settings**, you can specify scan mode, define the advanced options for scanning, action to be performed when virus is found and whether you want a backup of the files before taking any action on them. However, the default setting is adequate for scanning to keep your system clean.

8. In the **Username** text box, enter your username and your password in the **Password** text box.

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

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

10. Click **Next**.

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

11. Click **Add Folders**.

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

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

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

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

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

Editing a scan schedule

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

1. Open **Quick Heal antivirus**.

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

3. On the Files & Folders screen, click **Scan Schedule**.

   The Scan Schedule details screen appears.

4. Select the scan schedule that you want to edit and then click **Edit**.

5. Make the required changes in the scan schedule and then click **Next**.

6. On the Configure Scan Schedule screen, you can add or remove the drives and folders as per your preference and then click **Next**.

7. Check the summary of the modification in the scan schedule.

8. Click **Finish** to close the Scan Schedule dialogue.

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

Deleting a scan schedule

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

1. Open **Quick Heal antivirus**.

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

3. On the Files & Folders screen, click **Scan Schedule**.

   The Scan Schedule details screen appears.

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

   The confirmation screen appears.

5. Click **Yes** to remove the selected scan schedule.

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

To know about how to configure Scan Schedule, see [Scan Settings](#).

Exclude Files & Folders

With this feature, you can decide which files and folders should not be included during scanning for known viruses, DNAScan, Suspicious Packed files, and Behavior Detection*. This helps you avoid unnecessarily scanning files which have already been scanned or that you are sure should not be scanned.

You can exclude files from being scanned from the following scanning modules:

- Scanner
- Virus Protection
- Memory Scanner
- DNAScan

i (*) Behavior Detection is not available in Quick Heal AntiVirus Server Edition.

Configuring Exclude Files & Folders

To configure Exclude Files & Folders, follow these steps:

1. Open **Quick Heal antivirus**.

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

3. On the Files & Folders screen, click **Exclude Files & Folders**.

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

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

The New Exclude Item screen appears.

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

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

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

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

7. Click **OK**.

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

> ⚠️ • If you are getting warning for a known virus in a clean file, you can exclude it for scanning of Known Virus Detection.
>
> • If you are getting a DNAScan warning in a clean file, you can exclude it from being scanned for DNAScan.

> ℹ️ (*) Behavior Detection is not available in Quick Heal AntiVirus Server Edition.

Quarantine & Backup

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

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

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

Configuring Quarantine & Backup

To configure Quarantine & Backup, follow these steps:

1. Open **Quick Heal antivirus**.

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

3. On the Files & Folders screen, click **Quarantine & Backup**.

    The Quarantine & Backup details screen appears.

4. Select **Delete quarantine/backup files after** and set the number of days after which the files should be removed from Quarantine automatically. However, 30 days is set by default.

5. To see which files have been quarantined, click **View Files**. A list of the quarantine files appears. You can take any of the following actions on the quarantined files:

   ▪ Add: Helps you add new files from the folders and drives to be quarantined manually.

   ▪ Remove: Helps you remove any of the quarantine files from the Quarantine list. To remove a file, select the file and then click the **Remove** button.

   ▪ Restore : Helps you restore a quarantined file to its original location. When you find a quarantined file trustworthy and try to restore it, an option for adding the file to the exclusion list appears. You can add the file to the exclusion list so that the same file is not treated as suspected and quarantined again. To restore a file, select the files and then click the **Restore** button.

   ▪ Remove All: Helps you remove all the quarantined files from the Quarantine list. To remove all the files, click the **Remove All** button. On the confirmation massage, click **Yes** to remove all the files.

   ▪ Send: Helps you send the quarantined files to our research labs. To send a file, select the file and then click the **Send** button.

6. To close the Quarantine dialog, click the **Close** button.

Emails

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

Email Security includes the following features.

Email Protection

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

Configuring Email Protection

To configure Email Protection, follow these steps:

1. Open **Quick Heal antivirus**.

2. On the Quick Heal Dashboard, click **Emails**.

3. On the Emails screen, turn **Email Protection** on.

   However, Email Protection is turned on by default.

   Protection against malware coming through emails is activated.

4. To set further protection rules for emails, click **Email Protection**.

5. Select **Display alert message** if you want a message when a virus is detected in an email or attachment.

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

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. If you select this option, the following options are activated: 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 options: • Under User specified extensions, select the extensions that you want to retain so that the email attachments with such extensions are blocked and all the remaining extensions are deleted. • 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

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

Configuring Trusted Email Clients Protection

To configure Trusted Email Clients Protection, follow these steps:

1. Open **Quick Heal antivirus**.

2. On the Quick Heal Dashboard, click **Emails**.

3. On the Emails screen, turn **Trusted Email Clients Protection** on.

4. To add a new email client, click **Trusted Email Clients Protection**.

   The Trusted Email Clients Protection details screen appears.

5. Click **Browse** and select a trusted email client

6. Click **Add** to add the email client in the list.

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

Spam Protection

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

> ⓘ Spam Protection is not available in Quick Heal AntiVirus Pro and Quick Heal AntiVirus Pro Advanced.

Configuring Spam Protection

To configure Spam Protection, follow these steps:

1. Open **Quick Heal antivirus**.

2. On the Quick Heal Dashboard, click **Emails**.

3. On the Emails screen, turn **Spam Protection** on.

4. For further settings, click **Spam Protection**.

5. Select the **Tag subject with text (Recommended)**, to tag the subject of an email as SPAM.

6. Under **Spam protection level**, set the protection level:

   - Soft – Select this option if you receive only a few spam emails or you want to block only the obvious spam emails. There is little possibility of genuine emails being identified as spam.

- Moderate (Recommended) – Ensures optimum filtering. This is ideal if you receive a good many spam emails. However, there is possibility of some genuine emails being identified as spam. It is recommended that you select moderate filtering which is selected by default also.

- Strict – Enforces strict filtering criteria but is not ideal as the chances are high that some genuine emails may also be blocked. Select strict filtering only when you receive too many spam emails or better select alternative means to stop spam emails.

7. Select **Enable email black list** to create a blacklist of email addresses. The protection rules will be applicable on the blacklisted email addresses.

8. Select **Enable email white list** to create a whitelist of email addresses. The protection rules will be applicable on the whitelisted email addresses.

9. Select **Enable AntiSpam plugin** to implement the protection rules for AntiSpam plug-in.

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

Setting spam protection rule for blacklist

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

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

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

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

   The Customize button is activated.

2. Click **Customize**.

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

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

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

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

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

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

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

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

Setting spam protection rule for whitelist

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

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

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

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

   The Customize button is activated.

2. Click **Customize**.

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

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

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

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

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

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

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

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

Adding Domains to whitelist or blacklist

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

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

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

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

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

Internet & Network

This feature allows you to set the protection rules to protect your system from malicious files that can sneak into your system during online activities such as banking, shopping, and surfing.

Internet & Network includes the following features.

Firewall Protection

Firewall shields your system from intruders and hackers by monitoring and filtering incoming and outgoing network traffic. Any suspicious program that may be harmful to your computers or systems is blocked. Firewall protects your computers from malicious programs either from outside internet connection or from within networks incoming into your system.

Configuring Firewall Protection

To configure Firewall Protection, follow these steps:

1. Open **Quick Heal antivirus**.

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

3. Turn **Firewall Protection** on or off by using the toggle button.

   However, Firewall Protection is turned on by default.

4. To set Firewall Protection, click anywhere in the Firewall Protection area.

5. To enable monitoring of unsafe Wi-Fi Networks, turn **Monitor Wi-Fi Networks** on.

   If you have enabled this option and try to connect to the unsecured Wi-Fi connections, an alert will be shown. You can decide whether you want to connect to such unsecured connections.

6. To configure rules for accessing the Internet and control network traffic, set the following policies:

   - [Program Rules](): Create rules for programs accessing the Internet.
   - [Advanced Settings](): Create rules for incoming and outgoing network traffic.

Program Rules

With Program Rules, you can allow or block programs from accessing the Internet.

To create rules for programs, follow these steps:

1. On the Firewall Protection screen, click the **Configure** button next to Program Rules.

2. On the Configure Program Rules screen, click the **Add** button to add a program.

   Only an executable program can be added.

3. The program that you added is enlisted in the program list. Under the Access column, select **Allow** or **Deny** for accessing the network as required.

4. To save your setting, click **OK**.

Allow only trustworthy programs

Trustworthy programs are those programs that are verified and their identity is known while untrustworthy programs are those ones that are not verified or are suspicious. Malicious programs mask their identity to run a covert operation. Such programs may be harmful to the network and computers.

You can block all untrustworthy programs from accessing the Internet by selecting the **Allow only trustworthy programs** checkbox.

Security Level

Firewall security level includes the following:

- Low: Allows all incoming and outgoing connections.
- Medium: Monitors incoming traffic and displays the message as per suspicious behavior of an application.
- High: Monitors both incoming and outgoing traffics and displays the message as per suspicious behavior of an application.
- Block all: Blocks all incoming and outgoing connections. If you set this security level, Internet connection for all applications including Quick Heal antivirus will be blocked. For example, Quick Heal update and sending system information among other features may not work.

Advanced Settings

To create rules for incoming and outgoing network traffics, follow these steps:

1. On the Firewall Protection screen, click the **Configure** button next to Advanced Settings.

2. On the Advanced Settings page, select the following as required:

   - **Display Alert Message**: Select this option if you want to get alert messages if connections matching exceptions rule are made for blocked outbound connections. This applies to outbound connections only.

