Quick Heal

Security Simplified

Quick Heal Total Security for Mac

User Guide

Quick Heal Technologies Ltd.

www.quickheal.com

Copyright Information

Copyright © 2008-2026 Quick Heal Technologies Ltd. All rights reserved.

All rights are reserved by Quick Heal Technologies Ltd.

No part of this software may be reproduced, duplicated or modified in any form or incorporated into any information retrieval system, electronic or any other or transmitted in any form without prior permission of Quick Heal Technologies Ltd., Registered Office: CTS No. 1442 to 1445 Thube Park, Shivaji Nagar, Pune – 411005.

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 Total 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 the Document

This User Guide covers all the information about how to install and use Quick Heal Total Security in the easiest possible ways. We have ensured that all the details provided in this guide are updated to the latest enhancements of the software.

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

Convention	Meaning
Bold Font	Anything highlighted in bold indicates that it is a direction about how to carry out an action.
	This symbol indicates additional information or important information about the topic being discussed.
<Step 1> <Step 2>	The instruction mentioned in the numbered list indicates actions that you need to perform.

Quick Heal Total Security Highlights

Quick Heal Total Security ensures maximum protection against any possible threats or malware that may infect your system when you browse online, work in network environment, and access emails. You can schedule scanning, set rules for Quarantine and Backup for files, set parental control, and block malicious emails and spam.

- **Mac Security** keeps your Mac safe from viruses and malware. Scan your Mac, schedule scans, manage files you don't want scanned, recover quarantined files, and manage your protection settings.
- **Firewall Protection** adds an extra layer of security by helping keep unwanted network connections out of your Mac. It lets you manage your Mac's built-in firewall settings and choose which apps can receive incoming connections. You can also control how your Mac handles incoming connections, giving you more control over what can connect to your Mac.
- **Web Security** helps you set protection rules based on your needs to protect your Mac from malicious files and online threats that can sneak into your system during activities such as banking, shopping, and browsing.
- **Parental Control** helps you manage your children's or other users' online activities by restricting unwanted or inappropriate websites. You can block specific websites or entire categories of websites and schedule when Internet access is available.
- **AntiSpam and Email Security** helps keep unwanted and potentially harmful emails out of your inbox. **AntiSpam** blocks unwanted emails, while real-time cloud-based email security blocks emails that may contain suspicious or potentially dangerous links or attachments.
- **Dark Web Monitoring** helps you stay one step ahead by checking if your personal information, such as your email ID or phone number, has been exposed in a data breach. Choose the information you want to monitor and view the details if a data leak is found.
- **Self Protection** prevents Quick Heal product files from getting altered or modified by viruses and malware or tampered with by any other applications
- **Single Product Key** allows you to activate parallel Windows desktops.

- **Profile** lets you view your license details and copy them when needed

For more information, please visit www.quickheal.com.

Contents

Contents

Quick Heal Total Security **1**
Copyright Information 2
About the Document 3
Quick Heal Total Security Highlights 4
Getting Started **9**
Prerequisites 9
System Requirements 9
Installing Quick Heal Total Security 11
Uninstalling Quick Heal Total Security 21
Registration, Re-activation, Renewal **23**
Registration 23
Registering Online 23
Registering Offline 24
Re-activation 25
Renewal 25
Renewing Online 25
Renewing Offline 26
About Quick Heal Total Security Dashboard **27**
Quick Heal Total Security Dashboard 27
Quick Heal Total Security Features 28
Quick Heal Total Security Menus 29
Quick Access Options 29
Help Topics 30
About Quick Heal Total Security 30
Updating with definition files 31
Quick Heal Total Security Features **33**
Mac Security 33
Scan Settings 33

Virus Protection 37
Scheduled Scans 38
Exclude Files & Folders 41
Quarantine & Backup 43
Firewall Protection 44
Web Security 45
Browsing Protection 45
Phishing Protection 46
Parental Control 46
Configuring Parental Control 47
Email Security 50
Email Protection 50
Spam Protection 51
Dark Web Monitoring 54
Scanning Options 56
Scan My Mac 56
Custom Scan 56
Quick Heal Total Security Menus 58
Reports 58
Viewing Reports 58
Settings 59
Automatic Update 59
Self Protection 60
Password Protection 60
Proxy Support 61
Report Settings 62
Updating Software & Cleaning Viruses 63
Updating Quick Heal Total Security from Internet 63
Updating Quick Heal Total Security with definition files 64
Update Guidelines for Network Environment 64
Cleaning Viruses 65
Technical Support 67
Help 67
FAQs 67
Email Support 68
Call Us 68

Remote Session 68
Live Chat 69
Support Guidelines 69
Contact Quick Heal Technologies 70

1

Getting Started

Quick Heal Total Security 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 Total Security on your machine:

- A system with multiple anti-virus software programs installed may result in system malfunction. If any other anti-virus software program is installed on your system, you need to remove it before proceeding with the installation of Quick Heal Total Security.
- Close all open programs before proceeding with installation.
- We recommend you to keep a backup of your data in case your system is infected with viruses.
- Quick Heal Total Security must be installed with administrative rights.

System Requirements

To use Quick Heal Total Security, your system should meet the following minimum requirements:

- Mac OS 11.5, 12, 13, 14, 15, 26, 27
- Processor: Intel core or Apple's M series, A Series chip compatible
- 4 GB of RAM
- 1 GB free hard disk space
- Internet connection to receive updates

  The requirement is applicable only to 64-bit operating systems unless specifically mentioned.

The requirement is applicable to all flavors of the operating system.

The requirements provided are minimum system requirements. Quick Heal recommends your system has higher configuration than the minimum requirements to obtain best results.

To check for the latest system requirements, visit: www.quickheal.com.

Clients that support email scan

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

- Apple Mail Ver. 10.3 and later
- Thunderbird
- Sparrow
- Sea Monkey
- MailSmith

Clients that do not support email scan

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

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

SSL connections not supported

Email Protection does not support encrypted email connections that use Secure Sockets Layer (SSL). If SSL connections are being used, the emails are not protected by Email Protection.

Installing Quick Heal Total Security

To install Quick Heal Total Security on your machine, follow these steps:

1. Insert the installation CD/DVD in the drive.

   A window with the installer and uninstaller packages appears.

   In case, the installer does not appear, search for the disk image on your desktop and open it. Download or copy the installation file (Quick Heal Total Security.dmg) to your desktop, and then open it.

2. To launch the installer, click Quick Heal Total Security.pkg.

   The user acceptance agreement screen appears.

   macOS Sur and later versions ask permission to access DMG folder location that requires users' approval to run installer. However, the user interface of different versions may differ slightly.

3. Click Continue.

4. On the Welcome screen, click Continue.

   The ReadMe file appears. You are expected to read the Read Me file in its entirety.

5. Click Continue.

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

6. Click Continue.

7. Click Agree to proceed with the installation.

8. To initiate the installation, click Install.

   Quick Heal Total Security is set to be installed on your machine at the fixed location. Moreover, you cannot change the location while installing the software.

9. Provide your user credentials when prompted.

   Quick Heal Total Security installation process starts.

   Follow these steps to ensure that Quick Heal Total Security is compatible with macOS Sur and later. For other macOS, go to step 10 directly.

   Note: While installing Quick Heal Total Security v3.2 build on macOS Sur and later, the following warning message appears.

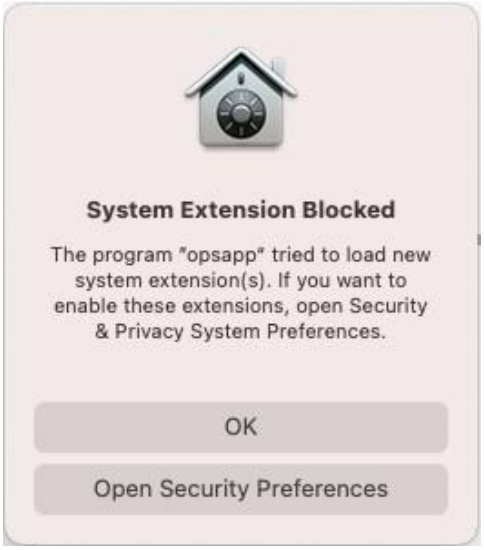


i. To continue for installation, click OK.

