Quick Heal Mobile Security & Quick Heal Total Security for Android

User Guide

Version 4.0

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. Quick Heal Mobile Security is the free version and Quick Heal Total Security is the paid premium version of the product. Some features are available only in the premium version. The product may be referred to by both names in the documentation as applicable.

What's New in this Version?

Features & Enhancements

- New and Improved design for better user experience
- Security and Privacy Score
- YouTube Supervision
- Screen Time Monitoring
- metaProtect console to manage the devices remotely
- Anti-spyware and Privacy Advisor

Contents

Getting Started

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

1. System Requirements

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

- Android 6.0 and later versions.
- Supported Android Screen Resolutions: Supports all Android screens.

2. 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.

3. Registering Quick Heal Mobile Security

After installation, you must register/activate Quick Heal Mobile Security to use all the features and protect your device

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.

2. Tap **Proceed**. The welcome screen appears.
3. Enter your name.
4. Enter your phone number and tap **Send OTP**. Quick Heal verifies your mobile number using the OTP received.
5. Tap **Next**. You are redirected to Protect my device screen.
6. Quick Heal requires access to contacts and phone calls. Tap **GRANT ALL**.
7. Then are redirected to Enable protection from fake links/websites screen.
8. Quick Heal requires accessibility permissions to enable security from fake links/websites. Tap **GRANT ACCESS**.

9. On the Accessibility Screen, navigate to Downloaded apps and search for Quick Heal.
10. Enable the toggle button for Quick Heal and tap **Allow** to grant Quick Heal full control of your device.
11. Tap back icon two times. You are redirected to **Connect a Google Account** screen.
12. Select the required Google account and tap NEXT. Further you are asked to Choose a Plan for your device:
    - To purchase via Play Store, select a plan and Tap **PROCEED**. Continue with the instructions to complete the purchase.
    - Tap **USE PRODUCT KEY**, if you already have purchased Quick Heal. Enter the product key.
      Note: Applicable if you have already purchased the license with existing email account.
    - Tap **CONTINUE WITH FREE VERSION**, if you want to try the trial version of product.
    - Tap **Transfer Ownership** if you want to transfer license from the existing device to current device. You need to uninstall Quick Heal from the existing device.
      (If you do not uninstall Quick Heal from existing device after transferring ownership, a piracy screen is displayed on current device after virus database update. You will not be able to Quick Heal on the current device unless Quick Heal app is uninstalled from previous device.)

      A license activation screen is displayed with the validity details.
13. Tap **NEXT** to continue. The Registration Complete screen is displayed.

    *Note: If you are proceeding with the free version, an **UPGRADE TO PREMIUM** option is displayed. After tapping on UPGRADE TO PREMIUM, you can purchase the premium plan via Play store or Product key through the Quick Heal website.*

Dashboard or the Home Screen

The dashboard (Home) is displayed when you start the application. You can also reach the dashboard when you tap **Home** icon on any of the feature screens.

The dashboard displays the following options:

1.Quick Scan

A quick scan lets you check if any viruses or malwares have infected your device app files.

2.Security Score

It indicates the level of protection your device has against viruses, malware, and other malicious programs.

Note:
Quick Heal provides you with a list of recommendations that you need to follow to improve your security score. Enable all the recommendations to get a high security score.

Under security recommendations, you can view status of recommendation:

- If you have not followed a recommendation, a “Get started” status is displayed against that feature.
- If you have already configured the recommendation, a “Completed” status is displayed for that feature.

3.Privacy Score

The Quick Heal Privacy score is a measure how safe is your data on your device.

Note:
Quick Heal provides you with a list of recommendations that you need to follow to improve your privacy score. Enable all the recommendations to get a high privacy score.

Under privacy recommendations, you can view status of all recommendations:

- If you have not followed a recommendation, a “Get started “status is displayed against that feature.
- If you have already configured the recommendation, a “Completed” status is displayed for that feature.

4. Recommendations

Dynamic recommendations are visible on your dashboard which indicate the set of actions you need to take to better protect your device. The recommendation cards may display status, action items pending, and important cyber related news.

5. What's New

This section keeps you informed about the latest security updates and tips to keep your device secure. We regularly publish new blogs, articles and announcements that keep you one step ahead of the cyber criminals.

Make sure that you are in touch with the latest announcements as they are super handy to be a smart internet individual in today's times.

Features

Tap the Features icon to view the all the features available for your device:

Group Name	Feature Name
Device Protection	Quick Scan
	Deep Scan
	Wi-Fi Security
	SafePe
	Threat Report
Internet and App Security	Safe Browsing
	Parental Control
	YouTube Supervision
	Play Store App Advisor
	App Lock
Data Protection	Anti-Theft
	Intruder Alert
	Secure Delete
Device Optimization	Device Cleaner
	Battery Saver
	Screen Time
Privacy Protection	Data Breach Alert
	Privacy Advisor
	Anti-Spyware

All features and their usage are detailed out in the upcoming sections.

1. Device Protection

This menu group allows you to perform a quick scan, deep scan on the device, check your Wi-Fi, secure your banking activities, and view threat reports for your device.

A. Quick Scan

Quick scan enables you to quickly scan all your device apps and files for any threat. If any threat is detected, an appropriate action is recommended that can fix the threat.
Note: Detection for 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 the Dashboard, navigate to **Device Protection > Quick Scan**.

3. Tap **Scan** to start scanning.
4. Tap **Stop Scan** if you want to stop the scanning process.

   The results of the scan will be available Threats Detected and Apps Scanned count.
   If any threat is detected in an app, an option to select and uninstall the app is displayed.

B. Deep Scan

Deep Scan helps to scan all the files, folders and apps on your device for possible threats, infections and vulnerabilities. It is more powerful than Quick Scan as it also checks for any fake apps and anti-keylogger malware installed on your phone that may steal information and confidential data.

If any threat is detected, an appropriate action is recommended that can fix the threat.
Note: Detection for 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 the Dashboard, navigate to **Device Protection** > **Deep Scan**.
3. Tap **Scan**.
   Deep scan of your device starts. Ensure that you have granted permission to enable scanning.
   You can view two options:
   - **Stop Scan**: To stop the scanning process
   - **Scan in the background**: Scan will run automatically in the background and you can use other features and apps on your device.

   If any threat is detected, you can take appropriate action to fix it. Threat report on metaProtect is generated as a result of the Deep Scan. To get full information about the threats detected, see Threat Report.

   Note: Scan in the background option is available only in Quick Heal Total Security (Premium).

C. Wi-Fi security

Wi-Fi Security checks if the Wi-Fi that your device is connected to is safe for financial transactions.

Wi-Fi Security also checks if your network is secure from vulnerabilities and is password protected.

To configure Wi-Fi Security, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. On the Dashboard, navigate to **Device Protection > Wi-Fi Security**.
3. Enter the PIN.
4. Toggle the Wi-Fi Security button to enable this feature. After Wi-Fi Security is enabled, it will check if the Wi-Fi network you are connecting to is secure.

D. SafePe

The SafePe feature protects all your financial apps that you use for financial transactions such as Google Pay, Paytm and others. It ensures that your payment apps are safe for online shopping, banking, and paying bills.

It performs several checks in the background such as malware infections or unknown security vulnerabilities before making any financial transactions using any app. This ensures your financial data is safe and secure with you.

To configure SafePe, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. On the Dashboard, navigate to **Device Protection > SafePe**. Turn on the toggle button to enable SafePe protection.
3. Click **Add An App**. A list of apps is displayed. Select the app for which you want to enable SafePe protection. You can select multiple apps for SafePe protection.
4. Click **Add.** The app is added to the protected list.

