



Quick Heal AntiVirus for Mobile

User Guide

Version 1.0

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.

This document is current as of the initial date of publication and may be changed by Quick Heal at any point of time.

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 document is the User Guide of Quick Heal AntiVirus for Mobile (hereafter referred to as “Quick Heal AntiVirus”).

This user guide covers all the information required to install and use Quick Heal AntiVirus. 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.
Quick Heal AntiVirus	Product Name
QHMAV	Short form of product name

Document History

Release No	Change Date	Change Summary
1.0	January 2018	Quick Heal AntiVirus released.

What's New in this Version?

Features	Description	Section
All	Released Quick Heal AntiVirus	All

Contents

1. Getting started.....	1
Prerequisites	2
System requirements.....	2
Installation of Quick Heal AntiVirus.....	2
Downloading Quick Heal AntiVirus installer	2
2. Registration, reactivation, and renewal	3
Registering Quick Heal AntiVirus	3
Registering licensed version	3
Share registration logs	4
Reactivating Quick Heal AntiVirus	5
Reactivating licensed version.....	5
Renewal of Quick Heal AntiVirus	6
Renewing licensed version.....	6
<i>Renewal through website</i>	6
<i>Call Us</i>	7
3. Dashboard	8
Optimize.....	8
Privacy.....	8
Secure.....	9
Settings.....	9
Dashboard cards	9
4. Features.....	11
Optimize.....	11
Configuring Optimize	11
Boost	12
<i>Optimize now</i>	12
<i>Summary</i>	13
<i>Auto optimize</i>	13
<i>RAM used by installed apps</i>	13
<i>List of uninstalled apps</i>	14
<i>Responsive Dashboard cards</i>	14
Battery.....	15

<i>Safe Charging</i>	15
<i>Battery Saver</i>	16
<i>Boost Now</i>	16
<i>Configure Battery Saving Mode</i>	17
<i>Auto Saving Mode</i>	17
<i>Responsive Dashboard cards</i>	18
Storage	18
<i>Summary</i>	19
<i>Auto Cleaning</i>	19
<i>Clear Browser history</i>	19
<i>Move data from Internal storage to SD card</i>	20
<i>Move data from SD card to Internal Storage</i>	20
<i>Delete Personal Data from Phone</i>	21
<i>Responsive Dashboard cards</i>	22
Data Usage	22
<i>Tracker</i>	23
<i>Summary</i>	24
<i>Set Data Plan</i>	24
<i>Responsive Dashboard card</i>	26
Privacy	26
AppLock.....	27
<i>Access AppLock through Fingerprint</i>	27
<i>Show prompt to lock newly installed apps</i>	28
<i>Scramble Keyboard</i>	29
<i>Intruders</i>	29
<i>Responsive Dashboard cards</i>	29
Vault	30
<i>Access Vault through Fingerprint</i>	30
<i>Contacts Vault</i>	31
<i>Removing contacts from vault</i>	32
<i>Intruders</i>	32
<i>Responsive Dashboard cards</i>	32
Block Numbers	32
<i>Blocked List</i>	33
<i>Block a Custom Series</i>	34
<i>Block SMS with Keywords</i>	35
<i>Block Unknown International Calls</i>	35
<i>Alert on Call Rejection</i>	35
<i>Block WAP/PUSH SMS</i>	35
<i>Register with DND</i>	35
<i>Responsive Dashboard cards</i>	36

Privacy Advisor	37
<i>Viewing app permissions</i>	38
<i>Responsive Dashboard cards</i>	38
Secure.....	38
Antivirus	39
<i>Scan now</i>	40
<i>List of Threats</i>	40
<i>Schedule Scan</i>	41
<i>Background Scan</i>	41
<i>On Install App Scan</i>	42
<i>Scan App Before Download</i>	42
<i>Scan from Cloud</i>	42
<i>Responsive Dashboard cards</i>	42
SafePe	43
<i>Managing and adding apps</i>	43
<i>Downloading apps through Genuine Apps link</i>	44
<i>Settings</i>	44
Anti-Theft	44
<i>Access Anti-Theft through Fingerprint</i>	45
<i>Anti-Theft</i>	45
<i>Phone Tracker</i>	46
<i>Intruders</i>	46
<i>Block phone when the airplane mode is turned ON</i>	46
<i>Block phone if a new SIM is inserted, to avoid intrusion</i>	46
<i>Notify on SIM change</i>	46
<i>Customize your Block Screen</i>	47
<i>Recovery Contacts</i>	47
<i>List of Trusted SIMs</i>	47
<i>Remote Actions</i>	47
<i>Unblock your Anti-theft block screen</i>	48
<i>Responsive Dashboard cards</i>	49
Security Advisor	49
<i>Risk Settings</i>	49
<i>Secure Settings</i>	50
5. Settings	52
Account Settings	52
Set PIN.....	52
<i>Responsive Dashboard card</i>	53
User Details	53
<i>Responsive Dashboard card</i>	53

App Settings	53
Set Notifications.....	54
Uninstall Protection	54
Intruder Image Capture	55
Intruder Gallery.....	55
Quick Setting on Status Bar	55
Clean Cache.....	56
Floating Window	56
<i>Enable Floating Window</i>	56
Application Statistics.....	57
News.....	57
Help Center	57
Help	57
FAQs	57
Contact Us.....	58
About.....	59
About Product.....	59
Uninstall Quick Heal AntiVirus App.....	59
How to use?	60
6. Index.....	61

Getting started

Quick Heal AntiVirus is the real-time security solution for Android devices.

Quick Heal AntiVirus is a one-stop security solution specifically designed for mobile devices. It protects your smartphone from viruses and malware. This application is very simple to install and easy to use.

With Quick Heal AntiVirus on your smartphone, you can:

- Make your device perform faster.
- Monitor the device battery.
- Limit your mobile data usage.
- Lock the applications so that no one can spy your data.
- Use Vault to make your contacts private.
- Track and locate the mobile device when lost or stolen.
- Manage all applications on the device.
- Block calls and SMS from an unwanted number and receive notification when the SIM card is changed.
- Floating Window on the Home screen.

During installation, read each installation screen carefully and follow the given instructions.

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

[Prerequisites](#)

[System requirements](#)

[Installation of Quick Heal AntiVirus](#)

Prerequisites

Guidelines for installing Quick Heal AntiVirus on the device:

- A device with multiple antivirus software applications installed, may result in the device malfunction. Before installing Quick Heal AntiVirus, remove other antivirus software applications to avoid any issues.
- Close all open applications before installing Quick Heal AntiVirus.

System requirements

To install Quick Heal AntiVirus, the device must meet the following criteria:

You can install Quick Heal AntiVirus on any Android mobile devices.

Supported Android versions and screen resolutions are as follows:

Supported Android Versions

Quick Heal AntiVirus is compatible with the following versions: 4.0 and later.

Supported screen resolutions

The following screen resolutions are supported:

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

Installation of Quick Heal AntiVirus

You can install Quick Heal AntiVirus on the device from Quick Heal Website.

Downloading Quick Heal AntiVirus installer

You can download the installer from the Quick Heal website either from mobile or from a PC.

1. Enter the following URL:

<http://quickheal.co.in/home-users/quick-heal-antivirus-for-android>

2. Click **Download**.

Quick Heal AntiVirus gets downloaded to your device.

If you have downloaded the installer on your PC, then copy the file to Android mobile.

On your device, follow and complete the registration process.

To know how to register the license, see [Registering Quick Heal AntiVirus](#).

Registration, reactivation, and renewal

After installation, you must register Quick Heal AntiVirus to avail of all the features and get technical support facility. You can activate and reactivate Quick Heal AntiVirus on any Android-supported mobile device including.

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

This chapter includes the following sections:

[Registering Quick Heal AntiVirus](#)

[Reactivating Quick Heal AntiVirus](#)

[Renewal of Quick Heal AntiVirus](#)

Registering Quick Heal AntiVirus

You can register Quick Heal AntiVirus in the following way:

Registering licensed version

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

1. Go to the Apps list on the device, and then tap the **Quick Heal AntiVirus** icon. The License Agreement screen is displayed.

The **I Agree to all Terms & Conditions of EULA** check box is selected by default. If you clear this option, you cannot proceed further for registration. To read the full license terms and conditions, tap **EULA**.

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

2. Tap **Agree**. You are redirected to mobile verification screen.



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

3. Enter valid mobile number and tap **Continue**.
Quick Heal will send you an OTP to your mobile number, which you entered recently.
4. In the new screen, enter the OTP and tap **Continue**.
If you have not received the OTP, you can tap **Resend OTP** link and request a new OTP.
In 24 hours, you can request OTP only three times. If you exceed the OTP limitation, you can again request the OTP only after 24 hours.
5. Enter the 20-digit product key. If you have purchased the product online, your product key will be sent to your registered email ID.



If you have not purchased a license, you can buy it by visiting our website. Tap **Buy Now** on the License Activation screen, which navigates you to the Quick Heal website.

6. Tap **Next**. After successful activation, a message with the expiry date of the product is displayed.
7. As soon as the application is activated, a brief demo is displayed.
 - To view the demo, tap **Next**.
 - To skip demo, tap **Skip**.
8. On the Demo screen, the **Allow to collect app Statistics** check box is selected by default. This option helps you to send the analytics data of Quick Heal AntiVirus for research purpose to the server. If you do not want to send the analytics data, clear this option.

After the device is registered with the application, dashboard cards are displayed to take the required action. Tap dashboard card to take the immediate action, or tap the arrow given at the bottom of the Home screen to go to the application.



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

Share registration logs

In case of any issue during the registration of the Quick Heal AntiVirus application, you can share the logs through the available options.

To share the logs, follow these steps:

1. Go to the Registration screen.
2. On the top right of the Registration screen, touch and hold the ? symbol. The Share Logs screen is displayed.
3. Tap **Share Logs**.

Reactivating Quick Heal AntiVirus

Reactivation of Quick Heal AntiVirus enables you to use the product until the end of the liable license period. You may need to reactivate the product if you have removed Quick Heal AntiVirus from the device, or in case you format the device, or you change the mobile device.

