

Quick Heal Mobile Security

User Guide

Version 2.5

Copyright & License Information

Copyright © 2018 Quick Heal Technologies Ltd. All Rights Reserved.

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

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




License Terms

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

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

About This Document

This user guide covers all the information required to install and use Quick Heal Mobile Security. The following table lists the conventions that we followed to prepare this guide:

| Convention | Meaning |
|---|---|
| Bold Font | Anything highlighted in bold indicates that it is a menu title, window title, check box, drop-down menu, dialog, button names, hyperlinks, and so on. |
|  | This is a symbol used for a note. Note supplements important points or highlights information related to the topic being discussed. |
|  | This is a symbol used for a tip. Tip helps users to apply the techniques and procedures to achieve a task in an easy way. |
|  | This is a symbol used for warning or caution. This is an advice either to avoid loss of data or damage to hardware. |
| <Step 1> <Step 2> | The instruction mentioned in the numbered list indicates actions that you need to perform. |

What's New in this Version?

| Features & Enhancements |
|---|
| <ul style="list-style-type: none">• Multiple enhancement to the features.• Implemented features such as AppLock, Individual Feature Purchase, Silent scan app before download etc. |

Contents

| | |
|---|----|
| 1. Getting started..... | 1 |
| Prerequisites | 1 |
| System requirements..... | 1 |
| Supported Android Versions..... | 1 |
| Supported Android Screen Resolutions..... | 1 |
| Downloading and Installing Quick Heal Mobile Security..... | 2 |
| 2. Registration and Reactivation | 3 |
| Registering Quick Heal Mobile Security..... | 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 Mobile Security..... | 9 |
| Reactivating Quick Heal Mobile Security..... | 9 |
| 3. Quick Heal Mobile Security Dashboard..... | 11 |
| Reward points | 11 |
| Message Center | 11 |
| Main menu | 11 |
| Dashboard alerts of Quick Heal Mobile Security..... | 12 |
| Security Shield..... | 12 |
| Menus | 12 |
| 4. Quick Heal Mobile Security Features | 14 |
| Security Shield..... | 14 |
| Increasing security level..... | 14 |
| Security Measures..... | 15 |
| Menus on Dashboard..... | 16 |
| Scan | 16 |
| Network Monitor | 17 |

| | |
|---|-----------|
| Set Data Usage Limit | 17 |
| View App Data Usage..... | 18 |
| Boost | 18 |
| AppLock..... | 18 |
| Quick Scan | 19 |
| Viewing detected threats..... | 19 |
| Parental Control..... | 19 |
| Configuring Parental Control | 19 |
| Blocking Access | 19 |
| Allowing Access..... | 20 |
| Web Security | 20 |
| Configuring Web Security | 20 |
| SafePe | 21 |
| Configuring SafePe..... | 21 |
| Managing apps..... | 21 |
| <i>Adding apps to SafePe via installed apps.....</i> | <i>21</i> |
| <i>Adding apps to SafePe via genuine apps link.....</i> | <i>22</i> |
| Battery Saver | 22 |
| Configuring Battery Saver | 22 |
| <i>Activating Battery Saver mode</i> | <i>23</i> |
| <i>Setting screen brightness</i> | <i>23</i> |
| <i>Setting Screen timeout</i> | <i>23</i> |
| Anti-Theft | 23 |
| Configuring Anti-Theft | 24 |
| <i>Access Anti-Theft through Fingerprint</i> | <i>24</i> |
| SIM Card Settings | 25 |
| Block on Airplane Mode..... | 25 |
| Track & Control | 26 |
| Customize Block Screen | 27 |
| <i>Customizing block screen</i> | <i>27</i> |
| Update Alternate Contacts | 28 |
| <i>Updating alternate contact numbers.....</i> | <i>28</i> |
| How to unblock your Anti-theft block screen?..... | 28 |
| <i>Unblock device with Temporary PIN</i> | <i>28</i> |
| <i>Unblock device with Google Authentication</i> | <i>29</i> |
| <i>Unblock device with Remote Device Management</i> | <i>29</i> |
| Block Calls | 30 |

| | |
|---|----|
| Configuring Block Calls..... | 30 |
| <i>Blocking unwanted calls</i> | 30 |
| <i>Block Spam (DND)</i> | 31 |
| Privacy Protection | 31 |
| Configuring Privacy Protection | 32 |
| Making Contacts Private | 32 |
| Privacy Advisor | 35 |
| Configuring Privacy Advisor | 35 |
| Viewing app permission..... | 35 |
| <i>Privacy Audit Notification</i> | 36 |
| Security Advisor | 36 |
| Configuring Security Advisor..... | 36 |
| Network Monitor | 38 |
| Configuring Network Monitor | 38 |
| Set Data Plan | 38 |
| Data Protection | 39 |
| Backup Data to Cloud..... | 39 |
| Custom Back up | 40 |
| Buy more space on cloud..... | 40 |
| Restore Backup from Cloud | 40 |
| Delete Backup from Cloud | 41 |
| Delete Personal Data | 41 |
| Reward points | 42 |
| How to redeem your reward points? | 42 |
| How to earn points?..... | 42 |
| <i>Earn points via Share</i> | 42 |
| <i>Earn points via Quick Action</i> | 43 |
| Main menus | 44 |
| Home | 44 |
| Settings..... | 44 |
| About Product | 44 |
| <i>Individual Feature Purchase</i> | 45 |
| Buy Premium or Extend Premium | 45 |
| Logs | 46 |
| <i>Activity Log</i> | 46 |
| <i>Threats Detected</i> | 46 |
| Help | 48 |

| | |
|---|----|
| 5. Settings | 49 |
| General..... | 49 |
| Change PIN | 49 |
| Track Activity Log | 50 |
| Status Notification | 50 |
| Quick Settings Notification | 50 |
| Manage Through Web | 50 |
| Create Web Account | 51 |
| News Notification | 51 |
| Application Statistics..... | 51 |
| Block Uninstallation | 52 |
| Capture Intruder | 52 |
| Scan | 52 |
| Background Scan..... | 53 |
| On Install App Scan | 53 |
| Scan App Before Download | 53 |
| Silent Scan app before download | 53 |
| Scan from Cloud..... | 53 |
| Vulnerability Scan | 53 |
| Scan SD Card | 53 |
| Schedule Scan | 54 |
| Delete Quarantined Files After | 54 |
| Device Privacy | 54 |
| Call Filter | 55 |
| Privacy Protection | 55 |
| Optimize..... | 55 |
| Device Performance..... | 55 |
| <i>Battery Saver</i> | 55 |
| <i>Boost</i> | 55 |
| Network Monitor | 56 |
| <i>Network Monitor</i> | 56 |
| <i>Data Plan</i> | 56 |
| AppLock..... | 56 |
| Show prompt to lock newly installed apps..... | 56 |
| Scramble Keyboard | 57 |
| Access AppLock through Fingerprint | 57 |
| Configuring Show Prompt and Scramble Keyboard | 57 |

| | |
|-----------------------------------|----|
| SafePe | 57 |
| Anti-Theft | 58 |
| Backup | 58 |
| Safe Charging | 59 |
| Detect Unsecure Wi-Fi | 59 |
| Detecting unsecure Wi-Fi | 59 |
| Show Ads | 59 |
| Configuring Show Ads option | 59 |
| 6. Help | 60 |
| Online Help | 60 |
| FAQs | 60 |
| Contact Us | 60 |
| Live Chat | 61 |
| Web Support | 61 |
| Support Center | 61 |
| Enable Debug Logs | 61 |
| Share App | 61 |
| Uninstall Quick Heal | 61 |
| 7. Index | 63 |

Getting started

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

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

[Prerequisites](#)

[System requirements](#)

Prerequisites

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

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

System requirements

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

Supported Android Versions

Quick Heal Mobile Security is compatible with the following versions: Android 4.0 to 7.0.

*Limited support for Android 8.0 and later versions.

Supported Android Screen Resolutions

The following Android screen resolutions are supported:

- All resolutions ranging from 240 x 320 to 1080 x 1920.