   - **Create Reports**: Select this option if you want a report to be created. You may also configure a different path to save the report.

   - **Network Connections**: Using this option, set a network profile for network connections.

   - **Traffic Rules**: Using this option, set rules for network traffic.

3. To save the settings, click **OK**.

Network Connections

With Network Connections, you can set a Firewall profile for network connections. Under Network Profile Settings, you can see the following settings.

Settings	Description
Network Profile	Home: All incoming and outgoing connections are allowed except exceptions. Work: All incoming and outgoing connections are allowed except exceptions. Public: All incoming and outgoing connections are allowed except exceptions. Restricted: All incoming and outgoing connections are blocked except exceptions. Note: The logic for network profile may be changed based on your requirement. For example, if a network environment is considered less risky, you may turn stealth mode on or off. Similarly, you may allow or block sharing of file and printer. However, default setting is ideal for required security.
Stealth Mode	Enabling Stealth Mode hides the system in the network making it invisible to others thus preventing attacks.
File & Printer Sharing	Allowing this option will enable you to share file & printer between other users and you. However, with sharing of files and printer, the files may be accessed by unauthorized entities.

Traffic Rules

With Traffic Rules, you can allow or block network traffic. You can add exception to allow or deny incoming and outgoing communications through IP addresses and ports.

To configure a policy, follow these steps:

1. On the Advanced Settings screen, click the **Traffic Rules** tab.

2. Click the **Add** button.

3. In the **Exception Name** text box, write a rule name and then select a protocol. Click **Next**.

   The protocol includes: TCP, UDP, and ICMP.

4. Under **Local IP Address**, select either **Any IP Address**, **IP Address**, or **IP Address Range**. Type the IP Address accordingly and then click **Next**.

5. Under **Local TCP/UDP** Ports, select either **All Ports**, **Specific Port(s)**, or **Port Range**. Type the Ports accordingly and then click **Next**.

6. Under **Remote IP Address**, select either **Any IP Address**, **IP Address**, or **IP Address Range**. Type the IP Address accordingly and then click **Next**.

7. Under **Remote TCP/UDP** Ports, select either **All Ports**, **Specific Port(s)**, or **Port Range**. Type the Ports accordingly and then click **Next**.

8. Under **Select Action**, select either **Allow** or **Deny**.

9. Under **Network Profile**, select either or a combination of the profile options such as **Home**, **Public**, **Work**, or **Restricted**.

10. Click **Finish**.

The following table describes the buttons and their functions.

Buttons	Description
Add	Helps you create an exception rule.
Delete	Helps you delete an exception rule from the list. Select the rule and then click **Delete**.
Up	Helps you move a rule upward to arrange according to your preference.
Down	Helps you move a rule downward to arrange according to your preference.
Default	Helps you set the rules to default settings.
OK	Helps you save your settings.
Cancel	Helps you cancel your settings and close the Advanced Settings dialog.

Browsing Protection

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

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

Configuring Browsing Protection

To configure Browsing Protection, follow these steps:

1. Open **Quick Heal antivirus**.

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

3. On the Internet & Network screen, turn **Browsing Protection** on.

   Browsing Protection is activated.

Malware Protection

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

Configuring Malware Protection

To configure Malware Protection, follow these steps:

1. Open **Quick Heal antivirus**.

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

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

   Malware Protection is enabled.

4. To set further security measures for malware protection, click anywhere on Malware Protection and then set the following options.

   - **Enable Adware detection**: If you want to detect any adware, select this option. If you enable this option, actions to be performed option is activated.

   - **Select action to be performed when adware is found**: Select one of the following actions to be performed when any adware is detected – Prompt, Repair, Skip.

Action	Description
Prompt	If you select this option, a message will appear when an adware is detected. The message will display the following options: • **Allow**: Click this button to allow the adware to execute. • **Remove**: Click this button to remove the adware. In case, the adware is not removed successfully, the adware is quarantined and will be cleaned in next Boot Time Scan. • **Close**: Click this button to close the message. However, the same message will keep appearing until you take an action.
Repair	Select this option if you want to repair a file. If an adware is found in a file during scan, it repairs the file. If the file cannot be repaired, it is quarantined and will be cleaned in the next Boot Time Scan.
Skip	Select this option if you want to take no action on a file.

Phishing Protection

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

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

Configuring Phishing Protection

To configure Phishing Protection, follow these steps:

1. Open **Quick Heal antivirus**.

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

3. On the Internet & Network screen, turn **Phishing Protection** on.

   Phishing Protection is activated.

   i Phishing Protection is not available in Quick Heal AntiVirus Pro and
   Quick Heal AntiVirus Pro Advanced.

Browser Sandbox

When you browse the Internet, you are clueless about which sites are trusted and verified. Trusted sites are those that publish their identity so that they are established as known entities. However, all untrusted sites are not fake sites or phishing sites. Untrusted websites may be commercial websites, suppliers, sellers, third parties, advertisements, and entertainment websites.

Malicious sites mask their identity to run a covert operation. These sites can hack your confidential credentials, infect your computer, and spread spam messages.

Browser Sandbox keeps you safe from any kind of malicious attacks. Browser Sandbox applies a strict security policy for all untrusted and unverified websites. If you open any downloaded files with Browser Sandbox turned on, such files open in Browser Sandbox to isolate any possible infection.

Configuring Browser Sandbox

To configure Browser Sandbox, follow these steps:

1. Open **Quick Heal antivirus**.

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

3. On the Internet & Network screen, turn **Browser Sandbox** on.

4. From the **Browser Sandbox** security level drop-down list, select the security level.

   The default setting is optimum and ideal for the novice users.

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

   However, this is not a mandatory feature for security and you may turn it off, if you prefer.

6. Select **Open the downloaded documents in sandbox environment*** to open any downloaded documents in isolated environment to prevent spread of virus infection.

7. Under **Control browser access to your personal data**, set the following options as required:

- To protect your confidential data (such as bank statements, pictures, important documents) 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. Therefore, your data is safe from being siphoned off.

- 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 the data cannot be manipulated or modified.

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

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

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

   This helps you clean temporary files.

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

	• Browser Sandbox is not available in Quick Heal AntiVirus Server Edition.
i	• This feature is supported on Internet Explorer, Google Chrome, and Mozilla Firefox browsers only. This feature is not supported on Microsoft Edge browser of Windows 10 operating system.
	• (*) This feature is supported on Windows 7 operating systems and later.

Safe Banking

With online banking, you can check your accounts, pay bills, buy and sell shares, and transfer money between different accounts. For doing these things, you visit a banking website, enter your identity credentials, and carry out the required transactions.

However, while visiting a banking website, you can become a prey to a fake banking website or when you type your credentials, the information can be phished to a fraudster. As a result, you may lose your money.

Safe Banking shields you from all possible situations where your identity or credentials can be compromised. Safe Banking launches your entire banking session in a secure environment that protects your vital data.

Safe Banking has the following features:

- Browser is launched in an isolated environment to prevent zero day malware from infecting the computer.
- Your banking activity is isolated from the Internet threat.
- All types of keystroke recording tools are blocked to safeguard against key logging of confidential data.
- Employs secure DNS to prevent hacking attacks.
- Ensures that you visit only verified and secured websites.

To work in the Safe Banking environment, follow these steps:

1. Setting Safe Banking
2. Launching Safe Banking

Setting Safe Banking

You can use the Safe Banking feature with the default settings. You may also configure the Safe Banking feature for enhanced security according to your requirement.

1. Open **Quick Heal antivirus**.

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

3. Click **Safe Banking**.

4. Select the following options as required:

   - **Protect against DNS based attacks**: Select this option to protect your system from visiting fraudulent websites. You may select a DNS network from the given DNS list or provide an alternate ID. The network connection will be established through the configured network only.

   - **Clipboard Sharing**: Select this option to allow clipboard sharing. You may allow sharing either or both from default desktop to isolated safe banking environment or other way round.

   - **Keyboard Shortcut Preference**: Select this option to create a shortcut key to switch from Safe Banking desktop to Windows desktop. Safe Banking is launched in an isolated environment and hence you cannot access any system or folder from this window. Creating a shortcut key helps you to switch between Safe Banking and Windows desktop.

5. To save your settings, click **Save Changes**.

Launching Safe Banking

You can access Safe Banking feature separately. When you install Quick Heal antivirus on your desktop, Safe Banking is also installed. A shortcut icon to Safe Banking is created on the desktop.

To launch a website in the Safe Banking shield, follow these steps:

1. Click the shortcut icon to **Safe Banking**. Or right-click the Quick Heal icon in the system tray and click **Safe Banking**.

   Safe Banking is launched. You can browse the websites that you want using the supported browsers available on the task bar.

   You can also bookmark a website so that you can browse such a website easily in future.

2. Click **Add Bookmark** and type the URL of the website on the Add Bookmark dialog. Click **Add**.
   You may also add a website to a category so that it is easy to search your preferred website later.

3. Click **View Bookmark** and click the URL that you want to run in the secure browser..

> i
> - Safe Banking is not available in Quick Heal AntiVirus Pro, Quick Heal AntiVirus Pro Advanced, and Quick Heal AntiVirus Server Edition.
> - This feature is supported on Internet Explorer, Google Chrome, and Mozilla Firefox browsers only. This feature is not supported on Microsoft Edge browser of Windows 10 operating system.

