COMODO
Creating Trust Online®

Comodo
Mobile Security for Android

Software Version 2.5

User Guide

Guide Version 2.5.111014

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Table of Contents

1.Introduction to Comodo Mobile Security

Comodo Mobile Security (CMS) provides Android devices with 'always on' protection against viruses, worms and scripts. In addition to core antivirus protection, CMS also features SMS & Call Blocking, Private Space, an effective Software & Process Manager, Data and Apps Backup and Data Traffic Monitor. The Anti Theft feature allows you to recover your device if it is misplaced, lost or even stolen. Please click the following links to jump straight to the area you need help with:

- **Downloading and Installing** - Describes from where to download and how to install CMS
- **Antivirus Scanner and Ad Blocker** - How to run antivirus scans and block push ad apps from appearing on your device
- **Privacy Advisor** - Describes how to view and manage apps whose privileges could compromise your privacy or cost you money.
- **Traffic Monitoring** - Describes how to configure the Traffic Monitoring service to check your GPRS/3G usage and alert you when you are about to reach your data-plan limit. You'll also learn how to use the firewall to control which apps connect to the Internet.
- **System Optimizer** - Explains how to improve the performance of your device by running a system optimization scan and terminating resource hungry processes.
- **Private Space** - Describes how to create and manage private contacts.
- **Software Manager** - Describes how to manage all the apps in your device
- **Call & SMS Blocking** - Describes how to filter out unwanted SMS messages and phone calls.
- **Backup** - Describes how to backup/restore your valuable data and apps to and from SD card.
- **Scheduled Tasks** - Learn how to schedule tasks such as antivirus scans to run automatically.
- **Anti Theft** - Describes how to protect and locate your device in the event it is lost or stolen. Includes remotely making your phone sound an alarm, getting the location of your missing device, remotely locking your device, remotely wiping your device of personal data and taking a photograph of the person currently in possession of the device.

- **CMS Settings and More** - Describes how to configure Comodo Mobile Security settings, leave feedback, check for updates and more.
- **Comodo Battery Saver** - Describes how to launch Comodo Battery Saver, an app that help to optimizes battery charge in your device.

2.Downloading and Installing CMS

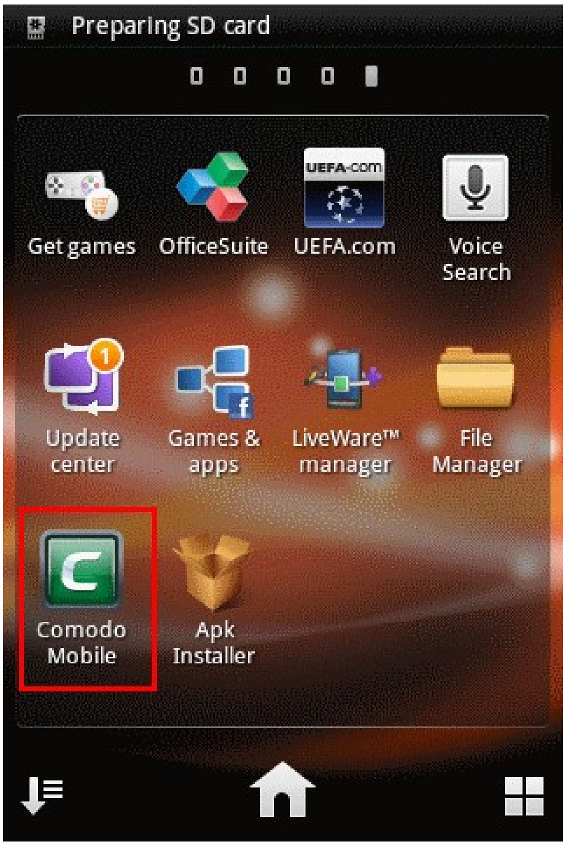
Comodo Mobile Security application is available at **https://m.comodo.com/**.

Step 1: Enter **https://m.comodo.com/** in the address bar of the browser in your android mobile phone or device.

Step 2: In the Comodo Mobile Security webpage, click the 'Free Download' button.

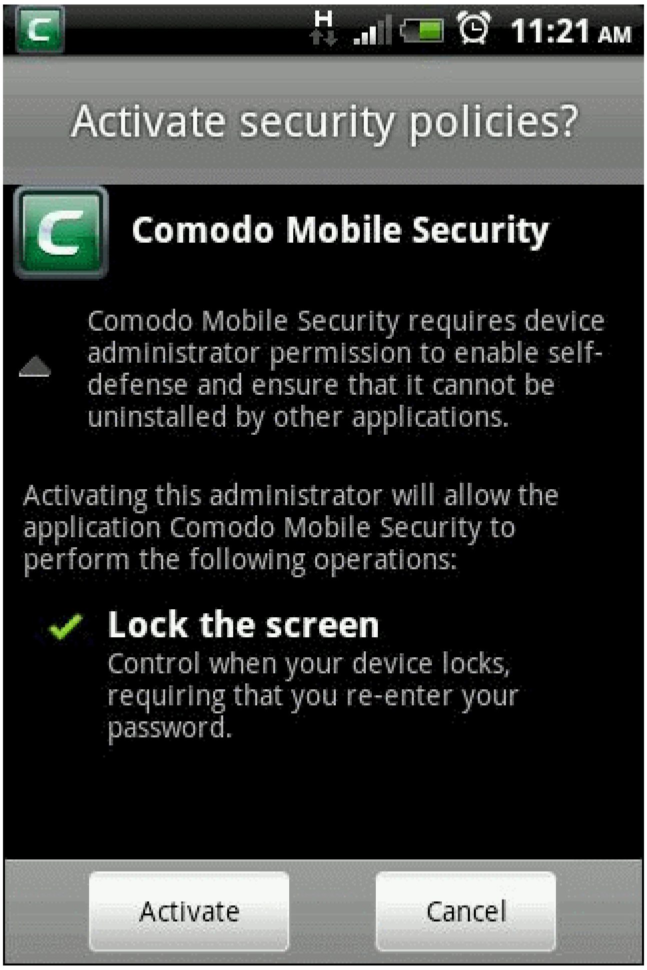
Alternatively, login to **https://play.google.com/store/apps/details?id=com.comodo.pimsecure** and click 'Install' button.

The application will be downloaded and installed automatically.
The Comodo Mobile Security icon will now be available in the screen.



Activation of Security Policies

If you are running CMS for the first time, CMS will request for administrator rights. Providing administrative privileges to CMS will enable it to activate its security policies and prevent it from being uninstalled by other third-party applications.



Activate security policies?

Comodo Mobile Security

Comodo Mobile Security requires device administrator permission to enable self-defense and ensure that it cannot be uninstalled by other applications.

Activating this administrator will allow the application Comodo Mobile Security to perform the following operations:

✓ **Lock the screen**
Control when your device locks, requiring that you re-enter your password.

- Tap 'Activate' to assign administrative privileges to CMS and activate the security policies.

Tip: You can also assign administrative rights and activate the security policies at anytime from the Settings screen. Refer to the section **CMS Settings and More** for more details.

3.Antivirus Scanner and Ad Blocker

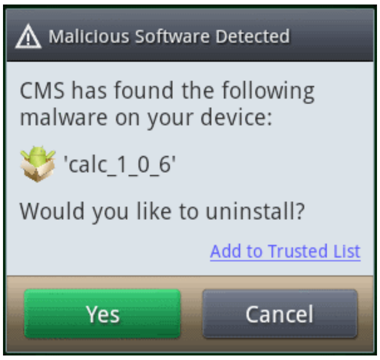
"Always on" virus protection and an on-demand scanner help keep your device clear of viruses and unsafe apps. One touch scans and scheduled scans are provided as well as a system "Health Check" feature that quickly identifies viruses, unsafe apps and potentially risky settings. In addition to real time virus protection, CMS also safeguards you from:

- Annoying Push Ads hosted by applications that you download from various sources
- Harmful USSD attacks from malicious webpages

Click the links below for help with common tasks:

- **How to run a device 'Health Check'**
- **How to run an antivirus scan**
- **How to schedule an antivirus scan**
- **How to add apps to trusted list**
- **How to update Comodo Mobile Security**
- **How to check the log**

The real time antivirus protection provides instant malware alert while an unsafe app is being installed.



Malicious Software Detected

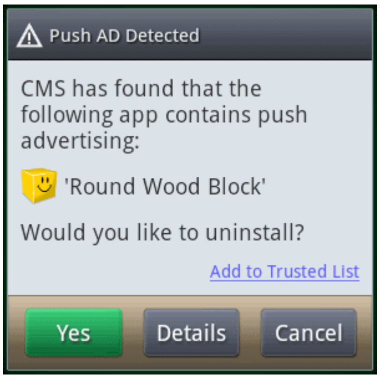
CMS has found the following malware on your device:

'calc_1_0_6'

Would you like to uninstall?

- Tap 'Yes' to uninstall or 'Cancel' to proceed with the installation. You can also add this app to **trusted list**. CMS will not scan the apps that are in the trusted list.

The Push Ad detector provides you warning in the notifications bar while apps that host push ads are being installed. Open the notification bar to view the message.



Push AD Detected

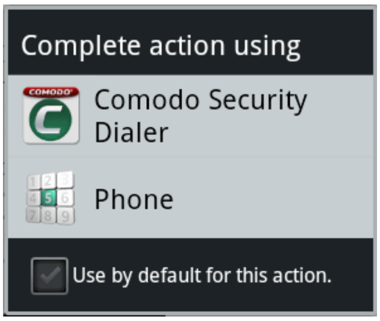
CMS has found that the following app contains push advertising:

'Round Wood Block'

Would you like to uninstall?

- Tap 'Yes' to uninstall or 'Cancel' to proceed with the installation. You can also add this app to **trusted list**. CMS will not scan the apps that are in the trusted list. Tap 'Details' to view the name of the advertiser and how the app may generally behave such as ads in the notification bar, create shortcuts and more.

Some of the malicious web pages you visit over Internet may invade your device by USSD attacks. The web page may send a message with a USSD code for performing a malicious activity such as resetting your device to factory settings, making you to loose your saved contacts and other valuable data. A typical USSD code will be similar to "*#NNNN#". CMS monitors each web page that you visit for possible USSD attack and if it detects any, it will alert you to choose Comodo Security Dialer to execute the code.

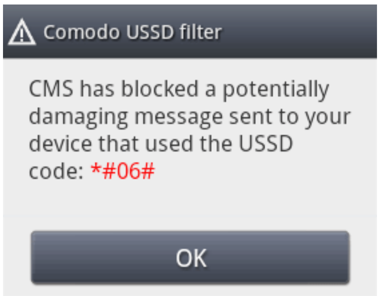


Complete action using

□ Use by default for this action.

- Select Comodo Security Dialer

If the message from the web page is a potential USSD attack, Comodo Security Dialer will block the attempt and safeguard your device.



Comodo USSD filter

CMS has blocked a potentially damaging message sent to your device that used the USSD code: *#06#

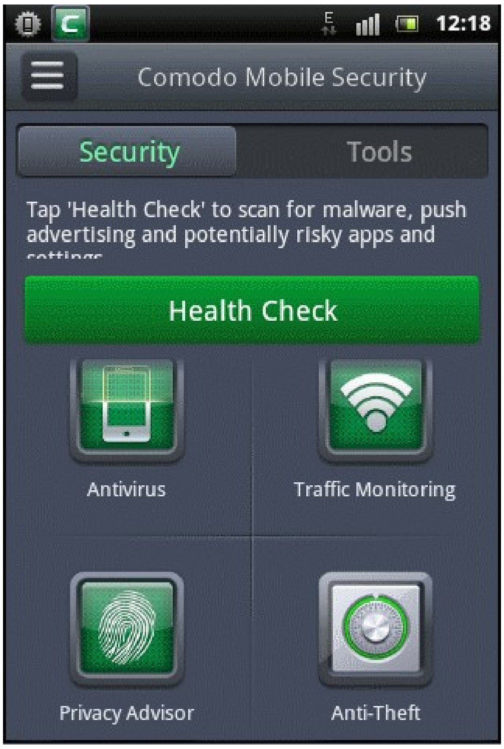
How to run a device 'Health Check'

A 'Health Check' is a full system scan that quickly identifies viruses, untrusted applications, push add apps and any potentially risky settings on your Android device.

To run a 'Health Check'

- Tap the CMS icon on your device.

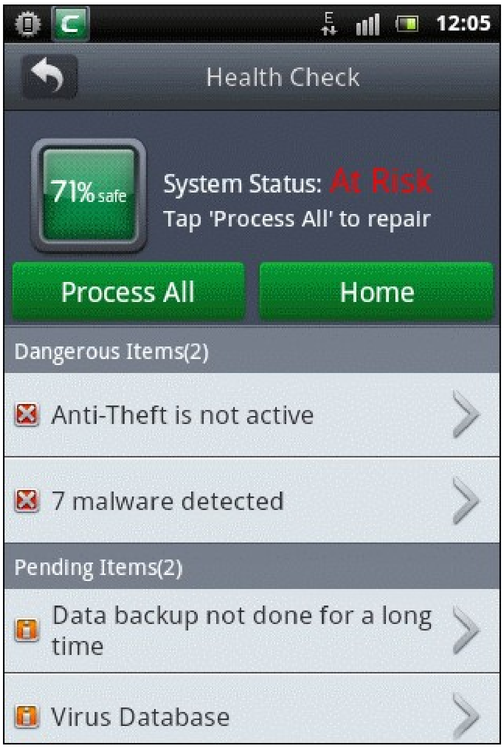
The home page of CMS under Security tab will open.



Tap 'Health Check' to scan for malware, push advertising and potentially risky apps and settings

- Tap the 'Health Check' button.

In addition to identifying viruses, the Health Check feature also checks for unsafe apps, push ad apps and potentially risky settings and displays the summary of dangerous items, pending items and secure items.



12:05

Health Check

71% safe

System Status: At Risk

Tap 'Process All' to repair

Dangerous Items(2)

☒ Anti-Theft is not active

☒ 7 malware detected

Pending Items(2)

Data backup not done for a long time

Virus Database

- Tap 'Process All' to repair all risky items displayed in the summary screen.

To repair the risky items individually, tap anywhere on an item. The next screen will depend on the item tapped. For example if you tap 'malware detected' bar, the 'Antivirus' results screen will be displayed for you to take further action. Refer to the '**Antivirus Results**' screen for more details.

How to run an antivirus scan

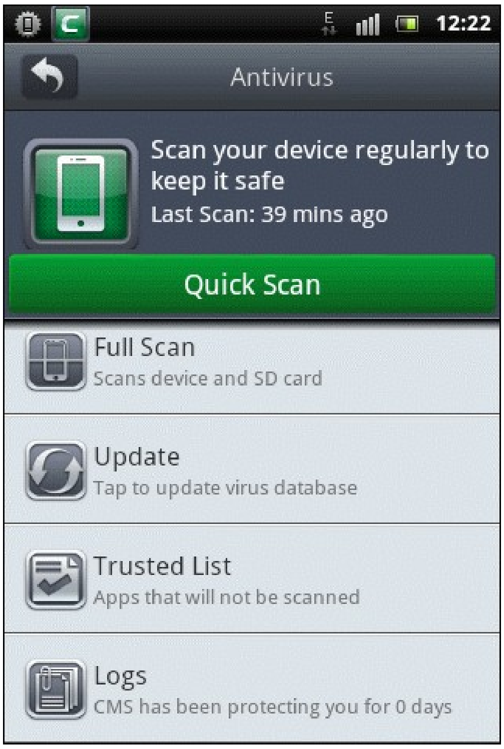
An antivirus scan performed by CMS on your android device detects viruses, push ad apps and unsafe apps and allows you to delete them. You have the option to run a Quick Scan or a Full Scan. While the Quick Scan will scan only the device memory, Full Scan will scan device memory as well as the SD card in the device.

Note: The hash values of .apk files will be sent to Comodo's File Lookup Service (FLS) one by one for detailed analysis, if the device is connected to the Internet via WiFi and 'Enable cloud scan for APK only' is enabled in the Settings screen. This is applicable to only .apk files and not other files in your device. If there is no WiFi connection, the results will be displayed according to the local scan.

To run an antivirus scan

- Tap 'Antivirus' in the home page of CMS under Security tab.

The 'Antivirus' screen will be displayed.



Scan your device regularly to keep it safe

Last Scan: 39 mins ago

Scans device and SD card

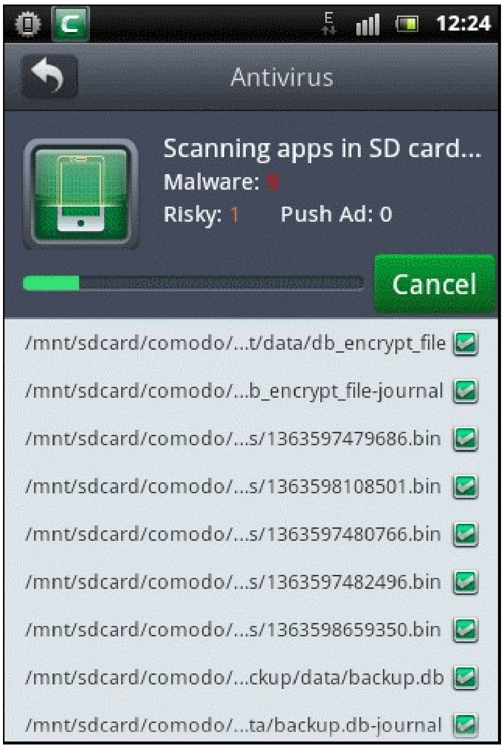
Tap to update virus database

Apps that will not be scanned

CMS has been protecting you for 0 days

- Tap 'Quick Scan' to scan only the internal memory of the device.
- Tap 'Full Scan' to scan both the internal memory and the SD card in the device.

The scanning process will begin.



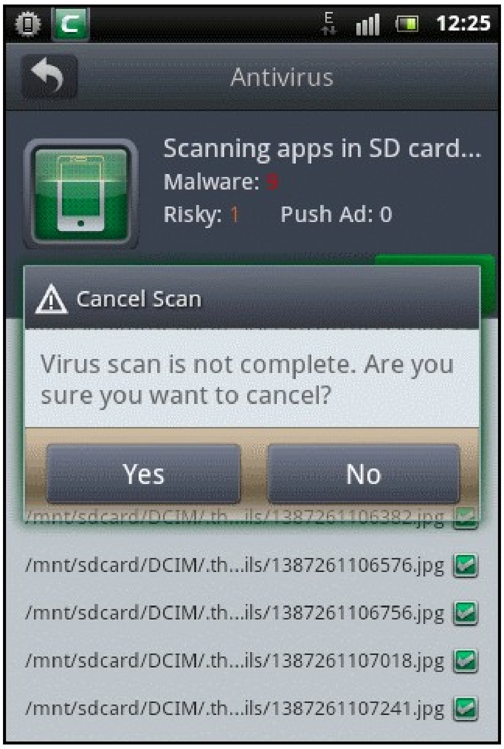
Scanning apps in SD card...

Malware: 9

Risky: 1 Push Ad: 0

```
/mnt/sdcard/comodo/...t/data/db_encrypt_file
/mnt/sdcard/comodo/...b_encrypt_file-journal
/mnt/sdcard/comodo/...s/1363597479686.bin
/mnt/sdcard/comodo/...s/1363598108501.bin
/mnt/sdcard/comodo/...s/1363597480766.bin
/mnt/sdcard/comodo/...s/1363597482496.bin
/mnt/sdcard/comodo/...s/1363598659350.bin
/mnt/sdcard/comodo/...ckup/data/backup.db
/mnt/sdcard/comodo/...ta/backup.db-journal
```

- Tap the 'Cancel' button if you want to cancel the scanning.



