

# Quick Heal Total Security

## **User Guide**

*Version 2.3*

## Copyright & License Information

---

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

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

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

### 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](http://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
<b>Bold Font</b>	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
2.3	November 2017	Changes related to new feature such as, on-board screen or a Welcome screen is displayed after first-time activation and reactivation of the application.

## What's New in this Version?

---

Features	Description	Section
On-board screen	On-board screen or a Welcome screen is displayed after first-time activation and reactivation of the application.	On-board screen, page no. 4

# Contents

---

1. Getting started.....	1
Prerequisites .....	1
System requirements.....	1
Supported Android Versions.....	1
Supported Android Screen Resolutions.....	1
Downloading and installing Quick Heal Total Security .....	2
2. Registration, reactivation, and renewal .....	3
Registering Quick Heal Total Security .....	3
Registering licensed version .....	3
On-board Screen .....	4
About Quick Heal RDM .....	4
Creating an account with Quick Heal RDM.....	6
<i>Creating and activating RDM via App Settings</i> .....	6
<i>Signing up with Quick Heal RDM</i> .....	7
<i>Signing up with Quick Heal RDM with Google account</i> .....	8
<i>Adding a device to Quick Heal RDM</i> .....	8
Enabling Manage Through Web .....	9
Reactivating Quick Heal Total Security .....	9
Reactivating licensed version.....	9
<i>Renewal of Quick Heal Total Security</i> .....	10
Renewing licensed version.....	10
<i>Buying a renewal key</i> .....	11
<i>Renew Online</i> .....	11
<i>Call Us</i> .....	11
<i>Locate Dealer</i> .....	11
3. Quick Heal Total Security Dashboard .....	12
Message Center .....	12
Main menu .....	12
Dashboard alerts of Quick Heal Total Security .....	12
Menus .....	13
Scan .....	13
SafePe .....	13
Optimize.....	13

Data.....	13
Privacy.....	13
4. Quick Heal Total Security features .....	14
Security Shield.....	14
Menus on Dashboard.....	16
Scan .....	16
<i>Quick Scan</i> .....	16
<i>Full Scan</i> .....	16
<i>Schedule Scan</i> .....	17
<i>Security Advisor</i> .....	17
<i>Privacy Advisor</i> .....	19
<i>Privacy Audit Notification</i> .....	20
SafePe .....	20
<i>Managing apps</i> .....	21
Optimize.....	22
<i>Performance Summary</i> .....	22
<i>Kill Running Apps</i> .....	22
<i>Network Usage Summary</i> .....	23
Data.....	24
<i>Backup data to cloud</i> .....	24
<i>Restore backup from cloud</i> .....	26
<i>Delete backup from Cloud</i> .....	26
<i>Delete Personal Data</i> .....	26
Privacy.....	27
<i>Call Filter</i> .....	27
<i>Privacy Protection</i> .....	28
<i>Parental Control</i> .....	31
<i>Block Spam (DND)</i> .....	32
Main Menus .....	33
Home.....	33
Settings.....	33
About Product.....	33
Logs .....	34
<i>Activity</i> .....	34
<i>Threats Detected</i> .....	34
Help.....	36
5. Settings .....	37
General.....	37

Set PIN .....	37
Track Activity Log .....	38
Notification Icon.....	38
Quick Setting Notification .....	38
Manage Through Web .....	38
Create Web Account.....	39
News Notification .....	39
Application Statistics.....	39
Uninstallation Protection.....	40
Find Intruder .....	40
Scan .....	41
Privacy.....	42
Optimize.....	42
Power Saving.....	43
Speed Up Device .....	44
<i>Apps Safe List .....</i>	<i>44</i>
Enable Network Monitor .....	45
Mobile Network .....	45
Set Data Plan.....	45
Data.....	46
SafePe .....	46
Anti-Theft .....	47
<i>Access Anti-Theft through Fingerprint .....</i>	<i>48</i>
SIM Card Settings.....	48
Block on Airplane Mode.....	49
Track & Control Device .....	49
Block Screen Details.....	50
Update Alternate Contacts .....	51
<i>How to unblock your Anti-theft block screen? .....</i>	<i>51</i>
Safe Charging .....	52
Detect Unsecure Wi-Fi .....	52
6. Help .....	54
<i>Online Help .....</i>	<i>54</i>
<i>FAQs .....</i>	<i>54</i>
<i>Contact Us .....</i>	<i>54</i>
<i>Uninstall Quick Heal .....</i>	<i>55</i>



7. Index..... 56

## 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: 4.0, and later.

#### Supported Android Screen Resolutions

The following Android screen resolutions are supported:

- All resolutions ranging from 240 x 320 to 1080 x 1920.
- Tablets are also supported.

## Downloading and installing Quick Heal Total Security

To download and install Quick Heal Total Security, follow these steps:

1. Go to Google Play store.
2. Search for the **Quick Heal Total Security** app.
3. Download and install the Quick Heal Total Security app from Google Play store.  
The Quick Heal app is added to the Apps list on your device.
4. To open the app, go to the Apps list 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 the 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 how to register your license, see [Registering Quick Heal Total Security](#).

## 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.

This chapter includes the following sections:

[Registering Quick Heal Total Security](#)

[About Quick Heal RDM](#)

[Reactivating Quick Heal Total Security](#)

[Renewal of Quick Heal Total Security](#)

### 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 the Apps list 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**.



Note:

---

To activate the product on the devices with Android OS 6.0 and later versions, you must grant the required phone permissions. Tap **Grant Access** to proceed further.

---

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

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.

4. Tap **Next**. A successful message with expiry date is displayed.



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.
- 

## On-board Screen

The one-time, on-board screen or a Welcome screen is displayed after first-time activation and reactivation of the application.

Two scan options are displayed:

- **SCAN:** This scan option helps to update the virus database followed with scan. In this scenario, the scan continues irrespective of the success or failure of the virus database update.
- **Scan in the background:** In this option, the virus database update and the scan process will take place in the background.

On tapping either options and completion of the process, the user is directed to the dashboard.