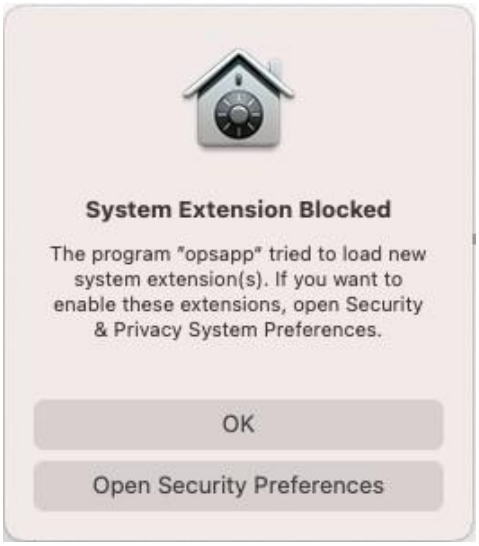
To allow the permission whenever a message appears, click OK. These permissions will ensure that the require settings are done. However, you must check the security settings carefully.

macOS Big Sur and later

For the Mac computers with **macOS Big Sur** and later, the following system extension prompts appear.



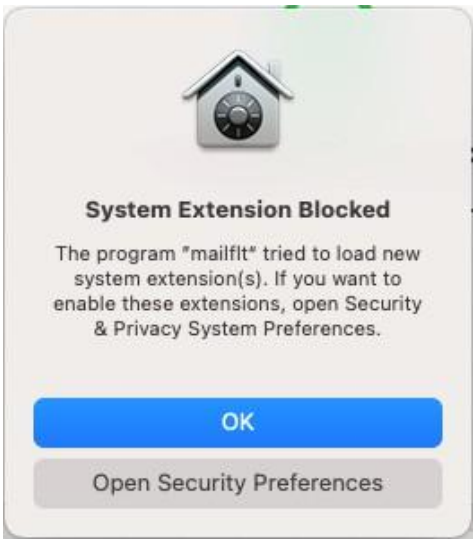
Message for Self Protection (ggcext)



Message for Online Protection (Opsext)



Message for Web Security (webfilt)



Message for Email Security (mailflt)

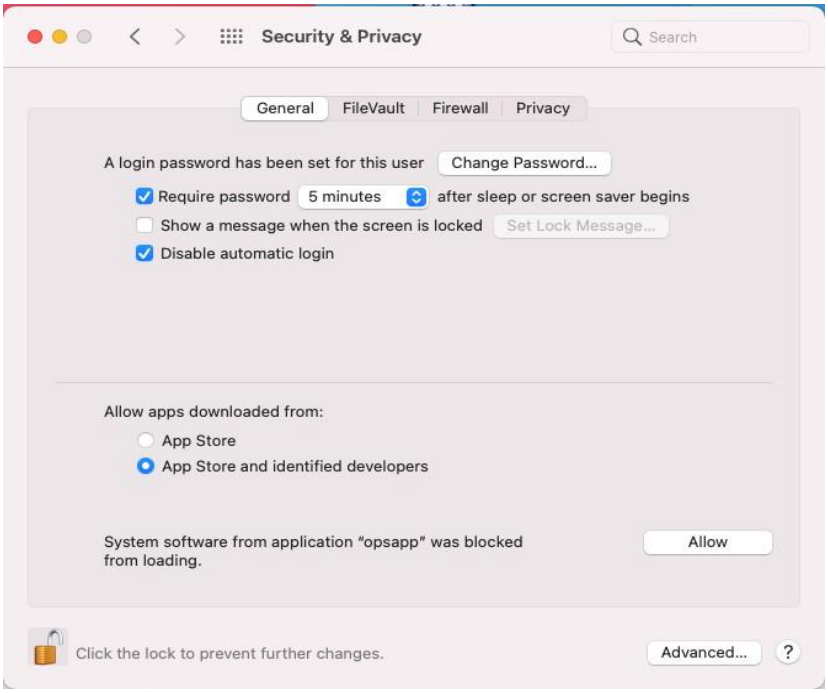
Security Preferences

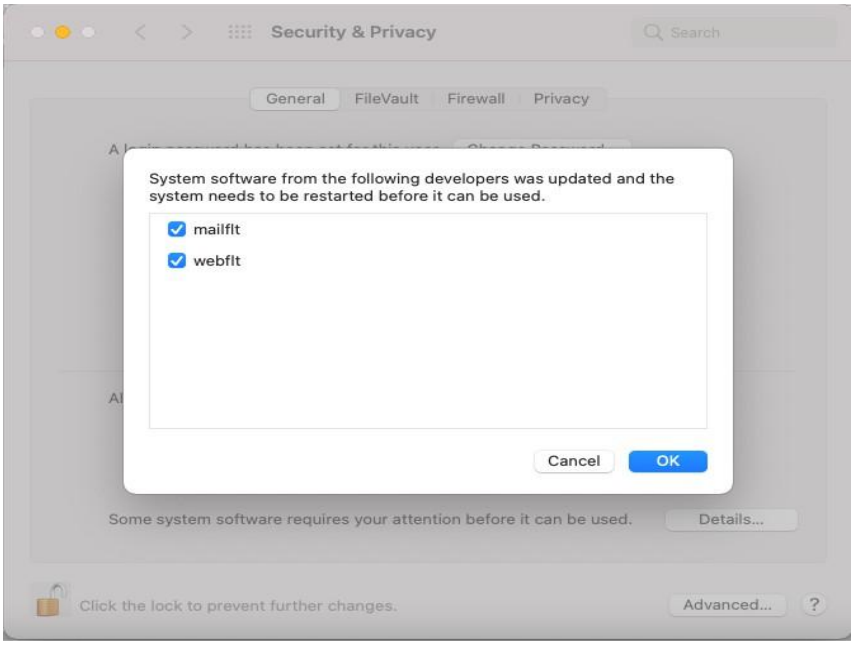
Ensure that the required security settings are done.

i. Go to System Preferences > Security & Privacy.

ii. Click the lock icon and provide the password if it is locked.

iii. Click the ALLOW button available next to the message 'System software from application "app name" was blocked from loading' as shown in the following screenshot.





Requires Permission to make Quick Heal Total Security Compatible with macOS Big Sur 11.5 and later version

Apps and Services of Quick Heal require permission to access system files on macOS Big Sur. After allowing all the Apps and Services, restart your computer.

After Quick Heal Total Security is installed successfully, the following prompts appear.

macOS Big Sur and later

For the Mac computers with **macOS Big Sur** and later, the following system extension prompts appear.



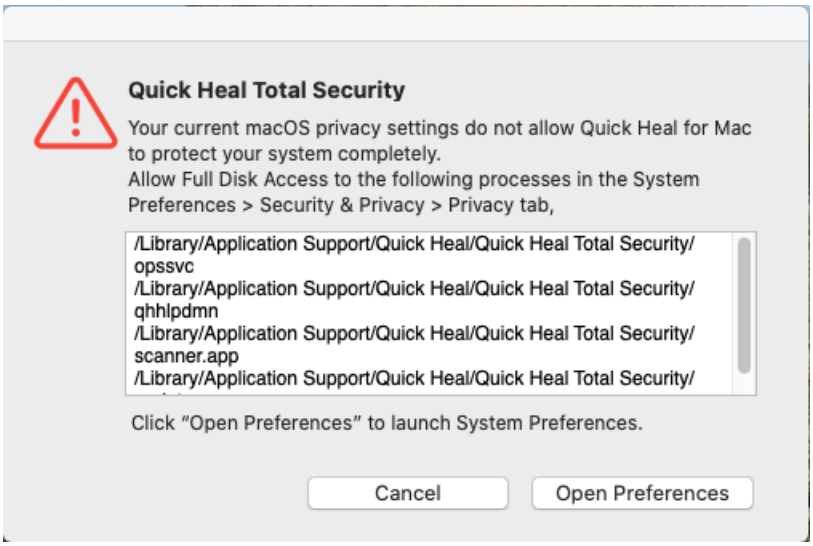
Email Security VPN Configurations



Web Security Network Content

Message from Quick Heal

The following message appears.



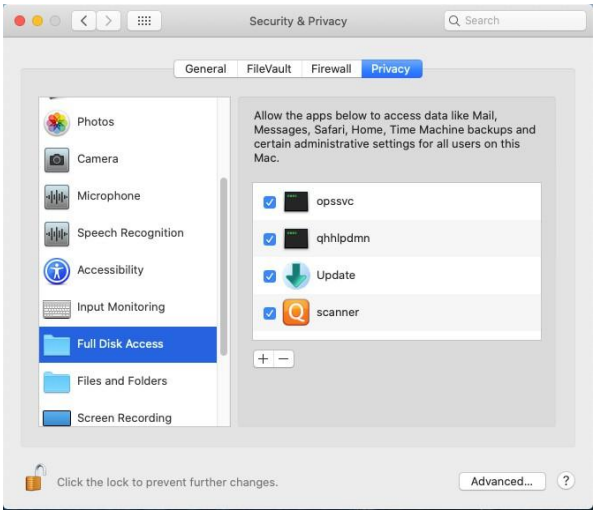
i. To make Quick Heal Total Security compatible with macOS Sur and later, ensure the following settings on macOS.