Reactivating licensed version

To reactivate the copy of Quick Heal AntiVirus licensed version, follow these steps:

1. Go to the Apps list on the device and tap the **Quick Heal AntiVirus** icon. The License Agreement screen is displayed.

The **I Agree to all Terms & Conditions of EULA** check box is selected by default. If you clear this option, you will not be able to proceed further for registration. To read the full license terms and conditions, tap **EULA**.

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

2. Tap **Agree**. You are redirected to mobile verification screen.



Note:

-
- To activate the product on the devices with Android OS 6.0 and later versions, you must grant the required phone permissions.
-

3. Enter valid mobile number and tap **Continue**.

Quick Heal will send you an OTP to your mobile number.

4. In the new screen, enter the OTP and tap **Continue**.

If you have not received the OTP, you can tap **Resend OTP** link.



Note:

In 24 hours, you can request OTP only three times. If you exceed the OTP limitation, you can again request the OTP only after 24 hours.

5. The product key is automatically retrieved from the data and product is activated.

A message with the expiry date of the product is displayed.

6. As soon as the product is activated, a brief demo is displayed.
 - To view the demo, tap **Next**.
 - To skip demo, tap **Skip**.
7. On the Demo screen, the **Allow to collect app Statistics** check box is selected by default. This option helps you to send the analytics data of Quick Heal AntiVirus for research purpose to the server. If you do not want to send the analytics data, clear this option.

After the device is registered with the application, dashboard cards are displayed to take the required action. Tap dashboard card to take the immediate action, or tap the arrow given at the bottom of the Home screen to go to the application.



Note:

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

Renewal of Quick Heal AntiVirus

You can renew the Quick Heal AntiVirus application in the following ways:

Renewing licensed version

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

To renew the licensed copy of Quick Heal AntiVirus, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap the **Settings** icon, and then tap **About Product**.
4. In the License Information section, tap **Renew**.
5. On the Renew License screen, enter the 20-digit renewal key, and then tap **Next**. The license is successfully renewed.
6. If you do not have a renewal key, you can purchase it by visiting our website. Tap **Buy Now** on the Renew License screen to buy the renewal key by using one of the following ways:

[Renewal through website](#)

[Call us](#)

Renewal through website

You can buy a renewal key and renew the license online. To renew the license through our website, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap the **Settings** icon, and then tap **About Product**.
4. In the License Information section, tap **Renew**.
5. Tap **Buy Now** to use the website to buy the renewal license through the website. You will be redirected to the Buy License screen.
6. Enter the 20-digit product key and then tap **Submit**. You can find the product key in the email sent to your registered email ID.

After renewing the license successfully, you need to update the license information on the device by going to Quick Heal AntiVirus **Dashboard > Settings > About Product > Update**.

Call Us

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

To use Call Us option, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Settings > About Product**.
4. In the License Information section, tap **Call Us**.

Dashboard

Dashboard is the default screen, which appears on the mobile device screen when you open Quick Heal AntiVirus (QHMAV) application. Dashboard is unique and helps to navigate easily to all the components of the application. All the associated features and status are displayed on the screen. All the features of the Quick Heal AntiVirus application are accessible from Dashboard.

Quick Heal AntiVirus Dashboard includes Optimize, Privacy, Secure, and Settings. Tap the required option.

You can find the following options on Dashboard:

[Optimize](#)

[Privacy](#)

[Secure](#)

[Settings](#)

[Dashboard cards](#)

Optimize

The Optimize option helps you to check the device performance, boost the device speed, back up files, monitor battery usage, and manage data plan. Optimize includes the following features: Boost, Battery, Storage, and Data Usage. To know about various features of Optimize, see [Optimize](#).

Privacy

The Privacy option helps you to secure the device from unauthorized users. You can restrict unauthorized users from viewing the contacts and the applications without your consent. You can lock applications and make contacts private. Also, block unwanted numbers and know the applications that access the device permissions. Tap the Privacy option to navigate to the features of Privacy. Privacy on Quick Heal

AntiVirus includes the following features: AppLock, Vault, Block Numbers, and Privacy Advisor. To know about various features of Privacy, see [Privacy](#).

Secure

The Secure option helps to boost the security of the device. It scans for potential threats present on the device. You can enhance the security settings to stop attempts to exploit vulnerabilities. You can scan the device, track the device location, and secure settings. Tap the Secure option to navigate to the features of Secure. You also get the privilege to have safe financial transaction. Secure on Quick Heal AntiVirus, includes the following features: Antivirus, SafePe, Anti-Theft, and Security Advisor. To know about various features of Secure, see [Secure](#).

Settings

The Settings option helps you to configure user details, floating window, provides uninstall protection, set notifications, and secure the device from unauthorized users. Tap the Settings icon to navigate to the settings. Settings on Quick Heal AntiVirus includes the following: Account settings, App settings, Help Center, and About. To know more about settings, see [Settings](#).

Dashboard cards

After the Quick Heal AntiVirus application is registered on the device, few dashboard cards to grant permissions are displayed on the devices with Android OS 6.0 and later versions.

The following cards are displayed:

- **Accessibility permission:** This permission is required to provide real-time protection for your device. Grant this permission to allow Quick Heal AntiVirus protect your phone from security risks and vulnerabilities.
- **App with Usage Access permission:** This permission is required to allow Quick Heal AntiVirus track what other applications you are using and how often. Grant this permission to know about other applications usage and other details.
- **SD card permission:** This permission is required to get access to your device SD card. Grant this permission to ensure the protection of your SD card during scanning and moving data from and to the SD card.
- **Overlay permission:** This permission is required to keep your personal information private and prevent unauthorized access by displaying Quick Heal AntiVirus on top of your phone. Grant this permission to safely lock your apps and secure your block screen by displaying on the top of the device interface.
- **Missing permissions:** These permissions are required to gain access to all the features. Grant this permission to enable the Quick Heal AntiVirus features. Most of the features cannot work without these permissions.

- **Data Saver permission:** This permission is required to keep your app updated. Grant this permission to allow Quick Heal AntiVirus run in data saver mode and keep your device updated.
- **Registration grant permission:** This permission is required to activate the Quick Heal AntiVirus application on your device. Grant this permission to manage your system settings such as brightness, display, etc.

Features

This section is to familiarize you with the features of Quick Heal AntiVirus. Use various features of Quick Heal AntiVirus to secure your device and its crucial data. Quick Heal AntiVirus features are as follows:

[Optimize](#)

[Privacy](#)

[Secure](#)

Optimize

The Optimize option includes: Boost, Battery, Storage, and Data Usage. This option helps you to check the device performance and improve the device speed. You can save the battery power and check the battery status. You can also increase the storage space and set the data plans. You can optimize the device effectively by ending unnecessary processes and browsing history. The Optimize option helps to clear the cached files accumulated by the various applications and clean up the memory.

Configuring Optimize

To configure the features of the Optimize option, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Optimize**. The features of Optimize are displayed.

Following options are available:

[Boost](#)

[Battery](#)

[Storage](#)

[Data Usage](#)

Boost

The Boost option enhances the device performance. It displays the status of the device performance and the RAM available on the device. There are three types of the Boost statuses: Low, Ok, and Good. Each status is represented by a color code.

Status and color codes are as follows:

Speed Level %	Status	Color code
Less than 30%	Low	Red
Greater than 30% and less than 50%	OK	Orange
Greater than 50%	Good	Green

To configure the options of Boost, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Optimize**, and then tap **Boost**. The status of the device performance, the percentage of unutilized RAM, and the other options are displayed.

Following options are available:

[Optimize Now](#)

[Summary](#)

[Auto Optimize](#)

[RAM used by Installed apps](#)

[List of uninstalled apps](#)

Optimize now

Optimizes and improves the device performance manually. The Optimize now option will initiate optimization of the device. It kills all the running applications and then displays the Boost status and percentage of the RAM available.

Manual device optimization

To optimize the device manually, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Optimize**, and then tap **Boost**. The Boost screen is displayed.
4. Tap **Optimize now** to manually start the device optimization process.
5. Tap the **Stop** option to end the optimization process or wait till the optimization process is completed, and then tap **Done**.

Summary

Displays the overall usage of the device RAM. You can view the overall RAM consumption and available RAM on the device.

Viewing usage summary

To view the summary, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Optimize**, and then tap **Boost**. The Boost screen is displayed.
4. Tap **Summary** to view the overall usage of the device RAM.

Auto optimize

Auto optimize improves the device performance automatically. Enable the Auto optimize option to optimize the device automatically at regular intervals up to four times in a day whenever the device speed is low.

Optimizing device automatically

To optimize the device automatically, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Optimize**, and then tap **Boost**. The Boost screen is displayed.
4. Enable **Auto optimize** to optimize the device automatically.



Note:

By default, this option is turned OFF.

RAM used by installed apps

Displays the list of all installed applications and the corresponding usage of the RAM.

To view the RAM used by installed apps, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Optimize**, and then tap **Boost**. The Boost screen is displayed.
4. Tap **RAM used by installed apps** to view RAM usage of individual apps.
 - If you want to uninstall the application that consumes more RAM, select the application, and then tap **Uninstall**.
 - You can also sort the applications by RAM used, Name of App, and Rarely used.

List of uninstalled apps

This list displays the list of all the applications that are uninstalled through the Quick Heal AntiVirus application.

Tap the application to navigate to Google Play to install it again if required.

- Tap **Clear List** to clear the uninstalled applications list.

Responsive Dashboard cards

The Dashboard responsive cards for the Boost option are:

- Dashboard responsive card is displayed to improve the device performance after installing the Quick Heal AntiVirus application.
- Dashboard responsive card is displayed every day to optimize the device at 10 AM, 1 PM, 4 PM, and 7 PM when available RAM is low.
- Dashboard responsive card is displayed if you have already configured auto optimization. The card displays the status of RAM.
- The **Device set to Awesome** card is displayed at 7 AM every day if the **Auto Optimize** option is turned ON.
- An Auto Optimize promotional card is displayed when you tap the **Optimize now** option manually for more than five times after activating the application. This is to configure the Auto Optimize option.
- Dashboard responsive card is displayed to inform the apps, which are respawning on every seventh day after installing the application.
- An Uninstall Heavy apps card is displayed after one month of installing the application. You can uninstall the applications that consume more RAM if required.

