Quick Heal

Security Simplified

Q Quick Heal Total Security

User Guide

Version 2.5.6

Copyright & License Information

About This Document

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

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

What's New in this Version?

Features & Enhancements
• Mobile data monitoring will be displayed one day delayed on Android OS version 10 • Data usage limit alert will not be displayed on Android OS version 10.

Contents

Chapter

1

Getting started

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

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

Prerequisites

System requirements

Prerequisites

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

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

* Close all open apps before installing Quick Heal Total Security.

System requirements

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

Supported Android Versions

Quick Heal Total Security is compatible with the following versions: Android 4.4 and later versions.

Supported Android Screen Resolutions

The following Android screen resolutions are supported:

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

Downloading and Installing Quick Heal Total Security

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

1. Go to Google Play store.

2. Search for the **Quick Heal Total Security** app.

3. Download and install the Quick Heal Total Security app from Google Play store.

   Quick Heal Total Security is added to the Apps list on your device.

4. To open the application on your device, go to the apps list and tap the **Quick Heal Total Security** icon.

   A license agreement screen appears.

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

   - **Agree to Privacy Policy**: Select this option to protect your personal information from being misused, unauthorized access or disclosure, loss, alteration or destruction.

5. Tap **I Agree**.

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

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

Chapter

2

Registration and Reactivation

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

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

This chapter includes the following sections:

[Registering Quick Heal Total Security](#)

[About Quick Heal RDM](#)

[Reactivating Quick Heal Total Security](#)

Registering Quick Heal Total Security

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

To register Quick Heal Total Security, follow these steps:

1. Go to the Apps list on your device, and then tap the **Quick Heal Total Security** icon.

    The license agreement appears.

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

    - **Agree to Privacy Policy**: Select this option to protect your personal information from being misused, unauthorized access or disclosure, loss, alteration or destruction.

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

    $\boxed{i}$ Note:

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

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

4. Two permissions screens are displayed to auto-configure below features:

- Background Scan

- On install app scan

- Battery saver

- BlockUninstall

- Capture Intuder

- unsecure Wifi

- Privacy Advisor

- Safe Charging

- Security Adviser

- Web Security

- Parental Control

> 📋 Note:
>
> To auto-configure all the above features, make sure that you grant all the required phone permission. If you tap Skip, then you may not be able to auto-configure the features.

After you give permissions and auto-configure the features, On-board screen appears.

On-board Screen

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

Two scan options are displayed:

- **SCAN**: This scan option helps to update the virus database followed with scan. In this scenario, the scan continues irrespective of the success or failure of the virus database update.

- **Scan in the background**: In this option, the virus database update and the scan process will take place in the background.

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

About Quick Heal RDM

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

You can manage the following features through the RDM portal:

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

Features	Description
Security Advisor	Helps to turn ON the Security Advisor settings remotely on the device.

Creating an account with Quick Heal RDM

Before you create an account with the Quick Heal RDM portal, you must activate Quick Heal app on your device with a valid product key. You can create and activate the RDM account via Quick Heal app Settings. To know how to activate Quick Heal app, see [Registering Quick Heal Total Security](#).

Creating and activating RDM via App Settings

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

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

2. Tap the **main menu** > **Settings**. If you have set the PIN, you will be asked to enter the PIN.

3. Tap **General**.

4. The Manage Through Web option is enabled by default**. Tap **Create Web Account** to create the RDM account. You will be navigated to the RDM portal to create your account.

   📘 Note:

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

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

   Fill the required details and create your RDM account.

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

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

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

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

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

Signing up with Quick Heal RDM

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

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

2. In the upper right area, click the **Sign up** button.

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

3. Enter the correct verification code.

   Read the license agreement and privacy policy documents carefully.

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

5. Click **Sign up**.

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

6. Check your email and click the **Activate** button or copy the link in your browser.

   You are redirected to the set password page of the Quick Heal RDM portal.

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

   Your account with the Quick Heal RDM portal is created successfully. Now you can manage your devices through Quick Heal RDM.

Signing up with Quick Heal RDM with Google account

You can create an account with the Quick Heal Remote Device Management (RDM) portal with your existing Google account also.

To sign up with your Google account, follow these steps:

1. Click the **Sign in with Google** button.

2. Enter Username and Password of your existing Google account.

   Read the service agreement and privacy policies carefully.

3. Click **Accept**.

4. On the **Create New Account** page, enter your valid mobile number and product key.

5. Enter the correct verification code.

   Read the license agreement and privacy policy documents carefully.

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

7. Click **Sign Up**.

   You have successfully created an account with the Quick Heal RDM portal. From now, you can log on to your Quick Heal RDM account using your existing Google account and manage your device.

   When you first log on to the Quick Heal RDM, you need to configure the Add Device page. To know how to add a device, see Adding a device to Quick Heal RDM.

Adding a device to Quick Heal RDM

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

To add a device, follow these steps:

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

2. Log on to the Quick Heal RDM portal.

   The Add Device page appears.

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

4. In the **Product Key** text box, enter the product key.

5. Click **Add**.

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

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

   The device is successfully added.

   $\boxed{i}$ Note:

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

Enabling Manage Through Web

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

To enable Manage Through Web, follow these steps:

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

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

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

Reactivating Quick Heal Total Security

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

Reactivating Quick Heal Total Security

To reactivate Quick Heal Total Security, follow these steps:

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

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

- **Agree to Privacy Policy**: Select this option to protect your personal information from being misused, unauthorized access or disclosure, loss, alteration or destruction.

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

   i Note:

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

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

Quick Heal Total Security Dashboard

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

Message Center

Main Menu

Dashboard alerts

Security Shield

Menus

Message Center

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

Main menu

Main menu or global menu is available on the top right of Dashboard. With this menu, you can configure various features for securing your device and data. This section also gives information about the product, view activity and threats logs. Also, get to know more about Quick Heal Total Security with the informative section of HELP: Online Help, FAQs, and Contact Us. You can also provide your valuable feedback to help improve the Quick Heal application.

To know about various features under main menu, see Main menu.

Dashboard alerts of Quick Heal Total Security

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

Security Shield

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

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

To know about various Security Measures, see Security Shield.