- Open System Preferences.
- Go to the Security & Privacy > Privacy tab.
- Click the lock icon and provide the password if it is locked.
- Select Full Disk Access in the left pane.

ii. Add the following processes on the given paths and then select the processes on the Security & Privacy Full Disk Access window:

- /Library/Application Support/Quick Heal/Quick Heal Total Security/opssvc
- /Library/Application Support/Quick Heal/Quick Heal Total Security/qhhlpdmn
- /Library/Application Support/Quick Heal/Quick Heal Total Security/scanner.app
- /Library/Application Support/Quick Heal/Quick Heal Total Security/update.app
- opsext (already present in the privacy section)
- ggcext (already present in the privacy section)

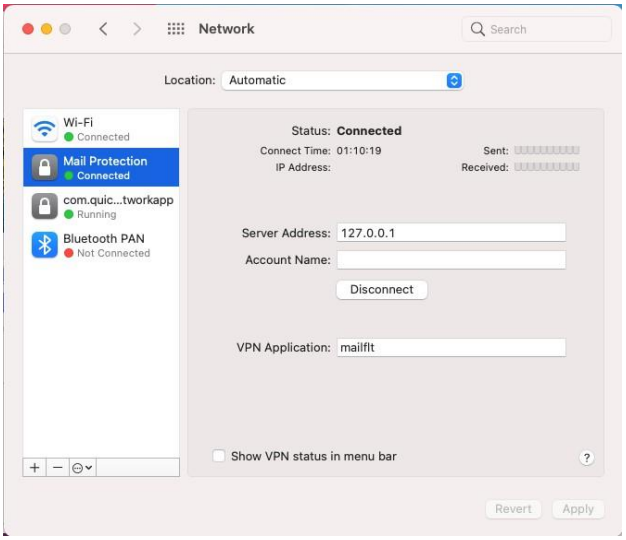
The following screenshot displays **Full Disk Access** configuration in **System Preferences**.

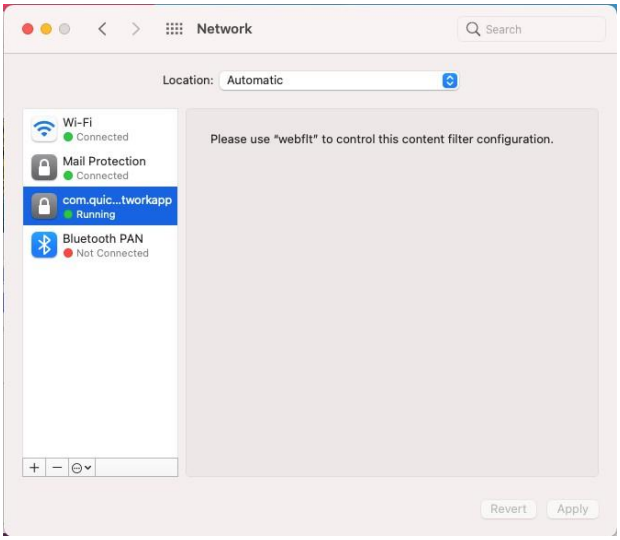




Full Disk Access

The following screenshot displays **mailflt** & **webflt** network extensions in connected state in System preferences > Network.





After all the System extensions are **Allowed** and required permissions are given, restart your computer.

10 To initiate the activation process, click Register Now.

11 Click Register Later or Continue to perform activation later.

12 On Summary page, click Close to close the installer window.

Uninstalling Quick Heal Total Security

Uninstalling Quick Heal Total Security exposes your system and your valuable data to virus threats. However, in case you need to uninstall Quick Heal Total Security, follow these steps:

1 Double-click the 'Quick Heal Un-installer' kept inside the application folder or insert the installation CD/DVD in the drive and click Quick Heal Un-installer.app.

A window with the installer and uninstaller packages appears.

In case it does not appear, search for the disk image on your desktop and open it.

Download or copy the installation file (Quick Heal Total Security.dmg) to your desktop, then open it.

Follow the instructions on the uninstallation wizard.

2 On the Welcome screen, click Yes.

3 Enter your password credentials and click OK.

You are prompted for credentials only if the Password Protection is enabled for Quick Heal Total Security.

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

4. To continue with uninstallation without saving the repository, click Next. If you want to retain the repository, deselect the options to the respective repositories and click Next.
5. Provide your user credentials.

   The uninstallation process starts.

   To unload Quick Heal product app extensions on macOS Sur and later "opsapp", "mailflt" & "webflt", you must provide your credentials.

   Upon completion, a message Quick Heal Total Security has been successfully uninstalled appears. You can provide your feedback and reasons for uninstalling Quick Heal Total Security by clicking Write to us the reason of uninstalling Quick Heal Total Security. Your feedback helps us improve the product quality.

   Please note the product key for future reference. You can copy the product key by clicking Copy to pasteboard also. You can also open a document and directly paste this information into the document. Restart is recommended after uninstallation. To restart click Restart Now, or click Restart Later to continue working on your machine and restart after some time.

2

Registration, Re-activation, Renewal

Registration

Quick Heal Total Security needs to be registered upon installation. It is strongly recommended that you register the copy immediately after installation to receive database updates regularly and get technical support. If the product is not regularly updated, it cannot protect your machine against new threats.

Registering Online

1. Go to Application > Quick Heal Total Security.
2. On the Quick Heal Total Security Dashboard, click Register Now. Alternatively, you can go to Menu > Help > Activation.
3. On the Registration Wizard, enter the 20-digit Product Key and click Continue.
   The Registration Information appears.
4. Enter relevant information in the Purchased From and Register for, Dealer Code (optional) and Bag Engineer Code (optional) text boxes and then click Continue.
5. Provide relevant information in the Name, Email Address, Contact Number text boxes. Select your choices in the Country, State and City lists.
   In case your State/Province and City are not available in the list, you can type your locations in the respective boxes, and then click Continue.
   A confirmation screen appears with the details entered in the preceding step. If any modifications are needed click Go Back to go to the previous screen and modify wherever required, and then click Continue.
   Your product is activated successfully. The expiry date of your license is displayed.
6. To close the Registration Wizard, click Finish.

Registering Offline

1. On the Registration screen, click Register Offline.
2. On the Offline Activation screen, visit the webpage below and fill in the offline activation form: https://www.quickheal.com/actinfo.htm
3. Use the Installation number displayed on the Offline Activation screen to complete the form. You can click Copy to pasteboard to copy the installation number.
4. After filling in the form, you will receive a license key file. Click Browse and select the license key file
5. Click Next to complete the offline registration process.

Re-activation

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

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

Renewal

You can renew your product license as soon as it expires by purchasing a renewal code. However, you are recommended to renew your product before your license expires so that your machine is protected without any interruption. You can get the renewal code from Quick Heal, or from the nearest distributor or reseller.

Renewing Online

To renew your machine online, follow these steps:

1. Go to Quick Heal Total Security > Menu > Quick Heal Total Security > About Quick Heal Total Security.
2. On the About Quick Heal Total Security screen, click Renew Now.
   If your license is about to expire soon or has already expired then the Renew Now button is displayed on Dashboard itself. Click Renew Now to go to the activation page.
3. Select I want to renew with renewal code. I already have renewal code with me and then click Next.
4. On the Registration Information screen, enter relevant information in the Purchased From, Email Address and Contact Number, Dealer Code (optional) and Bag Engineer Code (optional) text boxes, and then click Continue.
   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 Total Security is renewed successfully.

6 To complete the renewal process, click Finish.

In case you do not have the renewal code, select I do not have renewal code with me. I want to purchase renewal code online and then click Buy Now.

In case you renewed your license but its expiry date has not extended, select I have already renewed my license. Please update my license from server and then click Next.

If you have purchased an additional renewal code, then the renewal can be performed only after 10 days of the current renewal.

Renewing Offline

If the system is not connected to the Internet, click Renew Offline to renew the product without an Internet connection.

1 On the Registration screen, click Renew Offline.

2 On the Offline Renewal screen, visit the webpage below and fill in the offline renewal form: https://www.quickheal.com/offline_renewal

3 Use the Product Key and Installation number displayed on the Offline Renewal screen to complete the form. You can click Copy to pasteboard to copy the information.

4 After filling in the form, you will receive a license key file. Click Browse and select the license key file.

5 Click Continue to complete the offline renewal process.

3

About Quick Heal Total Security Dashboard

You can access Quick Heal Total Security from the desktop in any of the following ways:

- Click the Quick Heal icon in the menu bar and then select Open Quick Heal Total Security.
- Click the Quick Heal Total Security icon in Dock, if you have added Quick Heal Total Security to the Dock tray.
- In the Doc tray, click Finder and then select Applications under FAVORITES. Click Quick Heal Total Security in the Applications pane to open the application.