Battery

The Battery option helps you to monitor the battery usage of the device. You can kill all the applications that drain the device power. The battery status and the remaining hours for the battery to get drained is displayed. There are five types of the battery statuses: Critical, Low, Ok, Good, and Full. Each status is represented by a color code. Status and color codes are as follows:

Battery Level %	Status	Color code
Less than or equal to 10%	Critical	Red
11-30%	Low	Red
31-60%	OK	Orange
Greater than 60%	Good	Green
100%	Full	Green

The device plays an alarm when the battery of the device reaches the critical level or when the device is fully charged.



Note:

The alarm will not be played when the device is in the vibrate or silent mode.

To monitor and configure the Battery options, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Optimize**, and then tap **Battery**. The Battery screen is displayed.

The following options are available:

[Safe Charging](#)

[Battery Saver](#)

[Boost Now](#)

[Configure Battery Saving Mode](#)

[Auto Saving Mode](#)

Safe Charging

Displays the charging screen on the device. After the Safe Charging option is enabled, the charging screen appears whenever the device is connected to the charger and is locked.



Note:

To display the charging screen on the devices with OS 6.0 and later versions, you must grant permissions.

By default, this option is OFF.

To display the charging screen, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Optimize**, and then tap **Battery**. The Battery screen is displayed.
4. Tap **Safe Charging** to enable the option.

Battery Saver

To avail of all the options of Battery, you must enable Battery Saver. The options of Battery Saver include Boost Now, Configure Battery Saving Mode, and Auto Saving Mode.



Note:

To avail of all the battery features on the devices with OS 6.0 and later versions, you must grant permissions.

To enable Battery Saver, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Optimize**, and then tap **Battery**. The Battery screen is displayed.
4. Tap **Battery Saver**. The following options are enabled:

[Boost Now](#)

[Configure Battery Saving Mode](#)

[Auto Saving Mode](#)

Boost Now

Saves the power of the device manually. It helps to extend the battery life. It disables all the settings that consumes power and kills all the downloaded and system applications.



Note:

The Battery Saver option must be enabled to boost the battery life of the device.

To boost the battery life, follow these steps:

1. Open **Quick Heal AntiVirus**.
-

2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Optimize**, and then tap **Battery**. The Battery screen is displayed.
4. Tap **Boost Now**. The Save More Power screen is displayed.
5. Tap **Save Now** to activate the configured save mode options.

Configure Battery Saving Mode

This option, customizes the battery saving mode settings. The options, which are turned ON will be ignored during the power saving mode.



Note:

-
- In case you have not configured the power mode, default settings are configured.
 - The Battery Saver option must be enabled to configure the battery saving mode options.
-

To customize the battery saving mode settings, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Optimize**, and then tap **Battery**. The Battery screen is displayed.
4. Tap **Configure Battery Saving Mode**. The Configure Battery Saving Mode screen is displayed.
5. Configure the given settings: Brightness level, Wi-Fi, Sync, Bluetooth, Mobile Data, and Screen timeout as required. The options, which are turned ON will be ignored during power saving mode.

In case of the Screen timeout option, select the time from the drop-down options.

Auto Saving Mode

This option saves the power of the device automatically. With this option, you can set the power saving mode automatically when the battery level reaches 30%, 20%, 10%, and Not Set. A notification is displayed when the power saving mode is turned ON.

To enable auto saving mode, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Optimize**, and then tap **Battery**. The Battery screen is displayed.
4. Tap **Auto Saving Mode** to enable it and select the values from the list to activate auto battery saving mode at the selected battery level percentage. If you do not want to save the battery automatically, select **Not Set**.

After activating Auto Saving Mode, a notification about activation of the auto saving power mode is displayed.



Note:

- When you set a power saving mode to be turned ON at 30%, a notification is displayed when the percentage of battery remaining reaches 32%.
- The Battery Saver option must be enabled to configure Auto Saving Mode.

Responsive Dashboard cards

The following are Dashboard responsive cards of the Battery option:

- Good: A green color card along with a tip is displayed when the status is good.
- OK: An orange color card along with a tip is displayed when the status is OK.
- Low: A red color card is displayed with the **Save Power** option when the battery level is low.
- Low: A red color card is displayed when the battery level is low and Auto Battery Saving Mode is turned ON.
- Critical: A red color card is displayed with the **Save Power** option when the battery level is critical. In addition, a card is displayed to set the dark color wallpaper to save the battery.
- An Auto Saving Mode promotional card is displayed when you tap the **Save Power** option five times manually and if the Auto Power Saving Mode option is disabled. This is to configure the Auto Saving Mode option.

Storage

The Storage option helps you to clear the history of the device browser and Chrome. There are three types of the storage statuses: Low, Ok, and Good. Each status is represented by a color code. Status and color codes are as follows:

Storage %	Status	Color code
0-15%	Low	Red
16-50%	OK	Orange
Greater than 50%	Good	Green

To configure the Storage options, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Optimize**, and then tap **Storage**. The Internal Storage screen is displayed.



Note:

To access the features of storage on the devices with OS 6.0 and later versions, you must grant permissions.

The following options are available:

[Summary](#)

[Auto Cleaning](#)

[Clear Browser History](#)

[Move Data from Internal Storage to SD Card](#)

[Move data from SD card to Internal Storage](#)

[Delete Personal Data from Phone](#)

Summary

Displays the available total, internal, and external storage space. You can also view the total storage occupied by the device data and remaining available space.

To view the storage summary, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Optimize**, and then tap **Storage**. The Internal Storage screen is displayed.
4. Tap **Summary**. You can view the storage summary.

Auto Cleaning

Helps to clean the cache automatically.

Tap the **Auto Cleaning** option to clean the device automatically.



Note:

This option is available only for the devices with OS 5.0 and earlier versions.

Clear Browser history

Helps to clear the device browser history. To clear the device browsing history, turn ON the Clear Browser history option. The device browsing history will be cleared whenever cleaning of cache is initiated on the device. You can clear the browsing history automatically when auto cleaning is configured on the device.



-
- By default, this option is turned OFF.
 - Clear Browsing History clears the history of the Chrome and the default browser of the device.
 - This option is not available on the devices with OS 6.0 and later versions.
-

Move data from Internal storage to SD card

Helps to move the data from internal storage to SD card in case the internal memory storage is full. You can move the images, videos, music, and downloads as required.



-
- This option is not available on the devices with OS 4.4 version.
 - To move the data from internal storage to SD card on the devices with Android OS 6.0 and later versions, you must grant permissions.
-

To move the data from internal storage to SD card, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Optimize**, and then tap **Storage**. The Internal + SD Storage screen is displayed.
4. Tap **Move data from Internal Storage to SD card**. The Move Data screen is displayed. It also displays the remaining space in the internal storage.
5. Select the data that you want to move from internal storage to SD card. The data includes images, videos, music, and downloaded files.
6. Tap **Move to SD Card**. After the data is moved successfully, tap **Done**. You will be navigated to the Storage screen.

Move data from SD card to Internal Storage

Helps to move the data from SD card to internal storage in case the SD card is full. You can move the images, videos, music, and downloads as per the requirement.



-
- This option is not available on the devices with OS 4.4 version.
 - To move the data from SD card to internal storage on the devices with Android OS 6.0 and later versions, you must grant permissions.
-

To move the data from SD card to internal storage, follow these steps:

1. Open **Quick Heal AntiVirus**.
-

2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Optimize**, and then tap **Storage**. The Internal Storage screen is displayed.
4. Tap **Move Data from SD Card to Internal Storage**. The Move Data screen is displayed and it also show the remaining memory in external storage.
5. Select the data that you want to move from SD card to internal storage. The data includes images, videos, music, and downloads.
6. Tap **Move to Internal Storage**. After the data is moved successfully, tap **Done**. You will be navigated to the Storage screen.

Delete Personal Data from Phone

Helps to delete the personal data from the device. You can delete contacts, calendar events, messages, SD card (internal and external), and SIM data (contacts and messages). In this case, before deleting the data permanently, it is recommended to ensure that you do not require the data. The process will be continued in the background. While deleting the personal data, you can go back and continue working with the other features of Quick Heal AntiVirus.



Note:

- You cannot delete personal data on the external SD card on the devices with OS 4.4 version.
 - To delete the personal 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 AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Optimize**, and then tap **Storage**. The Internal Storage screen is displayed.
4. Tap **Delete Personal Data from Phone**. The Delete Personal Data from Phone screen is displayed.
5. Select the items that you want to delete. The items include contacts (phone contacts), calendar events, messages (phone messages), SD card (Internal and External), and SIM data (contacts and messages).
6. Tap **Delete**, enter **PIN**, and then tap **OK**.



Note:

- If SIM is not present in the phone, then the SIM Data option will be disabled.
- If Wipe command execution is in progress, then you cannot delete the personal data and vice versa.

Responsive Dashboard cards

Dashboard responsive cards of the Storage option are as follows:

- The Clean Cache card is displayed after installing the application.
- The Clean Cache card is also displayed once in a week if the Auto Clean cache option is turned OFF and if the data size in the cache memory reaches more than 100 MB.
- Auto cleaning of Cache card is also displayed to configure the cleaning of cache automatically.
- Move Photos to SD card is displayed when internal storage space is occupied by 35% of photos.



Note:

To move photos to SD card on the devices with OS 6.0 and later versions, you must grant permissions.

- Move applications to the SD card is displayed when the storage capacity left in the internal storage is less than 35%. You can move the applications from the internal storage to the SD card.



Note:

To move applications to the SD card on the devices with OS 6.0 and later versions, you must grant permissions.

- A Dashboard responsive card is displayed on the fifth day of activating the Quick Heal AntiVirus application to grant permissions if you have not granted the permissions yet.

Data Usage

The **Data Usage** option lets you track and monitor data usage limit. You can set, monitor, and control the data plan as per your requirement. After you set the data plan, you can view the mobile data and available days left. There are four types of statuses: Over Consumed, Ok, Good, and Under Consumed.

