Quick Heal

Security Simplified

Q Quick Heal Total Security

User Guide

Version 2.01

Copyright & License Information

Copyright © 2016 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.

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 Total Security. The following table lists the conventions that we 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 menu, dialog, button names, hyperlinks, and so on.
	This is a symbol used for a note. Note supplements important points or highlights information 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 a task in an easy way.
	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.

Document History

Release No	Change Date	Change Summary
2.01.00.066	Nov 2016	Support contact number updated.

What's New in this Version?

Features	Description	Section
India contact support	The contact number of the support team is changed.	Indian contact support page no. 50

Contents

Chapter

1

Getting started

Quick Heal Total Security is simple to install and easy to use application. During installation, read each installation screen carefully and follow the instructions. Quick Heal Total Security is compatible with the Android platform.

To install Quick Heal Total Security, ensure that you comply with the following requirements:

Prerequisites

System requirements

Prerequisites

Remember the following guidelines before installing Quick Heal Total Security on your device:

- A device with multiple antivirus software applications installed may result in system malfunction. Before installing Quick Heal Total Security, you must remove other antivirus programs to avoid any issues.
- Close all open apps before installing Quick Heal Total Security.

System requirements

You can install Quick Heal Total Security on any Android-supported mobile devices. Supported Android versions and screen resolutions are as follows:

Supported Android Versions

Quick Heal Total Security is compatible with the following versions: 2.3, 3.0, 4.0, and later.

Supported Android Screen Resolutions

The following Android screen resolutions are supported:

- Small screen – 240 x 320
- Normal screen – 320 x 480
- Large screen – 480 x 800
- Extra-large screen – 600 x 1024 (Newly added for tablet)

Installation of Quick Heal Total Security

You can install Quick Heal Total Security as follows:

[Downloading Quick Heal Total Security installer](#)

[Installing Quick Heal Total Security](#)

Downloading Quick Heal Total Security installer

Download the Quick Heal Total Security installer from the following website: http://www.quickheal.com/installer.

To download the installer, you need to enter a 20-digit valid product key of Quick Heal Total Security.

You can get the product key in the following places:

- If you have purchased a box version, then the product key is printed on a card inside the box.
- If you have purchased it online, then it is sent to your email address.

Installing Quick Heal Total Security

To install Quick Heal Total Security, follow these steps:

1. If you have downloaded the installer file from the website directly to the device, tap the **installer** file (.apk).

   If you have downloaded the installer file to your computer (PC), copy the installer file to the device. On the device, tap the **installer file** (.apk).

   A screen requesting for your consent to proceed with the installation appears.

2. Tap **Install**.

   After successful installation of Quick Heal Total Security, two buttons **Open** and **Done** appear.

3. Tap **Done** to finish the installation process.

   The Quick Heal app is added to the All Apps list on your device.

4. To open the app, go to All apps and tap the **Quick Heal Total Security** icon.

   A license agreement screen appears.

   The **Allow to Collect app statistics** check box is selected by default. This helps to send the analytics data to Quick Heal Total Security app for research purpose. If you do not want to send the analytics data, clear this option.

   The **Receive SMS/Email alerts** check box is selected by default. This helps you to send the alerts and Quick Heal updates. If you do not want to send the SMS alerts, clear this option.

5. Tap **I Agree.**

You are redirected to the Activation screen where you must register your product.

To know about how to register your license, see Registering Quick Heal Total Security.

Chapter

2

Registration, reactivation, and renewal

After installation, you must register Quick Heal Total Security to use all the features and get technical support facility.

You can use and reactivate Quick Heal Total Security on any Android-supported mobile device. However, you have to use the same mobile number that you entered or used while registering the product for the first time.

In case you change your mobile device, ensure that you have deactivated and uninstalled the product from your previous mobile device.

Registering Quick Heal Total Security

You can register Quick Heal Total Security in the following way:

Registering licensed version

To register a licensed copy of the product, follow these steps:

1. Go to All apps on your device and tap the **Quick Heal Total Security** icon.

    The license agreement appears.

    The **Allow to Collect app statistics** check box is selected by default. This helps to send the analytics data to Quick Heal for research purpose. If you do not want to send the analytics data, clear this option.

    The **Receive SMS/Email alerts** check box is selected by default. This helps to send the alerts and Quick Heal updates. If you do not want to send the SMS alerts, clear this option.

2. Tap **I Agree**.

    You are redirected to the Activation screen where you must register your product.

3. Enter your 20-digit product key.

You can get the product key in the following places:

4. If you have purchased a box version, then the product key is printed on a card inside the box.

5. If you have purchased it online, then it is sent to your email address.

$\boxed{i}$ Note:

If you have not purchased a license yet, you can buy it by visiting our website. A link to our website is given on the License Activation screen.

---

6. Tap **Next**.

7. Enter user details: Name, Mobile Number, and Email ID. Ensure that you enter the same mobile number that you are using in the device currently. An SMS will be sent to your mobile number to authenticate it.

$\boxed{i}$ Note:

If you are activating the Quick Heal app through SMS, the mobile number verification will not be done.

---

8. If you have configured your Google account on your device, the Google email address is displayed in the Email ID field. However, you can change the email address if required.

9. Tap **Next**. The Configure PIN screen appears.

10. Set your 4-digit PIN (PIN) and then confirm the PIN.

$\boxed{i}$ Note:

In case your device is already registered, please be noted that the password that you have set during the registration is not valid anymore. Set a new 4-digit PIN and access the application normally.

---

11. Tap **Next**.

12. Set up to three alternate contacts. Enter contact name or mobile number, which is available in your device contacts/phonebook. Tap to select the required contact from the drop-down list.

13. You can add up to three contacts. Repeat step 9 to add multiple contacts.

14. Enable the **Uninstallation Protection** option to secure the Quick Heal app from being removed by any unauthorized user. However, in case of licensed version, this option is selected by default. (A recommended option).

15. Tap **Activate**.

> ℹ️ **Note:**
>
> If you have enabled the Uninstallation Protection option, you are redirected to Activate device administrator (ADA) screen, where you can activate the ADA.

16. After authentication of your mobile number, a successful message with expiry date is displayed.

As soon as your app is activated, a scan of all apps is initiated automatically.

> ℹ️ **Note:**
>
> - Currently registration and reactivation through SMS are available only to the users in India
>
> - Mobile numbers listed in the National Do Not Call Registry (DND) list may or may not be able to register, reactivate, and deactivate through an SMS depending on the government's current telephone regulatory policies.

Introducing Quick Heal RDM

Quick Heal introduces the Quick Heal Remote Device Management (Quick Heal RDM) portal to control and manage your devices remotely. Quick Heal RDM allows you to access various features of Quick Heal Total Security on your device, when the device is not physically accessible or you are unable to locate it, or it is lost or stolen.

You can manage the following features through the RDM portal:

Features	Description
Data Backup	Backup your personal data to the Quick Heal Cloud. In this way, you save your data in the Cloud. In case you need your data, you can restore it from the Cloud to your device.
Locate	- Trace your device - To track the device location, when it is lost or stolen. Trace your device is helpful in getting back your device if it is lost or stolen. - Ring– Add to play the ringing bell on your device so that you can trace it by the ringing sound if it is located nearby.
Lock	To block your device to prevent misuse of your data when it is lost or stolen. When the device is locked through RDM, the image of the surrounding area of the device and location is also captured and displayed on RDM.
Unlock	To unlock the device remotely if you get your lost device back or if you have blocked the device by mistake.

Features	Description
Wipe	To wipe your device data when it is lost or stolen. The data from both the internal and external memories will be wiped in this case.
Auto Dial/Receive	To dial a call from your lost device silently to another mobile. Also, you can pick up a call on your lost or stolen device silently.
Auto Capture Image	To capture images of the surrounding area of the lost device secretly and the images are sent to your Cloud account and email address.
Auto Record Audio	To record audio of one minute on your device silently and the audio is sent to your Cloud account and email address.
Auto Record Video	To record video of one minute on your device silently and the video is sent to your Cloud account and email address.
Scan Device	To run a scan on the remote device if required.
Full Scan	To run a full scan of the device.
Scan Memory Card	To scan the memory card.
Background Scan	To change the Background Scan settings on your device remotely.
Automatic Backup	To change the Automatic Backup settings on your device remotely.
Parental Control	To configure the Parental Control settings on your device remotely.
Update virus database	To remotely update the virus database of Quick Heal Total Security on your device.
Privacy Protection	To maintain a private contacts list and secure important call logs and messages from such contacts.
Forward all calls	You can set a number to which you want all your incoming calls are forwarded. You can also enable/disable Call Forwarding option through remote SMS commands. The command should be in the following format: START_FORWARD <PIN> <number to which calls are to be forwarded> However, you can stop call forward whenever you want. To stop call forward, send the following command: STOP_FORWARD <PIN>

Features	Description
Set Privacy	To block calls and messages from unwanted callers. Disabling **Set Privacy** will disable **Call & Message Filter** feature.