Note: When you install Quick Heal, it automatically adds payment apps into SafePe list and secures the financial transactions.

E. Threats Report

Quick Heal generates regular reports that help you gauge the real-time security status of the device.

You can take appropriate action on an infected app or even restore the quarantined files, which you think are useful to you.

Five types of detected threats are available:

i. Resolved Threats

The Resolved Threats option displays the list of threats which have been resolved. Once an active threat is resolved from Active Threats list, it is moved to the Resolved Threats list.

To view the resolved threats, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. On the Dashboard, navigate to **Device Protection > Threat Reports**. The count for each threat type is displayed.
3. Tap **Resolved Threats**. The list of resolved threats is displayed.

ii. Active Threats

The Active Threats option displays the list of unresolved threats present in your device.

You can view the list of Active threats and take the appropriate action suggested against each threat to resolve it.

To view Active threats, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. On the Dashboard, navigate to **Device Protection > Threat Reports**. The count for each threat type is displayed.
3. Tap **Active Threats.** The list for Active Threats along with its suggested actions is displayed as follows:
    - To remove an application for which an Active Threat is detected, select the application and tap **Uninstall > OK**. The application will be uninstalled from the device.
    - To ignore, tap **Skip**.

iii. Quarantined Files

All suspicious files and apps that seem harmful for your device are moved to Quarantined folder. This is a secure environment where suspicious files are locked, and they cannot infect the system. You can always restore or delete these files as per your need.

Quarantined files are automatically deleted after a fixed duration to save your system space.

To restore the files, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. On the Dashboard, navigate to **Device Protection > Threat Reports.**
3. In the displayed 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**. The files are restored to their original location.
    - To delete the files, tap **Delete.**

iv. Vulnerable Threats

This option displays the list of vulnerable apps and files detected during the scan. They can infect your system if left unattended.

You can take appropriate action suggested again each threat to protect your device as follows:

- You can uninstall the vulnerable apps.
- In case you feel that file or app is safe to use, you can mark it as trusted. After you trust any particular app or file, it will be moved to the bottom of the list.

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

1. Open **Quick Heal Mobile Security**.
2. On the Dashboard, navigate to **Device Protection > Threat Reports.**
3. In the displayed list, tap **Vulnerable Threats**. The list of vulnerable threats is displayed. The following options are 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.

v. Ignored Threats

The Ignored Threats option displays the list of apps and files that Quick Heal found to be suspicious, but you selected to ignore it from the threats list. It may be because you trust the app or file and consider it safe to use.

Once you ignore any threat from the Active Threat list, they are moved to 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. On the Dashboard, navigate to **Device Protection > Threat Reports.**
3. In the displayed list, tap **Ignored Threats.** The list of ignored threats is displayed.
   Note: When user takes Ignored the Active/detected threat then it moves to the Ignored threat list.

2. Internet and App Security

You can configure the settings to browse the Internet safely, set locks for apps, configure Play Store Advisor. You can also configure the settings for Parental Control, and YouTube supervision.

Below settings are available:

A. Safe Browsing

Safe Browsing feature blocks all fraud links/websites that you can steal your data, install malware or harm your device.

Your data such as bank details, user credentials, social security information, and passwords can be stolen if are not browsing the web safely with Safe Browsing feature.

To configure Safe Browsing, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. On the Dashboard, navigate to **Internet & App Security > Safe Browsing**.
3. Tap the toggle button to enable the Safe Browsing feature on the device. Your device is now protected from all fraud links/websites that can harm your device.

   Note: Safe Browsing requires you to grant some specific permissions.

B. Parental Control

You can use Parental Control to manage and monitor the online content that your children can see on the mobile device. You can block inappropriate content on websites and apps that may be harmful to your children.

Note: Parental Control is a premium feature that is available in Quick Heal Total Security. If you enable Parental Control, we recommend you use Quick Heal browser for optimum results.

To configure Parental Control for the first time, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. On the Dashboard, navigate to **Internet and app security > Parental Control.**
3. Enter the PIN.
4. Tap the toggle button to enable Parental Control. You need to grant certain permissions on the device to Parental Control. Tap **Grant Access**.
5. After you enable Parental Control, you can view the following options:
   - Restricted
     - **Blocked Web Categories**: Use this option to block access to the websites based on categories.
     - **Blocked URLs**: Use this option to block access to certain websites.
     - **Blocked App categories**: Use this option to block access to apps based on categories.
   - Allowed
     - **Allowed URLs**: Use this option to allow access to certain websites, even if the category is blocked.
     - **Allowed Apps**: Use this option to allow access to certain apps even if the category is blocked.

- View Report on metaProtect website: Use this option to view all Parental Control reports
  Note: If you want to view the report on metaProtect website, you must register your account with it.

a. Restricted

This section provides you with the option of restricting access based on various parameters:

i. Blocked Web Categories

The Block Web Categories option provides you with the list of website categories blocked based on their appropriateness for children (below 18 years old).

You can modify the list of web categories blocked with below steps:

To block access to websites, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. On the Dashboard, navigate to **Internet & app security > Parental Control.**
3. Enter the PIN.
4. In the Restricted section, tap **Blocked Web Categories**.
   - To block a category, tap and select that category you want to block on the device. A block icon will be displayed for all the selected categories and these categories are now blocked.
   - To remove an already added category, tap the corresponding Block icon for that category. That category is now allowed to access.
   - Tap **Restore to Default** to select the default categories blocked.

ii. Blocked URLS

This option helps you block access to certain websites or URLs as required.

To configure access to specific websites or URLs, follow these steps:

1. Open Quick Heal Mobile Security.
2. On the Dashboard, navigate to **Internet & app security > Parental Control.**
3. Enter the PIN.
4. In the Restricted section, tap **Blocked URLs**.
   - Enter the URL to block and tap **Add.** The URL is added and is blocked. The added URLs are displayed in the list.
   - To remove an added URL, tap the cross mark for that URL, the URL is removed from the block list.

iii. Blocked App Categories

This option helps you block apps based on categories such as Dating, Entertainment, and others as required.

To configure block access to specific apps based on categories, follow these steps:

1. Open **Quick Heal Mobile Security.**
2. On the Dashboard, navigate to **Internet & app security > Parental Control.**
3. Enter the PIN.
4. In the Restricted section, tap **Blocked App Categories**.
   - Select the App categories that you want to block. A block icon is displayed for each selected category. Add any categories as required. The added categories are displayed in the list.
   - To remove an app added to the list, tap the block icon. The block mark is removed for that category.
   - Tap **Restore to Default** to select the default app categories blocked.

b. Allowed

i. Allowed URLS

This option helps you allow certain URLs to open even if they are from the blocked categories.

For example, if you have blocked News category, yet you want to allow a certain URL to be accessed from that category, you can add that URL under the allowed URLs under the Allowed section.

To add a certain website URL to the Allowed list, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. On the Dashboard, navigate to **Internet & app security > Parental Control.**
3. Enter the PIN.
4. In the Allowed section, tap **Allowed URLs**.
   - Enter the URL to block and tap **Add.** The URL is added. The added URLs are displayed in the list.
   - To remove an added URL, tap the cross mark for that URL, the URL is removed from the Allowed list.

ii. Allowed Apps

This option helps you to allow certain apps to open even if they are from the blocked categories.

For example, if you have blocked the FM Radio category, yet you want to allow a certain FM channel to be accessed from that category, you can add that app under the Allowed Apps under the Allowed section.