## About 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
<b>Change PIN</b>	To set the PIN and change it remotely if required.
<b>Data Backup</b>	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.
<b>Locate</b>	<ul style="list-style-type: none"> <li>• Trace your device - To track the device location, when it is lost or stolen. The Trace your device option is helpful in getting back your device if it is lost or stolen.</li> <li>• Ring– To play the ringtone on the device so that you can trace it if it is located nearby.</li> </ul>
<b>Lock</b>	To lock 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 captured and displayed on RDM.
<b>Unlock</b>	To unlock the device remotely if you get your lost device back or if you have locked the device by mistake.
<b>Wipe</b>	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.
<b>Auto Dial/Receive</b>	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.
<b>Auto Capture Image</b>	To capture images of the surrounding area of the lost device secretly and the images are sent to registered email address.
<b>Auto Record Audio</b>	To record audio of one minute on your device silently and the audio is sent to your registered email address.
<b>Auto Record Video</b>	To record video of one minute on your device silently and the video is sent to your registered email address.
<b>Update virus database</b>	To remotely update the virus database of Quick Heal Total Security on your device.
<b>Scan Device</b>	To run a scan on the remote device if required.
<b>Background Scan</b>	To change the Background Scan settings on your device remotely.

Features	Description
<b>On Install App Scan</b>	To run scanning of newly installed application on the device remotely if required.
<b>Browsing and Phishing Protection</b>	To enable the Browsing & Phishing Protection option on the device remotely.
<b>Anti-Theft</b>	To enable the option remotely to secure the phone in case the phone is lost or stolen.
<b>Automatic Backup</b>	To change the Automatic Backup settings on your device remotely.
<b>Parental Control</b>	To configure the Parental Control settings on your device remotely.
<b>Privacy Protection</b>	To maintain a private contacts list and secure important call logs and messages from such contacts.
<b>Call Forwarding</b>	To set a number to which you want all your incoming calls are forwarded. You can also enable/disable the 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>
<b>Privacy Advisor</b>	To turn ON the Privacy Advisor settings remotely on the device.
<b>Security Advisor</b>	To turn ON the Security Advisor settings remotely on the device.

## 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. You can create and activate the RDM account via Quick Heal app Settings. To know about how to activate Quick Heal app, see [Registering licensed version](#).

## Creating and activating RDM via App Settings

To create and activate the RDM account via Settings, follow these steps:

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

2. Tap the **main menu**, and then tap **Settings**. If you have set the PIN, you will be asked to enter PIN.
3. Tap **General** and go to the **Manage Through Web** option. This option is enabled by default.
4. Tap **Create Web Account** to create the RDM account. You will be navigated to the RDM portal to create your account.



Note:

---

The Manage Through Web option must be turned ON to create or log on to your RDM account.

---

5. If you already have RDM account, you need to sign in to the RDM account. Else tap **Sign Up** on the top left of the RDM portal to create your account.

Fill the required details and create your RDM account.

After your RDM account is created, an email to activate the account is sent to the registered email id.

6. Open the registered email, and then click the **Activate** button or copy the given link in the browser address bar.

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

7. Set your password, and then click **Save**.

You have successfully created an account with the Quick Heal RDM portal. Now, you can manage the 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 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.

When you first log on to the Quick Heal RDM portal, 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 to 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, enter the product key.
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 then click **Submit**.

The device is successfully added.



---

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.

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

## Reactivating licensed version

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

1. Go to the Apps list 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 the Quick Heal 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 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**.



---

To reactivate the product on the devices with Android OS 6.0 and later versions, you must grant the required phone permissions. Tap **Grant Access** to proceed further.

---

The License Activation screen is displayed.

3. 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.

4. Tap **Next**.

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



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.



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.

---

## 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 on the top right of Dashboard. 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 are which remind you of the actions to be taken to avoid any mishap.

### 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

To run a scan of your device memory, memory card, and installed applications and schedule a new scan. Also, notifies you about unsecure settings. To know about Scan and options, see [Scan](#).

### SafePe

To make a safe financial transaction using the banking/ financial/ ecommerce/ eWallets apps. To check whether the device environment is free from any malware or unknown vulnerabilities before performing any financial transaction using any app. To know about SafePe, see [SafePe](#).

### Optimize

To check your device performance, increase its speed and check network usage. To know about Optimize and options, see [Optimize](#).

### 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 also buy more space on cloud if required. You can delete the data from the Cloud as well as personal data. To know about Data and options, see [Data](#).

### Privacy

To block calls 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 Privacy and options, see [Privacy](#).

## 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
<b>Background Scan</b>	Enable <b>Background Scan</b> to scan your device continuously. This helps you to scan all apps, and files in real time and will detect threats instantly.
<b>Anti-Theft</b>	Enable <b>Anti-Theft</b> to track and locate your device when it is lost or stolen. If this feature is disabled, the device cannot be tracked.
<b>Auto-Backup</b>	Enable <b>Auto-Backup</b> 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.
<b>Browsing &amp; Phishing Protection</b>	Enable <b>Browsing &amp; Phishing Protection</b> to block infected and fraudulent websites. This protects your device from all the infected websites when you connect to the Internet and keeps you safe from any kind of malware and websites that try to steal your valuable data such as bank details, user credentials, social security information, and passwords.
<b>Network Monitor</b>	Enable <b>Network Monitor</b> to monitor and control the Internet usage. This helps you manage your Internet bandwidth.
<b>Parental Control</b>	Enable <b>Parental Control</b> 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.
<b>Power Saving</b>	Enable <b>Power Saving</b> 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.
<b>Privacy Advisor</b>	Enable <b>Privacy Advisor</b> 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.
<b>Security Advisor</b>	Enable <b>Security Advisor</b> to get an alert if the security settings on your device are low. This helps you to enhance your device security.
<b>Uninstallation Protection</b>	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.



<b>On Install App Scan</b>	To run scanning of newly installed application on the device. The <b>On Install App Scan</b> option helps to run a scan, whenever a new application is installed on the device.
<b>Detect Unsecure Wi-Fi</b>	Enable <b>Detect Unsecure Wi-Fi</b> to run a scan on the device to detect if you are connected to an unsecure Wi-Fi.
<b>Find Intruder</b>	Enable <b>Find Intruder</b> to capture an image of an intruder on two wrong PIN attempts.
<b>Safe Charging</b>	Enable <b>Safe Charging</b> to show the current battery status and estimated approximate time to charge whenever the device is connected to the charger.
<b>SafePe</b>	Enable <b>SafePe</b> to make a safe financial transaction using the banking/ financial/ ecommerce/ eWallets apps.