Menus

On Dashboard, you can see the following menus:

Menus	Description
Scan	This scan runs a full scan of your device and scans all apps, files, and data in real time and will detect threats and fake apps instantly.
Boost	Helps to check your device performance, increase its speed, and check network usage.
AppLock	Locks your device apps for privacy.
Quick Scan	Runs a scan of all the apps installed on your device.
Parental Control	Helps to restrict inappropriate content for kids when they are online.
Web Security	Provides protection from malicious and fraudulent websites.
SafePe	Helps for safe financial transaction using the banking/ financial/ ecommerce/ eWallet apps.
Battery Saver	Saves power and increase battery life.
Anti-Theft	Tracks and locates your device and secures its data if it is lost or stolen.
Block Calls	Blocks the unwanted calls.
Intruder	Displays the image of the intruder if someone had an unauthorized access to the device.
Privacy Advisor	Helps to detect potentially risky apps of your device.
Security Advisor	Notifies about insecure settings.
Network Monitor	Helps to monitor and control the network data usage.
Data Protection	Helps to backup and restore your data from Cloud. Also, securely delete the personal data.

To know about various features under menus, see Menus on Dashboard.

Chapter

4

Quick Heal Total Security Features

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

Security Shield

Menus on Dashboard

Main menus

Security Shield

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

Increasing security level

To increase the security level, follow these steps:

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

2. Tap **Security Shield.**

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

Security Measures

Security measures include the following options:

Security Measures	Description
Background Scan	Enable Background Scan to scan your device continuously. This helps you to scan all apps, files, and data in real time and will detect threats instantly.
Anti-Theft	Enable Anti-Theft to track and locate your device when it is lost or stolen. If this feature is disabled, the device cannot be tracked.

Battery Saver	Enable Battery Saver to save power. Battery saver mode takes various actions to save power and extend battery life. You can kill all the running apps, stop network usage, and reduce screen brightness to save the power.
Block Uninstallation	The Block Uninstallation option when enabled, blocks an unauthorized user from uninstalling Quick Heal app from your device. In case your device is lost or stolen, you may need to communicate with your device to track or locate it or perform other actions. To communicate successfully, it is important that Quick Heal app is active on your device.
Capture Intruder	Enable Capture Intruder option to capture the image of an intruder on two unsuccessful attempts to unlock the device with wrong PIN.
Network Monitor	Enable the Network Monitor option to monitor and control the data usage. This helps you manage your Internet bandwidth.
Safe Charging	Enable the Safe Charging option to show the current battery status and estimated approximate time to charge whenever the device is connected to the charger.
SafePe	Enable SafePe to make a safe financial transaction using the banking/ financial/ ecommerce/ eWallets apps.
Web Security	Enable Web Security to block infected and fraudulent websites. This protects your device from all the infected websites when you connect to the Internet and keeps you safe from any kind of malware and websites that try to steal your valuable data such as bank details, user credentials, social security information, and passwords.
Parental Control	Enable Parental Control to block inappropriate Web content and keep your kids safe online.
On Install App Scan	Enable the On Install App Scan option to run a scan whenever a new application is installed on the device.
Privacy Advisor	Enable Privacy Advisor and get alerts when your privacy is violated. For example, when you install apps on your device, some apps may use your user credentials, which you may not prefer. Privacy Advisor helps you to detect such apps that may be of potential risk.
Security Advisor	Enable Security Advisor to get notification about unsecure settings on your device. This helps you to enhance your device security.
Wi-Fi Security	Enable Detect Unsecure Wi-Fi to run a scan on the device to detect if you are connected to an unsecure Wi-Fi.

Menus on Dashboard

The menus on Dashboard include the following options:

Scan

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

Note:

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

To scan your device, follow these steps:

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

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

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

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

   View Threats: Displays the detected threats and fake apps. To get full information about the threats detected, see Threat Report.

Boost

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

To increase the device performance:

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

2. On Dashboard, tap **Boost**.

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

AppLock

The AppLock option helps to lock the applications installed on the phone. With AppLock, you can lock applications including 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.

You can unlock the applications with PIN/Pattern or fingerprint.

Locking the app with AppLock

To lock an application through AppLock, follow these steps:

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

2. On Dashboard, tap **AppLock** > enter the PIN.

$\boxed{i}$ Note:

If you are visiting first time, then you have to Set the PIN.

List of applications with lock icon is displayed.

3. Tap the lock icon of the app that you want to lock. The lock icon is highlighted.

You can also configure settings to display a prompt to lock a newly installed app and option for AppLock with PIN or Pattern.

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

Unlocking the app

1. Open Quick Heal Total Security.

2. On Dashboard, tap **AppLock**.

3. To unlock the locked app, in the AppLock screen, tap the active lock icon available in front of that app.

AppLock Settings

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

Show Prompt

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

Configure Show Prompt option

1. Open Quick Heal Total Security.

2. On the dashboard, tap **AppLock**. In AppLock screen, tap **Setting** icon.

3. In AppLock Settings screen, select the **Show Prompt** check box.

   ▪ To stop locking of newly installed apps, clear the Show Prompt check box.

Switch to PIN or Pattern

Quick Heal Total Security provides the options to unlock the apps. You can use PIN or set pattern to unlock the locked application. It provides the following options:

• **Use PIN to unlock**: This option allows you to use the Quick Heal Total Security app's PIN to unlock the locked application.

- **Use Pattern to unlock**: This option can be used to set a pattern and use it to unlock the locked applications.

Configuring PIN or Pattern to unlock the app

1. Open Quick Heal Total Security.

2. On the dashboard, tap **AppLock**. In AppLock screen, tap **Setting** icon.

3. In AppLock Settings screen, tap **Switch to PIN or Pattern**.

   - To unlock the app with PIN, select **Use PIN to unlock**.

     When you select this option, you can use the already set PIN to unlock the apps.

   - To Unlock the app with a pattern, select **Use Pattern to unlock**.

     When you select this option, you are directed to Set Pattern screen.

     i. Select the dots and set the pattern.

     ii. You must redraw the pattern and confirm.

     If you enter 3 to 4 wrong patterns at the time of confirmation, you have to reset the pattern again.

     On successfully setting the pattern, a success message is displayed.

   - When you configure the PIN or pattern, the respective information is displayed under the Switch to PIN or Pattern heading.

Change Pattern

The Change Pattern option is beneficial to set the new pattern to unlock those apps that were locked using AppLock functionality.