To add a certain website URL to the Allowed list, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. On the Dashboard, navigate to **Internet & app security > Parental Control.**
3. Enter the PIN.
4. In the Allowed section, tap **Allowed Apps**.
    - Enter the app to allow and tap **Add an App.** Select the app that you want to add and click **Add**. The added apps are displayed in the list.
    - To remove an added app, tap the cross mark for that app, the app is removed from the **Allowed** app list.

c. Selecting Browser for Parental Control

Select the browser that will be used to browse the Internet on your device. All the restriction applied using Parental control will be valid for the selected browser.

Choose browser options based on the security requirement from the following:

i. **Moderate Security**
   Use a standard Browser: Standard browsers such as Chrome, Mozilla etc. offer medium security and limited parental control where some fake websites may not get blocked.
ii. **High Security**
   Use Quick Heal Browser: Quick Heal browser provides complete security, and complete parental control of all harmful websites will be blocked by default.

To set a browser, follow these steps:

1. Open **Quick Heal Mobile Security.**
2. On the Dashboard, navigate to **Internet & app security > Parental Control.**
3. Enter the PIN. The Parental Control panel is displayed.
4. Tap the **Setting** icon on the upper right corner. You cannot access the Parental Control setting until you enable the Parental Control feature.
5. In the Browser Preference section, select the option as required
   - For **Moderate security** select the **Use a standard Browser** option
   - For **High security**, select the option to **Use Quick Heal browser**.
     Note: Access to all other browsers will be blocked if you select this option. If you use other browser apart from Quick Heal, then Parental Control block screen will be displayed on the browser.
   - To block Play Store access, select the option Block Play Store.

d. Viewing Report on metaProtect

You can view Parental Control reports on the metaProtect website by tapping **View** on the lower panel of the screen.

C.YouTube Supervision

You can control the usage of YouTube on your device such as blocking a channel, video. Simply configure restrictions based on your requirement from YouTube Settings.

For e.g., Block YouTube shorts from being played out on the device by enabling the block option for YouTube Shorts.

i. Enabling YouTube Supervision

To configure YouTube supervision for the first time, follow these steps:

1. Open **Quick Heal Mobile Security.**
2. On the Dashboard, navigate to **Internet & app security > YouTube Supervision.**
3. Tap the toggle button **YouTube Supervision to** enable the feature. You need to grant certain permissions on the device to **YouTube Supervision**. Tap **Grant Access**.
4. After you enable YouTube Supervision, you can view the following options:

- **Restricted**
    - **Blocked Channels and Videos**: Use this option to block access to websites based on channel names.
        - To add a Channel Name to block list, enter the channel name and tap **Add**. The channel is added to the block list.
        - Remove a Channel from the block list. Enter the channel name and tap the block icon. The channel is removed from the block list.
    - **Block by Categories**: Use this option to block access to certain video content on YouTube by categories such as Adult, Entertainment, and others as required. The following options are available:
        - **Block All**: Select **Block All** to select all categories to be blocked.
        - Block a category: Tap and select any category as required. A block icon is displayed for that category.
        - Remove a blocked category: Tap an already blocked category in the list. The block icon is removed for that category.
    - **Block by Keywords**: Use this option to block content based on keywords. For example, Hate, Crime and other as required.
        - Add a keyword and tap **Add**. The keyword is added to the list.
        - Remove keyword from list. Tap the cross icon for an already added icon, the keyword is removed from the list.
    - **Block by Search History**: Use this option to block access to content based on the YouTube Search History. You can use this option when you want to block the content that has already been watched on YouTube earlier and you do not want your mobile device user to watch the content again.
- **Allowed**
    - Allowed Channels & Videos: Use this option to allow access to certain websites, even from the blocked category.

- Add the name of the channel and tap **Add**. The channel is added to the list.
- Remove the channel from the Allowed list. Tap the channel already in the list and it is removed from the Allowed list.

ii. Viewing Report on metaProtect

You can view YouTube Supervision reports on the metaProtect website by tapping **View** on the lower panel of the screen.

Note: If you want to view the report on metaProtect website, you must register your account with it.

D. PlayStore App Advisor

Play Store App advisor protects you from risky apps. It automatically scans the app before and after installation from Google Play Store and warns you of risks associated with that app.

To configure App Advisor, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. On the Dashboard, navigate **to Internet and App Security > PlayStore App Advisor** to enable this feature.

E. App Lock

This option helps you lock any application of your device with a PIN or pattern to keep your data safe from unauthorized users. You can lock applications which may have your videos, audio, chats, confidential data, images that you want to protect from misuse.

When any user opens any locked app, the App Lock screen is shown to the user where user is prompted for a password. In the case of PIN, numeric screen is displayed and in case of pattern, pattern screen is displayed.

You can also use Fingerprint lock/unlock feature to unlock the app using fingerprint sensor.

a. Locking the app with App Lock

1. Open **Quick Heal Mobile Security**.
2. On the Dashboard, navigate to **Internet & App Security > App Lock.** Enter PIN or Pattern as set previously**.** The list of applications is displayed.
   Note: If you are visiting for the first time, you must set a new PIN.
3. Tap the corresponding lock icon for an app you want to lock.
   The app lock is now set upon that application. When any user tries to access the app, the device prompts for the PIN.

b. Unlocking the app

1. Open **Quick Heal Mobile Security**.
2. On the Dashboard, navigate to **Internet & App Security > App Lock**.
3. To unlock a locked app, in the App Lock screen, tap the active lock icon available in front of that app.
4. The App Lock is now removed from that application. It can be opened without any PIN or password.

c. App Lock Settings

The following settings options are available for the App Lock feature:

- Unlock using: Select the option you want the app to be unlocked i.e., PIN or Pattern as required.
- Scramble Keyboard: This randomly changes key positions when entering the PIN so it cannot be recorded.
  Note: This option is visible when you have selected the PIN option in Unlock using PIN or Pattern settings.
- Show Prompt: This option, if enabled, will show the lock prompt for the newly installed app on its own.

i. Unlock using PIN or Pattern

Quick Heal Mobile Security provides the options to unlock the apps using PIN or set pattern as below:

- PIN: This option allows you to use the Quick Heal Mobile Security app's PIN to unlock the locked application.
- Pattern: This option can be used to set a pattern to unlock the locked applications.

Changing PIN

To change the PIN, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. On the Dashboard, navigate to **Internet & App Security**, and tap **App Lock**. In the App Lock screen, tap **Setting** icon on the upper right corner.
3. In the App Lock Setting screen, under Unlock Using, select **PIN** and tap **Change PIN**.
4. Enter current PIN, new PIN, and confirm new PIN.
5. Tap **Proceed**. The PIN is updated.

Change Pattern

The Change Pattern helps you set a new pattern to unlock the locked apps.

*Note: This Change Pattern option is visible when you have selected the **Pattern** option in Unlock using 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. After drawing a pattern, you must confirm it. If you attempt 3 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 the Dashboard, navigate to **Internet & App Security**, and tap App Lock. In the App Lock screen, tap Setting icon on the upper right corner.

3. In the App Lock Setting screen, select **Pattern** and tap **Change Pattern**.

   You are redirected to the Reset Pattern screen.

   - Select at least 4 dots to draw a new strong pattern.
   - You must redraw the pattern and confirm.
     If you make 3 wrong pattern attempts at the time of confirmation, you have to reset the pattern.

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

ii. Scramble Keyboard

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

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

Note: This option is visible when you have selected the PIN from Unlock using option in settings.

