

COMODO
Creating Trust Online®



Comodo
Mobile Security for Android
Software Version 3.5

User Guide
Guide Version 3.5.011317

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Table of Contents

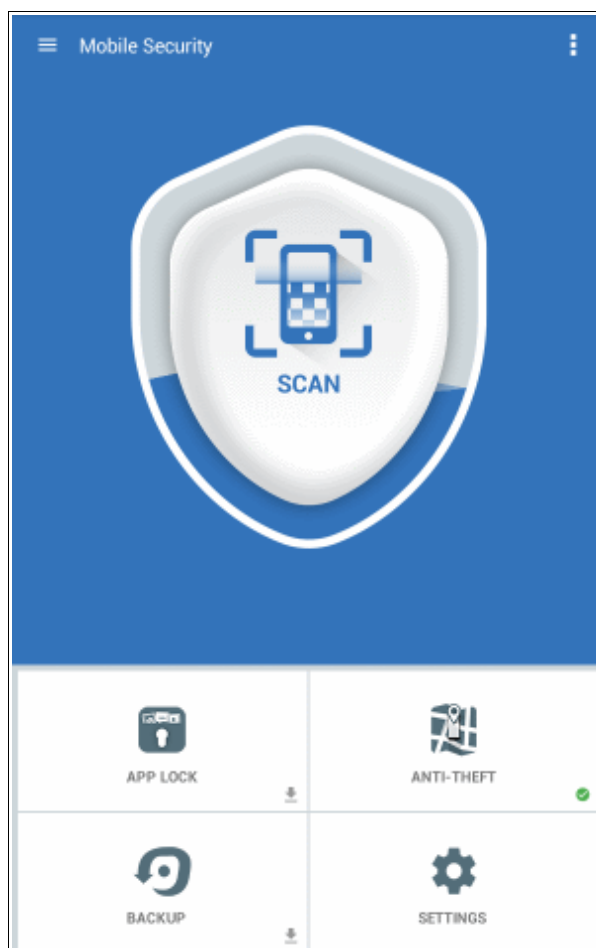
1. Introduction to Comodo Mobile Security	3
2. Downloading and Installing Comodo Mobile Security	5
3. Antivirus Scanner	7
3.1. Running a Manual Scan.....	8
3.2. Scheduling Antivirus Scans.....	12
3.3. Adding Applications to the Safe List.....	14
3.4. Blocking Calls.....	16
3.5. Viewing Antivirus Logs.....	20
3.6. Viewing Activity Logs.....	22
3.7. Configuring the Antivirus Scanner.....	24
4. Secure Browsing	27
5. Anti-theft	29
6. App Lock	30
7. Backup	31
8. About Comodo Mobile Security	32
9. Getting Help	34
10. Terms of Service	35
11. Privacy Policy	36
About Comodo	37

1. Introduction to Comodo Mobile Security

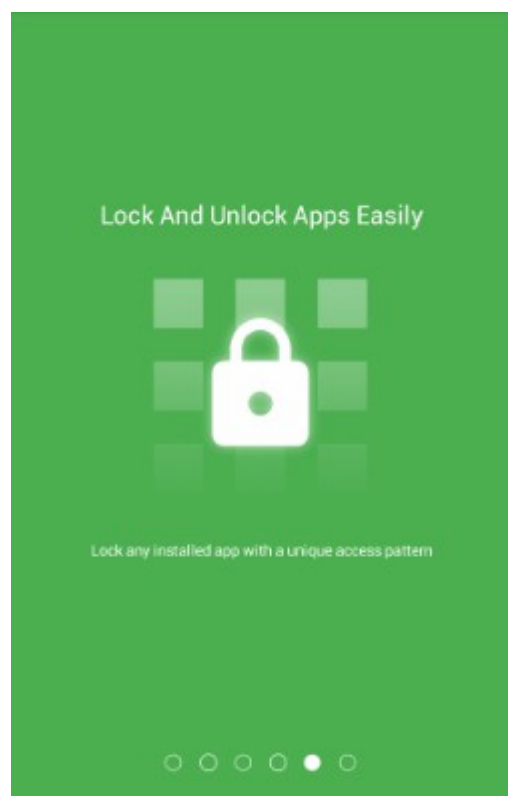
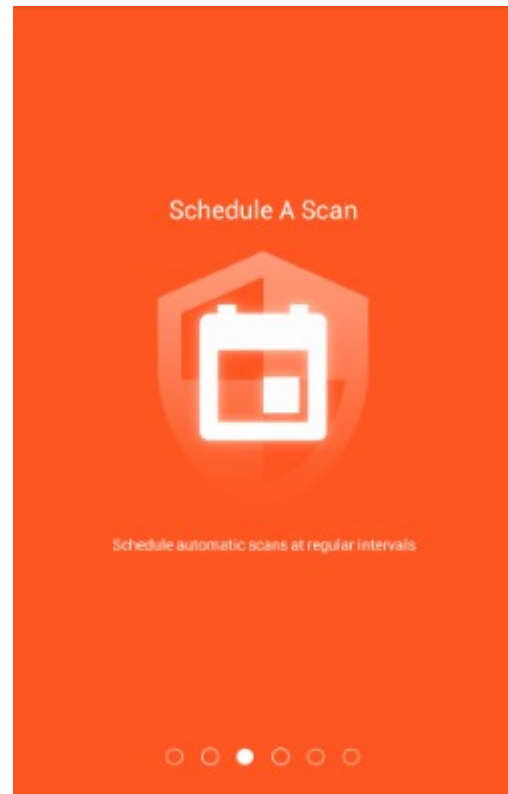
Comodo Mobile Security (CMS) provides Android devices with 'always-on' protection against viruses, worms and scripts.

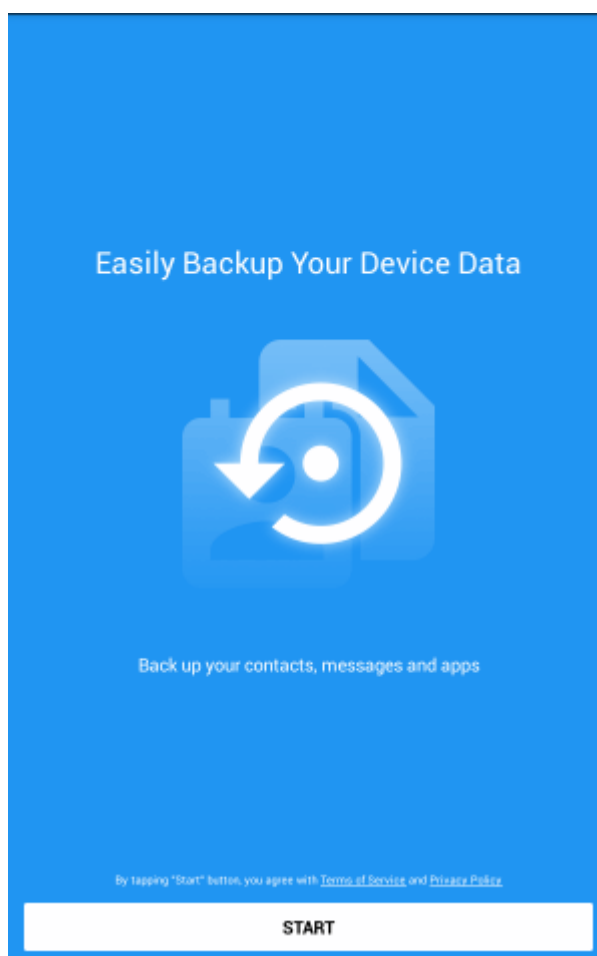
As part of a suite of mobile applications designed to improve the security of your device, CMS also contains built-in links to Comodo's Anti-Theft, App-Lock and Backup apps.

- **Antivirus** - Provides 'Always on' protection against viruses, worms and scripts.
- **Anti-theft** - Locate, lock or wipe your missing Android device to prevent data theft
- **Schedule a scan** – Allows you to run recurring virus scans according to a schedule of your choice.
- **Protect missing device** – Allows you to locate missing or stolen devices.
- **App -Lock** - Secure your apps with a unique pattern to prevent others from accessing them
- **Backup** – Create a reliable backup schedule for valuable data stored on your device



After downloading Comodo Mobile Security, a series of slides will introduce you to its main features:





Please click the following links to jump straight to the area you need help with:

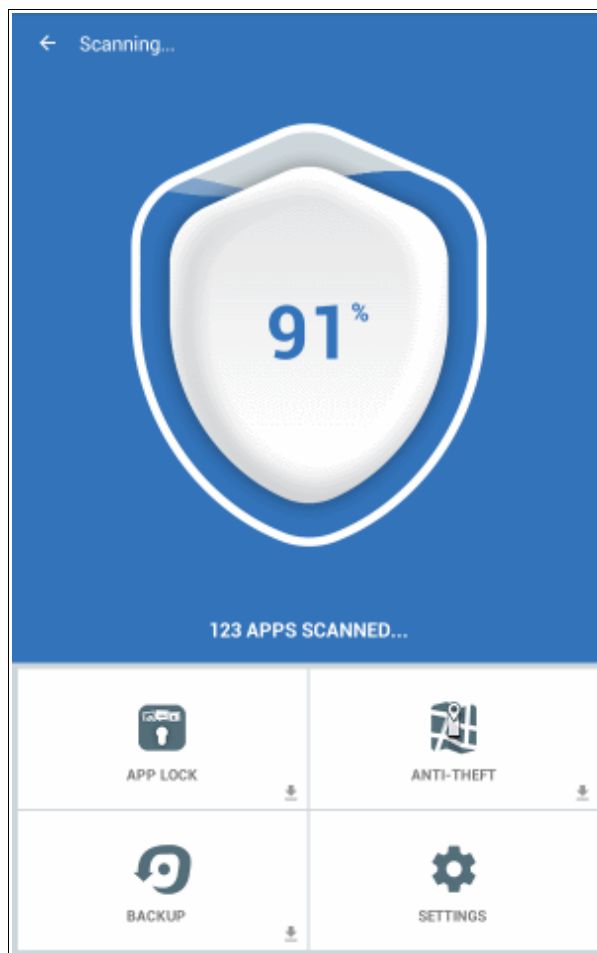
- **Downloading and Installing** - Describes how to download and install Comodo Mobile Security
- **Antivirus Scanner** - How to run antivirus scans and block push-ad apps from appearing on your device
- **Getting Help** – How to access help for the app.
- **Terms of Service** – Displays Comodo Mobile Security's User License Agreement.
- **Privacy Policy** – Displays the policies and practices followed by Comodo.
- **Secure Browsing** – How to block malicious websites.
- **Anti-theft**- Describes how to protect and locate your device in the event it is lost or stolen
- **App Lock** – Describes how to lock individual apps with a lock pattern to avoid others accessing them
- **Backup** - Describes how to backup/restore your valuable data and apps to and from SD card.
- **About Comodo Mobile Security**– Version and support information