Scanning apps in SD card...
Malware: 9
Risky: 1 Push Ad: 0

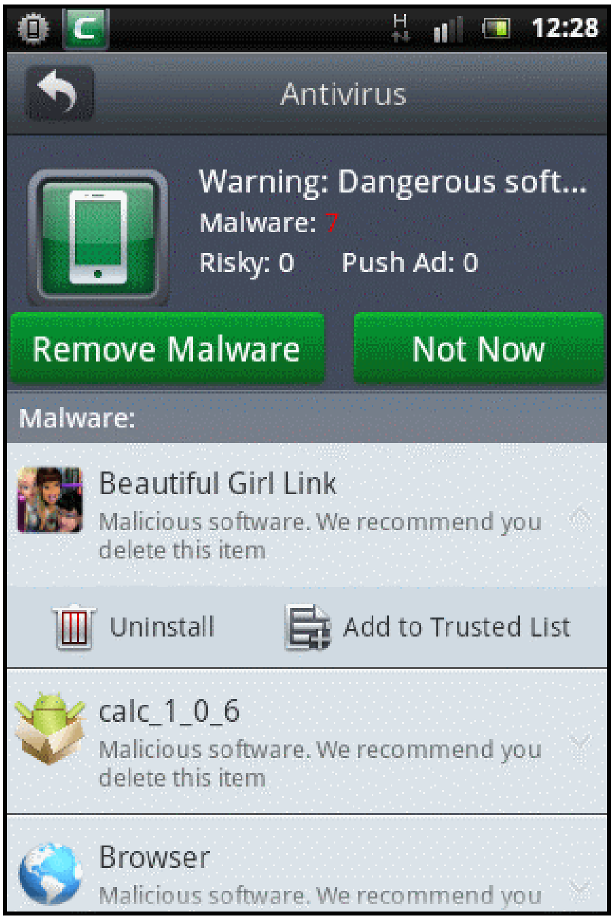
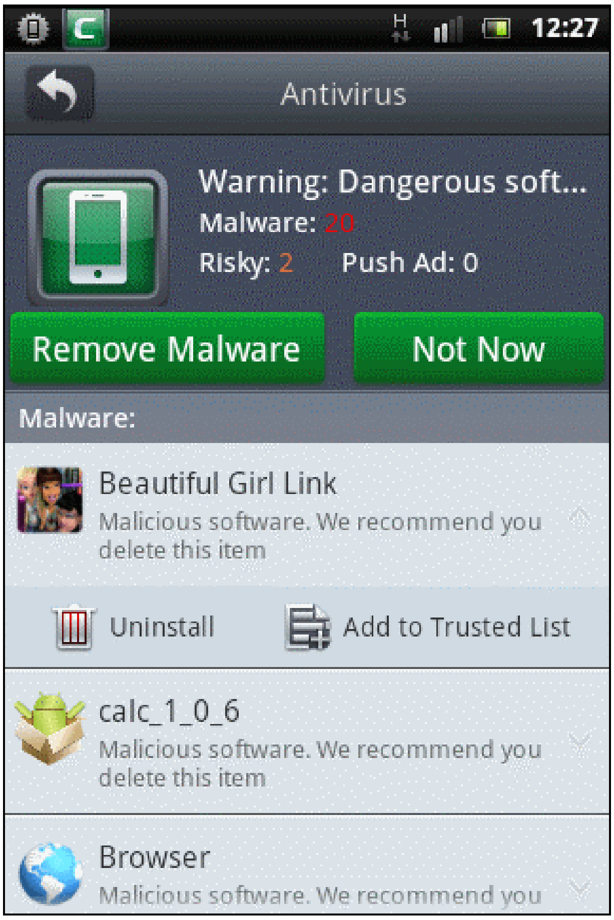
Cancel Scan

Virus scan is not complete. Are you sure you want to cancel?

/mnt/sdcard/DCIM/.th...ils/1387261106382.jpg
/mnt/sdcard/DCIM/.th...ils/1387261106576.jpg
/mnt/sdcard/DCIM/.th...ils/1387261106756.jpg
/mnt/sdcard/DCIM/.th...ils/1387261107018.jpg
/mnt/sdcard/DCIM/.th...ils/1387261107241.jpg

- Tap 'Yes' to confirm the cancellation or 'No' to continue the scanning process.

After the scan is complete, a summary of virus, push ad and unsafe apps in your device will be displayed. If apps infected with malware are found, the 'Remove Malware' button will be displayed.

Quick Scan Results	Full Scan Results
 12:28 Antivirus Warning: Dangerous soft... Malware: 7 Risky: 0 Push Ad: 0 Remove Malware Not Now Malware: Beautiful Girl Link Malicious software. We recommend you delete this item Uninstall Add to Trusted List calc_1_0_6 Malicious software. We recommend you delete this item Browser Malicious software. We recommend you	 12:27 Antivirus Warning: Dangerous soft... Malware: 20 Risky: 2 Push Ad: 0 Remove Malware Not Now Malware: Beautiful Girl Link Malicious software. We recommend you delete this item Uninstall Add to Trusted List calc_1_0_6 Malicious software. We recommend you delete this item Browser Malicious software. We recommend you

If no virus or unsafe apps are found, tap the 'Back' button to return to the 'Antivirus' screen.

If any viruses or unsafe apps are found tap 'Remove Malware' if you want to remove those items from your device. Tap 'Not Now' , if you do not want to take any action now. Scroll the screen to view all the items. Tapping on an item will display 'Uninstall' and 'Add to Trusted List' options.

- Tap the 'Remove Malware' button to remove all the infected apps in the results screen.
- Tap 'Uninstall' button below an app name to remove that item only.
- Tap 'Add to Trusted List' to add the item to the **trusted list**. When infected or potentially risky apps are added to the trusted list, CMS will not scan these items during subsequent scans.

A Full Scan results screen will also allow you to remove infected or malicious files from the SD card if any.

- Tap the button ✕ beside an item in the list to remove it.

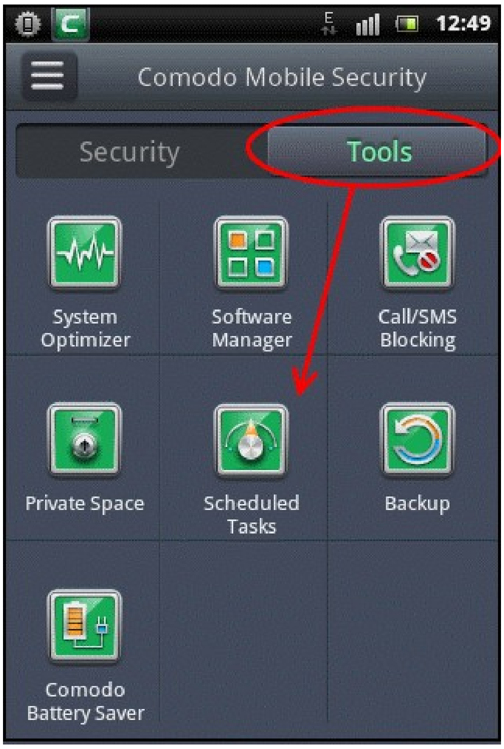
Please note that infected files detected in SD card can only be removed and cannot be added to trusted list.

How to schedule an antivirus scan

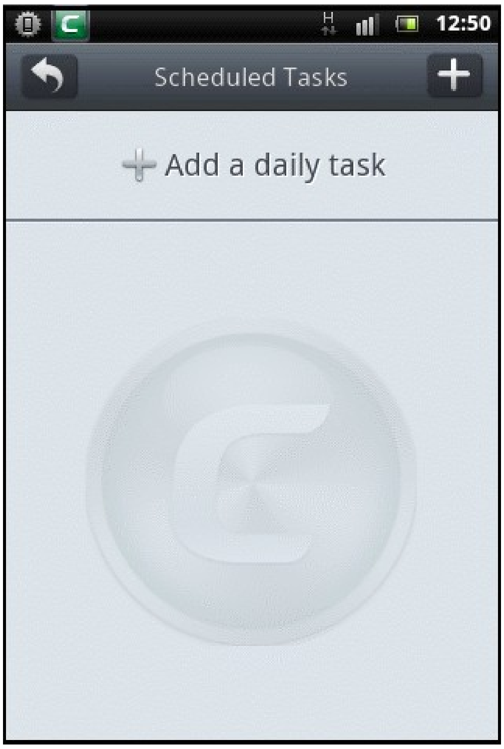
Scheduling an antivirus scan in your Android device automates the process of viruses and unsafe apps detection.

To schedule an antivirus scan

- Tap 'Tool's tab located at the top of CMS app and tap 'Scheduled Tasks'.

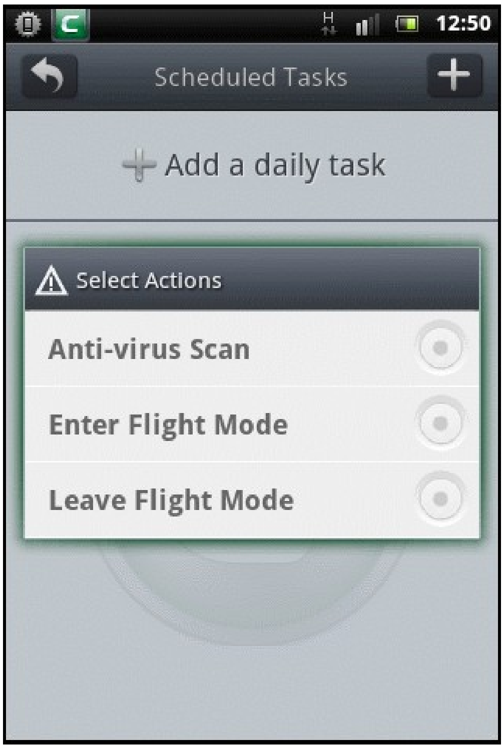


The 'Scheduled Tasks' screen will open.



- Tap the '+' button at the top or anywhere on the 'Add a daily task' row to add a new task.

The 'Select Actions' dialog will be displayed.13.CMS Settings and More|outline


Scheduled Tasks

Add a daily task

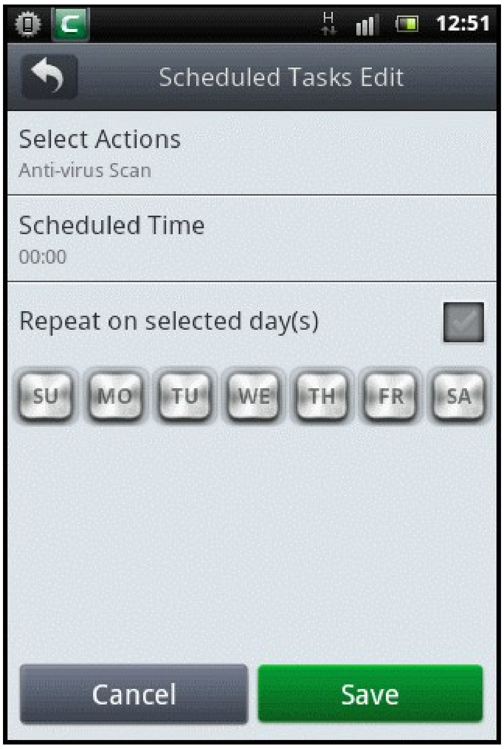
Select Actions

Anti-virus Scan ○

Enter Flight Mode ○

Leave Flight Mode ○

- Tap on 'Anti-virus Scan' bar.

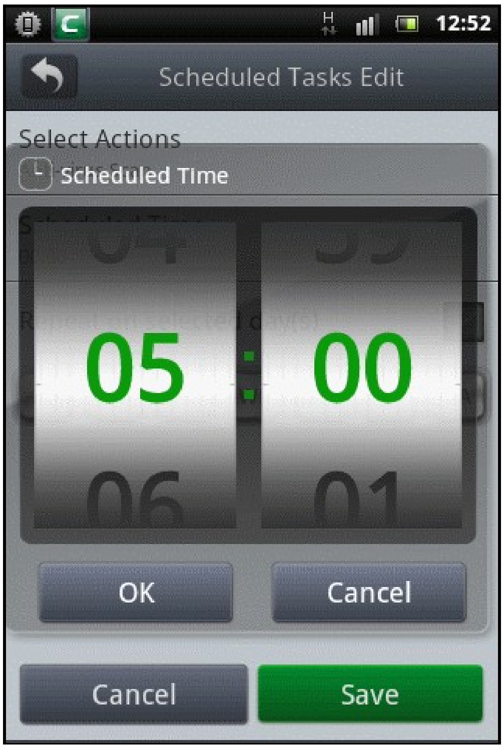

Scheduled Tasks Edit

Select Actions
Anti-virus Scan

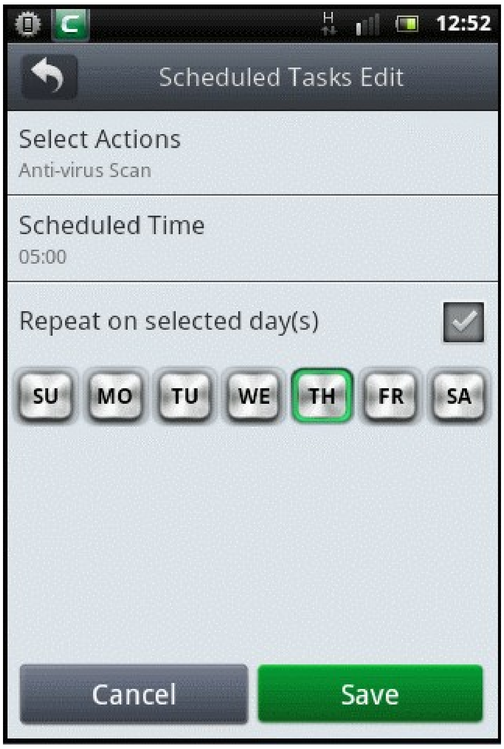
Scheduled Time
00:00

Repeat on selected day(s) ☑

- Tap the 'Scheduled Time' bar to set the time at which the antivirus scan should start.



- Tap 'OK' after selecting the time.
- Tap 'Repeat on selected day(s)' to select the day on which the scan should run.



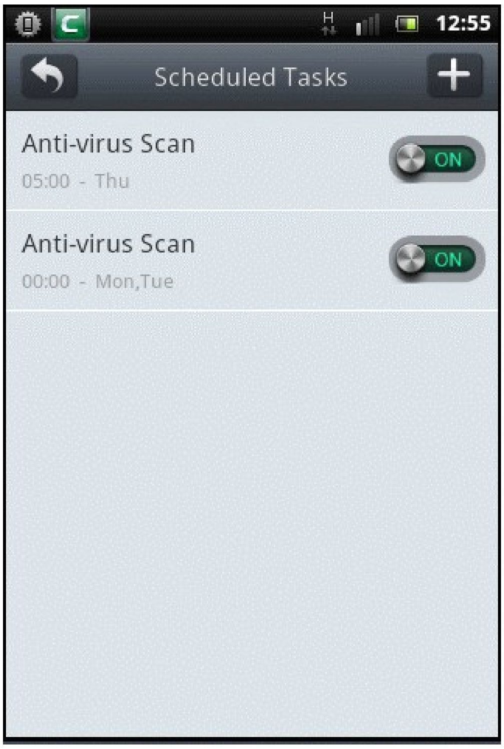
Select Actions
Anti-virus Scan

Scheduled Time
05:00

Repeat on selected day(s) ☑

- Selected the day on which the scan should run and tap the 'Save' button.
- Repeat the procedure to add as many scheduled tasks as you require in the same manner described above.

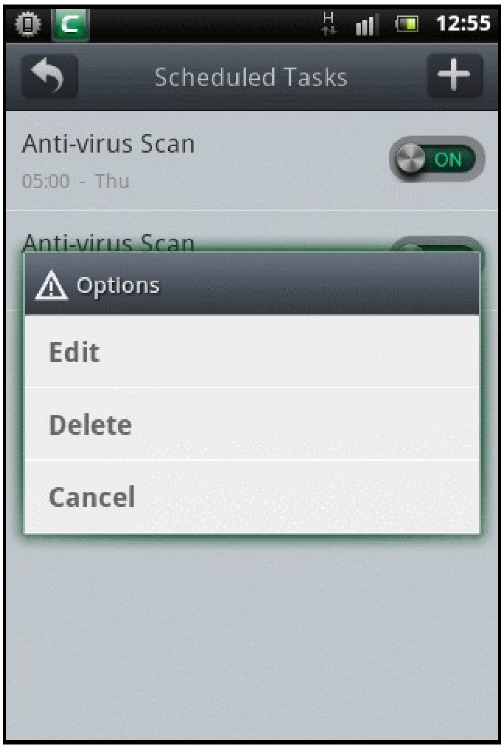
The list of scheduled tasks will be displayed.



Anti-virus Scan
05:00 - Thu
ON

Anti-virus Scan
00:00 - Mon,Tue
ON

- To disable a scheduled task, tap on the toggle switch to display 'OFF' condition. To enable it again, tap on it again.
- To edit or delete a scheduled task from your device, tap and hold briefly on the task.



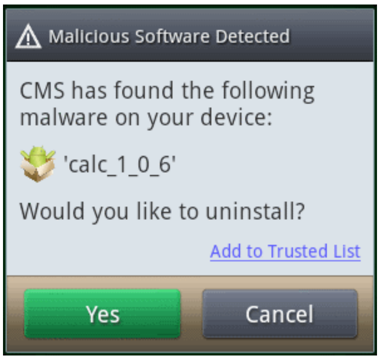
- Tap 'Edit' and edit the task.
- Tap 'Delete' to remove the task.

How to add apps to trusted list

CMS allows you to add apps to trusted list. This option is available in the results screen of antivirus scans and in the alerts screen while apps with malware or that hosts push ads are being installed. Once apps are added to the trusted list, CMS will not scan these items in the subsequent antivirus ad scans.

To add apps to trusted list

1. From the **real time alerts** screen while installing apps:



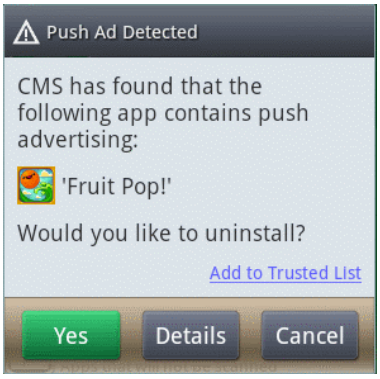
Malicious Software Detected

CMS has found the following malware on your device:

'calc_1_0_6'

Would you like to uninstall?

Add to Trusted List



Push Ad Detected

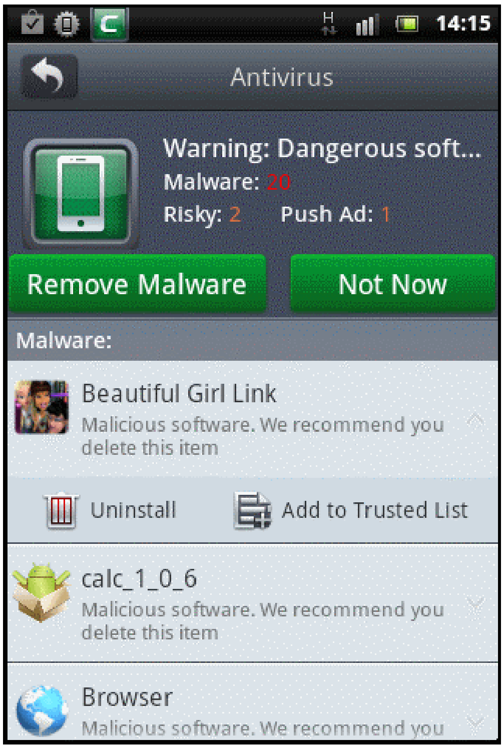
CMS has found that the following app contains push advertising:

'Fruit Pop!'

Would you like to uninstall?

Add to Trusted List

2. From the **antivirus results** screens.

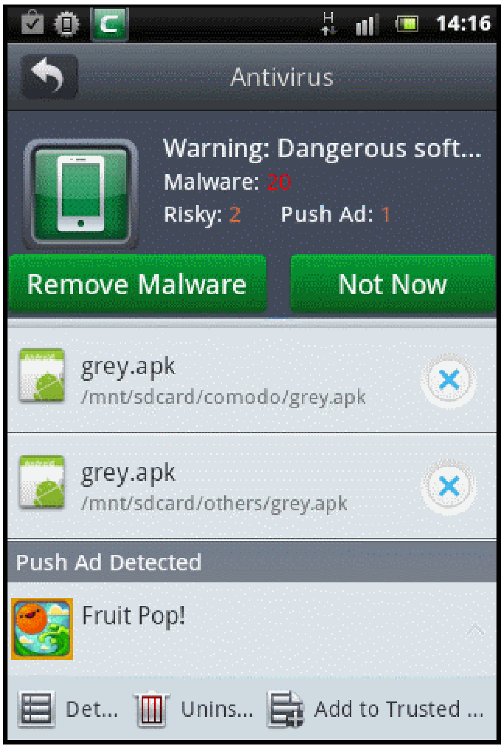


Warning: Dangerous soft...
Malware: 20
Risky: 2 Push Ad: 1

Beautiful Girl Link
Malicious software. We recommend you delete this item

calc_1_0_6
Malicious software. We recommend you delete this item

Browser
Malicious software. We recommend you



Warning: Dangerous soft...
Malware: 20
Risky: 2 Push Ad: 1

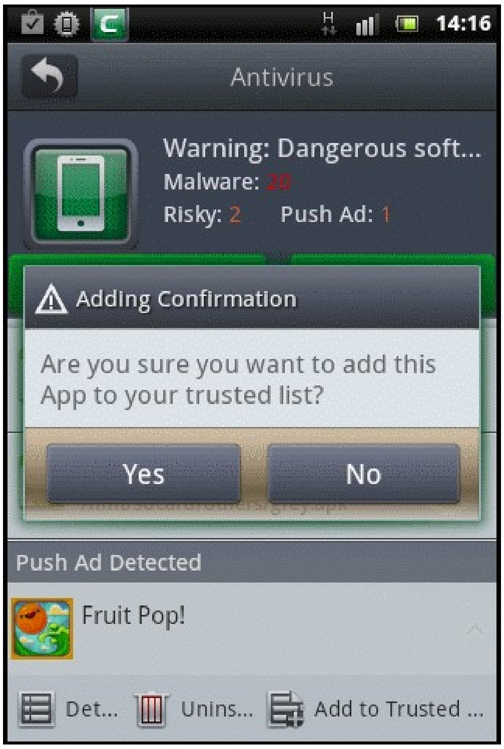
grey.apk
/mnt/sdcard/comodo/grey.apk

grey.apk
/mnt/sdcard/others/grey.apk

Fruit Pop!