## Menus on Dashboard

The menus on Dashboard include the following options:

### Scan

The **Scan** option lets you 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**.
3. Tap one of the following scan options:

[Quick Scan](#)

[Full Scan](#)

[Schedule Scan](#)

### Quick Scan

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

### Full Scan

To run a complete scan of your device and memory card. However, this scan may take some time to complete the action.



---

To run a full scan on the devices with OS 6.0 and later versions, you must grant permissions

---

## 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 schedule a scan on the devices with OS 6.0 and later versions, you must grant permissions.

---

To create a scan schedule, follow these steps:

1. Open **Quick Heal Total Security**.
2. On Dashboard, tap **Scan**.
3. Tap **Schedule Scan**.

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

4. To set a new scan schedule, tap **Schedule New Scan**.
5. Under **Set Time & Frequency** section, set time and frequency to start the scan automatically.

Time & Frequency include the options such as Scan while charging, Once a day, Once a week, and Once a month.



- 
- You can set only one type of frequency.
  - If Scan while charging is opted, 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

The **Security Advisor** option lets you 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**.
3. Tap **Security Advisor** to enable it. You can also enable this option from the Security Measures screen.





Note:

- The Security Advisor option is turned to OFF by default.
- To enable Anti-Theft and Antivirus on the devices with OS 6.0 and later versions, you must grant permissions.

4. On the **Security Advisor** screen, the security settings are displayed under following categories:
  - Risk Settings: The security settings, which are unsecure 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	Description
<b>Accounts &amp; Sync</b>	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.
<b>Bluetooth</b>	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.
<b>Device memory encryption</b>	<p>You can encrypt the data on your device. This ensures security by preventing unauthorized access to your data.</p> <p> Note:</p> <hr/> <p>The Device Memory Encryption setting is available only on supported OS.</p>
<b>Hotspot &amp; Tethering</b>	<p>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.</p> <p> Note:</p> <hr/> <p>The Hotspot and Tethering setting is available only on supported OS and vendors.</p>

<b>Anti-Theft</b>	Protects your device and its data. The <b>Quick Heal Anti-Theft</b> option lets you can trace, block, wipe data, dial a call, receive a call, capture image, record audio and video if your device is lost.
<b>Background Scan</b>	Shields your device against various types of threats. Keep this option enabled for security.
<b>Screen Lock</b>	If this option is disabled, your personal data may be at risk of misuse. Ensure that one of the screen lock options; Pattern, PIN, Password, or Finger Print is set to safeguard device data.
<b>Unknown App Sources</b>	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.
<b>USB Debugging</b>	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.
<b>Detect Unsecure Wi-Fi</b>	Communicating through an open or unsecured Wi-Fi network can put your data at risk. It is advisable to keep the setting ON.

### Privacy Advisor

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

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**.
3. Tap **Privacy Advisor** to enable it. You can also enable this option from the Security Measures screen. 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. If you find the app trustworthy, then you can trust the app by tapping the Trust button and then that app will be added to the Trusted Apps List.

Various permissions that an app may use are as follows:

Permissions	Description
<b>Access to Accounts</b>	Apps with this permission may request authentication credentials of the account. Such apps may add or remove accounts and delete your passwords
<b>Access to Contacts</b>	Apps with this permission can read, write, and share your personal contacts with their servers by compromising your data.
<b>Read Identity Info</b>	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.
<b>Tracking Locations</b>	Apps with this permission can update your device location to their servers, which may be harmful.
<b>Access to Messages</b>	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.
<b>Access to Network</b>	Apps with this permission allow network usage in the background.
<b>Other Permission</b>	Apps that have permissions other than those mentioned above are available under this category.

## Privacy Audit Notification

When you install or update any high-risk app on your device, a notification for Privacy Audit is displayed on the notification area. However, the Privacy Audit notification is displayed as soon as you install the apps. You can check the apps and the permissions they are using. If you find an app that violates your privacy or if you find your personal information is at risk, you can remove that app immediately.

## SafePe

The **SafePe** option lets you to make a safe financial transaction using the banking or financial or ecommerce or eWallets apps. This option helps you to check whether the device environment is free from any malware or unknown vulnerabilities before performing any financial transaction using any app. This option runs a scan of device root access, device integrity, device environment, file system, and network. You can add or remove your payment apps to this list.

To enable SafePe and view protected apps, follow these steps:

1. Open **Quick Heal Total Security**.
2. On Dashboard, tap **SafePe**. A confirmation pop-up is displayed.
3. Tap **Yes** to enable SafePe. The Protected Apps screen is displayed.



Note:

---

To enable SafePe on the devices with OS 6.0 and later versions, you must grant permissions.

---

## Managing apps

You can add or remove the apps to SafePe. You can also download the trusted apps on your device via genuine apps link.

To manage the apps added to SafePe, follow these steps:

1. Open **Quick Heal Total Security**.
2. On Dashboard, tap **SafePe**. The Protected Apps screen is displayed.
3. Tap **Manage Apps** icon on the bottom of the screen. The Manage Apps screen is displayed.

## Adding Apps

To add the apps to Safe list, follow these steps:

- i. Open **Quick Heal Total Security**.
- ii. On Dashboard, tap **SafePe**. The Protected Apps screen is displayed.
- iii. Tap the **Manage Apps** icon on the bottom of the screen. The Safe list, which includes the installed apps on your device, is displayed.
- iv. Select the check box of the required app and add to SafePe. In case you want to remove the app from SafePe, clear the check box next to the required app.

## Downloading apps through Genuine Apps link

The Genuine Apps link option allows you to download the genuine apps from the given link.