2. Downloading and Installing Comodo Mobile Security

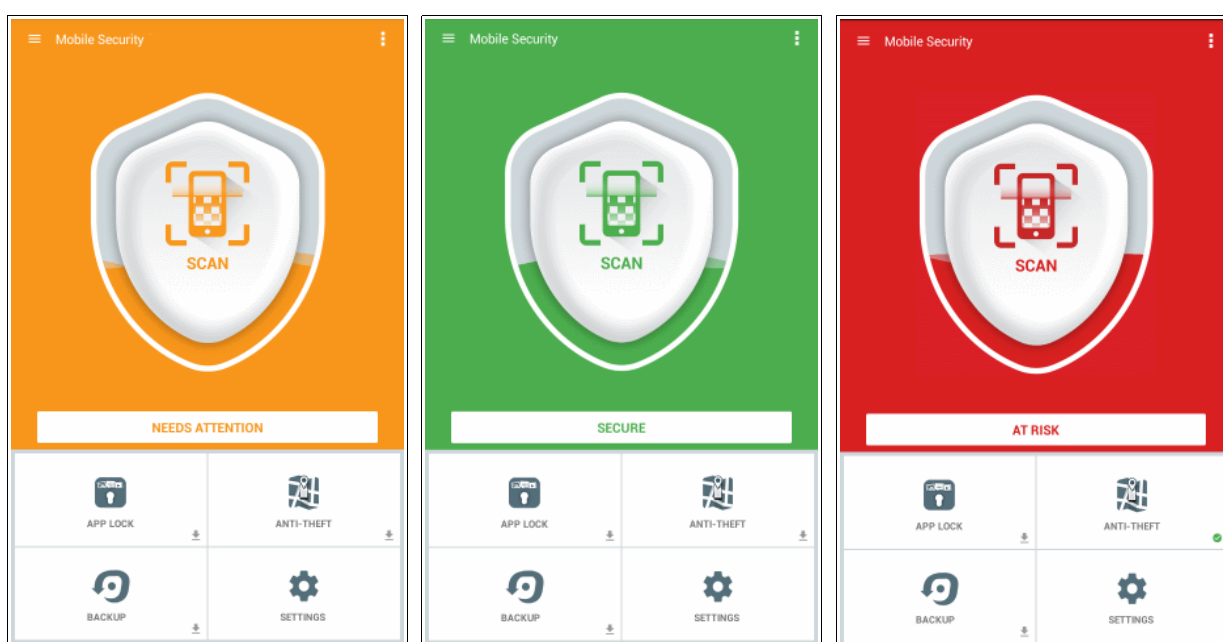
Comodo Mobile Security can be downloaded from Google Play at <https://play.google.com/store/apps/details?id=com.comodo.cisme.antivirus>

Note: You need a Google account in order to download applications from the Play store.

After successful installation, Comodo Mobile Security will automatically begin scanning your device:



The System Status screen indicates the current security status of your device. There are three possibilities: 'Needs Attention', 'Secure' and 'At Risk'.

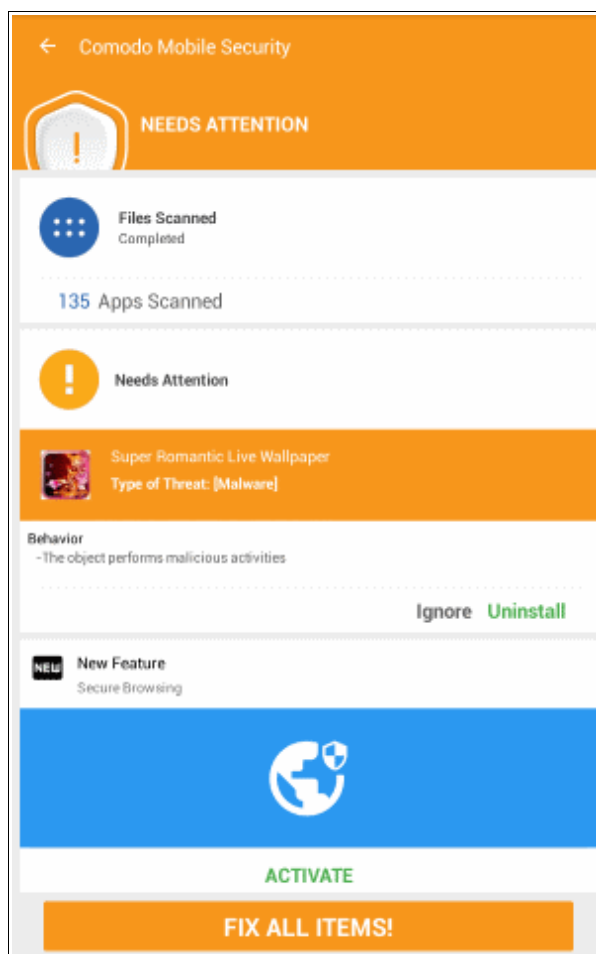


- **Secure** (Green background) means that no threats were detected and the virus database is up to date.
- **Needs Attention** (Yellow background) usually means you need to update the virus database. Please

ensure automatic updates are enabled in 'Settings'.

- **At Risk** (Red background) means a threat has been detected.

You can rectify 'At Risk' and 'Needs Attention' items by first tapping the message 'At Risk'/'Needs Attention' then the 'FIX ALL ITEMS' button. CMS will automatically take the necessary actions to resolve the problem.

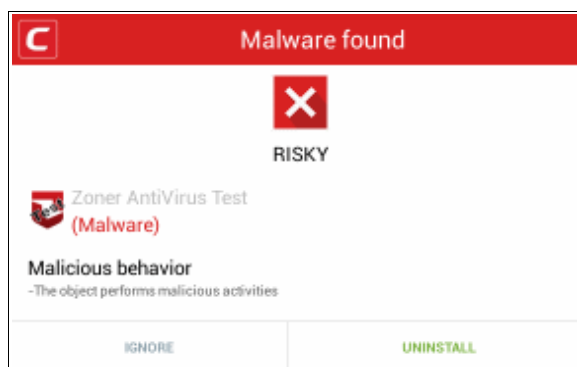


- If malicious items are discovered then you will be asked if you wish to remove or them. Refer to **Antivirus Scanner** section for more details:
- Tap 'FIX All ITEMS' to remove all discovered malware
- Tap 'Ignore' to postpone deletion of the malicious item
- Tap 'Uninstall' to remove a specific malicious app from your device
- Tap 'Activate' to update CMS with the latest new features.

3. Antivirus Scanner

Comodo Mobile Security features 'Always-on' anti-virus protection and an on-demand scanner to make sure your devices stays clear of viruses and unsafe apps. The on-demand scanner features one touch scans of your device and allows you to create scheduled scans.

The real-time antivirus scanner will show instant alerts if an unsafe app is detected:



- If you wish to ignore the warning, choose 'Ignore' and tap 'OK'. You will be alerted again when you next access the app.
- To prevent the app from being installed, choose 'Uninstall' and tap 'OK'. The app will be added to the 'Safe List'. CMS will not scan apps that are on the Safe List. For more details on the Safe List, refer to the section **Adding Files to Safe List**.

Note: For the antivirus scanner to scan the files on access, the 'Real time Protection' should have been enabled under Settings. Refer to the section **Configuring Antivirus Scanner** for more details.

Click the links below for help with common tasks:

- [How to run an on-demand antivirus scan](#)
- [How to schedule antivirus scans](#)
- [How to block calls](#)
- [How to add apps to Safe List](#)
- [How to view activity logs](#)
- [How to check the logs](#)
- [How to configure Antivirus Scanner](#)

3.1. Running a Manual Scan

A manual virus scan detects viruses, push-ad apps and unsafe apps on your device. By default, CMS will scan device storage, memory and any SD cards.

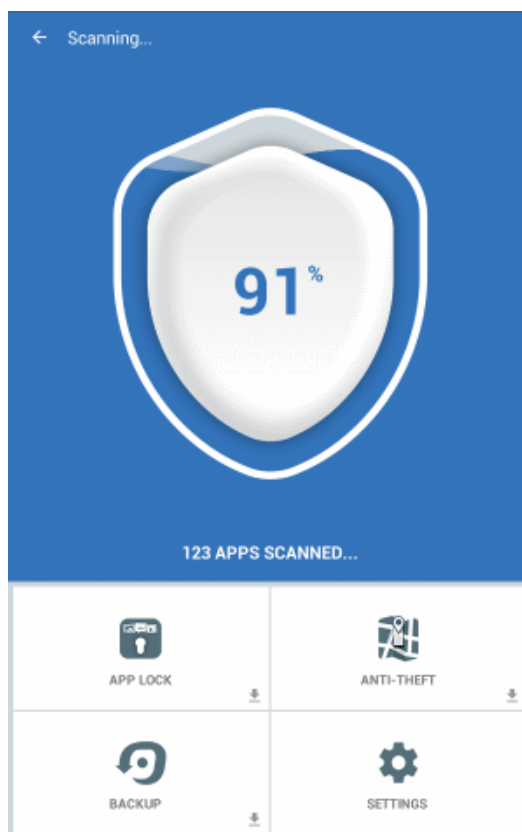
To run an antivirus scan



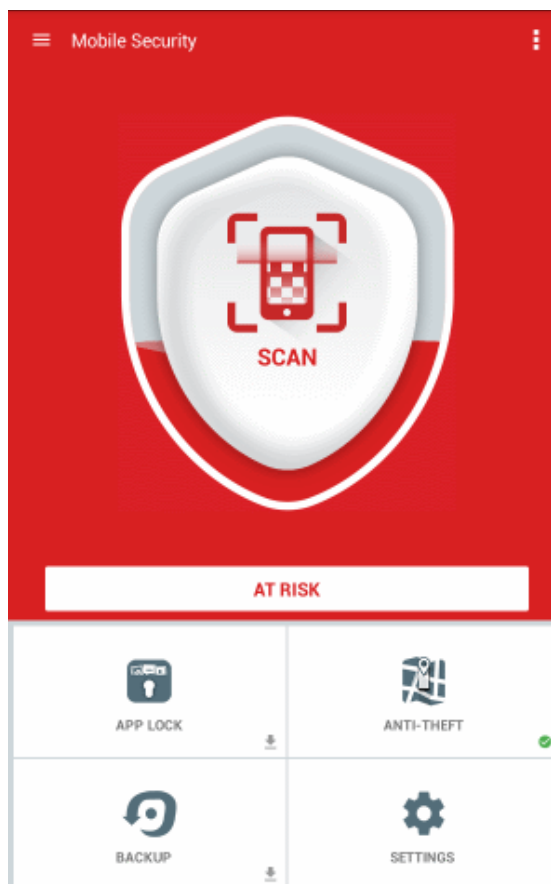
- Tap the scan icon from the home screen. The scan will run according to the settings configured in **Antivirus Settings**.

