Quick Heal

Security Simplified

Quick Heal Mobile Security
Quick Heal Total Security

User Guide

Version 3.1

Copyright & License Information

License Terms

Installation and usage of Quick Heal antivirus security for mobile is subject to user's unconditional acceptance of the Quick Heal end-user license terms and conditions.

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

Documentation Convention

This user guide is applicable to both Quick Heal Mobile Security and Quick Heal Total Security.

What's New in this Version?

Features & Enhancements
• Web Security feature is available in free variant of Mobile Security. • Integration of latest Google Android SKD v31. • User Onboarding and Permission flow has been enhanced. • Ads frequency has been increased in free variant of Mobile Security.

Contents

1. Getting started

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

System requirements

You can install Quick Heal Mobile Security on any of the following Android-supported mobile devices.

Supported Android Versions

- Android 5.0 and later versions.

Supported Android Screen Resolutions

- Supports all Android screens.

Downloading and Installing Quick Heal Mobile Security

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

1. Go to the Google Play store.

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

3. Download and install the **Quick Heal Mobile Security** app.

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

Registering Quick Heal Mobile Security

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

To register Quick Heal Mobile Security, follow these steps.

1. Go to the Apps list on your device and open the **Quick Heal Mobile Security** app.

    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 activation screen appears.

3. On the activation screen, tap **Grant Access**.

4. Allow all the permissions required.

5. Select an email address with which you want to activate the antivirus product.

6. On the installation successful screen, the following options appear.

   ▪ I DON'T HAVE PRODUCT KEY: Select this option if you do not have any product key. Quick Heal Mobile Security will be activated successfully. This version is free and has limited number of features.

   ▪ I HAVE PRODUCT KEY: Select this option, if you have a product key with you. Quick Heal Total Security will be activated successfully with all premium features.

   BUY PREMIUM: Select this option to buy any of the premium features.

Note: If any permission is required, allow all the required permissions.

Dashboard

Dashboard is the main area that appears when you open the application.

Scan

This quick scan allows you to scan the device and set security measures against possible vulnerabilities and privacy violation. It also detects the fake apps and anti-keylogger malware installed on your device that may steal information and confidential data. If any threat is detected, you can take appropriate action to fix it.

Note: Detection of fake apps and anti-keylogger is available in Quick Heal Total Security.

To scan your device, follow these steps.

1. Open **Quick Heal Mobile Security**.

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

   While scanning, you can take any of these actions.

   ▪ **Stop Scan**: To stop scan, tap **Stop Scan**.

Message notification

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 the latest news related to the digital security.

2. Features

This section includes the following features.

[Full Scan](#)

[Phone Boost](#)

[App Lock](#)

[Anti-Theft](#)

[SafePe](#)

[Parental Control](#)

[Data Breach Alert](#)

[Intruder](#)

[Web Security](#)

[Pocket Alarm](#)

[Motion Alarm](#)

[Wi-Fi Security](#)

[Privacy Advisor](#)

[Security Advisor](#)

[Secure Delete](#)

[Call Blocker](#)

[Safe Charging](#)

[Battery Saver](#)

[Network Monitor](#)

Full Scan

Full Scan helps to scan the full device and set security measures against possible vulnerabilities and privacy violation. It also detects the fake apps and anti-keylogger malware installed on your phone that may steal information and confidential data. If any threat is detected, you can take appropriate action to fix it.

Note: Detection of fake apps and anti-keylogger is available in Quick Heal Total Security.

To scan your device, follow these steps.

1. Open **Quick Heal Mobile Security**.

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

   Full scan of your device starts. Ensure that you have granted permission to enable
   scanning. You can view two options:

   Stop Scan: To stop scan, tap **Stop Scan**.

   Scan in the background: Scan runs in the background allowing to use the mobile app.

   If any threat is detected, you can take appropriate action to fix it. To get full information
   about the threats detected, see Threats Report.

   However, the Scan in the background option is available only in Quick Heal Total Security.

Phone Boost

With Phone Boost, you can optimize your device and improve its performance. Phone
Boost kills all the running apps, clears the app cache files, obsolete APKs, Junk files, and
thumbnail images to free hard disk space.