News Alert

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

Turning News Alert off

To turn News Alert off, follow these steps:

1. Open **Quick Heal antivirus**.

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

3. On the Internet & Network screen, turn **News Alert** off.

IDS/IPS

With IDS/IPS, your computer remains secure from unwanted intrusion attempts or attacks by the hackers.

Turning IDS/IPS ON

To turn IDS/IPS on, follow these steps:

1. Open **Quick Heal antivirus**.

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

3. On the Internet & Network scree, turn **IDS/IPS** on.

Parental Control

Parental Control is a very effective method to control the Internet access, application access, and computer access by the children and other users. This feature ensures that the children and other users do not visit inappropriate types of Web sites, and can only access the allowed applications so that they are safe from any virus threats. Parents can also limit access to the computer and Internet on a day and time basis.

Important things to do before configuring parental control!

To get the maximum benefits from the Parental Control feature, we recommend that you configure the following options:

First step

Check if you are logged in as an Administrative user to the computer on which you have installed Quick Heal antivirus. In case you are not an administrative user, we recommend that you create an Administrator account and configure it. Do not share the administrative credentials with the users for whom you are creating restricted accounts.

Second step

Create separate Standard accounts (Restricted user) for your children or other users. This way, they will have only limited access to the computer. This also helps you apply different protection policies to different users. The protection policies could include website preferences for each restricted user and a schedule for Internet access.

Third step

Set a password to restrict unauthorized users from modifying the settings or removing Quick Heal antivirus from the computer. To see how to set password to Quick Heal antivirus, see Quick Heal Password Protection.

Configuring Parental Control

To configure Parental Control, follow these steps:

1. Open **Quick Heal antivirus**.

2. On the Quick Heal Dashboard, click **Parental Control**.

   The Parental Control setting details screen appears.

3. Select **Display alert message**, if you want to receive alert message when the users visit a blocked website.

4. Under **Select whom to apply the settings**, select one of the following options:

- **Apply to all users**: Select this option if you want to apply the same setting to all users. If you select this option, the **All Users** option is displayed below.

- **Apply to specific users**: Select this option if you want to apply different settings to different users. If you select the **Apply to specific users** option, a list of all users is displayed below.

5. To configure further settings, click a user available under **Select whom to apply the settings**. Users are displayed based on the options whether you have selected **Apply to all users** or **Apply to specific users**.

   The protection rules screen appears. You can configure any or all of the following options based on your requirement.

   - [Internet Browsing Control](#)

   - [Application Control](#)

   - [PC Access Control](#)

6. After configuration, click **Save Changes** to save your settings.

> *i* Parental Control is available only in Quick Heal Total Security, Quick Heal Total Shield, and Quick Heal Internet Security.

Internet Browsing Control

Internet Browsing Control includes the following options.

Setting Restrict access to particular categories of website

With this feature, you can restrict access to the websites by categories. If you restrict a website category, all the websites under that category will be blocked.

If you want to restrict most of the websites in a category but allow certain websites in that category, you can do so by restricting that category and enlisting such websites in the exclusion list.

To restrict access to the website categories, follow these steps:

1. Open **Quick Heal antivirus**.

2. On the Quick Heal Dashboard, click **Parental Control**. The Parental Control setting details screen appears.

3. Click a user available under **Select whom to apply the settings**. Users are displayed based on the options whether you have selected **Apply to all users** or **Apply to specific users**.

4. On the protection rules screen, select **Internet Browsing Control**.

5. Select **Restrict access to particular categories of website**. A list of website categories appears.

6. On the Web Category screen, select an age group under **Block the website categories based on age group** for restricting access to certain types of websites for your children or other users. If you can select a certain age group, optimum settings will be applied. You may customize the predefined settings for an age group if required. To reset the customized settings of an age group, refresh the same age group. You may revert to the default settings anytime by selecting the Default option.

7. Under **Select access rights for below categories of website**, turn on a website category to allow access to the websites or turn off to deny access. Moreover, the default settings are optimal and ideal for novice users.

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

    ▪ On the Web Category dialogue, click the **Exclude** button.

    ▪ In the **Enter URL** text box, enter the URL of the website that you want to allow users to access and then click the **Add** button. Click **OK**.

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

8. Click **OK** and then confirm your preference. Click **OK**.

9. To save your settings, click **Save Changes**.

Setting Restrict access to particular website

With this feature, you can block access to specific websites. This is helpful when you want to restrict access to certain websites or if you have a shorter list of websites to restrict.

This option is also helpful when a websites does not fall in a selected category or you have restricted a websites category yet a certain website is still accessible.

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

1. Open **Quick Heal antivirus**.

2. On the Quick Heal Dashboard, click **Parental Control**. The Parental Control setting details screen appears.

3. Click a user available under **Select whom to apply the settings**. Users are displayed based on the options whether you have selected **Apply to all users** or **Apply to specific users**.

4. On the protection rules screen, select **Internet Browsing Control**.

5. Select **Restrict access to particular website** and then click the **Block List** button.

6. Click the **Add** button.

7. In the **Enter website** text box, 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 **www.abc.com** and its subdomains, the subdomains such as **mail.abc.com** and **news.abc.com** will also be blocked.

8. Click **OK** and then click **OK**.

9. To save your settings, click **Save Changes**.

Setting Schedule Internet access

With this feature, you can restrict your children to access Internet as per the configured time slot only. As soon as the configured time slot is over, access to the Internet is blocked.

To set Schedule Internet access, follow these steps:

1. Open **Quick Heal antivirus**.

2. On the Quick Heal Dashboard, click **Parental Control**. The Parental Control setting details screen appears.

3. Click a user available under **Select whom to apply the settings**. Users are displayed based on the options whether you have selected **Apply to all users** or **Apply to specific users**.

4. On the protection rules screen, select **Internet Browsing Control**.

5. Select **Schedule Internet access** and then click the **Configure** button.

   The Schedule internet access chart appears.

6. Under **Specify when the user can access the Internet**, select any of the following options:

   - **Always allow access to the Internet**: Select this option if you want to allow other users the Internet access without any restriction.

   - **Allow access to the Internet as per the schedule:** Select this option if you want to set restriction for accessing the Internet.

     The day and time schedule chart is activated.

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

       The selected cells are highlighted which indicates the allowed schedule.

7. Click **OK** and then click **OK**.

8. To save your settings, click **Save Changes**.

Application Control

Application Control includes the following options.

Setting Restrict access to particular categories of applications

With this feature, you can restrict access to the applications by categories. If you restrict an application category, all the applications under that category will be blocked.

If you want to restrict most of the applications in a category but allow certain applications in that category, you can do so by restricting that category and enlisting such applications in the exclusion list.

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

1. Open **Quick Heal antivirus**.

2. On the Quick Heal Dashboard, click **Parental Control**. The Parental Control setting details screen appears.

3. Click a user available under **Select whom to apply the settings**. Users are displayed based on the options whether you have selected **Apply to all users** or **Apply to specific users**.

4. On the protection rules screen, select **Application Control**.

5. Select **Restrict access to particular categories of application** and then click the **Categories** button. A list of application categories appears.

6. Turn on an application category to allow access to the applications in that category or turn off to deny access.

    If you want to exclude certain applications from the blocked category, enlist such an application in the exclusion list.

    ▪ On the Application Category dialog, click the **Exclude** button.

    ▪ Click the **Add** button and browse an application to add to the exclusion list. Click **OK**.

    Similarly, if you want to remove an application from the exclusion list, select the application and click **Remove**. Click **Remove All** to delete all the applications from the exclusion list.

7. Click **OK** and then click **OK**.

8. To save your settings, click **Save Changes**.

The following table describes the categories.

Categories	Description
CD/DVD Applications	Includes applications such as AC3 Filter, Alcohol, Alcohol 120%, AnyDVD, BlindWrite, and so on.
Chat Applications	Includes applications such as Camfrog Video Chat, ManyCam, Skype, and so on.
Download Manager	Includes applications such as Akamai Netsession, aTube Catcher, DamnVid, Download Manager Plus DownloadStudio, and so on.
Email Clients	Includes applications such as FlashMail, Foxmail, Idea!, Lotus Notes Client, Novell Groupwise, The Bat!, Thunderbird, Windows Mail, and so on.
File Sharing	Includes applications such as Ares, BearShare, BitComet, BitTorrent, and

Applications	so on.
Games	Includes applications such as 3D Sniper, 4st Attack, Adrenaline Rush, Agent Combat, Air Hawk, and so on.
Media Players	Includes applications such as AIMP3, ALLPlayer, Audacity, Avidemux, BS Player, and so on.
Miscellaneous	Includes applications such as 2X Client, Advanced SystemCare, AquaSnap, Autoruns, Checksum Control, and so on.
Web Proxy	Includes 602LAN SUITE, Anon Proxy Server, CCProxy, Fast and Secure Gateway to applications such as Internet Freedom, and so on.
USB Modems	Includes applications such as Huawei and so on.
Web Browsers	Includes applications such as America Online, Avant Browser, Comodo Dragon, Firefox, Google Chrome, and so on.

Restrict access to particular application

With this feature, you can block user access to specific applications. This is helpful when you want to restrict user access to certain applications or if you have a shorter list of applications to restrict.

This option is also helpful when an application does not fall in a selected category or you have restricted an application category yet a certain application is still accessible.