You will see a progress indicator when the scan is running:

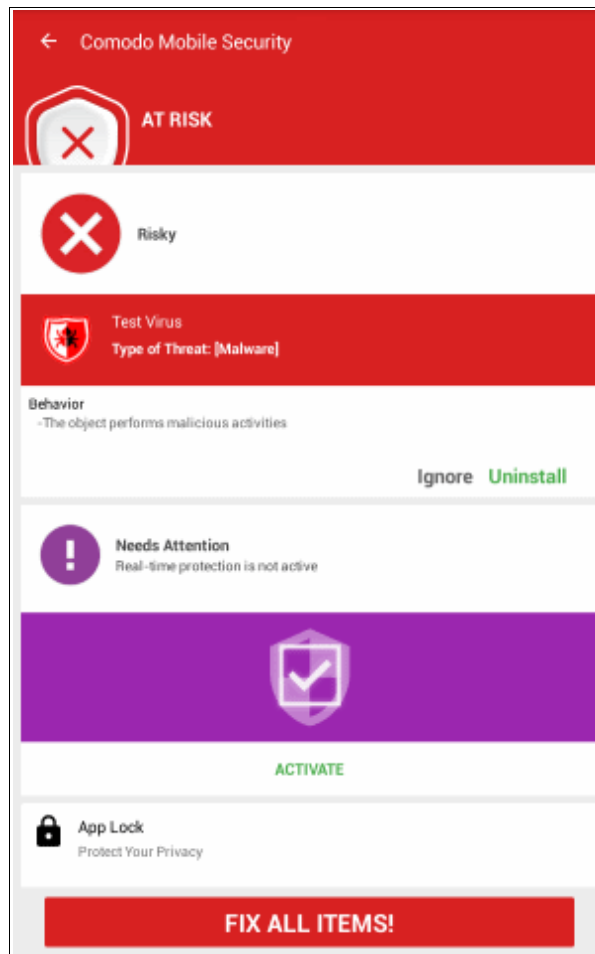
- You will see a progress indicator when the scan is running:



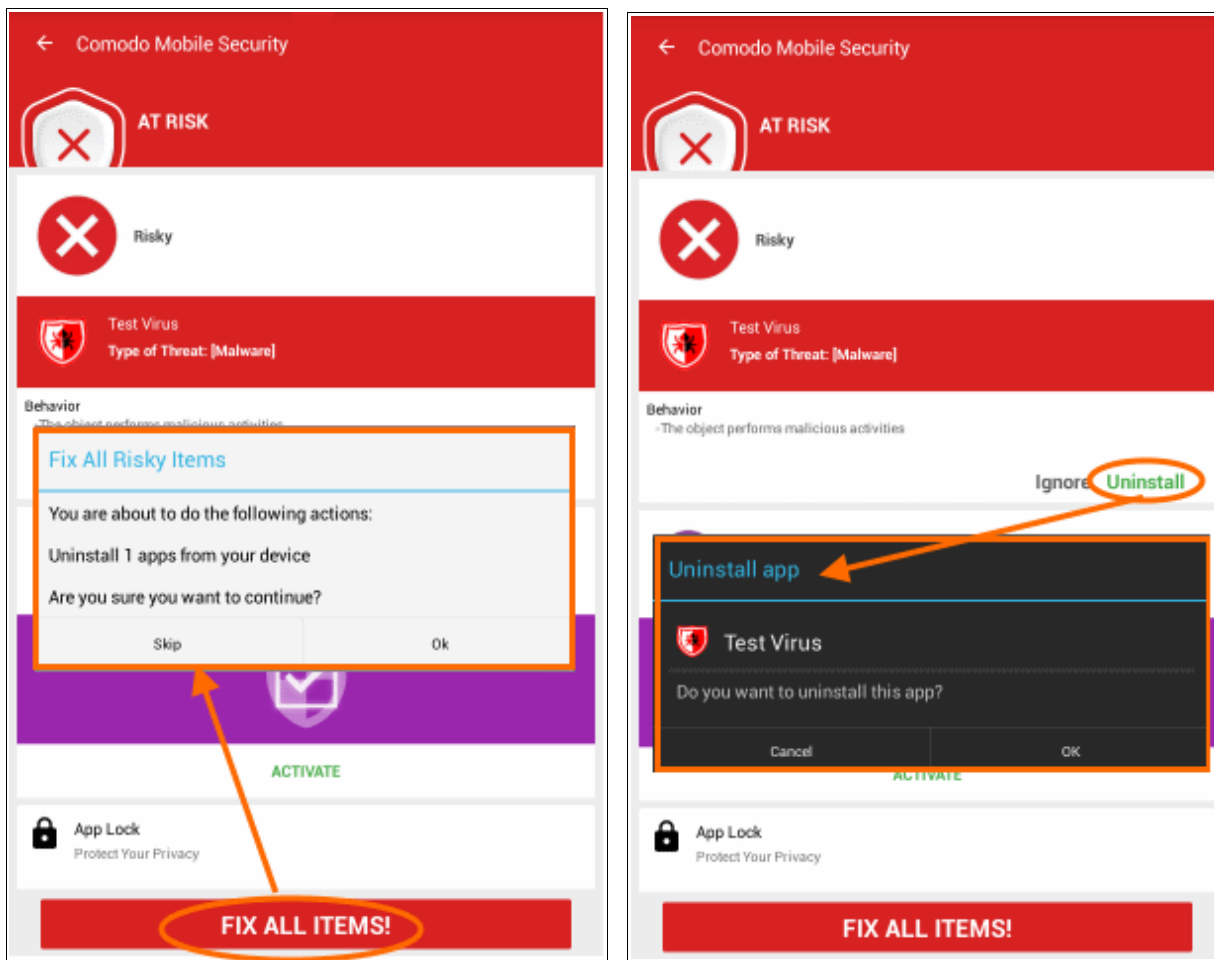
A result screen is displayed when the scan is finished:



- If threats were discovered, click the 'At Risk' button to remove them all.
- If no threats were found, tap the 'OK' button to return to the home screen.



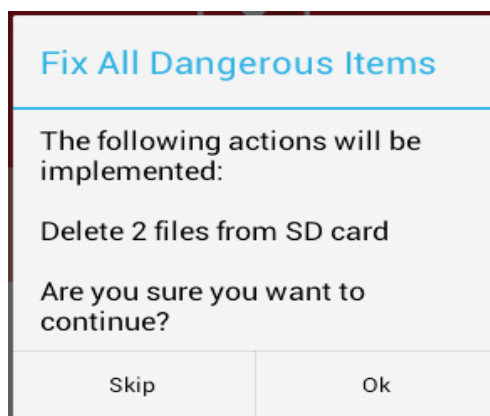
- To remove all items, tap 'FIX ALL ITEMS'
- You can deal with items individually by touching an item in the list to reveal further options:



- To uninstall the app/delete the file from the device/SD card, choose 'Uninstall' or 'Remove' and tap 'OK'.
- If you wish to ignore the warning at this moment, choose 'Ignore Once' and tap 'OK'. You will be alerted again when you next access the app.
- If you are confident that the app is safe, choose 'Ignore Permanently' and tap 'OK'. The app will be added to the 'Safe List'. CMS will not scan apps that are on the Safe List.

Please note that infected files detected on an SD card can only be removed and cannot be added to safe list.

A confirmation dialog will be displayed for removing the items.



- Tap 'OK' to continue

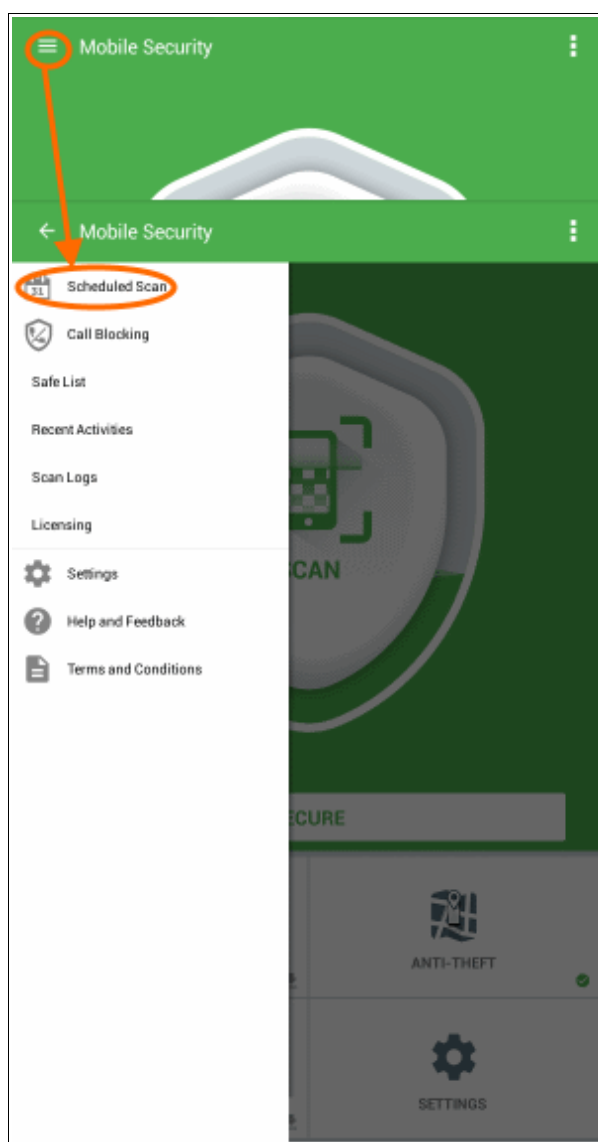
The selected items will be uninstalled from your device one-by-one.

3.2. Scheduling Antivirus Scans

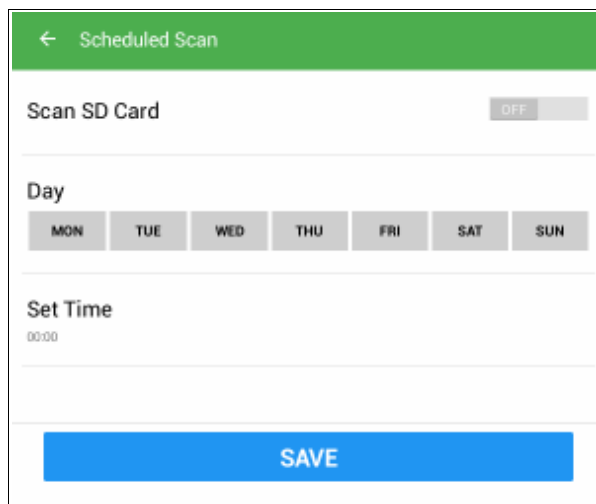
Comodo Mobile Security allows you to schedule automatic virus scans on your device. You can timetable scans to run every day or on specific days of the week at a preset time. You can view results of scheduled scans by tapping the notification in the notifications area.

To create a scan schedule

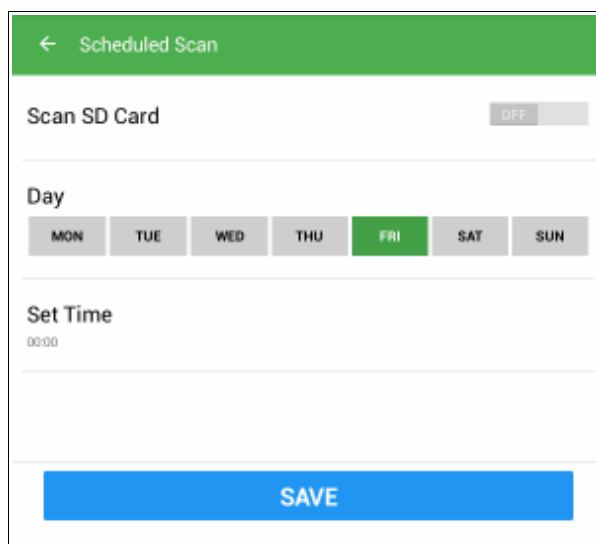
- Tap the menu button at the top left to open the menu bar
- Tap 'Scheduled Scan' from the menu bar:



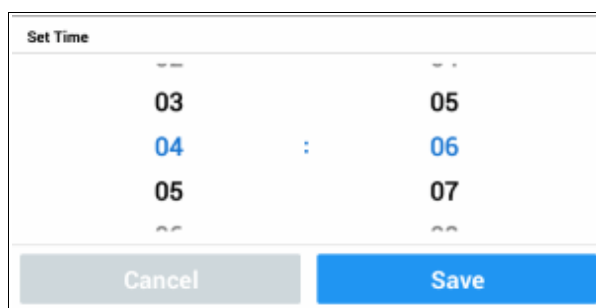
This will open the 'Scheduled Scan' screen:



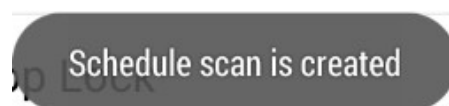
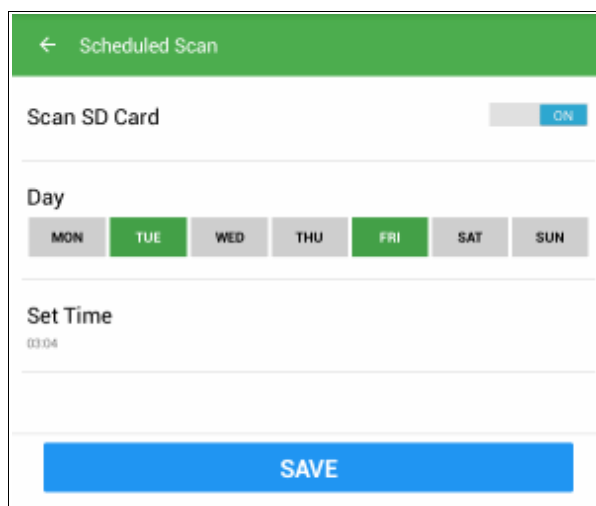
- If you want to scan items on your SD card during a scheduled scan, move the 'Scan SD Card' slider to 'On'.
- First, choose the day(s) of the week on which the scans should run. You can select multiple days.