Each status is represented by a color code. Status and color codes are as follows:

Data usage %	Status	Color code
0-40%	Under Consumed	Green

Data usage %	Status	Color code
41-80%	OK	Orange
81 -100%	Good	Green
Greater than 100%	Over Consumed	Red
0-40%	Under Consumed	Green



Note:

The Data Usage tracker is turned ON by default.

To configure Data Usage features, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Optimize**, and then tap **Data Usage**. The Data Usage screen is displayed.

The following options are available:

[Tracker](#)

[Summary](#)

[Set Data Plan](#)

Tracker

Helps to track and control the usage of mobile data and Wi-Fi. You can view and set data plan to control the mobile data usage. Tap Enable Tracker to control the mobile data usage.

To enable tracker, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Optimize**, and then tap **Data Usage**. The Data Usage screen is displayed.
4. Tap **Tracker** to enable the Tracker option.



Note:

-
- The Data Usage tracker is turned ON by default.
 - If the Tracker option is disabled, then you will not be able to view the summary of data usage and you cannot set data plan.
-

Summary

You can view your daily average data usage and data used in last seven days. You can also view Day-wise and App-wise data usage breakup.



Note:

If no mobile data is used after the Tracker is turned ON, then no entries will be listed in Day-wise data breakup chart.

Set Data Plan

The Set Data Plan option helps you configure the data usage plan to monitor and track the usage. The data plans of the Quick Heal AntiVirus application include: Monthly Plan and Custom Plan.

Monthly Plan

To set the Monthly Data Plan, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Optimize**, and then tap **Data Usage**. The Data Usage screen is displayed.
4. Tap **Set Data Plan**. The Set Data Plan screen is displayed.
5. In the **Data Plan** list, select **Monthly Plan**. The Monthly plan screen is displayed.
6. Enter the value of your data plan in MB or GB.
7. You can enter up to four digits following with two decimals. For example: xxxx. xx.
8. Select Start Date of every month to track the data usage from the specified date. Select the value the Start Date list.
9. Enter the data value in the Data used till date option if you have used any data before setting the data plan.



Note:

This option will be pre-filled with the value if you have already used mobile data before setting data plan.

10. Select **Notify me when the plan is over** to notify you when the data plan will end.



Note:

The option, Notify me when the plan is over, is enabled by default.

11. Select **Notify me when Daily limit is reached** to get a notification when the daily limit is reached.



Note:

The option, Notify me when Daily limit is reached, is enabled by default.

12. Tap **Save**. After saving the data plan, a card is displayed, which shows the daily limit of the data usage.

13. In case, you want to edit the monthly plan, tap **Edit** to modify the data plan.



Note:

- If the daily limit of the data usage is reached, a prompt is displayed to continue the data usage or to disconnect. If you tap **Continue**, then that message disappears. If you tap **Disconnect**, Mobile Data will be turned OFF. However, if you turn it ON again, the prompt is displayed to continue the data usage or to disconnect until you tap **Continue**.
 - If the Data plan is over, a prompt is displayed to continue or to discontinue the data usage. If you tap **Continue**, the message disappears. If you tap **Disconnect**, Mobile Data will be turned OFF. However, if you turn it ON again, the prompt is displayed to continue or to disconnect the data usage until you tap **Continue**.
 - Note that you will not be able to disconnect the data usage of the devices with OS 4.4 and later versions through Quick Heal AntiVirus. Hence, these users will be navigated to the Device Settings page to disable data usage manually.
-

Custom Plan

To set the customized data plan, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Optimize**, and then tap **Data Usage**. The Data Usage screen is displayed
4. Tap **Set Data Plan**. The Set Data Plan screen is displayed.
5. In the Data Plan list, select Custom Plan. The Custom Plan screen is displayed.
6. Enter the value of your data plan. You can select the value in MB or GB.
7. Enter the Start date and End date from the values given in the list.
8. Enter the Data value in Data used till Date if you have used any data before setting the data plan. This field will be pre-filled with the value if you have already used mobile data before setting data plan.
9. Select **Notify me when the plan is over** to receive notification.



Note:

This option will be pre-filled with the value if you have already used mobile data before setting data plan.

10. Select **Notify me when Daily limit is reached** to get a notification.



Note:

The option, **Notify me when Daily limit is reached**, is enabled by default.

11. Tap **Save**. After setting up the data plan, a card is displayed, which shows the daily limit of the data usage.

12. In case, you want to edit the custom plan, tap **Edit** to modify the data plan.



Note:

-
- If the daily limit of the data usage is reached, a prompt is displayed to continue the data usage or to disconnect. If you tap **Continue**, then that message disappears. If you tap **Disconnect**, Mobile Data will be turned OFF. However, if you turn it ON again, the prompt is displayed to continue the data usage or to disconnect until you tap **Continue**.
 - If the Data plan is over, a prompt is displayed to continue or to disconnect the data usage. If you tap **Continue**, the message disappears. If you tap **Disconnect**, Mobile Data will be turned OFF. However, if you turn it ON again, the prompt is displayed to continue or to disconnect the data usage until you tap **Continue**.
 - Note that you will not be able to disconnect the data usage of the devices with OS 4.4 and later versions through Quick Heal AntiVirus. Hence, these users will be navigated to the Device Settings page to disable data usage manually.
-

Responsive Dashboard card

If a Data plan is not set even after 10 days of installation of the Quick Heal AntiVirus application, then a Dashboard promotional card is displayed to let you know about the Data Usage option and to set your data plan.

Privacy

The Privacy option includes four features: AppLock, Vault, Block Numbers, and Privacy Advisor. This option helps you to secure the device from unauthorized users. You can restrict unauthorized users from viewing the contacts and applications without your consent. You can lock applications, make contacts private, block unwanted numbers, and know the applications that access the device permissions.

To configure the Privacy features, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Privacy**. The privacy features are displayed.

You can configure following features with Privacy option:

[AppLock](#)

[Vault](#)

[Block Numbers](#)

[Privacy Advisor](#)

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 AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Privacy**, and then tap **AppLock**. The Set PIN screen is displayed.
4. Enter New PIN, Re-enter New PIN and then tap **Save**. If you have already set the PIN through the other options, enter PIN, and then tap **Submit**.
5. Grant the permissions required, and then tap **Continue**.
6. The Lock Apps screen, which includes the list of applications, is displayed.
7. Tap the application that you want to lock. After locking the apps, the total count of locked applications is displayed in the parenthesis of the Lock apps screen. You can also search apps by typing the name of the app in the given Search field.

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 AntiVirus application asks you to enter the PIN that you have configured.



Note:

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

To configure the settings of AppLock, tap the **Settings** icon on the top right of the Lock apps screen.

The following settings are available:

[Show prompt to lock newly installed apps](#)

[Scramble keyword](#)

[Intruders](#)

Show prompt to lock newly installed apps

Displays a prompt to lock a newly installed application on the device. 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.

To display the prompt to lock the newly installed application, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Privacy**, and then tap **AppLock**.
4. Enter PIN of the device.

The Lock apps screen is displayed.



Note:

- You must set PIN to access this feature. If you have already set the PIN through the other options, enter PIN, and then tap **Submit**.
 - To show a prompt to lock the new app installed on the devices with OS 6.0 and later versions, you must grant permissions.
-

5. Tap the **Settings** icon on the top right of the Lock apps screen.
6. Tap **Show prompt to lock newly installed apps** to enable the option and to display the prompt when a new application is installed on the device.



Note:

In case the locked application is uninstalled and reinstalled on the device, then the application is locked automatically.

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 on the keyboard. The position of the numbers changes every time the keypad is activated so that only the actual user can see the scrambled digits. By default, Scramble Keyboard is turned OFF.

To enable Scramble Keyboard, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Privacy**, and then tap **AppLock**.
4. Enter PIN of the device. The Lock Apps screen is displayed.
5. Tap the **Settings** icon on the top right of the Lock apps screen.
6. Tap **Scramble Keyboard** to enable the random keypad.

Intruders

This option helps to view all the captured intruder images. The images are captured when an unauthorized person tries to access the locked applications in your absence. In this gallery, you can store up to 10 images. If there are more images, then the old images will be replaced with the new images.

To view intruder images, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Privacy**, and then tap **AppLock**.
4. Enter PIN of the device. The Lock Apps screen is displayed.
5. Tap the **Settings** icon on the upper right of the Lock apps screen.
6. Tap **Intruders** to view the intruder images gallery.



To capture and store intruder images on the devices with OS 6.0 and later versions, you must grant permissions.

Responsive Dashboard cards

The Dashboard responsive cards of the **AppLock** option are:

- After registration is completed, a Dashboard card is displayed that lets the user know about the AppLock feature.
- When an unauthorized user tries to unlock any one of the locked applications by entering incorrect PIN or incorrect fingerprint for two times, an image of that user will be captured

from the front camera of the device. The captured images are displayed on the responsive cards of the application. Maximum five images are displayed and if a new image is captured, then the old image will be replaced with the new image.

Vault

The Vault option helps to maintain a private contacts list. Quick Heal AntiVirus Vault provides Contacts vault. You can make contacts, call logs, and SMS logs to be private or non-private. Contact Vault allows you to secure important call logs and messages, which are received from the private contacts. Vault captures intruder images when an unauthorized user tries to access your contacts.

To access Vault directly from your Home screen, a shortcut is readily available on the Home screen else, you can create a shortcut for Vault on the device Home screen.

To configure Vault, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Privacy**, and then tap **Vault**. The Set PIN screen is displayed.
4. Enter New PIN, Re-enter New PIN and then tap **Save**. If you have already set the PIN through the other options, enter PIN.

The Vault screen is displayed.

 Note:

In case you have forgotten your PIN, tap **Forgot PIN**. The Forgot PIN screen is displayed. A temporary PIN will be sent to your recovery contact.

Access Vault through Fingerprint

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

 Note:

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

The following options are available:

[Contacts Vault](#)

[Intruders](#)

Contacts Vault

To add contacts to Vault that you want to make private and view the list. This list includes the contacts added from call logs, contacts, and numbers added manually.