To increase the device performance:

1. Open **Quick Heal Mobile Security**.

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

App Lock

This option helps to lock the applications installed on the phone. 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 App Lock

To lock an application through App Lock, follow these steps:

1. Open **Quick Heal Mobile Security**.

2. On Dashboard, tap **App Lock** and then enter the PIN.

   Note: If you are visiting for the first time, you must 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 App Lock 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 Mobile Security**.

2. On Dashboard, tap **App Lock**.

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

App Lock Settings

The App Lock option helps to lock the applications installed on the device. In Settings section, App Lock 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 Mobile Security**.

2. On Dashboard, tap **App Lock**. In App Lock screen, tap **Setting** icon.

3. In App Lock 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 Mobile 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 Mobile 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 Mobile Security**.

2. On Dashboard, tap **App Lock**. In App Lock screen, tap **Setting** icon.

3. In App Lock 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 App Lock 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.

Changing Pattern

To change the pattern, follow these steps:

1. Open **Quick Heal Mobile Security**.

2. On Dashboard, tap **App Lock**. In App Lock screen, tap **Setting** icon.

3. In App Lock 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 App Lock screen.

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.

App Lock through Fingerprint

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

Note: The Fingerprint option is supported only on the devices with 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 App Lock 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 App Lock screen:

- **Don't Lock this App**: This option will remove the app from App Lock 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 App Lock setting screen where user can choose lock options.

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.

Note: Anti-Theft is a premium feature and is available in Quick Heal Total Security.

Configuring Anti-Theft

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

1. Open **Quick Heal Mobile Security**.

2. On Dashboard, tap **Anti-Theft**. On the Anti-Theft Registration screen, tap **Activate Anti-Theft**.

   The Fingerprint Unlock option appears. You can set the fingerprint to access Anti-Theft. Alternatively, you can set PIN also.

3. Set the PIN and configure other settings. Tap **Register me**.

4. Grant permissions to enable Anti-Theft.

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

Access Anti-Theft through Fingerprint

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

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

Note:

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

You can configure the following settings for Anti-theft.

SIM Card Settings

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

To configure SIM Card Settings, follow these steps:

1. Open **Quick Heal Mobile Security**.

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

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

   - **Trusted SIM Cards**: You can create a list of 50 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 when you turn on Airplane or flight mode of the device. This ensures security to your device if it is lost or stolen.

To configure Block on Airplane Mode, follow these steps:

1. Open **Quick Heal Mobile Security**.

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

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

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

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

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

3. Ensure if Anti-Theft is enabled. If it is not enabled, tap **Activate 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 an account with [Remote Device Management](#) (RDM). The RDM account will be beneficial to use different features of mSuite remotely.

Creating Web (RDM) Account

1. Open **Quick Heal Mobile Security**.

2. Access Web account via either option:

   - On Dashboard, 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**.

Logging on to the RDM account

If you already have the RDM account, only then this option will be visible, else 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 Mobile Security**.

2. The Setting menu > 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.

SafePe

The SafePe option helps you to make a safe financial transaction using the banking, financial, 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 the device root access, device integrity, device environment, file system, and network.

Note: SafePe is a premium feature that you can buy as an individual feature and is also available in Quick Heal Total Security.

Configuring SafePe

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

1. Open **Quick Heal Mobile Security**.

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

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

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.

• Risky Device Alert: 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 Mobile Security**.

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

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

Adding apps to SafePe via installed apps

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

1. Open **Quick Heal Mobile Security**.

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

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

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

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

Adding apps to SafePe via genuine apps link

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

To download the genuine apps, follow these steps:

1. Open **Quick Heal Mobile Security**.

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

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

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

Parental Control

You can block infected and fraudulent websites and apps with the help of the 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, you can block unwanted websites and apps that may be harmful to your children.

Note: Parental Control is a premium feature that you can buy as an individual feature and is also available in Quick Heal Total Security.