- Tap anywhere in the 'Set Time' bar to specify the time at which the antivirus scan should commence on the selected day(s)



- Set the time in HH:MM format and tap 'Save' in the 'Time' dialog
- Tap 'Save' to confirm and implement your scan schedule:



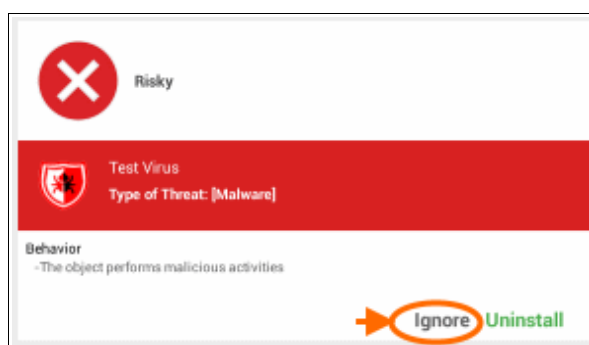
Antivirus will run automatically at the times you have specified. Scan results can be found in the notifications area. Tapping the notification will open the 'Scan Results' interface. Refer to the description of Scan Results in the previous section '[Running a Manual Scan](#)' for more details on handling the threats identified during automated scans.

3.3. Adding Applications to the Safe List

CMS allows you to add trustworthy apps to the safe list in order to exclude them from scanning. This option is available in the results screen of antivirus scans and in the warning screen that is shown if you try to install a dangerous app. Once a app is added to the safe list it will be skipped in subsequent virus scans.

From a real-time scan alert

- To whitelist an app from a malware alert, choose 'Ignore Permanently' and tap 'OK'

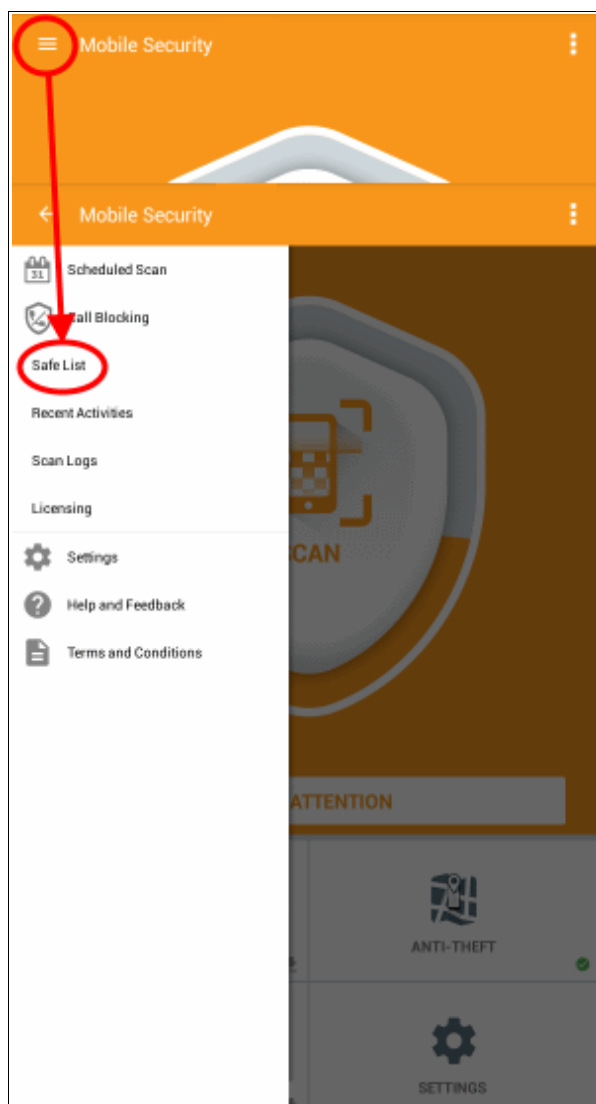


From the scan results screen

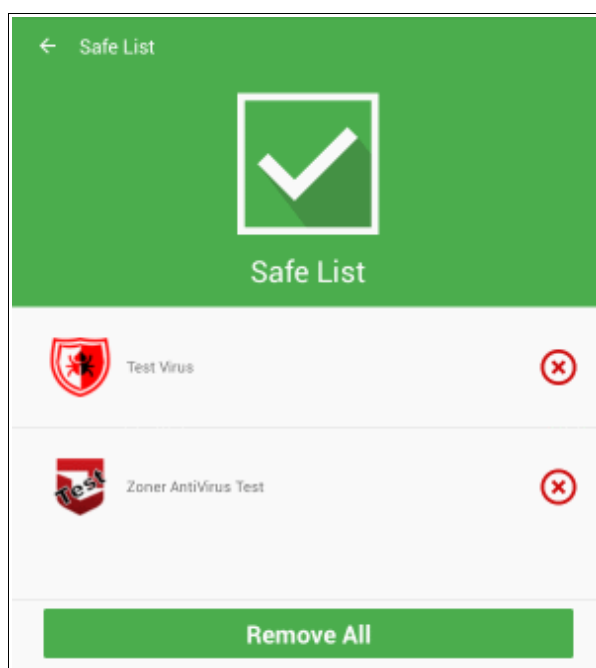
- To whitelist an app from the scan results screen, first tap the 'At Risk' button, then click the item in the 'scan results' you wish to whitelist:
- Choose 'Ignore' to add it to the safe list and tap 'OK'

To view and manage the Safe List

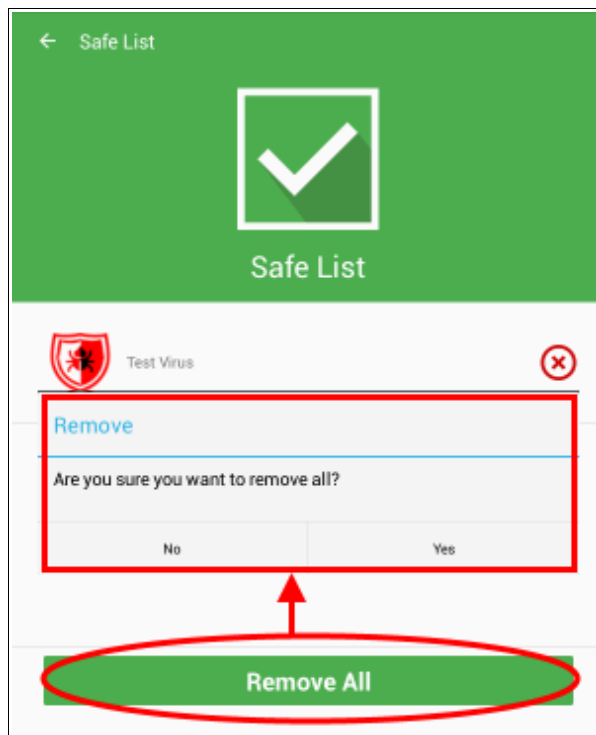
- Tap the menu button at the top left to open the menu bar
- Tap 'Safe List' from the menu bar:



The list of apps added to 'Safe List' will be displayed:



- To remove an individual app from the list, touch the 'X' button beside it
- To remove all the apps from the list at once, tap 'Remove All'.



- Tap 'Yes' in the confirmation dialog to remove the apps from the list.

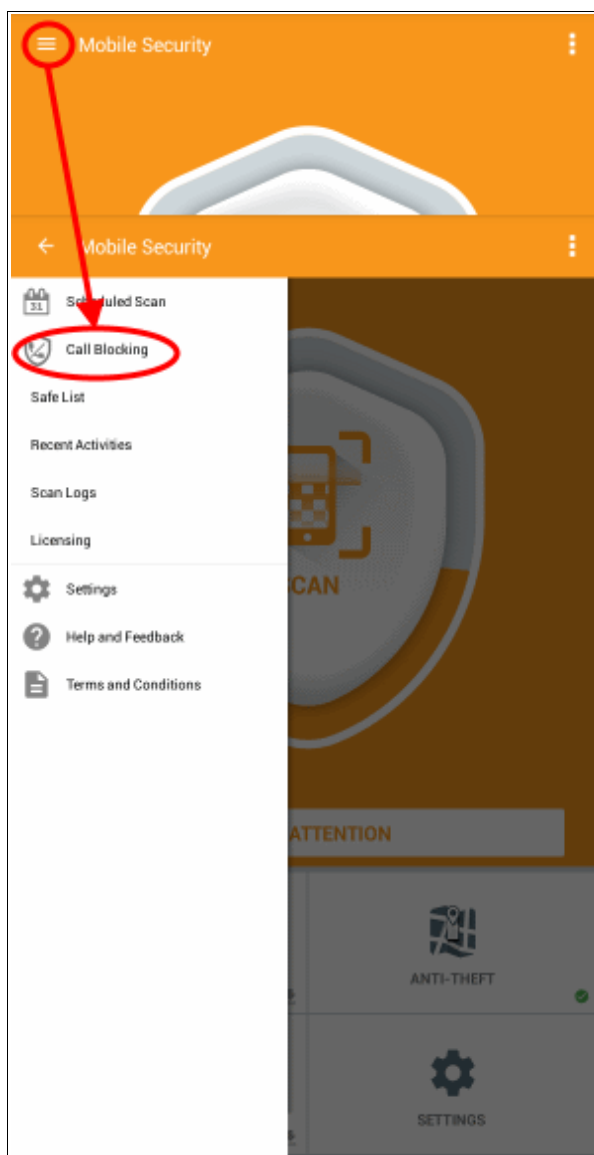
Note. Removing an app from the safe list does not remove it from your device, but means it will be included (and possibly flagged) in future virus scans.

3.4. Blocking Calls

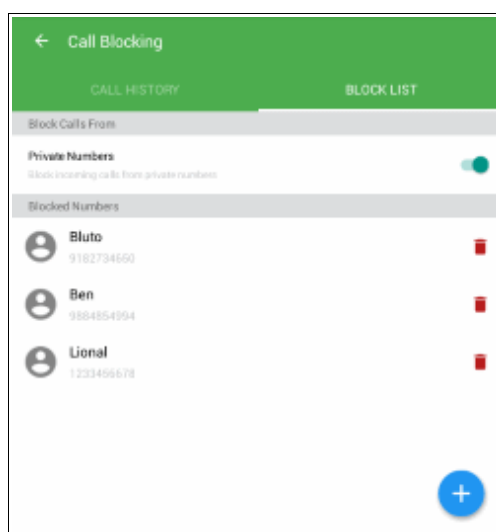
Comodo Mobile Security allows you block calls from specific numbers. You can specify numbers manually or import them from your contacts. You can also block calls from private numbers (caller ID hidden).