Downloading and Installing Quick Heal Mobile Security

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

1. Go to Google Play store.
2. Search for the **Quick Heal Mobile Security** app.
3. Download and install the Quick Heal Mobile Security app from Google Play store.
Quick Heal Mobile Security is added to the Apps list on your device.
4. To open the application on your device, go to the apps list and tap the **Quick Heal Mobile 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 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 to the user.

- If you do not want to receive the SMS alerts, clear this option.

5. Tap **I Agree**.

You are redirected to the Activation screen to register your product.

To know how to register your license, see [Registering Quick Heal Mobile Security](#).

Registration and Reactivation

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

You can use and reactivate Quick Heal Mobile Security on same Android supported mobile device.

This chapter includes the following sections:

[Registering Quick Heal Mobile Security](#)

[About Quick Heal RDM](#)

[Reactivating Quick Heal Mobile Security](#)

Registering Quick Heal Mobile Security

Quick Heal Mobile Security is simple and free to register. You can reactivate Quick Heal Mobile Security on the same device.

To register Quick Heal Mobile Security, follow these steps:

1. Go to the Apps list on your device, and then tap the **Quick Heal Mobile 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 receive the SMS alerts, clear this option.

2. Tap **I Agree**. The copy is activated.

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.



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.

- Tap **Grant Access** to proceed further.



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 option and completion of the process, the user is directed to the dashboard.

About Quick Heal RDM

The Quick Heal Remote Device Management (RDM) portal helps you to control and manage your devices remotely. Quick Heal RDM allows you to access various features of Quick Heal Mobile 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 |
|-------------|---|
| Change PIN | Set the PIN and change it remotely if required. |
| Data Backup | Backup your personal data to the Quick Heal Cloud. In case you need your data, you can restore it from the Cloud to your device. **Go premium to back up your data to the Cloud. |
| Locate | Trace your device – This option is helpful to track the device and get it back if it is lost or stolen. |

| Features | Description |
|-----------------------|--|
| | Ring – This option plays the ringtone on the device so that you can trace it if it is located nearby. |
| Lock | 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 also captured and displayed on RDM. **Go premium to capture the image of the surrounding area when the device is lost and locked through RDM. |
| Unlock | Helps to unlock the device remotely if you get your lost device back or if you have blocked the device by mistake. |
| Wipe | Helps to wipe your device data when it is lost or stolen. The data from both the internal and external memories will be wiped in this case. |
| Auto Dial/Receive | Helps to dial a call from your lost device silently to another device. Also, you can pick-up a call on your lost or stolen device silently. **Go premium to dial or receive a call remotely from the lost device. |
| Auto Capture Image | Helps to capture images of the surrounding area of the lost device secretly and the images are sent to registered email address. **Go premium to capture the images remotely of the surrounding area of the lost device secretly. |
| Auto Record Audio | Helps to record audio of one minute on your device silently and the audio is sent to your registered email address. **Go premium to record audio of one minute on the device silently. |
| Auto Record Video | Helps to record video of one minute on your device silently and the video is sent to your registered email address. **Go premium to record video of one minute on the device silently. |
| Update virus database | Helps to remotely update the virus definitions database of Quick Heal Mobile Security on your device. |
| Scan | Runs a scan on the remote device if required. |
| Background Scan | Helps to change the Background Scan settings on your device remotely if required. |
| On Install App Scan | Helps to run a scan of newly installed application on the device remotely if required. |
| Anti-Theft | Helps to enable the Anti-Theft option remotely to secure the device in case the device is lost or stolen. |
| Automatic Backup | Helps to change the Automatic Backup settings on your device remotely. **Go premium to configure the Automatic Backup settings on the device. |
| Parental Control | To configure the Parental Control settings on your device remotely. |

| Features | Description |
|--------------------|---|
| | **Go premium to configure the Parental Control settings on the device. |
| Privacy Protection | Helps to enable Privacy Protection options. **Go premium to avail Privacy Protection. |
| Call Forwarding | You can set a number to forward all your incoming calls. You can also enable/disable Call Forwarding option through remote SMS commands. The command should be in the following format: START_FORWARD <PIN> <number to which calls are to be forwarded> However, you can stop call forward whenever you want. To stop call forward, send the following command: STOP_FORWARD <PIN> |
| Privacy Advisor | Helps to turn ON the Privacy Advisor settings remotely on the device. |
| Security Advisor | Helps 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 how to activate Quick Heal app, see [Registering Quick Heal Mobile Security](#).

Creating and activating RDM via App Settings

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

1. Open **Quick Heal Mobile Security**.
2. Tap the **main menu** > **Settings**. If you have set the PIN, you will be asked to enter the PIN.
3. Tap **General**.
4. The Manage Through Web option is enabled by default. 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 or 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.

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

3. Enter the correct verification code.

Read the license agreement and privacy policy documents carefully.

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

5. Click **Sign up**.

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

6. 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.

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

Your account with the Quick Heal RDM portal is created successfully. Now you can manage your devices 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, you need to configure the Add Device page. To know how to add a device, see [Adding a device to Quick Heal RDM](#).

Adding a device to Quick Heal RDM

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

To add a device, follow these steps:

1. Visit Quick Heal RDM Portal at <https://mydevice.quickheal.com>.
2. Log on to the Quick Heal RDM portal.
The Add Device page appears.
3. In the **Name** text box, write a name to the device.
4. In the **Product Key** text box, 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 click **Submit**.

The device is successfully added.



Note:

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

Enabling Manage Through Web

To manage Quick Heal Mobile Security on your device through Quick Heal RDM, it is important that you always enable **Manage Through Web** option. 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 Mobile 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 Mobile Security

You need to reactivate your product if you have removed it from your device in case you format your device.

Reactivating Quick Heal Mobile Security

To reactivate Quick Heal Mobile Security, follow these steps:

1. Go to the Apps list on your device and then tap the **Quick Heal Mobile Security** icon. The license agreement screen appears.

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

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

2. Tap **I Agree**. The copy is reactivated.

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.



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.



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.
-

Chapter

3

Quick Heal Mobile Security Dashboard

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

[Reward points](#)

[Message Center](#)

[Main Menu](#)

[Dashboard alerts](#)

[Security Shield](#)

[Menus](#)

Reward points

The Reward points icon on the top right of Dashboard helps you view and redeem points. You can redeem these points to get access to the Pro features for a limited period. You can also earn points via two options such as Share and Quick action. To know more about reward points, see [Reward Points](#).

Message Center

Message Center includes notifications, news bytes, and information about offers. If you have enabled notification for a feature, the notification will be displayed here. In addition, you can also view latest news related to digital security.

Main menu

Main menu or global menu is available on the top right of Dashboard. With this menu, you can configure various features for securing your device and data. This section also gives information about the product, how to buy premium features, view activity and threats logs. Also, get to know more about Quick Heal Mobile Security with the informative section of HELP: Online Help, FAQs, Contact Us, and Share App.

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

Dashboard alerts of Quick Heal Mobile Security

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

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.

- Tap Security Shield, you are directed to Security Measures setting screen.

To know about various Security Measures, see [Security Shield](#).

Menus

On Dashboard, you can see the following menus:

| Menus | Description |
|--------------------|---|
| Scan | This scan runs a full scan of your device and scans all apps, files, and data in real time and will detect threats instantly. |
| Boost | Helps to check your device performance, increase its speed, and check network usage. |
| AppLock | Locks your device apps for privacy. |
| Quick Scan | Runs a scan of all the apps installed on your device. |
| Parental Control | Helps to restrict inappropriate content for kids when they are online. |
| Web Security | Provides protection from malicious and fraudulent websites. |
| SafePe | Helps for safe financial transaction using the banking/ financial/ ecommerce/ eWallet apps. |
| Battery Saver | Saves power and increase battery life. |
| Anti-Theft | Tracks and locates your device and secures its data if it is lost or stolen. |
| Block Calls | Blocks the unwanted calls. |
| Privacy Protection | Helps to maintain a private contacts list and secure important call logs and messages. |
| Privacy Advisor | Helps to detect potentially risky apps of your device. |
| Security Advisor | Notifies about insecure settings. |
| Network Monitor | Helps to monitor and control the network data usage. |

| | |
|-----------------|--|
| Data Protection | Helps to backup and restore your data from Cloud. Also, securely delete the personal data. |
|-----------------|--|

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

Quick Heal Mobile Security Features

Quick Heal Mobile Security provides various security features that help you secure your device and data. Features include:

[Security Shield](#)

[Menus on Dashboard](#)

[Reward Points](#)

[Main menus](#)

Security Shield

Security shield displays the security level through a graphical representation. This is 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.