Note:

This Change Pattern option is visible when you have selected the **Use Pattern to unlock** option in Switch to PIN or Pattern settings.

To create a strong pattern, you must select at least 4 dots. When you select the dots, the dots are highlighted. Thus, this gives a privilege to skip the dots and create your own strong pattern. After drawing a pattern, you must confirm the pattern. If you try to enter 3-4 wrong patterns, you are informed to reset the pattern.

To change the pattern, follow these steps:

1. Open Quick Heal Total Security.

2. On the dashboard, tap **AppLock**. In AppLock screen, tap **Setting** icon.

3. In AppLock Settings screen, tap **Change Pattern**.

4. In Change Pattern screen, select at least 4 dots to draw a strong pattern.

5. Confirm the pattern. The pattern is set successfully.

Scramble Keyboard

The purpose of this setting is to show random key ordering to enter the PIN on the AppLock screen.

[i] Note:

This option is visible when you have selected the **Use PIN to unlock** option in Switch to PIN or Pattern settings.

The position of the numbers changes every time the keypad is activated, so that only the actual user can see the scrambled digits.

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 Total Security application asks you to enter the PIN that you have configured.

[i] Note:

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

App Lock Screen

When user access any locked app then upon launch, app lock screen is shown to the user and selected AppLock option is visible. In case of PIN, numeric screen is displayed and in case of pattern, pattern screen is displayed.

If Fingerprint is already set, then the user can unlock the app using fingerprint sensor.

Below options are available on AppLock screen:

- **Don't Lock this App**: This option will remove the app from AppLock upon entering correct PIN.
- **Switch to PIN:** This option will change the pattern screen to numeric screen.
- **Lock Option**: This option will take user to AppLock setting screen where user can choose lock options.

Quick Scan

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

Viewing detected threats

To view the detected threats, follow either steps:

- Open **Quick Heal Total Security** > on Dashboard tap **Quick Scan** > tap **View Threats**.
- Open **Quick Heal Total Security** > tap **main menu** > **Threat Report**.

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

Parental Control

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

Configuring Parental Control

To configure Parental Control, follow these steps:

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

2. On Dashboard, tap **Parental Control** to enable it, and then tap **OK**.

    Note:

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

    Following options are available:

    - **Parental Control**: Use this option to disable Parental Control feature by clearing the check box.

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

    - **Allow Access**: Use this option to allow access to certain websites.

Blocking Access

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

To block access to websites, follow these steps:

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

2. On Dashboard, tap **Parental Control** > **Block Access**.

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

3. Under Block Web Categories, select the web categories that you want to block.

4. Tap **Block URLs**, type the website address that you want to block and tap the **plus** (+)sign.

The added web category or the URL gets blocked.

Allowing Access

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

To allow access to certain websites, follow these steps:

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

2. On Dashboard, tap **Parental Control** > **Allow Access**.

3. On the Allow Access screen, tap **Enter URL to allow access** text field and type the website address and then tap the **plus (+)** sign.

> $\boxed{i}$ Note:
>
> - The Parental Control feature provides multi-browser support to block websites.
> - Parental Control may not support any beta versions of the browsers.

Web Security

Web Security blocks infected and fraudulent websites on the browser. It protects your device from all the infected websites when you connect to the Internet and keeps you safe from any kind of malware and websites that try to steal your valuable data such as bank details, user credentials, social security information, and passwords.

Configuring Web Security

To configure Web Security, follow these steps:

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

2. On Dashboard, tap **Web Security.**

3. In the Web Security screen, select the **Web Security** check box to get complete protection from the infected and fraudulent websites.

> $\boxed{i}$ Note:
>
> - To enable Web Security on the device, you must grant permissions.
> - The Web Security feature provides multi-browser support to block websites.
> - Web Security may not support any beta versions of the browsers.

SafePe

The SafePe option helps you to make a safe financial transaction using the banking or financial or ecommerce or eWallets apps. This option helps you to check whether the device environment is free from any malware or unknown vulnerabilities before performing any financial transaction

using any app. This option runs a scan of device root access, device integrity, device environment, file system, and network.

Configuring SafePe

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

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

2. On Dashboard, tap **SafePe**. A confirmation dialog is displayed.

3. Tap **Yes** to enable SafePe. The Protected Apps screen is displayed. Different options are displayed to configure SafePe.

$\boxed{i}$ Note:

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

SafePe Setting

With settings, you can perform system, device, and network scan, and also get alert if the device is at risk.

• System Scan: With this scan, you can validate the file system and system apps on the device and also check for malicious system apps, jar, apk and files.

• Device Scan: Use this option to validate root status, changes in OS, and safe device environment.

• Network Scan: Use this option to check if the connected Wi-Fi is secure for financial transactions.

• Silent SafePe Scan: Set this option to receive an alert when the device is at risk.

Manage Apps

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

Managing apps

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

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

2. On Dashboard, tap **SafePe**. The Protected Apps screen is displayed.

3. Tap **Manage Apps**. The Manage Apps screen is displayed. Here you can add the app or download the apps from genuine apps link.

Adding apps to SafePe via installed apps

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

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

2. On Dashboard, tap **SafePe**. The Protected Apps list is displayed.

3. Tap the **Manage Apps** icon at the bottom of the screen. The Safe list, which includes the installed apps on your device, is displayed.

4. Select the check box of the required app and add to SafePe.

   ▪ In case, you want to remove the app from SafePe, clear the check box next to that app.

Adding apps to SafePe via genuine apps link

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

To download the genuine apps, follow these steps:

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

2. On Dashboard, tap **SafePe**. The Protected Apps screen is displayed.

3. Tap the **Manage Apps** icon at the bottom of the screen.

4. Tap **Genuine Apps** and then tap the app link that you want to download. You will be redirected to the Play store. After installing the apps, the apps are added to the Protected Apps list.

Battery Saver

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

Configuring Battery Saver

To configure Battery Saver, follow these steps:

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

2. On Dashboard, tap **Battery Saver.**

3. Battery Saver screen is displayed where you can configure the settings.

   ▪ You can keep the default settings by tapping the **Keep Default** button.

   Note:

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

4. On the Battery Saver screen, you can configure the following options:

   ▪ **Activate Battery Saver Mode When**: Set the battery level when the Battery Saver mode should start.

   ▪ **Set Screen Brightness to**: Set the screen brightness after Battery Saver mode starts.