To view blocked calls

- Tap the menu button at the top left to open the side bar.
- Tap 'Call blocking' from the menu:

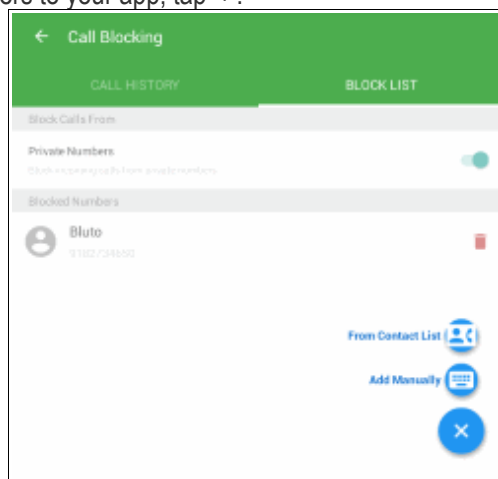


The list of blocked calls will be displayed.



- To remove an individual log entry from the list, touch the 'X' button beside it

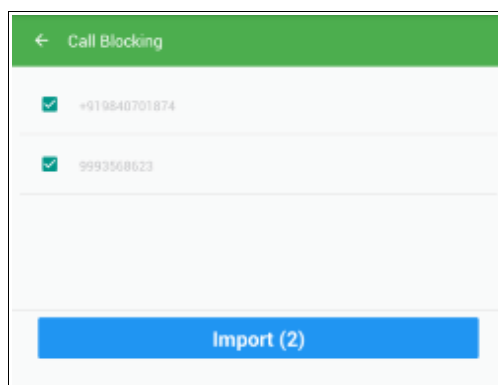
- To remove all the entries in the list at once, tap 'Remove All'.
- To add private numbers to your app, tap '+'.



You can add blocked callers in two ways:

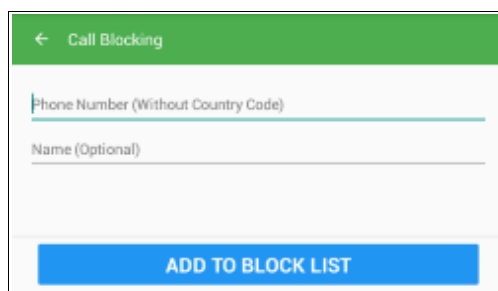
- Tap '+' button at the bottom corner and choose 'From Contact List'..
- Select the contacts and tap 'Import' button.

The contacts details that need to be entered will be displayed.

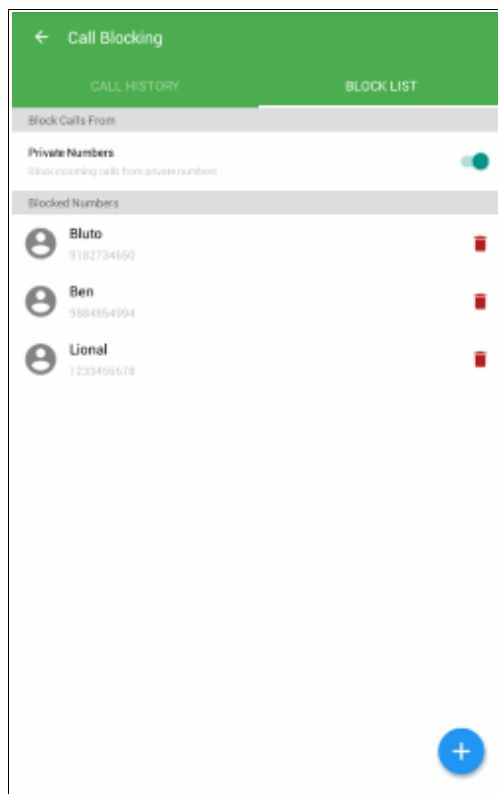


Or

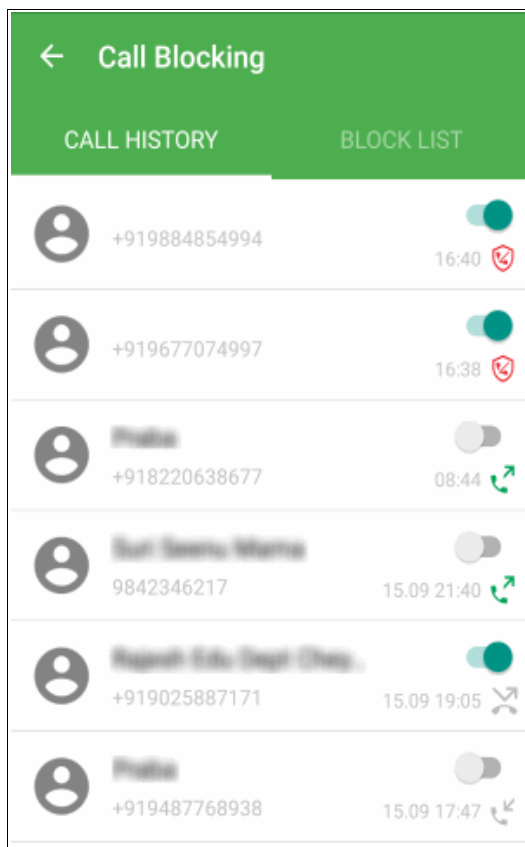
- Tap '+' button at the bottom corner and choose 'Add Manually'.
- Enter phone number and name
- Tap 'Add to Block List'.




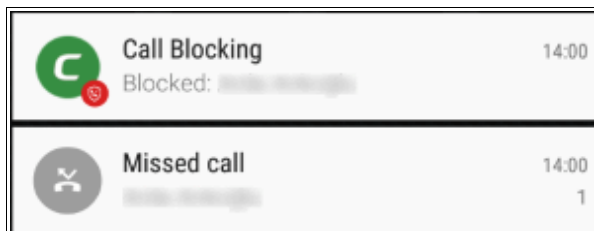
On adding contacts to the block list, the added contact details will be displayed in the 'Blocked List' tab.



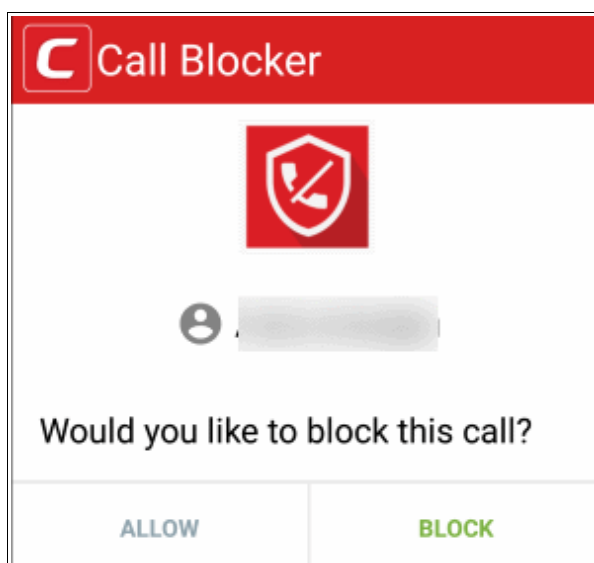
If the 'Private Numbers' option is turned on, CMS will block calls from people who hide their Caller ID. The Call History tab displays details of blocked and non-blocked calls.



The calls added to block list will appear with  symbol. The calls from other numbers too are present in history. CMS also provides contact details on missed block-listed calls.



CMS asks you for your preference on blocking if you have attended a short call.

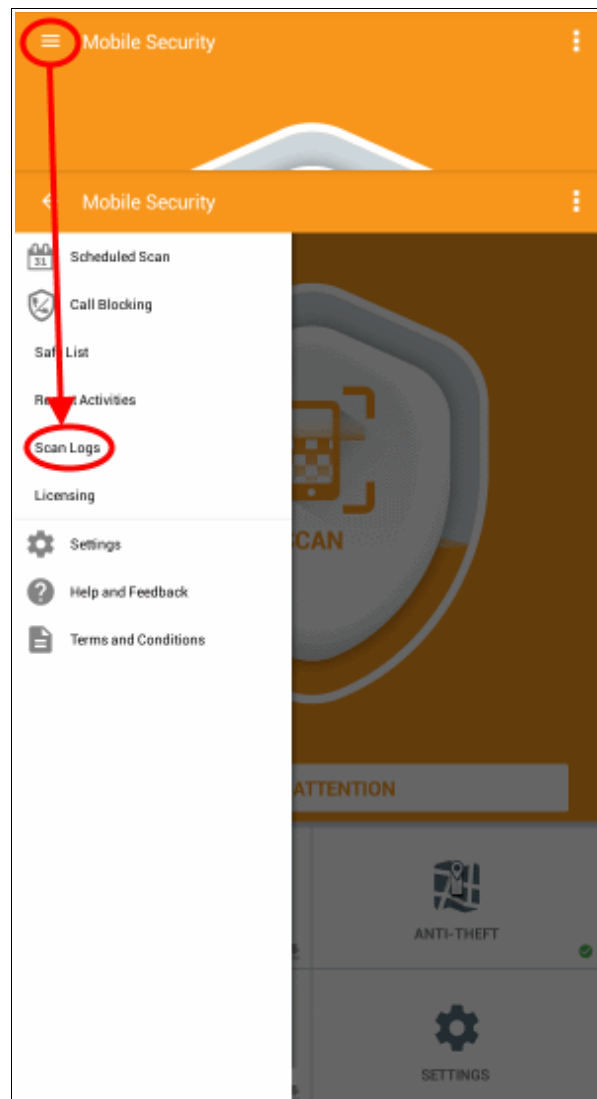


3.5. Viewing Antivirus Logs

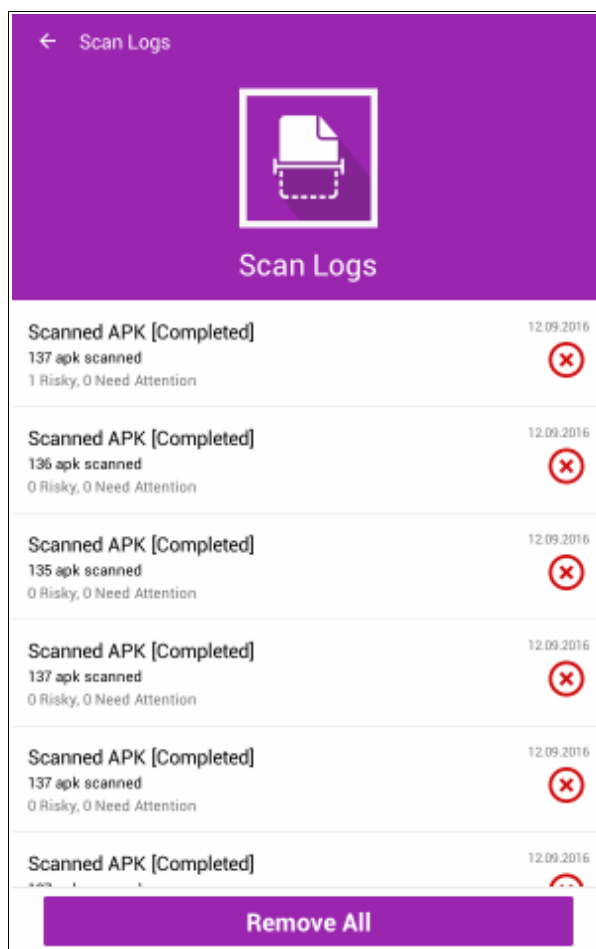
Comodo Mobile Security keeps a record of all apps that have been scanned on your device.

To view the antivirus scan log

- Tap the menu button at the top left to open the menu bar
- Tap 'Scan Logs' from the menu:



The log interface will show a list of real-time, manual and scheduled scans, along with the dates at which they were run. The number of threats and risks identified in each scan is also displayed.