Configure Scramble Keyboard

1. Open **Quick Heal Mobile Security**.
2. On the Dashboard, navigate to **Internet and App Security > App Lock**, tap Setting icon.
3. In the App Lock Settings screen, select the **Scramble Keyboard** check box. The setting is enabled and will randomly change the positions of keys on numerical keypad each time the password needs to be entered.
   - To stop scrambling the keypad, clear the **Scramble Keyboard** check box.

iii. Show Prompt

This option enables a prompt that asks you to lock a newly installed application as soon it is installed on the device. As a result, a prompt is displayed whenever you install a new application on the device.

Configure Show Prompt option

1. Open **Quick Heal Mobile Security**.
2. On the Dashboard, navigate to **Internet and App Security > App Lock**, tap Setting icon.
3. In the App Lock Settings screen, select the **Show Prompt** check box.
   - To stop the locking of newly installed apps, clear the **Show Prompt** check box.

d. 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 devices with native Fingerprint sensor.

e. App Lock Screen

When a user tries to open any locked app then, App Lock screen is prompted to unlock the app with a password.

In the 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.

The following options are available on App Lock screen on the upper right corner:

• **Unlock Permanently**: This option will unlock the app permanently upon entering correct PIN.

• **Forgot PIN**: This option helps you recover your PIN in case you forget it. You are prompted to unlock using

- Google Authentication: Login to your Google account and reset the PIN.
- Cloud Login to reset PIN: Login to your metaProtect account to reset PIN.

• **App Lock Setting**: This option will take the user to App Lock screen where user can choose the lock options.

3. Data Protection

Data is your most important asset. It is the backbone of your digital life and Quick Heal ensures it is safe and secure. Protecting data with very easy as Quick Heal offers several data protection features. You can wipe your data from your device from misuse if gets stolen or missing. You can also secretly capture selfies of anyone who tries to unlock your device without you knowing. Additionally, you can securely delete the data on your device so that it can never be recovered.

Below are the Quick Heal data protection features:

A. Anti-Theft

Anti-Theft helps you with several security options to secure your device data. With Anti-Theft, you can do the following:

- Send a ring command to your device
- Track the device location
- Wipe data from your device
- Secretly capture photos, audio and video of the surroundings of device which may help you track the device.

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

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

1. Open **Quick Heal Mobile Security**.
2. On the Dashboard, navigate to **Data Protection > Anti-Theft**.
3. Enter the PIN. Tap **Anti-Theft** toggle button to activate the feature.

a. Configure Anti-Theft Settings

i. Block on Airplane Mode

This feature blocks your device when a thief or intruder turns on Airplane or flight mode of the device to stop it from being tracked. This ensures your data is secure on your device as the device is blocked from being misused. The device can then be unblocked only from your metaProtect website account.

To configure Block on Airplane Mode for the device, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. On the Dashboard, navigate **to Data Protection > Anti-Theft**, and tap the **Settings** icon on the upper right corner.
3. Ensure that **Anti-Theft** feature is enabled.

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

ii. Emergency Contact Details

If the device is lost or stolen, and subsequently blocked with Anti-Theft settings, you can display 2 contact numbers on the blocked device to help the finder contact you.

Enter any two mobile numbers that will be visible on your blocked device. Anyone who may find your device can contact you via these contact details.

Adding Emergency Contact Details

1. Open **Quick Heal Mobile Security.**
2. On the Dashboard, navigate to **Data Protection > Anti-Theft**.
3. Tap the **Settings** icon on upper right corner.

   Ensure that Anti-Theft is enabled on the device.

4. Tap **Emergency Contact Details**.
5. On Emergency Contact Details screen, tap **Add a Contact.**
6. Select the contact as required from the Contacts list. The number is added to the Emergency Contact list.
7. To remove the alternate contacts, in the Emergency Contact Details screen, tap the (X) cross mark available in front of the contact.

iii. Log on to metaProtect

To manage your device remotely in case the device gets lost or is stolen, you have to create an account or use an existing account with metaProtect portal. Additionally, metaProtect account is beneficial to use several other features of Quick Heal Mobile Security remotely. For more information, click here.

iv. Unblock device

This option helps you to unblock your device if locked with Anti-Theft feature or if you forget your PIN. You can unlock your device through Google Authentication or through metaProtect website if you forget your PIN.

To unblock your device, follow these steps:

1. On the block screen, tap **Unlock Phone**. The Enter PIN screen is displayed. Enter the PIN to unlock your phone.
2. In case you forgot the PIN, tap **Forgot PIN?.** The Forgot PIN screen is displayed with two options to unblock your phone.

- **Google Authentication**: Use this option to validate your Gmail account. Enter your google account and tap Login. The Google Authentication screen is displayed. Follow the steps displayed on screen to authenticate your account.
- **Cloud Login to reset PIN**: Use this option to reset PIN through the metaProtect website. Tap **Go to metaProtect** website to reset PIN. Enter your metaProtect Mobile number/Email and password to logon to metaProtect website. Navigate to the **Dashboard > Settings > Change PIN** section and set a new PIN for the device.

B. Intruder Alert

The Intruder Alert feature helps to secretly capture the selfie image of any person who tries to unlock your device without your knowledge or permission.

If someone enters a wrong password two times consecutively to unlock your device, the Intruder Alert feature will capture the snapshots of that person using the front and rear cameras along with date, time, and the location of the intruder.

Then, it will send these images to your registered email address with all these details. This information may help you to track your device in case it is lost or stolen. In the Intruder Alert email, Intruder location (Provided GPS is enabled on device) and Date/time will also be captured.

Note: If your device does not have a front camera, no image can be captured.

Intruder Alert 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 the Dashboard, navigate to **Data Protection > Intruder Alert.**
3. Enter the PIN.
4. Tap the toggle button to **Capture Intruder's photo**.
5. To set up or change an email address to receive the intruder's photos by email, tap the settings icon on the upper right corner and then add /change the email address. Tap **Save** to save the changes.

C. Secure Delete

The Secure Delete feature helps you to delete the data on your device permanently that can never be recovered. Deleting data without secure delete may leave trace of the data that can be recovered using specialized apps.

With Secure Delete, you can delete confidential data permanently so that it cannot be undeleted or recovered in any way with any application.

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

To delete data securely, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. On the Dashboard, navigate to **Data Protection > Secure Delete**.
3. Select data from the following data types to delete.
    - Contacts
    - Calendar Events
    - Internal & External Card
4. After selecting the data type, tap **Delete**.
   A confirmation message appears. Tap **Delete**.

4. Device Optimization

Quick Heal Mobile security helps you optimize the resources on your mobile device such as speed, battery life, and manage your screentime to minimize exposure to the mobile screen.

Below are the features:

A. Device Cleaner

You can optimize your device and improve its performance using Phone Boost. Phone Boost kills the apps in the background, clears the app cache files, obsolete APKs, junk files, and thumbnail images to free system space on your device.

To increase the device performance:

1. Open **Quick Heal Mobile Security**.
2. On the Dashboard, navigate to **Device Optimization > Device Cleaner**, then tap **Clean**.
   Your device is boosted and further option to clear more files is displayed. You can view details of the junk files, cache files and delete them if required.

B. Battery Saver

The Battery Saver option helps you save power and increase usage time of device before charging battery again. You can configure the settings to save power based on your priority.

To configure Battery Saver, follow these steps:

1. Open Quick Heal Mobile Security.
2. Navigate to **Device Optimization > Battery Saver.**

Ensure that you have enabled this feature after granting the required permissions to enable this feature.