Quick Heal Total Security Dashboard

When you open Quick Heal Total Security, Dashboard appears. The Quick Heal Total Security Dashboard is the main area from where you can access all the features.

Dashboard is divided into various sections: Quick Heal Total Security menu, system security notification area, Quick Heal Total Security features and scan your machine option.

System security notification area indicates whether your system is secured and whether you need to take any action with the help of message and protection icon.

System security notification area provides indication of the security status of Quick Heal Total Security with the help of colored icons. The colored icons and their specific meaning are described as follows:

Icons	Description
Green	Indicates that Quick Heal Total Security is configured with optimal settings and your system is protected.
Orange	Indicates that a feature of Quick Heal Total Security needs your attention, if not immediately, but at the earliest.
Red	Indicates that Quick Heal Total Security is not configured with optimal settings and your immediate attention is needed. The action corresponding to the message needs to be executed immediately to keep your system protected.

System security notification area is your instant interface to vital protection settings that can affect files, folders, emails, and so on. It also allows users to configure protection against viruses that try to gain entry through Internet, external drives and emails. Quick Heal Protection Center is split into two sections.

Each colored icon has an action associated with it which needs to be executed by the user.

Quick Heal Total Security Features

Quick Heal Total Security ensures complete protection against any possible threats or malware that may infect your system through various means. Quick Heal Total Security shields your system in the following ways:

Features	Description
Mac Security	Helps you configure scan preferences, virus protection, schedule scan, exclude files and folders from scanning, and set rule for quarantine and files backup.
Web Security	Helps you protect your system against malicious threats when you are browsing the Internet, or when you transfer data across the network, and parents can control their children's Internet usage.
Email Security	Helps you protect your system against malicious threats and spam that try to sneak into your system through emails.

The following are frequently used features:

Features	Description
Scan	Launches the scanner that scans the machine based on scanning preferences.

Quick Heal Total Security Menus

With the Quick Heal Total Security menus, you can configure the general settings for taking updates automatically, password protect your Quick Heal Total Security so that no unauthorized person can access the Quick Heal Total Security application, provide settings for proxy support and removing reports from the list automatically. The Quick Heal Total Security menu includes the following:

Menu	Description
Settings	Helps you customize and configure the settings of Quick Heal Anti-Virus such as Automatic Update, Internet Settings, Password Protection, Reports Settings.
Reports	Helps you view the activity reports of Scanner, Virus Protection, Email Protection, Quick Update, Anti-Phishing, Browsing Protection, Parental Control.

Quick Access Options

Quick access options are the options that you use to access Quick Heal Total Security, turn on or off Virus Protection, update the product, and scan the machine when required.

The quick access options include the following:

Options	Description
Open Quick Heal Total Security	Launches Quick Heal Total Security.
Enable / Disable Virus Protection	Helps you turn on or turn off Virus Protection.
Update Now	Helps you update Quick Heal Total Security.
Scan My Mac	Helps you scan your machine for viruses.

Help Topics

The Help topics assist you in understanding Quick Heal Total Security features, how to use them, and seek technical support when required.

To access the desktop integrated Help topics, follow these steps:

1. Go to Quick Heal Total Security > Menu > Help > Quick Heal Total Security Help.
   The Help topics appear.
2. Search for the information that you want.

About Quick Heal Total Security

The About Quick Heal Total Security screen includes the information about the product, license, options for renewing license, updating the product, viewing details of the user license.

To access the About Quick Heal Total Security screen, follow these steps:

- Go to Quick Heal Total Security > Menu > Quick Heal Total Security > About Quick Heal Total Security Help.

The About screen appears.

The About screen includes the following information:

- Quick Heal Total Security product details: Product Name, Product Version, Service Pack, Virus Database Date.
- License Information: Customer Name, Registered for (individual or organization name), License validity date.
- License Agreement: Click License Agreement to view the End-User License Agreement (EULA) and review the terms and conditions for using Quick Heal Total Security.
- Renew Now: Helps you renew your license online.
- Update Now: Helps you update your machine with the latest signature.

The License Information and the End-User License Agreement (EULA) are available under this section.

Update License Details: Helps you to synchronize your existing license information with Quick Heal Activation Server. In case you want to renew your existing subscription and you do not know how to renew it or you face 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. You just need to follow these steps:

- Be connected to the Internet.
- Click Update License Details.
- Click Continue to update your existing subscription.

Updating with definition files

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

1 Go to Quick Heal Total Security > Menu > Quick Heal Total Security > Check for Updates....

2. On the Welcome to Total Security Update screen, click Continue.
   The Select the mode you prefer for updating Total Security screen appears.
3. Select Pick from specified location.
4. Type the path or click the File button to the file location, and then click Continue.

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

4

Quick Heal Total Security Features

The Quick Heal Total Security features include the most important features that help you set the scanning preference, protection rules for your machine, scanning schedule, set rules for Quarantine and Backup for files, apply protections for online browsing, set parental control, and block malicious emails and spam.

These features provide optimum protection to your system. Moreover, these features have to be kept enabled all the time. If you disable these features, for any reason, then the corresponding icons for them will turn red.

Mac Security

The Mac Security option on Dashboard helps you customize the settings that concern the protection of files and folders in your system. With Mac Security, you can set scanning preferences, apply rules for virus protection, schedule scanning, exclude files and folders from being scanned, and set rules for quarantine and backup files.

Mac Security includes the following:

Scan Settings

With Scan Settings, you can customize the way a scan is to be performed and the action that needs to be taken when a virus is detected. However, the default settings are optimal and can provide the required protection to your machine.

To configure Scan Settings, follow these steps:

1. On the Quick Heal Total Security Dashboard, click Mac Security.
   The Mac Security setting details screen appears.
2. Click Scan Settings.

3 Set the appropriate option for scan type, action to be taken if virus is found in the files, and whether you want to take the backup of the previous setting.

4 Click Save to save your settings.

Select scan type

- Automatic (Recommended): Automatic scanning type is the default scanning mode, which is recommended as it ensures optimal protection that your machine requires. This setting is an ideal option for novice users as well.
- Advanced: Select Advanced mode if you want to customize the scanning behavior. This is ideal for experienced users only. When you select the Advanced option, the Configure button is enabled and you can configure the Advanced setting for scanning.

Action to be taken when virus is found

Action that you select here will be taken automatically if virus is found, so select an action carefully. The actions and their descriptions are as follows:

Actions	Description
Repair	During scanning if a virus is found, it repairs the file or automatically quarantines it, if it cannot be repaired. When the scan is over, a summary window appears providing the details about all the actions taken and other scan details. If the infectious file is a Backdoor, Worm, Trojan, or Malware, then Quick Heal Total Security automatically deletes the file.
Delete	Deletes a virus-infected file without notifying you. When the scan is over, a summary window appears providing the details about all the actions taken and other scan details. Once the files are deleted, they cannot be recovered.
Skip	If this option is selected the files are scanned but no action is taken on the infected files and they are skipped. Select this option if you want to take no action even if a virus is found. When the scan is over a summary report appears providing all the scan details.
Backup before taking action	The scanner keeps a backup of the infected files before disinfecting them. The files that are stored in the backup can be restored from the Quarantine menu.

Configuring Advanced Scan Type

To configure Advanced Scan type, follow these steps:

1. On the Quick Heal Total Security Dashboard, click Mac Security.
   The Mac Security setting details screen appears.
2. Click Scan Settings.
3. In Scan type, select Advanced.
   The Configure button is enabled.
4. Click Configure.
   The Advanced Scan setting details screen appears.
5. Check Items to be scanned for Windows-based malwares.
   By default, this option is selected.
6. Select one of the following items for scanning:
   - Scan executable files: Select this option if you want to scan only the executable files.
   - Scan all files: Select this option if you want to scan all types of files. However, it takes time to execute this option and the scanning process slows down considerably.
7. Turn Scan archived files ON, and then configure the scanning preference for the archive files such as zip files and so on.
8. To close the Archive Files screen, click OK. To close the Advanced Scan setting, click OK and then click Save to save your settings.

Scan archive files

If you select Scan archive files, then the scanner will also scan archive files such zip files, archive files, and so on. If you select Scan archive files, the Configure button is enabled and helps you configure the way scanner should treat malicious archive files.

You can scan files of various archive file types till five levels down so to ensure no files are left from being scanned.
Following are the actions that you can select to be taken when a virus is found in any of the archive files:

Actions	Description
Quarantine	Select this option if you want to quarantine an archive file that contains a virus.
Delete	Select this option if you want to delete an archive file that contains virus-infected files. However, you are not notified if a file is deleted, though its report is generated that you may see in the Reports list.
Skip	Select this option if you want to take no action even if a virus is found in any of the archive files. However, this option is selected by default.