Increasing security level

To increase the security level, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. Tap **Security Shield**.
3. On the Security Measures screen, enable the features that you require to enhance the security of your device and its data.

Security Measures

Security measures include the following options:

| Security Measures | Description |
|----------------------|---|
| Background Scan | Enable Background Scan to scan your device continuously. This helps you to scan all apps, files, and data in real time and will detect threats instantly. |
| Anti-Theft | Enable Anti-Theft to track and locate your device when it is lost or stolen. If this feature is disabled, the device cannot be tracked. |
| Auto-Backup | Enable Auto-Backup to back up your data to the Quick Heal Cloud. You can retrieve your data whenever you require. This helps you in case you change your device or if your previous device is lost. ** Go Premium to back up your data to the Quick Heal Cloud. |
| Battery Saver | Enable Battery Saver to save power. Battery saver mode takes various actions to save power and extend battery life. You can kill all the running apps, stop network usage, and reduce screen brightness to save the power. **Go Premium to extend the battery life through the Battery Saver options. |
| Block Uninstallation | The Block Uninstallation option 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 app is active on your device. |
| Capture Intruder | Enable Capture Intruder option to capture the image of an intruder on two unsuccessful attempts to unlock the device with wrong PIN. |
| Network Monitor | Enable the Network Monitor option to monitor and control the data usage. This helps you manage your Internet bandwidth. **Go Premium to manage and control the data usage through Network Monitor. |
| SafePe | Enable SafePe to make a safe financial transaction using the banking/ financial/ ecommerce/ eWallets apps. **Go Premium to enable SafePe and configure the options. **SafePe can be purchased as an individual feature. |
| Web Security | Enable Web Security 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. |

| | |
|-----------------------|---|
| | **Go Premium to perform safe browsing through Web Security. |
| Parental Control | <p>Enable Parental Control to block inappropriate Web content and keep your kids safe online.</p> <p>**Go Premium to block infected and fraudulent websites for your kids with the help of Parental Control.</p> <p>**Parental Control can be purchased as an individual feature.</p> |
| On Install App Scan | Enable On Install App Scan option to run a scan whenever a new application is installed on the device. |
| Detect Unsecure Wi-Fi | Enable Detect Unsecure Wi-Fi to run a scan on the device to detect if you are connected to an unsecure Wi-Fi. |
| Privacy Advisor | Enable Privacy Advisor and get alerts when your privacy is violated. For example, when you install apps on your device, some apps may use your user credentials, which you may not prefer. Privacy Advisor helps you to detect such apps that may be of potential risk. |
| Safe Charging | Enable the Safe Charging option to show the current battery status and estimated approximate time to charge whenever the device is connected to the charger. |
| Security Advisor | Enable Security Advisor to get notification about unsecure settings on your device. This helps you to enhance your device security. |

Menus on Dashboard

The menus on Dashboard include the following options:

Scan

The Scan option helps to scan full device and set security measures against possible vulnerabilities and privacy violation. Scanning of your device helps you to be sure that your device is secure. If threats detected, you can take appropriate actions to enhance your device security.



Note:

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

To scan your device, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. On Dashboard, tap **Scan**.

Full scan of your device starts. You can view two options:

Stop Scan: To interrupt the ongoing scan, use this option.

View Threats: Displays the threats detected. To get full information about the threats detected, see [Threats Detected](#).

Network Monitor

The Network Monitor option lets you view a summary of your network setting in a graphical representation.

**Go Premium to avail of the features of the Network Monitor option.

To view the summary, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. On Dashboard, tap **Network Monitor**.

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

If you access this screen for the first time, a link to set Data Usage is made available. Tap this link to configure the data usage limit. 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 network data usage limit.

To set the data usage limit, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. You can set data from either option:
 - On Dashboard, tap **Network Monitor > Set Data Usage Limit**.
 - Tap main menu > **Settings > Optimize**. Select **Network Monitor** check box.
3. Configure the following options as required:
 - **SIM type:** In case of dual SIM, this option helps to select the SIM for which 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:** 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 the data usage.
- **Notify if data usage reaches:** Set this option to receive alerts if the data usage reaches the set limit.

- **Disconnect after max limit is reached:** Set this option to disconnect the data usage after the max data usage limit is reached.



Note:

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

- **Already used data from max limit:** Set this option to set a value of the network data that you have already used.

View App Data Usage

The View App Data Usage option helps you to view the data usage for an individual app.

Boost

With Boost, you can optimize your device and improve its performance. Boost option kills all the running apps to increase the device performance. You can also enhance your device performance from the Status Notifications where this option is available.

To increase the device performance:

1. Open **Quick Heal Mobile Security**.
2. On Dashboard, tap **Boost**.

This process kills unwanted apps and shows how much free space is available.

AppLock

The AppLock option helps to lock the applications installed on the phone. With AppLock, you can lock all the personal data that you want to keep confidential. The applications include both system and downloaded apps. You can protect the data from any kind of misuse. In addition, you can use scramble keyboard to avoid predicting the PIN while entering on a keypad. You can lock the applications which contain the videos, audio, chats, confidential data, images, etc.

To lock an application through AppLock, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. On Dashboard, tap **AppLock**.
List of applications with lock icon is displayed.
3. Tap the lock icon of the app that you want to lock. The lock icon is highlighted.
 - To unlock the app, again tap on the active **lock** icon.

You can also configure settings to display a prompt to lock a newly installed app.

You can also prevent detection of PIN when you enter a PIN with the help of scramble keyboard option.

To know more about the settings, see [AppLock](#).

Quick Scan

The Quick Scan option runs a scan of all the apps installed on your device. This is a fast scan. The status notifications also show the Quick Scan option. It scans the device and shows if any threats are detected. For more details, see [Threats Detected](#).

Viewing detected threats

To view the detected threats, follow either steps:

- Open **Quick Heal Mobile Security** > on Dashboard tap **Quick Scan** > tap [View Threats](#).
- Open **Quick Heal Mobile Security** > tap **main menu** > [Threats Detected](#).

You can either Uninstall or Ignore the threats. But it is recommended to uninstall the infected apps.

Parental Control

You can block infected and fraudulent websites with the help of Parental Control option. This option helps to differentiate between good and bad online content for your children and assists you to control their online activities. Thus, accordingly you can make changes to the settings or block such unwanted websites that may harm you or may steal your confidential information.

****Go Premium to block infected and fraudulent websites with the help of Parental Control option.**

****Parental Control can be purchased as an individual feature.**

Configuring Parental Control

To configure Parental Control, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. On Dashboard, tap **Parental Control** to enable it, and then tap **OK**.



Note:

To enable Parental control on the device, you must grant permissions.

Following options are available:

- **Block Access:** Use this option to block access to particular websites categories. You can block websites by categories or by adding URLs.
- **Allow Access:** Use this option to allow access to certain websites.

Blocking Access

The Block Access option helps you to block websites based on your priorities such as blocking unwanted, suspected, or adult websites for your children. You can block websites by categories or by adding URLs.

To block access to websites, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. On Dashboard, tap **Parental Control > Block Access**.

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

3. Under Block Web Categories, select the web categories that you want to block.
4. Tap **Block URLs**, type the website address that you want to block and tap the **plus (+)** sign.

The added web category or the URL gets blocked.

Allowing Access

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

To allow access to certain websites, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. On Dashboard, tap **Parental Control > Allow Access**.
3. On the Allow Access screen, tap **Enter URL to allow access** text field 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 support any beta versions of the browsers.

Web Security

Web Security blocks infected and fraudulent websites on the browser. It 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.