Creating an account with Quick Heal RDM

Before you create an account with the Quick Heal RDM portal, you must activate Quick Heal app on your device with a valid product key. To know about how to activate Quick Heal app, see [Registering licensed version](#).

1. After your device is registered on Quick Heal Total Security, 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**.

   You have successfully created an account with the Quick Heal RDM portal. From now, you can manage your device through the Quick Heal RDM portal.

Signing up with Quick Heal RDM

You can create an account with the Quick Heal Remote Device Management (RDM) portal manually in the following way:

1. Visit Quick Heal RDM at 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 the Quick Heal RDM portal.

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

   Your account with the Quick Heal RDM portal is created successfully. From now, you can manage your device through Quick Heal RDM.

Signing up with Quick Heal RDM with Google account

You can create an account with the Quick Heal Remote Device Management (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 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**.

   You have successfully created an account with the Quick Heal RDM portal. From now, 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 a device to Quick Heal RDM

When you first log on to the Quick Heal RDM portal, configure the Add Device page that appears. To manage your device remotely, you need to add your devices in Quick Heal RDM.

To add a device, follow these steps:

1. Visit Quick Heal RDM Portal at https://mydevice.quickheal.com.

2. Log on to the Quick Heal RDM portal.

   The Add Device page appears.

3. In the **Name** text box, write a name to the device.

4. In the **Product Key** text box, the product key is already pre-filled.

5. Click **Add**.

   A One Time Password (OTP) is sent to your device. The **One Time Password** text box, **Submit** and **Resend OTP** buttons are made available on the Quick Heal RDM portal.

6. Enter the One Time Password and click **Submit**.

   The device is successfully added.

> **Note:**
>
> In case you do not receive OTP, you can send OTP again by clicking the **Resend OTP** button.

Enabling Manage Through Web

To manage Quick Heal Total Security on your device through Quick Heal Remote Device Management, it is important that you always keep the option **Manage Through Web** enabled. However, you can disable this option if you do not want to control the device through the web portal or the device.

To enable Manage Through Web, follow these steps:

1. Open **Quick Heal Total Security**.

2. Tap the **main menu,** and then tap **Settings**.

3. Tap **General** and then select the **Manage Through Web** check box.

Reactivating Quick Heal Total Security

Reactivation of Quick Heal Total Security ensures that you use the product until the liable license period. You may need to reactivate your product if you have removed it from your device in cases such as, you format your device, or you change your device.

Reactivation of Quick Heal Total Security using the same product key is possible only with the registered mobile number on any mobile device.

Reactivating licensed version

To reactivate Quick Heal Total Security license, follow these steps:

1. Go to All apps on your device and then tap the **Quick Heal Total Security** icon.

   The license agreement appears.

   The **Allow to Collect app statistics** check box is selected by default. This helps to send the analytics data to Quick Heal for research purpose. If you do not want to send the analytics data, clear this option.

   The **Receive SMS/Email alerts** check box is selected by default. This helps to send the alerts and Quick Heal updates. If you do not want to send the SMS alerts, clear this option.

2. Tap **I Agree**.

   The License Activation screen is displayed.

   If your device is not connected to the Internet, a screen with the option **Try with SMS** appears. This helps you to activate your product through SMS. However, if SIM is not present in the device, a message that your device is not connected to the Internet appears.

3. Enter your 20-digit product key.

   You can get the product key in the following places:

4. If you have purchased a box version, it is printed on a card inside the box.

5. If you have purchased it online, it is sent to your email address.

i Note:

If you have not purchased a license yet, you can buy it by visiting our website. A link to our website is given on the License Activation screen.

6. Tap **Next**.

7. Set your 4-digit PIN (PIN) and then confirm the PIN.

i Note:

In case your device is already registered, please be noted that the password that you have set during the registration is not valid anymore. Set a new 4-digit PIN and access the application normally.

8. Tap **Next**.

9. Set up to 3 alternate contact numbers. Enter contact name or mobile number, which is available in your device contacts/phonebook. Tap to select the required contact from the drop-down list.

10. You can add up to three contacts. To add multiple contacts, repeat step 7.

11. If you want to secure the Quick Heal app from being removed by any unauthorized user, enable the **Uninstallation Protection** option. However, in case of licensed version, this option is selected by default. (A recommended option).

12. Tap **Activate**.

i Note:

If you have enabled the Uninstallation Protection option, you are redirected to Activate device administrator (ADA) screen, where you can activate the ADA.

13. Your license is reactivated successfully, and you will also get the expiry date of your license.

As soon as your app is reactivated, a scan of all apps is initiated automatically.

i Note:

- Currently registration and reactivation through SMS are available only to the users in India

- Mobile numbers listed in the National Do Not Call Registry (DND) list may or may not be able to register, reactivate, and deactivate through an SMS depending on the government's current telephone regulatory policies.

Renewal of Quick Heal Total Security

Quick Heal Total Security is renewed as follows:

Renewing licensed version

If your product license has expired, you cannot use important features of Quick Heal Total Security. Therefore, your mobile device gets exposed to different types of threats. To avoid this, we strongly recommend you to renew your license before it expires.

To renew your license copy of Quick Heal Total Security, follow these steps:

1. Open **Quick Heal Total Security**.

2. Tap the **main menu** and then tap **About Product**.

3. Tap **Renew**.

4. On the **Renew License** screen, enter the renewal key and tap **Next**.

   Your license is successfully renewed.

   If your device is not connected to the Internet, a screen with the option **Try with SMS** appears. This helps to renew your product through SMS. However, if SIM is not present in the device, a message that your device is not connected to the Internet appears.

   If you do not have a renewal key, you can purchase it by visiting our website. A link to our website is given on the **Renew License** screen.

Buying a renewal key

You can renew your license by using one of the following ways:

Renew Online

You can buy a renewal key and renew the license online. After renewing your license online successfully, you need to update your license information on the device by going to Quick Heal Total Security Dashboard > main menu > About Product > Update.

Call Us

You can call our Renewal team to assist you in buying a renewal key and renewing your license.

Locate Dealer

You can contact the nearest dealer in your locality to buy a renewal key.

[i] Note:

If you renew online or you get your license renewed by our Support team, you need not proceed with renewal as it is already done. However, if you buy a renewal key and want to renew manually, follow the steps mentioned in Renewing license version section.

Chapter

3

Quick Heal Total Security Dashboard

Quick Heal Total Security Dashboard is the main area, which appears on your mobile device screen when you open the application. Dashboard includes the following areas:

Message Center

Message Center includes notifications. If you have enabled notification for a feature, the notification will be displayed here.

Main menu

Main menu or global menu is available in the notification area. With this menu, you can set various features for securing your device and data.

To know about various features of the main menu, see [Main menu](#).

Dashboard alerts of Quick Heal Total Security

Dashboard alerts displays status of various events such as the Background Scan is enabled or disabled, your license is going to expire or has expired. The Dashboard alert messages, which remind you of the actions to be taken to avoid any mishap, includes the following based on current events:

- Register Now!
- License expires today!
- License expired!
- Device is secure!

Security Shield

Security shield displays the security level through a graphical representation based on the security measures that you have set on your device and for the data. You can increase the device security if required.

To know about various features of security shield, see [Security Shield](#).

Menus

On Dashboard, you can see the following menus:

Scan Device

Scan your phone memory, memory card, and installed applications.

Optimize Device

Checks your device performance, increase its speed and check network usage.

Secure Data

To secure your data. You can back up the data in the Cloud and restore the data from the Cloud to your device whenever required. You can delete the data from the Cloud as well as personal data.

Set Privacy

To block calls and messages from unwanted callers, and make contacts private so that only you can access them. For safe browsing experience, you can set Parental Control for your children and other users. You can also register your number with National Do Not Call Directory to block commercial calls and messages.

To know about various features of menus, see [Menus on Dashboard](#).