Archive Scan level

Set the scan level till which you want to scan the archive files. You can set till five levels down inside the archive files. By default, the scanning is set to level 2. However, you can increase the archive scan level which may though affect the scanning speed.

Select archive type to scan

You can select the archive file types that you want to scan from the archive files list. Some of the common archive file types are selected by default. However, you can change your setting as you prefer.

Types	Description
Select All	Select the checkbox to select all the archive file types available in the list.

When the scan is complete, a summary report appears providing the details about all the actions taken and other scan details, irrespective of the option that you had configured.

Virus Protection

With Virus Protection, you can continuously monitor your machine from viruses, malwares, and other malicious threats. Such threats try to sneak into your machine from various sources such as email attachments, Internet downloads, file transfer, file execution and so on.

It is recommended that you always keep Virus Protection enabled to keep your machine clean and protected from any potential threats. However, Virus Protection is enabled by default that you can disable if required.

To configure Virus Protection, follow these steps:

1. On the Quick Heal Total Security Dashboard, click Mac Security.
   The Mac Security setting details screen appears.
2. To protect your machine from malicious threats, turn Virus Protection ON.
3. To configure Virus Protection further, click Virus Protection.
4. On the Virus Protection screen, do the following:
   - Items to scan – Select this checkbox if you want to scan Windows-based malwares. However, this checkbox is selected by default.
   - Scan network volume – Select this option if you want to scan network volumes that are mounted on your machine. However, this option is turned on by default.
   - Display notifications – Select YES if Display notifications is selected, it displays an alert message whenever a malware is detected. This feature is selected by default.
   - If virus found – Select an action to be taken when virus is found in a file such as Repair, Delete, and Deny Access.
   - Backup before taking action – Select this option if you want to take a backup of a file before taking an action on a file. Files that are stored in backup can be restored from the Quarantine menu.
5. To save your setting, click Save.

Action to be taken when virus is detected

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

Turning Off Virus Protection

Turn Virus Protection OFF. However, when you try to turn off Virus Protection, an alert message is displayed. Turning Virus Protection OFF is suggested only when you really require this. Moreover, you can set it off for a certain period of time so that it turns ON automatically thereafter.

Following are the options for turning Virus Protection OFF for a certain period:

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

Select an option and click OK.

Once you turn off Virus Protection, its icon color changes from green to red in Menu Bar Tray, which means that Virus Protection has been disabled temporarily or permanently based on your selection. If you have selected any of the options for turning off temporarily or after next boot then the icon color changes back from red to green after the certain time passes or at the next boot. If you have selected to disable permanently, then the icon color remains red until you enable Virus Protection manually.

Scheduled Scans

With Schedule Scans, you can define time when to begin scanning of your machine automatically. You can schedule multiple number of scan schedules so that you can

initiate scanning of your machine at your convenient time. Frequency can be set for daily and weekly scans, that can additionally refine your request to schedule it to occur at fixed boot at fixed time.

Configuring Schedule Scans

To configure Schedule Scans, follow these steps:

1. On the Quick Heal Total Security Dashboard, click Mac Security.
2. On the Mac Security setting screen, click Schedule Scans.
   The Scheduled Scans details screen appears. Here you see a list of all schedules for scanning, if you had defined any before.
3. To create a new schedule for scanning, click Add.
   The Add Scheduled Scan screen appears where you can create a new scan schedule name, its frequency, and other details.
4. In the Scan name text box, type a scan schedule name.
5. Set Scan Frequency:
   - Daily: Select the Daily option if you want to initiate scanning of your machine daily. However, this option is selected by default.
   - Weekly: Select the Weekly option if you want to initiate scanning of your machine on a certain day of the week. When you select the Weekly option, the Weekly list is enabled where you can select a day of the week.
6. Set Scan Time:
   - Start scan at first boot: Select the Start scan at First Boot option to schedule the scanner to scan at first boot of the day. When you select Start at first boot, you do not have to specify the time of the day to start the scan. Scanning takes place only during the first boot irrespective at what time you start the system.
   - Start scan at Fixed Time: Select the Start scan at fixed time option if you want to initiate the scanning of your machine at a certain time. When you select Fixed Time, the Start Time list is enabled where you can fix the time for scanning. However, this option is selected by default.
7. Set Scan priority.

- High: Select the High option if you want to have the scanning priority at high.
- Low: Select the Low option if you want to have the scanning priority at low. However, this option is selected by default.

8 Scan location:
- Click Configure to open the Scan location screen, where you can select files and folders for scanning. You can set multiple locations. Select the Drives, folder or multiple folders to be scanned and press OK. You can configure Exclude Subfolder while scanning specific folder. This will ignore scanning inside the subfolders while scanning.

9 Scan settings:
- Click Configure to open the Scan Settings screen. Under Scan Settings, you can specify specific items to be scanned, action required to be taken if a virus is found and use of advanced options while scanning. By default setting is set for adequate options for scanning.
  - In Scan type, select one of the options from Automatic and Advanced. To know about how to configure scan setting, see Scan Settings, p-31.
  - Select YES if you want to have a backup of files before taking any action on them, otherwise select NO if you want no backup of files. This option is selected by default.

10 To save your settings, click Save.

Editing Schedule Scan

You can modify any of the scheduled scans whenever required. To edit a scheduled scan, follow the steps:

1 On the Quick Heal Total Security Dashboard, click Mac Security.

2 On the Mac Security setting screen, click Schedule Scans.
A list of all scan schedules appears.

3 Select a scan schedule and then click Edit.

4 In the Add Schedule Scan screen, change the scan schedule as required.

5 To save your settings click Save and then click Close.

Removing Schedule Scan

If you do not require a scan schedule, you can remove it whenever you require. To remove a scan schedule, follow these steps:

1. On the Quick Heal Total Security Dashboard, click Mac Security.
2. On the Mac Security setting screen, click Schedule Scans.
   A list of all scan schedules appears.
3. Select a scan schedule, and then click Remove.
4. Click YES to confirm if you are sure to remove the scan schedule, and then click Close.

Exclude Files & Folders

With Exclude Files & Folders, you can decide which files and folders should not be included during scanning for known viruses or issues. This helps you avoid unnecessary repetition of scanning of the files which have already been scanned or you are sure should not be scanned. You can exclude files from scanning from both of the scanning modules Mac Security Scanner and Virus Protection.

Total Security Scanner scans files and folders when you scan manually while Virus Protection scans each file and folder when accessed automatically.

Configuring Exclude Files & Folders

To configure Exclude Files & Folders, follow these steps:

1. On the Quick Heal Total Security Dashboard, click Mac Security.
2. On the Mac Security setting screen, click Exclude Files & Folders.
   The Exclude Files & Folders details screen appears. Here you see a list of files and folders to be excluded from scanning, if you have added any.
3. Click Add.
4. On the New Exclude Item screen, click the File button or Folder button to add relevant file or folder to the list.

When you add a folder, you can check Exclude Subfolders so that the subfolders are also excluded from scanning.

5 Select a file or folder, and then click Open to add the selected file or folder and then click Save to save your settings.

6 To close the Exclude Files and Folders screen, click Close.

Editing Exclude Files & Folders

You can change your setting for Exclude Files & Folders if you require so in the following way:

1 On the Quick Heal Total Security Dashboard, click Mac Security.

2 On the Mac Security setting screen, click Exclude Files & Folders.
The Exclude Files & Folders details screen appears. Here you see a list of files and folders to be excluded from scanning that you have added.

3 Under Location, select a file or folder, and then click Edit.

4 On the New Exclude Item screen, click the File button or Folder button to add another file or folder to the list.
When you add a folder, you can check Exclude Subfolders so that the subfolders are also excluded from scanning.

5 Select a file or folder, and then click Open to add the selected file or folder and then click Save to save your settings.

6 To close the Exclude Files and Folders screen, click Close.

Removing Exclude Files & Folders

You can remove any files or folders that you included in the Exclude Files & Folders list if you require so in the following way:

1 On the Quick Heal Total Security Dashboard, click Mac Security.

2 On the Mac Security setting screen, click Exclude Files & Folders.
The Exclude Files & Folders details screen appears. Here you see a list of files and folders to be excluded from scanning that you have added.

3 Under Location, select a file or folder, and then click Remove. You can remove all files and folders from the list by clicking Remove All.
The selected files or folders are removed from the exclusion list.