****Go Premium to perform safe browsing through Web Security.**

Configuring Web Security

To configure Web Security, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. On Dashboard, tap **Web Security**.
3. In the Web Security screen, select the **Web Security** check box to get complete protection from the infected and fraudulent websites.



Note:

- To enable Web Security on the device, you must grant permissions.
- The Web Security feature provides multi-browser support to block websites.
- Web Security may not support any beta versions of the browsers.

SafePe

The SafePe option helps 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.

****Go Premium to avail of the features of the SafePe option.**

****SafePe can be purchased as an individual feature.**

Configuring SafePe

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

1. Open **Quick Heal Mobile Security**.
2. On Dashboard, tap **SafePe**. A confirmation dialog is displayed.
3. Tap **Yes** to enable SafePe. The Protected Apps screen is displayed. Different options are displayed to configure SafePe.



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 Mobile Security**.
2. On Dashboard, tap **SafePe**. The Protected Apps screen is displayed.
3. Tap **Manage Apps**. The Manage Apps screen is displayed. Here you can add the app or download the apps from genuine apps link.

Adding apps to SafePe via installed apps

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

1. Open **Quick Heal Mobile Security**.
2. On Dashboard, tap **SafePe**. The Protected Apps list is displayed.
3. Tap the **Manage Apps** icon at the bottom of the screen. The Safe list, which includes the installed apps on your device, is displayed.
4. 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 that app.

Adding apps to SafePe via 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:

1. Open **Quick Heal Mobile Security**.
2. On Dashboard, tap **SafePe**. The Protected Apps screen is displayed.
3. Tap the **Manage Apps** icon at the bottom of the screen.
4. Tap **Genuine Apps** and then tap the app link that you want to download. You will be redirected to the Play store. After installing the apps, the apps are added to the Protected Apps list.

Battery Saver

The Battery Saver option helps to kill power-consuming apps and configure the settings to save power based on your priority.

Configuring Battery Saver

To configure Battery Saver, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. On Dashboard, tap **Battery Saver**.
3. Battery Saver screen is displayed where you can configure the settings.
 - You can keep the default settings by tapping the **Keep Default** button.



Note:

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

4. On the Battery Saver screen, you can configure the following options:
 - **Activate Battery Saver Mode When:** Set the battery level when the Battery Saver mode should start.
 - **Set Screen Brightness to:** Set the screen brightness after Battery Saver mode starts.

- **Set Screen Timeout:** Set the screen timeout after the Battery Saver mode starts.
- **Disable Wi-Fi:** Select this check box to disable Wi-Fi network automatically when Battery Saver mode starts.
- **Disable Bluetooth:** Select this check box to disable Bluetooth network automatically when Battery Saver mode starts.
- **Disable Sync:** Select this check box to disable auto-sync of the device automatically in Battery Saver mode.

Activating Battery Saver mode

1. Open **Quick Heal Mobile Security**.
2. On Dashboard menu, tap **Battery Saver > Activate Battery Saver Mode When**.
3. In Set Battery Level screen, tap percentage list and select required option and tap **OK**.

Setting screen brightness

1. Open **Quick Heal Mobile Security**.
2. On Dashboard menu, tap **Battery Saver > Set Screen Brightness to**.
3. In Set Screen Brightness screen, on percentage toggle bar, set required percentage and tap **OK**.

Setting Screen timeout

1. Open **Quick Heal Mobile Security**.
2. On Dashboard menu, tap **Battery Saver > Set Screen Timeout**.
3. In Set Screen Timeout screen, select the required time from the list and click **OK**.

Anti-Theft

The Anti-Theft options help to secure your device when it is lost or stolen. Anti-Theft provides many useful features such as block or allow access to certain SIM cards, automatically lock the device when untrusted SIM is changed, and track and control device remotely when it is lost or stolen. You can also add alternate contact number to your blocked device screen, so that a message can be sent to that contact if the device is lost.



Note:

The Anti-Theft option is turned OFF by default.

Configuring Anti-Theft

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

1. Open **Quick Heal Mobile Security**.
2. Enable Anti-Theft from either option:
 - On Dashboard menu, tap **Anti-Theft**. On Confirmation dialog, tap **Yes**.
 - Tap the **main menu > Settings > Anti-Theft**.
 - You can also enable the Anti-Theft through Security Measures by selecting the **Anti-Theft** check box.

After enabling the Anti-Theft option, the Set PIN screen is displayed.

3. 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.
4. Tap **Add from Contacts** to add the alternate contacts. You can set up to two alternate contact numbers. 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.

5. 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 Anti-Theft 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](#)

[Customize Block Screen](#)

[Update Alternate Contacts](#)

SIM Card Settings

The SIM Card Settings option lets you block or allow access to certain SIM cards, configure 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 Mobile Security**.
2. Access Anti-Theft via either option:
 - On Dashboard menu, tap **Anti-Theft**.
 - Tap **main menu > Settings > Anti-Theft**.
3. Ensure if Anti-Theft is enabled. If it is not enabled, tap **Anti-Theft**.
4. In Anti-Theft screen, tap **SIM Card Settings** and configure the following options:
 - **Block on SIM Change:** Enable this option if you want your device to be blocked as soon as untrusted SIM is changed. This helps you to secure your device as it can be unblocked only by an authenticated PIN.
 - **Notify on SIM Change:** Enable this option if you want to get a notification on SIM change. This notification is sent to the alternate contact numbers added to your block screen.
 - **Trusted SIM Cards:** 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

This feature blocks 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 Mobile Security**.
2. Access Anti-Theft via either option:
 - On Dashboard menu, tap **Anti-Theft**.
 - Tap **main menu > Settings > Anti-Theft**.

3. Ensure if Anti-Theft is enabled. If it is not enabled, tap **Anti-Theft**.
4. In Anti-Theft screen, select the **Block on Airplane Mode** check box.

Track & Control

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

To configure Track & Control option, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. Access Anti-Theft via either option:
 - On Dashboard menu, tap **Anti-Theft**.
 - Tap **main menu > Settings > Anti-Theft**.
3. Ensure if Anti-Theft is enabled. If it is not enabled, tap **Anti-Theft**.
4. On Anti-Theft screen, tap **Track & Control**.



Note:

Location services must be enabled to control your device remotely.

The following features appear and you can send commands for various actions. The command includes the set PIN number and the action.

- **Activate Location Services:** Helps you configure mobile settings to enable GPS. This will help in tracking the device location.
- **Device Locator:** Helps you trace the geographical location of your lost device. To get the device location, send this command:
TRACE PIN (For example – TRACE XXXX)
- **Block Device:** Helps you lock your device remotely if it is lost or theft. It sends you the location of the device and images captured. To lock the device, send this command:
BLOCK PIN (For example – BLOCK XXXX)
- **Unblock Device:** In case your device is blocked by mistake or you get back the lost device and want to unblock it, send this command:
UNBLOCK PIN (For example – UNBLOCK XXXX)
- **Wipe Data:** Helps you wipe the data from the lost device remotely. To wipe data, send this command:
WIPE PIN (For example – WIPE XXXX)
- **Ring Device:** 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 PIN (For example – RING XXXX)

- **Dial Call:** 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 PIN (For example – CALL XXXX)

** Buy Premium to send this command to access the device remotely.

- **Record Audio:** 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 PIN (For example – AUDIO XXXX)

** Buy Premium to send this command to access the device remotely.

- **Record Video:** 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 PIN (For example – VIDEO XXXX)

** Buy Premium to send this command to access the device remotely.

- **Capture Image:** 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 PIN (For example – PHOTO XXXX)

** Buy Premium to send this command to access the device remotely.

Customize Block Screen

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.

Customizing block screen

1. Open **Quick Heal Mobile Security**.
2. Access Anti-Theft via either option:
 - On Dashboard menu, tap **Anti-Theft**.
 - Tap **main menu > Settings > Anti-Theft**.
3. Ensure if Anti-Theft is enabled. If it is not enabled, tap **Anti-Theft**.
4. On Anti-Theft screen, tap **Customize Block Screen**. You can customize the following:

- Message displayed: By default a message is added.
- To change the message content, clear the **Use default message** check box. Type in the new message.
- You can view the alternate contact numbers.
- To view how the customized block screen looks, tap **View Demo**.