- **Set Screen Timeout**: Set the screen timeout after the Battery Saver mode starts.

- **Disable Wi-Fi**: Select this check box to disable Wi-Fi network automatically when Battery Saver mode starts.

- **Disable Bluetooth**: Select this check box to disable Bluetooth network automatically when Battery Saver mode starts.

- **Disable Sync**: Select this check box to disable auto-sync of the device automatically in Battery Saver mode.

Activating Battery Saver mode

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

2. On Dashboard menu, tap **Battery Saver** > **Activate Battery Saver Mode When.**

3. In Set Battery Level screen, tap percentage list and select required option and tap **OK**.

Setting screen brightness

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

2. On Dashboard menu, tap **Battery Saver** > **Set Screen Brightness to**.

3. In Set Screen Brightness screen, on percentage toggle bar, set required percentage and tap **OK**.

Setting Screen timeout

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

2. On Dashboard menu, tap **Battery Saver** > **Set Screen Timeout**.

3. In Set Screen Timeout screen, select the required time from the list and click **OK**.

Anti-Theft

The Anti-Theft options help to secure your device when it is lost or stolen. Anti-Theft provides many useful features such as block or allow access to certain SIM cards, automatically lock the device when untrusted SIM is changed, and track and control device remotely when it is lost or stolen.

To configure anti-theft, your device must be added to the RDM account.

If in any care, in your previous app versions the anti-theft is already configured, but you have not added your device in to the RDM account, then after the upgrade of Quick Heal application, you must configure the anti-theft feature again.

Note:

The Anti-Theft option is turned OFF by default.

Anti-Theft Alarm

Anti-Theft alarm gets triggered when the position of the device or the light effect on the device is changed. Thus, it is helpful to avoid any theft and provides protection from pickpockets. To use the anti-theft alarm feature, you must configure the Anti-theft feature first.

Anti-theft Alarm works on the motion and light sensors. If any of the sensors are not available in the device, then that specific alarm option will not be displayed.

Configuring Anti-Theft and Alarm

1. Open Quick Heal Mobile Security.

2. On Dashboard menu, tap **Anti-Theft.**

3. On the Anti-Theft screen, tap **Activate Anti-Theft**.

4. On Set PIN dialog box, add new PIN and then tap **Submit**.

   i Note:

   If PIN is already set, then you will get Enter PIN dialog box.

5. Enter email ID and password to create RDM account.

6. Tap **Contact** icon. You are redirected to your Contact list, where you can select and add the alternate contact numbers (maximum two alternate contact numbers can be added.)

   i Note:

   To access your contact list on the devices with Android OS 6.0 and later versions, you must grant the required contact permissions.

7. Tap **Register me**. You are redirected to the permissions screen.

8. To activate anti-theft feature, provide the requested permissions such as:

   - Missing Permissions Matter: Tap Grant Permissions to give access to calendar, pictures and record video, access device location, record audio, access photos, media and files.

   - Preserve Your Privacy: Tap Grant Permission to allow Quick Heal application to show things on top of other apps.

   - Activate Do Not Disturb: Grant this permission to use Anti-Theft commands. On Do Not disturb Permission screen, tap the required permissions.

9. Anti-Theft and Alarm features get enabled and three options are displayed:

   - **Take me to Anti-Theft Alarm**: Tap this option to configure Activate Motion Alarm and Activate Pocket Alarm options.

     o **Activate Motion Alarm**: When you tap this option, the timer starts for five seconds and then alarm gets activated. Either you can stop or activate it. After activation, if

the phone receives motion sensors, alarm starts ringing. You can stop it by entering the PIN.

- o **Activate Pocket Alarm**: When you want to use this option, tap this option and activate the alarm. The timer starts. Keep the device in your pocket. If you or someone else remove the device from the pocket, the alarm will trigger.

- o To see the guide and get help on how to activate theft alarm, tap **How to activate Theft alarm**.

- o **Anti-Theft Settings**: Tap this option to make changes to the Anti-Theft settings.

- ▪ **Take me to Settings**: Tap this option to go to Anti-Theft Settings.

- ▪ **Back to Dashboard**: Tap this option to go back to Dashboard.

$\boxed{i}$ Note:

If your device is already added to the RDM account, then your email ID will be shown automatically on the registration screen.

If you already have an RDM account and you want to add the device in the same account, then you should use the same password used for registering the RDM account.

If you are a registered user and already have RDM account, then you will get Login Web Account option on the Anti-Theft settings screen.

Access Anti-Theft through Fingerprint

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

You can also use the Fingerprint access to unblock the Anti-Theft Block screen.

$\boxed{i}$ Note:

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

- In case of the Anti-Theft block screen, intruder images are captured after two unsuccessful Fingerprint attempts.

You can configure the following settings for Anti-theft:

SIM Card Settings

Block on Airplane Mode

Customize Block Screen

Update Alternate Contacts

Create Web Account

SIM Card Settings

The SIM Card Settings option lets you block or allow access to certain SIM cards, configure device to be locked as soon as SIM is changed and create a trusted SIMs list.

To configure SIM Card Settings, follow these steps:

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

2. On Dashboard menu, tap **Anti-Theft**.

3. Ensure if Anti-Theft is enabled. If it is not enabled, tap **Anti-Theft.**

4. In Anti-Theft screen, tap **SIM Card Settings** and configure the following options:

   - **Block on SIM Change**: Enable this option if you want your device to be blocked as soon as untrusted SIM is changed. This helps you to secure your device as it can be unblocked only by an authenticated PIN.

   - **Notify on SIM Change**: Enable this option if you want to get a notification on SIM change. This notification is sent to the alternate contact numbers added to your block screen.

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

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

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

Block on Airplane Mode

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

To configure Block on Airplane Mode, follow these steps:

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

2. On Dashboard menu, tap **Anti-Theft**.

3. Ensure if Anti-Theft is enabled. If it is not enabled, tap **Anti-Theft.**

4. In Anti-Theft screen, select the **Block on Airplane Mode** check box.

Customize Block Screen

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

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

Customizing block screen

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

2. On Dashboard menu, tap **Anti-Theft**.

3. Ensure if Anti-Theft is enabled. If it is not enabled, tap **Anti-Theft.**

4. On Anti-Theft screen, tap **Customize Block Screen**. You can customize the following:

   ▪ Message displayed: By default, a sample message is added.