- Tap the 'Add to Trusted List' link.

In the confirmation dialog click 'Yes' to add the app to trusted list.



14:16

Antivirus

Warning: Dangerous soft...
Malware: 20
Risky: 2 Push Ad: 1

Adding Confirmation

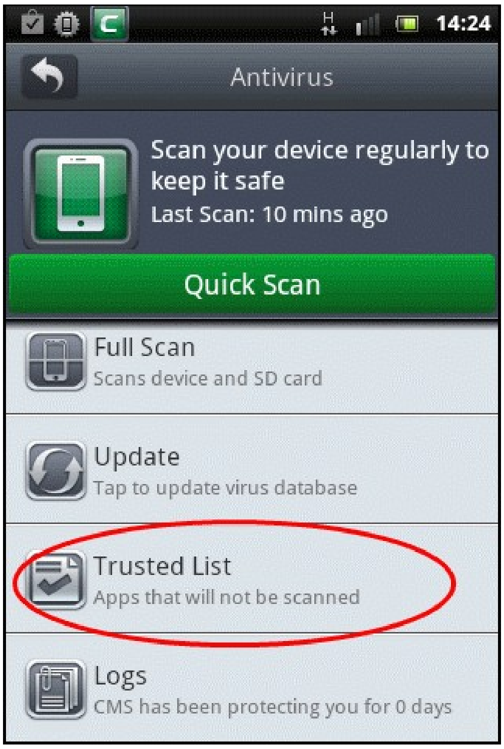
Are you sure you want to add this App to your trusted list?

The apps will be added to the trusted list.

To view the trusted list and delete apps

- Tap 'Antivirus' in the CMS home screen under 'Security' tab.

In the 'Antivirus' screen, tap 'Trusted List' bar.



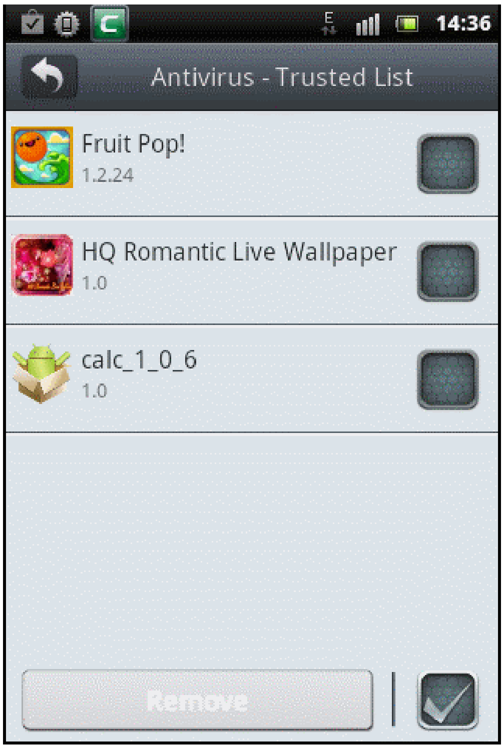
14:24

Antivirus

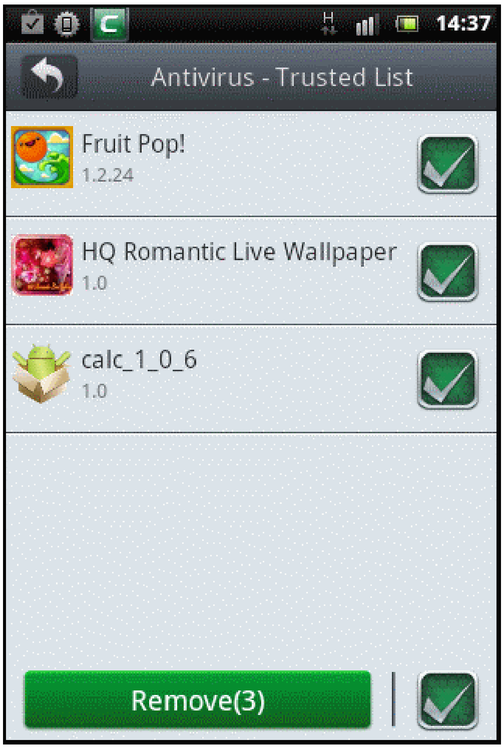
Scan your device regularly to keep it safe
Last Scan: 10 mins ago

Quick Scan
Full Scan
Scans device and SD card
Update
Tap to update virus database
Trusted List
Apps that will not be scanned
Logs
CMS has been protecting you for 0 days

The list of apps added to trusted list will be displayed:



- To remove app(s) from the list, tap on the box at the far right and tap the 'Remove' button.
- To remove all the apps from the list, tap on the box next to the 'Remove' button and tap 'Remove'.



Please note that removing the app from the list will not delete the application from your device. CMS will again display the removed app in the results screen during the subsequent scans if found to be infected or hosts push ads.

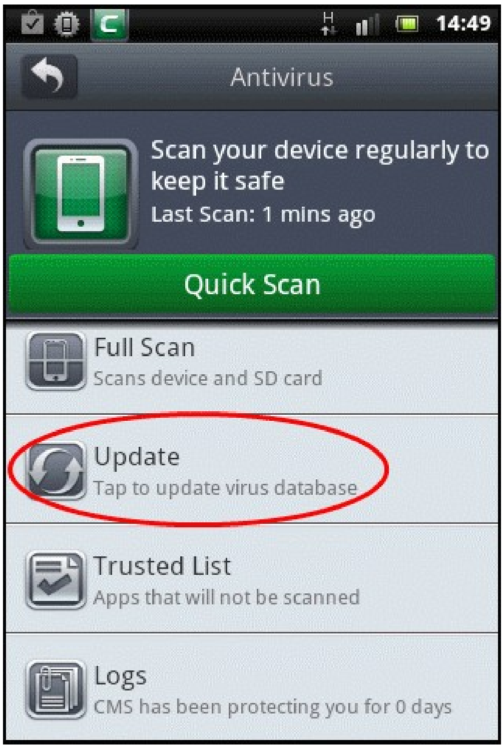
How to update virus database

Use the latest version of CMS antivirus database to protect your device from zero day threats. CMS automatically checks for virus database updates.

To update virus database

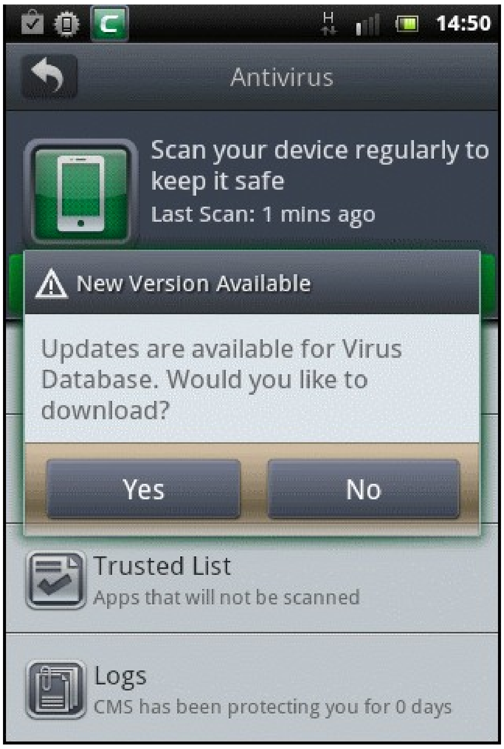
- Tap 'Antivirus' in the CMS home screen under 'Security' tab.

In the 'Antivirus' screen, tap the 'Update' bar.



14:49
Antivirus
Scan your device regularly to keep it safe
Last Scan: 1 mins ago
Quick Scan
Full Scan
Scans device and SD card
Update
Tap to update virus database
Trusted List
Apps that will not be scanned
Logs
CMS has been protecting you for 0 days

CMS will check and display the following screen if any newer version of virus database is available:



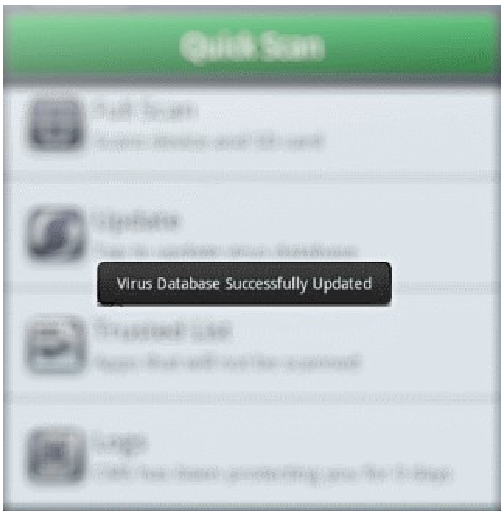
New Version Available

Updates are available for Virus Database. Would you like to download?

14:50
Antivirus
Scan your device regularly to keep it safe
Last Scan: 1 mins ago
Yes
No
Trusted List
Apps that will not be scanned
Logs
CMS has been protecting you for 0 days

- Tap 'Yes' to update the virus database.

The virus database will be updated and after successful completion the following screen will be displayed.



Virus Database Successfully Updated

If the current version of virus database is the latest, then 'Database is up to date' message will be displayed.

Please note that virus database can also be updated from the **Settings** screen.

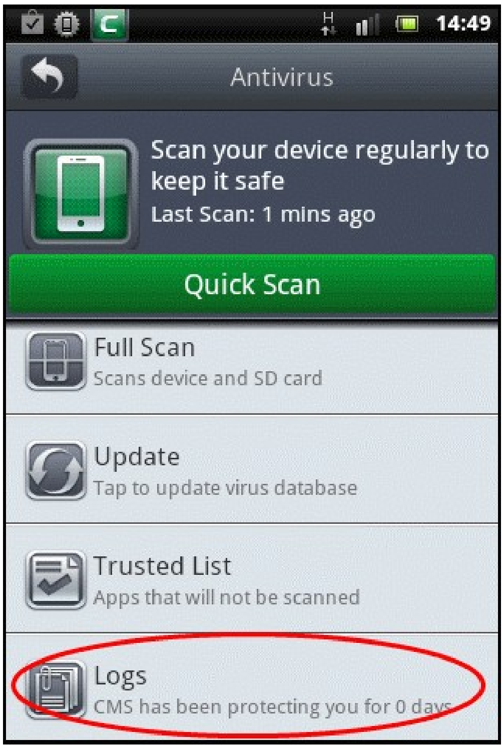
How to check the log

CMS keeps a log of manual scanning and scheduled scanning run in your device.

To view virus scan log

- Tap 'Antivirus' in the CMS home screen under 'Security' tab.

In the 'Antivirus' screen, tap the 'Logs' bar.



Scan your device regularly to keep it safe

Last Scan: 1 mins ago

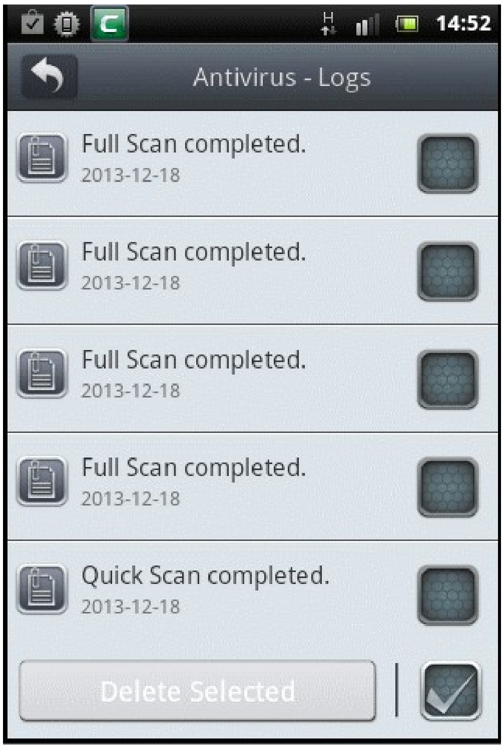
Full Scan
Scans device and SD card

Update
Tap to update virus database

Trusted List
Apps that will not be scanned

Logs
CMS has been protecting you for 0 days

The Antivirus Logs list will be displayed.



Full Scan completed.
2013-12-18

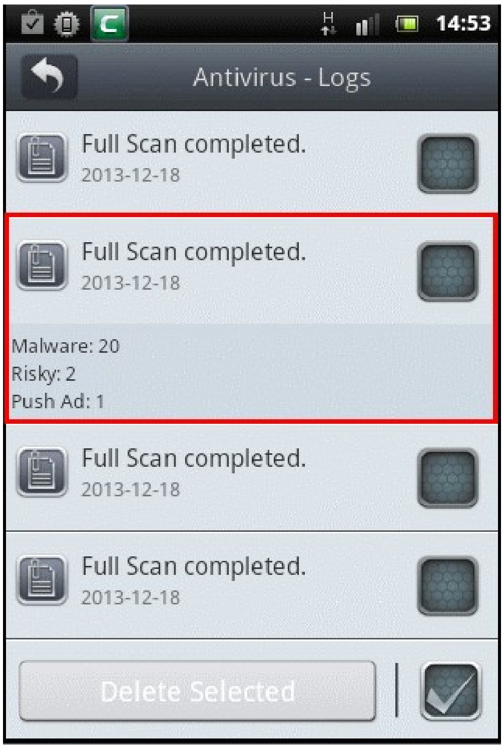
Full Scan completed.
2013-12-18

Full Scan completed.
2013-12-18

Full Scan completed.
2013-12-18

Quick Scan completed.
2013-12-18

- Tap on any of the log in the list to view the details of the antivirus scan.



Full Scan completed.
2013-12-18

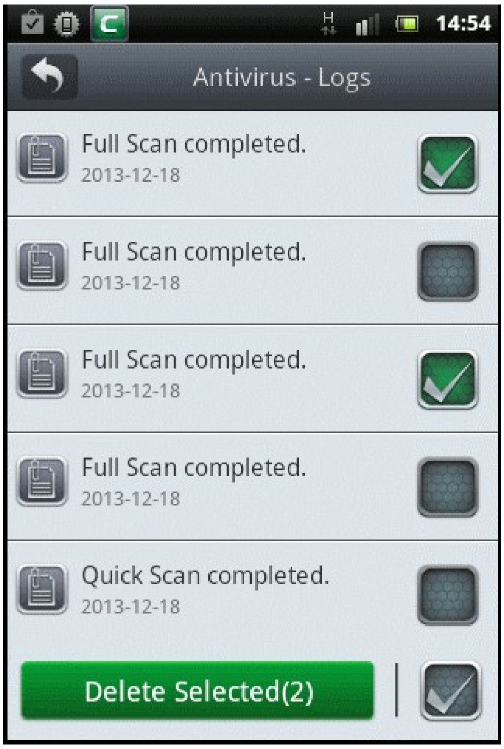
Full Scan completed.
2013-12-18

Malware: 20
Risky: 2
Push Ad: 1

Full Scan completed.
2013-12-18

Full Scan completed.
2013-12-18

- To delete all the logs in the list, tap the box next to the 'Deleted Selected' button at the bottom right. All the logs will be selected.
- To delete specific log(s), tap on the box at far right of the respective logs.



Full Scan completed. 2013-12-18 ☑

Full Scan completed. 2013-12-18 □

Full Scan completed. 2013-12-18 ☑

Full Scan completed. 2013-12-18 □

Quick Scan completed. 2013-12-18 □

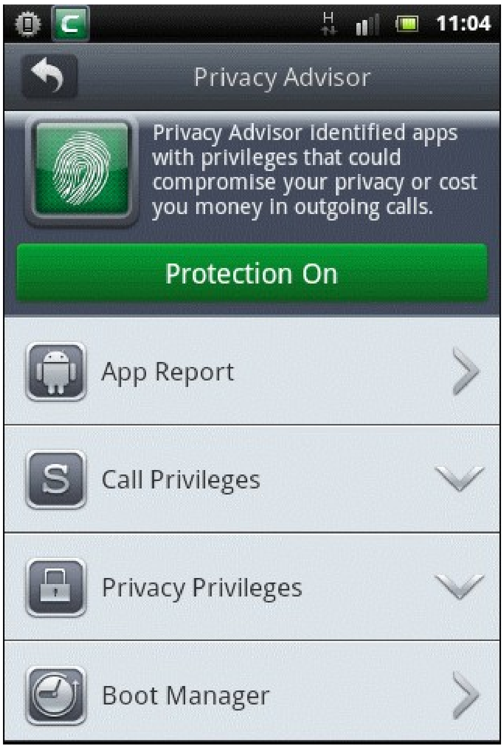
- Tap the 'Delete Selected' button.

The selected logs will be deleted.

4. Privacy Advisor

Privacy Advisor identifies those apps on your device whose permissions could allow them to compromise your privacy or cost you money in outgoing calls/texts.

Important Note: To enable this feature, your Android device should be rooted. Please note that rooting the device may invalidate the warranty for your device.



Privacy Advisor

Privacy Advisor identified apps with privileges that could compromise your privacy or cost you money in outgoing calls.

The 'Protection On' button toggles between On and Off statuses for rooted devices. If the button is in 'On' status, the settings configured for each of the app under the four main categories will be enabled. Keeping this button in 'Off' status will disable the Privacy Advisor feature, meaning the settings configured for the apps will not be enabled.

Click the links below for help with common tasks:

- **How to view and manage apps that have various access privileges**
- **How to identify and manage apps that have call and SMS privileges**
- **How to identify and manage apps that have privacy privileges**
- **How to manage apps that have device boot access**

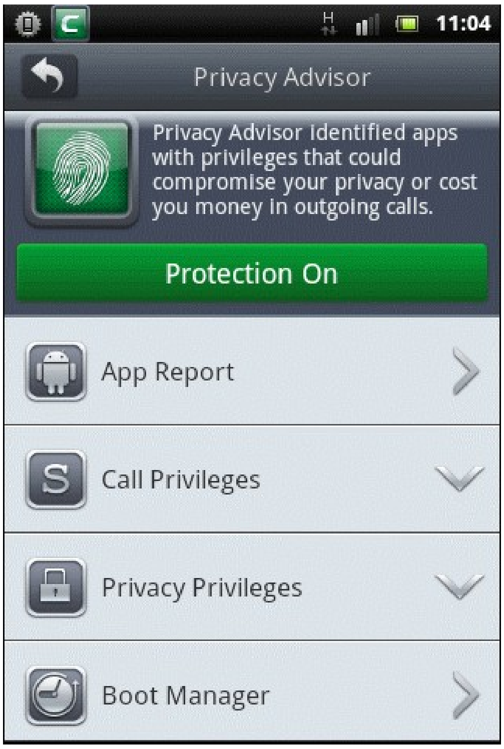
How to view and mange apps that have various access privileges

The App Report feature in Privacy Advisor displays all installed apps as well as system apps that have various privileges such as location tracking, access to device details and so on.

To view and manage apps that have various access privileges

- Select 'Privacy Advisor' in the CMS home screen under the 'Security' tab.

The Privacy Advisor screen will be displayed.

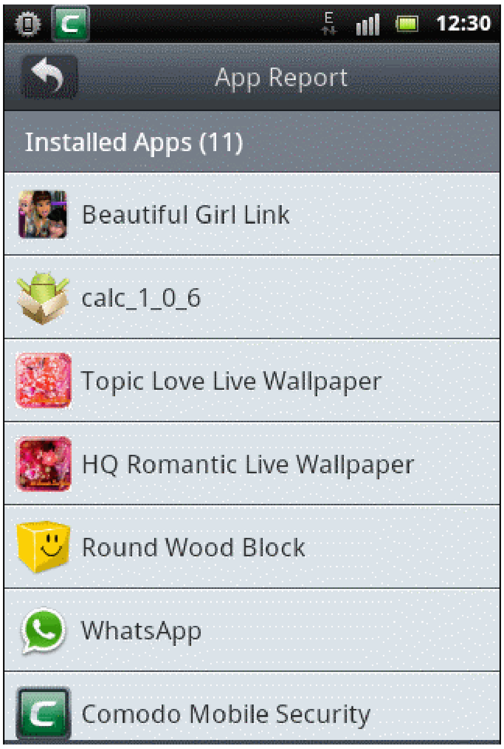


Privacy Advisor

Privacy Advisor identified apps with privileges that could compromise your privacy or cost you money in outgoing calls.

- Tap 'App Report'.

The list of apps, installed as well as system apps, that have various privileges will be displayed.