To download the genuine apps, follow these steps:

- i. Open **Quick Heal Total Security**.
- ii. Tap **SafePe**. The Protected Apps screen is displayed.
- iii. Tap the **Manage Apps** icon on the bottom of the screen.
- iv. Tap the **Genuine Apps Link** option and then tap the app link that you want to download. You will be redirected to the Google Play store.

## Optimize

The **Optimize** option checks your device performance and increases the security measures if required. It kills running apps to increase the device speed. Optimize includes the following:

[Performance Summary](#)

[Kill Running Apps](#)

[Network Usage Summary](#)

### 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, status of the device performance is displayed as Low, Medium, and High. If you find that the device is slow, this option 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 least used) or their name and add them to Safe List.

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

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

### Kill Running Apps

The **Kill Running Apps** option lets you 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 the 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**.
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 **Settings > Optimize > Apps Safe List**.

## Network Usage Summary

The **Network Usage Summary** option lets you 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**.
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 available. Tap this link to configure the data usage limit. After you set the data usage limit by using the link, it does not appear again.

## Set Data Usage Limit

The **Set Data Usage Limit** option lets you set the data usage limit.

To set the data usage limit, follow these steps:

- i. Open **Quick Heal Total Security**.
- ii. On Dashboard, tap **Optimize**.
- iii. Tap **Network Usage Summary**.
- iv. Tap the link **Set Data Usage Limit** for Mobile Network.

Configure the following options as required:

- **SIM type:** To select the SIM that you want to set the data plan in case of a dual SIM phone.



Note:

---

The SIM Type option is available only on the devices with OS 6.0 and later versions.

- **Billing Date:** Set the start date of your data plan.
- **Set data usage limit:** Set this option to activate the succeeding options.
- **Max data usage limit:** Set this option to fix the maximum limit to control data usage.
- **Notify if data usage reaches:** To get alerts if the data usage reaches the set limit.
- **Disconnect after max limit is reached:** To disconnect the data usage after the max data usage limit is reached.





Note:

---

The option is available only on the devices with OS 4.4 and earlier versions.

---

- Already used data from max limit: To set a value of the network data that you have already used.

## View App Data Usage

The **View App Data Usage** option lets you 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:

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

## Data

The **Data** option lets you 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 Data, follow these steps:

1. Open **Quick Heal Total Security**.
2. On Dashboard, tap **Data** and then select one of the following options:

[Backup data to Cloud](#)

[Restore Backup from Cloud](#)

[Delete Backup from Cloud](#)

[Delete Personal Data](#)

### Backup data to cloud

The **Backup data to cloud** option lets you 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.



Note:

---

To back up your data to cloud on the devices with OS 6.0 and later versions, you must grant permissions.

---

To back up the data, follow these steps:

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

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

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

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

4. 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 > Data > Backup data to cloud > Auto-Backup**.

Set time and frequency.

5. Tap **Save**.

### Custom Back up

You can take back up of pictures, music, and videos directly through third party applications. If there is no space to store the customized backed up data, you can avail of the Buy Space option.

To take back up through third party applications, follow these steps:

- i. Go to any third party application. For example: Gallery.
- ii. Select the media file that you want to backup to cloud, and then tap the **Share** option.
- iii. Select the **Quick Heal** icon to back up the media, and then backup is initiated.

### Buy more space on cloud

To purchase more storage capacity on Quick Heal Cloud. You can buy from the three storage options available: 2 GB, 5 GB, and 10 GB. You can buy as per your requirement. The purchased capacity will be added to the storage immediately after the completion of the purchase. This storage capacity is valid till the expiry of the product license.

To buy more space on Quick Heal Cloud, follow these steps:

- i. Open **Quick Heal Total Security**.
- ii. On Dashboard, tap **Data**.
- iii. Tap **Backup data to cloud**.

If there is no space to store the backed up data, the **Buy Space** option is displayed.

- iv. Tap **Buy Space** if you want to buy more space on cloud. The Buy more space on Cloud screen is displayed. The storage options available and the cost of space are displayed.
- v. Select the storage options as required, and then tap **Submit**. Enter your details and complete the transaction. You can buy storage capacity using various banking methods. Space will be added to the storage immediately.

## Restore backup from cloud

The **Restore backup from cloud** option lets you 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.



Note:

---

To restore your data from cloud on the devices with OS 6.0 and later versions, you must grant permissions.

---

To restore your data, follow these steps:

1. Open Quick Heal Total Security.
2. On Dashboard, tap **Data**.
3. Tap **Restore backup from cloud**.

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

4. Tap **Restore**.



Note:

---

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

---

## Delete backup from Cloud

The **Delete backup from Cloud** option lets you 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 **Data**.
3. Tap **Delete backup from cloud**.

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

4. Tap **Delete**.

## Delete Personal Data

The **Delete Personal Data** option lets you 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.



Note:

---

To delete your data on the devices with OS 6.0 and later versions, you must grant permissions.

---

To delete the data, follow these steps:

1. Open **Quick Heal Total Security**.
2. On Dashboard, tap **Data**.
3. Tap **Delete Personal Data**.

Select the data that you want to delete.

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



Note:

---

You cannot delete data from external SD cards on the devices with KitKat OS.

---

4. Tap **Delete**.

## Privacy

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

To configure Privacy, follow these steps:

1. Open **Quick Heal Total Security**.
2. On Dashboard, tap **Privacy**.
3. Select one of the following options:

[Call Filter](#)

[Privacy Protection](#)

[Parental Control](#)

[Block Spam \(DND\)](#)

## Call Filter

The **Call Filter** option lets you block calls 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 Filter, follow these steps:

1. Open **Quick Heal Total Security**.
2. On Dashboard, tap **Privacy**.
3. Tap **Call Filter**.

The Blocked List includes

- Blocked Numbers – Displays all blocked numbers.

## 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 the Block Call option that you want to block. Tap **Add to Blocked Numbers List**.
- Phone Logs: You can choose a contact from phone logs and select the Block Call option 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 the Block Call option that you want to block. Tap **Add to Blocked List**.
- Custom: You can block all calls from a series of certain numbers (Ex: 4000000000). You can also specify whether a contact should begin or end with such series.



---

This feature will not block numbers configured in anti-theft.

---

## 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.



---

SMS is not supported on the devices with OS 4.4 and later versions.