   ▪ To change the message content, clear the **Use default message** check box. Type in the new message.

   ▪ You can view the alternate contact numbers.

   ▪ To view how the customized block screen looks, tap **View Demo**.

Update Alternate Contacts

With the Update Alternate Contacts option, you can add and update contact numbers to be displayed on the blocked device screen. Ensure that you have saved the active alternate contact numbers. You can add up to two alternate contact numbers that will receive the notification.

Updating alternate contact numbers

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

2. On Dashboard menu, tap **Anti-Theft**.

3. Ensure if Anti-Theft is enabled. If it is not enabled, tap **Anti-Theft.**

4. On Anti-Theft screen, tap **Update Alternate Contacts**.

5. In the new screen, tap **Add from Contacts**.

6. You can search the contact or select the contact and tap **Add Contact**.

   ▪ To remove the alternate contacts, in the Update Alternate Contacts screen, tap the **(X) multiplication** sign available in front of the contact.

Create Web Account

To manage your device remotely in case the device gets lost or is stolen, you can create your Web (Remote Device Management) account. The Web (RDM) account will be beneficial to use different features of mSuite remotely. You can get more information about remotely managed features and how to create RDM account, see [Creating an Account with Quick Heal RDM](#).

Creating Web (RDM) Account

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

2. Access Web account via either option:

   ▪ On Dashboard menu, tap **Anti-Theft** > **Create Web Account.**

   ▪ Tap **main menu** > **Settings** > **General** > **Create Web Account**.

   You are redirected to the Remote Device Management portal.

3. Add in your user name and password and then click **Sign in**.

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

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

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

   For more information, see [Creating and activating RDM via App Settings](#)

Login Web Account

To log on to Remote Device Management portal directly from the application, you can use this option.

If you already have the RDM account, then only this option will be visible, or you will see the Create Web Account option.

Logging on to the Web Account

To log on to the RDM portal directly from the application:

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

2. Log on to RDM portal using either options:

   ▪ On Dashboard menu, tap **Anti-Theft** > **Login Web Account.**

   ▪ Tap **main menu** > **Settings** > **General** > **Login Web Account**.

How to unblock your Anti-theft block screen?

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

Unblock device with Google Authentication

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

To validate your Gmail account, follow these steps:

1. On the block screen, tap **Unblock Screen**. The Enter PIN screen is displayed.

2. In case you forgot the PIN, tap **Forgot PIN?**. The Forgot PIN screen is displayed with two options to unblock your phone.

3. Tap **Google Authentication**. The Google Authentication screen is displayed.

   - In case of no Internet connectivity, the Configure Internet screen is displayed.

4. To configure the Internet, follow these steps:

   i. On the Configure Internet screen, enable Mobile to turn ON mobile date, or enable Wi-Fi to turn ON Wi-Fi.

   ii. If you want to configure the Wi-Fi settings, tap the **Wi-Fi** option. The Configure Wi-Fi screen is displayed.

   iii. Enter **Network SSID**, select **Security** and then tap **Connect**. The Security options include Open, WEP, and WPA_WPA2_PSK. If you select WEP, and WPA_WPA2_PSK security options, then you must enter the password to connect to the Wi-Fi.

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

Unblock device with Remote Device Management

This option informs that you can reset your PIN through the RDM portal.

To reset your PIN through the RDM portal, follow these steps:

1. On the block screen, tap **Unblock Screen**. The Enter PIN screen is displayed.

2. In case you forgot the PIN, tap **Forgot PIN?.** The Forgot PIN screen is displayed.

   The two options to unblock your phone are displayed.

3. Tap **Remote Device Management**. The Remote Device Management screen is displayed.

4. Log on to the RDM portal using the URL provided on the screen.

[i] Note:

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

Block Calls

The Block Calls option helps you to block unwanted calls. With this option, you can easily block unwanted calls from both local and all unknown international numbers. This option can block all commercial calls and also block a number of particular series.

[i] Note:

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

- This feature is not applicable for Android OS version 9 and 10.

Configuring Block Calls

To configure Block Calls, follow these steps:

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

2. To enable Call Block follow either option:

   - On Dashboard menu, tap **Block Calls** > **Yes**.

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

3. The Block Calls option is enabled. Different options to block the calls is displayed.

Blocking unwanted calls

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

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

2. On Dashboard tap **Block Calls**. Different options are displayed:

   - **Block Number**: Use this option to enter the number and block it.

     o Type the number and tap **Add to Blocked Numbers List**.

   - **Contact List**: Use this option to block number from contact list.

     o You can add a contact from the Contact list and tap **Add to Blocked List**.

   - **Custom**: Use this option to block the calls from custom series (Ex: 4000000000). You can also specify whether a contact should begin or end with such series.

     o In the text field, enter 3-20 characters and select the Starting with or Ending with option.

       ℹ Note:

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

   - **Blocked List**: Displays the numbers that were blocked with the help of Block Calls option.

Intruder

The Intruder option displays the image of the intruder who tried to access your device without your permission. Ensure that the Capture Intruder option is enabled in the Settings section. To get more information about intruder, see [Capture Intruder](#).

Privacy Advisor

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

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

Configuring Privacy Advisor

To configure Privacy Advisor, follow these steps:

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

2. To enable Privacy Advisor, use either option:

   - On Dashboard, tap **Privacy Advisor** > **Yes**.

   - Tap Security Shield and in Security Measures screen, select **Privacy Advisor** check box.

     The applications are displayed with the permissions that are assigned.

Viewing app permission

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

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

2. On dashboard, tap **Privacy Advisor**.

3. Tap the application.

   - If you find that an app uses any crucial information, you can uninstall that app by tapping **Uninstall**.

   - If you find the app trustworthy, then you can trust the app by tapping **Trust** and in confirmation screen tap **Yes**. This app will be added to the Trusted Apps List.

Various permissions that an app may use are as follows:

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

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

Privacy Audit Notification

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

Viewing Trusted Apps

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

2. On dashboard, tap **Privacy Advisor.**

3. Tap settings icon on upper-right corner.

   A list of trusted apps is displayed, if any app is marked as trusted.

Security Advisor

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

Configuring Security Advisor

To configure Security Advisor, follow these steps:

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

2. To enable Security Advisor, use either option:

   - On Dashboard, tap **Security Advisor**.