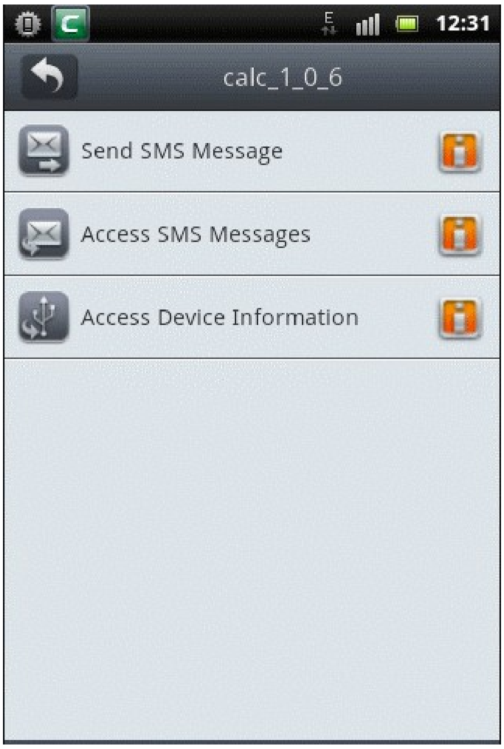
App Report

Installed Apps (11)

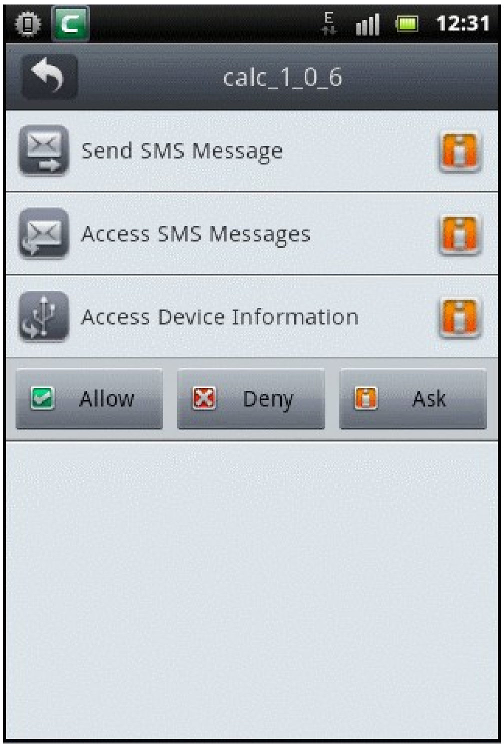
- Beautiful Girl Link
- calc_1_0_6
- Topic Love Live Wallpaper
- HQ Romantic Live Wallpaper
- Round Wood Block
- WhatsApp
- Comodo Mobile Security

- Tap on an app to view its privileges

The privileges for the selected app with its current status will be displayed.



- Tap on any of the privileges to configure its settings.



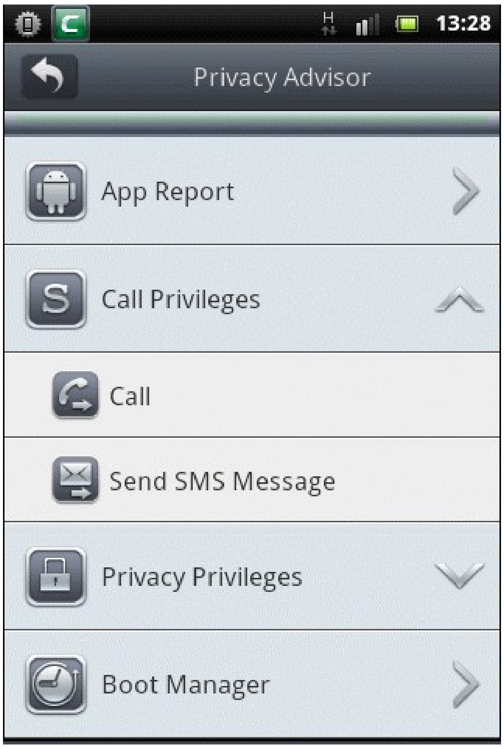
  - **Allow** - CMS will allow this privilege for the app
  - **Deny** - CMS will deny this privilege for the app
  - **Ask** - CMS will seek permission from the user whether to allow or deny this privilege for the app
- Select the permission level from the above options

How to identify and manage apps that have call and SMS privileges

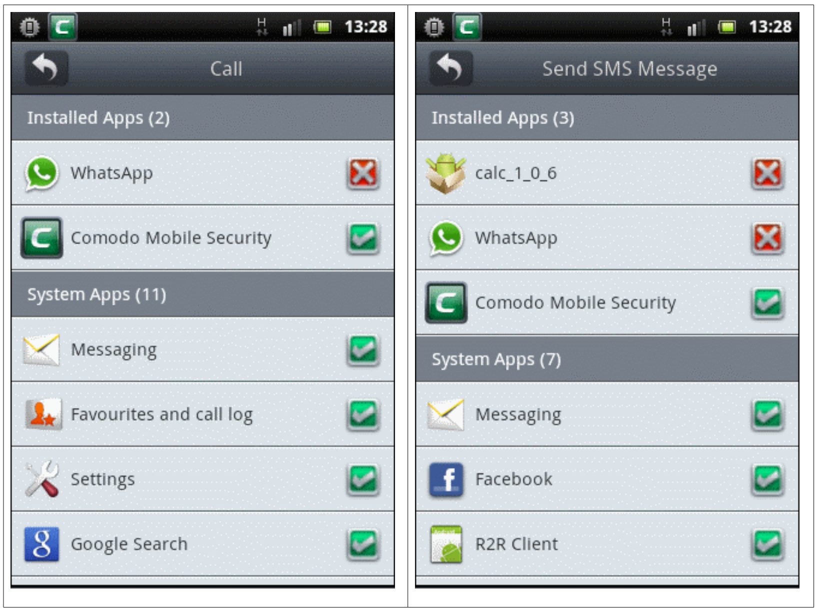
CMS is capable of identifying and listing installed as well as system apps that have call and / or SMS privileges that could compromise your privacy and cost you money in outgoing calls / text messages.

To view and manage apps with call / SMS privileges

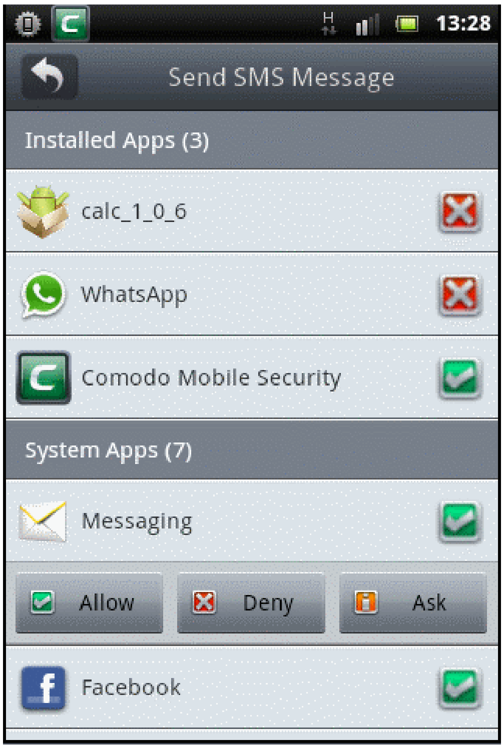
- Select 'Privacy Advisor' in the CMS home screen under the 'Security' tab.
- Tap 'Call Privileges' to expand the section.



- Tap anywhere on 'Call' or 'Send SMS Message' bars to view the list of apps that have call / SMS privileges and its current permission level.



- Select the app that you want to configure its permission settings.



- **Allow** - CMS will allow this privilege for the app
- **Deny** - CMS will deny this privilege for the app
- **Ask** - CMS will seek permission from the user whether to allow or deny this privilege for the app

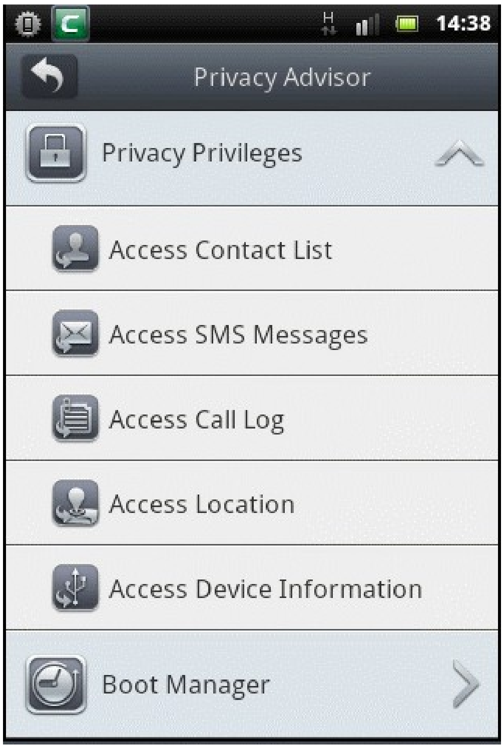
- Select the permission level from the above options

How to view and and manage apps with privacy privileges

The Privacy Privileges feature in Privacy Advisor displays all installed apps as well as system apps that have privacy privileges such as accessing contact list, text messages, cal logs and so on.

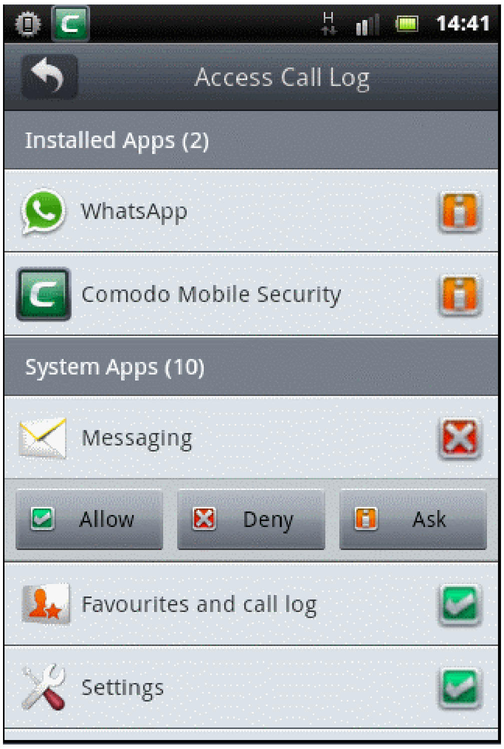
To view and manage apps with privacy privileges

- Tap 'Privacy Advisor' in the CMS home screen under the 'Security' tab.
- Tap 'Privacy Privileges' to expand the section.



- **Access Contact List** - Apps that have access to your contact list. These apps could collect details such as your friends' phone numbers, email address and other data.
- **Access SMS Messages** - Apps that have access to your text messages. These apps could leak your confidential conversations.
- **Access Call Log** - Apps that have access to your phone call logs. These apps could leak a history of the calls you have made and received.
- **Access GPS Location** - Apps that could track your location. These apps could leak your location and track your traveling activities.
- **Access Device Information** - Apps that have access to your device details. These apps could use device information for, amongst other items, targeted marketing campaigns.

Select any app from one of the lists above to manage its settings. An example of the 'Manage Applications' screen is shown below:



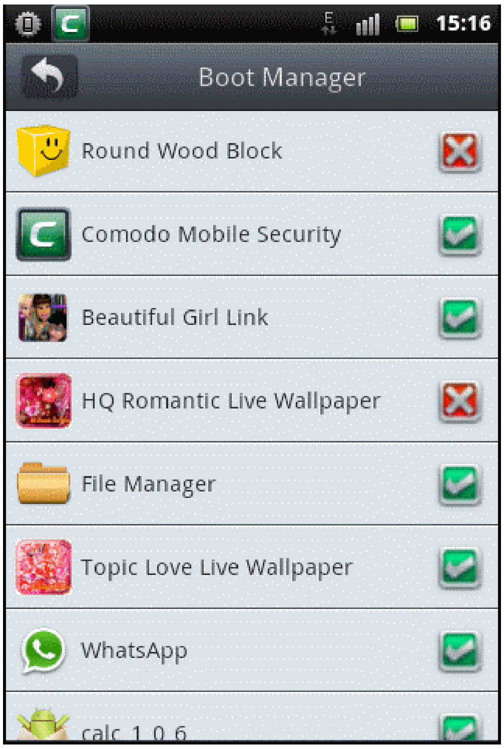
  - **Allow** - CMS will allow this privilege for the app
  - **Deny** - CMS will deny this privilege for the app
  - **Ask** - CMS will seek permission from the user whether to allow or deny this privilege for the app
- Select the permission level from the above options

How to view and manage start up apps

The Boot Manager feature in Privacy Advisor displays all installed apps that start automatically when the device boots up. Disabling apps from auto-starting speeds boot up time and conserves battery.

To view and manage start up apps

- Tap 'Privacy Advisor' in the CMS home screen under the 'Security' tab
- Tap 'Boot Manager' to view all the start up apps



The ✓ icon beside app(s) indicates the start up apps and ☒ icon indicates apps that are disabled during start up. To enable or disable an app from starting up during device boot up, click anywhere on the row of the app. The status icon at the far end will change accordingly.

5. Traffic Monitoring

The Traffic Monitoring utility helps you to keep track of your usage of 2G/3G data on a daily or monthly basis. Apart from providing an statistical overview of usage over time, it can also alert you if you are about to reach your Internet or data plan limits. This allows you to:

- Control how much traffic you use on a daily and monthly basis
- Quickly find out if you are paying your provider for more traffic than you ever realistically use
- Make informed decisions about future data plan selections

You can view real-time statistics of data usage by each application running currently, identify the data expensive applications and to stop or uninstall them.

The Firewall feature in Traffic Monitoring allows you block apps in the device from accessing the Internet.

Important Note: To access the Firewall feature, your Android device should be rooted. Please note that rooting the device may invalidate the warranty for your device.

Click the links below for help with Traffic Monitoring:

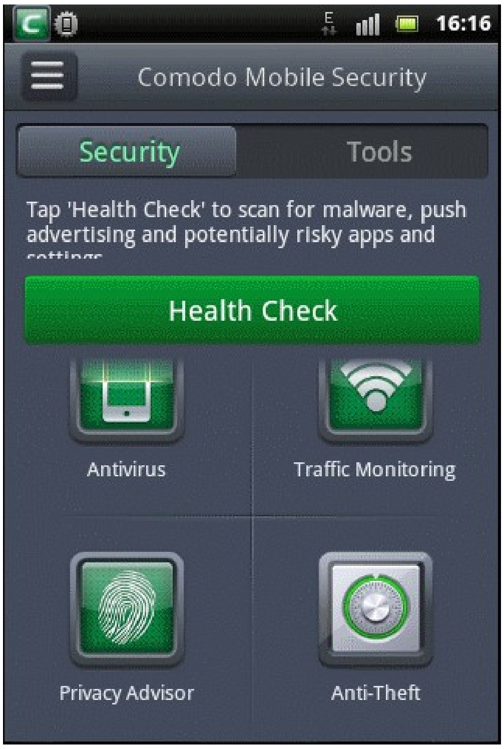
- **How to access the Traffic Monitoring interface and view the statistics**
- **How to configure Traffic Monitoring**
  - **How to enable/disable Traffic Monitoring**
  - **How to enable/disable summary in notification panel**
  - **How to set your monthly quota**

  - How to set your current usage
  - How to set the monthly renewal/billing date of your data plan
  - How to set the alert limit
  - How to set your daily usage limit
  - How to reset Traffic Monitoring statistics and data
- How to view data usage on per application basis
- How to block apps accessing the Internet using Firewall

To access the Traffic Monitoring Interface and view the statistics

- Tap the CMS icon on your device.

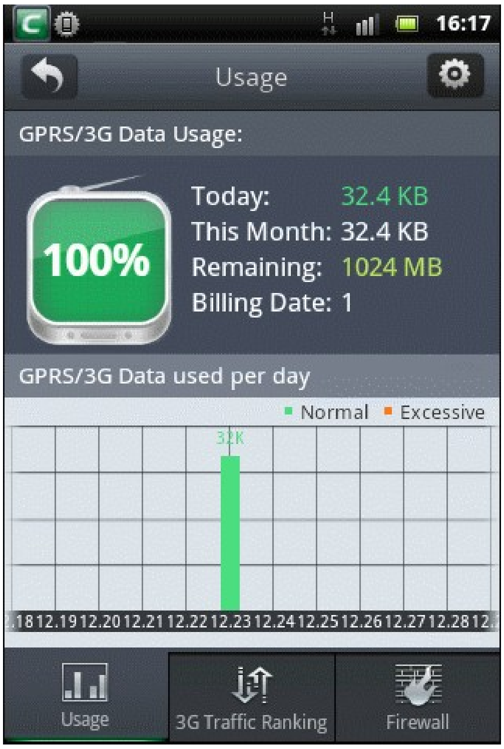
The home page of CMS under Security tab will open.



Tap 'Health Check' to scan for malware, push advertising and potentially risky apps and settings

- Tap 'Traffic Monitoring'.

By default, the 'Usage' screen will be displayed.



Today: 32.4 KB
This Month: 32.4 KB
Remaining: 1024 MB
Billing Date: 1

The interface displays the statistics of your current Internet usage through 2G/3G networks.

GPRS/3G Usage:

The total data usage remaining for the current month is indicated under 'GPRS/3G Usage' as a percentage of the monthly quota set, with the background color alerting the remaining amount:

- 100% - 20% - Green
- 20% - 5% - Yellow
- 5% - 0% - Red

- **Today**: Indicates total Internet usage till current time for today through GPRS/3G
- **This Month**: Indicates total Internet usage till today from the last renewal/billing date

Note: The renewal billing date can be set to any date of the month depending on your billing cycle or your data plan renewal date, so that the usage measurement will be reset and started afresh from the set date every month. Refer to '**Configuring Traffic Monitoring**' for more details on setting the Renewal/Billing date.

- **Remaining**: Indicates the amount of data remaining in current renewal period/billing cycle
- **Billing Date**: Indicates the date of renewal or billing for the next month.

GPRS/3G data used per day:

A graphical representation of Internet usage per day of the current month. The color of the bar changes depending on the percentage of data traffic used on that day with respect to monthly quota.

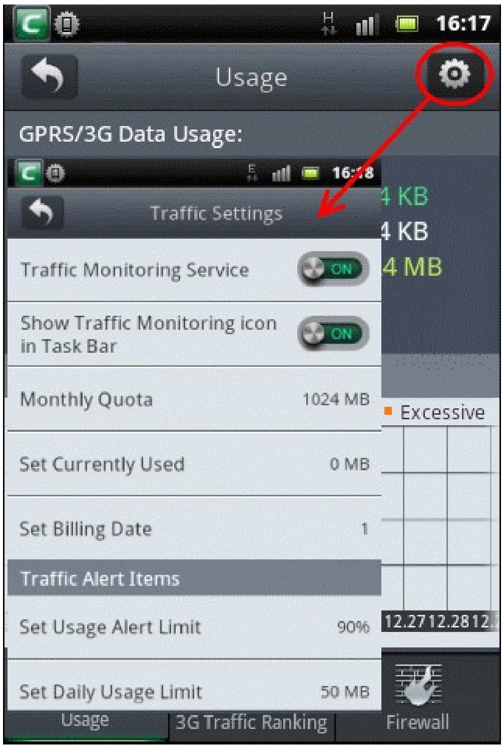
If you want Traffic Monitor to start the monitoring from the start, you can clear the statistics at any time. Refer to **Clearing Traffic Monitoring Statistics** for more details.

The Traffic monitoring feature also displays the summary of today's data usage and remaining usage for the month in the notification panel. You can view this by dragging down the notification bar at the top of the screen.

Note: For display of summary in the notification area, '**Show Traffic Monitoring icon on Task Bar**' should have been enabled in the '**Settings**' interface.

To configure Traffic Monitoring

- Open the 'Settings' interface by tapping the Settings icon at the top right.

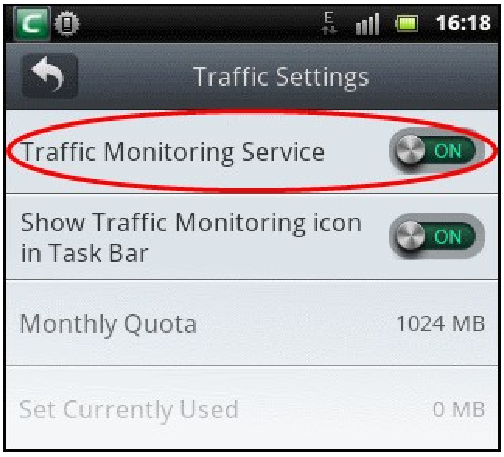


Traffic Settings

Traffic Monitoring Service	ON
Show Traffic Monitoring icon in Task Bar	ON
Monthly Quota	1024 MB
Set Currently Used	0 MB
Set Billing Date	1
Traffic Alert Items	
Set Usage Alert Limit	90%
Set Daily Usage Limit	50 MB

Enabling/Disabling Traffic Monitoring Service

- Open the 'Traffic Settings' interface by tapping the Settings icon at the top right.
- To toggle the feature between enabled and disabled states, tap anywhere on the ' Traffic Monitoring Service' bar.



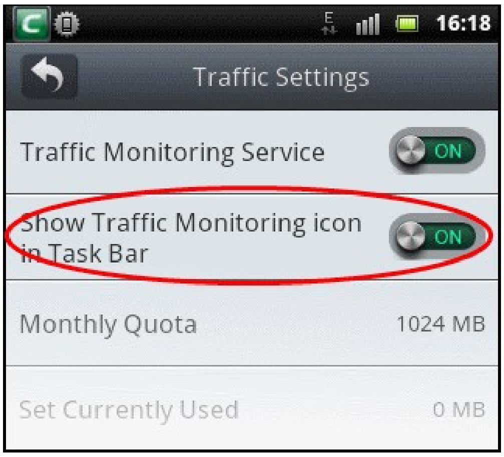
Traffic Settings

Traffic Monitoring Service	ON
Show Traffic Monitoring icon in Task Bar	ON
Monthly Quota	1024 MB
Set Currently Used	0 MB

Enabling/Disabling Traffic Monitoring Summary at Notification Panel

If enabled, Traffic Monitoring will display in the notification panel a summary of your today's data usage and the usage available for the month depending on your Monthly Quota. To view the notification, drag the notification bar at the top of your device screen.