Note:

- You will not be able to view the private contacts and messages in the normal contacts or messages folder.
- To add contacts and access the features of Vault on the devices with OS 6.0 and later versions, you must grant permissions.

Adding contacts to Vault

To view contacts and add contacts to Contacts Vault, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Privacy**, and then tap **Vault**.
4. Enter PIN. The Vault screen is displayed.
5. Tap **Contacts Vault**. The Add Contacts to Vault screen is displayed. You can add contacts to Vault in the following ways: From Call Logs, From Contacts, and Enter Number.
 - **Plus + sign:** On every screen, after adding a contact the plus + sign is displayed on top of the screen. You can tap the plus + sign and go back to Add Contacts to Vault screen and select the option to add new numbers to the existing list. Select either options to add the contacts.

From Call Logs: This option helps to add a number to Vault from call logs. Select and add the numbers to Vault. After adding a number to Vault, both the past and future call logs and SMS from that number will be made private.

To add the number from call logs to Vault, follow these steps:

- i. In Add Contacts to Vault screen, tap **From Call Logs**. List of call logs is displayed on the From Call Logs screen.
- ii. Select the number from call log that you want to add to Vault, and then tap **Add**.

From Contacts: To add a number to Vault from the device contacts list. Select the contacts that you want to add to Vault. After adding to Vault, the contact will be saved exclusively in the private contact list.

To add contacts from Contacts list to the Vault, follow these steps:

- i. In the Add Contacts to Vault screen, tap **From Contacts**. List of device contacts is displayed on the From Contacts screen.
- ii. Select the contact that you want to add to Vault, and tap **Add**.

Enter Number: To enter a mobile number manually and add to Vault. You can enter any mobile number manually to make them private.

To enter a number manually and add to Vault, follow these steps:

- i. In the Add Contacts to Vault screen, tap **Enter Number**. The **Add Number** pop-up is displayed.
 - ii. Enter the mobile number that you want to make private, and then tap **Add**.
- You can directly call the newly added contact by tapping it in the list and then tapping the **Call this number** option.



Note:

-
- You will not be able to make messages to private on the devices with OS 4.4 and later versions.
 - If you want to restore the private contacts and their data to the device contacts, then give a long tap for a few seconds on the private contact and tap the **Restore** icon.
 - Deleting the private contacts will permanently remove the contact details along with the private data such as call and SMS logs.
-

Removing contacts from vault

- Long press the contact from the list. Delete option is visible. Tap **Delete**.

Intruders

This option helps to view all the intruder images. The images are captured when an unauthorized person tries to access Vault in your absence. In this gallery, you can store up to 10 images. If there are more images, the old images will be replaced with the new images.



Note:

To view and capture intruder images to Vault on the devices with OS 6.0 and later versions, you must grant permissions.

Responsive Dashboard cards

Dashboard responsive cards of the Vault option are:

- Dashboard responsive card is displayed only when an intruder image is captured. This card displays five latest intruder images that were captured.
- A Vault promotional card will be displayed after 8 days of registration to let the user know about Vault and how to configure it.

Block Numbers

The Block Numbers 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 Numbers is turned OFF by default on the devices with OS 6.0 and later versions. To access all the features of Block Numbers on the devices with OS 6.0 and later versions, you must grant permissions.
-

To configure the options of Block Numbers, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Privacy**, and then tap **Block Numbers**. The Block Numbers screen is displayed.
4. Enable **Block Numbers** to configure other options.



Note:

It is mandatory to enable the Block Numbers option to configure the available options.

The following options are available:

[Blocked List](#)

[Block a Custom Series](#)

[Block SMS with Keywords](#)

[Block Unknown International Calls](#)

[Alert on Call Rejection](#)

[Block WAP/ PUSH SMS](#)

[Register with DND](#)

Blocked List

This option helps to add the numbers to the block list to block all the calls and messages from a new number if required. You can also view the list of numbers that you have blocked.

To add and view the blocked list, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Privacy**, and then tap **Block Numbers**. The Block Numbers screen is displayed.
4. Enable Block Numbers, and then tap **Blocked List** to add and view the blocked numbers.
You can add new numbers to the blocked list with the following options: From Phone Logs,

From Contacts, and Enter a Number to Block. You can also view the blocked numbers list and add new numbers to the blocked list by tapping the plus sign (+).

You can block a new number using the following options:

- **From Phone Logs:** You can block a number from phone logs. Select the check box against a call log, and then tap Add.
- **From Contacts:** You can block a number from the device contact list. Select the check box against a contact, and then tap Add.
- **Enter a Number to Block:** To block a number by entering manually. Enter the number, and then select block calls from this number, or block SMS from this number or both, and then tap Add.



Note:

Before you remove an unknown number from the blocked list, you can save the unknown number to your contact list. To add the unknown number to the contact list, tap the cross sign (×) to remove the number and then select the **Add Contact to Phonebook** check box to add the number to the device contacts list.

You can view the call and message history of the blocked numbers by tapping the number. An SMS from the blocked number can be forwarded, copied, deleted, and you can move the SMS to the Inbox if required. Select the SMS and perform the action as per your requirement.

Block a Custom Series

Blocks all the calls and messages from a series of numbers. You can add a number that starts with and ends with the particular series.

To add a new series, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Privacy**, and then tap **Block Numbers**. The Block Numbers screen is displayed. Enable **Block Numbers**, and then tap the **Block a Custom Series** option. The Block a Custom Series screen is displayed.
4. Select Start with or End with as required, and then enter the digits.
5. Select the **Block calls from this Number** option or **Block SMS from this Number** option or both as required.
6. Tap **Add**. After adding a series, you can add new series by tapping the plus sign (+) on the top right of the Block a Custom Series screen.



Note:

- You cannot block Non-numeric senders.
 - You must enter at least three digits to block the custom series.
-

Block SMS with Keywords

Helps to block messages related to a particular keyword.

- Tap **Block SMS with Keywords**, enter the keyword, and then tap **Add**. All the message, which includes such keywords, will be blocked. This is helpful in blocking spams and other harmful messages.
- To remove the keyword, tap the cross sign (**×**), which is available next to the keyword.
- To add new keywords, tap the plus sign (**+**) on the top right of the Block SMS with Keywords screen.



Note:

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

Block Unknown International Calls

Helps to block all unknown international calls. Enable this option to block incoming calls from an International number that is not saved in the phonebook. Enable **Block Unknown International Calls** to block unknown international calls. To view the blocked international calls, go to the **Blocked List** option.

Alert on Call Rejection

Enable this option to get an alert when you reject a call thrice. If you reject an unknown call for three times, an alert is displayed for 20 seconds to add the rejected call to the blocked list.

Block WAP/PUSH SMS

Enable this option to block WAP/PUSH messages.



Note:

Block WAP/PUSH SMS is not supported on the devices with OS 4.4 and later versions.

Register with DND

This option helps to register the number with the National Do Not Call Directory (TRAI) to block commercial or telemarketing calls.

To register with DND, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.

3. Tap **Privacy**, and then tap **Block Numbers**. The Block Numbers screen is displayed.
4. Enable **Block Numbers**, and then tap **Register with DND**. The Register with DND screen is displayed.

Register with DND provides following ways to block the telemarketing calls and SMS:

- **Call to TRAI:** Helps you to dial a call to TRAI. Tap Call to TRAI to register a complaint to TRAI through a phone call.
- **SMS to TRAI:** Helps you to send a message to TRAI to block or allow the telemarketing calls and SMS. Following are the options to send SMS to TRAI:
 - **Block Telemarketing Calls & SMS:** Blocks all commercial calls and messages.
 - **Allow Telemarketing Calls & SMS:** Unblock all the calls and SMS that are previously blocked. Your device will start receiving all the telemarketing calls and SMS.
 - **Block Selective SMS & All Calls:** Helps you to block all the calls, but in case of SMS, you can select categories to stop receiving SMS whenever required. Select the category, tap **Block**, and then tap **Report**.



Note:

In case you want to unblock any category, you must allow all the categories through the **Allow Telemarketing Calls & SMS** option.

- **Complaint To TRAI:** Allows you to report a number from which you receive unwanted calls or SMS even after registering the number with DND. You should report such complaint within three days span of receiving a call or message from that number.



Note:

- Track the DND service status on the number by entering this link on the address bar of the browser: <http://www.nccptrai.gov.in/nccpreistry/search.misc>
- You can de-register your number later from the DND list if required.

This option is not available outside India.

Responsive Dashboard cards

Dashboard responsive cards of the Block Numbers option are:

- Dashboard responsive card is displayed at 9 AM for every 7 days if the Spam SMS count reaches 10 or more. This card helps you to view and delete the Spam messages.
- A promotional responsive card is displayed after deleting the Spam messages, which shows the result of deletion of Spam messages and promotes the **Block SMS with keywords** feature.
- The Activate Call Block Dashboard responsive card is displayed on the devices with OS 6.0 and later versions to enable the Block Numbers option. This card is displayed after

the registration of the Quick Heal AntiVirus application and after a week if the Block Numbers option is not enabled yet.

Privacy Advisor

The Privacy Advisor option helps you to detect the applications that collect your personal information such as user credentials, contacts, social security number, and passwords. You can monitor applications with various permissions such as Cost You Money, Access Your Personal Data, Access to Accounts, Capture Media, Track Your Location, Use Your Networks, Access Your Identity Info, and Request Device Admin. You can also add the applications to the trusted list as per your requirement.

To know about the applications that access the data, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Privacy** and then tap **Privacy Advisor**. The Privacy Advisor screen is displayed.
4. Enable the **Privacy Advisor** option to know the apps that access the personal information.



Note:

If the Privacy Advisor option is disabled, all the permissions will also be disabled.

The permissions available for applications are:

- **Cost You Money:** Applications with this permission can make calls and send messages without your consent. Extra charges can be applied for making calls and sending SMS.
- **Access Your Personal Data:** Applications with this permission may access the Call logs, Contacts, SMS logs, calendar events, and the Profile. Malicious Applications might read the confidential messages or delete them before you even receive them.
- **Access to Accounts:** Applications with this permission may request authentication credentials of your accounts. Such applications may add or remove accounts and delete your passwords.
- **Capture Media:** Applications with this permission may read, edit, share, and delete the pictures, audio, and video files.
- **Track Your Location:** Applications with this permission can track and update the device location to their servers, which may be harmful.
- **Use Your Networks:** Applications with this permission allow network usage in the background.
- **Access Your Identity Info:** Applications with this permission can share your phone's IMEI number, phone number, calendar, and serial number of the phone to their server without your consent.