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

1. Open **Quick Heal antivirus**.

2. On the Quick Heal Dashboard, click **Parental Control**. The Parental Control setting details screen appears.

3. Click a user available under **Select whom to apply the settings**. Users are displayed based on the options whether you have selected **Apply to all users** or **Apply to specific users**.

4. On the protection rules screen, select **Application Control**.

5. Select **Restrict access to particular application** and then click the **Block List** button.

6. Click the **Add** button and browse an application to block it.

    Similarly, if you want to remove an application from the blocked list, select the application and click **Remove**. Click **Remove All** to delete all the applications from the blocked list.

7. Click **OK** and then click **OK**.

8. To save your settings, click **Save Changes**.

Note: Application Control will function only if Virus Protection is enabled.

PC Access Control

With this feature, you can restrict your children to access your computer or laptop as per the configured time slot only. As soon as the configured time slot is over, the computer will be

locked. However, they can log on with their credentials after the allotted time is over but for forty-five seconds only. They can log in as many times as they prefer, however the computer will be locked every forty-five seconds.

To configure PC Access Control, follow these steps:

1. Open **Quick Heal antivirus**.

2. On the Quick Heal Dashboard, click **Parental Control**. The Parental Control setting details screen appears.

3. Click a user available under **Select whom to apply the settings**. Users are displayed based on the options whether you have selected **Apply to all users** or **Apply to specific users**.

4. On the protection rules screen, select **PC Access Control** and then click the **Configure** button. The Schedule PC access chart appears.

5. Under **Specify when the user can access the PC**, select any of the following options:

   - **Always allow access to the PC**: Select this option if you want to allow users to access your computer without any restriction.

   - **Allow access to PC as per the schedule:** Select this option if you want to set a time-slot for accessing the computer.

     o Daily access time limit: Lets you allot time on hourly basis. Users can access the computer for the allowed time duration at any point of time during a day.

     o Daily access time-slots (clock time): Select the cells for the days and times during which you want to allow access to the computer. Users can access the computer only during the allowed time window.

     The selected cells are highlighted which indicates the allowed schedule.

6. Click **OK** and then click **OK**.

7. To save your settings, click **Save Changes**.

Creating an Administrator account

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

To create an Administrators account, follow these steps:

1. Click **Start > Control Panel**.

2. Click **User Accounts**.

3. Your account type is displayed below your user name. Check if your account type is Administrator. If your account type is not Administrator, you need to change it to Administrator Account.

Quick Heal Password Protection

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

To know about how to enable password protection of Quick Heal antivirus, see Password Protection.

Creating restricted user accounts

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

To create restricted user accounts, follow these steps:

For Microsoft Windows XP operating system:

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

For Microsoft Windows Vista/Windows 7 operating system:

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

External Drives & Devices

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

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

Autorun Protection

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

Configuring Autorun Protection

To configure Autorun Protection, follow these steps:

1. Open **Quick Heal antivirus**.

2. On the Quick Heal Dashboard, click **External Drives & Devices**.

3. On the External Drives & Devices screen, turn **Autorun Protection** on.

   Autorun Protection is activated.

Scan External Drives

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

Configuring Scan External Drives

To configure Scan External Drives, follow these steps:

1. Open **Quick Heal antivirus**.

2. On the Quick Heal Dashboard, click **External Drives & Devices**.

3. On the External Drives & Devices screen, turn **Scan External Drives** on.

   Scan External Drives is activated.

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

5. Select one of the following options:

   - **Scan files on the root of the drive only**: Select this option if you want to scan the files on the root of the drive only. The files within the folders on the root drive are skipped. This scan takes little time but is less safe. However, this option is selected by default.

   - **Scan full drive**: Select this option if you want to scan all the files on the USB-based drive. This scan takes time but is safer.

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

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

Data Theft Protection

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

Configuring Data Theft Protection

To configure Data Theft Protection, follow these steps:

1. Open **Quick Heal antivirus**.

2. On the Quick Heal Dashboard, click **External Drives & Devices**.

3. On the External Drives & Devices screen, turn **Data Theft Protection** on.

   Data Theft Protection is activated.

4. Click **Data Theft Protection** and do any of the following options:

   - **Read only and no write access to external drives:** Allows transfer of data from the USB drives and CD/DVD devices to the system but not vice versa . However, this option is selected by default.

   - **Block complete access to external drives:** Blocks transfer of data between the system and all external devices.

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

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

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

> **i** Data Theft Protection is not available in Quick Heal AntiVirus Pro, Quick Heal Internet Security, and Quick Heal Internet Security Essentials. .

Scan Windows Mobile

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

Configuring Scan Windows Mobile

To configure Scan Windows Mobile, follow these steps:

1. Open **Quick Heal antivirus**.

2. On the Quick Heal Dashboard, click **External Drives & Devices**.

3. On the External Drives & Devices screen, turn **Scan Windows Mobile** on.

   Scan Windows Mobile is activated.

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

Quick Access Features

Quick Access Features provides quick access to some of the important features such as Scan options and PCTuner[1] on Dashboard itself. It also displays latest news from Quick Heal.

The Quick Heal Secure Browse shortcut icon on your desktop helps you launch your default browser in Sandbox for secure browsing. This helps you browse securely even if you have kept Browser Sandbox[2] turned off. Safe Banking[3] can be launched using the desktop shortcut icon.

> (1) PCTuner is available only in Quick Heal Total Security and Quick Heal Total Shield.
> (2) Browser Sandbox is not available in Quick Heal AntiVirus Server Edition.
> (3) Safe Banking is not available in Quick Heal AntiVirus Pro, Quick Heal AntiVirus Pro Advanced, and Quick Heal AntiVirus Server Edition.

Scan

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

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

Performing Full System Scan

This feature helps you initiate a complete scan of all boot records, drives, folders, files, and vulnerabilities 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 Dashboard, select **Scan > Full System Scan**.

   The scan starts.

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

Performing Custom Scan

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

To scan specific folders, follow these steps:

1. Open **Quick Heal antivirus**.

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

3. On the Custom Scan screen, a list of items is displayed in the Scan Item list if you have added any items to scan. If you have not added any item before or you want to scan some new items, click **Add** to add the scan items.

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

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

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

    The scan begins.

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

Performing Memory Scan

To perform a memory scan, follow these steps:

1. Open **Quick Heal antivirus**.

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

To set Boot Time Scan, follow these steps:

1. Open **Quick Heal antivirus**.

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

   Boot Time Scan has the following options:

   ▪ Quick Scan: Scans only system pre-defined locations that are at high risk to viruses.

   ▪ Full System Scan: Scans the entire system. This may be time consuming.

3. Click **Yes**.

4. To restart the system for scanning immediately, click **Yes**. To scan the system later, click **No**.

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

Performing Vulnerability Scan

Vulnerabilities are the flaws present in the operating system settings and applications that can be misused by hackers. If you identify these vulnerabilities in time, you can fix or patch them to make your system secure.

Vulnerability Scan in the new version of Quick Heal antivirus brings to you a comprehensive preventive detection method. It identifies vulnerabilities in the operating system settings and applications so that you can fix or patch the vulnerabilities before your system is compromised.

To run Vulnerability Scan, follow these steps:

1. Open **Quick Heal antivirus**.

2. On the Quick Heal Dashboard, select **Scan > Vulnerability Scan**.

   Vulnerability Scan checks for vulnerabilities of the following types:

   Vulnerable System Settings: Detects vulnerable operating system settings that could lead to security threats.

   Vulnerabilities found in Applications: Detects vulnerabilities present in the applications that are installed on your computer.

   When the scan is complete, a summary of the scan is displayed. If you want to see the detailed report on the detected vulnerabilities, click a category from **Vulnerable System Settings** and **Vulnerabilities found in Applications**.

When scan is complete, a report on vulnerabilities is displayed with following details.

Report types	Description
Vulnerable System Settings	Displays detected vulnerabilities in the operating system settings. To see the report in detail, click **Vulnerable System Settings** on the Vulnerability Scan screen. All the vulnerabilities detected in the system settings are listed along with their fixes. You can apply fixes to the vulnerabilities by clicking **Fix it** under **Action**.
Vulnerabilities found in Applications	Displays detected vulnerabilities in the applications installed on your computer. To see the report in detail, click **Vulnerabilities found in Applications** on the Vulnerability Scan screen. All the vulnerabilities are listed along with their links to the patches. To apply the patches, click **Yes** under **Patch Available**. You will be redirected to the relevant websites from where you can download the patches and apply them. If no patch is available, you may consider upgrading the application or contact the support of the application vendor.

> *i* Vulnerability Scan is not available in Quick Heal AntiVirus Pro and Quick Heal AntiVirus Pro Advanced.

Performing Mobile Scan

With PC2Mobile Scan, you can scan a wide range of Android, iOS, and Windows mobile phones. Before scanning your mobiles, see the following conditions.

- Mobile Scan feature is supported on Microsoft Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, and Windows 10 operating systems.
  (Note: Mobile Scan is not supported on Windows XP for iOS devices.)

- For Windows Mobile based devices (Windows Mobile version 3.0 and earlier to version 7.0), you should have Microsoft Active Sync 4.5 or later for Windows XP (32-bit); and Windows Mobile Device Center for Windows Vista, Windows 7, Windows 8, Windows 8.1, or Windows 10 operating system.

- Install PCSuite and the device driver on your computer. Once your device gets connected to PCSuite, exit from PCSuite.