- Open the 'Traffic Settings' interface by tapping the Settings icon at the top right.
- To enable/disable the display at the notification panel, tap anywhere on the 'Show Traffic Monitoring icon on Task Bar' bar.



16:18

Traffic Settings

Traffic Monitoring Service ON

Show Traffic Monitoring icon in Task Bar ON

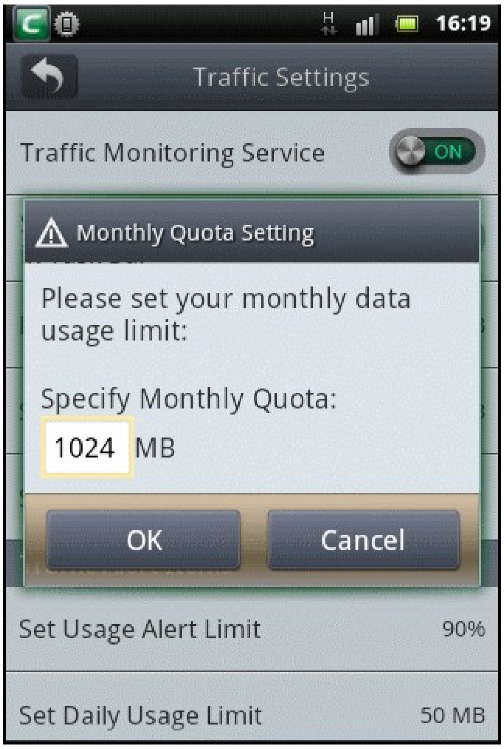
Monthly Quota 1024 MB

Set Currently Used 0 MB

Setting Your Monthly Quota

You can set the limit on your monthly Internet usage depending on your data plan. Traffic monitoring service will display the remaining amount in the main interface and provide an alert on reaching the limit, based on the quota set in this interface.

- Open the 'Traffic Settings' interface by tapping the Settings icon at the top right.
- Tap on the 'Monthly Quota' bar.



16:19

Traffic Settings

Traffic Monitoring Service ON

Monthly Quota Setting

Please set your monthly data usage limit:

Specify Monthly Quota:

1024 MB

Set Usage Alert Limit 90%

Set Daily Usage Limit 50 MB

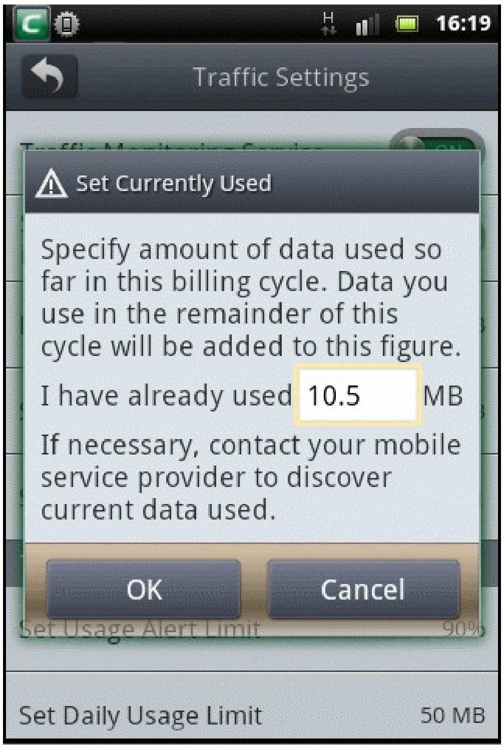
- Enter your monthly usage limit (in MB) in the 'Monthly Quota Setting' dialog and tap 'OK'

The entered limit will be displayed in the 'Monthly Quota' bar of the 'Settings' interface.

Setting your Currently Used Data

You can enter the amount of data usage done so far in the current billing cycle, so that Traffic monitoring will take that into account and add it to the current usage in order to calculate the remaining amount. If you do not know the amount of data usage till date, you can contact your mobile service provider and get the usage amount.

- Open the 'Traffic Settings' interface by tapping the Settings icon at the top right.
- To enter current usage, tap the 'Set Currently Used' bar



Set Currently Used

Specify amount of data used so far in this billing cycle. Data you use in the remainder of this cycle will be added to this figure.

I have already used 10.5 MB

If necessary, contact your mobile service provider to discover current data used.

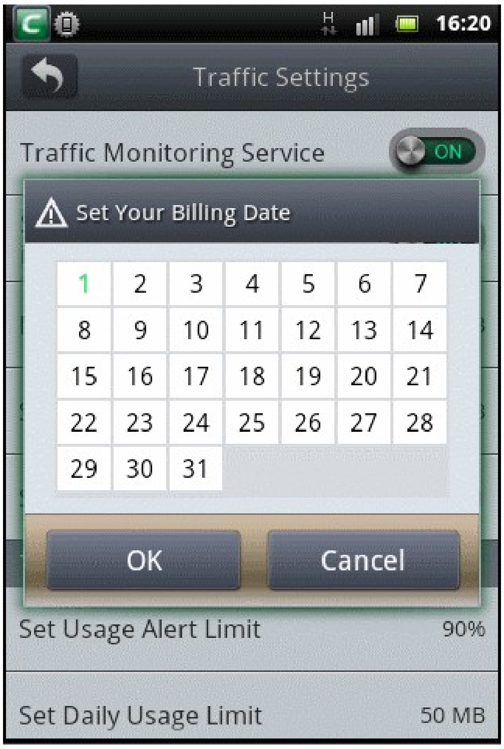
- Enter the usage done so far in the 'Set Currently Used' dialog and tap 'OK'.

The entered amount will be added to your current usage data.

Setting Monthly Billing/Renewal Date of the Billing Cycle

You can set your monthly billing date or monthly renewal date of your data plan to enable Traffic Monitoring to calculate your usage for the current month from the specified date.

- Open the 'Traffic Settings' interface by tapping the Settings icon at the top right.
- To set the billing/renewal date of your data plan, tap 'Set Billing Date' bar.


16:20
Traffic Settings
Traffic Monitoring Service
ON

Set Your Billing Date

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

OK
Cancel
Set Usage Alert Limit 90%
Set Daily Usage Limit 50 MB

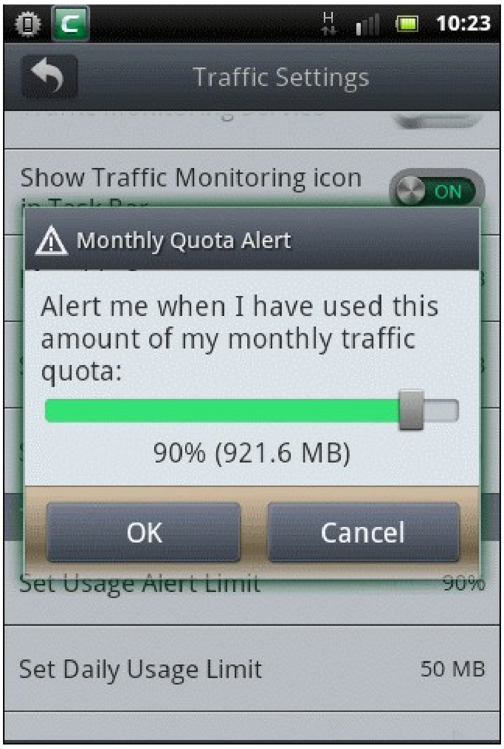
- Select the billing date (1~31) and tap 'OK'.

Alert Settings

Setting the Alert Limit

Traffic Monitoring service will raise an alert when your usage is about to reach your set monthly quota. You can set the usage amount at which you want to be alerted, as percentage of your monthly quota.

- Open the 'Traffic Settings' interface by tapping the Settings icon at the top right.
- To set the alert limit, tap 'Set Usage Alert Limit' bar



Alert me when I have used this amount of my monthly traffic quota:

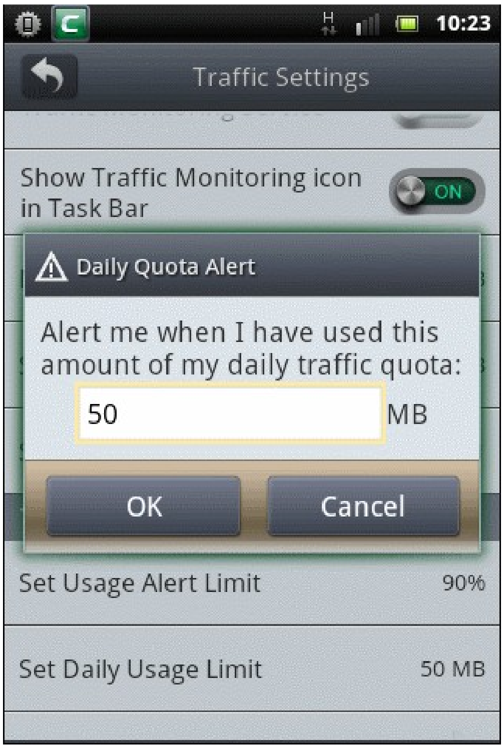
90% (921.6 MB)

- Move the slider to the percentage you want to set as alert limit and tap OK.

Setting Daily Usage Limit

You can set a daily Internet traffic usage limit in MB. You will receive an alert when you are close to exceeding this limit. This can help you quickly gauge whether or not your typical daily usage will keep you within the monthly traffic limit set by your provider. Your daily traffic consumption is also indicated as a bar graph in the 'Traffic Monitoring' interface. This graph also provides an 'at a glance' overview of historical daily usage - including whether or not you exceeded your daily limit on that day.

- Open the 'Traffic Settings' interface by tapping the Settings icon at the top right.
- To set your daily usage limit, tap 'Set Daily Usage Limit' bar.



Traffic Settings

Show Traffic Monitoring icon in Task Bar ON

Daily Quota Alert

Alert me when I have used this amount of my daily traffic quota:

50 MB

Set Usage Alert Limit 90%

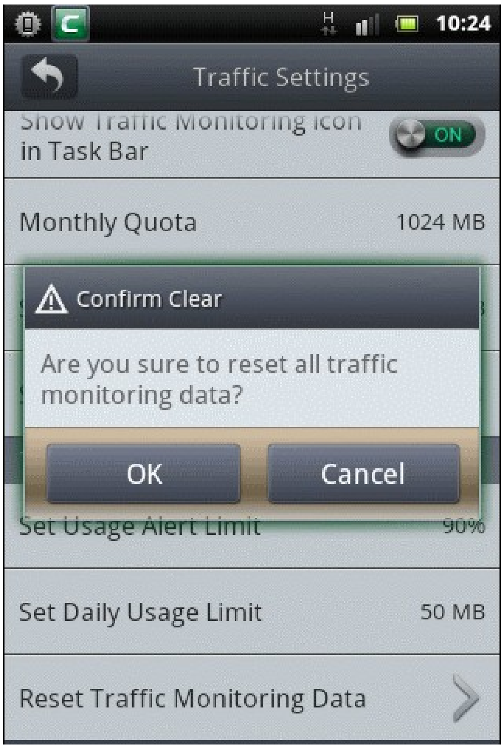
Set Daily Usage Limit 50 MB

- Enter your usage limit for a day (in MB) in the 'Daily Quota Alert' dialog and tap 'OK'.

Clearing Traffic Monitoring Statistics

You can reset the usage amount calculated so far and the other statistics retained by Traffic Monitoring Service.

- Open the 'Traffic Settings' interface by tapping the Settings icon at the top right.
- To clear all the stored data related to Traffic Monitoring, tap 'Reset Traffic Monitoring Data' bar.



Traffic Settings

Show Traffic Monitoring icon in Task Bar ON

Monthly Quota 1024 MB

Confirm Clear

Are you sure to reset all traffic monitoring data?

Set Usage Alert Limit 90%

Set Daily Usage Limit 50 MB

Reset Traffic Monitoring Data

- Tap OK in the confirmation dialog.

All the traffic statistics in the application will be deleted and the traffic measurement will be started newly.

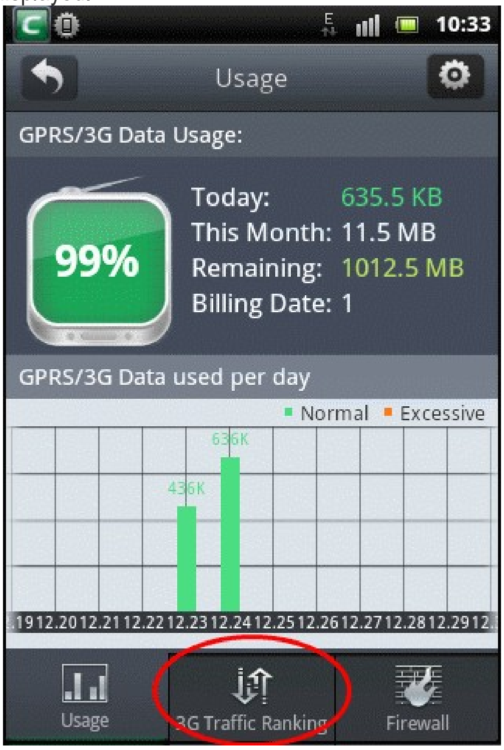
Viewing Cellular Data Traffic per Application

The 2G/3G Data Traffic Ranking feature in Traffic Monitoring of Comodo Mobile Security also allows you to view a break-up details of 2G/3G data usage by each application connecting to the Internet on a daily basis. The indication of real-time data usage by each application enables you to identify the applications that are using the data traffic excessively and running unnecessarily.

To view cellular data usage per application

- Tap 'Traffic Monitoring' in the CMS home screen under 'Security' tab.

By default, the 'Usage' screen will be displayed.



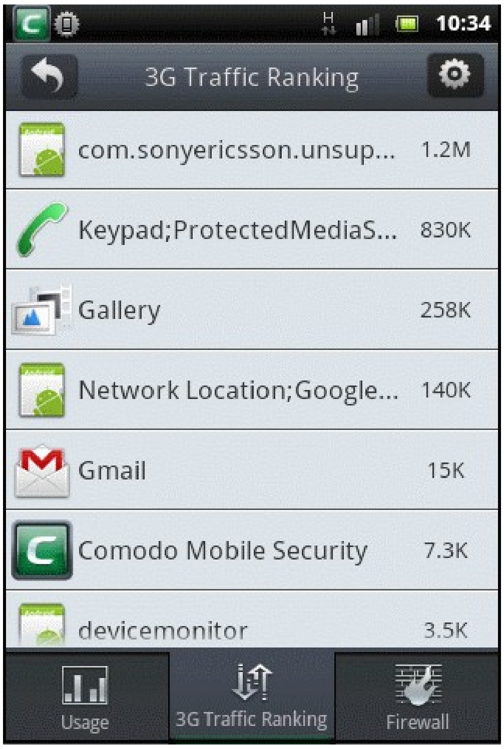
GPRS/3G Data Usage:

Today: 635.5 KB
This Month: 11.5 MB
Remaining: 1012.5 MB
Billing Date: 1

GPRS/3G Data used per day

- Tap '3G Traffic Ranking' at the bottom.

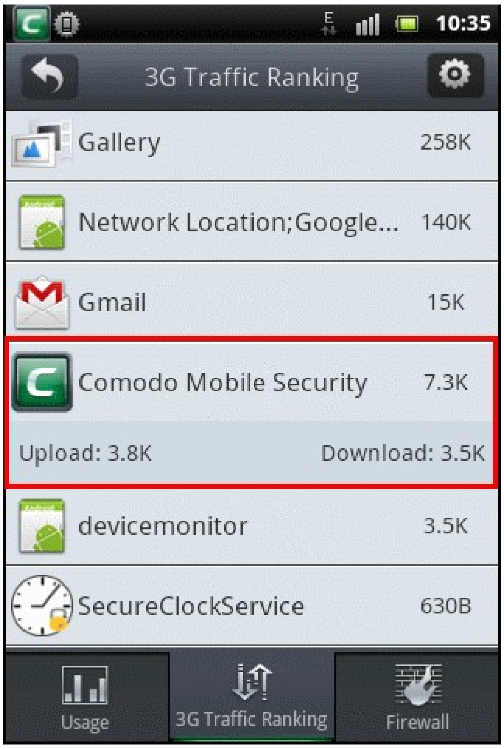
The list of apps that had used data with 3G will be displayed and ranked data usage wise. The highest data used app will be displayed first and the least at the last.



3G Traffic Ranking

com.sonyericsson.unsup...	1.2M
Keypad;ProtectedMediaS...	830K
Gallery	258K
Network Location;Google...	140K
Gmail	15K
Comodo Mobile Security	7.3K
devicemonitor	3.5K

- To view more details on the data usage by an application, tap on the application. The upload and download data used by the application will be displayed.



3G Traffic Ranking

Gallery	258K
Network Location;Google...	140K
Gmail	15K
Comodo Mobile Security	7.3K
Upload: 3.8K	Download: 3.5K
devicemonitor	3.5K
SecureClockService	630B

Blocking apps from accessing the Internet using Firewall

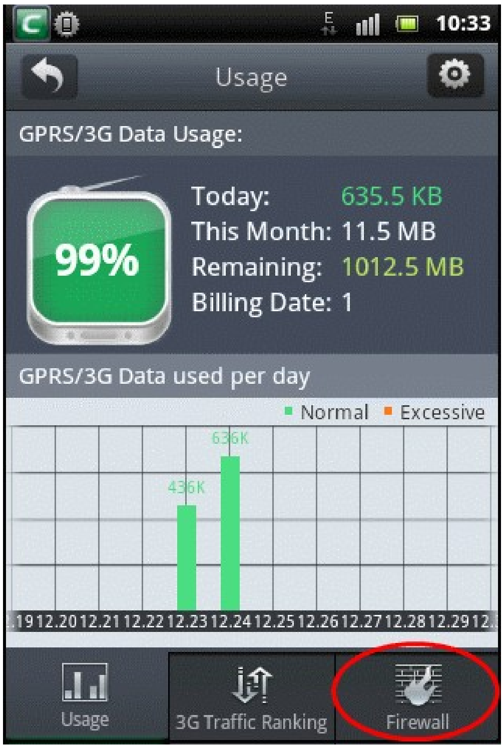
The firewall allows you greater control over which apps are allowed to connect to the Internet. You can control whether an app is allowed to connect using Wi-Fi, 2G/3G, both or neither.

Important Note: To access the Firewall feature, your Android device should be rooted. Please note that rooting the device may invalidate the warranty for your device.

To block apps from accessing the Internet using firewall

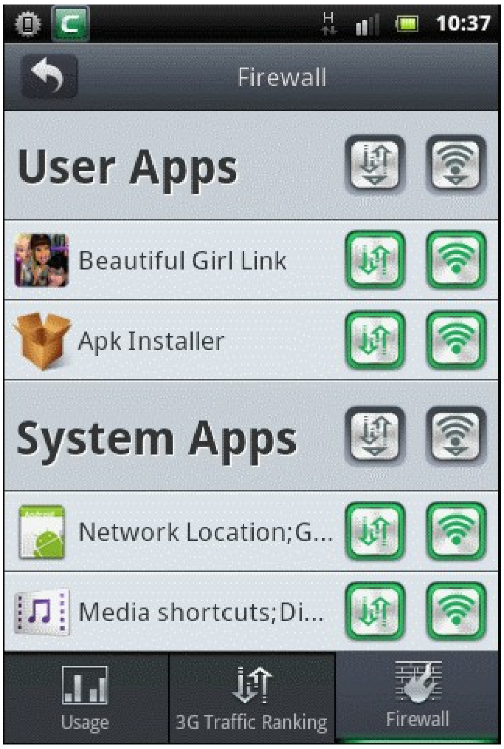
- Tap 'Traffic Monitoring' in the CMS home screen under 'Security' tab.

By default, the 'Usage' screen will be displayed.



- Tap 'Firewall' at the bottom.

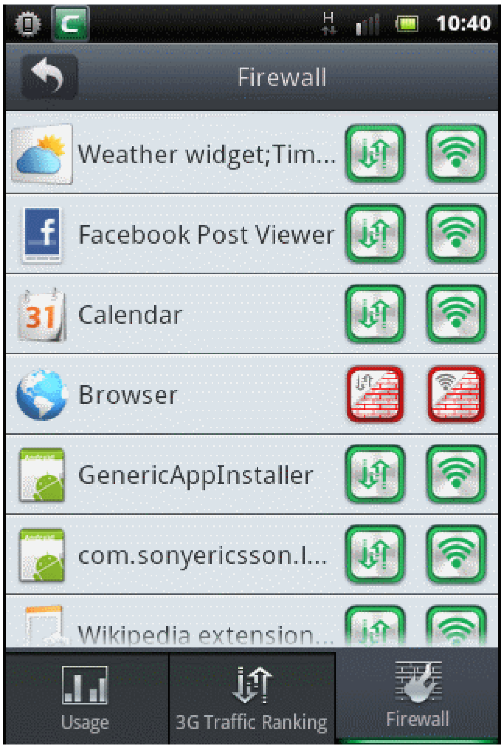
The list of user apps as well as system apps that connects to the Internet will be displayed.