Update Alternate Contacts

With the Update Alternate Contacts option, 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. You can add up to two alternate contact numbers that will receive the notification.

Updating alternate contact numbers

1. Open **Quick Heal Mobile Security**.
2. Access Anti-Theft via either option:
 - On Dashboard menu, tap **Anti-Theft**.
 - Tap **main menu > Settings > Anti-Theft**.
3. Ensure if Anti-Theft is enabled. If it is not enabled, tap **Anti-Theft**.
4. On Anti-Theft screen, tap **Update Alternate Contacts**.
5. In the new screen, Tap **Add from Contacts**.
6. You can search the contact or select the contact and tap **Add Contact**.
 - To remove the alternate contacts, in the Update Alternate Contacts screen, tap the **(X)** **multiplication** sign available in front of the contact.

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 various security reasons. Whenever the device gets blocked, you can unblock your screen with the PIN 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.

Unblock device with 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:

1. On the block screen, tap **Unblock Screen**. The Enter PIN screen is displayed.
2. In case you forgot the PIN, tap **Forgot PIN?** The Forgot PIN screen is displayed with three options to unblock your phone.

3. Tap **Get Temporary PIN**. The Get Temporary PIN screen is displayed.
4. Tap **Send**. A temporary PIN is sent to the alternate contact numbers that you have added to the customize block screen while configuring Anti-Theft.



Note:

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

Unblock device with Google Authentication

This option helps you to unblock your screen by validating your Gmail account.

To validate your Gmail account, follow these steps:

1. On the block screen, tap **Unblock Screen**. The Enter PIN screen is displayed.
2. In case you forgot the PIN, tap **Forgot PIN?**. The Forgot PIN screen is displayed with three options to unblock your phone.
3. Tap **Google Authentication**. The Google Authentication screen is displayed.
 - In case of no Internet connectivity, the Configure Internet screen is displayed.
4. To configure the Internet, follow these steps:
 - i. On the Configure Internet screen, enable Mobile to turn ON mobile data, or enable Wi-Fi to turn ON Wi-Fi.
 - ii. 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.
5. After the Internet is connected, check your email address, enter the password of your Gmail account and then tap **Login**.

Unblock device with 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:

1. On the block screen, tap **Unblock Screen**. The Enter PIN screen is displayed.
2. In case you forgot the PIN, tap **Forgot PIN?**. The Forgot PIN screen is displayed.
The three options to unblock your phone are displayed.
3. Tap **Remote Device Management**. The Remote Device Management screen is displayed.
4. Log on to the RDM portal using the URL provided on the screen.



Note:

If Internet is not available, you must configure Internet to access the RDM portal. To know how to configure your Internet, see [Configuring Internet](#)

Block Calls

The Block Calls option helps you to block unwanted calls and messages. With this option, you can easily block unwanted calls from both local and all unknown international numbers. You can also block messages from unwanted local numbers. This option blocks all commercial calls and messages if required. You can also block a number of particular series or messages by adding keywords.



Note:

-
- SMS blocking is not supported on the devices with OS 4.4 and later versions.
 - Block Calls is turned OFF by default on the devices with OS 6.0 and later versions. To access all the features of Block Calls on the devices with OS 6.0 and later versions, you must grant permissions.
-

Configuring Block Calls

To configure Block Calls, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. To enable Call Block follow either option:
 - On Dashboard menu, tap **Block Calls > Yes**.
 - Tap **main menu > Settings > Device Privacy** > select the **Block Calls** check box.
3. The Block Calls option is enabled. Different options to block the calls is displayed.

Blocking unwanted calls

To block unwanted calls, you can use following options and steps:

1. Open **Quick Heal Mobile Security**.
2. On Dashboard tap **Block Calls**. Different options are displayed:
 - **Block Number:** Use this option to enter the number and block it.
 - Type the number and tap **Add to Blocked Numbers List**.
 - **Phone Logs:** Use this option to block the number from phone logs.
 - You can choose a contact from the phone logs and tap **Add to Blocked List**.
 - **Contact List:** Use this option to block number from contact list.
 - You can add a contact from the Contact list and tap **Add to Blocked List**.

- **Custom:** Use this option to block the calls from custom series (Ex: 40000000000). You can also specify whether a contact should begin or end with such series.
 - In the text field, enter 3-20 characters and select the Starting with or Ending with option.



Note:

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

- **Blocked List:** Displays the numbers that were blocked with the help of Block Calls option.
- **Block Spam (DND):** When SIM is present and it is noticed that the call numbers are mostly from India, this option is visible.

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 Mobile Security**.
2. Tap **Block Calls** and then tap **Block Spam (DND)**.
3. Register the number in one of the following ways:
 - **Fully Block:** Use this option to block all commercial calls and SMSs.
 - **Fully Unblock:** Use this option to unblock all telemarketing calls and SMS.
 - **Partially Block:** Use this option to block all commercial calls, but you will continue to get SMSs from the selected telemarketing categories.
 - **Report a Number:** Use this option 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.



Note:

- You can de-register your number later from DND list if required.
 - This option is not available outside India.
 - TRAI complaint may not be reported for Reliance SIM.
-

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.

****Go Premium to keep your personal info private & prevent unauthorized access.**



Note:

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

Configuring Privacy Protection

To configure Privacy Protection, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. To enable privacy protection, use either option:
 - On Dashboard, tap **Privacy Protection**.
 - Tap main menu > **Settings** > **Device Privacy** > select **Privacy Protection**.

Making Contacts Private

1. Open **Quick Heal Mobile Security**.
2. On Dashboard, tap **Privacy Protection**.
3. To make a contact private, tap **Add Private Contact**.

Different options to make a contact private is displayed:

- **Add Number:** Use this option to make a number private.
 - **Add from Phone Logs:** Use this option to select numbers from phone log and make private.
 - **Add from Contact List:** Use this option to add numbers from Contact list and make private.
4. 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.
- 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 Mobile Security**.
2. On Dashboard, tap **Privacy Protection**.

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

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

Clearing any of the options will delete them permanently.

4. 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, then 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 on 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.

Privacy Advisor

The Privacy Advisor option allows you to 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.

Configuring Privacy Advisor

To configure Privacy Advisor, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. To enable Privacy Advisor, use either option:
 - On Dashboard, tap **Privacy Advisor** to enable it.
 - Tap Security Shield and from Security Measures screen select **Privacy Advisor** check box.

The applications are displayed with the permissions that are assigned.

Viewing app permission

To view the permissions that an app is assigned, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. On dashboard, tap **Privacy Advisor**.
3. Tap the application.
 - If you find that an app uses any crucial information, you can uninstall that app by tapping **Uninstall**.
 - If you find the app trustworthy, then you can trust the app by tapping **Trust** and in confirmation screen tap **Yes**. This app will be added to the Trusted Apps List.

Various permissions that an app may use are as follows:

| Permissions | Description |
|--------------------|---|
| Access to Accounts | Apps with this permission may request authentication credentials of the account. Such apps may add or remove accounts and delete your passwords. |
| Access to Contacts | Apps with this permission can read, write, and share your personal contacts with their servers by compromising your data. |
| Read Identity Info | The apps with this permission can share phone state including IMEI number, phone number, and serial number of the phone to their server without your consent. |

| | |
|--------------------|--|
| Tracking Locations | Apps with this permission can update your device location to their servers, which may be harmful. |
| Access to Messages | Apps with this permission are allowed to read, write, or send SMS from the device. Malicious apps may read your confidential messages or delete them before you receive. |
| Access to Network | Apps with this permission allow network usage in the background. |
| Other Permission | Apps that have permissions other than those mentioned above are available under this category. |

Privacy Audit Notification

When you install 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 that an app that violates your privacy or if you find your personal information is at risk, you can remove that app immediately.

Security Advisor

The Security Advisor notifies about insecure settings and lets you check the possible vulnerabilities present on the device. You can enhance the security settings to stop such attempts to exploit vulnerabilities.