Configuring Parental Control

To configure Parental Control, follow these steps:

1. Open **Quick Heal Mobile Security**.

2. On Dashboard, tap **Parental Control** to enable it. A confirmation screen appears. To confirm, tap **Yes**.

   Ensure that you have granted permission to enable Parental Control. Following options are available:

   ▪ **Enable Parental Control**: Select Parental Control to enable this feature.

   ▪ **Block Web Access**: Use this option to block access to the websites.

   ▪ **Allow Web Access**: Use this option to allow access to certain websites, even from the blocked category.

   ▪ **Set Browser for Parental Control**: Use this option to select a browser for secure access. If you enable Parental Control, you are recommended to use Quick Heal browser for desired result.

- **Block App Categories**: Use this option to block access to the apps by categories.

- **Allowed apps**: Use this option to allow certain apps even from the blocked categories.

- **Block Play Store**: Select this option if you want to prevent installation of apps. Access to Play Store will be blocked.

- **Parental Control Report**: If you want to receive a report on web access and data usage, you must register with Remote Device Management and add your device and do the required settings.

Block Web Access

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

To block access to websites, follow these steps:

1. Open **Quick Heal Mobile Security**.

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

   The Parental Control screen is displayed with the 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 URL gets blocked.

Allow Web Access

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

To allow access to certain websites, follow these steps:

1. Open **Quick Heal Mobile Security**.

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

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

   Note:

   - Parental Control provides multi-browser support to block websites.
   - Parental Control may not support any beta versions of the browsers.

Set Browser for Parental Control

If you have enabled Parental Control, you can configure the settings for security for any browser. However, it is recommended that you select Quick Heal browser for desired result.

To set a browser, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. On Dashboard, tap **Parental Control** > **Set browsers for Parental Control**.
3. Select the supported browsers from **Use a standard browser** or **Quick Heal browser**.

> Note: You can select a standard browser that Quick Heal Mobile Security supports. However, the security settings may be limited on standard browsers. We recommend Quick Heal browser for better security as all security settings will be implemented without any restriction.

Block App Categories

Using this option, you can block access to the apps by their categories. If you block a category, all the apps of that category will be blocked.

To block access to the app categories, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. On Dashboard, tap **Parental Control** > **Block App Categories.**
3. Select the app categories.

Allowed apps

Using this option, you can allow access to certain apps, even from the blocked categories. For example, if you block the Social category but you want to allow Facebook, you can do so here.

To allow access to the apps, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. On Dashboard, tap **Parental Control** > **Allowed apps.**
3. All the apps installed on your mobile appear. Select the apps that you want to allow to access.

Parental Control Report

Using this option, you can view the reports about how your children are using the internet. You can also configure the settings to receive the report on scheduled time automatically.

To view or receive the report, you must first register with Remote Device Management (RDM). RDM allows to add your device, implement certain settings on the device, and monitor certain settings on the device remotely.

To know how to configure RDM, see [Create Web Account](#).

Date Breach Alert

Data breach means unethical access to the data of individuals and organizations that are supposed to be secured from unauthorized people. Hackers hack into the organizations' data system and disclose or steal personal information of the people who register or sign up with such organizations.

You must keep a watch whether your data is ever breached or leaked.

Configuring Data Breach Alert

To configure Data Breach Alert, follow these steps.

1. Open **Quick Heal Mobile Security**.

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

3. Tap **Get Started**.

4. Select an email for which you want to detect if your personal information has ever been leaked. You can even type a new email address.

5. Tap **Check for Data Breaches**.

Note:

○ Sometimes, it may take time to fetch the report on data breach depending on the volume of data.

○ Some recommendations about how to secure your data are also mentioned.

○ If you want to check data breaches with another email, swipe on the email address to the left. The options Stop Monitoring and Change Email appear. Tap the Change Email option and then select or type another email address.

Learn how to secure your data

If your data is leaked, do not panic. Securing your personal information is in your own hands. Take the following steps to make your personal information more secure.

Step 1

Set a strong password with the affected websites or services. If the same password was used in other places, change it immediately. Never re-use old passwords.

Step 2

Enable 2-factor authentication if available on those websites or services.

Note: Intruder is a premium feature and is available in Quick Heal Total Security.