- For scanning Android devices, ensure that the device is connected via USB cable, and **USB debugging** and **Stay awake** options must be enabled.

- For iPhone (Mac) devices, iTunes must be installed on your system.

Scanning mobiles through PC2Mobile Scan

With PC2Mobile Scan, you can scan mobiles in the following way:

1. Open **Quick Heal antivirus**.

2. On the Quick Heal Dashboard, click **Scan** and then select **Mobile Scan**.

3. Connect a mobile phone to your PC using USB cable.

4. Click the **Search Mobile** button.

5. Click the **Start Search** button.

   A search for the model of the connected mobile phone is carried out.

6. Select the mobile from the list. Click **Start Scan**.

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

   $\boxed{i}$ The Mobile Scan feature is available only in Quick Heal Total Security.

Quick Heal PCTuner

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

To know more about PCTuner, see Quick Heal PCTuner Dashboard.

News

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

Quick Heal Menus

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

Settings

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

Settings includes the following features.

Import and Export Settings

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

Importing and Exporting the Quick Heal antivirus Settings

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

1. Open **Quick Heal antivirus**.
2. On the Quick Heal Dashboard, click **Settings**.
3. On the Settings screen, click the **Import/Export** tab.
4. On the Import/Export Settings dialog, select either of the following options.

   - **Export settings to a file**: Helps you export the current settings to a .dat file.

   - **Import settings from a file**: Helps you import the settings from a .dat file.

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

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

> *i* • The settings can be imported from the same product flavor and the same version only. For example, the settings of Quick Heal AntiVirus Pro version 17.00 can be imported to Quick Heal AntiVirus Pro version 17.00 only.
> • The settings of the following features cannot be exported or imported:
>   ▪ Scheduled Scans
>   ▪ Password Protection

Automatic Update

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

Configuring Automatic Update

To configure Automatic Update, follow these steps:

1. Open **Quick Heal antivirus**.

2. On the Quick Heal Dashboard, click **Settings**.

3. On the Settings screen, 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 the following options:

   ▪ **Download from Internet** – Helps you download the updates to your system from the Internet.

   ▪ **Pick update files from the specified path** –Helps you pick the updates from a local folder or a network folder.

   ▪ **Copy update files to specified location** – Helps you save a copy of the updates to your local folder or network folder.

   ▪ Check for the latest version of Quick Heal antivirus:

     o **Notify me when upgrade is available**: Select this option if you want to be notified when there is a new upgrade available.

o **Automatically download the upgrade**: Select this option if you want a new upgrade when available get downloaded automatically on your system. Then you need to install it to upgrade your current version.

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

Selecting Update Mode

Quick Heal antivirus provides multiple update modes that you can select according to your convenience.

Pick update files from specified path

This option is best suitable if Quick Heal antivirus is installed on multiple computers. You can download the updates on a single computer and set a path on other computers to pick the updates from the destination computer. The other computers will take the updates from the specified path as the new updates are available automatically. This helps you save the Internet bandwidth.

Copy update files to specified location

This option is suitable if you are working offline. You can download the updates at a specific location or on other computer and share the updates with pen drive or other multimedia. If this option is selected and the location of the system is specified, the complete update process takes place automatically.

Note: Automatic Update works on compatible systems. Your computers should have the same Quick Heal antivirus product name, product version, and architecture such as 32-bit or 64-bit operating system installed to process the update successfully.

Internet Settings

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

The following Quick Heal antivirus modules require these changes.

- Registration Wizard
- Quick Update
- Messenger

Configuring Internet Settings

1. Open **Quick Heal antivirus**.

2. On the Quick Heal Dashboard, click **Settings**.

3. On the Settings screen, click **Internet Settings**.

4. Select **Enable proxy settings**.

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

5. In **Type** list, select the proxy type from HTTP, SOCKS V4, SOCKS V5 based on your preference.

6. In the **Server** text box, enter the IP address of the proxy server or domain.

7. In the **Port** text box, enter the port number of the proxy server.

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

8. Enter your user name and password credentials.

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

Registry Restore

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

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

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

Configuring Registry Restore

1. Open **Quick Heal antivirus**.

2. On the Quick Heal Dashboard, click **Settings**.

3. On the Settings screen, click **Registry Restore**.

4. Select **Restore critical system registry areas** to restore the critical system registry during the scan. Critical System Registry areas are generally changed by malware to perform certain task automatically or to avoid detection or modification by system applications such as Disabling Task Manager, and Disabling Registry Editor.

5. Select **Repair malicious registry entries** to scan system registry for malware related entries. Malware and its remains are repaired automatically during the scan.

Self Protection

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

Configuring Self Protection

1. Open **Quick Heal antivirus**.

2. On the Quick Heal Dashboard, click **Settings**.

3. On the Settings screen, turn **Self Protection** on.

   However, Self Protection is turned on by default.

Password Protection

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

Safe Mode Protection

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

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

Configuring Password Protection

To configure Password Protection, follow these steps:

1. Open **Quick Heal antivirus**.

2. On the Quick Heal Dashboard, click **Settings**.

3. On the Settings screen, turn **Password Protection** on.

   The Password Protection settings screen appears.

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

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

5. To enable safe mode protection, select **Enable Safe mode protection**.

6. Click **Save Changes**.

Report Settings

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

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

Configuring Report Settings

To configure Report Settings, follow these steps:

1. Open **Quick Heal antivirus**.

2. On the Quick Heal Dashboard, click **Settings**.

3. On the Settings screen, click **Report Settings**.

    The Report Settings screen appears.

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

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

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

Report Virus Statistics

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

Configuring Report Virus Statistics

To configure Report Virus Statistics, follow these steps:

1. Open **Quick Heal antivirus**.

2. On the Quick Heal Dashboard, click **Settings**.

3. On the Settings screen, turn **Report Virus Statistics** on.

    The Report Virus Statistics is activated.

Remotely Manage Quick Heal

To manage Quick Heal antivirus on your device through Quick Heal RDM, it is important that you always keep the option Remotely Manage Quick Heal enabled. However, you can disable this option if you do not want to control the device through the web portal.

To enable Remotely Manage Quick Heal, follow these steps:

1. Open **Quick Heal antivirus**.

2. On the Quick Heal Dashboard, click **Settings**.

3. Turn **Remotely Manage Quick Heal** on.

If you have not added any device yet, the Add your Quick Heal product page appears. This page displays the description about how to add a device along with the link to the Quick Heal RDM portal.

Quick Heal Remote Device Management

Quick Heal Remote Device Management or Quick Heal RDM is a cloud-based web portal that provides you a comprehensive monitoring facility to manage and control computers and laptops remotely.

With Quick Heal RDM, you can view certain security status of the devices, license history and license details, and renew the licenses.

To take advantage of Quick Heal RDM, follow these steps:

1. Creating an account with the Quick Heal RDM web portal
2. Adding devices to the Quick Heal RDM web portal

Creating an account with the Quick Heal RDM web portal

Before you create an account with Quick Heal RDM portal, you must activate Quick Heal antivirus on your device with a valid product key. To know about how to activate Quick Heal antivirus, see Registration of Quick Heal.

1. Once Quick Heal antivirus is registered on your device, the Quick Heal RDM sign-up screen appears. To get the sign-up invite, enter your email address and then click **Next**.

   An email about how to activate the Quick Heal RDM account is sent to your email address.

2. Check your email and click the **Activate** button or copy the given link in your browser.

   You are redirected to the Set Password page of Quick Heal RDM portal.

3. Set your password and then click **Save**.

   Your account with the Quick Heal RDM portal is created successfully. To manage a device, you must add the device in the Quick Heal RDM portal first.

Signing up with the Quick Heal RDM web portal

You can create an account with Quick Heal RDM directly from the web portal also.

To sign up with Quick Heal RDM, follow these steps:

1. Visit Quick Heal RDM on the following website: https://mydevice.quickheal.com.

2. In the upper right area, click the **Sign up** button.

3. Enter your username or email address, valid mobile number, and product key.

4. Enter the correct verification code.

   Read the License Agreement and Privacy Policy documents carefully.

5. Select the I agree to the Quick Heal License Agreement and Privacy Policy option.

6. Click **Sign up**.

   An email about how to activate the Quick Heal RDM account is sent to your email address.

7. Check your email and click the **Activate** button or copy the link in your browser.

   You are redirected to the set password page of Quick Heal RDM.

8. Set your password and then click **Save**.

   Your account with the Quick Heal RDM portal is created successfully. To manage a device, you must add the device in the Quick Heal RDM portal first.

Signing up with the Quick Heal RDM web portal with Google account

You can create an account with the Quick Heal RDM portal with your existing Google account also.

To sign up with your Google account, follow these steps:

1. Click the **Sign in** with Google button.

2. Enter your Username and Password of your existing Google account.

   Read the service agreement and privacy policies carefully.

3. Click **Accept**.

4. On the Create New Account page, enter your valid mobile number and Product Key.

5. Enter the correct verification code.

   Read the License Agreement and Privacy Policy documents carefully.

6. Select the **I agree to the Quick Heal License Agreement and Privacy Policy** option.

7. Click **Sign up**.

   Your account with the Quick Heal RDM portal is created successfully. From now onwards, you can log on to your Quick Heal RDM account using your existing Google account and manage your device.

   On first log on to the Quick Heal RDM, you need to configure the Add Device page. To know how to add a device, see Adding a device to Quick Heal RDM.