4 To close the Exclude Files and Folders screen, click Close.

Quarantine & Backup

Quarantine & Backup helps in safely isolating the infected or suspected files. When a file is added to Quarantine, Quick Heal Total Security encrypts the file and keeps it inside the Quarantine folder. Being kept in an encrypted form, these files cannot be executed and hence are safe. Quarantine also keeps a copy of infected file before repairing if the Backup before repairing option is selected in the Scanner Settings. With Quarantine & Backup, you can also set a rule for removing the files after a certain period of time and having a backup of the files.

Configuring Quarantine & Backup

To configure Quarantine & Backup, follow these steps:

1 On the Quick Heal Total Security Dashboard, click Mac Security.

2 On the Mac Security setting screen, click Quarantine & Backup.

3 In Delete files automatically after, drag the slider to select days after which the files should be removed from the Quarantine folder automatically.

Setting this feature helps in removing the quarantine/backup files after the configured period of time. The removal of files is set to 30 days by default.

4 Click View Files to see the quarantined files. You can take any of the following actions on the quarantined files:

- Add File: You can add files from folders and drives to be quarantined manually.
- Restore: You can restore the selected files if required.
- Submit For Analysis: You can submit the selected file to the Quick Heal research lab for further analysis from the Quarantine list. Select the file you want to submit and then click Submit For Analysis**.**
- Delete: You can delete the selected files from the quarantine list.
- Remove All Files: You can remove all the Quarantine files from the Quarantine list.

In Quarantine, when you select a file and click the Submit button, a prompt appears requesting permission to provide your email address. You also need to provide a reason for submitting the files. Select one of the following reasons:

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

Firewall Protection

With Firewall Protection, you can manage your Mac's built-in firewall from Quick Heal. It helps protect your Mac from unwanted incoming network connections.

To configure Firewall Protection:

1. Open Quick Heal Total Security.
2. Select Mac Security.
3. Select Firewall Protection.
4. Use the Firewall Protection toggle to turn the protection on or off.
   - **On:** Firewall Protection is enabled and helps protect your Mac from unwanted incoming network connections.
   - **Off:** Firewall Protection is disabled.

You can also configure the following Firewall settings:

- **Block all incoming connections**
  Turn this on to block incoming connections. Some system services may still be allowed to connect.
- **Choose which apps may receive incoming connections**
  Use the toggle next to an app to allow or block incoming connections. You can also use + to add an app.
- **Automatically allow built-in software to receive incoming connections**
  Turn this on to allow built-in software to receive incoming connections automatically when required.
- **Automatically allow downloaded signed software to receive incoming connections**
  Turn this on to allow downloaded signed software to receive incoming

connections automatically.

- **Enable stealth mode**

  Turn this on to ignore network access attempts from unauthorized applications.

Web Security

With Web Security, you can set the protection rules to save your machine from malicious files that can sneak into your system during online activities such as banking, shopping, surfing and so on. You can also set parental control to monitor online activities of your children and other users so that you restrict them from accessing any unwanted websites.

Web Security includes the following:

Browsing Protection

With Browsing Protection, you can block malicious websites while browsing so that you do not come in contact with malicious websites and you are secure. However, Browsing Protection is enabled by default.

Configuring Browsing Protection

To configure Browsing Protection, follow these steps:

1. On the Quick Heal Total Security Dashboard, click Web Security.
2. Enable Browsing Protection.

You can disable Browsing Protection whenever you prefer.

Phishing Protection

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

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

Configuring Phishing Protection

To configure Phishing Protection, follow these steps:

1. On the Quick Heal Total Security Dashboard, click Web Security.
2. Enable Phishing Protection.

You can disable Phishing Protection whenever you prefer. However, you are advised always to keep Phishing Protection enabled.

Parental Control

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

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

Important things to do before configuring parental control!

To get utmost benefits from the parental control feature, we recommend you follow a few steps:

Configuring Parental Control

To configure Parental Control, follow these steps:

1. On the Quick Heal Total Security Dashboard, click Web Security.
2. On the Web Security setting screen, click Parental Control.
3. Configure the following options based on your requirement:
   - Restrict access to websites based on the category: When you select this option, you restrict access to all websites under a similar category.
   - Restrict access to websites as specified by user: When you select this option, you restrict access to specific websites only.
   - Schedule Internet access: This option helps you schedule Internet accessibility for your children or other users.
4. To save your settings, click Save.

Restrict access to websites based on category

The Restrict access to websites based on the category feature in Parental Control has a vast range of website categories to allow or deny access to them based on the requirements. Once you restrict or allow a website category, all the websites falling under a category are blocked or allowed. This is helpful if you are sure to restrict or allow all the websites under a category. Moreover, if you want to restrict most of the websites in a category but allow certain websites of that category, which is either required or you rely on, you can do so by excluding such websites in the Exclude list.

To configure access restriction for website categories, follow these steps:

1 On the Quick Heal Total Security Dashboard, click Web Security.

2 On the Web Security setting screen, click Parental Control.

3 Under Restrict access to websites, switch Based on the category to YES to restrict website categories.

The Configure button is enabled.

4 Click Configure.

- A list of website categories whose access can be allowed or denied appears. Click the Allow or Deny button available next to each category that you want to allow or restrict as required. Moreover, the default settings are perfect for novice users and they can retain the default settings for their children.
- You can also exclude a website from being blocked, despite it being in the blocked category, by adding it to the Exclude list. For example, if you have blocked the Social Networking and Chat category, but you still want to provide access to Facebook, you can do so by enlisting the website in the Exclude list.

  i. On the Web Category list, click Exclude for excluding the websites.

  ii. Enter the URL of the website in the list that you want to allow users to access and then click Add.

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

  iii. You can also block the subdomain of a blocked website. 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 will also be blocked.

  iv. To save the changes, click OK.

5 Click OK and then click Save to save your settings.

Restrict access to websites as specified

The Restrict access to websites as specified by user feature in Parental Control helps you block specific websites. This is helpful when you are sure to restrict certain websites and when your list is shorter than it can be in a website category. This is also helpful when a website does not fall in a correct category or you have restricted a website category yet a certain website is accessible that you want to block.

To configure access restriction for specific websites, follow these steps:

1 On the Quick Heal Total Security Dashboard, click Web Security.

2 On the Web Security setting screen, click Parental Control.

3. Under Restrict access to websites, switch As specified by user to YES to restrict specific websites.
   The Configure button is enabled.
4. Click Configure.
   A list for adding websites appears.
5. Enter the URL of the website to be blocked and then click Add.
   You can add as many websites as you require. Moreover, you can remove any website whenever you require so. Select the websites that you want to remove and click Remove. You can also remove all the websites in the list by clicking Remove All.
6. Click OK.
7. To save your settings, click Save.

Schedule Internet access

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

To configure Schedule Internet access, follow these steps:

1. On the Quick Heal Total Security Dashboard, click Web Security.
2. On the Web Security setting screen, click Parental Control.
3. Switch Schedule Internet access to YES to configure Internet accessibility to your children.
   The Configure button is enabled.
4. Click Configure.
   The Schedule Internet Access setting details screen appears.
5. Select one of the following:
   - Always allow access to the Internet: Select this option if you want to allow access without any restriction to your children.

- Allow access to the Internet as per the schedule: Select this option if you want to schedule Internet accessibility for your children. When you select this option, the routine chart for the days of the week is enabled.
  - Click a cell in the routine chart for a time period of a day. You can select any time period of any day based on your requirement.
  - If you want to schedule a regular period of time for the entire week (like 8:00 AM to 10:00 AM for all days in a week), hover over the time period, or if you want to restrict access to Internet for an entire day (like Sunday) hover over the day, an arrow appears. Click the time period or the day, your restriction applies accordingly. Your children can access the Internet only during the allowed schedule.

6 To save your setting, click OK.

Time Specification	Description
Allowed Time	All the cells appearing in green color indicate allowed time frequency for accessing the Internet.
Blocked Time	All the cells not appearing in green color indicate blocked time frequency for accessing the Internet.

Email Security

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

Email Security includes the following.

Email Protection

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

However, Email Protection is enabled by default and the default settings provide the required protection to the mailbox from malicious emails. We recommend that you always keep Email Protection enabled to ensure email protection.

Configuring Email Protection

To configure Email Protection, follow these steps:

1. On the Quick Heal Total Security Dashboard, click Email Security.
2. On the Email Security setting screen, enable Email Protection.

   Protection against malwares coming through emails is enabled.
3. To configure further, protection rules for emails, click Email Protection.
4. Turn Notify on email ON if you want an alert message when a virus is detected in an email or attachment.

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

5. Select one of the following actions to be taken if virus is found.
   - Repair: Select Repair to get your emails or attachment repaired when a virus is found
   - Delete: Select Delete to delete the infected emails and attachments.

   If the attachment cannot be repaired then it is deleted.