Chapter

4

Quick Heal Total Security Features

Quick Heal Total Security provides various security features that help you secure your device and your data. Features include the following options:

Security Shield

Menus on Dashboard

Main menus

Security Shield

Security shield displays the security level through a graphical representation based on the security measures that you have set on your device and the data. You can increase the security level whenever the device requires.

To increase the security level, follow these steps:

1. Open **Quick Heal Total Security**.

2. Tap **security shield.**

3. On the Security Measures screen, enable the features that you need to enhance security to your device and data.

Security measures include the following options:

Security Measures	Description
Background Scan	Enable **Background Scan** to scan your device continuously. This helps you to scan all apps, files, and data in real time and will detect threats instantly.
Action on Detected Virus	Enable **Action on Detected Virus** to take an action on a virus that is detected on your device. The action will be taken automatically according to the settings that you have configured. Actions include Repair, Delete, and Skip.
Anti-Theft	Enable **Anti-Theft** to track and locate your device when it is lost or stolen. If this feature is disabled, the device cannot be tracked.
Auto-Backup	Enable **Auto-Backup** to back up your data to the Quick Heal Cloud. You can retrieve your data whenever you require. This helps you in case you change your device or if your previous device is lost.
Browsing Protection	Enable **Browsing Protection** to block infected websites when you connect to the Internet on your device. This protects your device from all the infected websites and keeps you safe from any kind of malware.
Network Monitor	Enable **Network Monitor** to monitor and control the Internet usage. This helps you manage your Internet bandwidth.
Parental Control	Enable **Parental Control** to block unwanted content when browsing websites. You can block the websites that include adult content and social networking websites. This way you can ensure that your children or other users do not visit any unwanted websites.
Personal Security	Enable **Parental Control** if you want help when there is an emergency. We recommend you always to keep this feature enabled so that an SOS message with your current location is sent to alternate contacts on the device and social networking sites. If this option is disabled, you cannot send panic alert or message.
Phishing Protection	Enable **Phishing Protection** to block fraudulent websites that try to steal your valuable data such as bank details, user credentials, social security information, and PIN.
Power Saving	Enable **Power Saving** to save power. Power saving mode takes various actions to save power so that your battery lasts longer. You can kill all running apps, stop network usage, and reduce screen brightness.

Privacy Advisor	Enable **Privacy Advisor** and get alerts when your privacy is violated. For example, when you install apps on your device, some of them use your user credentials, which you may not prefer.
Security Advisor	Enable Security Advisor to get an alert if the security settings on your device are low. This helps you to enhance your device security.
Uninstallation Protection	Uninstallation Protection when enabled blocks an unauthorized user from uninstalling Quick Heal app from your device. In case your device is lost or stolen, you may need to communicate with your device to track or locate it or perform other actions. To communicate successfully, it is important that Quick Heal is active on your device.
Find Intruder	Enable **Find Intruder** to capture an image of an intruder on two wrong PIN attempts.

Menus on Dashboard

The menus on Dashboard includes the following options:

Scan Device

With the **Scan Device** option, you can scan your device and set security measures against possible vulnerabilities and privacy violation. Scanning of your device helps you give a clear idea about whether your device is secure. You can take appropriate actions to enhance your device security.

To scan your device, follow these steps:

1. Open **Quick Heal Total Security**.

2. On Dashboard, tap **Scan Device**.

3. Tap one of the following scan options:

[Quick Scan](#)

[Custom Scan](#)

[Schedule Scan](#)

Quick Scan

This is a fast scan and scans all the apps installed on your device.

Custom Scan

Lets you to select one of the various scan options. You can customize and initiate a scan as per your requirement. This includes the following:

Full Scan

Full scan is a complete scan, which scans your device and memory card. However, this scan may take some time to complete the action.

Scan All Apps

Scans all the installed apps.

Scan Selected Apps

Scans only the selected apps from all those apps that are installed on your device. When you select this scan option, all the apps are displayed in the **Select Apps** list. Select the apps and tap **Scan**.

Scan Memory Card

Scans memory card only.

Scan Selected Folders

Scans folders, which are selected by you on your device. When you select this scan option, all the folders are displayed in the **Select Folders** list. Select the folders and tap **Scan**.

Schedule Scan

Schedule Scan helps you to scan at the scheduled time and frequency. This helps you to scan your device at the defined schedule automatically.

To create a scan schedule, follow these steps:

1. Open **Quick Heal Total Security**.

2. On Dashboard, tap **Scan Device.**

3. Tap **Schedule Scan**.

   The **Scheduled Scans** screen displays all the planned scans if you have created any.

4. To set a new scan schedule, tap **Schedule New Scan**.

5. Under **Select Data**, select one of the following scan options: Full Scan, Scan All Apps, Scan Selected Apps, Scan Memory Card, and Scan Selected Folders.

6. Under **Set Time & Frequency** section, set time and frequency to start the scan automatically.

   Time & Frequency includes the **Scan while charging** options: Once a day, Once a week, and Once a month.

[i] Note:

- If Scan while charging is opted then, your device is scanned once in 24 hours while charging with battery level at least 50% or more.

- If you select **Once a day**, specify the time.

- If you select **Once a week**, specify day and time.

- If you select **Once a month**, specify date and time.

Security Advisor

With the **Security Advisor** option, you can check the possible vulnerabilities present on the device. You can enhance the security settings to stop such attempts to exploit vulnerabilities.

To configure Security Advisor, follow these steps:

1. Open **Quick Heal Total Security**.

2. On Dashboard, tap **Scan Device**.

3. Tap **Security Advisor**.

4. In **Security Advisor** screen, the security settings are displayed under following categories:

   - Risk Settings: The security settings, which are insecure, are listed here.

   - Secure Settings: The security settings, which are secure, are listed here.

The security settings that are listed under Risk Settings include a setting icon next to them. You can increase the security level by using the setting icon. When you tap the setting icon, you are redirected to the respective security features where you can configure them.

Security settings are as follows:

Security Settings	Description
Accounts & Sync	Device receives data from synced accounts or sites that increases the risk of hacking and account misuse. It is advisable to turn this option to off when not required.
Bluetooth	Data transfer through Bluetooth might put your device and its data at risk. It is advisable to turn this option to off when not required.
Device memory encryption	You can encrypt the data on your device. This ensures security by preventing unauthorized access to your data. [i] Note: The Device Memory Encryption setting is available only on supported OS.

Hotspot & Tethering	Data shared through Wi-Fi Hotspot, USB and Bluetooth Tethering is at risk to be hacked. To prevent data hacking, turn this option to off when not required. ⓘ Note: The Hotspot and Tethering setting is available only on supported OS and vendo
Quick Heal Anti-Theft	Protects your device and its data. With the **Quick Heal Anti-Theft** option, you can trace, block, wipe data, dial a call, receive a call, capture image, record audio and video if your device is lost.
Quick Heal Background Scan	Shields your device against various types of threats. Keep this option enabled for security.
Screen Lock	If this option is disabled, your personal data may be at risk of misuse. Ensure that one of the screen lock options is set to safeguard device data.
Unknown App Sources	If any app is installed from a source other than Google Play, then that app might pose a threat to your device. Therefore, it is advisable that you turn this option to off.
USB Debugging	If USB debugging is enabled, your device is at risk of being hacked and your data can be misused. Turn this option to off for security.
Wi-Fi	Communicating through an open or unsecured Wi-Fi network can put your data at risk. It is advisable to connect Wi-Fi only on a secure network.

Privacy Advisor

With the **Privacy Advisor** option, you can detect the applications that collect your personal information such as user credentials, contacts, social security number, and PINs. You can also get notifications about those applications, which send SMS, call premium numbers or access Internet without your knowledge.

You can monitor applications with various permissions such as Access to Accounts, Access to Contacts, Read Identity Info, Tracking Location, Access to Messages, and Access to Network.

To configure Privacy Advisor, follow these steps:

1. Open **Quick Heal Total Security**.

2. On Dashboard, tap **Scan Device**.

3. Tap **Privacy Advisor**. The applications are displayed with the permissions that are assigned.

To view the permissions that an app is assigned, tap the application. If you find that an app uses any crucial information, you can uninstall that app by tapping the **Uninstall** button.