Adding devices to the Quick Heal RDM web portal

To manage your devices remotely, you need to add your devices in the Quick Heal RDM. On first log on to the Quick Heal RDM portal after creating an account with it, you are prompted to add devices.

To add a device, follow these steps:

1. Visit Quick Heal RDM Portal on the following website: https://mydevice.quickheal.com.

2. Log on to the Quick Heal RDM portal.

The Add Device page appears.

3. Type a name to the device and enter the product key.

   You can give any name to the device that you prefer.

4. Click **Add**.

   A One Time Password (OTP) is generated. To get OTP, go to your desktop application and do the following:

   i. Open **Quick Heal antivirus** on your desktop and click **Settings**.

   ii. Turn **Remotely Manage Quick Heal** on.

       A validation is carried out and OTP is displayed on the Quick Heal Remote Device Wizard.

5. Enter this OTP on the Quick Heal RDM web portal and click **Submit**.

   The device is added successfully.

6. Once the OTP is validated on the portal, click **Next** on the Quick Heal Remote Device Wizard on the desktop.

7. To close the wizard, click **OK**.

Restore Default Settings

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

Restoring Default Settings

To restore default settings, follow these steps:

1. Open **Quick Heal antivirus**.

2. On the Quick Heal Dashboard, click **Settings**.

   The Settings details screen appears.

3. On the Restore Default Settings, click the **Default All** button.

   Your Quick Heal antivirus is reverted to the default settings.

Tools

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

Tools includes the following features.

Hijack Restore

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

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

Using Hijack Restore

To use Hijack Restore, follow these steps:

1. Open **Quick Heal antivirus**.

2. On the Quick Heal Dashboard, click **Tools**.

    The Tools details screen appears.

3. Under Cleaning & Restore Tools, click **Hijack Restore**.

4. On the Hijack Restore screen, select **Check All** to select all the browser settings in the list.

5. Select **Restore default host file** to restore the default host file.

6. Select **Restore important system settings** to restore important system settings.

7. To initiate restoring your settings, click **Restore Now**.

Restore Default Host File

The default host file includes the following options:

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

This feature includes the following options.

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 screen are as follows:

Restore Now	Helps you initiate restoring the settings that you selected.
Undo	Helps you undo your settings done on the current screen. 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

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

Using Track Cleaner

To use Track Cleaner, follow these steps:

1. Open **Quick Heal antivirus**.

2. On the Quick Heal Dashboard, click **Tools**.

   The Tools details screen appears.

3. Under Cleaning & Restore Tools, click **Track Cleaner**.

   The Track Cleaner screen appears. This displays a list of all the programs opened recently.

4. Select the programs whose traces you want to remove or select **Check All** to select all the programs in the list.

5. To initiate cleaning, click **Start Cleaning**.

6. To close the Track Cleaner window, click **Close**.

Anti-Rootkit

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

However, it is recommended that Quick Heal Anti-Rootkit should be used by a person who has good knowledge of the operating system or with the help of Quick Heal Technical Support engineer. Improper usage of this program could result in unstable system.

Using Quick Heal Anti-Rootkit

To use Anti-Rootkit, follow these steps:

1. Open **Quick Heal antivirus**.

2. On the Quick Heal Dashboard, click **Tools**.

    The Tools details screen appears.

3. Under Cleaning & Restore Tools, click **Anti-Rootkit**.

    A message appears that recommends you to close all other applications before launching Anti-Rootkit.

4. In the left pane on the Anti-Rootkit screen, click the **Start Scan** button.

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

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

5. Select the appropriate action against each threat displayed. For example, you can terminate the rootkit Process, rename the rootkit Registry entry/Files and Folders.

After taking the action, you should restart your system so that rootkit cleaning takes place.

Stop Scanning	Helps you stop the scan while the scan is under way.
Close	Helps you close the Anti-Rootkit window. If you choose to close the Anti-Rootkit window while scanning is in progress, it will prompt you to stop the scan first.
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 configure what items to scan.

Configuring Quick Heal Anti-Rootkit Settings

1. Open **Quick Heal Anti-Rootkit**.

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

    The Tools details screen appears.

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

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 options: **Detect Hidden Process** – scans the hidden processes running in the system. **Detect Hidden Registry Items** – scans the hidden items in Windows Registry. **Detect Hidden files and folders** – scans the hidden files and folders in the system and executable ADS (Alternate Data Streams). You can further choose from the following options: • 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

Alternate Data Streams or ADS allows the data to be stored in hidden formats that are linked to a normal visible file. Streams are not limited in size and there can be more than one stream linked to a normal file. ADS is a security risk because streams are almost completely hidden.

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

Scanning Results and Cleaning Rootkits

1. Open **Quick Heal Anti-Rootkit**.

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

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

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

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

Tabs that appear on the Scan Results screen

Process	After the scan is complete, Quick Heal Anti-Rootkit will detect and display a list of hidden processes. You can select the Process tab for termination, but ensure that the list of processes does not include any known trusted process. Quick Heal Anti-Rootkit also displays a summary of total number of processes scanned and hidden processes detected.
Terminating Hidden Process	After selecting the list of processes to close, click the Terminate button. If a process is successfully terminated, then its PID (Process Identifier) field will show n/a and process name is appended by Terminated. All terminated Processes will be renamed after a restart.

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

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

	Queued.

Cleaning Rootkits through Quick Heal Emergency Disk

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

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

Step 1

To create Quick Heal Emergency Disk, follow the link Create Emergency Disk, p - 77.

Step 2

1. Open **Quick Heal Anti-Rootkit**.

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

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

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

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

Step 3

1. Boot your system using **Quick Heal Emergency Disk**.

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

Creating Emergency Disk

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

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

To create an Emergency Disk, follow these steps:

1. Open **Quick Heal antivirus**.

2. On the Quick Heal Dashboard, click **Tools**.

   The Tools details screen appears.

3. Under Cleaning & Restore Tools, click **Create Emergency Disk**.

4. On the Create Emergency Disk screen, click the link and download the required package for emergency tool.

5. Extract the downloaded package on your system. For example: `c:\my documents\qhemgpkg`.

6. Provide the extracted package path, and click **Next**.

7. To create Emergency Disk, select any one of the options that are displayed on the screen. For example, select either Create Emergency USB disk or Create Emergency CD/DVD.

   Note: Creating Emergency Disk using CD/DVD is not supported on Microsoft Windows 2003 and earlier versions. However, you can create Emergency Disk on USB drives.

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.
- While using a USB device, rewritable CD/DVD, take a backup as the device will be formatted.
- To boot the system from either USB or CD/DVD, you have to set Boot sequence in BIOS.
- Once the scan is complete, you must remove the Emergency USB disk or CD/DVD before restarting the computer, otherwise it will again boot in the boot shell.

Using Emergency Disk

1. Insert **Emergency Disk** in your CD/DVD/USB drive.

2. Restart your system.

3. Emergency Disk starts scanning all the drives automatically. It will disinfect the infection, if found.

4. Restart your system.

Launch AntiMalware

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

Launching Quick Heal AntiMalware

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

- Select **Start > Programs > Quick Heal antivirus > Quick Heal AntiMalware**.
- Right-click the Quick Heal Virus Protection icon in the Windows system tray and select Launch Antimalware.
- Open **Quick Heal antivirus** and click **Tools.** Under **Cleaning & Restore Tools**, click **Launch AntiMalware**.

Using Quick Heal AntiMalware

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

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

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

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 to 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. The feature **Set System Restore point before cleaning** is not available in Windows 2000 operating system.
Details	Helps you redirect to the Web site of Quick Heal.

View Quarantine Files

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

Launching Quarantine Files

1. Open **Quick Heal antivirus**.

2. On the Quick Heal Dashboard, click **Tools**.

   The Tools details screen appears.

3. Under Cleaning & Restore Tools, click **View Quarantine**.

   A list of all quarantined and backed up files is displayed.

You can perform the following tasks on the Quarantine dialog:

Add	Helps you quarantine a file manually.
Remove	Helps you remove a quarantined and backed up file.
Restore	Helps you restore a quarantined file to its original location.
	When you find a quarantined file trustworthy and try to restore it, an option for adding the file to the exclusion list appears. You can add the file to the exclusion list so that the same file is not treated as suspected and quarantined again.
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 the Quick Heal research labs, you are prompted to provide your email address and a reason for submitting the file. The reasons include the following ones:

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 antivirus as a malicious file.

USB Drive Protection

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

To configure USB Drive Protection, follow these steps:

1. Open **Quick Heal antivirus**.

2. On the Quick Heal Dashboard, click **Tools**.

   The Tools details screen appears.

3. Under Preventive Tools, click **USB Drive Protection**.

4. In the Select a removable drive list, all the removable drives plugged into your system are listed. Select the drive and click the Secure Removable Drive button.

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

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

System Explorer

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

To use system explorer, follow these steps:

1. Open **Quick Heal antivirus**.

2. On the Quick Heal Dashboard, click **Tools**.

   The Tools details screen appears.

3. Under Diagnostic Tools, click **System Explorer**.

Windows Spy

This feature helps you find more information about an application or process. Sometimes we keep getting dialog boxes or messages that are actually shown by spyware or some malware that we are unable to locate. In such a case, this tool can be used to find out more information about the application by dragging the target on to the dialog or window that appears on the screen. This tool will provide following information about the dialog or a window.

- Application Path
- 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 Dashboard, click **Tools**.

   The Tools details screen appears.