6. Switch Backup before taking action to YES if you want to have a backup of the emails before taking an action on them.

   You can revert to default settings anytime you require so by clicking Set Defaults.
7. To save your settings, click Save.

Spam Protection

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

Spam Protection is not supported on Apple's M1 chip.

Configuring Spam Protection

To configure Spam Protection, follow these steps:

1. On the Quick Heal Total Security Dashboard, click Email Security.
2. On the Email Security setting screen, turn Spam Protection ON.
3. To configure further protection rules for spam, click Spam Protection.
4. Turn Tag subject with text ON to include the tag "spam" to the suspicious emails.
5. 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.
6. Select one of the following:
   - Turn White List ON if you want to allow emails from the email addresses enlisted in the white list to skip from spam protection filter, and then click Configure to enter the email addresses.
   - Turn Black List ON if you want to filter out emails from the email addresses enlisted in the black list and then click Configure to enter the email addresses.
7. Click OK.
8. To save your settings, click Save.

Setting spam protection rule for White List

White List is the list of email addresses from which all emails are allowed to skip from spam protection filter irrespective of their content. No emails from the

addresses listed here are passed through the SPAM filter. It is suggested that you configure only such email addresses which you rely fully.

To add email addresses in the White List, follow these steps:

1. Turn White List ON.
   The Configure button is enabled.
2. Click Configure.
3. Enter the email addresses in the list and click Add.

   Edit or Remove Email: 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.

   Import White List: You can import the White List by clicking Import. This is very helpful if you have a long list of email addresses to enlist.

   Export White List: You can export the White List by clicking Export. This exports all the email addresses existing in the list. This is helpful if you want to import the same email addresses later. You can simply import the email addresses list.
4. To save your settings, click OK.

Setting spam protection rule for Black List

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

To add email addresses in the Black List, follow these steps:

1. Turn Black List ON.
   The Configure button is enabled.
2. Click Configure.
3. Enter the email addresses in the list and click Add.
   Important: While entering an email address, be careful that you do not enter the same email address in the black list that you entered in the white list, else a message appears.

Edit or Remove Email: 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.

Import Black List: You can import the Black List by clicking Import. This is very helpful if you have a long list of email addresses to enlist.

Export Black List: You can export the Black List by clicking Export. This exports all the email addresses existing in the list. This is helpful if you want to import the same email addresses later. You can simply import the email addresses list.

4 To save your settings, click OK.

Adding Domains to White List or Black List

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

1 Turn White List or Black List On and click Customize.

2 Type the domain and click Add. For editing an existing entry, click Edit.

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

3 To save the changes, click OK.

Dark Web Monitoring

Dark Web Monitoring helps you check whether your monitored information has been exposed in a data breach. You can monitor information such as your email ID or phone number.

To access Dark Web Monitoring:

1. Open Quick Heal Total Security.
2. Select Email Security.
3. Select Dark Web Monitoring.

The Dark Web Monitoring screen shows the latest results for your monitored information.

- **Refresh**

  Select Refresh to check for the latest results.
- **Edit monitoring info**

  Select Edit monitoring info to add or update the information you want to monitor.
- **View leaks**

  If a data leak is found, select View leaks to view the available details.

Monitoring Results

The results are grouped into the following sections:

- **Results with your info**

  Shows data leaks found for the information you are monitoring, such as your email ID or phone number.
- **Results with other info**

  Shows other information found along with your monitored information in a data leak. The number of detected leaks is shown for each type of information.

Note: Dark Web Monitoring does not send notifications in Quick Heal Total Security for Mac. The results are refreshed when you launch the application.

5

Scanning Options

Scan My Mac option on Dashboard provides you with options of scanning your system in various ways so that you can scan as you require. You can initiate scanning of your entire system, drives, network drives, USD drives, folders or files, certain locations (Custom Scan). Although the default settings for manual scan are usually adequate, you can adjust the options for manual scan.

Scan My Mac

Scan My Mac is a complete scanning of your system. With Scan My Mac, you can scan the entire machine, files and folders excluding mapped network drives, folders, and files whenever you think your system needs scanning. However, if you keep Virus Protection enabled, you need not run a manual scan. Moreover, the default setting for manual scan is usually adequate, you can adjust the options for manual scan if required.

To initiate Scan My Mac, follow these steps:

1. On the Quick Heal Total Security Dashboard, click the Scan My Mac list showing at the bottom right.
2. On the scan option, click Scan My Mac to initiate complete scanning of your machine.

Upon completion of the scan, you can view the scan report under Reports > Scanner Reports.

Custom Scan

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

To initiate Custom Scan, follow these steps:

1. On the Quick Heal Total Security Dashboard, click the Scan My Mac list showing at the bottom right.
2. On the scan option, click Custom Scan.
3. Click Add to locate the path of the desired folder or drives that you want to scan.

   You can select multiple folders for scanning. If you want to remove a file from being scanned, select the file and click Remove. To remove all the files from scan, click Remove All.
4. To initiate scanning, click Start Scan.

   Upon completion of the scan, you can view the scan report under Reports > Scanner Reports.

6

Quick Heal Total Security Menus

The Quick Heal Total Security menus, available on the top left corner on the Quick Heal Total Security Dashboard, give you instant access to the settings and report topics options irrespective of the feature being accessed.

With the Quick Heal Total Security menus, you can configure general settings to take the updates automatically, password-protect your Quick Heal Total Security settings so unauthorized users cannot access your settings, set proxy support, and schedule removing reports from the report list.

Reports

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

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

- Scanner
- Virus Protection
- Email Protection
- Automatic Update
- Browsing Protection
- Phishing Protection
- Parental Control

Viewing Reports

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

1. On the Quick Heal Total Security Dashboard, click Reports.
   A Reports list appears.
2. To view the report of a feature, click the report name. For example, if you want to view the report on Virus Protection, click Virus Protection Reports.

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

Buttons	Actions
Details	Helps you view a detailed report of the selected record.
Delete	Helps you delete the highlighted report in the list.
Delete All	Helps you delete all the reports.

Settings

With Settings, you can configure some of the common settings of Quick Heal Total Security such as you can decide whether you want to take the updates automatically, password-protect your Quick Heal Total Security settings so unauthorized users cannot access your settings, set proxy support, and scheduling the removal of reports from the report list. However, the default settings are optimal and ensure complete security to your system.

Settings includes the following.

Automatic Update

With Automatic Update, Quick Heal Total Security can take the updates automatically to keep your software updated with the latest virus signatures to protect your system from new malwares. To get the updates regularly, your machine on which Quick Heal Total Security is installed needs to be connected to the Internet. It is recommended that you always keep Automatic Update enabled, which is enabled by default.

Configuring Automatic Update

To configure Automatic Update, follow these steps:

1. On the Quick Heal Total Security Dashboard, click Settings.
2. On the Settings screen, turn Automatic Update ON and then click Automatic Update.
3. On the Automatic Update screen, turn Show notification YES.
   By default, this feature is enabled. If Show Notification is turned on, you receive a notification each time new updates are received and you get a notification pop-up on Dashbaord.

4. Select one of the following:
   - Download from Internet: This option helps you download the updates to your machine from Quick Heal server. This option is selected by default.
   - Pick from specified path: Select this option if you want to pick the updates from a local folder or a network folder. This is helpful when your machine is not connected to the Internet. After selecting this option, browse the path to pick the updates from the shared location.
5. Switch Save update files to YES.
   Select this option if you want to save a copy of the updates downloaded to your local folder or network folder. The Browse button is enabled. The Save update files option is enabled when you select Download from Internet.
6. Click Browse to specify a folder or network folder to save a copy of the updates downloaded from the Internet.
7. To save your settings, click Save.

Self Protection

With Self Protection, you can restrict unauthorized users from altering or tampering the files, folders, configurations, and List entries of Quick Heal Total Security configured against malware. It is recommended that you always keep Self Protection turned on.

Configuring Self Protection

To configure Self Protection, follow these steps:

1. On the Quick Heal Total Security Dashboard, click Settings.
2. On the Settings screen, turn Self Protection ON.
   However, Self Protection is turned on by default.

Password Protection

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

Configuring Password Protection

To configure Password Protection, follow these steps:

1. On the Quick Heal Total Security Dashboard, click Settings.
   Password Protection is turned off by default that you can turn on if required.
2. On the Settings screen, turn Password Protection ON.
   The password protection screen appears.
3. Enter password in the New Password text box and then confirm the password by entering it in Retype New Password.
   If you are setting the password for the first time, then Existing Password is disabled.
4. To reset your password, click Password Protection.
5. To save your setting, click Save.