Intruder

The Intruder feature helps to capture the image if any unauthorized person who tries to access your device without your knowledge or permission. If someone enters a wrong password two times consecutively to unlock your device, such a person is considered an intruder. The Intruder feature will capture the snapshots of the person using the front and rear cameras along with date, time, and the location of the intruder. It will send an email to the configured email address with all these details. This helps you to track your device in case it is lost or stolen.

Note:

- If your device does not have a front camera, no image can be captured.
- Intruder is a premium feature and is available in Quick Heal Total Security.

To enable Intruder, follow these steps.

1. Open **Quick Heal Mobile Security**.
2. On Dashboard, tap **Intruder**.
3. Select **Capture Intruder's Selfie** to enable this feature.
4. To set an email address, select the **Enable Email Address** option and then add an email address. You can edit the email address whenever you prefer.

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

Note:

- To enable Web Security on the device, you must grant permissions.
- Web Security may not support any beta versions of the browsers.

Pocket Alarm

Helps you to protect your device from theft by alerting when someone tries to remove the phone from your pocket.

Note: Pocket Alarm is a premium feature and is available in Quick Heal Total Security.

Configuring Pocket Alarm

To configure Pocket Alarm, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. On Dashboard, tap **Pocket Alarm** and enter the PIN.
3. Tap **Activate Alarm** to activate this feature.

Motion Alarm

Helps you to protect your device from theft by alerting when someone tries to move your device from the place you have kept.

Note: Motion Alarm is a premium feature and is available in Quick Heal Total Security.

Configuring Motion Alarm

To configure Motion Alarm, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. On Dashboard, tap **Pocket Alarm** and enter the PIN.
3. Tap **Activate Alarm** to activate this feature.

Wi-Fi Security

Wi-Fi Security scans the Wi-Fi network that you connect. This feature checks if your network is secure. This helps you to prevent accessing unsecure Wi-Fi network or fix the security issues.

Configuring Wi-Fi Security

To configure Wi-Fi Security, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. On Dashboard, tap **Wi-Fi Security** and enter the PIN.
3. Select **Wi-Fi Security** to enable this feature.

   If Wi-Fi Security is enabled, it will check if the Wi-Fi network you are connecting is secure.

Privacy Advisor

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

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

Configuring Privacy Advisor

To configure Privacy Advisor, follow these steps:

1. Open **Quick Heal Mobile Security**.

2. Select **Privacy Advisor** to enable this feature.

   The applications are displayed with the permissions that are assigned.

Viewing app permission

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

1. Open **Quick Heal Mobile Security**.

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

3. Tap the application.

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

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

Various permissions that an app may use are as follows.

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

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

Privacy Audit Notification

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

Viewing Trusted Apps

1. Open **Quick Heal Mobile 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

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

Configuring Security Advisor

To configure Security Advisor, follow these steps:

1. Open **Quick Heal Mobile Security**.

2. Select **Security Advisor** to enable this feature.

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
Accounts & Sync	The device receives data from synced accounts or sites that increases the risk of hacking and account misuse. It is advisable to turn this option to OFF when not required.
Bluetooth	Data transfer through Bluetooth might put your device and its data at risk. It is advisable to turn this option to off when not required.
Device Memory Encryption	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. Note: The Device Memory Encryption setting is available only on supported OS.
Hotspot & Tethering	Data shared through Wi-Fi Hotspot, USB and Bluetooth Tethering is at risk to be hacked. To prevent data hacking, turn this option to OFF when not required. Note: The Hotspot and Tethering settings are available only on supported OS and vendors.
Anti-Theft	Protects your device and its data. This option allows you to trace, block, wipe data, and ring the device if your device is lost.
Background Scan	Shields your device against various types of threats. Keep this option enabled for security.
Screen Lock	If this option is disabled, your personal data may be at risk of misuse. Ensure that Pattern, PIN, Password or Finger Print screen lock options are set to safeguard the device data.
USB Debugging	If USB debugging is enabled, your device is at risk of being hacked and your data can be misused. Turn this option to OFF for security.
Wi-Fi 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.