Various permissions that an app may use are as follows:

Permissions	Description
Access to Accounts	Apps with this permission may request authentication credentials of the account. Such apps may add or remove accounts and delete your PIN.
Access to Contacts	Apps with this permission can read, write, and share your personal contacts with their servers by compromising your data.
Read Identity Info	The apps with this permission can share phone state including IMEI number, phone number, and serial number of the phone to their server without your consent.
Tracking Locations	Apps with this permission can update your device location to their servers, which may be harmful.
Access to Messages	Apps with this permission are allowed to read, write, or send SMS from the device. Malicious apps may read your confidential messages or delete them before you receive.
Access to Network	Apps with this permission allow network usage in the background.
Other Permission	Apps that have permissions other than those mentioned above are available under this category.

Privacy Audit Notification

When you install a new app on your device, a notification for Privacy Audit is displayed on the notification area after 15 days. However, the Privacy Audit notification is displayed as soon as you install 10 or more apps within 15 days. You can check the apps for what permissions they are using. If you find that an app violates your privacy or your personal information is at risk, you can remove that app immediately.

Optimize Device

The **Optimize Device** option checks your device performance and increases the security measures if required. It kills running apps to increase the device speed, and provides a summary of the network usage. Optimize Device includes the following:

Performance Summary

Kill Running Apps

Apps Safe List

Performance Summary

Performance Summary shows current performance of your device. It includes number of all running apps, CPU usage, battery level, and memory usage.

Based on the device performance a graph is displayed as Low, Medium, and High. If you find that the device is slow, you can increase the device speed by killing the running apps by using the following options:

Speed Up Device

Kills all the running apps to increase the device performance.

View Running Apps

Lets you to view all the running apps and kill them selectively. You can see the details of all running apps, sort them based on usage (Memory usage, CPU usage, and RAM usage) or their name and add them to Safe List.

When you tap **View Running Apps**, the Running Apps screen appears.

Select the apps and tap **Kill App** to stop the apps or add them to **Safe List**. You can also uninstall such an app.

Kill Running Apps

With the **Kill Running Apps** option, you can increase your device speed. When you run a number of apps on your device, or sometimes third-party apps run automatically, they consume memory and reduce device speed. You can boost the device performance by killing the running apps.

To kill a running app, follow these steps:

1. Open **Quick Heal Total Security**.

2. On Dashboard, tap **Optimize Device**.

3. Tap **Kill Running Apps**.

   All the running apps are displayed.

   Carry out one of the following actions as required:

   - To kill an app, select the check box next to the app and tap **Kill App**.

   - To add an app to the Safe List, select the check box next to the app and tap **Add to Safe List**. If you want to remove an app from Safe List, you can do so by following the path Optimize Device > Apps Safe List.

Apps Safe List

Apps Safe List assists you to add apps installed on your device to the Safe List. This helps you not to kill these apps when you run the Kill Running Apps feature. However, it is advisable that you add only the required apps.

To add an app to the Safe List, follow these steps:

1. Open **Quick Heal Total Security**.

2. On Dashboard, tap **Optimize Device**.

3. Tap **Apps Safe List**.

   App Safe List appears. It displays the apps if you have added any.

4. To add a new app, tap **Add apps to safe list**.

   All the apps installed on your device are listed under **Select Apps**.

5. Select the check box next to the apps that you want to add and tap **OK**.

   You can remove an app from the Safe List if you want it to be killed.

Network Usage Summary

With the Network Usage Summary option, you can view a summary of your network setting in a graphical representation.

To view the summary, follow these steps:

1. Open **Quick Heal Total Security**.

2. On Dashboard, tap **Optimize Device**.

3. Tap **Network Usage Summary**.

   The Network Summary screen displays the current data usage of your network setting.

   If you access this screen for the first time, a link to set Data Usage is made available. Tap this link to configure the data usage limit. Once you set the link, it does not appear again.

Set Data Usage Limit

With the **Set Data Usage Limit** option, you can change the data usage limit.

To change the data usage limit, follow these steps:

i. Open **Quick Heal Total Security**.

ii. On Dashboard, tap **Optimize Device.**

iii. Tap **Network Usage Summary.**

iv. Tap the link **Set Data Usage Limit** for either Mobile Network or Wi-Fi Networks.

   The Mobile Network Monitor or Wi-Fi Network Monitor screen appears as per your selection.

The process for setting both the networks is similar.

v.　Configure the following options as required:

vi.　Billing Date: Set a billing date that monitors data usage for one month.

vii.　Set data usage limit: Enable this option to activate the succeeding options.

viii.　Max data usage limit: You can fix the maximum limit to control data usage.

ix.　Notify if data usage reaches: You can get alerts if the data usage reaches the set limit.

x.　Disconnect after max limit is reached: If this option is enabled, your network will be disconnected once the max data usage limit is reached.

xi.　Already used data from max limit: You can set a value of the network data that you have already used.

Reset Data Usage

With the **Reset Data Usage** option, you can clear current summary of data usage. The record will be restarted.

View App Data Usage

With the **View App Data Usage** option, you can view data usage for an individual app.

You can view further details of data usage of an app by tapping that particular app. This helps you find whether an app consumes data unnecessarily. To control this, you can take an appropriate action from the following:

- o　Add to Safe List: Helps you add an app to Safe List so that the app is not killed.
- o　Uninstall: Helps you uninstall the app that you think consumes data unnecessarily.
- o　Kill App: Helps you kill the app.

Secure Data

With the **Secure Data** option, you can secure your data by saving it to the Quick Heal Cloud. You can back up, retrieve, and delete data as per your requirement.

To use Secure Data, follow these steps:

1. Open **Quick Heal Total Security.**

2. On Dashboard, tap **Secure Data** and then select one of the following options:

- ▪　Backup data to Cloud: To save your valuable data such as Contacts, Calendar Events, and Messages (SMS) by saving them to the Cloud. This way your data is safe and you can retrieve it whenever you require.

- ▪　Restore Backup from Cloud: To restore data from Cloud to your device.

- ▪　Delete Backup from Cloud: To delete your backed up data from Cloud. Before you take this action, be sure that you do not require the data as it will be deleted permanently.

- Delete Personal Data: To delete personal data from your device.

Backup data to cloud

With the **Backup data to cloud** option, you can back up and save your data to Quick Heal Cloud. This is helpful in case you factory reset or lose your device resulting in loss of your data. You can restore your data from Cloud easily.

To back up the data, follow these steps:

1. Open **Quick Heal Total Security**.

2. On Dashboard, tap **Secure Data**.

3. Tap **Backup data to cloud**.

4. On the Backup Data screen, select the data that you want to back up.

5. To back up your data automatically to the Quick Heal Cloud at certain time, you can enable Auto-Backup.

   Alternately, you can also set Auto-Backup through Quick Heal Total Security Dashboard > **Secure Data** > Backup data to cloud > **Auto-Backup**.

6. Set time and frequency.

7. Tap **Save**.

Restore backup from cloud

With the **Restore backup from cloud** option, you can restore your data from Cloud to your device. However, the data restored will be from the date it was last backed up to the Cloud.

To restore your data, follow these steps:

1. Open **Quick Heal Total Security.**

2. On Dashboard, tap **Secure Data**.

3. Tap **Restore backup from cloud**.

4. On the Restore Data screen, select the data type that you want to restore.

5. Tap **Restore**.

   Note:

   Media data may not be restored on SD cards on devices with KitKat OS.

Delete backup from Cloud

With the **Delete backup from Cloud** option, you can delete all the data from the Cloud. However, before deleting the data, be sure that you do not require it as it will be deleted permanently.

To delete the data, follow these steps:

1. Open **Quick Heal Total Security**.

2. On Dashboard, tap **Secure Data**.

3. Tap **Delete backup from cloud**.

4. On the Delete Data screen, select the data type that you want to delete.

5. Tap **Delete**.

Delete Personal Data

With the **Delete Personal Data** option, you can delete personal data from the device. However, before deleting the data, be sure that you do not require it as it will be deleted permanently.

To delete the data, follow these steps:

1. Open **Quick Heal Total Security**.

2. On Dashboard, tap **Secure Data**.

3. Tap **Delete Personal Data**.

4. Select the data that you want to delete.

   Data to Delete includes Contacts, Calendar Events, Messages, SD Card (Internal & External), SIM Data (Contacts & Messages).

   i Note:

   Data from SD cards may not be deleted on devices with KitKat OS.

5. Tap **Delete**.

Set Privacy

With the **Set Privacy** option, you can block calls and messages from a contact, maintain a private contacts list, secure important call logs and messages from such contacts, set Parental Control. You can also register your number with National Do Not Call Directory to block commercial calls and messages.