Proxy Support

With Proxy Support, you can enable proxy support, set proxy type, configure IP address, and port of the proxy for using Internet connection. If you are using a proxy server on your network, or using Socks Version 4 & 5 network then you need to enter the IP address (or domain name) and port of the proxy, SOCKS V4 & SOCKS V5 server in Internet settings.

However, if you configure Proxy Support, you have to enter your user name and password credentials. The following Quick Heal modules require these changes:

- Registration Wizard
- Mac Security Update
- Web Security (Browser protection, Phishing protection and Parental Control)

Configuring Proxy Support

To configure Proxy Support, follow these steps:

1. On the Quick Heal Total Security Dashboard, click Settings.
2. On the Settings screen, click Proxy Support.

3 On the Proxy Support screen, turn Proxy support ON to enable proxy support.
The Select proxy type, Enter server, Enter port, and user credentials text boxes are enabled.

4 Select the proxy type from HTTP, SOCKS V4, SOCKS V5 based on your preference.

5 In the Enter Server text box, enter the IP address of the proxy server or domain name.

6 In Enter port text box, enter the port number of the proxy server.
By default, port number is set as 80 for HTTP and 1080 for SOCKS V4, SOCKS V5.

7 Enter user name and password credentials.

8 To save your settings, click Save.

Report Settings

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

Configuring Report Settings

To configure Report Settings, follow these steps:

1. On the Quick Heal Total Security Dashboard, click Settings.
2. On the Settings screen, click Report Settings.
3. On the Report Settings screen, turn Automatically delete reports ON to remove reports after the specified number of days. If you want to retain all the reports generated, turn Automatically delete reports OFF.
4. Select the period from the Delete after list after which you want the reports to be deleted.
5. To save your setting, click Save.

7

Updating Software & Cleaning Viruses

The updates for Quick Heal Total Security are released regularly on the website of Quick Heal that contain detection and removal of newly discovered viruses. To prevent your machine from new viruses, you should have the updated copy of Quick Heal Total Security. By default, Quick Heal Total Security is set to update automatically from the Internet. This is done without the intervention of the user. However, your machine must be connected to the Internet to get the updates regularly. Automatic updates can also be applied from local or network path, but that path should have the latest set of definitions.

Some important facts about the Quick Heal Total Security updates are:

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

Updating Quick Heal Total Security from Internet

The Update Now feature keeps your copy of Quick Heal Total Security updated automatically through the Internet. However, your machine must be connected to the Internet to get the updates regularly. This feature works for all types of Internet connections (Dialup, ISDN, Cable, etc.).

You can also update Quick Heal Total Security manually whenever required so in any of the following's ways:

- Click the Quick Heal Total Security icon in the menu bar, and then select Update Now.

- If the Quick Heal Total Security Dashboard is open, click Update Now which appears if the protection is out of date.
- Open Quick Heal Total Security, and then on the menu bar, go to Quick Heal Total Security > About Quick Heal Total Security. On the About Quick Heal Total Security page, select Update Now.

  Update of Quick Heal Total Security is initiated.

  Ensure that your machine is connected to the Internet, Total Security Update connects to the Quick Heal Total Security website and downloads the appropriate update files for your software and applies it thereafter to your copy thus updating it to the latest available update file.

Updating Quick Heal Total Security with definition files

If you have the update definition file with you, you can update Quick Heal Total Security without connecting to the Internet. It is useful for Network environments with more than one machine. You are not required to download the update file on all the machines within the network. You can download the latest definition files from the Quick Heal website on one computer and then update all other machines with definition files.

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

1. On the Quick Heal Total Security Dashboard, click Settings.
2. Turn Automatic Update ON, and then click Automatic Update.
3. Turn Show notification ON to receive notification when updated is needed.
4. Check Pick from specified path, and then specify the location from where the updates are to be picked up.
5. To save your settings, click Save.

   Your copy of Quick Heal Total Security is updated from the specified location.

Update Guidelines for Network Environment

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

1. Setup one computer (may be a server) as the master update machine. Suppose server name is SERVER.
2. Make QHUPD folder in any location. For example: QHUPD.
3. Assign the Read-Only sharing right to this folder.
4. On the Quick Heal Total Security Dashboard, click Settings.
5. On the Settings screen, click Automatic Update.
6. Switch Save update files to Yes.
7. Click Browse and locate the QHUPD folder. Click Open.
8. To save your setting, click Save.
9. On all other computers within the network, launch Quick Heal Total Security.
10. Go to the Settings details screen and select Automatic Update.
11. Select Pick update files from specified path.
12. Click Browse.
13. Locate the SERVER₩QHUPD folder from Network Neighborhood. Alternatively, you can type the path as ₩₩SERVER₩QHUPD.
14. To save the settings, click Save.

Cleaning Viruses

Quick Heal warns you of a virus infection when:

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

Cleaning viruses encountered during scanning

Quick Heal Total Security is adequately configured with all the required settings with default installation to protect your machine. If a virus is detected during scanning, Quick Heal Total Security tries to repair the virus. However, if it fails to repair the files of the viruses, such files are quarantined. In case you have customized the default scanner settings, then take an appropriate action when a virus is found.

Scanning Options

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

Options	Description
Status Tab	Displays the status on scanning.
Action Tab	Displays the action taken on the files.
Pause	Helps you pause scanning while scanning is under process. This is a temporary break and you may restart scanning after some time.
Stop	Helps you stop the scanning process. This is a permanent break and you cannot restart scanning from the same instance.
Scanning Status	Displays the status of scanning process in percent.

8

Technical Support

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

Help

The Help options provide comprehensive support where you can find answers to your queries in a wide variety of ways. You can find answers to frequently asked questions, send an email about your queries, or call our technical support team.

The Help includes the following.

FAQs

FAQs help you find answers to the most frequently asked questions and concerns. Moreover, it is advisable that you check the FAQs at least once before using other support options, as you may find an answer to your question there.

To use FAQs, follow these steps:

1. On the Quick Heal Total Security menu bar, go to **Help**.
2. Click **Visit FAQs** under **FAQs**.

   Check the FAQs for answers to your questions. If you do not find an appropriate answer, then submit your queries to us.

Email Support

With Email Support, you can send us an email about your queries so that experts at Quick Heal can reply to you with an appropriate answer.

To use Email Support, follow these steps:

1. On the Quick Heal Total Security menu bar, go to **Help**.
2. Click **Send Email** under **Email Us**.

Call Us

With Call Us, you can call our Quick Heal technical experts for instant support.

The following are the contact numbers for phone support: 1800-121-7377 / 7030067377.

Support hours: Monday–Sunday, 7:00 AM–11:00 PM IST.

Remote Session

With Remote Session, you can connect your system remotely with our support experts. Remote Session is useful when you need assistance from our experts. However, it is advised that you use this support when you are connected over telephone.

To use Remote Session, follow these steps:

1. On the Quick Heal Total Security menu bar, go to **Help**.
2. Under **Remote Session**, click **Start Session**.
   The Remote Support terms agreements screen appears.
3. Click I Agree.

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

Live Chat

With Live Chat, you can connect with Quick Heal technical experts for assistance with your queries.

To use Live Chat, follow these steps:

1. On the Quick Heal Total Security menu bar, go to Help.
2. Under Live Chat, click Website or WhatsApp to connect with Quick Heal support.

Support Guidelines

When is the best time to call?

Quick Heal Technologies Ltd. provides technical support Monday–Sunday, from 7:00 AM to 11:00 PM IST (Indian Standard Time).

Which number to call?

Quick Heal users in India can call +91 - 70300 67377.

Quick Heal users in India can also call us at the Toll-Free support number 1800-121-7377.

For support in other Countries:

Email: support@quickheal.com

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

For country-specific support, visit: https://www.quickheal.co.in/support

Details that are necessary during the call

- Product Key: Is included inside the box of your product. If the product is purchased online, then the Product Key can be obtained from the email confirming the order.
- Information about the Mac computer: Brand, processor type, RAM capacity, the size of the hard drive and free space on it, as well as information about other peripherals.
- Operating System: name, version number, language.
- Software Version: Version of the installed anti-virus and the virus database.
- Software Type: Software product installed on the machine.

- Internet Connection: Is the machine connected to a network? If yes - contact the system administrators first. If the administrators can't solve the problem, they should contact the Quick Heal technical support.
- Other Details: When did the problem first appear? What were you doing when the problem appeared?

What should I say to the technical support personnel?

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

Contact Quick Heal Technologies

Quick Heal Technologies Limited
(Formerly Known as Quick Heal Technologies Pvt. Ltd.)
Registered office at CTS No. 1442 to 1445 Thube Park,
Shivaji Nagar, Pune – 411005.

Telephone: +91 20 66813232
Email: info@quickheal.com

Official Website: www.quickheal.com