Secure Delete

Helps you to delete the data in a secure way. Deleting data in a normal way may leave the trace of the data and can be tracked by the tracking apps. With Secure Delete, you can delete the confidential data permanently without leaving any trace behind.

> Note: Secure Delete is a premium feature and is available in Quick Heal Total Security.

Deleting data securely

To delete data securely, follow these steps:

1. Open **Quick Heal Mobile Security**.

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

3. Select data from the following data types to delete.

   - Contacts

   - Calendar Events

   - SD Card

   - SIM Data

4. After selecting the data type, tap **Delete**. A conformation message appears. Tap **Yes**.

Enter the PIN. Grant permission you have not granted yet.

Call Blocker

The Call Blocker 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.

> Note: This feature is supported on Android 8 and earlier versions.

Configuring Call Blocker

To configure Call Blocker, follow these steps:

1. Open **Quick Heal Mobile Security**.

2. On Dashboard, tap **Call Blocker** > **Yes**.

3. The Call Blocker option is enabled. Different options to block the calls is displayed.

Blocking unwanted calls

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

1. Open **Quick Heal Mobile Security**.

2. On Dashboard tap **Call Blocker**. 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.

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

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

Safe Charging

Helps to do safe charging. When you plug in your device for charging, the possibility is that the device is over charged. You need to check it again and again to ensure that the device is not over charged. Safe Charging gives a signal by ringing to switch off charging when the device is fully charged.

Setting Safe Charging on

To set Safe Charging on, follow these steps:

1. Open **Quick Heal Mobile Security**.

2. On Dashboard, tap **Safe Charging** and enter the PIN.

3. Select **Safe Charging** to enable this feature.

Battery Saver

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

Configuring Battery Saver

To configure Battery Saver, follow these steps:

1. Open **Quick Heal Mobile Security**.

2. On Dashboard, tap **Battery Saver.** Ensure that you have granted permission to enable this feature.

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

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

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

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

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

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

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

Activating Battery Saver mode

1. Open **Quick Heal Mobile Security**.

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

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

Setting screen brightness

1. Open **Quick Heal Mobile Security**.

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

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

Setting Screen timeout

1. Open **Quick Heal Mobile Security**.

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

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

Network Monitor

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

Note: This feature is supported on Android 8 and earlier versions.

Configuring Network Monitor

To configure data usage limit, follow these steps:

1. Open **Quick Heal Mobile Security**.

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

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 Mobile 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.

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

3. Setting menu

The Setting menu includes the following.

Upgrade to Premium

Using this option, you can upgrade your license easily.

To upgrade the license, follow these steps:

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

2. Tap the **Setting** menu and tap the **Upgrade to Premium** button.

    Upgrade to Premium: Includes SafePe, Parental Control, Advanced Anti-Theft, Intruder, Web Security, Schedule Scan, Background Scan, Secure Delete, Pocket Alarm, Motion Alarm, Fake App detection, Anti-KeyLogger detection.

    Add-on Features: Includes Parental Control and SafePe as adds-on features.

3. Tap **All Features** or **Add-on Features** as per your preference.

    - **Buy Premium**: Helps you to buy the all features or add-on features as per your preference and make the required payment.

    - **Have a Product Key**: Helps you to upgrade the license from Quick Heal Mobile Security to Quick Heal Total Security using the Product Key that you have purchased. With this option, you can have all the features but cannot buy add-on features.

    - **Don't have a Product Key, Purchase now**: If you select this option, you are redirected to the website of Quick Heal where you can buy your license key.

About Protection

Quick Heal protects your data and device from all kinds of malware, fake apps, adware, and riskware. Quick Heal detects malware at real time to prevent any kind of data loss or phishing attempt.

Here we display important information regarding the protection features that Quick Heal provides.

To check about the features, follow these steps:

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

2. Tap the **Setting** menu and tap **About Protection**.

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, SafePe, Safe Charging, and Wi-Fi Security.

To access Settings, follow these steps:

1. Open **Quick Heal Mobile Security.**

2. Tap the **Setting** menu and tap **Settings**.

3. Enter your PIN**.** The Settings screen appears. Configure the settings as required.

   Settings includes the following options:

   - [General](#)
   - [Scan](#)
   - [Optimize](#)
   - [SafePe](#)
   - [Alert on Camera and Microphone](#)
   - [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 Mobile Security**.