To configure Set Privacy, follow these steps:

1. Open Quick Heal Total Security.

2. On Dashboard, tap **Set Privacy**.

3. Select one of the following options:

   Call & Message Filter

   Message Exception List

   Privacy Protection

Parental Control

Register with TRAI

Call & Message Filter

With the **Call & Message Filter** option, you can block calls and messages from a contact. In case of two SIMs in a dual SIM device, call behavior for different devices may differ from the device's SIM settings. In the same way, in case of two SIMs device, it initiates the call through primary SIM without asking the user for SIM selection. If there is only secondary SIM in the device, it initiates the call through secondary SIM.

To configure Call & Message Filter, follow these steps:

1. Open **Quick Heal Total Security**.

2. On Dashboard, tap **Set Privacy**.

3. Tap **Call & Message Filter**.

   The Blocked List includes:

   ▪ Blocked Numbers – Displays all blocked numbers.

   ▪ Blocked Keywords – Displays all blocked keywords.

Blocked Numbers

To block a number, tap **Add New Contact to Block** and select one of the following ways:

▪ Enter Number: You can type a number and select either or both of the options Block Call and Block Messages that you want to block. Tap **Add to Blocked Numbers List**.

▪ Phone Logs: You can choose a contact from phone logs and select either or both of the options Block Call and Block Messages that you want to block. Tap **Add to Blocked List**.

▪ Add from Contact List: You can add a contact from the phone book and select either or both of the options Block Call and Block Messages that you want to block. Tap **Add to Blocked List**.

▪ Custom: You can block all calls and messages from a series of certain numbers or characters (Ex: TM-LMFINE, 4000000000). You can also specify whether a contact should begin or end with such series.

$\boxed{i}$ Note:

- KitKat OS does not support SMS blocking.

- This feature will not block numbers configured in anti-theft or during the time of registration.

Blocked Keywords

To block a keyword, tap **Blocked Keywords**. Enter keyword to block messages and tap the plus sign. If a message includes such keywords, it will be blocked. This is helpful in blocking spams and other unwanted messages. To remove the keyword, tap the cross sign in front of the keyword.

Message Exception List

You can move a blocked non-numeric sender to this list if you want to receive messages from this contact.

To move a contact to this list, follow these steps:

1. Open **Quick Heal Total Security**.

2. On Dashboard, tap **Set Privacy**.

3. Tap **Call & Message Filter**.

4. Tap the minus sign next to a non-numeric sender.

    The sender is enlisted in Message Exception List.

Privacy Protection

Privacy Protection can maintain a private contacts list and secure important call logs and messages from such contacts. You can customize contacts, call logs, and SMS logs to be private or both private and non-private based on your priority. In case of two SIMs in a dual SIM device, call behavior for different devices may differ from the device's SIM settings. To configure Privacy Protection, follow these steps:

1. Open **Quick Heal Total Security**.

2. On Dashboard, tap **Set Privacy**.

3. Tap **Privacy Protection**.

4. To make a contact private, tap **New Private Contact**.

5. Type a contact in any of the following ways:

6. Enter Number: You can type a number.

7. Phone Log: You can select numbers from phone log.

8. Add from Contact List: You can add numbers from the phone book.

9. When you add a number, the following options may appear. Select any one or a combination of the following:

    - Contact

    - Call Logs

- SMS

Note:

- If you select the contact, it will be available exclusively in the private contact list. If you clear it, the contact will be present both in non-private contact list and private contact list.

- Also, if you select Call Logs and SMS, both the previous and future Call Logs and SMS will be made private.

- If you clear Call Logs and SMS, the previous Call Logs and SMS will be available exclusively in the device logs while future SMS and Call logs will be made private.

Conditions related to making contacts private

- If you make a contact with multiple numbers as private, all the numbers and their call and SMS logs will also be made private.

- If you want to get a notification when you get SMS from a private contact, you should ensure that the Notification option under Privacy Protection is selected. (Dashboard > main menu > Settings > Set Privacy > Notification).

- No backup will be provided for private data through the Backup feature.

- A blacklisted number cannot be made private. Hence, to make a blacklisted number private, first remove it from the blacklist.

Making a private contact non-private

You can restore a private contact to your device phone book whenever you prefer. To make a private contact non-private, follow these steps:

1. Open **Quick Heal Total Security**.

2. On Dashboard, tap **Set Privacy**.

3. Tap **Privacy Protection**.

4. Tap the minus icon next to a contact.

   The following options may appear depending on your device data:
   - Contact
   - Call Log
   - SMS

5. Select the options that you want to restore to the device.

   Clearing any of the options will delete them permanently.

6. Tap **OK**.

The contact along with the data is restored successfully.

If a contact with multiple numbers is made non-private, all the numbers and their call and SMS logs will also be made non-private.

[i] Note:

- If you want to uninstall Quick Heal app, it is recommended that you restore your private data before uninstalling the app to avoid data loss.

- If you are restoring a non-contact which has no SMS or call logs, that non-contact will be permanently deleted.

Privacy Protection after Quick Heal license expires

- All call logs and SMS of private contacts will be routed to the device logs instead of Private Contact list after the license expires.

- You cannot add contacts to the Private Contact list.

- You cannot view private contacts along with SMS and other details, but you can restore them to the device to view them.

Private Calls and SMS related facts

Some of the important facts related to private calls and SMS are as follows:

Calls

- You can view private call logs and call them back, delete such call logs, or send messages to them.

- Only last 200 call logs are saved in the private call log section. Entries exceeding that limit will be deleted automatically without any notification.

SMS

- You can view private SMS from private contacts and copy, delete, or forward such SMS to any other contacts.

- Only last 500 SMS are saved in the private SMS log section. Entries exceeding that limit will be deleted automatically without any notification.

KitKat OS Compatibility

- Privacy Protection does not support SMS on KitKat OS.

Impact of using the Delete Personal Data option on Privacy Protection

Using the Delete Personal Data option has the following impact:

Contacts

- If you delete the contacts using the Delete Personal Data option, the details of private contacts such as contact name, address, images, email address, and other details will be deleted. However, the contact numbers will remain in the private contacts list.

- Call logs of all private contacts will be deleted permanently and cannot be retrieved.

Messages

- If you delete the messages using the Delete Personal Data option, all the SMS of private contacts will be deleted permanently. However, the contact numbers will remain in the private contact list.

- You cannot retrieve all the SMS of the private contacts.

Using Wipe on Privacy Protection

- Using the WIPE command, you can delete your data from the lost or stolen device. After you send the wipe command, all your data from private and non-private contacts will be deleted permanently.

- You can send the WIPE command with any mobile device to your lost device. You can also send the WIPE command through our web portal Quick Heal RDM.

- Data that will be deleted includes contacts, SMS, Calendar events, and data of internal and external memory.

Parental Control

You can block infected and fraudulent websites with the help of Parental Control option. This prevents you from accessing unwanted sites that may harm you or may steal your confidential information. You can also control online activities of your children or other users of your mobile device.

To configure Parental Control, follow these steps:

1. Open **Quick Heal Total Security**.

2. On Dashboard, tap **Set Privacy**.

3. Tap **Parental Control**.

   Select one of the following options:
   - Block Access: To block access to particular websites. You can block websites by categories or by adding URLs.
   - Allow Access: To allow access to certain websites.

Block Access

You can block websites based on your priorities such as you do not want your children to access unwanted web sites or any suspected websites. You can block websites by categories or by adding URLs.

To block access to websites, follow these steps:

 i. Open **Quick Heal Total Security**.

 ii. On Dashboard, tap **Set Privacy**.

 iii. Tap **Parental Control**.

 iv. Tap **Block Access**.

  The Parental Control screen is displayed with two options, Block Categories, and Block URLs.

 v. Under Block Categories, select the categories that you want to block.

 vi. Tap **Block URLs**, type the website address that you want to block and tap the plus sign.

Allow Access

This option is helpful in case you have blocked an entire category, but you want to allow access to a certain website from the blocked category.

To allow access to certain websites, follow these steps:

 i. Open **Quick Heal Total Security**.

 ii. On Dashboard, tap **Set Privacy**.

 iii. Tap **Parental Control**.

 iv. Tap **Allow Access**.

 v. In Parental Control screen, tap **Enter URL to allow access** section and type the website address. Then tap the plus sign.

$\boxed{i}$ Note:

- The Parental Control feature supports Android's default browser and Chrome browser version 25 or later.

- Parental Control may not work properly on default browser of Android 4.0 and later.

- Parental Control does not support any beta versions of Chrome.