Scroll up or down to view the full list of apps. The first box at the right of each app represents 2G/3G connection and the second box represents WiFi connection.

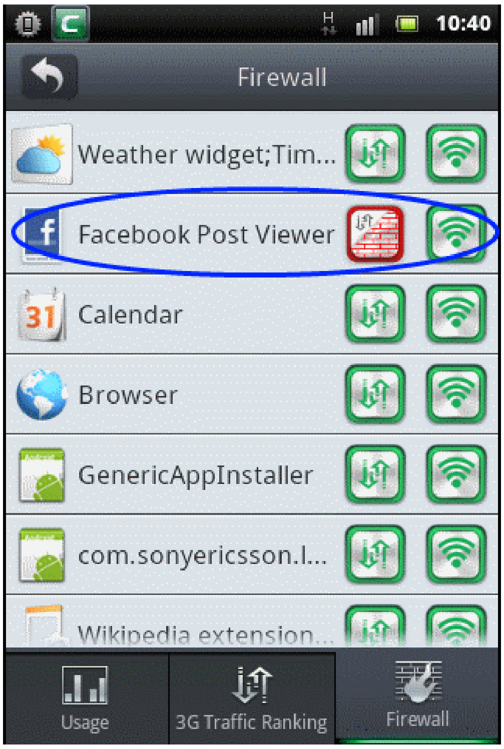
- To block an app from connecting to the Internet, tap on both the boxes in the bar.

The boxes turn red meaning the app cannot connect to the Internet by any means. An example is shown below.



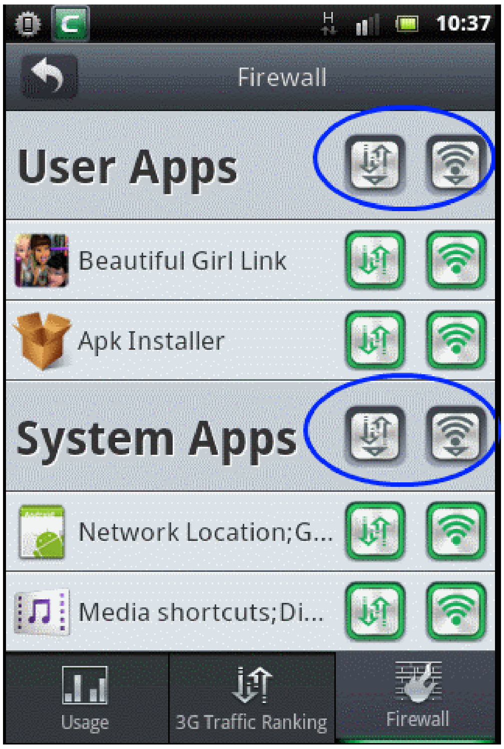
- Tap on the boxes once again to enable the app to connect to the Internet.

If you want an app to connect only via WiFi and not via 2G/3G connection, then tap on the first box in the row.



The 2G/3G box turns red and the app can connect to the Internet only via WiFi connection. Similarly you can allow an app to connect to the Internet only via 2G/3G connection and deny access via WiFi.

You can select and block or allow Internet connection via WiFi / 2G/3G all apps by tapping on the respective boxes at the top beside User Apps / System Apps.



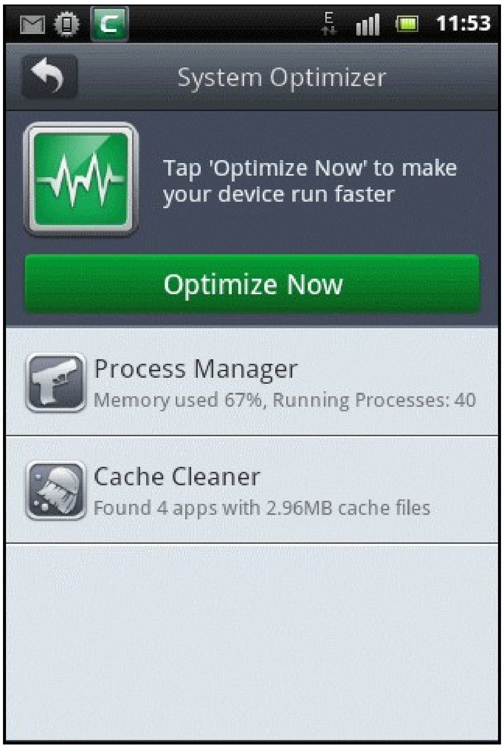
6. System Optimizer

CMS gives you full visibility and control over running processes. You can see how many are running, how much memory each uses and can quickly close down the ones you don't want. Software Manager helps you kill apps and clean temporary files in cache memory which may be slowing down your phone down. Click the links given below for more details.

- How to optimize your device with a single tap
- How to view and kill the processes running in your Android device
- How to clean cache memory

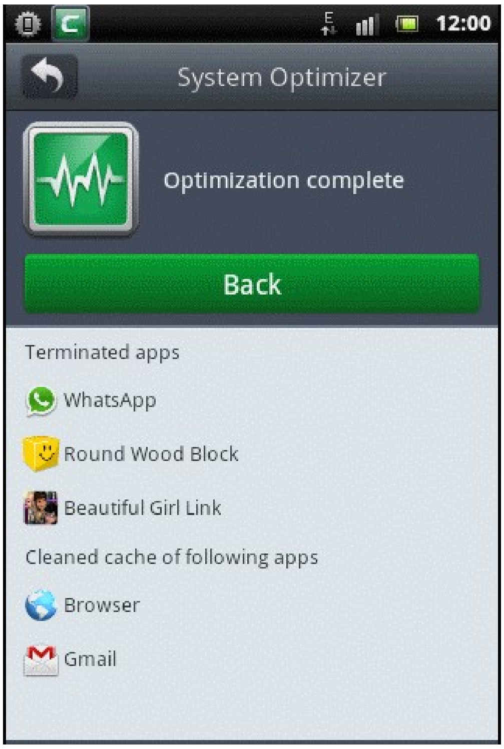
How to optimize your device your device with a single tap

- Tap the CMS icon on your device.
- Tap 'Tool's tab located at the top or swipe to the left and tap 'System Optimizer'.


11:53
System Optimizer
Tap 'Optimize Now' to make your device run faster
Optimize Now
Process Manager
Memory used 67%, Running Processes: 40
Cache Cleaner
Found 4 apps with 2.96MB cache files

In the 'System Optimizer' screen, tap the 'Optimize Now' button.

CMS will terminate apps that are running and also clean the cache memory. The list of terminated apps and cleaned cache memory for the apps will be displayed.



Optimization complete

Terminated apps

WhatsApp

Round Wood Block

Beautiful Girl Link

Cleaned cache of following apps

Browser

Gmail

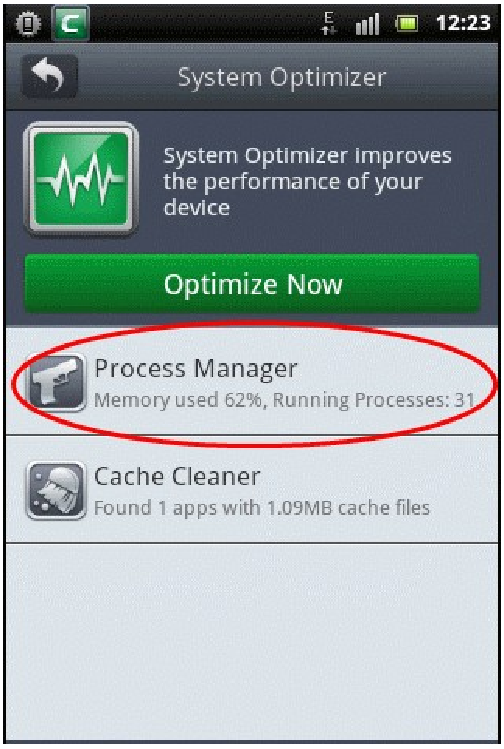
- Tap the 'Back' button to return to the 'System Optimizer' home screen.

How to view and kill the processes running in your Android device

The System Optimizer feature allows you to view and kill running processes. It also displays the memory used by each of them and available memory at the top.

To view running process

- Tap the CMS icon on your device.
- Tap 'Tool's tab located at the top or swipe to the left and tap 'System Optimizer'.



System Optimizer

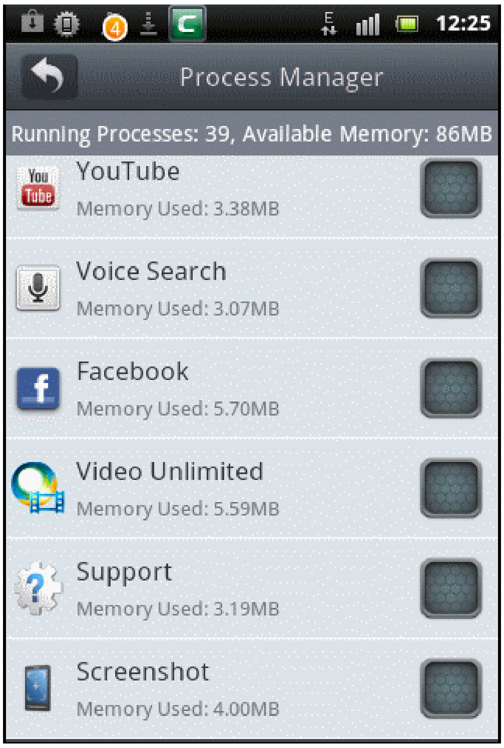
System Optimizer improves the performance of your device

Optimize Now

Process Manager
Memory used 62%, Running Processes: 31

Cache Cleaner
Found 1 apps with 1.09MB cache files

- Tap the Process Manager bar, which displays the number of processes running and the memory used.



Process Manager

Running Processes: 39, Available Memory: 86MB

YouTube
Memory Used: 3.38MB

Voice Search
Memory Used: 3.07MB

Facebook
Memory Used: 5.70MB

Video Unlimited
Memory Used: 5.59MB

Support
Memory Used: 3.19MB

Screenshot
Memory Used: 4.00MB

The list of running processes and the memory used by each of them will be displayed.

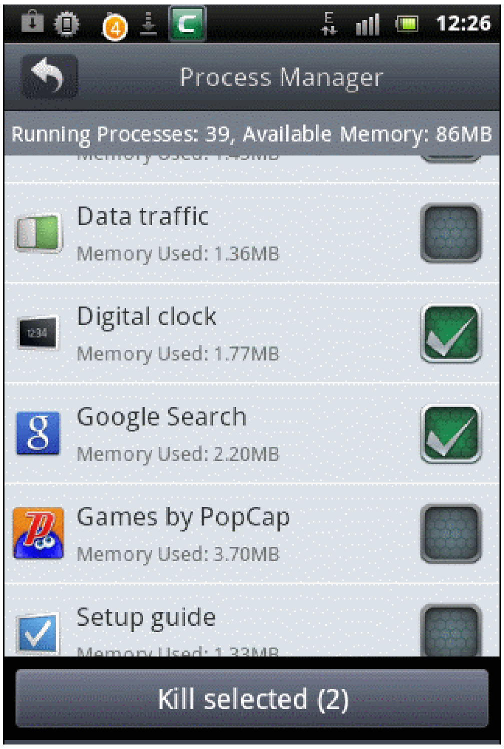
To kill the running process

- Tap the CMS icon on your device.
- Tap 'Tool's tab located at the top or swipe to the left and tap 'System Optimizer'.

- Tap the Process Manager bar, which displays the number of processes running and the memory used.

The Process Manager screen displays the list of running process. You can choose to kill a single or running multiple processes.

- Tap on the box(es) at the far end of the process that you want to kill.



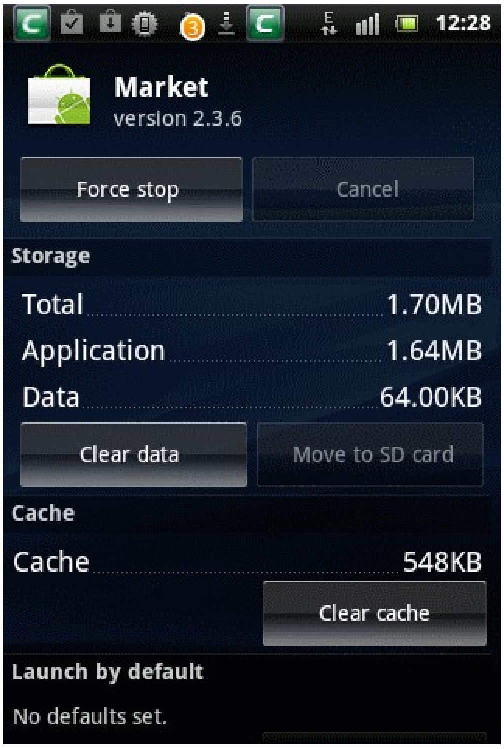
Running Processes: 39, Available Memory: 86MB

Data traffic Memory Used: 1.36MB	□
Digital clock Memory Used: 1.77MB	☑
Google Search Memory Used: 2.20MB	☑
Games by PopCap Memory Used: 3.70MB	□
Setup guide Memory Used: 1.33MB	□

- Tap 'Kill Selected'.

The selected running process(es) will be terminated and the memory used will be freed up.

Depending on the type of process selected, you can force stop, uninstall, move to SD card, clear data or clear cache. Tap on any of the running process bar in the screen. An example of the 'Manage Applications' screen is shown below:

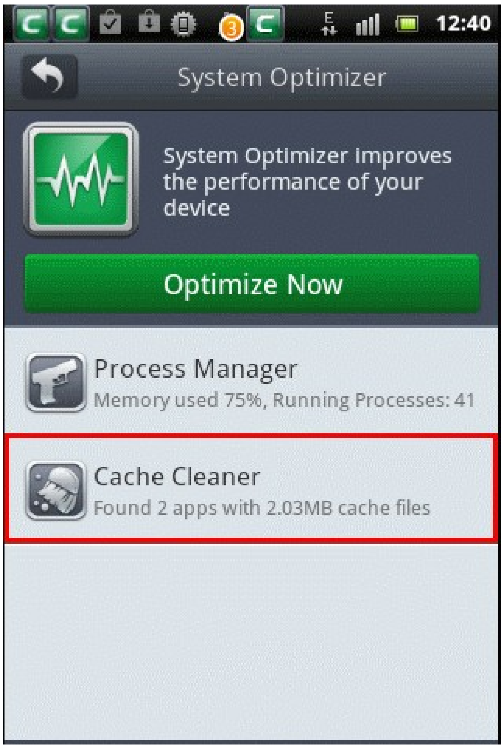


Total	1.70MB
Application	1.64MB
Data	64.00KB
Cache	548KB

No defaults set.

How to clean cache memory

- Tap the CMS icon on your device.
- Tap 'Tool's tab located at the top or swipe to the left and tap 'System Optimizer'.
- Tap the Cache Cleaner bar, which displays the number of apps that currently uses cache memory for storing temporary files.

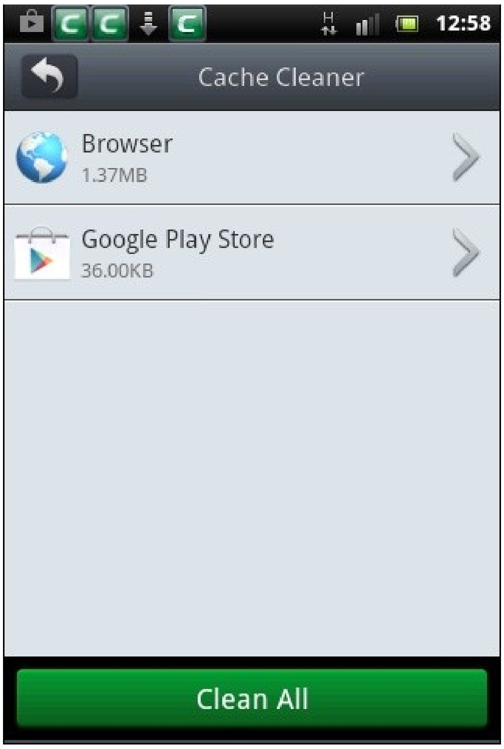


System Optimizer improves the performance of your device

Memory used 75%, Running Processes: 41

Found 2 apps with 2.03MB cache files

The list of apps with caches files will be displayed.

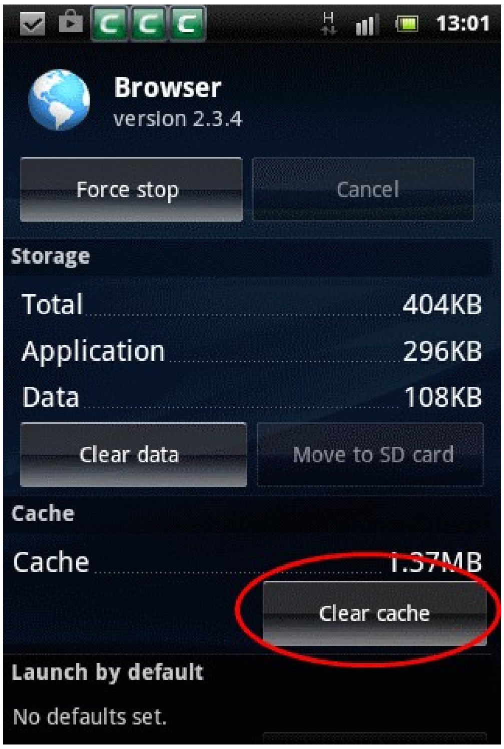


Browser
1.37MB

Google Play Store
36.00KB

You can choose to clean all the cache files of all the apps or clean for a particular app. To clean the cache file of a single app, tap anywhere on the bar.

The Manage Application screen will be displayed.



Browser
version 2.3.4

Storage

Total 404KB
Application 296KB
Data 108KB

Cache

Cache 1.37MB

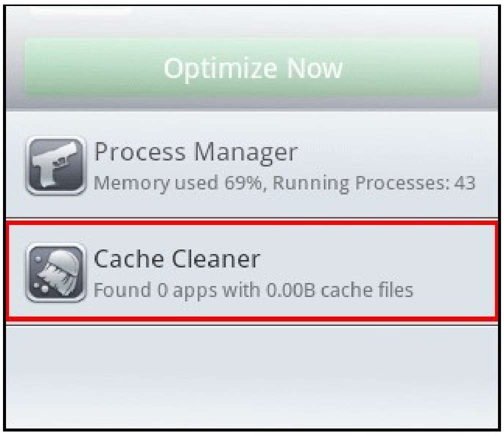
Launch by default

No defaults set.

- Tap 'Clear cache'.

The cache files for the selected app will be cleared.

To clear all the cache files, tap the 'Clean All' button. All the temporary files will be cleared.


Optimize Now
Process Manager
Memory used 69%, Running Processes: 43
Cache Cleaner
Found 0 apps with 0.00B cache files

7.Private Space

Your Private Space is where you store contacts, phone numbers and text messages that are for your eyes only. Once added, you will be the only person able to view these contacts and any communications from them. In addition, you can password protect apps in your device and encrypt images and other files / folders.

Click the links below for help with common tasks:

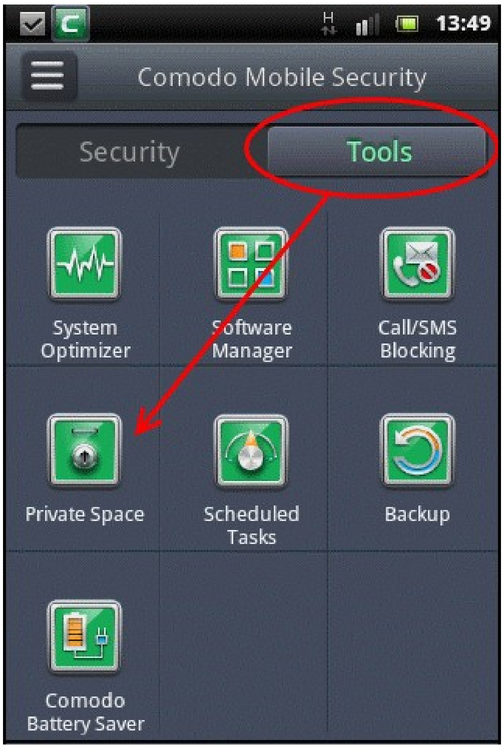
- How to set a password for your private space
- How to add contacts into your private space
- How to import a private contact's records
- How to manage a private SMS message
- How to manage a private call
- How to password protect your apps in your device
- How to reset a forgotten password
- How to change your password
- How to encrypt your files
- How to decrypt your files

How to set a password for your private space

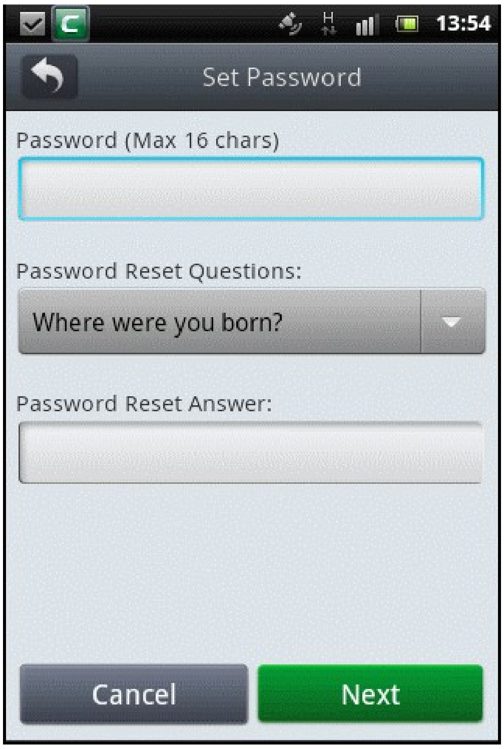
Setting a password for your private space is a very easy and quick process.