Configuring Security Advisor

To configure Security Advisor, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. To enable Security Advisor, use either option:
 - On Dashboard, tap **Security Advisor**.
 - Tap Security Shield and in Security Measures screen, select **Security Advisor** check box.



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.

3. On the Security Advisor screen, the security settings are displayed under the following categories:
 - Unsecure 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 Unsecure Settings include a setting icon next to them. You can increase the security level by using the setting icon. When you tap the Setting icon, you are redirected to the respective security features where you can configure them.

Security settings are as follows:

| Security Settings | Description |
|--------------------------|---|
| Accounts & Sync | The device receives data from synced accounts or sites that increases the risk of hacking and account misuse. It is advisable to turn this option to OFF when not required. |
| Bluetooth | Data transfer through Bluetooth might put your device and its data at risk. It is advisable to turn this option to off when not required. |
| Device Memory Encryption | <p>You can encrypt the data on your device. This ensures security by preventing unauthorized access to your data. It is advisable to turn this option to ON to secure your data from unauthorized access.</p> <p> Note:</p> <p>The Device Memory Encryption setting is available only on supported OS.</p> |
| Hotspot & Tethering | <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> <p>The Hotspot and Tethering settings are available only on supported OS and vendors.</p> |
| Anti-Theft | Protects your device and its data. This option allows you to trace, block, wipe data, and ring the device if your device is lost. |
| Background Scan | Shields your device against various types of threats. Keep this option enabled for security. |
| Screen Lock | If this option is disabled, your personal data may be at risk of misuse. Ensure that Pattern, PIN, Password or Finger Print screen lock options are set to safeguard the device data. |
| Unknown App Sources | If any app is installed from a source other than Google Play, then that app might pose a threat to your device. Therefore, it is advisable that you turn this option to OFF. |
| USB Debugging | If USB debugging is enabled, your device is at risk of being hacked and your data can be misused. Turn this option to OFF for security. |

| | |
|-----------------------|--|
| Detect Unsecure Wi-Fi | Communicating through an open or unsecured Wi-Fi network can put your data at risk. It is advisable to connect Wi-Fi only on a secure network. Turn this option to OFF for security. |
|-----------------------|--|

Network Monitor

The Network Monitor option sets data usage limit for mobile network. On tapping Network Monitor, network summary is displayed.

Configuring Network Monitor

To configure data usage limit, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. To configure Network Monitor, use either option:
 - On Dashboard menu, tap Network Monitor. The Network Consumption Summary is displayed.
 - Tap **main menu** > Settings > **Optimize** > select **Network Monitor** check box.
3. In Network Consumption Summary screen, you can set data usage limit and view app data usage.

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

Set Data Plan

With this option, you can set the data plan for your device.

****Go Premium to set the data plan and manage the usage of your data.**

To set the data plan, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. Use either option to set the data plan:
 - On Dashboard tap **Network Monitor** > **Set Data Usage Limit**.
 - Tap main menu > **Settings** > **Optimize** > tap **Data Plan**.

The Data Plan screen is displayed.
3. The Data Plan screen shows the following options to be configured.
 - SIM Type: Helps 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: Helps to set the start date of the data plan.
- Set data usage limit: Helps 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: Helps to set the maximum limit of the data usage.
- Set data usage warning limits: Helps to receive the notification on reaching the maximum data usage limit.
- Already used data: Helps to view the already used data while setting the data plan.

Data Protection

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

****Go Premium to avail of the features of the Data Protection option.**

To use Data Protection, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. On Dashboard, tap **Data Protection** 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 Mobile Security**.
2. On Dashboard, tap **Data Protection**.
3. Tap **Backup data to cloud**.

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

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

1. Go to any third party application. For example: Gallery.
2. Select the media file that you want to backup to cloud, and tap the **Share** option.
3. 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:

1. Open Quick Heal Mobile Security.
2. On Dashboard, tap **Data Protection**.
3. Tap **Backup data to cloud**.

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

4. 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.
5. 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 Mobile Security**.
2. On Dashboard, tap **Data Protection**.
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 the 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 Mobile Security**.
2. On Dashboard, tap **Data Protection**.
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.

****Go Premium to use the Delete Personal Data option.**



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 Mobile Security**.
2. On Dashboard, tap **Data Protection**.
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), and SIM Data (Contacts & Messages).



Note:

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

4. Tap **Delete**.

Reward points

The Reward points icon on the top right of Dashboard helps you to view and redeem points. You can redeem these points to get access to Pro features for a limited period. You can also earn points via two options such as Share and Quick action.



Note:

Backup is not available for subscription of premium through reward points.

How to redeem your reward points?

To redeem your reward points to get access to pro features, follow these steps:

1. Open **Quick Heal Mobile Security**.
Dashboard is displayed.
2. Tap the **Reward points** icon on the top right of Dashboard.
A pop-up screen with total points available in your account is displayed. You can also view the points required to go premium for one week.
3. Tap **Redeem Now** to redeem your points for one week premium subscription. If you redeem your points for one week subscription, the successful message screen is displayed.
4. If you tap **Later**, the Points Earned screen is displayed which include total available points in your account and more options to avail of different subscriptions.



Note:

This option is not available when you purchase paid subscription for 1 year.

How to earn points?

To earn more points to get Pro features. This option provides two ways to earn points such as Share and Quick Action.

Earn points via Share

To earn points via Share option, follow these steps:

1. Open **Quick Heal Mobile Security**.
Dashboard is displayed.
2. Tap the **Reward points** icon on the top right of Dashboard. The Points Earned screen is displayed.
3. Go to the **How to earn points** section and tap the **Share** option.
The Share App options are displayed.

4. Select any of the sharing option as required and share the Quick Heal Mobile Security application.

Share the application with your friend. You will earn points when your friend installs & activate the app.

Earn points via Quick Action

To earn points via Quick Action option, follow these steps:

1. Open **Quick Heal Mobile Security**.
Dashboard is displayed.
2. Tap the **Reward points** icon on the top right of Dashboard. The Points Earned screen is displayed.
3. Go to the **How to earn points** section and tap the **Quick Action** option. The Quick Action screen is displayed. Two options such as **News** and **Scan & Earn**.
4. Tap the required option and earn points.



Note:

-
- Points will be added to your account only if the ad is displayed when you perform the action. To view ads, enable the **Show ads** option in Settings. To enable show ads, go to **Quick Heal Mobile Security > main menu > Settings > Show Ads**.
 - The Show Ads option is visible only when you purchase premium through reward points.
-

Main menus

Main menu or global menu includes the following:

[Home](#)

[Settings](#)

[About Product](#)

[Buy Premium or Extend Premium](#)

[Logs](#)

[Help](#)

Home

The Home option lets you go to the Home screen or Dashboard of Quick Heal Mobile Security.

Settings

Settings include features related to application settings such as setting PIN, securing uninstallation of Quick Heal app, setting scan options, setting device privacy, Optimize, AppLock, SafePe, Anti-Theft, safe charging, detect unsecure Wi-Fi, and show ads. To know more about Settings, see [Settings](#).

To access Settings, follow these steps:


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

About Product

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

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

| Areas | Details | Buttons & Icons |
|---|-----------------------------------|--|
| Quick Heal Mobile Security product details | Product name & Version | <ul style="list-style-type: none"> • Update: Helps to update the virus database and license subscription details. • Rate: Helps to rate the app if you find it useful. • Share: Helps to share the Quick Heal application via various methods. |
| License Information | Product key & License expiry date | <ul style="list-style-type: none"> • Buy Premium: Helps to buy premium to gain full access to all the features. |

| | | |
|--------------------------|--------------------------|--|
| | | <ul style="list-style-type: none"> • User Details: Helps to update your details such as Username, Email ID and Mobile Number.  You can verify or update your mobile number only once. <ul style="list-style-type: none"> • Feature Purchase: Shows information about individual features that are purchased and their expiry. |
| Legal Information | Copyright of the product | Helps to know the license information of the application. |

Buy Premium or Extend Premium

You will view either options depending on the purchase.