---

To configure Privacy Protection, follow these steps:

1. Open **Quick Heal Total Security**.
2. On Dashboard, tap **Privacy**.
3. Tap **Privacy Protection** to enable it. You can also enable this option from the Privacy option of Settings.
4. To make a contact private, tap **New Private Contact**.
5. Type a contact in any of the following ways:
  - Enter Number: You can type a number.
  - Phone Log: You can select numbers from phone log.
  - Add from Contact List: You can add numbers from the phone book.
6. When you add a number, the following options may appear. Select any one or a combination of the following:

- Contact
- Call Logs
- SMS



Note:

- 
- You can add up to 50 contacts to private contacts list.
  - To make a contact private on the devices with OS 6.0 and later versions, you must grant permissions.
- 

### Conditions related to making contacts private

The following are the conditions related to make 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 > Privacy > Privacy Protection > Notifications**).
- 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 **Privacy**.
3. Tap **Privacy Protection**.
4. Tap the **minus** icon next to a contact to restore it. You can also restore it from the Contact Details screen.

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.



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

The following privacy protection is offered after 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

The following are the important facts related to private 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

The following are the important facts related to private SMS:

- You can view private SMS from private contacts and copy, delete, or forward such SMS to any other contacts.
- Only last 1000 SMS are saved in the private SMS log section. Entries exceeding that limit will be deleted automatically without any notification.

### Impact of using Delete Personal Data on Privacy Protection

The following are the impacts of using the Delete Personal Data option Privacy Protection:

#### Contacts and messages

The following are the impacts of delete personal data on contacts and message:

- If you delete the contacts and messages 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 and messages of all private contacts will be deleted permanently and cannot be retrieved.

### Using Wipe on Privacy Protection

The following are the impacts of 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.
- Data that will be deleted includes contacts, SMS, Calendar events, and data of internal and external memory. However, the contact numbers will remain in the private contacts list.

### Parental Control

You can block infected and fraudulent websites with the help of the 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 **Privacy**.
3. Tap **Parental Control** to enable it and then tap **OK**.



Note:

---

To enable Parental control on the devices with OS 6.0 and later versions, you must grant permissions.

---

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 **Privacy**.
- iii. Tap **Parental Control**.
- iv. Tap **Block Access**.

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

- v. Under Block Websites, select the websites 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 **Privacy**.
- iii. Tap **Parental Control**.
- iv. Tap **Allow Access**.
- v. On the Parental Control screen, tap **Enter URL to allow access** section and type the website address and then tap the **plus(+)** sign.



Note:

- 
- The Parental Control feature provides multi browser support to block websites.
  - Parental Control may not work properly on default browser of Android 4.0 and later.
  - Parental Control does not support any beta versions of the browsers.
- 

### Block Spam (DND)

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 **Privacy** and then tap **Block Spam (DND)**.
3. Register the number in one of the following ways:
  - Fully Block: Lets you to block all commercial calls and SMSs.

- Fully Unblock: To unblock all telemarketing calls and SMS.
- 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.



- 
- 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](#)

[Logs](#)

[Help](#)

### Home

The **Home** option lets you 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 know more about Settings, see [Settings](#).

To access Settings, follow these steps:

1. Open **Quick Heal Total Security**.
2. Tap **main menu**, and then tap **Settings**.
3. Enter your PIN. The Settings screen appears.


### About Product

The **About Product** 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 by 60 days for free if you refer Quick Heal app to your friends. However, this button does not appear if you use it once. User Details: To update your details such as Username, Email ID and Mobile Number.  You can verify or update your mobile number only once.
Legal Information	Copyright of the product	To know the license information of the application.

## Logs

Logs include activity logs and information about the detected threats.

## Activity

The **Activity** option lets you 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. Threats detected is categorized into four types: Unresolved, Resolved, Quarantined, and Vulnerabilities. The following are the detected threat types:

[Resolved](#)

[Unresolved](#)

[Quarantined](#)

[Vulnerabilities](#)

## Resolved

Displays the list of resolved applications. After you resolve the threats from Unresolved type list, the threats are displayed in the Resolved type list. You can clear the list by tapping the **Clear** option.

To view the resolved threats, follow these steps:

- i. Open **Quick Heal Total Security**.  
Dashboard is displayed.
- ii. Tap **main menu**, and then tap **Threats Detected**. The Threats Detected screen is displayed.
- iii. Under the View drop-down list, tap **Resolved**. The list of resolved threats is displayed.

## Unresolved

Displays the list of unresolved harmful application threats detected during the scan. You can view the count of unresolved threats. You have to take an action to resolve the threats.

To view the unresolved threats, follow these steps:

- i. Open **Quick Heal Total Security**.  
Dashboard is displayed.
- ii. Tap **main menu**, and then tap **Threats Detected**. The Threats Detected screen is displayed.
- iii. Under the View drop-down list, tap **Unresolved**. The list of unresolved threats is displayed.
- iv. Tap **Uninstall** to remove the application from the device, and then tap **Ok**. Else, tap **Skip** to ignore it.

## Quarantined

Displays the list of repaired files. You can restore and delete the files. This option also helps to delete the quarantined files automatically after selected number of days.

To restore the files, follow these steps:

- i. Open **Quick Heal Total Security**.  
Dashboard is displayed.
- ii. Tap **main menu** and then tap **Threats Detected**. The Threats Detected screen is displayed.
- iii. Under the View drop-down list, tap **Quarantined**. The list of **Quarantined** files is displayed.
- iv. Select the check box next to the files, and then tap **Restore**. To delete the files, tap **Delete**.



Note:

---

It is mandatory to grant the storage permissions on the devices with 6.0 and later versions to restore the files.

---

## Vulnerabilities

Displays the list of vulnerable apps and files detected during the scan. The app or file that has the highest vulnerability percentage will be listed at the top. You can trust and uninstall the vulnerable apps. In case of vulnerable files, you can trust and delete. After you trust any particular app or file, it will be moved to the bottom of the list.

All the apps and files that detected during the scan are displayed as per the vulnerability severity. Depending on the issue severity, the application provides you with recommendations to take necessary action on it.