Register with TRAI

You can register your number with National Do Not Call Directory (TRAI) to block commercial or telemarketing calls. If you have Quick Heal app on your device and you are registering a number

with DND, you do not need to write SMS commands and send to 1909. India. You can simply register your number with the following options, Fully Block, and Partially Block, in the following way:

1. Open **Quick Heal Total Security**.

2. Tap **Set Privacy** and then tap **Register with TRAI**.

3. Register the number in one of the following ways:

   ▪ Fully Block: Lets you to block all commercial calls and SMSs.

   ▪ Partially Block: Lets you to block all commercial calls, but you will continue to get SMSs from the selected telemarketing categories.

   ▪ Report a Number: Lets you to report a number, which is sending an unsolicited call or SMS to you even after registering your number with DND. You should report such number within three days of receiving the call or message.

   [i] Note:

   • You can deregister your number later from DND list if required.

   • This option is unavailable outside India.

   • TRAI complaint may not be reported for Reliance SIM.

Main Menus

Main menu or global menu includes the following:

[Home](#)

[Settings](#)

[About Product](#)

[News](#)

[Logs](#)

[Help](#)

Home

With the **Home** option, you can go to the Home screen or Dashboard of Quick Heal Total Security.

Settings

Settings include features related to application settings such as setting PIN, securing uninstallation of Quick Heal app, setting scan options, setting privacy, and Anti-Theft.

To access Settings, follow these steps:

1. Open **Quick Heal Total Security.**

2. Tap main menu and then tap **Settings**.

3. Enter your PIN and then tap **Submit**.

    Settings screen appears.

Using Forgot PIN

If you have forgotten your PIN, you can reset it.

To reset your PIN, follow these steps:

1. Open **Quick Heal Total Security**.

2. Tap **main menu** and then tap **Settings**.

3. Tap **Forgot PIN**.

    The Get Temporary PIN screen appears.

    It includes a description about how to reset your PIN. A temporary PIN will be sent to your alternate contacts. You can also reset the PIN through Quick Heal RDM, as its URL is displayed on the screen.

    $\boxed{i}$ Note:

    Carrier charges may apply.

4. Tap **Yes**.

5. Check the message in alternate contacts and then type the temporary PIN on your device screen.

    The Reset PIN screen appears.

6. Type a new PIN and then retype it in Confirm PIN field.

7. Tap **Submit**.

    If your device is blocked and you have forgotten your PIN, you have to follow the same steps 1-7, as mentioned above, for unblocking the device.

    To know about the Setting features, see [Settings](#).

About Product

This section provides information on license details, product details, and other information.

To get product details, follow these steps:

1. Open **Quick Heal Total Security**.

2. Tap **main menu** and then tap **About Product**.

The About Product (Quick Heal Total Security) screen includes the following information:

Areas	Details	Buttons & Icons
Quick Heal Total Security product details	Product name & Version	Update: To update the virus database and license subscription details. Share: To share the link of Quick Heal app with your friends.
License Information	Product key & License expiry date	Renew: To renew the license. Extend: To extend your license validity for free if you refer Quick Heal app to your friends. However, this button does not appear if you use it once.
User Information	Username, User email address & Mobile Number	Update User Data Edit icon: To update your email ID and verify your mobile number. [i] Please note that after the number is successfully verified, you cannot verify again or update your mobile number.

News

With the **News** option, you can see the news related to virus threats, new malware, or any warning for digital security. Quick Heal sends the news to you regularly. Latest ten messages are displayed.

Logs

Logs include activity logs and information about the detected threats.

Activity

With the **Activity** option, you can see the activity logs of various features such as Anti-theft, Scan, Background Scan, Parental Control, and Update. You can filter the logs based on days and security features.

Threats Detected

To check the status of the infected files and apps. You can take an appropriate action on an infected app or even restore the quarantined files, which you think are useful to you.

Help

Quick Heal provides various methods to help you and resolve your issues.

For details on help, see [Help](#).

Settings

The Settings menu includes the following options:

[General](#)

[Scan](#)

[Set Privacy](#)

[Secure Data](#)

[Optimize Device](#)

[Personal Security](#)

[Anti-Theft](#)

General

With General option, you can configure features related to the application. This option includes the following:

Change PIN

This option helps to change your PIN. You need to enter the correct PIN to access **Settings** and **Anti-Theft** options.

To change the PIN, follow these steps:

1. Open **Quick Heal Total Security**.

2. Tap the **main menu** icon and then tap **Settings**.

3. Tap **General** and then tap **Change PIN**.

4. Type your new PIN and then retype it in Confirm PIN field.

5. Tap **Submit**.

Internet Settings

With the **Internet Settings** option, you can configure the Internet connection settings which are used by Quick heal Total Security.

To configure **Internet Settings**, follow these steps:

1. Open **Quick Heal Total Security**.

2. Tap the **main menu** icon and then tap **Settings**.

3. Tap **General** and then tap **Internet Settings**.

   Select one of the following networks:

   - Use Wi-Fi Only

   - Use Mobile Network Only

   - Use Any Network

Track Activity Log

With the **Track Activity Log** option, you can track activity logs of a certain period.

To configure Track Activity, follow these steps:

1. Open **Quick Heal Total Security**.

2. Tap the **main menu** icon and then tap **Settings**.

3. Tap **General** and then tap **Track Activity**.

   Select one of the following periods:

   - 7 days

   - 30 days

   - 45 days

Notification Icon

If you enable the notification option, the Quick Heal app icon and its current status are displayed in the device notification area.

To enable Notification icon, follow these steps:

1. Open **Quick Heal Total Security**.

2. Tap the **main menu** icon and then tap **Settings**.

3. Tap **General** and then tap the **Notification Icon** check box to enable the Notification icon.

Quick Setting Notification:

Enable the **Quick Setting notification** option to have a quick access to device setting options. This option includes the following: Wi-Fi, Bluetooth, Mobile Data, Brightness, and Torch.

To enable **Quick Setting Notification**, follow these steps:

1. Open **Quick Heal Total Security**.

2. Tap the **main menu** icon and then tap **Settings**.

3. Tap **General** and then tap the **Quick Setting Notification** Icon check box to enable the Quick Setting Notification Icon option.

Manage Through Web

You can manage Quick Heal Total Security on your device through Quick Heal Remote Device Management (Quick Heal RDM). You can perform various functions through this Cloud-based portal such as, you can back up the data to the Cloud, restore data from Cloud to your device, locate and track your device if it is lost or stolen. You can also perform many other activities to control your device and secure your data.

However, to control the device with Quick Heal RDM, it is important that you always keep the option Manage Through Web-enabled.

To enable Manage Through Web, follow these steps:

1. Open **Quick Heal Total Security**.

2. Tap the **main menu** icon and then tap **Settings**.

3. Tap **General** and then tap the **Manage Through Web** check box to enable it.

To know different features of Quick Heal RDM, see [Introducing Quick Heal Remote Device Management portal](#) (Quick Heal RDM).

News Notification

Quick Heal sends latest news related to virus threat, new malwares, or any warning for digital security in public interest to you regularly. All the news is listed under the Message Center. A notification about the latest news is also displayed on the notification bar. However, if you have disabled News Notification, you will not receive any notification either in the notification area or in Message Center.

It is advisable that you keep this option enabled, so you are updated with the latest news for security.

To enable News Notification, follow these steps:

1. Open **Quick Heal Total Security**.

2. Tap the **main menu** icon and then tap **Settings**.

3. Tap **General** and then tap the **News Notification** check box to enable it.

Application Statistics

Quick Heal is installed and used on a vast range of devices including mobile, tablet, and other handheld SIM or SIM-less devices. We strive to make our app more and more compatible with all the latest devices. To make our app more competent, we continuously carry out research on

our features and apps. To do this, we collect statistics from various sources and one of the source is the user community itself.

By enabling this option, you allow your app statistics to be shared with our server. However, you can disable it if you prefer.

To enable Application Statistics, follow these steps:

1. Open **Quick Heal Total Security**.

2. Tap the **main menu** icon and then tap **Settings**.

3. Tap **General** and then tap the **Application Statistics** check box to enable it.

Uninstallation Protection

The Uninstallation Protection option can secure the Quick Heal app from being removed by any unauthorized user. If you have a licensed copy, this option is selected by default. It is recommended that you always keep this option enabled. In case your device is lost or stolen, no one can remove the app from your device. This will help you to connect with your device to communicate and track it down.