   - Tap Security Shield and in Security Measures screen, select **Security Advisor** check box.

   i Note:

   The Security Advisor option is turned to OFF by default.

To enable Anti-Theft and Antivirus on the devices with OS 6.0 and later versions, you must grant permissions.

3. On the Security Advisor screen, the security settings are displayed under the following categories:

   ▪ Unsecure Settings: This option lists unsecure settings.

   ▪ Secure Settings: This option lists secure settings.

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

Security settings are as follows:

Security Settings	Description
Anti-Theft	Protects your device and its data. This option allows you to trace, block, wipe data, and ring the device if your device is lost.
Bluetooth	Data transfer through Bluetooth might put your device and its data at risk. It is advisable to turn this option to off when not required.
Device Memory Encryption	You can encrypt the data on your device. This ensures security by preventing unauthorized access to your data. It is advisable to turn this option to ON to secure your data from unauthorized access. ℹ️ Note: The Device Memory Encryption setting is available only on supported OS.
Unknown App Sources	If any app is installed from a source other than Google Play, then that app might pose a threat to your device. Therefore, it is advisable that you turn this option to OFF.
USB Debugging	If USB debugging is enabled, your device is at risk of being hacked and your data can be misused. Turn this option to OFF for security.
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.
Background Scan	Shields your device against various types of threats. Keep this option enabled for security.
Hotspot & Tethering	Data shared through Wi-Fi Hotspot, USB and Bluetooth Tethering is at risk to be hacked. To prevent data hacking, turn this option to OFF when not required.

	ⓘ Note:
	The Hotspot and Tethering settings are available only on supported OS and vendors.
Screen Lock	If this option is disabled, your personal data may be at risk of misuse. Ensure that Pattern, PIN, Password or Finger Print screen lock options are set to safeguard the device data.
Wi-Fi Security	Communicating through an open or unsecured Wi-Fi network can put your data at risk. It is advisable to connect Wi-Fi only on a secure network. Turn this option to OFF for security.

Network Monitor

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

Configuring Network Monitor

To configure data usage limit, follow these steps:

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

2. To configure Network Monitor, use either option:

   - On Dashboard menu, tap **Network Monitor**. The Network Consumption Summary is displayed.

   - Tap **main menu** > **Settings** > select **Network Monitor** check box.

3. In Network Consumption Summary screen, you can set data usage limit and view app data usage for an individual app.

Set Data Usage Limit

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

To set the data plan, follow these steps:

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

2. On Dashboard tap **Network Monitor** > **Set Data Usage Limit**.

   The Data Plan screen is displayed.

3. The Data Plan screen shows the following options to be configured.

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

   ⓘ Note:

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

- Billing date: Helps to set the start date of the data plan.

- Set data usage limit: Helps to set the limit of the data usage on your device. Enable the Set data usage limit option to configure the data plan.

- Max data usage limit: Helps to set the maximum limit of the data usage.

- Set data usage warning limits: Helps to receive the notification on reaching the maximum data usage limit.

$\boxed{i}$ Note:

This option is not available for Android version 10.

- Already used data: Helps to view the already used data while setting the data plan.

Data Protection

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

To use Data Protection, follow these steps:

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

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

Backup Data to Cloud

Restore Backup from Cloud

Delete Backup from Cloud

Securely Data Deletion

Backup Data to Cloud

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

$\boxed{i}$ Note:

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

To back up the data, follow these steps:

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

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

3. Tap **Backup Data to Cloud**.

4. On the Backup Data screen, select the data for which you want to take the backup.

   ▪ **Auto-Backup when charging**: To back up your data automatically to the Quick Heal Cloud at scheduled time, you can enable this option and then tap **Save**.

5. Tap **Backup Data**.

Custom Back up

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

*For existing users, after renewal or expiry of the product, this feature will not be available. For new users, backup feature will not be available.

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

1. Go to any third party application. For example: Gallery.

2. Select the media file that you want to backup to cloud, and tap the **Share** option.

3. Select the **Quick Heal** icon to back up the media and then backup is initiated.

Buy more space on cloud

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

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

1. Open Quick Heal Total Security.

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

3. Tap **Backup Data to Cloud**.

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

4. Tap **Buy Space** if you want to buy more space on cloud. The Buy more space on Cloud screen is displayed. The storage options available and the cost of space are displayed.

5. Select the storage options as required, and then tap **Submit**. Enter your details and complete the transaction. You can buy storage capacity using various banking methods. Space will be added to the storage immediately.

Restore Backup from Cloud

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

*New users will not be able to use this feature. Existing users will not be able to use this feature after renewal or expiry.

i Note:

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

To restore your data, follow these steps:

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

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

3. Tap **Restore Backup from Cloud**.

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

4. Tap **Restore**.

   i Note:

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

Delete Backup from Cloud

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

To delete the data, follow these steps:

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

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

3. Tap **Delete Backup from Cloud**.

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

4. Tap **Delete**.

Securely Data Deletion

The Securely Data Deletion option lets you delete personal data from the device. However, before deleting the data, be sure that you do not require it as it will be deleted permanently.

i Note:

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

To delete the data, follow these steps:

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

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

3. Tap **Securely Data Deletion**.

Select the data that you want to delete.

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

[i] Note:

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

4. Tap **Delete**.

Main menus

Main menu or global menu includes the following:

Home

Settings

About Product

Buy Premium or Extend Premium

Logs

Help

Home

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

Settings

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

To access Settings, follow these steps:

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

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

3. Enter your PIN**.** The Settings screen appears.

About Product

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

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

Areas	Details	Buttons & Icons
Quick Heal Total Security product details	Product name & Version	• Update: Helps to update the virus database and license subscription details. • Share: Helps to share the Quick Heal application via various methods.
License Information	Product key & License expiry date	• **Buy Premium**: Helps to buy premium to gain full access to all the features. • **User Details**: Helps to update your details such as Username, Email ID and Mobile Number.

		ℹ️ You can verify or update your mobile number only once. **Feature Purchase**: Shows information about individual features that are purchased and their expiry.
Legal Information	Copyright of the product	Helps to know the license information of the application.

Buy Premium or Extend Premium

You will view either options depending on the purchase.

- **Buy Premium**: To have a new purchase, you will view Buy Premium.

- **Extend Premium**: If you have already bought the app, you will view Extend Premium.