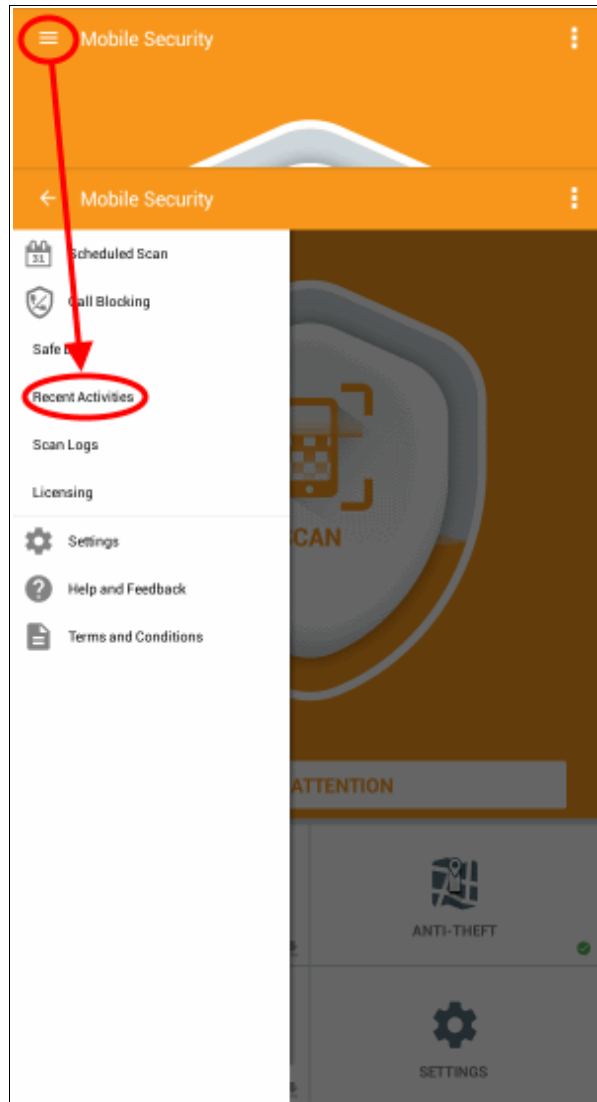
- To remove an individual log entry from the list, touch the 'X' button beside it
- To remove all the entries in the list at once, tap 'Remove All'.

3.6. Viewing Activity Logs

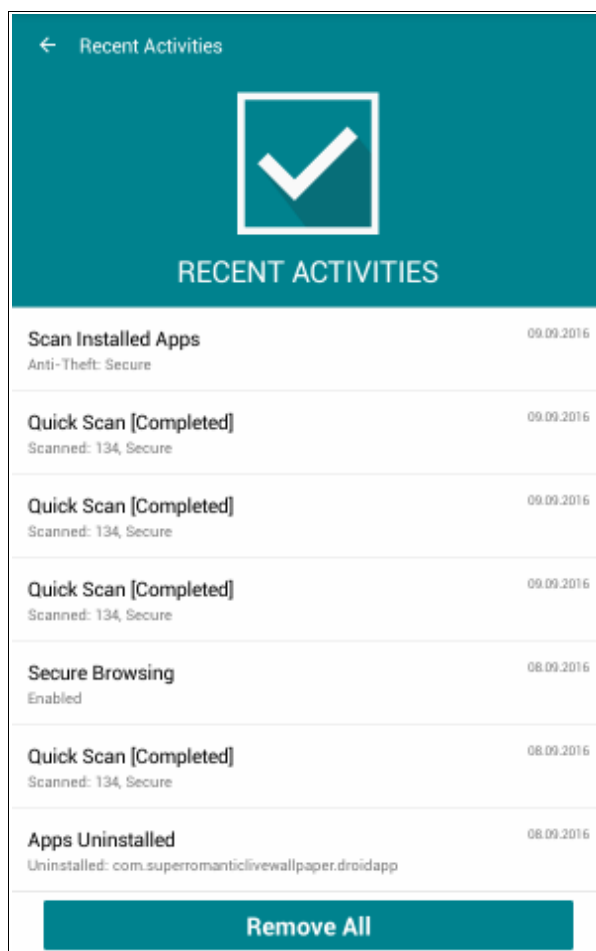
The 'Recent Activities' log allows you to view a list of actions recently performed by CMS. This includes items like antivirus scans, apps added to the safe list, settings changes and enabling or disabling of features. Each entry also includes the date of the activity and the results of the activity.

To view the activity logs

- Tap the menu button at the top left to open the menu bar
- Tap 'Recent Activities' from the menu bar.



The 'Recent Activities' list will be displayed.



The following events are listed in recent activity logs:

- Quick scans
- Full scans
- Real time protection scans
- Cloud scans
- Addition of apps to the safe list
- Setting changes

To clear the list, tap 'Remove All'.

3.7. Configuring the Antivirus Scanner

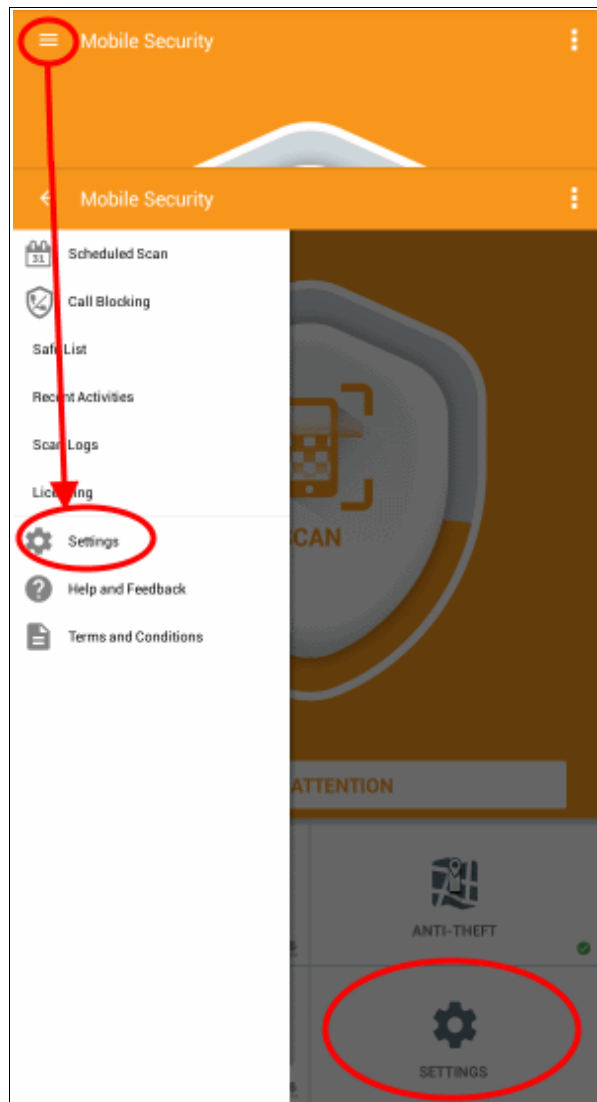
The 'Settings' area allows you to enable or disable real-time protection and to configure various other preferences.

To Access 'Settings' from CMS:

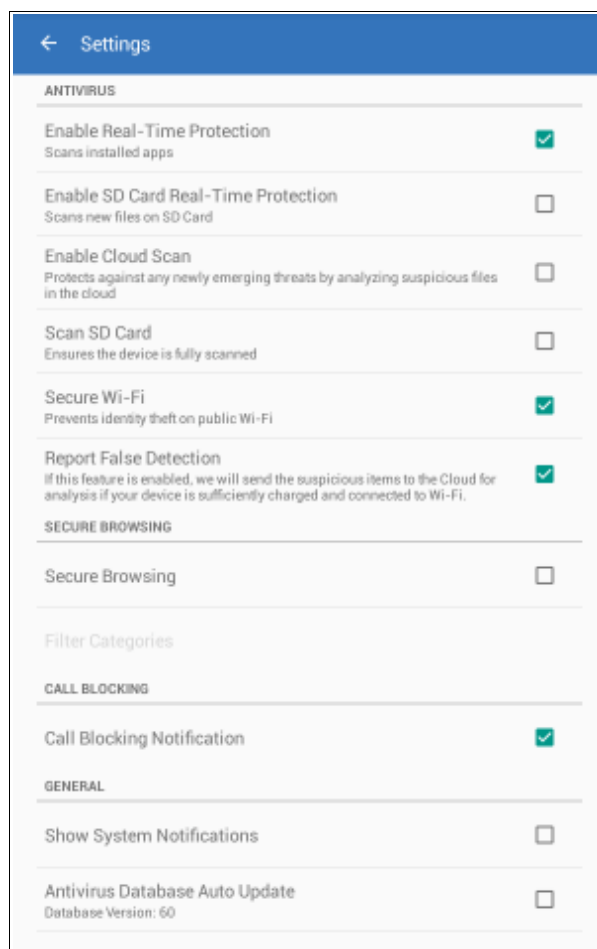
- Tap the 'Settings' icon at the bottom right of the home screen

Or

- Tap the menu button at the top left to open the menu bar
- Tap 'Settings' from the menu bar.



The 'Settings' pane will open.



Antivirus Settings:

- **Enable Real-Time Protection** – Have this option selected to ensure your device is constantly protected by the antivirus scanner. **(Default = Enabled)**.
- **Enable SD Card Real-Time Protection** – Select this option to ensure files on your SD card are also monitored for viruses in real time. **(Default = Disabled)**.
- **Enable Cloud Scan** - Enabling this option means CMS will be even more effective because it will also consult Comodo's online virus database when scanning each item. Because the cloud servers contain the very latest malware signatures, CMS will be capable of detecting zero-day malware even if the local database is out-dated. **(Default = Disabled)**.
- **Scan SD Card** – Select this option if you want data on your SD card to be scanned as part of an on-demand or scheduled scan. **(Default = Disabled)**.
- **Secure Wi-Fi** – Select this option to secure your connection to the internet when using public Wi-Fi. **(Default = Enabled)**.
- **Report False Positive** – Request a review of files that were flagged as malicious by CMS, but you believe to be safe. **(Default = Enabled)**
- **Secure Browsing** – Select this option to filter specific urls from the browser. **(Default = Disabled)**.
- **Call Blocking Notification** – Select this option if you want to be notified whenever CMS blocks a call from one of your blocked numbers. **(Default = Enabled)**.
- **Show System Notification** – Select this option if you want notifications from CMS to be displayed in the notification area. **(Default = Disabled)**.
- **Antivirus Database Auto Update** – Select this option if you want the antivirus database to be updated periodically. **(Default = Disabled)**

4. Secure Browsing

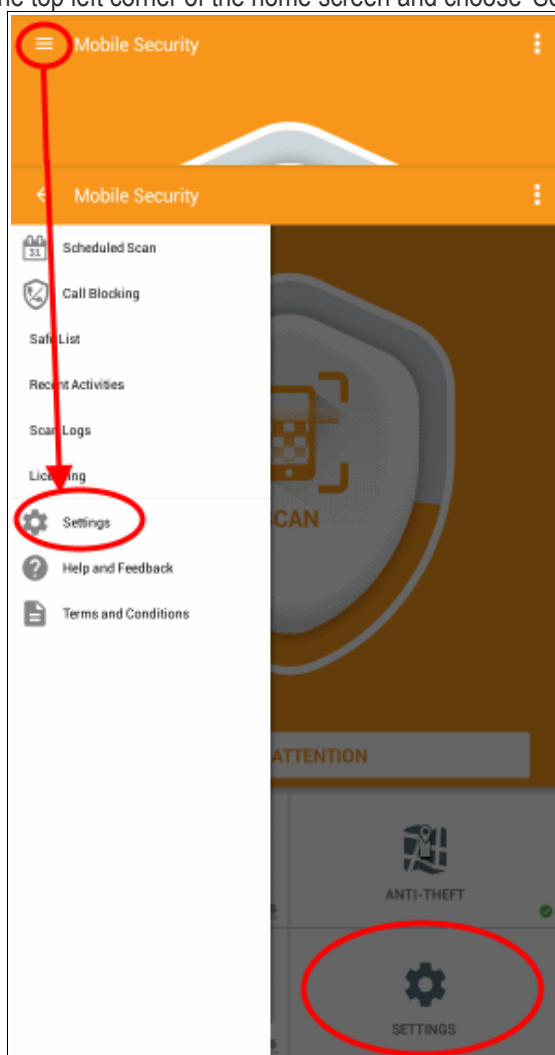
Secure Browsing is a URL filter which protects you online by automatically blocking access to malicious websites.