2. Tap the **Setting menu** > **Settings** > **General** > **Change PIN**.

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

To change the PIN, follow these steps:

1. Open **Quick Heal Mobile Security**.

2. Tap the **Setting menu** > **Settings** > **General** > **Change PIN**.

3. Tap **Submit**.

Track Activity Log

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

To configure Activity Log, follow these steps:

1. Open **Quick Heal Mobile Security**.

2. Tap the **Setting 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 Mobile Security**.

2. Tap the **Setting menu** > **Settings** > **General.**

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

Status Bar Icons

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

To enable Quick Setting Notification, follow these steps:

1. Open **Quick Heal Mobile Security**.

2. Tap the **Setting menu** > **Settings** > **General.**

3. Select the **Status Bar Icons** check box to enable it.

Manage Through Web

You can manage Quick Heal app on your device through [Quick Heal Remote Device Management](#) (Quick Heal RDM). You can also perform many other activities to control your device and secure your data.

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

To enable Manage Through Web, follow these steps:

1. Open **Quick Heal Mobile Security**.

2. Tap the **Setting menu** > **Settings** > **General.**

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

Create Web Account

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

To create web account, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. Tap the **Setting menu** > **Settings** > **General**.
3. Tap **Create Web Account**. You are directed to the RDM web portal where you can create your account.

Log on to Quick Heal RDM

If you already have created an account with Quick Heal Remote Device Management (RDM), log on to the RDM portal. For more details, see [Create Web Account](#).

News Notification

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

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

To enable News Notification, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. Tap the **Setting menu** > **Settings** > **General**.
3. Select the **News Notification** check box to enable it.

Application Statistics

Quick Heal is installed and used on a vast range of devices including mobile, tablet, and other handheld SIM or SIM-less devices. We strive to make our app more and more compatible with all the latest devices. To make our app more competent, we continuously carry out research on our features and apps. To do this, we collect statistics from various sources and one of the 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 Mobile Security**.
2. Tap the **Setting menu** > **Settings** > **General.**
3. Select the **Application Statistics** check box to enable it.

Block Uninstallation

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

To enable Block Uninstallation, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. Tap the **Setting 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**.

Scan

The Scan option lets you configure various scan options.

To set scan, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. Tap the **Setting menu** > **Settings** > **Scan** and set different scan options.

Real time Scan

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

- To activate this option, select the **Real time 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: Schedule Scan is a premium feature and is available in Quick Heal Total Security.

To create a scan schedule, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. Tap the **Setting 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.

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 Mobile Security**.

2. Tap the **Setting 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 Mobile Security**.

2. Tap the **Setting menu** > **Settings** > **Optimize.**

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

SafePe

You can enable SafePe here. To know about how to configure SafePe, see SafePe.

Alert on Camera and Microphone

Sometimes malware can turn on the camera and microphone of your mobile device without your knowledge. This may result in sneak peak of your private life. Hence, it is important that you must ensure you know when the camera and microphone are turned on.

When camera is turned on, the camera icon is shown in green color and when microphone is turned on, the microphone icon is shown in yellow color. This helps you take appropriate action, if required.

For this, always keep the option Alert on Camera and Microphone enabled, so you get a notification in case they are turned on.

To enable Alert on Camera and Microphone, follow these steps:

1. Open **Quick Heal Mobile Security**.

2. Tap **Setting menu** > **Settings**

3. Enable **Alert on Camera and Microphone.**

Safe Charging

You can enable Safe Charging here. To know about how to configure Safe Charging, see
Safe Charging.

Wi-Fi Security

You can enable Wi-Fi Security here. To know about how to configure Wi-Fi Security, see
Wi-Fi Security.

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.

Creating activity log

To create activity log, follow these steps:

1. Open **Quick Heal Mobile Security.**

2. Tap the **Setting** menu and tap **Activity Log**.

3. Tap the filter icon to create the activity log.

4. On the filter screen, select the duration and features for which you need the activity log. Tap **Show Logs**. Activity log is displayed.