3. Under Diagnostic Tools, click **Windows Spy**.

4. Drag the mouse pointer on the application.

   A window will be opened displaying the above mentioned information.

5. If you want to terminate that application or window, click **Kill Process**.

Exclude File Extensions

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

Creating Exclusion List for Virus Protection

1. Open **Quick Heal antivirus**.

2. On the Quick Heal Dashboard, click **Tools**.

   The Tools details screen appears.

3. Under Diagnostic Tools, click **Exclude File Extensions**.

4. Enter the file extension that needs to be excluded from the Virus Protection scan and click **Add**.

5. If the added extension is incorrect, then select the extension added in the list and click **Remove** to delete it.

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

Reports

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

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

- Scanner
- Virus Protection
- Email Protection
- Scan Scheduler
- Behavior Detection[1]
- Quick Update
- Memory Scan
- Phishing Protection[2]
- Registry Restore
- Boot Time Scanner

- AntiMalware Scan
- Firewall Protection
- Parental Control[3]
- IDS & IPS
- Browsing Protection
- PC2Mobile Scan[4]
- Vulnerability Scan[5]
- Safe Banking[6]
- Anti-Keylogger

> (1) Behavior Detection is not available in Quick Heal AntiVirus Server Edition.
> (2) Phishing Protection is not available in Quick Heal AntiVirus Pro and Quick Heal AntiVirus Pro Advanced.
> (3) Parental Control is available only in Quick Heal Total Security, Quick Heal Total Shield, and Quick Heal Internet Security.

(4) PC2Mobile Scan is available only in Quick Heal Total Security.

(5) Vulnerability Scan is not available in Quick Heal AntiVirus Pro and Quick Heal AntiVirus Pro Advanced.

(6) Safe Banking is not available in Quick Heal AntiVirus Pro, Quick Heal AntiVirus Pro Advanced, and Quick Heal AntiVirus Server Edition.

Viewing Reports

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

1. Open **Quick Heal antivirus**.

2. On the Quick Heal Dashboard, click **Reports**.

   A Reports list appears.

3. In the **Reports for** list, click a feature to view its report.

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

Button	Action
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 options:

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, see Reports.

Help

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

The Help feature includes the following options.

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

- **Submit System Information**: Helps you submit information of your system to Quick Heal for analysis.

  For details on how to submit System Information, see System Information.

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

  For more details on Support, see Technical Support.

- **About**: The About section of Quick Heal antivirus includes the following information:

  - Quick Heal Version

  - License details

  - License validity

  - Update Now option

The following buttons are also available in the About section:

Renew Now License Details	Helps you renew your existing subscription.
	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	Helps you update virus database of Quick Heal.

System Information

Quick Heal 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 the Running processes, Registry, System files like Config.Sys, Autoexec.bat, and system and application event logs.
To get Quick Heal 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 it 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 malware 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 Dashboard, select **Help > Submit System Information**.

   The System Information wizard opens.

2. Click **Next** to continue.

3. Select a reason for submitting the system information. If you are suspecting new malware 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.

Updating Quick Heal & Cleaning Viruses

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

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

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

Some important facts about the Quick Heal antivirus updates are:

- All the Quick Heal antivirus updates are complete updates including Definition File Update and Engine Updates.

- All the Quick Heal antivirus security updates also upgrade your version whenever required, thus making the new features and technology available for your protection.

- Quick Heal Update is a single step upgrade process.

You can update Quick Heal antivirus manually whenever necessary in any of the following ways:

Updating Quick Heal from Internet

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

To update Quick Heal antivirus, follow these steps:

1. Select **Start > Programs > Quick Heal antivirus > Quick Update**.

2. Follow the instructions and click the **Next** button.

3. Select **Download from Quick Heal 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 website, downloads the appropriate upgrade files for your copy of Quick Heal antivirus, and applies it thereafter to your copy, thus updating it to the latest available update file.

Updating Quick Heal 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 antivirus. You can download the latest definition files from the website of Quick Heal from http://www.quickheal.com/update.

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

1. Select **Start > Programs > Quick Heal antivirus > Quick Update**.

2. Follow the instructions and click the **Next** button.

3. Select **Pick from specified path**.

4. Click **File** to locate the definition file. Select the update file.

5. Click **Next**.

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

Update Guidelines for Network Environment

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

1. Setup one computer (may be the server) as the master update machine. Suppose server name is SERVER.

2. Make **QHUPD** folder in any location. For example: **C:\QHUPD**. Assign Read-Only sharing rights to this folder.

3. Select **Start > Programs > Quick Heal antivirus > Quick Heal antivirus**.

4. On Dashboard, select **Settings > Automatic Update**.

5. Select **Copy update files to specified location**.

6. Click **Browse** and locate the **QHUPD** folder. Click **OK**.

7. Click **Save Changes** to save this setting.

8. On all user computers within the network launch **Quick Heal antivirus**.

9. Under **Settings**, go to the **Automatic Update** page.

10. Select **Pick update files from specified path**.

11. Click **Browse**.

12. Locate the `SERVER\QHUPD` folder from Network Neighborhood. Alternatively you can type the path as `\\SERVER\QHUPD`.

13. Click **Save Changes** to save the settings.

Cleaning Viruses

Quick Heal antivirus warns you of a virus infection when:

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

Cleaning viruses encountered during scanning

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

Scanning Options

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

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 computers (if connected to a network) and doing malicious activity.

Whenever a virus is detected during memory scan, a Boot Time Scan is automatically scheduled to run the next time you boot your system. Boot Time Scan will scan and clean all drives

including NTFS partitions before the desktop is completely loaded. It will detect and clean even the most typical Rootkits, spywares, special purpose Trojans, and loggers.

Restart required during cleaning for some malwares

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

Cleaning of Boot/Partition viruses

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

Responding to virus found alerts from Virus Protection

Virus Protection of Quick Heal antivirus 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 Virus Protection.

Quick Heal PCTuner

Quick Heal PCTuner is a tool 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.

> *i* **PCTuner** is available only in Quick Heal Total Security and Quick Heal Total Shield.

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 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
Tuneup	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

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

- 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.

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

Tuneup

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

Auto Tuneup

Auto Tuneup performs **Disk Cleanup**, **Registry Cleanup**, **Traces Cleanup**, and **Defragmenter**. It is ideal for novice users, and for users who do not want to waste time by performing individual Cleanup activity. Only the items deleted by Disk Cleanup and Registry Cleanup can be recovered.

Customizing Auto Tuneup

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

1. Select **Tuneup > Settings**.

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

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

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

3. Click **Apply** to save the new settings.

4. Click **Close** to exit without saving the settings.

Performing Auto Tuneup

To execute Auto Tuneup, follow these steps:

1. Select **Tuneup > Auto Tuneup**.

2. Click **Settings** if you want to customize Auto Tuneup as mentioned in the previous section.

3. Click **Start** to begin Auto Tuneup.

4. Click **Stop** if you want to halt the Auto Tuneup; else click **Close** after completion of Auto Tuneup.

Disk Cleanup

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

Performing Disk Cleanup

To execute Disk Cleanup, follow these steps:

1. Select **Tuneup > Disk Cleanup**.

2. Click **Settings** if you want to Customize Disk Cleanup.

3. Click **Start**.

   A list with file locations and its junk category appears.

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

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

5. Clear the locations that need to be skipped by Disk Cleanup.

   There are four other fields that display the following information:

- **Files Found**: The total number of files found by Disk Cleanup.

- **Total Size**: The size of the total number of files found by Disk Cleanup.

- **Files Selected**: The number of files selected for deletion.

- **Selected File Size**: The size of the number of files selected for deletion.

6. Click **Remove Files** to remove the files.

7. Click **Close** to exit Disk Cleanup.

Registry Cleanup

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

Performing Registry Cleanup

To execute Registry Cleanup, follow these steps:

1. Select **Tuneup > Registry Cleanup**.

2. Click **Settings** if you want to Customize Registry Cleanup as mentioned in the previous section.

3. Click **Start**.

   A list with registry entries and their path appears.

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

   Each registry entry will be preceded by a check box. All registry entries are selected by default.

5. Clear the registry entries that need to be skipped by Registry Cleanup.

6. 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.

7. Click **Remove Entries** to remove the files.

8. Click **Close** to exit Registry Cleanup.

Traces Cleanup

This feature removes traces from the Internet history and MRU (Most Recently Used) list of various applications. It safely deletes history, cleans the cookies, cache, auto-complete forms and passwords. Traces such as auto complete entries and saved passwords need to be deleted to ensure that user privacy is not breached. It also erases the traces from popular application

programs such as Microsoft Office applications, Adobe Acrobat Reader, Media Player, WinZip, WinRAR and traces such as Browser Cookies, and Saved Passwords.

Performing Traces Cleanup

To execute Traces Cleanup, follow these steps:

1. Select **Tuneup > Traces Cleanup**.

2. Click **Settings** if you want to Customize Traces Cleanup as mentioned in the previous section.

3. Click **Start**.

   A list with applications containing traces appears.

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

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

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

6. 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.

7. Click **Clean Items** to remove traces from the applications listed.

8. Click **Close** to exit Traces Cleanup.

Defragmenter

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

Using Defragmenter

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

1. Select **Tuneup > Defragmenter**.

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

2. Select **Defragment at next boot** to perform defragmentation the next time you start the system; else select **Defragment at every boot** to perform defragmentation every time you start the system.