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

- Enable Battery Saver: Set the battery level when the Battery Saver mode should start.
- Set Screen Brightness: Set the screen brightness after Battery Saver mode starts.
- Set Screen Timeout: Set the screen timeout after the Battery Saver mode starts.

Activating Battery Saver mode

1. Open **Quick Heal Mobile Security**.
2. Navigate to **Device Optimization > Battery Saver**
3. Tap the **%** for Enable Battery Saver. Select the percentage at which the Battery Saver should get activated and tap **Okay**.

Setting screen brightness

4. Open **Quick Heal Mobile Security**.
5. Navigate to **Device Optimization > Battery Saver.**
6. **Tap** the **%** for **Set Screen Brightness**. Select the percentage at which screen brightness should become when the Battery Saver is activated and tap **Okay**.

Setting Screen timeout

1. Open **Quick Heal Mobile Security**.
2. On the Dashboard, navigate to **Device Optimization > Battery Saver.**
3. **Tap** the **%** for **Set Screen Timeout**.
4. Select the duration after which screen should turn off once the Battery Saver is activated.
5. Tap **Okay**.

Additional Settings

- Disable Sync: Select this check box to disable auto-sync of the device automatically in Battery Saver mode.
- Auto Boost: Select this checkbox to kill apps when the screen is off for 30 mins.
- Disable Bluetooth: Select this check box to disable Bluetooth network automatically when Battery Saver mode starts.

C. Screen Time

Most individuals spend countless hours sitting in front of their screens. It might be due to their work or entertainment needs which can have serious impact on their health.

A study found that 50% of people spend over 10 hours/day using their laptops and mobile devices and suffer from migraines, eye pain, loss of focus etc. It is widely known that extended screen time causes eye strain, headaches, disrupts sleep and other physical discomfort.

To help you manage your screen item, we provide you with all your time spent on the screen so that you can build routine to cut down on your screen time and enjoy improved health.

You can use the following Screen Time options for managing device usage and reducing the negative effects associated with extended periods of screen time.

Enabling Screen Time

1. Open **Quick Heal Mobile Security**.
2. On the Dashboard, navigate to **Device Optimization > Screen Time.**
3. Tap the toggle button to enable Screen Time.
4. Set the Daily Screen Time and App Time.

Setting Screen Time

1. Open **Quick Heal Mobile Security**.
2. On the Dashboard, navigate to **Device Optimization > Screen Time.**
3. Tap **Set Screen Time** and set the Daily Screen Time Goal as required.
4. Tap **Done**.

Setting App Time

1. Open **Quick Heal Mobile Security**.
2. On the Dashboard, navigate to **Device Optimization > Screen Time.**
3. Tap **Set App Time**.
4. Tap the clock icon for the app for which you want to set the time. The Set App Time dialog is displayed.
5. Set the Time in HH/MM.
6. Tap **Okay**.

Viewing Reports

1. Open **Quick Heal Mobile Security**.
2. On the Dashboard, navigate to **Device Optimization > Screen Time > Report.**
3. View Screen Time Insights, Weekly Screen Time Goal, Daily App-wise Goal.

- In Screen Time Insights graph, your daily screen time in HH/MM is shown in Pie chart form.
- In Weekly Screen Time Goal graph, the Screen Time graph for the whole week is displayed according to your daily usage.
- In Daily App-wise Goal graph, app-wise utilization is displayed.

▪ Viewing Report on metaProtect

You can view screen time reports on the metaProtect website by clicking View on the lower panel of the screen.

5. Privacy Protection

Your digital identity is as important in today's times as your Adhar card in your real life. It becomes imperative you protect it as cyber criminals can misuse it and harm you. Quick Heal enables you easily secure your digital identity with several features such as data breach alert, protection from risky apps collecting your data information and protection from spywares feature from spying on you.

Below are the privacy protection features:

A. Date Breach Alert

Data breach means unethical access to the data of individuals and organizations that are supposed to be secured from cyber criminals. Using the Data Breach Alert feature, you can check whether your data is ever breached or leaked online.

To configure Data Breach Alert, follow these steps:

1. Open **Quick Heal Mobile Security**.
2. On the Dashboard, navigate to **Privacy Protection > Data Breach Alert**.
3. By default, the email address that is already configured on your device is selected. If you want to check for data breaches against a specific address, then select the radio button corresponding to that email address and tap the 'Check for Data Breaches' button.
4. If you want to check for data breaches with another email, then select 'Enter email id' and enter the email address.
5. Tap **Check for Data Breaches**. The feature checks if your email address has ever been leaked online and notifies you if a breach is found.
   - If breaches are found against the searched email address, then the 'Data Breach Found' screen will display the number of breaches.
   - If no breaches are found against the searched email address, then the 'Data Breach Not Found' screen will be displayed.

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

Finally, recommendations are mentioned om how to secure your data in case of data breach.

6. You can use the option Stop Monitoring to stop monitoring for data breaches.

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.

Step 3

Change the password of the affected email address on its website or app.

B. Privacy Advisor

The Privacy Advisor detects those applications that collect your personal information such as usernames, contacts, and passwords. You can also get notifications about the applications on your device that can send SMS, call people, or access the Internet without your knowledge.

Additionally, it helps you monitor various permissions granted to every application such as Access to Google Accounts, Access to Contacts, Read Identity Info, Tracking Location, Access to Messages, and Access to Network.

You can modify the permissions using Privacy Advisor as it flags applications in three risk types:

- **High Risk Applications**: These apps collect your identity and personal data and its misuse may cost you money or these apps can act as spyware to spy on your activities.
- **Medium Risk Applications**: These applications collect sensitive permissions, and you may risk your privacy by allowing these app permissions.
- **Low Risk**: These applications collect permissions which are not risky for your device.
- **Trusted Applications:** These applications are flagged as trusted by you.

Configuring Privacy Advisor

To configure Privacy Advisor, follow these steps:

1. Open **Quick Heal Mobile Security.**
2. On the Dashboard, navigate to **Privacy Protection > Privacy Advisor**. Tap **Privacy Advisor.**
3. 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 the Dashboard, navigate to **Privacy Protection > Privacy Advisor**.
3. Tap either of these permission categories: **High Risk Applications**, **Medium Risk Applications** or **Low Risk Applications**. The list of applications for that category appears.
4. Tap the application for which you want to view/modify the permissions. The permissions are displayed.

- If you find that an app uses any crucial information, you can uninstall that app by tapping **Uninstall App**.
- If you find the app trustworthy, then you can trust the app by tapping **Trusted App** and in confirmation screen tapping **Yes**. This app will be added to the Trusted Apps List.

The various permissions that an app may use are as follows:

Permissions	Description
Access to Google Accounts	Apps with this permission may request authentication credentials of the Google 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 & compromise your data.
Read Identity Info	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 them.
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.

C. Anti-Spyware

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

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

For this, always keep the Anti-Spyware option enabled, so you get a notification in case they are turned on.

To configure Anti-Spyware, follow these steps:

1. Open **Quick Heal Mobile Security.**
2. On the Dashboard, navigate to **Privacy Protection > Anti-Spyware**. Tap **Anti-Spyware.**
3. Enable toggle button to enable the feature.

Navigation

The Hamburger menu items can be accessed by tapping the **Hamburger** icon on the upper left corner. The menu helps you navigate to the settings, metaProtect, about, license details, help & support and feedback.