- Request Device Admin: Applications with this permission may get device admin privileges and manage the device. Such applications might be difficult to uninstall.

Viewing app permissions

To view the applications that access the private details, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Privacy**, and then tap **Privacy Advisor**. The Privacy Advisor screen is displayed.
4. Enable the **Privacy Advisor** option to know the permissions that are accessed by the applications on the device.
5. Tap the permission that you want to view. The applications that have the particular permission(s) are displayed.
6. Tap the application to view the other permissions it can access. All the permissions that application may access are displayed. You can view the other permissions that the application might access by tapping **Other Permissions**.
7. Tap the **Trust** option to add the application to the trusted apps list or tap **Uninstall** option to remove the application from the device if required.

To view the apps added to the trusted list, follow these steps:

- Tap the **Shield** icon on the top right of the Privacy Advisor screen. You can view the apps added to the trusted apps list.
- Tap the application to view the other permissions it can access. All the permissions that the application may access are displayed.
- Tap the **Don't trust** option to remove the application from the trusted apps list else tap the **Uninstall** option to remove the application from the device if required.

Responsive Dashboard cards

The Dashboard responsive cards of the Privacy Advisor option are:

- Dashboard responsive card is displayed to turn ON the Privacy Advisor option if it is turned OFF for 15 days.
- Dashboard responsive card is displayed when you turn ON the Privacy Advisor option or when you install or update high risky apps on the device.

Secure

The Secure option includes: Antivirus, SafePe, Anti-Theft, and Security Advisor. This option helps to check the possible threats present on the device. You can enhance the security settings to stop attempts to exploit vulnerabilities. You can track the device location when it is lost or

theft. You may also get notifications if insecure settings are turned ON. With SafePe, you get the experience of secured online financial transactions.

To configure the Secure features, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Secure**. The Secure options are displayed.

You can configure the following options with Secure:

[Antivirus](#)

[SafePe](#)

[Anti-Theft](#)

[Security Advisor](#)

Antivirus

The Antivirus option helps to scan the device and set security measures against possible vulnerabilities and privacy violation. Scanning of the device gives a clear idea about the security of the device. You can take appropriate actions to enhance the device security. You can view the list of threats detected during the scan. You can also view the application and file threats detected under separate categories. As a precaution, you get the option to scan the app even before you download it.

With Antivirus option, you can also scan the apps before downloading them from the app store.

To secure the device, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Secure**, and then tap **Antivirus**. The Antivirus screen is displayed.

The following actions are available:

[Scan now](#)

[List of Threats](#)

[Schedule Scan](#)

[Background Scan](#)

[On Install App Scan](#)

[Scan App Before Download](#)

[Scan from Cloud](#)

Scan now

Helps you to run a scan on the device. All the downloaded applications are scanned with this scan. You can uninstall or ignore the applications that are virus affected. All the downloaded applications are scanned in this scan.



Note:

- If Background Scan is turned OFF, then the Scan now option will run a full scan on the device.
 - It is recommended to uninstall the threats detected after the scan.
-

To scan the device, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Secure**, and then tap **Antivirus**. The Antivirus screen is displayed.
4. Tap **Scan now** and the scanning will be initiated. The threats will be detected after the scan.

List of Threats

Displays the threats that were detected during the scan. List of Threats is categorized into four types: Unresolved, Resolved, Quarantined, and Vulnerabilities. The following are the list of threats:

[Unresolved](#)

[Resolved](#)

[Quarantined](#)

Unresolved

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

To resolve the threats, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Secure**, and then tap **Antivirus**. The Antivirus screen is displayed.
4. Tap **List of Threats**, and then tap **Unresolved**. The list of unresolved threats is displayed.
5. Tap **Uninstall** to remove the application from the device, and then tap **Ok**.

Resolved

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

Quarantined

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

To restore the files, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Secure**, and then tap **Antivirus**. The Antivirus screen is displayed.
4. Tap **List of Threats**, and then tap **Quarantined**. The list of repaired files is displayed.
5. Select the check box next to the files, and then tap **Restore**. To delete the files, tap **Delete**. Select to delete the Quarantined files after 7 days, 30 days, and 45 days.

Schedule Scan

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

To schedule a scan, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Secure**, and then tap **Antivirus**. The Antivirus screen is displayed.
4. Tap **Schedule Scan**. You can view all the planned scans if you have created any.
5. To schedule a new scan, tap **Schedule New Scan**.
6. In the **Set Schedule Scan** section, set the time and frequency to start the scan automatically. Schedule Scan has four options to set the time and frequency: Scan while charging, Once a day, Once a week, and Once a month.
 - If you select **Scan while charging**, the device will be scanned once in 24 hours while the device is connected to the charger or charging for the first time in a day with the 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.

Background Scan

To run a real-time scan on the device. This option is enabled by default to perform the background scan automatically on the device, whenever an application is downloaded or updated.



Note:

To run background scan on the devices with Android OS 6.0 and later versions, you must grant permission when you enable the Background Scan option.

On Install App Scan

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

Scan App Before Download

Scan App Before Download: Helps to scan the apps on Google Play Store before even you download the apps. It also informs if the app is unsecure and risks behind installing the app.



Note:

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

Scan from Cloud

This option helps you to scan through Cloud. Cloud scanning allows scanning of all the installed applications and .apk files available on the device storage. Enable this option to perform cloud scanning.



Note:

Ensure to check your Internet connectivity before performing cloud scanning.

Responsive Dashboard cards

The Dashboard responsive cards of the Antivirus option are:

- Dashboard responsive card is displayed to remind you to scan the device if Background Scan is disabled.
- Dashboard responsive card is displayed to inform you that the threats detected during background scan are quarantined.
- Dashboard responsive card is displayed if no action is taken on the detected application threats.
- Dashboard responsive card is displayed to inform you to enable Accessibility service for Quick Heal AntiVirus. Dashboard responsive card is displayed to show the result of the vulnerability scan.
- Dashboard responsive card is displayed to run your first scan on the device after activating the Quick Heal AntiVirus application.

SafePe

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

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

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap Secure, and then tap **Antivirus**. The Antivirus screen is displayed.
4. Tap **SafePe**. On SafePe screen, tap toggle bar of SafePe and enable the feature. Following options are enabled:
 - Protected Apps: Displays all the protected apps under SafePe.
 - Manage Apps: Helps you to add apps to the Protected Apps list.
 - Genuine Apps Link: Displays links to download and install the genuine apps.
 - Settings: Helps to check the device environment is free of vulnerabilities before any financial transaction using any app.



Note:

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

Managing and adding 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 AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap Secure, and then tap **Antivirus**. The Antivirus screen is displayed.
4. Tap **SafePe** and then tap **Protected Apps**. The Protected Apps list is displayed.
5. Tap the Manage Apps icon on the bottom of the screen. The Manage Apps screen is displayed.
6. Tap the toggle bar of the app to add it to the Protected list. The app is added to the Protected Apps list.

- In case, you want to remove the app, tap the app toggle bar again. On the confirmation screen, tap **OK**.

Downloading apps through Genuine Apps link

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

To download the genuine apps, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Secure**, and then tap **Antivirus**. The Antivirus screen is displayed.
4. Tap **SafePe** and then tap **Genuine Apps Link**. The links to download and install the genuine app is displayed.
5. Tap the genuine app icon. You are directed to Google Play Store, from where you can download and install the app.

Settings

The SafePe option helps to make a safe financial transaction using the banking/ financial/ ecommerce/ eWallets apps. Thus, it helps to check whether the device environment is free from any malware or unknown vulnerabilities before performing any financial transaction using any app. You can also enable the option. To know more about SafePe, see [SafePe](#).

- **System Scan:** Enable this option to validate the file system and system apps on your device. It also checks for malicious system apps, jar, apk and 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, and safe device environment of device.
- **Network Scan:** Enable this option to validate the connected network and know whether the Wi-Fi connected is secure to do the financial transactions.

Anti-Theft

The **Anti-Theft** option helps you to secure the phone in case the phone is lost or stolen. This feature lets you block the phone when the trusted SIM is changed or whenever the airplane mode is turned ON. An SMS will be sent to the recovery contacts when the SIM is changed. This option helps you to unblock the device if you forget the PIN. You can also capture intruder images when an unauthorized user attempts to enter an incorrect PIN to unblock the anti-theft block screen.

To configure the Anti-Theft settings, follow these steps:

1. Open **Quick Heal AntiVirus**.

2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Secure**, and then tap **Anti-Theft**. The Anti-Theft screen is displayed.

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 AntiVirus application asks you to enter the PIN that you have configured.

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



-
- 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.
-

The following options are available:

[Anti-Theft](#)

[Phone Tracker](#)

[Intruders](#)

[Block phone when the airplane mode is turned ON](#)

[Block phone if a new SIM is inserted, to avoid intrusion](#)

[Notify on SIM change](#)

[Customize your Block Screen](#)

[Recovery Contacts](#)

[List of Trusted SIMs](#)

[Remote Actions](#)

Anti-Theft

Enable the Anti-Theft option to configure the settings. If this feature is disabled, you cannot configure the settings.



The Anti-Theft option is turned OFF by default.

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

1. Open **Quick Heal AntiVirus**.

2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Secure**, and then tap **Anti-Theft**. The Anti-Theft screen is displayed.
4. Tap the **Anti-Theft** option to enable it. The Set PIN screen is displayed.
5. Enter New PIN, Re-enter New PIN and then tap **Save**. If you have already set the PIN through the other options, the Recovery Contacts screen is displayed.
6. Tap **Add from Contacts** to add recovery contacts. You can set up to two recovery contacts. Select the contact from the device contacts or phonebook, and then tap **Add**.