To perform actions on vulnerable apps and files, follow these steps:

- i. Open **Quick Heal Total Security**.  
Dashboard is displayed.
- ii. Tap **main menu** and then tap **Threats Detected**. The Threats Detected screen is displayed.
- iii. Under the View drop-down list, tap **Vulnerabilities**. The list of vulnerable threats is displayed.
- iv. Tap the **Trust** option to make the vulnerable app or file as trusted entity. If you want to uninstall any application, tap **Uninstall**. In case you want to remove files, tap **Delete** to remove the files from the device.



Note:

---

It is mandatory to grant the storage permissions on the devices with 6.0 and later versions to delete the files.

---

## Help

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

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

## Settings

---

The Settings menu include the following options:

[General](#)

[Scan](#)

[Privacy](#)

[Optimize](#)

[Data](#)

[SafePe](#)

[Anti-Theft](#)

[Safe Charging](#)

### General

The **General** option lets you configure features related to the application. This option includes the following:

#### Set PIN

The **Set PIN** option helps you to set the PIN. You must enter the correct PIN to access features of the application. After the PIN is set on your device, the name of option changes to Change PIN. The **Change PIN** option helps to change the PIN.

To set 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 **Set PIN**.
4. Enter New PIN, Re-Enter PIN, and then tap **Submit**.

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. Tap **Submit**.

## Track Activity Log

The **Track Activity Log** option lets you 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 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 enable the Manage Through Web option.

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 [About Quick Heal RDM](#) (Quick Heal RDM).

## Create Web Account

To create the account on the Quick Heal RDM portal. This option is enabled only if the Manage Through Web option is enabled.

To create web account, follow these steps:

1. Open **Quick Heal Total Security**.
2. Tap the **main menu** icon and then tap **Settings**.
3. Tap **General**.
4. Enable **Manage Through Web**, and then tap **Create Web Account**. You will be navigated to the Quick Heal RDM portal.

## 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. 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

The **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

The **Scan** option lets you 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 repair action is taken immediately. To activate this option, enable Background Scan.
  - **On Install App Scan:** To run scanning of newly installed application on the device. The On Install App Scan option helps to run a scan, whenever a new application is installed on the device.
  - **Scan App Before Download:** To run the scanning of the apps on Google play store before you download. It also informs you if the app is unsecure and risks behind installing the app.



Note:

---

To run a scan before downloading the app on the all versions of Android OS, you must grant permissions.

---

- **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.

---

- **Vulnerability Scan:** To run a vulnerability scan on the device. Enable this option to perform the vulnerability scan on the device, whenever a scan is performed on the device.
- **Scan SD card:** To run a scan of the Memory card of your device.
- **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.



Note:

---

To run a scan of your SD card on the device with OS 6.0 and later versions, you must grant permissions.

---

- **Trusted Apps List:** The apps, which are made to trust are listed here. This option is visible only when the Privacy Advisor option is turned ON.
- **Browsing & Phishing Protection:** To block infected, malicious, fraudulent, and phishing websites. Enable this option to block harmful websites.

## Privacy

The **Privacy** option lets you block international calls, get alert when you reject calls, enable Privacy Protection, Parental Control, and other features.

To configure Privacy, follow these steps:

1. Open **Quick Heal Total Security**.
2. Tap the **main menu** and then tap **Settings**.
3. Tap **Privacy** to configure the following settings:
  - **Call Block:** Enable this option to enable call filtering. This option is turned ON by default. You must enable this option to access other options of Call Filter.



Note:

---

To enable call block on the devices with OS 6.0 and later versions, you must grant permissions.

---

- **Notifications:** Enable this option to get notification for blocked calls under Message Centre.
- **Alert on Call Rejection:** 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.
- **International Calls:** Enable this option 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 [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](#).

## Optimize

The **Optimize** option lets you check your device performance, increase the device speed, and set data plan.

To configure the Optimize option, follow these steps:

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

2. Tap the **main menu** and then tap **Settings**.
3. Tap **Optimize**. The Optimize screen is displayed.

Optimize includes the following options:

[Power Saving](#)

[Speed Up Device](#)

[App Safe List](#)

[Enable Network Monitor](#)

[Mobile Network](#)

## Power Saving

The **Power Saving** option helps to kill power-consuming apps and 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. Tap **Optimize**.
4. By default, Power Saving is disabled. Select the **Power Saving** check box to enable it.
5. After enabling Power Saving, the Power Saving dialog box is displayed to configure the settings. Else, you can keep the default settings by tapping the **Keep Default** button. In case you want to change the settings later, tap **Power Saving**.



Note:

---

To enable Power Saving on the devices with OS 6.0 and later versions, you must grant permissions.

---

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.
  - **Set Screen Timeout:** Set the screen timeout after the 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.
- **Disable Sync:** Select this option to disable sync automatically when power saving mode starts.

## Speed Up Device

The **Speed Up Device** option lets you 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 is enabled. If it is not enabled, select the **Optimize** check box.
4. Tap **Optimize** 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.

## Apps Safe List

The Apps Safe List option 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**.
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.

## Enable Network Monitor

The **Enable Network Monitor** option lets you enable Network Monitor and set Mobile 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. Tap **Optimize**.
4. Select **Enable Network Monitor** check box to configure Mobile Network.



Note:

---

To enable network monitor on the devices with OS 6.0 and later versions, you must grant permissions.

---

## Mobile Network

The **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. Tap **Optimize**.
4. Tap **Mobile Network**. The Mobile Network Monitor screen is displayed.



Note:

---

If Mobile Network option is not enabled, then select the **Enable Network Monitor** check box.

---

5. 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](#).

## Set Data Plan

To set the data plan for your device.

To set the data plan, follow these steps:

1. Open **Quick Heal Total Security**.
2. Tap the **main menu** icon and then tap **Settings**.

### 3. Tap **Optimize**.

### 4. Tap **Mobile Network**. The Mobile Network Monitor screen is displayed.

The Mobile Network Monitor screen includes Sim Type, Billing date, Set data usage limit, Max data usage limit, Notify if data usage reached, and Already used data.

- SIM Type: To select the SIM that you want to set the data plan.