1. Settings

This section contains the settings for the following features:

A. General

You can configure the following options:

i. Reset PIN

You can reset your device PIN. Enter current PIN, new PIN, and confirm new PIN to change the PIN to access the device.

ii. Application Notifications

You can enable this button to allow app and ongoing notifications to be displayed.

iii. Application Statistics

You can enable this button to allow app to send app usage statistics to Quick Heal servers. This information helps Quick Heal improve the product and make it work better for you.

iv. Block Uninstallation

You can enable this feature to block any attempts by unauthorized users to uninstall the Quick Heal Mobile Security application from the device.

B. Feature Settings

You can configure the following features on your device:

a. Deep Scan

A deep scan checks all areas of your device, including all files, pictures, videos, and apps, to detect any virus or threat. You can schedule the scans at required intervals to run automatically.

i. Schedule a Scan

Select Schedule a scan, the following scheduling options are displayed. Select as

required. Tap the Edit Pencil icon to set the time on the displayed clock for the day, week, and month options as required.

- Scan while charging
- Once a day
- Once a week
- Once a month

ii. Delete Quarantined Files

Quarantined files are suspected malicious files that are encrypted and moved to a secure folder where they cannot be executed and cannot infect other files.
Select a duration post which these files are automatically deleted to save on your system space.

- After 7 days
- After 30 days
- After 45 days

b. App Lock

You can configure this option to set up a PIN or a Pattern lock to prevent unauthorized access to a particular app on your device such as WhatsApp, YouTube etc.

i. Unlock Using

- PIN: If you have setup a PIN for your device, you will see a Change PIN option to change the PIN to access the device.
  For more information, see Changing PIN.
- Pattern: You can select a specific pattern to be swiped on your keypad to access the device. Tap **Change Pattern** to set a pattern to use the device.
  For more information, see Change Pattern.

ii. Scramble Keyboard

Select this option to randomly change the position of keys on keypad while entering the PIN so that overlookers cannot memorize the PIN by looking at the position.

iii. Show Prompt

Select this option to show a lock option for newly installed apps.

c. Anti-Theft

First you need to enable this feature by toggling the feature button from the **Data Protection > Anti-Theft** menu. The following options are displayed for Anti-Theft settings:

i. Block on Airplane Mode

Enable this feature to block your device when stolen/lost. When any user tries to switch off the Airplane Mode, your device will be locked and you can open it via your secure PIN/password only.

ii. Emergency Contact Details

Enter any two mobile numbers that will be visible on your blocked device if lost/stolen. Anyone who may find your device can contact you via these contact details.

iii. Log on to metaProtect

Tap this option, and you are navigated to the metaProtect website that enables you to remotely monitor and manage the safety of all your devices from a single dashboard.

d. Parental Control

Parental Control features enable you to restrict access to any website, mobile app on your device which you don't want your children to open. Additionally, you can set up time limits for using your device post which device gets automatically locked.

To configure Parental Control:
Select the browser that will be used to browse the Internet on your device. All the restriction applied using Parental control will be valid for the selected browser. Choose browser options based on the security requirement from the following:

i. Moderate Security

Use a standard Browser: Standard browsers such as Chrome, Mozilla etc. offer medium security and limited parental control where some fake websites may not get blocked.

ii. High Security

Use Quick Heal Browser: Quick Heal browser provides complete security, and complete parental control of all harmful websites will be blocked by default.

iii. Block Play Store

If you want no new apps can be downloaded on your device without your permission. Select this option to block apps from being downloaded or installed from Play Store on your device.

e. Intruder Alert

First, you have to enable this feature on your device if not done already. Grant access permissions to enable Intruder Alert.
To get the secret selfie of anyone trying to unlock your device, provide an email address. Images of the intruder will be sent to your registered email address.

f. YouTube Supervision

You can control the usage of YouTube on your device such as blocking a channel, video. Simply configure restrictions based on your requirement from YouTube Settings.

For e.g., Block YouTube shorts from being played out on the device by enabling the block option for YouTube Shorts.

2.Go to metaProtect

Tap this feature, you are navigated to the metaProtect website. You can access the metaProtect website using your username and password, that you set up during registration. If you do not have a metaProtect account you can create a new account.

To access your metaProtect account or create a new account, follow these steps:

1. Tap **Go to metaProtect**. You are redirected to the metaProtect website.
2. If your account is already created on metaProtect, enter your mobile number/Email and password and then click **Sign in**.
3. Alternatively, you can sign in with your Google account also or sign up with a new account by clicking the **Sign Up** link. You are redirected to the Sign-up page. For more information, click here.

3. About

This section displays the following information about the product:

- Build version and the types of protection provided by Quick Heal
- Virus Definition and option to update database of virus definitions
- Option to share Quick Heal App with friends
- Legal information such as End User License Agreement
- Option to uninstall Quick Heal using the **Uninstall** button

4. License Details

This section displays the following details about Quick Heal license:

- Product Key and Premium Validity
- Licensed to (Tap **Update** to update the user details such as username, email address and phone number)
- Purchase Details

5. Help and Support

You can access the following support options for this product.

i. FAQs

View the Frequently Asked Questions about this product. Click here to access FAQs.

ii. Online Help

View the online help pages for this product. Click here to view the online help.

iii. Live Chat

Chat online with our support staff.

iv. Enable App Logs

Enable this option to share application logs with Quick Heal. These logs are helpful to troubleshoot the issues faced by customers.

v. Call Us

The Toll-free telephone numbers and the support timings for calling support team

6. Feedback

Submit your feedback about using this product.

metaProtect

1. Introduction

Quick Heal metaProtect enables you to manage and monitor the security of all your digital devices remotely via a single dashboard. You can also manage device protection of all your family members along with their license subscriptions, view device reports, and access various other important security features.

A. Signing Up on metaProtect website

1. To sign up for metaProtect website, you can select either of the following:
   - Access the metaProtect website at https://metaprotect.quickheal.com/
   - Access the metaProtect website through device. On the hamburger menu, tap **Go to metaProtect**.

     You are redirected to the sign up page on metaProtect website.
2. Click the **Sign up** button.
3. Enter your name, product key, and email address.

   Note: Username should start with alphabet, may contain special characters, numbers and must not exceed 50 characters in length.
4. You are required to validate your email address by an OTP sent on your specified email address.
5. Enter valid mobile number.
6. Enter and confirm your password.
7. Click **Create Account** to successfully create your account.

   Next, use your registered email address and password to login to metaProtect. You can also sign in using your Google or Facebook account.

B. Signing In to metaProtect through device

1. Open **Quick Heal Mobile Security**.
2. On the Hamburger menu, tap **Go to metaProtect**. You can also access metaProtect through the link on Parental Control and YouTube Supervision feature.

You are redirected to the metaProtect website.

3. Enter your mobile number/email address and password.
4. Click **Sign In**.
   The metaProtect dashboard is displayed.

2. Profile

You can access your profile details through the Profile icon on the upper right corner of the website. You can view or edit your account details. Use the **Logout** button to logout of metaProtect.

A. Viewing/Editing My Account details

1. Open **Quick Heal Mobile Security**.
2. On the upper right corner, click the **Profile** icon.
3. Click **My Account**. Your account details are displayed.
4. Click the **Edit** icon for the corresponding field if you want to edit the details.
5. Click **Save**.

B. Changing your password

1. Open **Quick Heal Mobile Security**.
2. On the upper right corner, click the **Profile** icon.
3. Click **Change Password**.
4. On the **Update Password** dialog box, enter your old password, your new password, confirm password.
5. Click **Update Password**. Your password is updated.