To set a password for your private space

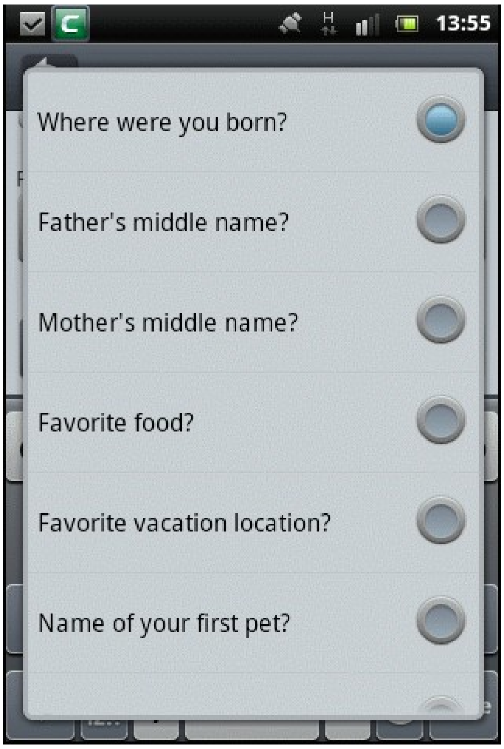
- Tap the CMS icon on your device.
- Tap 'Tool's tab located at the top or swipe to the left and tap 'Private Space'.



The 'Set Password' screen will be displayed.



- Tap the 'Password' field and enter your password and tap 'Next'.
- Tap the drop-down icon ▾ to select the Reset Questions.



Where were you born? ●

Father's middle name? ○

Mother's middle name? ○

Favorite food? ○

Favorite vacation location? ○

Name of your first pet? ○

- Select a Reset Question and enter your Password Reset Answer.
- Tap 'OK' to confirm your setting or 'Cancel' to cancel the setting.

That's it. Your password for using the private space is set and enter it each time you access this feature.

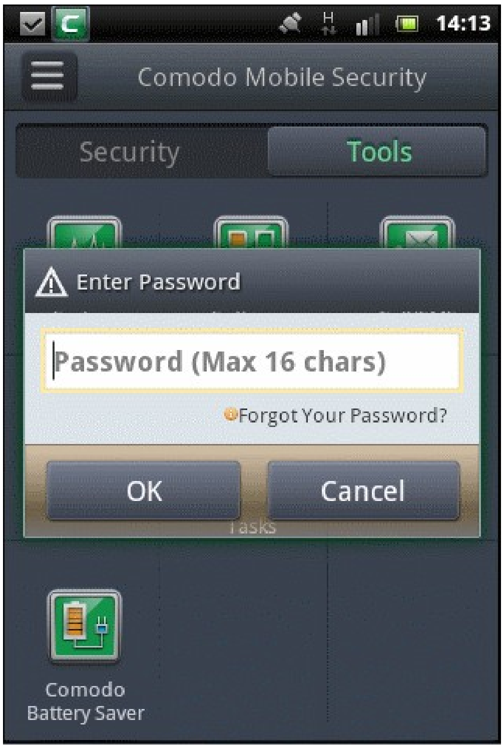
How to add contacts into your private space

You can add contacts manually, import from call records or SMS records into your private space.

To add contacts into your private space

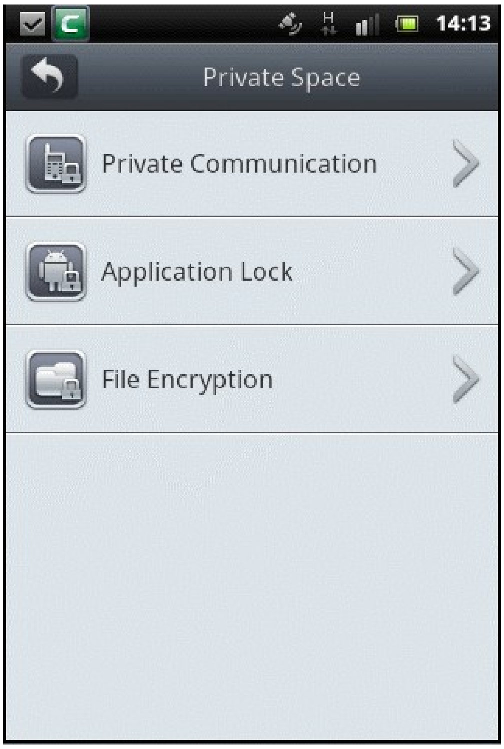
- Tap the CMS icon on your device.
- Tap 'Tool's tab located at the top or swipe to the left and tap 'Private Space'.

The 'Enter Your Password' screen will be displayed.



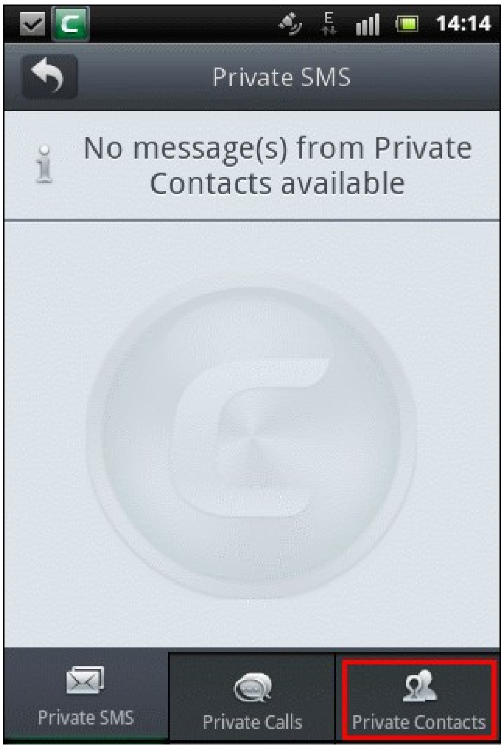
- Tap the 'Password' field and enter the password that you have set in this field.

The Private Space screen will be displayed.



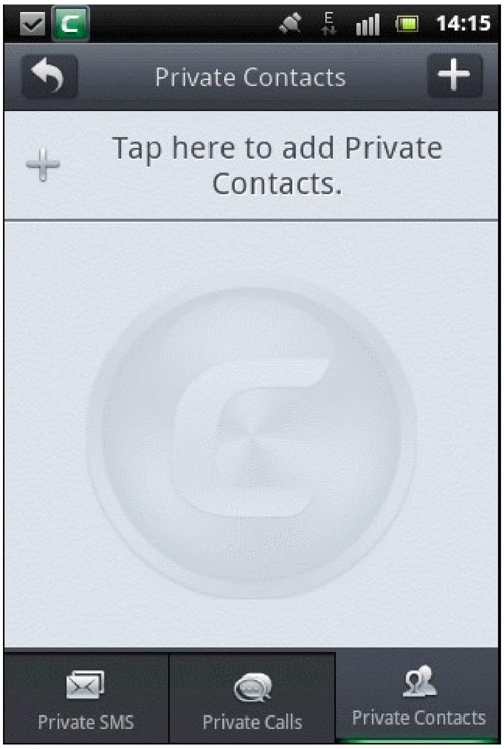
- Tap 'Private Communication'.

By default, the 'Private SMS' screen will be displayed.



No message(s) from Private Contacts available

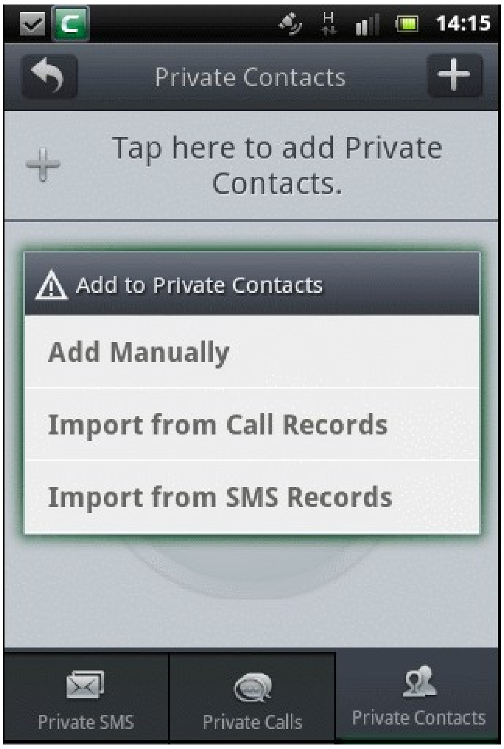
- Tap 'Private Contacts' located at the bottom of the screen.



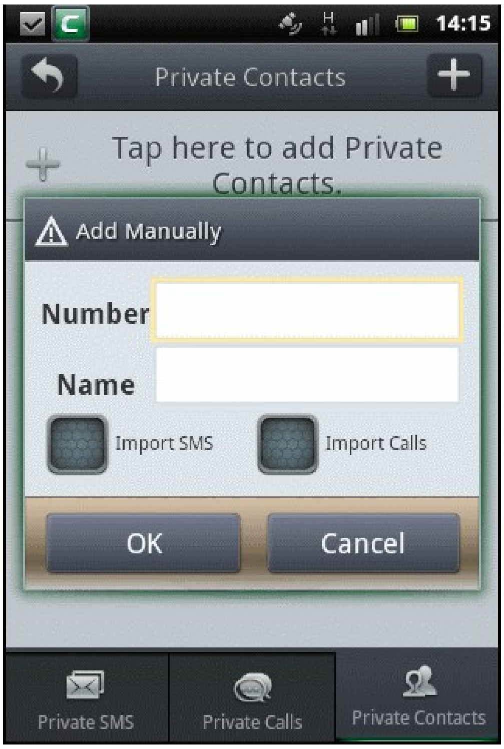
Tap here to add Private Contacts.

- Tap + to add contacts or on the row at the top.

The 'Add to Private Contacts' screen will be displayed. You have the following options:



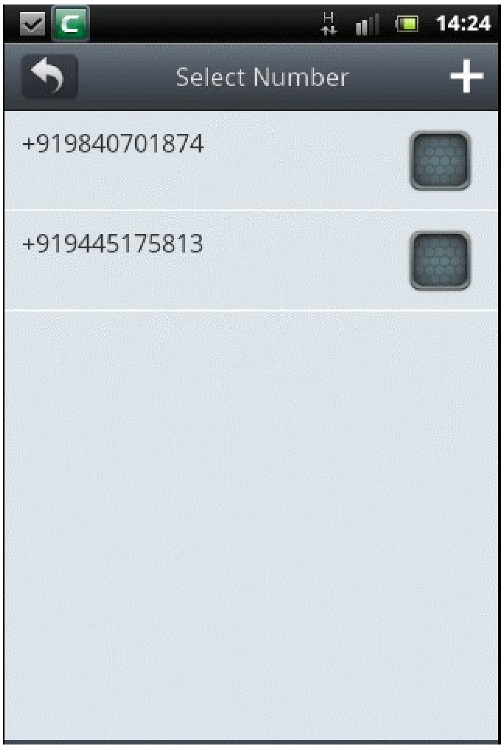
- **Add Manually** - Tap this bar to add your contacts manually.



  - Tap the 'Number' field and enter the phone number that you want to add.
  - Tap the 'Name' field and enter the name of the contact.
  - Select whether you want import only calls or only messages or both from the 'Import Calls and 'Import SMS' options and tap 'OK'.

- **Import from Call Records** - Tap this bar to add phone numbers that are in your call records.
- **Import from SMS Records** - Tap this bar to add phone numbers from SMS messages record in your device.

The phone numbers in your call or message records will be displayed.

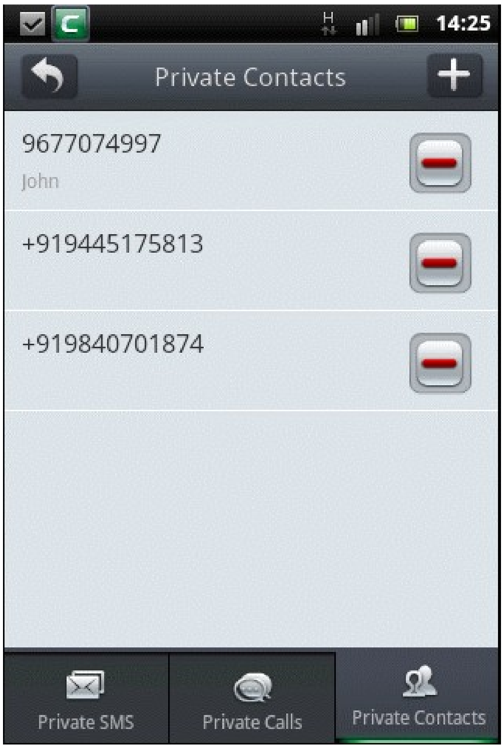


+919840701874

+919445175813

- Select the box beside the number(s) that you want to add to Private Contacts and tap + at the top right of the screen.

The list of added numbers will be displayed.



9677074997
John

+919445175813

+919840701874

If you want to delete a contact from the list, tap the − button beside a number and confirm it in the 'Confirm Deletion' screen.

Note: If you add contacts by 'Import from Call Records' or 'Import from SMS Record' method, only the number will be added and no previous records of the added contact will be imported into private space. Refer the topic '**How to import a private contact's records**' to know how to import a private contact's call and SMS records from your system records.

How to import a private contact's records

You can import the call and SMS records of a newly added private contact from the system records. Once a contact's call/SMS records are imported, then only you will be able to view these records in future.

To import a private contact's records

- Tap the CMS icon on your device.
- Tap 'Tool's tab located at the top or swipe to the left and tap 'Private Space'.

The 'Enter Your Password' screen will be displayed.

- Tap the 'Password' field and enter the password that you have set in this field.

The Private Space screen will be displayed.

- Tap 'Private Communication'.

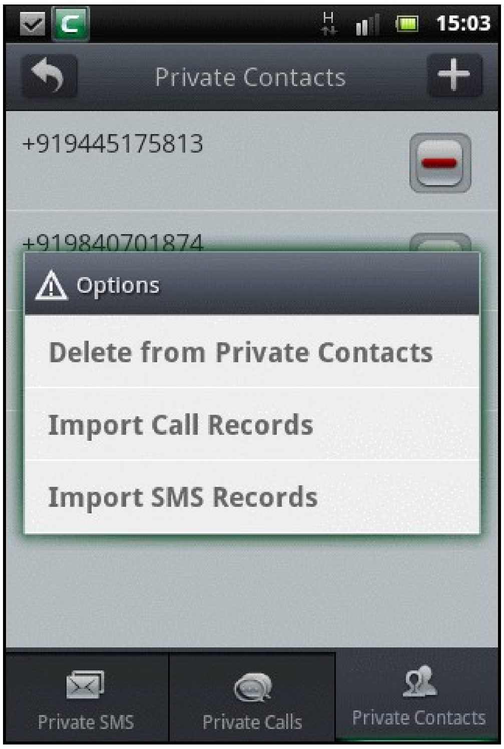
By default, the 'Private SMS' screen will be displayed.

- Tap 'Private Contacts' located at the bottom of the screen.

The list of added numbers to Private Contacts will be displayed. Refer '**How to add contacts into your private space**' for adding contacts to your Private Space if you have not done already.

- Tap and hold briefly on a contact that you want to import the records from the system.

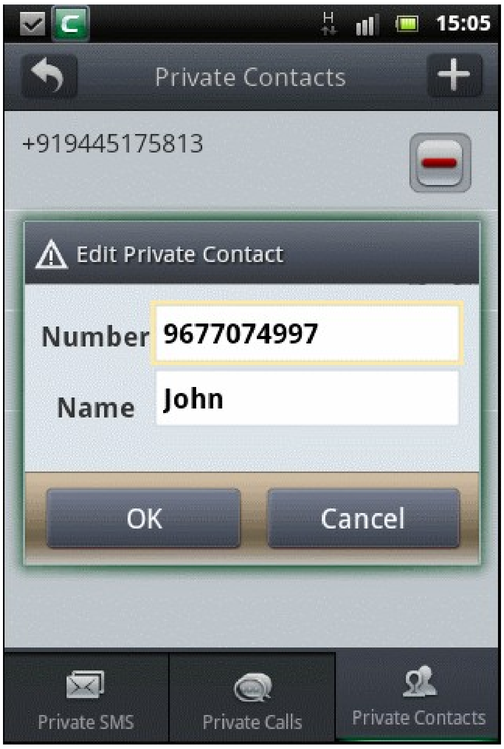
The Options screen will be displayed. You have the following options:



- **Delete from Private Contacts** - Tap this bar if you want to delete the selected contact from the 'Private Contact' list and confirm it in the 'Confirm Deletion' screen.
- **Import from Call Records** - Tap this bar to import call records of the selected contact from the system into 'Private Calls'.

- **Import from SMS Records** - Tap this bar to import SMS message records of the selected contact from the system into 'Private SMS'.

You can edit contact details by tapping on a 'Contact' bar once. The 'Edit Private Contact' screen will be displayed.



Number 9677074997

Name John

Edit the contact number and name in the 'Number' and 'Name' fields respectively and tap 'OK'.

How to manage a private SMS message

In the 'Private SMS' screen, you can view, delete or reply to a SMS message. You can also export the message to your system.

To manage a private SMS message

- Tap the CMS icon on your device.
- Tap 'Tool's tab located at the top or swipe to the left and tap 'Private Space'.

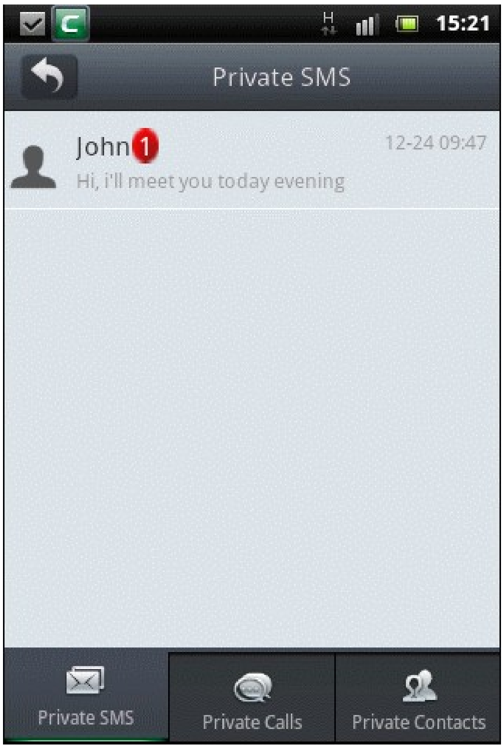
The 'Enter Your Password' screen will be displayed.

- Tap the 'Password' field and enter the password that you have set in this field.

The Private Space screen will be displayed.

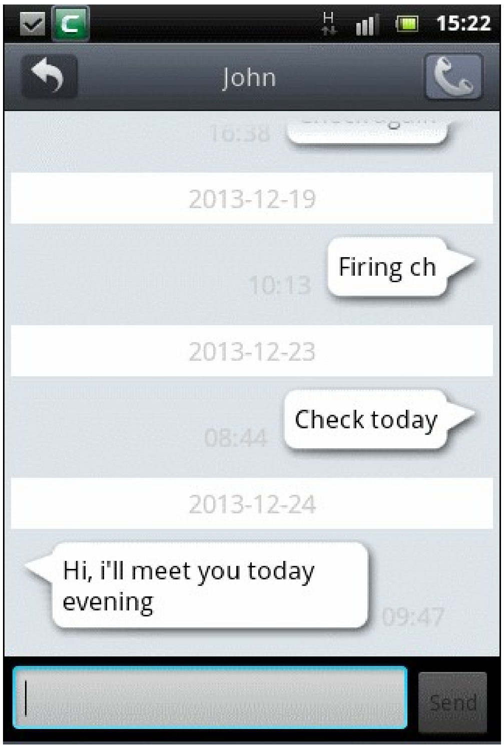
- Tap 'Private Communication'.

By default, the 'Private SMS' screen will be displayed.



In the list of private SMS messages, if a number is marked in red beside a contact it indicates the number of unread messages from that contact.