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

Individual Feature Purchase

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

To purchase premium, follow these steps:

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

   Dashboard is displayed.

2. Tap main menu and then tap **Buy Premium** or **Extend Premium**.
   - If you want to purchase the premium features, then only Buy Premium option is displayed.

   - If you already have premium subscription, then Extend Premium option is displayed.

   The Premium Purchase screen is displayed.

3. If you want to buy the premium features, then in Features section, select the required options:
   - **SafePe Feature**: Select this option if you want to purchase only SafePe feature.

   - **Parental Control Feature**: Select this option if you want to purchase only Parental Control feature.

   - **All Premium Feature**: Select this option if you want to buy all the premium features of Quick Heal Total Security.

4. If you want to extend your premium subscription, then in Purchase Options section, select the mode of purchase:
   - **From Google**: Select this option if you want to purchase through Google Play store.

▪ **Enter Product Key**: Select this option if you have already purchased a product key.

> [i] Note:
>
> SafePe and Parental Control features cannot be purchased with Enter Product Key option.

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

Logs

Logs include activity logs and information about the detected threats.

Activity Log

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

Threat Report

This option helps to check the status of the infected files and apps. You can take an appropriate action on an infected app or even restore the quarantined files, which you think are useful to you. The detected threats are categorized into four types: Resolved, Not Resolved, Quarantined, and Vulnerabilities. The following are the detected threat types:

[Resolved](#)

[Not Resolved](#)

[Quarantined](#)

[Vulnerabilities](#)

Resolved

The Resolved option displays the list of resolved applications. After you resolve the threats from Not Resolved type list, the threats are displayed in the Resolved type list. You can clear the list by tapping the **Clear** option.

To view the resolved threats, follow these steps:

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

2. Tap **main menu** > **Threat Report**. The Threat Report screen is displayed.

3. In the View list, tap **Resolved**. The list of resolved threats is displayed.

Not Resolved

The Not Resolved option displays the list of unresolved, fake, harmful application threats detected during the scan. You can view the count of unresolved threats. You have to take an action to resolve the threats.

To view the unresolved threats, follow these steps:

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

2. Tap **main menu** > **Threat Report**. The Threat Report screen is displayed.

3. In the View list, tap **Not Resolved**. The list of unresolved threats is displayed.

   - To remove the application from the device, tap **Uninstall** > **OK**.

   - To ignore, tap **Skip**.

Quarantined

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

To restore the files, follow these steps:

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

2. Tap **main menu** > **Threat Report**. The Threat Report screen is displayed.

3. In the View list, tap **Quarantined**. The list of Quarantined files is displayed.

   - To restore the files, select the check box next to the files, and then tap **Restore**.

   - To delete the files, tap **Delete**.

Note:

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

Vulnerabilities

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

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

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

1. Open Quick Heal Total Security.

2. Tap **main menu** > **Threat Report**. The Threat Report screen is displayed.

3. In the View list, tap **Vulnerabilities**. The list of vulnerable threats is displayed.

   - Trust: Tap the Trust option to make the vulnerable app or file as trusted entity.

   - Uninstall: Use this option to uninstall any application.

   - Delete: Use this option to remove the files from the device.

i Note:

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

Help

Quick Heal provides various options to assist you and resolve your issues.

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

Chapter

5

Settings

The Settings menu include the following options:

General

Scan

Device Privacy

Optimize

SafePe

Network Monitor

Backup Data

Safe Charging

Wi-Fi Security

General

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

Change PIN

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

To set the PIN, follow these steps:

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

2. Tap **main menu** > **Settings** > **General** > **Change PIN**.

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

To change the PIN, follow these steps:

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

2. Tap **main menu** > **Settings** > **General** > **Change PIN**.

3. Tap **Submit**.

Track Activity Log

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

To configure Activity Log, follow these steps:

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

2. Tap **main menu** > **Settings** > **General** > **Track Activity Log**.

3. In Track Activity Log for dialog, select one of the following option to track the logs for; 7 days or 30 days 45 days.

App Notification

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

To enable App Notification, follow these steps:

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

2. Tap **main menu** > **Settings** > **General.**

3. Select the **App Notification** check box to enable notifications.

Quick Settings Notification

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

To enable Quick Setting Notification, follow these steps:

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

2. Tap **main menu** > **Settings** > **General.**

3. Select the **Quick Settings Notification** check box to enable it.

Manage Through Web

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

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

To enable Manage Through Web, follow these steps:

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

2. Tap **main menu** > **Settings** > **General.**

3. Select the **Manage Through Web** check box to enable it.

To know different features of Quick Heal RDM, see [About Quick Heal RDM](#) (Quick Heal RDM).

Create Web Account

With this option, you can create the account on the Quick Heal RDM portal. This option is enabled only if the Manage Through Web option is enabled.

To create web account, follow these steps:

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

2. Tap **main menu** > **Settings** > **General**.

3. Tap **Create Web Account**. You are directed to the RDM web portal where you can create your account.

Login Web Account

If you already have the RDM account, then Login Web Account option will be visible. For more details, see [Login Web Account](#).

News Notification

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

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

To enable News Notification, follow these steps:

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

2. Tap **main menu** > **Settings** > **General**.

3. Select the **News Notification** check box to enable it.

Keylogger Notifications

Keylogger is a malicious app which records your keyboard stroke and can be used as a phishing application. Usually such apps are not detected unless they perform any malicious activity in the background.

When Quick Heal Total Security detects such app, then you can uninstall or ignore the keylogger app. If you ignore, it will show in your message center.

Application Statistics

Quick Heal is installed and used on a vast range of devices including mobile, tablet, and other handheld SIM or SIM-less devices. We strive to make our app more and more compatible with all the latest devices. To make our app more competent, we continuously carry out research on our features and apps. To do this, we collect statistics from various sources and one of the sources is the user community itself.

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

To enable Application Statistics, follow these steps:

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

2. Tap **main menu** > **Settings** > **General.**

3. Select the **Application Statistics** check box to enable it.

Block Uninstallation

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

To enable Block Uninstallation, follow these steps:

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

2. Tap **main menu** > **Settings** > **General**.

3. Select the **Block Uninstallation** check box to enable it.

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

4. On confirmation dialog, tap **OK**.

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

Capture Intruder

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

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

To enable Capture Intruder, follow these steps:

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

2. Tap **main menu** > **Settings** > **General.**

3. Select the **Capture Intruder** check box to enable it.

Scan

The Scan option lets you configure various scan options.