- **Buy Premium:** To have a new purchase, you will view Buy Premium.
- **Extend Premium:** If you have already bought the app, you will view Extend Premium.

These options help to gain full access to all the features of the product. The premium features include Backup and Restore, Anti-theft advance commands, Web Security, Parental Control, and SafePe. Quick Heal Mobile Security also provides option to purchase individual features.

Individual Feature Purchase

You can purchase individual features and use the subscription for specified time. The individual feature purchase is applicable to SafePe and Parental Control.

To purchase premium, follow these steps:

1. Open **Quick Heal Mobile Security**.
Dashboard is displayed.
2. Tap **main menu** and then tap **Buy Premium** or **Extend Premium**.
3. The **Premium Purchase** screen is displayed with the features and mode of purchase.
4. In Features section, select the required options:
 - **SafePe Feature:** Select this option if you want to purchase only SafePe feature.
 - **Parental Control Feature:** Select this option if you want to purchase only Parental Control feature.
 - **All Premium Feature:** Select this option if you want to buy all the premium features of Quick Heal Mobile Security.
5. In Purchase Options section, select the mode of purchase:
 - **From Google:** Select this option if you want to purchase through Google Play store.
 - **Enter Product Key:** Select this option if you have already purchased a product key.



Note:

SafePe and Parental Control features cannot be purchased with Enter Product Key option.

- **Redeem Points (Ads):** Select this option if you want to buy premium pack with reward points in your wallet. To know how to redeem points, see [How to redeem your reward points.](#)

4. Select the required options and tap **Buy**.

Logs

Logs include activity logs and information about the detected threats.

Activity Log

The Activity Log option helps you to view the activity logs of various features such as Anti-theft, Scan, Background Scan, and Update. You can filter the logs based on days and security features.

Threats Detected

This option helps 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. The detected threats are categorized into four types: Resolved, Not Resolved, Quarantined, and Vulnerabilities. The following are the detected threat types:

[Resolved](#)

[Not Resolved](#)

[Quarantined](#)

[Vulnerabilities](#)

Resolved

The Resolved option displays the list of resolved applications. After you resolve the threats from Not Resolved 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:

1. Open **Quick Heal Mobile Security**.
2. Tap **main menu > Threats Detected**. The Threats Detected screen is displayed.
3. In the View list, tap **Resolved**. The list of resolved threats is displayed.

Not Resolved

The Not Resolved option 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:

1. Open **Quick Heal Mobile Security**.
2. Tap **main menu > Threats Detected**. The Threats Detected screen is displayed.
3. In the View list, tap **Not Resolved**. The list of unresolved threats is displayed.
 - To remove the application from the device, tap **Uninstall > OK**.
 - To ignore, tap **Skip**.

Quarantined

This option 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:

1. Open **Quick Heal Mobile Security**.
2. Tap **main menu > Threats Detected**. The Threats Detected screen is displayed.
3. In the View list, tap **Quarantined**. The list of Quarantined files is displayed.
 - To restore the files, 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:

1. Open **Quick Heal Mobile Security**.
2. Tap **main menu > Threats Detected**. The Threats Detected screen is displayed.

3. In the View list, tap **Vulnerabilities**. The list of vulnerable threats is displayed.
 - Trust: Tap the Trust option to make the vulnerable app or file as trusted entity.
 - Uninstall: Use this option to uninstall any application.
 - Delete: Use this option 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 options to assist you and resolve your issues.

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

Settings

The Settings menu include the following options:

[General](#)

[Scan](#)

[Device Privacy](#)

[Optimize](#)

[AppLock](#)

[Network Monitor](#)

[SafePe](#)

[Anti-Theft](#)

[Backup](#)

[Safe Charging](#)

[Detect Unsecure Wi-Fi](#)

[Show Ads](#)

General

The General option helps to configure features related to the application. This option includes the following:

Change PIN

The Change PIN option helps you to set the PIN. You must enter the correct PIN to access the features of the application. After the PIN is set on your device, the name of the 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 Mobile Security**.
2. Tap **main menu > Settings > General > Change PIN**.

3. Enter New PIN, Re-Enter PIN, and then tap **Submit**.

To change the PIN, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. Tap **main menu > Settings > General > Change PIN**.
3. Tap **Submit**.

Track Activity Log

The Track Activity Log option helps you to track activity logs for certain period.

To configure Activity Log, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. Tap **main menu > Settings > General > Track Activity Log**.
3. In Track Activity Log for dialog, select one of the following option to track the logs for; 7 days or 30 days 45 days.

Status Notification

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

To enable Status Notification, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. Tap **main menu > Settings > General**.
3. Select the **Status Notification** check box to enable notifications.

Quick Settings Notification

Enable the Quick Settings 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 Mobile Security**.
2. Tap **main menu > Settings > General**.
3. Select the **Quick Settings Notification** check box to enable it.

Manage Through Web

You can manage Quick Heal Mobile 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 Mobile Security**.
2. Tap **main menu > Settings > General**.
3. Select 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

With this option, you can 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 Mobile Security**.
2. Tap **main menu > Settings > General**.
3. Enable **Manage Through Web**, and then tap **Create Web Account**. You will be navigated to the Quick Heal RDM portal to create the account.

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 the 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 Mobile Security**.
2. Tap **main menu > Settings > General**.
3. Select 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 Mobile Security**.
2. Tap **main menu > Settings > General**.
3. Select the **Application Statistics** check box to enable it.

Block Uninstallation

The Block Uninstallation 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.

To enable Block Uninstallation, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. Tap **main menu > Settings > General**.
3. Select the **Block Uninstallation** check box to enable it.

You are redirected to the Block Uninstallation dialog to activate the device administrator.

4. On confirmation dialog, tap **OK**.
5. To proceed further, tap **Activate**.

Capture Intruder

The Capture Intruder option helps to capture the intruder image 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 Capture Intruder, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. Tap **main menu > Settings > General**.
3. Select the **Capture 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 Mobile Security**.
2. Tap **main menu > Settings > Scan** and set different scan options.

Background Scan

Helps you to scan your device in real time. With this option, 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, select the **Background Scan** check box.

On Install App Scan

The On Install App Scan option helps to run a scan, whenever a new application is installed on the device.

- To activate this option, select the **On Install App Scan** check box.

Scan App Before Download

With this option, you can scan apps before it is downloaded from the Google Play Store.

- To activate this option, select the **Scan App Before Download** check box.
You need to provide access permission to enable this option.

Silent Scan app before download

This option is dependent on Scan App Before Download option. With this option, the app is scanned silently from the Google Play Store without informing the user.

- To activate this option, make sure the **Scan App Before Download** option is enabled and then select the **Silent Scan app before download** check box.

Scan from Cloud

Scan from Cloud option helps you to scan through Cloud. Cloud scanning allows scanning of all the installed applications and .apk files available on the device storage.

- To activate this option, select the **Scan from Cloud** check box.



Note:

Ensure to check your Internet connectivity before performing Cloud scanning.

Vulnerability Scan

Enable this option to scan for the potential vulnerabilities on the device.

- To activate this option, select the **Vulnerability Scan** check box.

Scan SD Card

This option is helpful to run a scan of the newly inserted SD card on the device.

- To activate this option, select the **Scan SD Card** check box.

Schedule Scan

Schedule Scan allows you to schedule a new scan by adding time and frequency. This helps you to scan your device at the defined schedule automatically.



Note:

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 Mobile Security**.
2. Tap **main menu > Settings > Scan > Schedule Scan**.

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

3. To set a new scan schedule, tap **Schedule New Scan**.
4. Under the 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 selected then your device is scanned once in 24 hours while charging with battery level at least 50% or more.
- If you select **Once a day**, specify the time.
- If you select **Once a week**, specify day and time.
- If you select **Once a month**, specify date and time.

5. Set the scan schedule and tap **Save**.

Delete Quarantined Files After

Helps you to set a period after which all the quarantined files will 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.

Device Privacy

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

To configure Device Privacy , follow these steps:

- Tap main menu > **Settings** > **Device Privacy** > select **Block Calls** check box.