3. Dashboard

This is the default screen that appears when you log on to metaProtect. The dashboard displays the overall device health and the features that you can use to manage your devices remotely.

A banner on the top of dashboard displays real time important information about the product such as expiry status of licenses.

A. Device Health

This section includes Security and Privacy scores, recommendations, and related details.

Security score: It indicates the level of protection your device has against viruses, malware, and other malicious programs.

It offers personalized recommendations that you need to act on to protect your device. To achieve a high security score, enable maximum recommendations that are offered.

Privacy Score: It indicates how safe is your data and digital identity on your device.

It also offers easy to understand recommendations that you need to follow to achieve a high privacy score.

- To view recommendation details for the devices, follow these steps:
    1. In the left pane, click **Dashboard**.
    2. On the **Device Health** screen, click **View Details**.

You can view the recommendations for another device by selecting the device from the device drop-down on the upper right corner.

- To sync the score of devices with metaProtect, click **Sync score**.

B. Device Features

This section offers a range of security features that enables you to manage your device remotely.

To use these features, follow these steps:

1. On the Dashboard, select the device from the device drop-down on the upper right corner.
2. Navigate to the **Device Features** section.
   The available features are displayed, on a horizontal moving banner that moves to the left.
3. Navigate to the feature that you want to use by clicking the corresponding feature icon on the moving banner.

   The feature page is displayed with the available options for that feature.
4. Click the corresponding action buttons for that feature.

   The following table describes the features and the available options.

Feature	**Description**
Locate	Track the location for the selected device with location age, date, time, and real-time location on the world map. Follow below steps to get device location: • Enable location tracking for the device using **Trace Device** toggle button on upper right corner. • Refresh the page with latest location. • Select the duration from the drop-down list, for which you want to view the location history. • Click **Delete All** to delete the location history.
Lock	Enables you to lock your device if stolen or lost. You can lock or unlock your device remotely by clicking the corresponding **Lock** or **Unlock** button. *Note: Feature available only if Anti-Theft has been enabled on the device previously.*
Wipe	Enables you to wipe the data on your device if lost or stolen by clicking **Wipe All Data**. *Note: Feature available only if Anti-Theft has been enabled on the device previously.*
Anti-Theft	Enables you to capture photos, surrounding audio and video, and dial calls from your lost or stolen device. The

	following options are available in Total Security only: • Auto Capture Image: Click **Auto Capture Image** to capture the image of an unauthorized person who tries to access your device when lost or stolen. • Auto record Audio: Click **Auto Record Audio** to record the audio from the device to know about its surroundings when lost or stolen. • Auto record Video: Click **Auto Record Video** to record the video from the device to know about its surroundings when lost or stolen. • Auto Dial: Click **Auto Dial** to dial a call from the lost or stolen mobile to the mentioned mobile number. This is applicable only for Android versions 9.0 and lower. *Note: Features available only if Anti-Theft has been enabled previously.*
Update VDB	Click **Update** to update the virus database on your device to the latest database available on Quick Heal Cloud.
Scan Device	Click **Scan Now** to scan the device storage folders for viruses.
Sync Score	Click **Sync Score** to sync the latest score from device to cloud. Refresh the page to view the latest scores.
Sync	Click **Sync Now** to sync device information.
Ring Device	Click **Ring Device** to ring a bell on the device. This can help you locate the device if nearby.

C. Dynamic Content

Announcements related to the new product release and related features, articles and blogs related to latest happenings in the cyber world, and Quick Heal products with price and buying options appear dynamically. Additionally, offers and surveys are displayed.

4. Users

The user who logins to metaProtect portal first becomes the super admin. It can add other users and assign roles to the users as required. It can view devices and license details of all other users.

A. Adding User

To add a user, follow these steps:

1. On the left pane, navigate to **Users** > **Add User**.
2. Enter the name, select a role, and email address.
   You can assign role of admin, member, or child to the user.
3. Click **Add**.

   An invitation is sent to the specified email address. The user status will be shown as pending till the user completes the account setup process.
4. Click **Done**.

B. Activating newly added User Account

Users who are sent an invitation receive an email on how to set up their metaProtect account.

1. Click **Setup Account** button in your mail.
2. You are redirected to the metaProtect website with the name and email address prefilled.
3. Enter and confirm a password.
4. Click **Sign Up** and your account will be successfully created.

C. Viewing User details

1. On the left pane, navigate to **Users**.
2. Select the User to view the user details. The following details are displayed for every user:
   - Name
   - Role
   - Email
   - Phone Number
   - Age
   - Gender

D. Deleting a user

1. On the left pane, click **Users**.

   You are redirected to the Users page.

2. Click the user that you want to delete. The user details are displayed.
3. Click **Delete User**. The selected user is deleted.

E. Viewing device details

You can view details for your own devices as well as for other user devices added to your account. Follow below steps to view device details:

1. On the left pane, click **Users.**

   You are redirected to the Users page.

2. Select the user and click **View Device**.

   You are redirected to the Devices page.

   The following details are displayed for the selected user device:

   - Device Name
   - Phone Number
   - Product Name
   - Product Key
   - OS and Model
   - Make
   - IMEI
   - Wireless Mac Address
   - SIM number
   - Total Space

F. Viewing License Details

1. On the left pane, click **Users**.

   You are redirected to the Users page.

2. Click **View License** and your license details will be displayed.

5. Devices

Your device details are listed in My Devices section. The User Devices section contains the details of user devices that you have added.

You can add remove, transfer ownership of devices and manage the displayed device features.

A. Adding Devices

1. On the left pane, click **Devices.**
2. Click **Add Device** on the upper right corner.
3. Enter your device name and corresponding product key.
4. Click **Add**.

   Your device is added and listed in the devices section.

B. Viewing device details

You can view details for your own devices as well as user devices.

1. On the left pane, click **Devices**.

   You are redirected to the Devices page.
2. You can select the device from **My devices** or **User Devices** section to view the details.

   The following details are displayed for the selected device:

   - Device Name
   - Phone Number
   - Product Name
   - Product Key
   - OS
   - Model
   - Make
   - IMEI
   - Wireless Mac Address
   - SIM number
   - Total Space

C. Transferring ownership of device

1. On the left pane, click **Devices**.
   You are redirected to the Devices page.
2. Click the device for which you want to change ownership.
3. To transfer the device ownership to a new user, click **Transfer Ownership**.

   Transfer Ownership dialog box is displayed.
4. Select the new user and click **Transfer**.

   The device is transferred to the new user.

D. Removing a device

1. On the left pane, click **Devices**.
   You are redirected to the Devices page.
2. Click the device and click **Remove Device**.
3. Click **Delete** on the confirmation dialog box.

6. Score

The score tab displays the security and privacy scores for your devices and user devices. Here you can do the following:

- **View details**: Click **View Details** for each user to view their security score and privacy score with recommendations to improve the scores of the device.
- **Sync Score**: Click **Sync Score** for each user to sync the score details from the device to metaProtect.

7. Reports

metaProtect offers easy to use graphical reports that keep you updated about your device health. Here you get to access the following reports:

A. Parental Control Reports

For all the restriction policies created using Parental Control, you get to see reports in metaProtect. Further, you can schedule parental control reports of your kid's web and app usage on your registered email address as per your schedule.

To schedule a report, follow these steps:

1. Click **Schedule** on the upper right corner of the screen.
2. Click **Add Schedule** on the dialog box.

   You are redirected to the Schedule Report page.
3. Select the report type, report Schedule, start schedule on, end schedule on, time, and enter the email address.
4. Click **Save Changes**.