Note:

---

The SIM Type option is available only on the devices with OS 6.0 and later versions.

- Billing date: To set the start date of the data plan.
- Set data usage limit: To set the limit of the data usage on your device. Enable the Set data usage limit option to configure the data plan.
- Max data usage limit: To set the maximum limit of the data usage.
- Notify if data usage reached: To receive the notification on reaching the maximum data usage limit.
- Already used data: To view the already used data while setting the data plan.

## Data

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

To use Data, follow these steps:

1. Open **Quick Heal Total Security**.
2. Tap the **main menu**, and then tap **Settings**.
3. Select the **Data** check box to enable it.
4. Tap **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**.

## SafePe

The **SafePe** option helps to make a safe financial transaction using the banking/ financial/ ecommerce/ eWallets apps. To check whether the device environment is free from any malware

or unknown vulnerabilities before performing any financial transaction using any app. You can also enable the option. To know more about SafePe, see [SafePe](#).

You can configure the following settings:

- **System Scan:** Enable this option to validate the file system & system apps on your device. It also checks for malicious system apps, jar, apk & files.



Note:

---

The System Scan option is turned ON by default. You cannot change the settings.

---

- **Device Scan:** Enable this option to validate the root status, changes in OS other than manufacturer changes, & safe device environment of device.
- **Network Scan:** Enable this option to validate the connected network and know whether the Wi-Fi connected is secure to do the financial transactions.

## Anti-Theft

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



Note:

---

The Anti-Theft option is turned OFF by default.

---

To enable the Anti-Theft option, follow these steps:

1. Open **Quick Heal Total Security**.
2. Tap the **main menu**, and then tap **Settings**.  
You can also enable the Anti-Theft through Security Measures.
3. Tap the **Anti-Theft** option to enable it. The Set PIN screen is displayed.
4. Enter New PIN, Re-enter New PIN, and then tap **Save**. If you have already set the PIN through the other options, the Add From Contacts screen is displayed.
5. Tap **Add from Contacts** to add the alternate contacts. You can set up to two alternate contacts. Select the contact from the device contacts or phonebook, and then tap **Add**.



Note:

---

After adding the alternate contacts on the devices with OS 6.0 and later versions, you must grant all the permissions to enable the Anti-Theft option.

---

6. Tap **Next**, and then tap **Done**. The Anti-Theft option is enabled.



## Access Anti-Theft through Fingerprint

If your device has Fingerprint sensor, you can use your fingerprint to access the Anti-theft feature. To access this feature through Fingerprint, at least one fingerprint must be configured. After five unsuccessful fingerprint scans, the Quick Heal application asks you to enter the PIN that you have configured.

You can also use the Fingerprint access to unblock the Antitheft Block screen.



Note:

- 
- The Fingerprint option is supported only on the devices with Fingerprint sensor.
  - In case of the Anti-Theft block screen, intruder images are captured after two unsuccessful Fingerprint attempts.
- 

You can configure the following settings for Anti-theft:

[SIM Card Settings](#)

[Block on Airplane Mode](#)

[Track & Control Device](#)

[Block Screen Details](#)

[Update Alternate Contacts](#)

## SIM Card Settings

The **SIM Card Settings** option lets you 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:
  - **Block on SIM Change:** Enable this option if you want your device to be blocked as soon as SIM is changed. This helps you secure your device as it can be unblocked 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 blocked 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.

## Block on Airplane Mode

The **Block on Airplane Mode** option 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 Block on Airplane Mode, follow these steps:

1. Open **Quick Heal Total Security**.
2. Tap **main menu** and then tap **Settings**.
3. Tap **Anti-Theft** to configure Block on Airplane Settings:
4. Tap **Block on Airplane Mode** to enable it.

## Track & Control Device

The **Track & Control Device** option lets you track and control your device even if it is lost or stolen. You can locate the device, block 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.
- **Block 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 block the device, send this command:  
BLOCK antitheft\_ PIN (For example – BLOCK XXXX)
- **Unblock Device Remotely:** 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)



Note:

---

Pickup call remotely is not supported on devices with OS 5.0 and later versions.

- **Record Audio Remotely:** Helps you record audio of one minute on your device silently and send it to your registered 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 registered 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 registered 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)

## Block Screen Details

When the device is blocked, 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.

### How to unblock your Anti-theft block screen?

The **Anti-Theft** option helps you to secure the phone in case the phone is lost or stolen. In this framework, the device may get blocked due to the various security reasons. Whenever the device gets blocked, you can unblock your screen with the PIN that that you have added while configuring Anti-Theft. In case you forgot the PIN, Quick Heal provides three options to unblock your phone; Get Temporary PIN, Gmail Authentication, and Remote Device Management.

- **Get Temporary PIN:** This option helps you to send a temporary PIN to the recovery contacts to reset your PIN.

To get a temporary PIN, follow these steps:

- Tap the **Unblock phone** option on the block screen. The Enter PIN screen is displayed.
- Tap **Forgot PIN?** In case you forgot the PIN. The Forgot PIN screen is displayed.
- Tap **Get Temporary PIN.** The Get Temporary PIN screen is displayed.
- Tap **Send.** A temporary PIN is sent to the recovery contact numbers that you have added while configuring Anti-Theft.



Note:

---

Please be notified that carrier charges may apply to send a message.

---

- **Google Authentication:** This option helps you to unblock your screen by validating your Gmail account.

To validate your Gmail account, follow these steps:

- Tap the **Unblock phone** option on the block screen. The Enter PIN screen is displayed.
- Tap **Forgot PIN?** In case you forgot the PIN. The Forgot PIN screen is displayed. The three options to unblock your phone are displayed.
- Tap **Google Authentication.** The Google Authentication screen is displayed. In case of no Internet connectivity, the Configure Internet screen is displayed.

To configure the internet, follow these steps:

- On the Configure Internet screen, enable Mobile to turn ON mobile data, else, enable Wi-Fi to turn ON Wi-Fi.
- If you want to configure the Wi-Fi settings, tap the **Wi-Fi** option. The Configure Wi-Fi screen is displayed.