To enable Uninstallation Protection, follow these steps:

1. Open **Quick Heal Total Security**.

2. Tap the **main menu** icon and then tap **Settings**.

3. Tap **General** and then select the **Uninstallation Protection** check box to enable it.

   You are redirected to the Activate device administrator (ADA) screen. Read the terms and conditions on the ADA screen.

4. To proceed further, tap **Activate**.

Find Intruder

Find Intruder option can detect if any unauthorized person has accessed your device. If an incorrect PIN is entered two times to unblock your device, an image of the user will be captured from front camera of the device. However, if your device does not have a front camera, no image will be captured.

If unblocking is attempted for Anti-theft, the image will be sent to your Cloud account. If it is attempted for device lock screen, the image is stored in the Quick Heal intruder folder of the device.

To enable Find Intruder, follow these steps:

1. Open **Quick Heal Total Security**.

2. Tap the **main menu** icon and then tap **Settings**.

3. Tap **General** and then select the **Find Intruder** check box to enable it.

Scan

With the **Scan** option, you can configure various scan options.

To set Scan, follow these steps:

1. Open **Quick Heal Total Security**.

2. Tap the **main menu** and then tap **Settings.**

3. Tap **Scan** and set the following:

    -   Background Scan: Helps you scan your device in real time. All apps, files, or folders that you access are scanned. If any threat is detected, the action that you set is taken immediately. To activate this option, enable Background Scan.

    -   Action when a Virus is found: Helps you select an action to be taken when a virus is detected on your device. The actions include Repair, Delete, and Skip. The selected action works automatically whenever a virus is detected.

    -   Delete Quarantined Files After: Helps you to set a period after which all the quarantined files should be removed. The period includes 7 Days, 30 Days, and 45 Days.

    -   Apps Excluded from Scan: Helps you exclude apps from being scanned. You are recommended to exclude only those apps which you trust. This helps you to reduce memory consumption.

    -   Folders Excluded from Scan: Helps you exclude folders to be scanned. You are recommended to exclude only such folders where you have placed trusted files. This helps you reduce memory consumption.

    -   Scan from Cloud: To run a cloud scan. This option helps you to scan through Cloud. Cloud scanning allows scanning of all the installed applications and .apk files available on the device storage. Enable this option to perform cloud scanning.

        Note:

        Ensure to check your Internet connectivity before performing cloud scanning.

Set Privacy

With the **Set Privacy** option, you can block non-numeric senders and international calls, get alert when you reject calls or delete SMS, enable Privacy Protection, Parental Control, and other features.

To configure Set Privacy, follow these steps:

1. Open **Quick Heal Total Security**.

2. Tap the **main menu** and then tap **Settings**.

3. Select the Set Privacy check box to enable it.

4. Tap **Set Privacy** to configure the following settings:

- Non-numeric Senders: Enable this option to block all non-numeric senders (Ex: TD-TMLN). In -addition, this option blocks Flash messages and WAP Push Messages.

- Notifications: This options is enabled to get notification for blocked calls and messages under Message Centre.

- Alert on Call Rejection: You can enable this option to get an alert when you reject a call. If you reject an unknown call, an alert is displayed for 20 seconds to add the rejected call to the Blocked List.

- Alert on SMS Delete: You can enable this option to get an alert when you delete an SMS. If you delete SMS from an unknown number or non-numeric sender, an alert is displayed for 20 seconds to add deleted sender to the Blocked List.

- International Calls: This option can be enabled to block all unknown international calls.

- Privacy Protection: Enable this option to activate Privacy Protection. To know about what features are in Privacy Protection, see [Set Privacy](#).

- Notifications: Enable this option to get notification when you get an SMS from a private contact under Message Centre.

- Parental Control: Enable this option to activate Parental Control. To know about what features are in Parental Control, see [Parental Control](#).

- Browsing Protection: Enable this option to activate Browsing Protection.

- Phishing Protection: Enable this option to activate Phishing Protection.

Secure Data

Secure Data option secures your data by saving it to Quick Heal Cloud. You can back up, retrieve, and delete data as per your requirement.

To use Secure Data, follow these steps:

1. Open **Quick Heal Total Security.**

2. Tap the **main menu** and then tap **Settings.**

3. Select the **Secure Data** check box to enable it.

4. Tap **Secure Data** to configure the following settings:

- Auto-Backup: Enable this option to take the backup automatically. If you enable this option, the succeeding options under Select Data to Backup are activated.

- Select Data to Backup: Select the data that you want to back up.

- Set Time & Frequency: Set time and frequency when the backup should be taken. Frequency includes: Backup while charging, Once a day, Once a week, Once a fortnight, and Once a month.

5. Tap **Save**.

Optimize Device

With the **Optimize Device** option, you can check your device performance, increase the device speed, and set network preferences.

To configure Optimize Device option, follow these steps:

1. Open Quick Heal Total Security.

2. Tap the **main menu** and then tap **Settings.**

3. By default, Optimize Device is enabled. If it is not enabled, select the **Optimize Device** check box.

   Optimize Device includes the following options:

   [Power Saving](#)

   [Speed Up Device](#)

   [Enable Network Monitor](#)

   [Mobile Network](#)

   [Wi-Fi Network](#)

Power Saving

With the **Power Saving** option, you can configure the settings to save power based on your priority.

To configure Power Saving, follow these steps:

1. Open **Quick Heal Total Security**.

2. Tap the **main menu** and then tap **Settings**.

3. By default, Optimize Device is enabled. If it is not enabled, select the **Optimize Device** check box.

4. Tap **Optimize Devic**e to configure the settings.

5. By default, Power Saving is enabled. If it is not enabled, select the **Power Saving** check box.

6. Tap **Power Saving** to configure the following settings:

   ▪ Activate Power Saving Mode When: Set the battery level when power saving mode should start.

   ▪ Set Screen Brightness to: Set the screen brightness after power saving mode starts.

   ▪ Disable Wi-Fi: Select this option to disable Wi-Fi network automatically when power saving mode starts.

- Disable Bluetooth: Select this option to disable Bluetooth network automatically when power saving mode starts.

- Disable Mobile Network: Select this option to disable mobile network automatically when power saving mode starts.

- Kill all Apps: Enable this option to kill all running apps when power saving mode starts. This helps in saving power.

- Do not Kill Apps in Safe List: Enable this option if the apps in the Safe List are not to be killed when you run Kill All Apps.

Speed Up Device

With the **Speed Up Device** option, you can increase the device speed.

To increase device speed, follow these steps:

1. Open **Quick Heal Total Security**.

2. Tap the **main menu** and then tap **Settings**.

3. By default, Optimize Device is enabled. If it is not enabled, select the **Optimize Device** check box.

4. Tap **Optimize Device** to configure the settings.

5. Tap **Speed Up Device** and then configure the following:

   - Kill Apps When Screen is OFF: Enable this option if you want to kill all running apps when screen is off.

   - Kill Apps When Screen is OFF for: Set a time when the running apps should be killed if the screen is off for some specific time. The time interval includes 4 hours, 2 hours, 1 hour, and 30 minutes.

   - Enable Apps Kill Schedule: Enable this option to schedule killing of running apps after certain intervals.

   - Kill Apps After: Set the interval after which Kill Apps should run again and again. The intervals include 12 hours, 9 hours, 6 hours, and 3 hours.

Enable Network Monitor

With the **Enable Network Monitor** option, you enable Network Monitor and set Mobile Network and Wi-Fi Network to control data usage limit.

To enable Network Monitor, follow these steps:

1. Open **Quick Heal Total Security**.

2. Tap the **main menu** icon and then tap **Settings**.

3. By default, Optimize Device is enabled. If it is not enabled, select the **Optimize Device** check box.

4. Tap **Optimize Device**.

5. Select **Enable Network Monitor** check box to configure Mobile Network and Wi-Fi Network.

Mobile Network

Mobile Network option sets data usage limit for mobile network.

To configure data usage limit, follow these steps:

1. Open **Quick Heal Total Security**.

2. Tap the **main menu** icon and then tap **Settings**.

3. By default, Optimize Device is enabled. If it is not enabled, select the **Optimize Device** check box.

4. Tap **Optimize Device.**

5. Tap **Mobile Network**.

> ![i] Note:
>
> If Mobile Network option is not enabled, then select the **Enable Network Monitor** check box.

6. Select the **Set data usage limit** check box and add different attributes to set data usage limit.

   To know how to configure data usage limit, see [Set Data Usage Limit](#).