Note – Secure browsing only supports Google Chrome at the moment. Please ensure you have Google Chrome installed to use this feature.

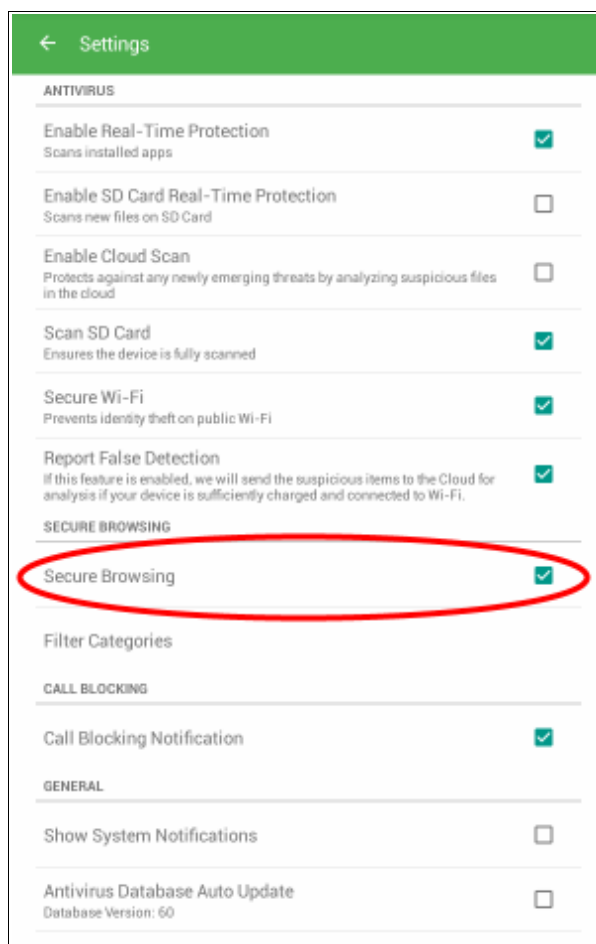
Secure browsing can be enabled in settings or by tapping 'Activate' in the scan results screen.

To enable secure browsing:

- Tap the 'Settings' icon at the bottom right of the home screen or
- Tap the menu bar on the top left corner of the home screen and choose 'Settings'.

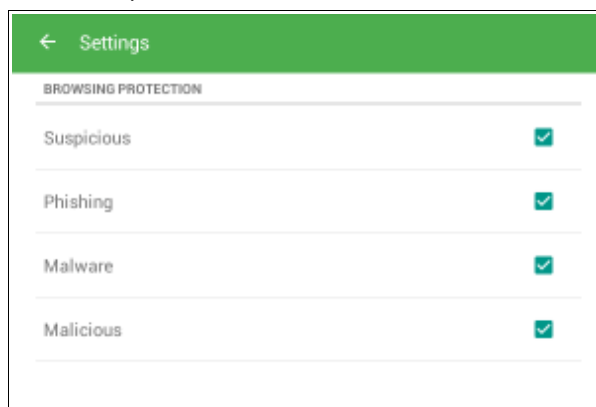


- Enable the Secure browsing option. Please note that this option is disabled by default.

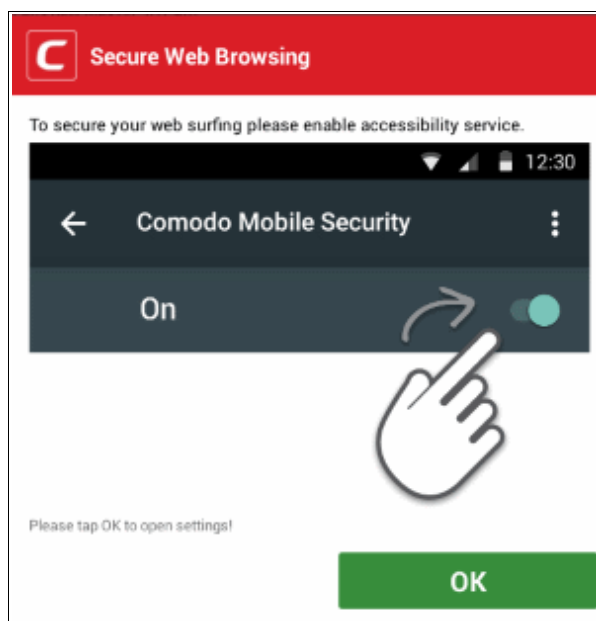


Antivirus Settings:

- CMS ships with four preset categories which can be enabled or disabled according to your preference:
 - **Malware** - 'Malware' is malicious software. If this category is enabled, CMS blocks urls that lead to download executable files that are malicious.
 - **Suspicious** – Automatically blocks access to sites that have evidences of malicious activities/contents.
 - **Phishing** – Automatically blocks known phishing websites.
 - **Malicious** – Automatically blocks web pages containing unwanted links that lead urls/hyperlinks which steal user login credentials, personal information etc.



After browser protection is enabled, CMS will redirect you to mobile accessibility settings where you need to turn 'ON' CMS browser security. Then Chrome will display setting information 'Comodo Mobile Security Secure Browsing Activated' each time you open the browser.



Comodo Mobile Security Secure Browsing Activated

5. Anti-theft

Comodo Anti-Theft allows you to locate your missing Android device and to remotely prevent unauthorized access to data stored on the device.

As the 'Swiss army knife' of anti-theft applications, Comodo Anti-Theft provides multiple ways to find and protect your device. All security features can be activated by logging-in to your Comodo Anti-Theft website account and sending commands to your lost device.

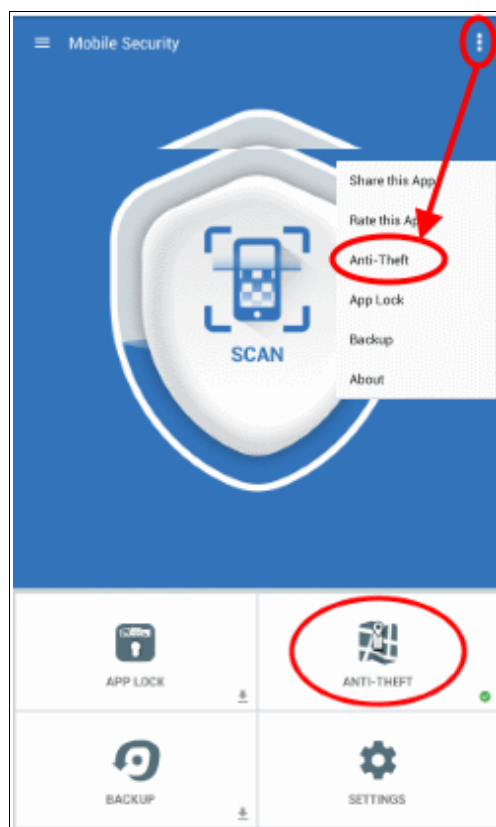
- Locate – Enables you to get the precise location of your lost device on Google Maps
- Remote Lock – Lock the home screen of your lost device to prevent people from accessing its data. It can be unlocked only on entering your Comodo Anti-Theft password
- Sound an alarm – Generate a siren from the misplaced device to locate it
- Remote Wipe – Delete all confidential data stored on the missing device
- Take Photo – Silently capture an image of the person in possession of the device without their knowledge

To Access Comodo Anti-Theft from CMS:

- Tap the 'Anti-Theft' icon at the bottom right of the home screen

Or

- Tap the menu button at the top left to open the menu bar
- Tap 'Anti-Theft' on the menu bar.



- If Comodo Anti-Theft is not already installed, you will be taken to the Google play store to download and install it. After installation, choosing 'Anti-Theft' will open the application.
- If Comodo Anti-Theft is already installed, the app will be opened.

For more details on using Comodo Anti-Theft, please refer to the products full guide at <https://help.comodo.com/product-168-Comodo-Anti-Theft-For-Android.html>

6. App Lock

Comodo App Lock prevents applications and games on your smart phone or tablet from being accessed by others without your knowledge. You can lock any game or app you desire using a lock pattern of your choice. App Lock is great for protecting information on shared devices and provides another layer of data security if your device is ever lost or stolen.

App Lock allows you to:

- Secure your contacts and calendar events from the prying eyes of others
- Protect your banking and financial apps from being accessed by others
- Safeguard social website pages like Facebook, Twitter from nosy friends
- Hide private conversations through messenger apps like Whatsapp and Skype
- Shield pictures and videos shared through media sharing apps like Instagram
- Prevent children from making unwanted purchases from shopping apps
- Stop others playing your favorite games, ruining your save points or spending your in-game credits

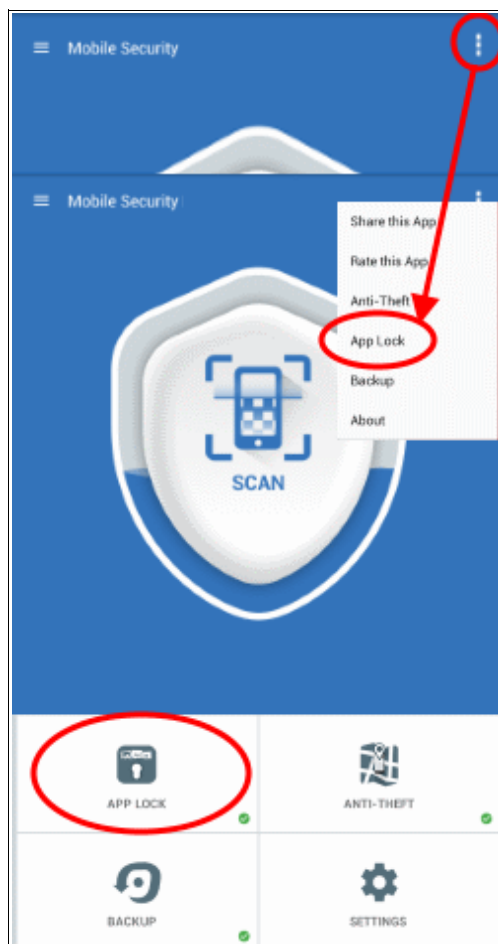
... and more.

To Access Comodo 'App Lock' from CMS:

- Tap the 'App Lock' icon at the bottom right of the home screen

Or

- Tap the menu button at the top left to open the menu bar
- Tap 'App Lock' on the menu bar.



- If Comodo App Lock is not already installed, you will be taken to the Google play store to download and install it. After installation, choosing 'App Lock' will open the application.
- If Comodo App Lock is already installed, the app will be opened.

For more details on using Comodo App Lock, please refer to the products full guide at

<https://help.comodo.com/topic-327-1-680-8408-Introduction-to-Comodo-Applock-for-Android.html>

7. Backup

Comodo Backup for Android allows you to backup and restore valuable data such as text messages, contacts, bookmarks, applications and photos. This is especially useful if you have to restore your device to factory settings at any time.