3. **Defragment system paging file (Virtual Memory)** and **Defragment Windows Registry** are not selected by default. You can select any of these two or both for the Defragmenter to perform. We recommend that you keep these options selected.

4. Click the **Apply** button to save these settings, or else click **Close** to exit without saving.

Scheduler

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

Customizing Scheduler

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

1. Select **Tuneup >Scheduler**.

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

2. 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

3. To schedule a new tuneup activity, click **New**.

   The Configure Tuneup Schedule screen appears.

4. 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.

5. Clear the items that need to be skipped by Scheduler feature.

6. **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.

7. Enter **User Name** and **Password**.

8. Click **Apply** to save the new settings or else click **Close** to exit without saving the settings.

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

Settings

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

Customizing Disk Cleanup

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

1. Select **Tuneup > Settings**.

   The Tuneup Settings screen appears.

2. Click **Disk Settings**.

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

3. Clear the items that need to be skipped by Disk Cleanup feature.

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

5. Click **Apply** to save the new settings or else click **Close** to exit without saving the settings.

Customizing Registry Cleanup

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

1. Select **Tuneup >Settings**.

   The Tuneup Settings screen appears.

2. Click **Registry Settings**.

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

3. Clear the items that need to be skipped by Registry Cleanup feature.

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

5. Click **Apply** to save the new settings or else click **Close** to exit without saving the settings.

Customizing Traces Cleanup

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

1. Select **Tuneup > Settings**.

   The Tuneup Settings screen appears.

2. Click **Traces Settings**.

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

3. Clear the items that need to be skipped by Traces Cleanup feature.

4. **Take backup before deleting the items** is selected. If this option is not selected, Registry Cleanup will delete all the items without taking the backup. We recommend that you keep it selected.

5. Click **Apply** to save the new settings or else click **Close** to exit without saving the settings.

Tools

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

Duplicate File Finder

This feature removes duplicate files of various pre-defined file categories. It searches for duplicate files on user-specific locations. The user can also provide a folder exclusion list, to be omitted from the scan of duplicate files. Duplicate files will be deleted using One Pass, Two Pass or DoD deletion method as per your preference. The default deletion method is One Pass.

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

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

Deleting Duplicate Files

To delete duplicate files, follow these steps:

1. Select **Tools > Duplicate File Finder**.

2. To modify Duplicate File Finder settings, click **Options**.

   The Quick Heal Duplicate File Finder Options window appears.

3. In the **Please select a duplicate category type** list; clear the categories that need to be skipped by the Duplicate File Finder.

   In the Exclude folder(s) list, you can add exclusion lists for Duplicate File Finder to skip.

4. Click the **Add Folder** button to add the locations for exclusions. Select a location and click **Clear** if the added location is incorrect. Click **Clear All** to remove all exclusion locations added.

   The **Use Secure Delete** option is activated and **One Pass Random – Quick Data Destruction** deletion method is selected by default. You can select any deletion method. See Deletion Methods to know about different deletion methods.

5. Click the **Apply** button to save the modification of settings or else click the **Close** button to exit without saving any modified settings.

6. Click **Add Path** to add the path for Duplicate File Finder to search for duplicate files.

   The Browse for folder window appears.

7. Browse for the required folder. Select **Exclude sub-folder** if you want to exclude the sub-folders within the folder in the scan. **Exclude sub-folder** option is not selected by default.

8. Click **OK** after selecting the required path. If the added path is incorrect, select that path and click **Clear** to delete the path. Click **Clear All** to delete all the added paths from the list.

9. Click **Start Search**.

10. 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.

11. Click **Check All** to select all the duplicate files within the expanded originals.

12. Click **Delete** to delete all the duplicate files.

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

Secure Delete

This feature is used for deleting unwanted files or folders completely from the system. In case you want to delete any confidential data, Secure Delete helps you delete the data making it absolutely impossible to recover by any means. Data deleted using the Delete function of Windows can be recovered using a Recovery Software as the link to such data remains in the cluster of hard drives. The Secure Delete feature of Quick Heal PCTuner deletes the file or

folders directly from the hard drive making it unrecoverable even if a Recovery Software is used.

Deletion Methods

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

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

i (#) Quick Heal PCTuner is available only in Quick Heal Total Security and Quick Heal Total Shield.

Using Secure Delete

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

1. Select **Tools > Secure Delete**.

2. Click the **Options** button.

   The Select Secure Delete Method window appears.

3. Select the deletion method and click the **Accept** button. Select **Enable Right Click Secure Delete (Context Menu)** to facilitate deleting any data by just right-clicking Secure Delete.

4. Click the **Add File** button to locate the file you want to delete.

5. Click the **Add Folder** button to locate the folder and its sub-folders you want to delete.

6. If the selection for file deletion is incorrect, select the file and click **Clear**. Click **Clear All** to delete all the selections.

7. Click **Continue**.

8. A window appears with the message that the deletion is unrecoverable. It also helps you to change the deletion method. If you want to change the deletion method at this stage, click **Options**. Click **Yes** to proceed with the deletion process.

   The selected files are deleted and a Deletion Summary screen appears.

9. Click the **View Report** button to view the report of the deletion process or else click **Close** to exit from Tools Menu.

Startup Booster

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

Using Startup Booster

To use Startup Booster, follow these steps:

1. Select **Tools > Startup Booster**.

2. Click **Start Search**.

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

3. Select the applications that need to be removed from loading every time your system starts.

4. Click **Remove** to remove the application from the list or else click **Close** to exit.

Service Optimizer

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

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

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

Using Service Optimizer

To use Service Optimizer, follow these steps:

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

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

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

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

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

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

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

Reports

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

The menu items in the Reports menu are as follows.

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

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

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

Button	Action
Prev	Helps you display the detailed report of the previous record in the list.
Next	Helps you display the detailed report of the next record in the list.
Print	Helps you take out the print of the detailed report.
Save As	Helps you save the detailed report in text format on your system.
Close	Helps you exit from the Report window.

Auto Tuneup Reports

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

1. Select **Reports > Auto Tuneup**.

2. Select the required record in the list.

3. Click the **Details** button.

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

Disk Cleanup Reports

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

1. Select **Reports > Disk Cleanup**.

2. Select the required record in the list.

3. Click the **Details** button.

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

Registry Cleanup Reports

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

1. Select **Reports > Registry Cleanup**.

2. Select the required record in the list.

3. Click the **Details** button.

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

Traces Cleanup Reports

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

1. Select **Reports > Traces Cleanup**.

2. Select the required record in the list.

3. Click the **Details** button.

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

Scheduler Reports

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

1. Select **Reports > Scheduler**.

2. Select the required record in the list.

3. Click the **Details** button.

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

Secure Delete Reports

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

1. Select **Reports > Secure Delete**.

2. Select the required record in the list.

3. Click the **Details** button.

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

Duplicate File Finder Reports

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

1. Select **Reports > Duplicate File Finder**.

2. Select the required record in the list.

3. Click the **Details** button.

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

Startup Booster Reports

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

1. Select **Reports > Startup Booster**.

2. Select the required record in the list.

3. Click the **Details** button.

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

Service Optimizer Reports

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

1. Select **Reports > Service Optimizer**.

2. Select the required record in the list.

3. Click the **Details** button.

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

Restore Reports

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

1. Select **Reports > Restore**.

2. Select the required record in the list.

3. Click the **Details** button.

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

Restore

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

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

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

Restoring Reports

To restore, follow these steps:

1. Select the required restore point.

2. Click the **Restore** button.

3. A message box appears with the following prompt: **Are you sure you want to restore the backup?** Click **Yes** if you want to restore the backup or else click **No** if you do not want to restore the backup.

4. If you have clicked **Yes** in the previous step, the backup is restored and a message **The selected backup was restored successfully** appears. Click **OK** to complete the restore process.

Deleting Reports

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

1. Select the required restore point.

2. Click the **Delete** button.

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

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.

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.

To see the support options, follow these steps:

1. Open **Quick Heal antivirus**.

2. On the Quick Heal Dashboard, select **Help > Support**.

   Support includes the following options.

   Web Support: Includes **Visit FAQ** (Frequently Asked Questions) and **Visit Forums** – where you can submit your queries to get an appropriate answer.

   Email Support: Includes **Submit Ticket** that redirects you to our Support webpage. Here you can read some of the most common issues with answers. If you do not find an answer to your issue you submit a ticket.

   Live Chat Support: Using this option, you can chat with our support executives.

   Phone Support: Includes phone numbers. You can call our support team and get your issues resolved.

   Remote Support: This support module helps us easily connect to your computer system remotely and assist you in resolving technical issues.

Support by Phone

For Quick Heal AntiVirus Server Edition, customers based in India can dial Toll Free number: 1800-212-7377.

For all other desktop products, customers based in India can dial Toll Free number: 1800-121-7377.

To know a relevant contact number, customers from outside India should visit www.quickheal.com/contact_support.

Other Sources of Support

To get other sources of support, please visit www.quickheal.com/support-center-faqs.

Things to Do if the Product Key is Lost

Product Key serves as your identity to your Quick Heal antivirus. 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.

Head Office Contact Details

Quick Heal Technologies Limited

(Formerly Known as Quick Heal Technologies Pvt. Ltd.)

Reg. Office: Marvel Edge, Office No. 7010 C & D, 7th Floor,

Viman Nagar, Pune 411014.

Telephone: +91 20 66813232

Official Website: www.quickheal.com

Email: info@quickheal.com

Index