To set scan, follow these steps:

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

2. Tap **main menu** > **Settings** > **Scan** and set different scan options.

Background Scan

Helps you to scan your device in real time. With this option, all apps, files, or folders that you access are scanned. If any threat or fake app is detected, the repair action is taken immediately.

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

On Install App Scan

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

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

Scan App Before Download

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

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

Silent Scan app before download

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

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

Scan from Cloud

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

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

  Note:

  Ensure to check your Internet connectivity before performing Cloud scanning.

Vulnerability Scan

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

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

Schedule Scan

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

Note:

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

To create a scan schedule, follow these steps:

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

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

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

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

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

   Time & Frequency include the options such as Scan while charging, Once a day, Once a week, and Once a month.
   - You can set only one type of frequency.
   - If Scan while charging is selected then your device is scanned once in 24 hours while charging with battery level at least 50% or more.
   - If you select **Once a day**, specify the time.
   - If you select **Once a week**, specify day and time.
   - If you select **Once a month**, specify date and time.

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

Delete Quarantined Files After

Helps you to set a period after which all the quarantined files will be removed. The period includes 7 Days, 30 Days, and 45 Days.

Note:

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

Device Privacy

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

Configuring Device Privacy

To configure Device Privacy , follow these steps:

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

Call Filter

To filter calls with different parameters, follow these steps:

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

2. Tap **main menu** > **Settings** > **Device Privacy**.

3. Select the required option:

   - Block Calls: Select this option to configure Block Calls option and to block unwanted calls. You must enable this option to access other options on the screen.

   - Notifications: Select this option to receive notifications if any call is blocked.

   - International Calls: Select this option if you want to block all the unknow international calls.

Optimize

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

To configure the Optimize option, follow these steps:

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

2. Tap **main menu** > **Settings** > **Optimize**. The Optimize screen is displayed.

3. Optimize includes the following options:

Battery Saver

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

To know about complete Battery Saver options, see Battery Saver.

Auto Boost

The Auto Boost option allows you to increase the device speed.

To increase device performance, follow these steps:

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

2. Tap **main menu** > **Settings** > **Optimize.**

3. In Optimize screen, select **Auto Boost** check box.

Backup Data

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

To enable Backup, follow these steps:

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

2. Tap the **main menu** > **Settings** > **Backup Data.**

3. Configure the following settings:

   - **Auto-Backup**: Enable this option to take the backup automatically when charging. If you enable this option, the succeeding options under Select Data to Backup get active.

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

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

4. Tap **Save**.

SafePe

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

To enable SafePe, follow these steps:

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

2. Tap the **main menu** > **Settings.**

3. Select the **SafePe** check box**.**

You can configure the following settings:

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

     Note:

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

- Device Scan: Enable this option to validate the root status, changes in OS other than manufacturer changes, & safe device environment of device.

- Network Scan: Enable this option to validate the connected network and know whether the Wi-Fi connected is secure to do the financial transactions.

- Silent SafePe Scan: Enable this option to be notified if the device is not secure at the time of any transaction. You will not receive alert for protected apps if the device is secure.

Network Monitor

This setting helps to configure Network Monitor and Data Plan.

[i] Note:

The mobile data monitoring will be delayed by one day on Android version 10.

Configuring Network Monitor

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

To enable Network Monitor, follow these steps:

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

2. Tap **main menu** > **Settings**.

3. Select the **Network Monitor** check box to configure Mobile Network.

[i] Note:

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

Data Plan

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

Safe Charging

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

To enable Safe Charging, follow these steps:

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

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

3. Select the **Safe Charging** check box to display the charging screen.

[i] Note:

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

Wi-Fi Security

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

Detecting unsecure Wi-Fi

To enable Wi-Fi Security, follow these steps:

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

2. Tap **main menu** > **Settings.**

3. Select the **Wi-Fi Security** check box to inform you about the unsecure Wi-Fi.

Chapter

6

Help

The Help option lets you read FAQs, check our contact numbers, and uninstall Quick Heal if required. You can also provide your valuable feedback and contribute to make our application more efficient.

To view Help, follow these steps:

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

2. Tap the **main menu**.

3. In the Help section, tap either of the following options:

   - Online Help

   - FAQ

   - Contact Us

   - Uninstall Quick Heal

Feedback

The user must provide their valuable feedback to enhance the Quick Heal application. Thus, in three days after activation the user receives a form to provide the feedback. In case, if the user has already provided the feedback before the third day, this feedback form will not be generated.

You receive feedback form in two scenarios:

- Uninstall Quick Heal: When you use the Uninstall Quick Heal option from the Main Menu, the feedback form is displayed. The user is directed to the Device Administrator screen to disable the Quick Heal application.

- Directly uninstall: When the user taps and holds the Quick Heal icon to uninstall the app, and the Device Administrator is enabled then also the user is directed to the feedback form.

To give your feedback:

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

2. Tap **Main Menu** > **Feedback**.

[i] Note:

- When you first activate or upgrade the Quick Heal application, in three days, you receive a feedback form to give your feedback on overall app experience.

- If in case, within three days, you yourself go to Main Menu and give the feedback about the application, then you will not receive the feedback form again.

3. Select different smileys to express your feedback.

- For Bad and Okay smiley, you have to provide specific reasons why you are unhappy with the application. Tap **Submit**.

- For Good and Best expression, tap **Submit**. You are requested to go to Google Play Store and rate the application.

Online Help

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

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

2. Tap **main menu** > **Online Help**.

- You are redirected to the Help file.

FAQs

Includes answers to the frequently asked questions (FAQ) related to Quick Heal Total Security.

- Open **Quick Heal Total Security** > tap **main menu** > **FAQs**.

You are redirected to FAQs.

Contact Us

Includes various support facilities:

Live Chat

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

Web Support

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

Support Center

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

Enable Debug Logs

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

Note:

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

Uninstall Quick Heal

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

To uninstall Quick Heal Total Security, follow these steps:

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

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

   A confirmation screen appears.

3. Tap **OK**.

4. Type your PIN for authentication and tap **Submit**. If PIN is not set, the app will directly start the license deactivation process.

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

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

Index