Backup data is stored in the root directory of SD card or phone storage.

Backup allows you to:

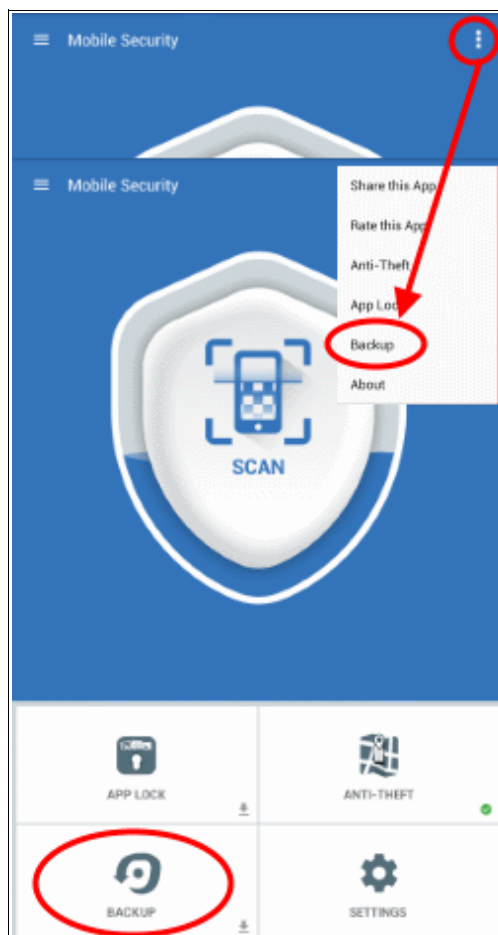
- Backup Contacts
- Change SD Card location

To access Comodo Backup:

- Tap the 'Backup' icon at the bottom right of the home screen

Or

- Tap the menu button at the top left to open the menu bar
- Tap 'Backup' on the menu bar.



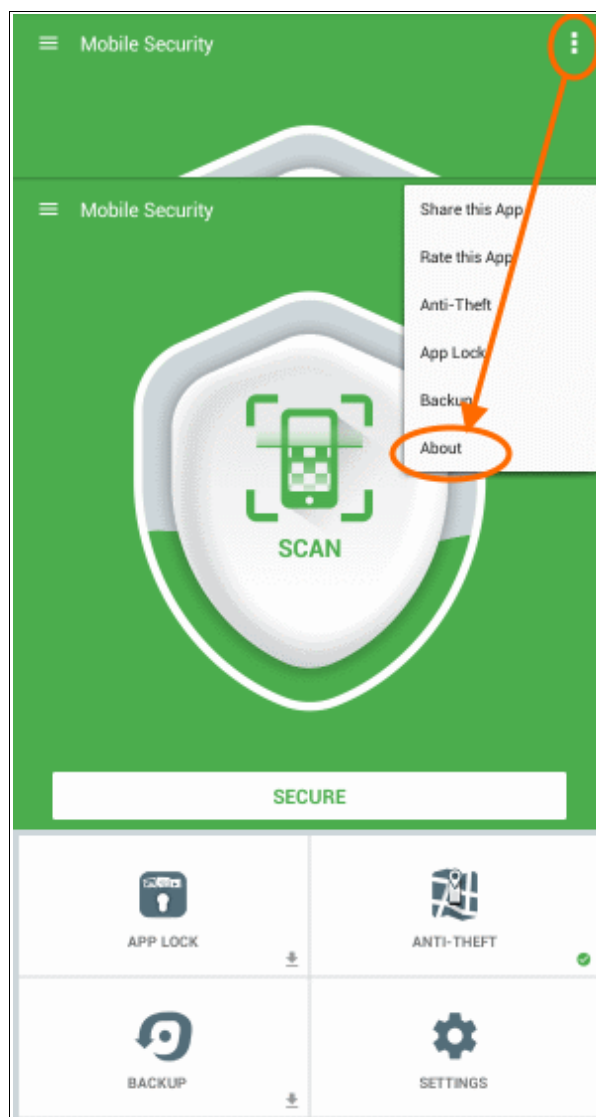
- If Comodo Backup is not already installed, you will be taken to the Google play store to download and install it. After installation, choosing 'Backup' will open the application.
- If Comodo Backup is already installed, the app will be opened.

For more details on using Comodo App Lock, please refer to the products full guide at:

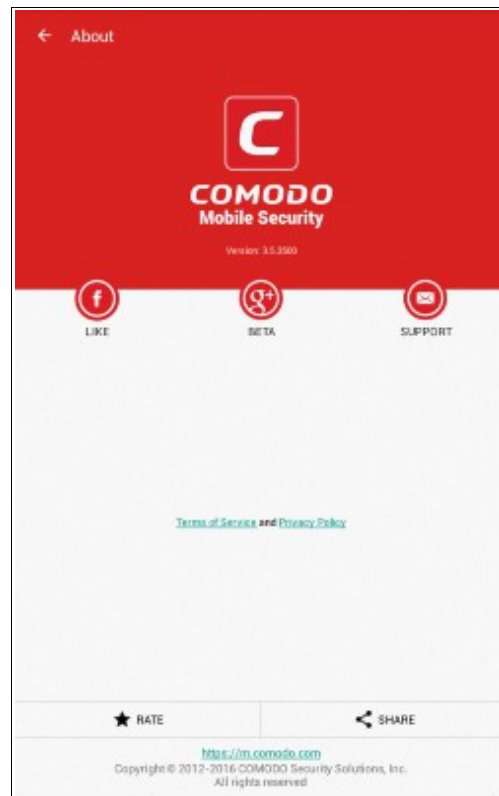
<https://help.comodo.com/topic-326-1-678-8393-Introduction-to-Comodo-Mobile-Backup-for-Android.html>

8. About Comodo Mobile Security

The 'About Us' screen can be accessed from the Comodo Mobile Security interface by touching the options icon at the top right of the home screen and choosing 'About As'.



'About Us' contains the current product version and copyright information and other helpful links. If you are unable to find a solution for a problem, you can send your query to antivirus@comodo.com. A link to <https://m.comodo.com/> allows you to view, to select and download a new Comodo products for your mobile device.

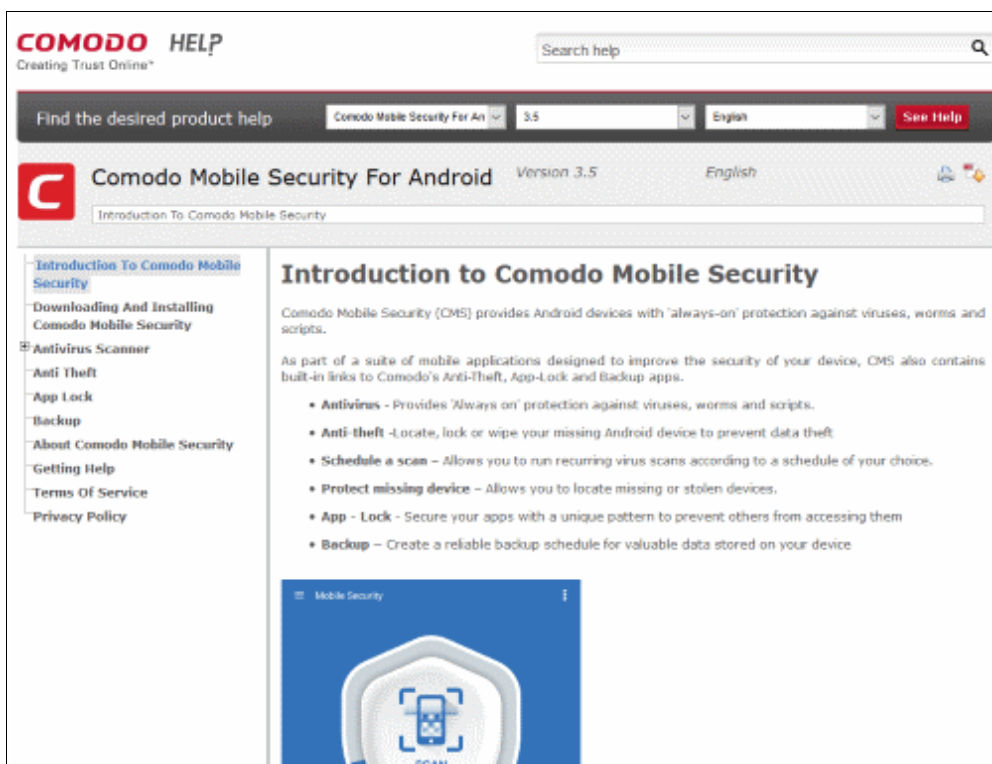


9. Getting Help

Comodo Mobile Security features a built-in help guide that contains explanations of the functionality and usage of the application.

To open the built-in guide

Tap the menu button from the CMS home screen and choose 'Help and Feedback' from the side drawer. It opens Comodo Mobile Security's online help guide at <https://help.comodo.com/topic-162-1-713-8445-Introduction-to-Comodo-Mobile-Security.html>



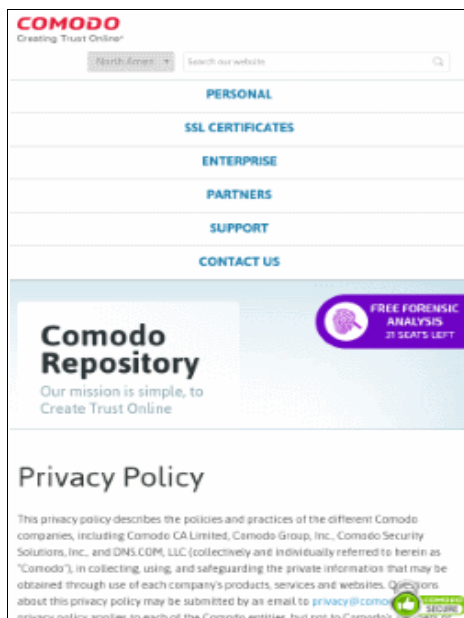
10. Terms of Service

Tap the menu button from the CMS home screen and choose 'Terms of Service' from the side drawer. It opens Comodo Mobile Security's User License Agreement.



11. Privacy Policy

Tap the menu button from the CMS home screen and choose 'Privacy Policy' from the side drawer. It opens Comodo Mobile Security's privacy policy in the preferred browser.



About Comodo

The Comodo organization is a global innovator and developer of cyber security solutions, founded on the belief that every single digital transaction deserves and requires a unique layer of trust and security. Building on its deep history in SSL certificates, antivirus and endpoint security leadership, and true containment technology, individuals and enterprises rely on Comodo's proven solutions to authenticate, validate and secure their most critical information.

With data protection covering endpoint, network and mobile security, plus identity and access management, Comodo's proprietary technologies help solve the malware and cyber-attack challenges of today. Securing online transactions for thousands of businesses, and with more than 85 million desktop security software installations, Comodo is Creating Trust Online®. With United States headquarters in Clifton, New Jersey, the Comodo organization has offices in China, India, the Philippines, Romania, Turkey, Ukraine and the United Kingdom.

Comodo Security Solutions, Inc.

1255 Broad Street,

Clifton, NJ 07013

United States

Tel: +1 (888) 266-6361

Tel: +1 (703) 581-6361

Email: EnterpriseSolutions@Comodo.com

Comodo CA Limited

3rd Floor, 26 Office Village, Exchange Quay, Trafford
Road, Salford, Greater Manchester M5 3EQ,

United Kingdom.

Tel : +44 (0) 161 874 7070

Fax : +44 (0) 161 877 1767

For additional information on Comodo - visit <http://www.comodo.com>.