You can select Web or Application to view the reports. The following reports are displayed:

- Activity Summary
- Web Usage Report
- App Usage Report

B. YouTube Reports

YouTube reporting enables you keep track of usage of YouTube app on your device. You can view time spent on YouTube across different channels. This report gives you the frequency of visits to various YouTube channels and videos.

C. Screen Time Reports

Screen time reports give you the total time spent on your device. You may view it day-wise or week wise and setup restrictions to cut down on your screen time.

You can schedule the screen time report that is sent to your registered email address as per the schedule. To schedule a report, follow these steps:

1. Click **Schedule** on the upper right corner of the screen.
2. Click **Add Schedule** on the dialog box.

   You are redirected to the Schedule Report page.
3. Select the report type, report Schedule, start schedule on, end schedule on, time, and enter the email address.
4. Click **Save Changes**.

You can view the reports for the following:

- Daily App-wise Goal
- Weekly Screentime Goal

- Weekly App Usage

The report is generated when the date changes.

D. Threat Report

The threat report displays the details of threats captured in your device such as Date, Virus Details and Status of the threats. Also, the Threat Types Report displays a pie chart with different threat categories and their percentage.

8. License

You can view your license details in two sections as follows:

- My Licenses: License of the Admin user devices.
- User Licenses: License details of the user devices added by the Admin.

  The following details are available:

  - Name and Email
  - Phone Number
  - Product Name and Build Version
  - License Validity and Activation Date

You can renew the license if expiring or expired by clicking the **Renew** button.

9. Features

You can manage the device settings from metaProtect and apply (publish) to the devices as required. You can publish the settings for the following features:

A. Screen Time

You can set up screen time limits on your device using metaProtect.

To configure the settings, follow these steps:

1. On the left pane, navigate to **Settings > Screen Time**.
2. Click **Set Daily Screen Time** to set the time.
   - Select the hours and minutes from the drop-down list of **Set Time Goal**.
   - Set the time in HH/MM. Click **Save** and **Publish Now** to ensure that the settings will be reflected on your device.

3. Click **App Time** to view the apps for which the monitoring of screen time is enabled. It is a read only setting.

B. Scan

You can scan the devices for any viruses, and threats.
To scan the device, follow these steps:

1. On the left pane, navigate to **Settings** > **Scan**.
2. Enable the **Schedule a Scan** toggle button.
3. Select one of the following to schedule the scan as required:
    - Scan while charging
    - Once a day
    - Once a week
    - Once a month
4. Select one of the following to delete quarantined files:
    - After 7 days
    - After 30 days
    - After 45 days
5. Click **Save** and **Publish Now**.

C. Anti-Theft

You can configure the Anti-Theft settings to get updates in case your device gets stolen or lost.

To configure the settings, follow these steps:

1. On the left pane, navigate to **Settings > Anti-Theft**.
2. Enable **Anti-Theft** toggle button.
3. Select the **Block on Airplane Mode** to block the device if airplane mode is turned on by the unauthorized user.
4. Enter the Primary number and alternate numbers.
5. Click **Save** and **Publish Now**.

D. Device Optimiser

You can enable Battery Saver so that your battery lasts longer.

1. On the left pane, navigate to **Settings > Device Optimiser**.
2. Enable the **Battery Saver** toggle button.

E. Smart Parenting

You can configure parental control settings to manage the digital content that your kids can view online.

To configure the settings, follow these steps:

1. On the left pane, navigate to **Settings > Smart Parenting**.
2. Enable the **Smart Parenting** toggle button.
3. Click **Restrict Categories** and select the categories to block the kids from accessing the selected categories. For example, Adult, Crime and Violence, Games. You can select **Select All** option to block all the categories.
4. Click **Excluded Websites**.
   - Enter the website URL and click **Add URL/Website**.
   - You can delete the added URL by clicking the delete icon.
     Note: Added URLs are reflected on the device only when you save the settings.
5. Click **Block Particular Website**.
   - Enter the website URL and click **Add URL/Website**.
   - You can delete the added URL by clicking delete icon.
     Note: Added URLs are reflected on the device only when you save the settings.
6. Click **Set Browser for Parental Control**.
   - Select **Standard Browsers allowed** for moderate security or **select Use a Quick Heal browser** for higher security.
7. Click **Block App Categories** and select the categories to block the kids from accessing the selected app categories. For example, Art & Design, Comics, Entertainment. You can select **Select All** option to block all the categories.
8. Click **Allowed Apps**.

Allowed Apps setting from metaProtect is read-only. To enlist an app in the **Allowed Apps** list, make the required settings from the device settings.

9. Click **Block new app installs on the device**.

Enable **Block Play Store** to avoid installation of new apps.

10. Click **Save** and **Publish Now**.

*Note: Click **Restore Default** to restore the default settings on the device.*

F. YouTube Supervision

You can monitor and control the content viewed on YouTube by users on their devices using this feature.

To configure the settings, follow the steps:

1. On the left pane, navigate to **Settings > YouTube Supervision**.
2. Toggle the **YouTube Supervision** button to enable the feature.
3. Toggle the **Block YouTube Shorts** button to enable the feature blocking YouTube short videos.
4. In the Restricted section, you can do the following:
   - Block Channels: Add the channel names that you want to block.
   - Block Videos: Add the video names that you want to block.
   - Block by Categories: Select the categories that you want to block.
   - Block Keywords: Add the keywords by which you want content to be blocked when searching.
5. In the Allowed section, you can do the following:
   - Allow Channels: Add the channels that can be viewed.
   - Allow Videos: Add the channels that can be viewed.
6. Click **Save** and **Publish Now**.

G. Online Safety

You can enable Play Store App Advisor, SafePe, Wi-Fi security and Safe Browsing remotely through metaProtect.

1. On the left pane, navigate to **Settings > Online Safety**.
2. Enable the toggle buttons for the following to enable features as required:
   - Play Store App Advisor

- SafePe
- Wi-Fi Security
- Safe Browsing

3. Click **Save** and **Publish Now**.

H. Device PIN

You can change the PIN remotely from metaProtect to prevent unauthorized access of device.
To change the PIN, follow these steps:

1. On the left pane, navigate to **Settings** > **Device PIN**.
2. Enter the PIN and confirm PIN.
3. Click **Save** and **Publish Now**. The new PIN is reset for the device from metaProtect.

I. Privacy

You can remotely enable the device camera to secretly record/click pictures of anyone trying to unlock your device without your permission.

1. On the left pane, navigate to **Settings > Privacy**.
2. Enable the toggle button for **Intruder Alert**.

J. Anti-Spyware

You can set up notifications to alert you if any app is using your camera or microphone without your knowledge or permission.

1. On the left pane, navigate to **Settings > Anti-Spyware**.
2. Enable the Anti-Spyware toggle button to track the unauthorized use of microphone and camera by apps.

10. Activity

You can view the various activities carried out on the metaProtect portal by the admin and the added users. The following details are available under Activity logs:

- User: Displays the name of the user.
- Device: Displays the name of the device.
- Action: Displays the action carried out by the user.
- Description: Displays the information about the action.
- Date and Time: Displays the date and time when the action was carried out.
- Status: Displays the status of the action, whether success, failed.

Filter Options

- To filter results by Status, Action, and Date & Time, click the Filter icon on the upper right corner. Select the options as required and click Apply.
- You can filter results by users and devices by selecting the required options and combinations from the drop-down list of All Users and All Devices.
- You can sort the data in ascending or descending order by clicking the corresponding column names.