Wi-Fi Network

With the **Wi-Fi Network** option, you can set mobile network.

To configure Mobile Network, follow these steps:

1. Open **Quick Heal Total Security**.

2. Tap the **main menu** and then tap **Settings**.

3. By default, Optimize Device is enabled. If it is not enabled, select the **Optimize Device** check box.

4. Tap **Optimize Device** to configure the Wi-Fi Network settings.

5. Tap **Wi-Fi Network**.

> ![i] Note:
>
> Ensure that Enable Network Monitor is enabled.

   To know how to configure data usage, see [Set Data Usage Limit](#).

Personal Security

With the **Personal Security** option, you can get help when you are in emergency or in danger by pressing the Power button for 7-10 times.

To configure Personal Security, follow these steps:

1. Open **Quick Heal Total Security**.

2. Tap **main menu** icon and then tap **Settings.**

3. Select the **Personal Security** check box to enable it

4. Tap **Personal Security** to configure following settings:

    ▪ SOS Message: Type a message to be sent in case of Emergency to alternate contacts that you have set at the time of registration and to your accounts of social networking sites. You can change these contacts any time from Anti-Theft setting.

    ▪ Send Panic Message: Enable this option if you want to send the SOS message and your location to alternate contacts when you are in emergency. If you disable this option, the SOS message and your location cannot be sent to alternate contacts.

Anti-Theft

With the **Anti-Theft** option, you can block or allow access to certain SIM cards, secure your device by automatically locking it when SIM is changed, track and control device remotely when it is lost or stolen, and update alternate contacts to which message is to be sent if the device is lost.

You can configure the following settings for Anti-theft:

SIM Card Settings

Lock on Airplane Mode

Track & Control Device

Lock Screen Details

Update Alternate Contacts

SIM Card Settings

With the **SIM Card Settings** option, you can block or allow access to certain SIM cards, set device to be locked as soon as SIM is changed and create a trusted SIMs list.

To configure SIM Card Settings, follow these steps:

1. Open **Quick Heal Total Security**.

2. Tap **main menu** and then tap **Settings**

3. Ensure if Anti-Theft is enabled. If it is not enabled, select the **Anti-Theft** check box.

4. Tap **Anti-Theft** to configure SIM Card Settings.

5. Tap **SIM Card Settings** and configure the following:

   ▪ Lock on SIM Change: Enable this option if you want your device to be locked as soon as SIM is changed. This helps you secure your device as it can be unlocked only by an authentic PIN.

   ▪ Notify on SIM Change: Enable this option if you want to get a notification on SIM change. This helps you know why the SIM has been changed and what action you need to take.

   ▪ Trusted SIMs: You can create a list of trusted SIM cards. If you use multiple SIM cards and you frequently change the cards you can enlist all your SIM cards. In this way, your device will not be locked when you change a SIM card.

   You may use multiple SIM cards because of network or business reasons. For example, if you travel to different states or geographical locations and you need to use local SIM card for communication, you may use multiple SIM cards.

   To add SIMs to the Trusted SIMs list, restart the phone with a new SIM and add the SIM to the Trusted SIMs list when prompted.

Lock on Airplane Mode

This feature locks your device as soon as Airplane or flight mode of the device is turned to on. This ensures security to your device if it is lost or stolen.

To configure Lock on Airplane Mode, follow these steps:

1. Open **Quick Heal Total Security**.

2. Tap **main menu** and then tap **Settings.**

3. Ensure if Anti-Theft is enabled. If it is not enabled, select the **Anti-Theft** check box.

4. Tap **Anti-Theft** to configure Lock on Airplane Settings:

5. Tap **Lock on Airplane Mode** to enable it.

Track & Control Device

With the **Track & Control Device** option, you can track and control your device even if it is lost or stolen. You can locate the device, lock it, and wipe data from the device for security. This can help you to get back your lost device.

To configure Track & Control Device, follow these steps:

1. Open **Quick Heal Total Security**.

2. Tap **main menu** and then tap **Settings.**

3. Tap **Anti-Theft** and then tap **Track & Control Device**.

   The following features appear: You can send command for various actions:

   ▪ Mobile Device Locator: Helps you trace the geographical location of your lost device. To get the device location, send this command:

TRACE antitheft_ PIN (For example – TRACE XXXX)

- Mobile GPS: Helps you configure mobile settings to enable GPS. This will help in tracking device location.

- Lock Device Remotely: Helps you lock your device remotely if it is lost or theft. It sends you the location of the device and images captured. To lock the device, send this command:

BLOCK antitheft_ PIN (For example – BLOCK XXXX)

In case your device is blocked by mistake or you get it back and want to unblock it, send this command:

UNBLOCK antitheft_ PIN (For example – UNBLOCK XXXX)

- Wipe Data Remotely: Helps you wipe the data from the lost device remotely. To wipe data, send this command:

WIPE antitheft_ PIN (For example – WIPE XXXX)

- Dial Call Remotely: Helps you dial a call from your lost device silently to another mobile. This helps you to listen to the possible conversation going on near your lost device. To dial a call, send this command:

CALL antitheft_ PIN (For example – CALL XXXX)

- Pickup Call Remotely: Helps you pick up a call on your lost or stolen device silently. This helps you listen to the possible conversation going on near your lost device. To pick up a call, send this command:

PICKUP antitheft_ PIN (For example – PICKUP XXXX)

- Record Audio Remotely: Helps you record audio of one minute on your device silently and send it to your Cloud account and email address. This helps in recording possible conversation going on near your lost device. To record audio, send this command:

AUDIO antitheft_ PIN (For example – AUDIO XXXX)

- Record Video Remotely: Helps you record video of one minute on your device silently and send it to your Cloud account and email address. This helps in recording video of possible conversation going on near your lost device. To record video, send this command:

VIDEO antitheft_ PIN (For example – VIDEO XXXX)

- Capture Image Remotely: Helps you capture images of the surrounding area near the lost device secretly and send them to your Cloud account and email address. To capture image, send this command:

PHOTO antitheft_ PIN (For example – PHOTO XXXX)

- Ring Device Remotely: You can locate your device by ringing it if you think it is in the nearby area. To ring the device, you need to send this command:

RING antitheft_PIN (For example – RING XXXX)

Lock Screen Details

When the device is locked, a message and the alternate contact numbers appear on the blocked device screen. A message is already present by default that you can edit as per your preference.

Ensure that you have active alternate contact numbers so that you can track all the activities carried out on your device successfully.

Update Alternate Contacts

You can add and update contact numbers to be displayed on the blocked device screen and get messages from your lost device. Ensure that you have saved the active alternate contact numbers.

Chapter

6

Help

With the **Help** option, you can read FAQs, check our contact numbers, and uninstall Quick Heal if required.

To view Help, follow these steps:

1. Open **Quick Heal Total Security**.

2. Tap the **main menu**.

   In the Help section, tap either of the following options:
   - Online Help
   - FAQ
   - Contact Us
   - Uninstall Quick Heal

Online Help

This includes the online help of Quick Heal Total Security. If you want to know about the features and to configure them, you can access it. Tap **Online Help**, you are redirected to our website where you can browse the Help file.

FAQs

Includes answers to the frequently asked questions (FAQ) related to Quick Heal Total Security. To see FAQs, you are redirected to our website.

Contact Us

Includes various support facilities.

Live Chat

To get online technical support or answers to your issues by speaking with our technical experts.

Web Support

If you have a query and want to submit a ticket, you can visit our Web Support system. Here you can submit a ticket with your issues. Our experts will revert to you with an appropriate answer.

Support Center

You can call us at the following numbers: 1800 121 7377 between 8:00 AM to 11:00 PM IST (India Standard Time) between Monday to Saturday.

9:30 AM to 06:30 PM IST on Sunday.

Uninstall Quick Heal

Removing Quick Heal Total Security leaves your device insecure to virus threats. However, in case you change your device or you need to format your device, you may need to uninstall Quick Heal.

To uninstall Quick Heal Total Security, follow these steps:

1. Open **Quick Heal Total Security**.

2. Tap the **main menu** and then tap **Uninstall Quick Heal**.

    A confirmation screen appears.

3. Tap **OK**.

4. Type your PIN for authentication and tap **Submit**.

    Your license is first deactivated and then you are further asked to confirm for uninstallation. In case you cancel uninstallation, your product will be deactivated but will not be removed from your device.

    If you access the Quick Heal app later, you need to activate it first.

Index

U