Call Filter

To get complete information about Block Calls, Notifications, Alert on Call Rejection, International Calls, see [Block Calls](#)

Privacy Protection

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

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

Optimize

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

****Go Premium to avail of the features of the Optimize option.**

To configure the Optimize option, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. Tap **main menu** > **Settings** > **Optimize**. The Optimize screen is displayed.
3. Optimize includes the following options:

Device Performance

Battery Saver

This option helps to save the battery life. Activate this option by selecting **Battery Saver** check box.

To know about complete Battery Saver options, see [Battery Saver](#).

Boost

The Boost option allows you to increase the device speed.

To increase device performance, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. Tap **main menu** > **Settings** > **Optimize**.
3. In Boost screen, you can configure the following options:
 - 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 the specified 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.

Network Monitor

This setting helps to configure Network Monitor and Data Plan.

Network Monitor

This option allows you to enable Network Monitor and set Mobile Network to control data usage limit.

****Go Premium to avail of the features of the Network Monitor option.**

To enable Network Monitor, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. Tap **main menu > Settings > Optimize**.
3. Select the **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.

Data Plan

This option helps to set the data plan. To get complete information about it, see [Set Data Plan](#).

AppLock

The AppLock option helps to lock the applications installed on the device. In Settings section, AppLock helps to configure the settings of Show Prompt and Scramble Keyboard options.

Show prompt to lock newly installed apps

Display a prompt to lock a newly installed application on the device with Show Prompt option. If this option is enabled, then a prompt is displayed whenever you install a new application on the device. This helps to secure the application from the moment it is installed on the device.

Scramble Keyboard

The purpose of this setting is to show random key ordering on the AppLock screen. This is to prevent detection of PIN from unauthorized users when you enter a PIN with the help of keyboard. The position of the numbers changes every time the keypad is activated so that only the actual user can see the scrambled digits.

Access AppLock through Fingerprint

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



Note:

The Fingerprint option is supported only on the devices with Fingerprint sensor.

If user has given accessibility permission to QH app then the locked app can be unlocked using fingerprint, otherwise user has to enter PIN to unlock the app.

Configuring Show Prompt and Scramble Keyboard

To enable or disable Show Prompt and Scramble Keyboard options, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. Tap **main menu > Settings > AppLock**.

Two options are displayed.

- **Show Prompt:** To show a prompt before locking newly installed app, select this check box.
- **Scramble Keyboard:** To prevent detection of PIN from unauthorized users, select this check box.

SafePe

The SafePe option helps to make a safe financial transaction using the banking/ financial/ ecommerce/ eWallets apps. SafePe checks 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.
- **Risky Device Alert:** Enable this option to be notified if the device is not secure at the time of any transaction. You will not receive alert for protected apps if the device is secure.

Anti-Theft

Anti-Theft provides many useful features such as block or allow access to certain SIM cards, automatically lock the device when untrusted SIM is changed, track and control device remotely when it is lost or stolen, displays alternate contact numbers on block screen etc.

- To configure Anti-Theft and get complete information about it, see [Anti-Theft](#).

Backup

The Backup option is available to enable the backup option from Data Protection. Backup helps to secure your data by saving it to Quick Heal Cloud. You can back up, retrieve, and delete data as per your requirement. To get more information about backup options, see [Data Protection](#).

****Go Premium to avail of the features of the backup.**

To enable Backup, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. Tap the **main menu > Settings**.
3. Select the **Backup** check box to enable it.
4. 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**.

Safe Charging

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 Mobile 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.

Detecting unsecure Wi-Fi

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

1. Open **Quick Heal Mobile Security**.
2. Tap **main menu > Settings**.
3. Select the **Detect Unsecure Wi-Fi** check box to inform you about the unsecured Wi-Fi.

Show Ads

When this option is selected, you will receive advertisements in the application.

Configuring Show Ads option

To enable Show Ads option, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. Tap **main menu > Settings**.
3. Select the **Show Ads** check box to receive advertisements.

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 Mobile Security**.
2. Tap the **main menu**.
3. In the Help section, tap either of the following options:
 - Online Help
 - FAQ
 - Contact Us
 - Share App
 - Uninstall Quick Heal

Online Help

This includes the online help of Quick Heal Mobile Security. If you want to know about the features and to configure them, you can access it.

- In the app tap **main menu > Help > 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 Mobile Security.

- In the app tap **main menu > Help > FAQs**. You are directed to FAQs.

Contact Us

Includes various support facilities:

Live Chat

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

Web Support

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

Support Center

You can call us at the following numbers: 1800 212 7377 between 08:00 AM to 11:00 PM IST (India Standard Time) between Monday to Saturday.

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.

Share App

The Share App option lets you share the Quick Heal Mobile Security installer (.apk) using NFC (Near Field Communication), Bluetooth, and Wi-Fi Direct. The installer file can also be shared using other sharing applications available on your device through the **Other Apps** option.

Uninstall Quick Heal

Removing Quick Heal Mobile 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 Mobile Security, follow these steps:

1. Open **Quick Heal Mobile 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, 44
Access Anti-Theft through Fingerprint, 24
Activity, 46
Allow Access, 20
Anti-Theft, 23
Application Statistics, 51

B

Backup, 58
Backup data to cloud, 39
Block Access, 19
Block Calls, 30
Block on Airplane Mode, 25
Block Spam (DND), 31
Block Uninstallation
 Activate device administrator, 52
Block Uninstallation, 52
Blocked Numbers, 30
Boost, 55
Buy Premium, 45

C

Capture Intruder, 52
Contact Us
 live chat, web support, support contacts, 60
Create Web Account, 51
Creating an account with Quick Heal RDM, 6
Custom Back up, 40
Customize Block Screen, 27

D

Data Protection, 39
Delete backup from Cloud, 41
Delete Personal Data, 41
Detect Unsecure Wi-Fi, 59
Device Privacy, 54
 block international calls, enable Privacy Protection, 55
Downloading and Installing Quick Heal Mobile Security, 2

E

Enable Network Monitor, 56

G

General, 49
Getting started, 1

H

Help, 48, 60
 FAQ, contact us, uninstall Quick Heal, 60
How to earn points, 42
How to redeem your reward points, 42
How to unblock your Anti-theft block screen?, 28

L

Logs, 46

M

Main menus, 44
Manage Through Web, 50
 manage device through Quick Heal RDM, 9
Menus on Dashboard, 16
Mobile Network, 38

N

Network Monitor
 manage mobile network, Wi-Fi, 56
News Notification, 51

O

Optimize, 55
 Device performance, save power, speed up device, set
 data plan, 55

P

Parental Control, 19
 allow websites, block websites, 19
Prerequisites, 1
Privacy Advisor, 35

Privacy Audit Notification, 36
Privacy Protection, 31
 private contacts, nonprivate contacts, 32

Q

Quarantined, 47
Quick Heal Mobile Security Dashboard, 11
Quick Heal Mobile Security Features, 14
Quick Heal RDM
 features, 3, 4
Quick Heal Remote Device Management
 Quick Heal RDM, Cloud portal, 50
Quick Scan, 19
Quick Setting Notification, 50

R

Reactivating Quick Heal Mobile Security, 3, 9
Register Product
 through Internet and SMS, 3
Registering Quick Heal Mobile Security, 3, 6
Registration and reactivation, 3
Resolved, 46
Restore backup from cloud, 40
Reward points, 42

S

Safe Charging, 59
SafePe, 21
Scan, 16
Scan Device, 52

Secure Data
 back up data, restore data, delete data securely, 39
Security Advisor, 36
Security Shield, 14
Set Data Plan, 38
Set Data Usage Limit, 17
Set PIN, 49
Settings, 49
Share App, 61
SIM Card Settings, 25
Supported Android
 versions, screen resolutions, 1
System requirements, 1

T

Threats Detected, 46
Track & Control Device, 26
 locate device, send commands to device, 26
Track Activity Log, 50
Trusted SIM
 multiple SIM cards, local SIM, 25

U

Uninstall Quick Heal
 uninstalling, deactivating, 61
Unresolved, 47
Update Alternate Contacts, 28

V

View App Data Usage, 18