Note:

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

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

Phone Tracker

To locate your phone if lost or stolen. This option simplifies the device tracking. Tapping the **Phone Tracker** option will navigate you to location settings, where you can enable the location settings and the Phone Tracker option. Disabling location settings will disable the Phone Tracker option also.

Intruders

This option helps to view all the captured intruder images. The images are captured when an unauthorized person tries to access the device in your absence. You can store up to ten images. If there are more images, the old images will be replaced with the new images.

Block phone when the airplane mode is turned ON

Enable this feature to block the device as soon as the airplane mode of the device is turned ON. This ensures the security of the device if it is lost or stolen.

Block phone if a new SIM is inserted, to avoid intrusion

Enable this option to block the device as soon as the SIM is changed. This helps you to secure the device as it can be unblocked by an authentic PIN only.

Notify on SIM change

Enable this option to get a notification to the recovery contact numbers on SIM change. This helps you know the reason why the SIM has been changed and what action you need to take.

Customize your Block Screen

To customize the message that appears on the block screen. When the device is blocked, a message and the recovery contact numbers appear on the blocked device screen. A default message is already present on the block screen; however, you can edit the message if required.



Note:

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

Recovery Contacts

You can add up to two recovery contacts with two numbers to each contact, which are displayed on the block screen. These contact numbers will receive messages whenever an SIM is changed or you forgot the PIN.



Note:

Ensure that you have saved the active recovery contact numbers

List of Trusted SIMs

You can create a list of trusted SIM cards. If you use multiple SIM cards and you frequently change the cards, you can enlist all the SIM cards. In this way, the device will not be blocked whenever you change an 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 cards 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.

Remote Actions

To perform actions on the device remotely by sending commands. This helps you locate, trace, and control the device when it is lost or stolen. This might help you to get back the lost device. You can also block the device and wipe your personal data to secure the device.

You can perform following remote actions with this option:

- Trace phone remotely: Traces the geographical location of the lost device. To get the device location, send this command:
TRACE PIN (For example – TRACE XXXX)
- Block phone remotely: Blocks the device remotely if it is lost or stolen. It sends you the location of the device and captured images. To block the device, send this command:

BLOCK PIN (For example – BLOCK XXXX)

- Unblock phone remotely: Helps you to unblock the device if the device is blocked by mistake or you got back your lost or stolen device and want to unblock it, send this command:

UNBLOCK PIN (For example – UNBLOCK XXXX)

- Wipe data remotely: Wipes the data from the lost device remotely. To wipe data, send this command:

WIPE PIN (For example – WIPE XXXX)

- Ring phone remotely: Locates the device by playing a ringtone on it if you think it is in the nearby surroundings. To ring the device, send this command:

RING PIN (For example – RING XXXX)

Unblock your Anti-theft block screen

The Anti-Theft option helps you to secure the phone in case the phone is lost or stolen. In this framework, the device may get blocked due to the various security reasons. Whenever the device gets blocked, you can unblock your screen with the PIN that you had set. In case you forgot the PIN, Quick Heal AntiVirus provides different options to unblock your phone; Get Temporary PIN and Gmail Authentication.

Get Temporary PIN

This option helps you to send a temporary PIN to the recovery contacts to reset your PIN.

To get a temporary PIN, follow these steps:

1. Tap the **Unblock phone** option on the block screen. The Enter PIN screen is displayed.
2. Tap **Forgot PIN?** in case you forgot the PIN. The Forgot PIN screen is displayed.
3. Tap **Get Temporary PIN**. The Get Temporary PIN screen is displayed.
4. Tap **Send**. A temporary PIN is sent to the recovery contact numbers that you have given during the registration.



Note:

Carrier charges may apply to send a message.

Google Authentication

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

To validate your Gmail account, follow these steps:

1. Tap the **Unblock phone** option on the block screen. The Enter PIN screen is displayed.
2. Tap **Forgot PIN?** in case you forgot the PIN. The Forgot PIN screen is displayed. The three options to unblock your phone are displayed.

3. Tap **Google Authentication**. The Google Authentication screen is displayed. In case of no Internet connectivity, the Configure Internet screen is displayed.

To configure the Internet, follow these steps:

- 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.
- iv. After the Internet is connected, check your email address, enter the password of your Gmail account and then tap **Login**.

Responsive Dashboard cards

Dashboard responsive cards of Anti-Theft option are:

- Dashboard responsive card is displayed after eight days of registration if the location settings of the device are turned OFF.
- Dashboard responsive card is displayed to turn ON the Anti-Theft option if turned OFF.

Security Advisor

The Security Advisor option helps to enhance the mobile security. Enable Security Advisor to get an alert if the security settings on your device are low. You can check the possible vulnerabilities present on the device. You can enhance the security settings to stop attempts to exploit vulnerabilities. The Security Advisor option helps to connect to the secured Wi-Fi networks only. A notification will be sent to the device in case the device is connected to an open Wi-Fi network. Turn OFF the Wi-Fi option by tapping the notification.

Security Advisor settings are: Risk Settings and Security Settings. Tap the **Security Advisor** option to enable it.

The following settings are available:

[Risk Settings](#)

[Secure Settings](#)

Risk Settings

The settings that are enabled for a long time and if there might be a chance of a possibility of vulnerabilities, then these insecure settings will be listed under Risk Settings.

Risk Settings include the Secure Now option available next to listed insecure settings. Turn the settings to OFF by tapping the **Secure Now** option. When you tap the **Secure Now** option, you will be redirected to the respective security features where you can configure them.



Note:

- To enable the Quick Heal AntiVirus Anti-Theft setting, which is listed under Risk Settings on the devices with OS 6.0 and later versions, you must grant all the required permissions.
- To enable the Quick Heal AntiVirus Background Scan setting, which is listed under Risk Settings on the devices with OS 6.0 and later versions, you must grant all the required permissions.

Secure Settings

The risk settings that are turned OFF will be listed under Secure Settings.



Note:

These two options can be configured only when the **Security Advisor** option is enabled.

You can configure the following settings on your phone to enhance the 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 the device and its data at risk. It is advisable to turn this option to OFF when not required.
Phone memory encryption	<p>You can encrypt the data on the device. This ensures security by preventing unauthorized access to the data. It is advisable to turn this option to ON to secure your data from unauthorized access.</p> <p> Note:</p> <hr/> <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 if not required.</p> <p> Note:</p> <hr/> <p>The Hotspot and Tethering setting are available only on supported OS and vendors.</p>

Settings	Description
Quick Heal AntiVirus Anti-Theft	Protects the device and its data. With this feature, you can trace, block, wipe data, dial a call, receive a call, capture image, record audio and video if the device is lost. Turn this option to ON to protect from Theft.
Quick Heal AntiVirus Background Scan	Shields the device against various types of threats. Keep this option enabled for security. Turn this option to ON for security.
Screen Lock	If this option is disabled, the personal data may be at risk of misuse. Ensure that one of the screen lock options is set to safeguard the device data. Turn this option to ON to avoid misuse of data.
Unknown App Sources	If any application is installed from a source other than Google Play, then that application might pose a threat to your device. Therefore, it is advisable to turn this option to OFF.
USB Debugging	If USB debugging is enabled, the device is at risk of being hacked and the data can be misused. Turn this option to OFF for security.
Wi-Fi	Communicating through an open or unsecured Wi-Fi network can put the data at risk. It is advisable to connect Wi-Fi only on a secure network. Turn this option to OFF for security.

Settings

The **Settings** section helps you configure the various settings of Quick Heal AntiVirus and secures the device from unauthorized users. You can configure various settings as follows:

[Account Settings](#)

[App Settings](#)

[Help Center](#)

[About](#)

Account Settings

Account Settings help you to configure the settings related to the user account. Account settings include following settings:

[Set PIN](#)

[User Details](#)

Set PIN

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

To set the PIN, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap the **Settings** icon, and then go to **Account Settings**.
4. Tap **Set PIN**.
5. Enter New PIN, Re-Enter new PIN, and then tap **Save**. You have set PIN.

To change the PIN, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap the **Settings** icon, and then go to **Account Settings**.
4. Tap **Change PIN**.
5. Enter Old PIN, New PIN, and Re-Enter New PIN.
6. Tap **Save**.

Responsive Dashboard card

The Set PIN Dashboard card is displayed after activating the Quick Heal AntiVirus application to configure new PIN. This PIN has to set to access the AppLock, Vault, and Anti-Theft features.

User Details

The User Details option lets you edit the profile details. You can edit Username, Email ID, Country, and Mobile Number. To edit user details, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
4. Tap the **Settings** icon, and then go to Account Settings. Tap **User Details**.
5. Edit Username, Email ID, Country, and Mobile Number.



Note:

You can edit Username only once.

6. Tap **Save**.

Responsive Dashboard card

Dashboard responsive card is displayed on the fifth day of registration to update the user details such as Username, Email id, and contact number.

App Settings

App Settings allow you to configure the settings related to the application. App Settings include the following settings:

[Set Notifications](#)

[Uninstall Protection](#)

[Intruder image Capture](#)

[Intruder Gallery](#)

[Quick Settings on Status Bar](#)

[Floating Window](#)

[Application Statistics](#)

[Create Web Account](#)

[News](#)

Set Notifications

The Set Notifications option helps to display notifications of the status of the selected feature. The notifications are displayed in the device notification area.

To set notifications, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap the **Settings** icon, and then go to App Settings.
4. Tap Set Notifications.
5. Tap **Turn ON/OFF all Notifications**, and then select the **feature** to get the notifications of the selected feature.

Uninstall Protection

The Uninstall Protection option secures the Quick Heal AntiVirus application from being removed by any unauthorized user. It is recommended that you always keep this option enabled. In case the device is lost or stolen, no one can remove the application from the device. This will help you to connect with the device to communicate and track the device.

To enable Uninstall Protection, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap the **Settings** icon, and then go to **App Settings**.
4. Tap **Uninstall Protection** option to enable it.



Note:

You must set PIN to access this feature. If you have already set the PIN through the other options, enter PIN, and then tap **Submit**.

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

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

Intruder Image Capture

The Intruder Image Capture option helps to detect if any unauthorized person has accessed your application, locked applications, Vault or tries to unblock the block screen by entering the incorrect PIN. If an incorrect PIN is entered two times to open your application, locked applications or Vault, an image of that user will be captured from the front camera of the device. However, if the device does not have a front camera, no image will be captured.