5. Select the activity logs and then tap **Share**. Share the log through email or other sources.

Threats 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 Threats
- Active Threats
- Quarantined

- [Vulnerability](#)
- [Ignored Threats](#)

Resolved Threats

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

To view the resolved threats, follow these steps:

1. Open **Quick Heal Mobile Security**.

2. Tap the **Setting** menu and tap **Threats Report**.

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

Note: When user takes any action on Active/Detected Threat, its moves to the Resolved Threats list.

Active Threats

The Active Threats option displays the list of unresolved, harmful application threats detected during the scan. You can view the count of unresolved threats. You have to take an action to resolve the threats.

To view the unresolved threats, follow these steps:

1. Open **Quick Heal Mobile Security**.

2. Tap the **Setting** menu > **Threats Report**.

3. In the View list, tap **Active Threats**. The list of unresolved threats is displayed.

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

    - To ignore, tap **Skip**.

Quarantined

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

To restore the files, follow these steps:

1. Open **Quick Heal Mobile Security**.

2. Tap the **Setting** menu > **Threats Report**.

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**.

Vulnerability

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

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

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

1. Open **Quick Heal Mobile Security**.

2. Tap the **Setting** menu > **Threats Report**.

3. In the View list, tap **Vulnerability**. 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.

Ignored Threats

The Ignored Threats option displays the list of resolved applications. After you ignore the threats from the Active Threat list, the threats are displayed in the Ignored Threat list. You can clear the list by tapping the **Clear** option.

To view the ignored threats, follow these steps:

1. Open **Quick Heal Mobile Security**.

2. Tap the **Setting** menu and tap **Threats Report**.

3. In the View list, tap **Ignored Threats**. The list of ignored threats is displayed.

Note: When user takes Ignored the Active/detected threat then its moves to the Ignored threat list.

Feedback

The users may provide their feedback to us. Feedback helps us to improve the Quick Heal application.

To give feedback, follow these steps:

1. Open **Quick Heal Mobile Security**.

2. Tap the **Setting** menu > **Feedback**.

3. Select your feedback rating and then tap **Submit**.

Help/Support

The Help/Support option allows to take advantage of our support facilities.

To go to Help, follow these steps:

1. Open **Quick Heal Mobile Security**.

2. Tap the **Setting** menu and tap **Help/Support**.

3. Help includes the following options.

   Live Chat: To get 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. Our experts will revert to you with an appropriate answer.

   Support Center: You can call us at the following numbers.

   - Toll Free number: 1800-121-7377

   - Toll Number: 7030067377

   - WhatsApp No.: +91 7030067377

   Timing
   - Monday – Saturday: 8:00 AM and 11:00 PM IST (Indian Standard time).

   - Sunday: 9.00 AM to 6.00 PM (IST).

   Other Contacts
   - Email: support@quickheal.com

   - For more details on support, check at https://www.quickheal.co.in/support

   Online Help: This includes the online help of the Quick Heal app.

   FAQs: Includes a number of frequently asked questions (FAQ) that offer solutions to several queries and issues.

   Enable Debug Logs:

   If you face any issue with the application and want to share its logs, capture 4-5 screenshots showing the issue and then select the **Setting** menu > **Help/Support** > **Enable Debug Logs** and tap **Share Logs**. The files/images will be sent to the Quick Heal support team, who will reply you with a solution.

License Details

This section shows the license key, the license type, and owner details. You can also update the license information, renew, and upgrade your license.

To view the license details, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. Tap the **Setting** menu and tap License Details.

About Product

This section provides information about the product, virus database, product license information, and a share option using which you can share the Quick Heal app with your friends.

To view the product details, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. Tap the **Setting** menu and tap **About Product**.

   Update: Helps to update the virus database.
   Share: Helps to share the Quick Heal application via various methods.

Uninstall Quick Heal

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

To uninstall Quick Heal Mobile Security, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. Tap the **Setting** menu and then tap **Uninstall Quick Heal**. Enter the PIN. A confirmation screen appears.
3. Tap **OK**.

   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.