- iii. Enter **Network SSID**, select **Security** and then tap **Connect**. The Security options include Open, WEP, and WPA\_WPA2\_PSK. If you select WEP, and WPA\_WPA2\_PSK security options, then you must enter the password to connect to the Wi-Fi.
- iv. After the internet is connected, check your email address, enter the password of your Gmail account, and then tap **Login**.
  - Remote Device Management: This option informs that you can reset your PIN through the RDM portal.  
To reset your PIN through the RDM portal, follow these steps:
    - i. Tap the **Unblock phone** option on the block screen. The Enter PIN screen is displayed.
    - ii. Tap **Forgot PIN?** in case you forgot the PIN. The Forgot PIN screen is displayed. The three options to unblock your phone are displayed.
    - iii. Tap **Remote Device Management**. The Remote Device Management screen is displayed. Log on to the RDM portal using the URL provided on the screen.



Note:

---

In case of no Internet connectivity, you must the configure internet to access the RDM portal. To know how to configure your internet, see [Configuring Internet](#).

---

## Safe Charging

The **Safe Charging** option displays the current battery status and estimated approximate time to charge. After the Safe Charging option is enabled, the charging screen appears whenever the device is connected to the charger and when the device is locked.

To enable Safe Charging, follow these steps:

1. Open **Quick Heal Total Security**.
2. Tap **main menu** and then tap **Settings**.
3. Select the **Safe Charging** check box to display the charging screen.



Note:

---

To enable Safe Charging on the devices with OS 6.0 and later versions, you must grant permissions.

---

## Detect Unsecure Wi-Fi

The **Detect Unsecure Wi-Fi** option runs a scan of the Wi-Fi. After the Detect Unsecure Wi-Fi is enabled, this option notifies you if you are connected to an unsecure Wi-Fi.

To enable Detect unsecure Wi-Fi, follow these steps:

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

2. Tap **main menu**, and then tap **Settings**.
3. Select the **Detect Unsecure Wi-Fi** check box to inform you about the unsecure Wi-Fi.

## Help

---

The **Help** option lets you 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](#)

[FAQs](#)

[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.

## Enable Debug Logs

Helps to share the logs with the support team in case you face any issue with the application. This option is disabled default. To make it visible, tap the **Quick Heal** icon on the Contact Us screen 4-5 times. This option is disabled by default. To enable this option, select the check box next to it



Note:

---

To enable this option on the devices with OS 6.0 and later versions, you must grant permissions.

---

## Uninstall Quick Heal

Removing Quick Heal Total Security leaves your device unsecure 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**. If PIN is not set, the app will directly start the license deactivation process.

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

---

## A

About Product, 33  
    product key, license expiry date, 33  
Access Anti-Theft through Fingerprint, 48  
Anti-Theft, 47  
Application Statistics, 39

## B

Backup data to cloud, 24  
Block on Airplane Mode, 49  
Block Screen Details, 50  
Block Spam (DND), 32

## C

Call & Message Filter  
    block calls, block SMS, 27  
Call Filter, 27  
Contact Us  
    live chat, web support, support contacts, 54  
Create Web Account, 39  
Creating an account with Quick Heal RDM, 6  
Custom Back up, 25

## D

Dashboard, 12  
Delete backup from Cloud, 26  
Delete Personal Data, 26  
Detect Unsecure Wi-Fi, 52  
Downloading and installing Quick Heal Total Security, 2

## E

Enable Debug Logs, 55

## F

FAQs, 54  
Find Intruder, 40

## G

General, 37  
Getting started, 1

## H

Help, 54  
    FAQ, contact us, uninstall Quick Heal, 54  
How to unblock your Anti-theft block screen?, 51

## K

Kill Running Apps, 22

## L

Live Chat, 54  
Logs, 34

## M

Main Menus, 33  
Manage Through Web, 38  
    manage device through Quick Heal RDM, 9  
Menus, 13  
Menus on Dashboard, 16

## N

Network Monitor  
    manage mobile network, Wi-Fi, 45  
Network Usage  
    set data usage, 23  
News Notification, 39  
Notification Icon, 38

## O

Online Help, 54  
Optimize Device, 42  
    increase device speed, 22  
    save power, speed up device, manage network connections, 42

## P

Parental Control, 31  
    allow websites, block websites, 31  
Prerequisites, 1  
Privacy Advisor, 19  
Privacy Audit Notification, 20

Privacy Protection, 28  
 private contacts, nonprivate contacts, 28

## Q

Quarantined, 35  
 Quick Heal RDM  
 features, 3, 4  
 Quick Heal Remote Device Management  
 Quick Heal RDM, Cloud portal, 38  
 Quick Heal Total Security Features, 14  
 Quick Setting Notification, 38

## R

Reactivating Quick Heal Total Security, 3, 9  
 Register Product  
 through Internet and SMS, 3  
 Registering  
 licensed version, free trial, 3  
 Registration, reactivation, and renewal, 3  
 Renewal Key  
 renew online, locate dealer, call us, 11  
 Renewal of Quick Heal Total Security, 3, 10  
 Resolved, 35  
 Restore backup from cloud, 26

## S

SafePe, 20  
 Scan App Before Download, 41  
 Scan Device, 41  
 quick scan, custom scan, schedule scan, 16  
 Secure Data, 24, 46  
 back up data, restore data, delete data securely, 24  
 Security Advisor, 17

Security Shield, 14  
 Set Data Usage Limit, 23  
 Set PIN, 37  
 Set Privacy, 27, 42  
 block calls, block SMS, 27  
 setting Parental Control, browsing, phishing, 42  
 Settings, 33, 37  
 SIM Card Settings, 48  
 Speed Up Device, 22  
 Supported Android  
 versions, screen resolutions, 1  
 System requirements, 1

## T

Track & Control Device, 49  
 locate device, send commands to device, 49  
 Trusted SIM  
 multiple SIM cards, local SIM, 48

## U

Uninstall Quick Heal  
 uninstalling, deactivating, 55  
 Uninstallation Protection, 40  
 Activate device administrator, 40  
 Unresolved, 35  
 Update Alternate Contacts, 51

## V

View App Data Usage, 24

## W

Web Support, 55