To enable the Intruder Image Capture option, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap the **Settings** icon, and then go to **App settings**.
4. Tap **Intruder Image Capture** to capture the intruder images.

Intruder Gallery

The Intruder Gallery option lets you view the intruder images. Intruder images are captured when any unauthorized user tries to access the device. If an incorrect PIN is entered two times to unlock the applications or unlock the device, an image of that user will be captured from the front camera of the device. Gallery consists of the intruder images.

To view Intruder Gallery, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap the **Settings** icon, and then go to **App settings**.
4. Enter PIN. All the intruder images are displayed.



Note:

- If your device has Fingerprint sensor, you can use your fingerprint access to view the intruder images.
- Intruder Gallery can store up to ten images.

Quick Setting on Status Bar

Enable the **Quick Settings on Status Bar** option to have a quick access to device settings options. This option includes the following: Quick Heal AntiVirus app, Optimize, Clean Cache, and Scan.

To enable Quick Settings on Status Bar, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap the **Settings** icon, and then go to **App settings**.

4. Tap to enable the Quick Settings on Status Bar option.

Clean Cache

To clean the cache manually. Clean Cache helps to remove the application cache, system cache, and browsing history.

To clean the device cache, follow these steps:

1. Open the **Quick Heal AntiVirus** quick setting notification.
2. Tap the **Clean Cache icon** on the notification. The Clean Cache screen is displayed and cleaning of cache memory will be initiated.



Note:

To clean the cache on the devices with OS 6.0, the user will be redirected to the device Settings screen to clean the cache manually.

Floating Window

The Floating Window option lets you quickly free up the memory. The Floating Window can be viewed on the Home and the Apps list screen. Tapping the Floating icon launches the floating window, which displays Switch ring and App ring along with the Status button.

- **Status button:** Displays the percentage of currently available RAM and tapping it will free up the RAM used by the apps. The color of the ring depends on the status of the device. There are three types of the Boost statuses: Low, Ok, and Good.
 - If the RAM is low, then status ring color changes to red.
 - If the RAM is OK , then status ring color changes to orange.
 - If the RAM is good, then status ring color changes to green.



Note:

Enable the Accessibility Service option for Quick Heal AntiVirus to make Floating window work more effectively. Enabling the Floating window option will force stop the running downloaded applications to free up the memory and to improve the performance of the device.

- **Switch ring:** Lets you toggle options such as Wi-Fi, Bluetooth, Torch Light, Brightness, Sound, Battery, and Clean cache. Touch and hold the setting to redirect you to the particular the Settings screen on your device.
- **App ring:** Displays the running apps, and then tapping the application kills the selected application and boosts the speed of your device.

Enable Floating Window

To enable Floating Window, follow these steps:

1. Open **Quick Heal AntiVirus**.

2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap **Settings**, and then go to **App settings**.
4. Tap **Floating Window** to enable it.

Application Statistics

Quick Heal AntiVirus is installed and used on a vast range of devices. We strive to make our application more and more compatible with all the latest devices. To make our application more competent, we continuously carry out research on our features and applications. Hence, we collect statistics from various sources and one of the sources is the user community itself.

By enabling this option, you allow the app statistics to be shared with our server. However, clear this option if you do not want to share the phone statistics.

To enable Application Statistics, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap the **Settings** icon and then go to **App settings**.
4. Tap to enable the **Application Statistics** option.

News

The News option shows the news related to virus threats, new malware, or any warnings related to digital security. Quick Heal AntiVirus sends the news to you regularly. Latest ten messages are displayed in this section.

Help Center

Quick Heal AntiVirus provides various methods to help you in using the app and resolve the issues. You can view Online Help, read FAQs, and check our contact numbers. Help Center includes the following options:

[Help](#)

[FAQs](#)

[Contact us](#)

Help

The online help of Quick Heal AntiVirus is available on the device after you install Quick Heal AntiVirus. To know about the features and to configure them, you can access the Help. Tap **Help**, you will be able to view the Help file.

FAQs

The FAQs option includes answers to the frequently asked questions (FAQ) related to Quick Heal AntiVirus. To see FAQs, tap **FAQs** and you will be redirected to our website.

Contact Us

You can contact us in the following ways:

[Live chat](#)

[Submit query](#)

[India contact support](#)

[Enable share logs](#)

[Share logs](#)

Live chat

To get spot online technical support or answers to the issues by speaking with our technical experts. Tap **Live Chat** to get live support.

Submit query

To submit a ticket to the experts to resolve any issue.

To submit a query, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap the **Settings** icon.
4. In the Help center section, tap **Contact Us**, and then tap **Submit Query**.
5. Enter the details and select the **I have read important instructions** check box.
6. Tap **Submit**.

India contact support

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.

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

Enable Share logs

Logs include activity logs and information about the detected threats. This option allows you to share logs. To make this option visible, tap the **Contact Us** option 5-7 times.

Share logs

In case of any issue, you can share the logs through the available options.



Note:

Turn ON the **Enable Share Logs** option to share logs.

About

The **About** option provides you the product details. About includes the following options:

[About product](#)

[Uninstall Quick Heal AntiVirus app](#)

[How to use?](#)

About Product

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

To get product details, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap the **Settings** icon.
4. In the About section, tap **About Product**. The Virus Database, Build Version, License Information, and Liabe Validity period are displayed.
5. To update the Virus database, tap **Update**.
6. Tap **Renew** to renew the license. The Renew License screen is displayed.
7. Tap **Extend** to increase the license validity free for two months. You can extend the validity by referring the Quick Heal AntiVirus app to the friends. This button is visible only for one attempt.

Uninstall Quick Heal AntiVirus App

Removing Quick Heal AntiVirus from the device leaves the device insecure to virus threats. However, in case you change the device or you need to format the device, you may need to uninstall Quick Heal AntiVirus.

To uninstall Quick Heal AntiVirus, follow these steps:

1. Open **Quick Heal AntiVirus**.
2. Tap the arrow given at the bottom of the Home screen. Dashboard is displayed.
3. Tap the **Settings** icon.
4. In the About section, tap **Uninstall Quick Heal AntiVirus App**. A confirmation screen appears.
5. Tap **Continue**.
6. Type PIN for authentication, if PIN is not set, the app will directly start the license deactivation process.

First, your license is deactivated and then you are asked to confirm for uninstallation. In case you cancel uninstallation, the product will be deactivated, but will not be removed

from the device. After deactivation, you cannot access the Quick Heal AntiVirus application. To access the Quick Heal AntiVirus application, you must activate it again.

How to use?

This section gives you a brief demo on how to use the Quick Heal AntiVirus application.

We have covered the basics in this section for better understanding of the application.

Index

About	59	Delete Personal Data	21
About Product	59	Downloading Quick Heal Antivirus	2
product key, license expiry date	59	Enable Share Logs	58
Access Anti-Theft through Fingerprint	45	Enter a number to block	34
Access to Accounts	37	Enter Number	32
Account Settings	52	FAQs	57
Alert on Call Rejection	35	Floating Window	56
Android screen resolutions	2	From Call Logs	31
Android Versions	2	From Contacts	31
Anti-Theft	44, 45	Help	57
Antivirus	39	Help Center	57
App Settings	53	How to unblock your Anti-theft block screen?	48
Application Statistics	57	How to use	60
AppLock	27	India Contact Support	58
Auto Battery Saving Mode	17	Intruder gallery	55
Auto Cleaning	19	Intruder Image Capture	55
Auto Optimize	13	List of Threats	40
Background Scan	42	List of trusted SIMs	47
Battery	15	List of Uninstalled Apps	14
Block a Custom Series	34	Live Chat	58
Block all International calls	35	Lock Phone Remotely	48
Block Message from keywords	35	Monthly Plan	24
Block Number	32	Move Data from Internal Storage to SD card	20
Block phone if a new SIM is inserted, to avoid intrusion ..	46	Move Data from SD Card to Internal Storage	20
Block Phone when Airplane mode is turned on	46	News	57
Block WAP/PUSH SMS	35	Notify on SIM change	47
Blocked List	33	Optimize	11
Boost	12	Optimize Device	
Call to TRAI	36	save power, speed up device, manage network	
Capture Media	37	connections	11, 27
Change PIN	52	Optimize Now	12
Clean Cache	56	Personal Data	37
Clear Browser history	19	Phone Tracker	46
Configure Battery Saving Mode	17	Prerequisites	2
Contact US	58	Privacy	26
Contacts Vault	31	Privacy Advisor	37
Cost you Money	37	Quarantined	41
Custom Plan	25	Quick Heal Antivirus	1
Customize the block screen	47	Quick Setting on Status Bar	55
Data Usage	22	RAM used by installed Apps	13

Reactivating Quick Heal Antivirus	5	Share Logs	58
Register Product		Show Charging Screen	15
through Internet and SMS	3	Show prompt to lock newly installed apps.....	28
Register with DND.....	35	SMS to TRAI.....	36
Registering		Spam messages	36
licensed version, free trial	3	Storage	18
Registering licensed version	3	Submit Query	58
Registering Quick Heal Antivirus.....	3	Summary	13, 19, 24
Remote Actions.....	47	Supported Android	
Renewal of Quick Heal Antivirus.....	6	versions, screen resolutions.....	2
Request Device Admin	38	System requirements	2
Resolved	41	Trace phone remotely	47
Responsive Dashboard card.....	26	Track your Location	37
Ring Phone Remotely.....	48	Uninstall Protection.....	54
Risk Settings.....	50	Uninstall Quick Heal Antivirus	59
Scan from Cloud.....	42	Uninstallation Protection	
Scan Now	40	Activate device administrator	54
Schedule Scan	41	Unresolved	40
Scramble Keyboard	29	Use your Networks.....	37
Secure	39	User Details	53
Secure Settings	50	Vault	30
Security Advisor	49	View Intruder images	46
Set Data Plan.....	24	View Intruder Images	29, 32
Set Notifications	54	Wipe Data Remotely	48
Settings	52		