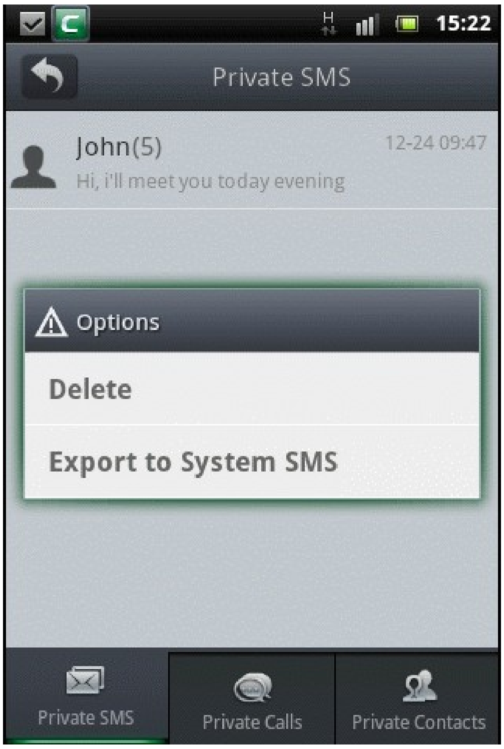
- Tap anywhere on a private SMS bar once.



You can view the message and can reply in this screen by entering the reply message in the message field and tapping 'Send'.

- Tap and hold briefly on a private SMS message.

The 'Options' screen will be displayed.



- **Delete** - Tap this bar to delete the message from the device.
- **Export to System SMS** - Tap this bar to export the message to your system SMS records. The message will no longer be in 'Private SMS'.

How to manage a private call

In the 'Private Calls' screen, you can view, delete or export the call records to your system.

To manage a private call

- Tap the CMS icon on your device.
- Tap 'Tool's tab located at the top or swipe to the left and tap 'Private Space'.

The 'Enter Your Password' screen will be displayed.

- Tap the 'Password' field and enter the password that you have set in this field.

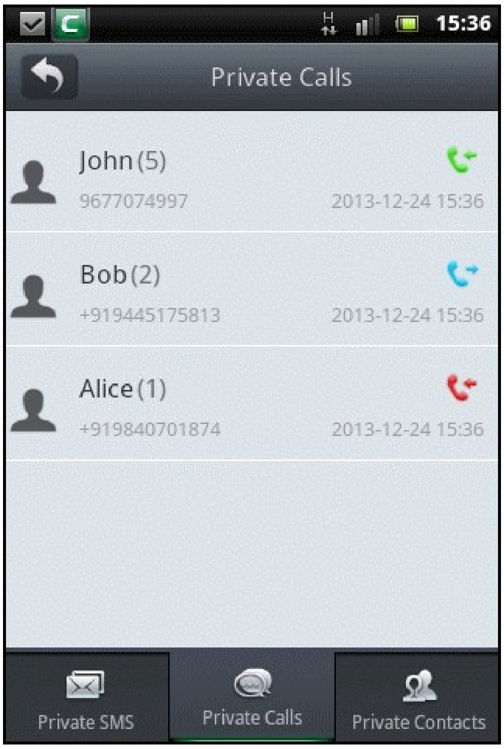
The Private Space screen will be displayed.

- Tap 'Private Communication'.

By default, the 'Private SMS' screen will be displayed.

- Tap 'Private Calls' located at the bottom of the screen.

The list of Private Calls will be displayed.



John (5)
9677074997 2013-12-24 15:36

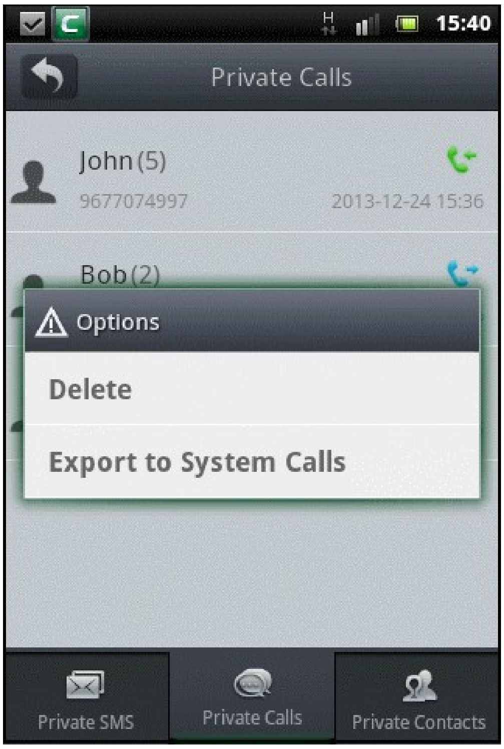
Bob (2)
+919445175813 2013-12-24 15:36

Alice (1)
+919840701874 2013-12-24 15:36

You can view the call details of the contact such as date and time, duration of the call, whether it is incoming, outgoing or a missed call. Green, blue or red color phone icon beside a call detail indicates incoming, outgoing and missed call respectively.

- Tap anywhere on the private call bar to view the call records of the contact.
- Tap anywhere once again on the private call bar to close the details view.
- Tap and hold briefly on a private call.

The 'Options' screen will be displayed.



- **Delete** - Tap this bar to delete the call detail from the device.
- **Export to System SMS** - Tap this bar to export the call records to your system call records. The call records will no

longer be in 'Private Calls'.

How to password-protect your apps in your device

The password protection feature prevents applications in your device from being launched without proper credentials.

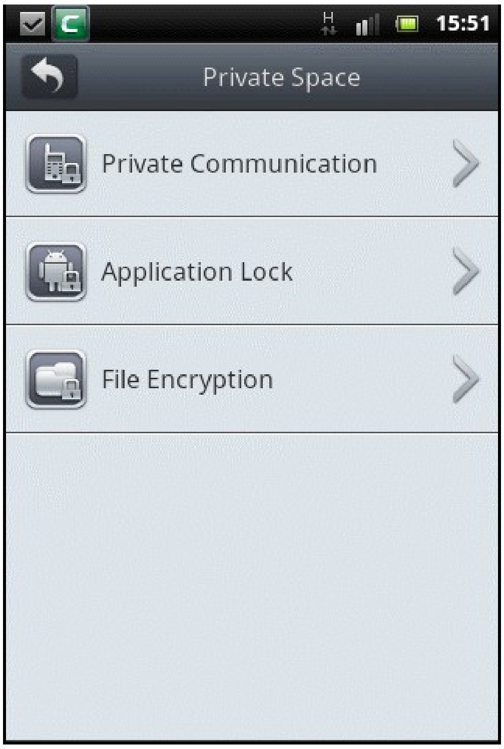
To password-protect your applications

- Tap the CMS icon on your device.
- Tap 'Tool's tab located at the top or swipe to the left and tap 'Private Space'.

The 'Enter Your Password' screen will be displayed.

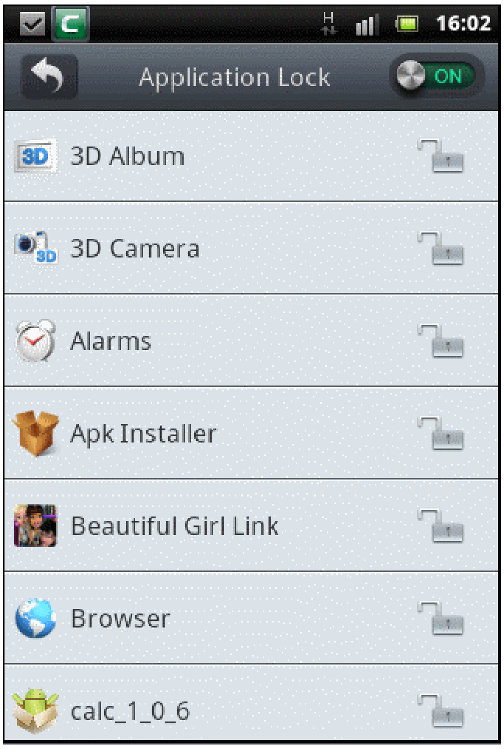
- Tap the 'Password' field and enter the password that you have set in this field.

The Private Space screen will be displayed.



- Tap 'Application Lock'.

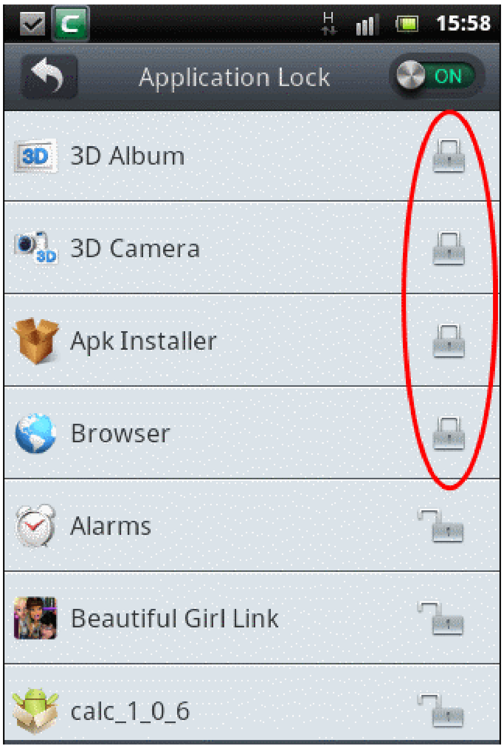
All the apps in the device will be listed in alphabetical order with open-lock icon at the far end indicating its unlocked status.



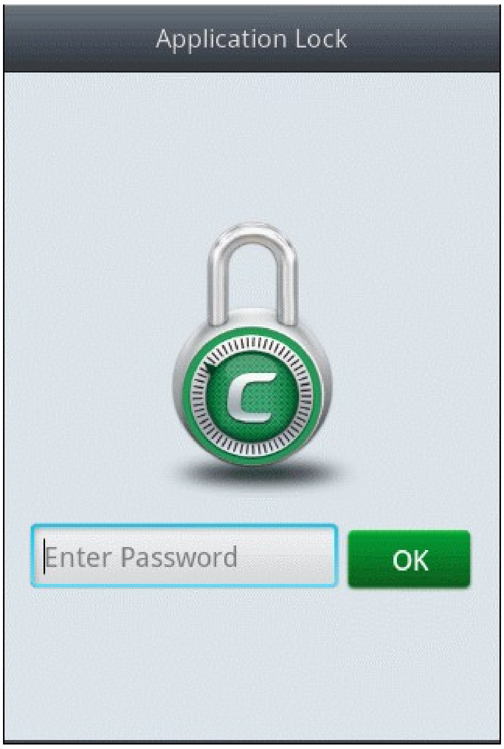
Note: Make sure the toggle button at the top right of the screen is in 'On' status.

- Tap anywhere on the bar of the app(s) that you want to lock.

All the locked apps will be displayed at the top of the list with the closed-lock icon at the far end indicating its locked status.



The locked apps can be accessed only after entering the **password** that you set for Private Space. If you try to access any of the locked apps, the following 'Application Lock' screen will be displayed.



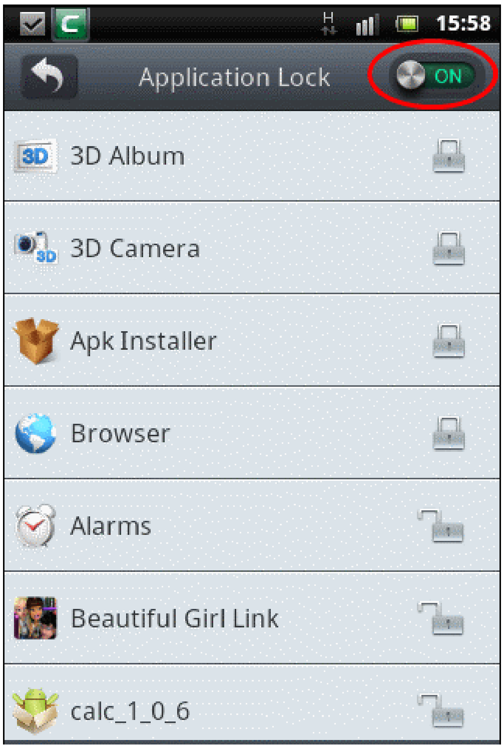
- Enter the **password** that you set for 'Private Space' and tap 'OK'.

If you have forgotten your password, 'Refer '**How to reset a forgotten password**' to set a new password.

- To unlock an app, tap anywhere on the bar.

The app will no longer be password-protected.

You can also enable or disable the application lock service by tapping the ON/OFF toggle button located at the top right.



The locked applications in the list will be password-protected only if the toggle button is in 'ON' status. To unlock all the locked apps, tap on it to display 'OFF' status.

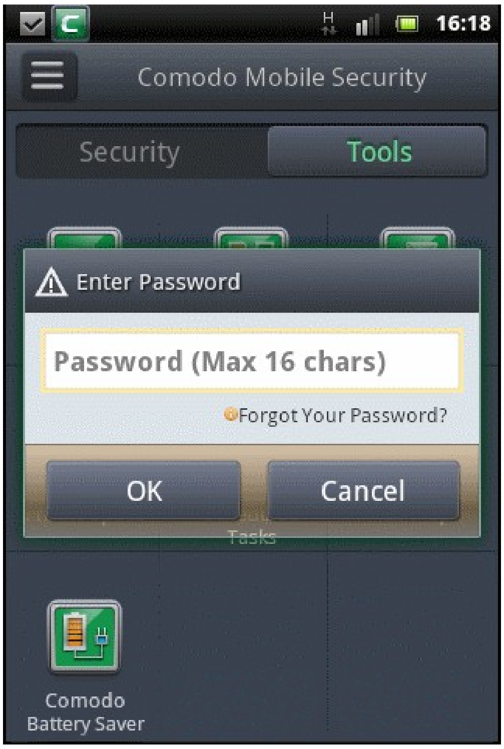
How to reset a forgotten password

In case you have forgotten your password, you can reset the password.

To reset a forgotten password

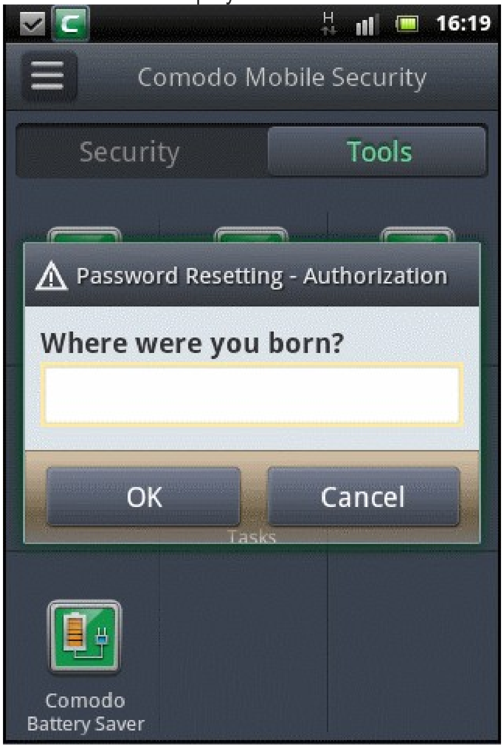
- Tap the CMS icon on your device.
- Tap 'Tool's tab located at the top or swipe to the left and tap 'Private Space'.

The 'Enter Your Password' screen will be displayed.



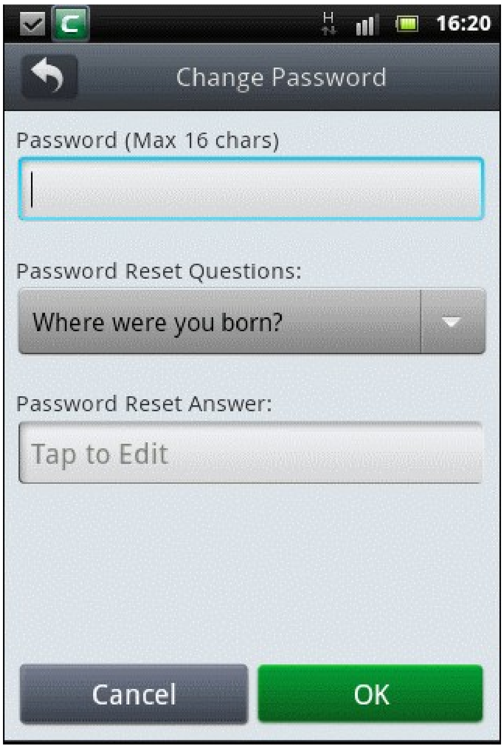
- Tap 'Forgotten Password?'

The 'Password Resetting - Authorization' screen will be displayed.



- Enter your Password Reset answer and click 'OK'.

The 'Change Password' screen will be displayed.



- Tap the 'Password' field and enter your new password.
- Tap 'Password Reset Questions' if you want to reset the password reset Q&A, select the question and enter the answer in the 'Password Reset Answer' field.
- Tap 'OK'.

That's it. Your new password for using the private space is set and enter it each time you want to access this feature.

How to change your password

You can change the current 'Private Space' password if you feel it is compromised or for any other reason.

To change your password

- Tap the CMS icon on your device.
- Tap 'Tool's tab located at the top or swipe to the left and tap 'Private Space'.

The 'Enter Your Password' screen will be displayed.

- Tap the 'Password' field and enter the password that you have set in this field.

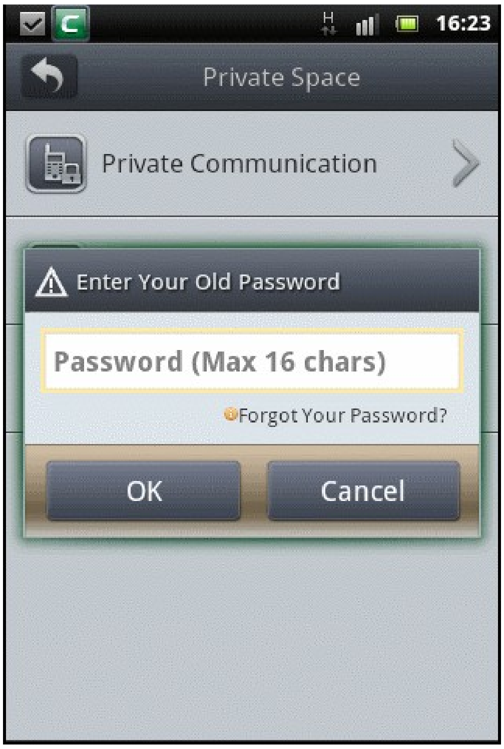
The Private Space screen will be displayed.

- Tap the menu key in your device.

The 'Modify Password' screen will be displayed.

- Tap 'Modify Password'.

The 'Enter Your Old Password' screen will be displayed.


16:23

Private Space

Private Communication

Enter Your Old Password

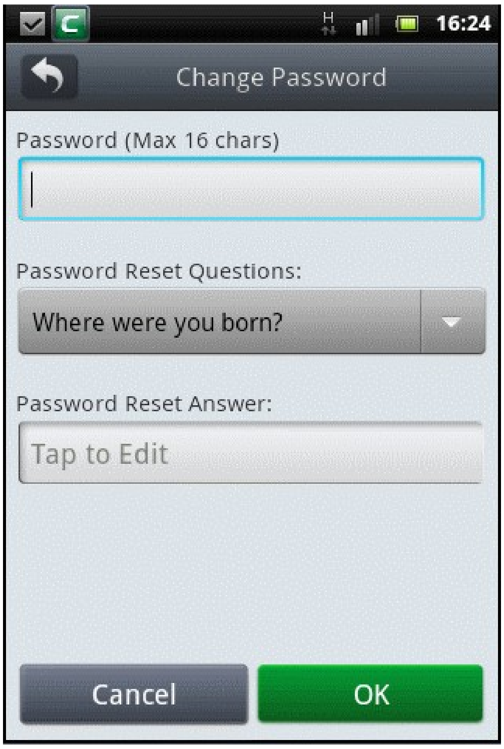
Password (Max 16 chars)

Forgot Your Password?

OK Cancel

- Tap the 'Password' field and enter the old password.

The 'Change Password' screen will be displayed.


16:24

Change Password

Password (Max 16 chars)

Password Reset Questions:

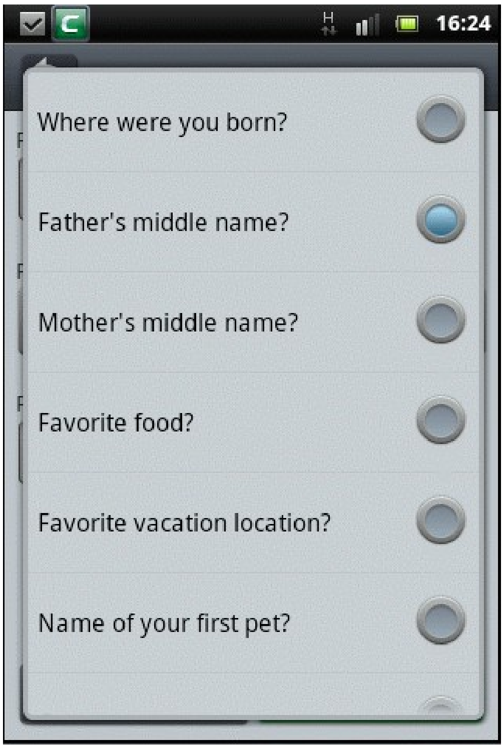
Where were you born?

Password Reset Answer:

Tap to Edit

Cancel OK

- Tap the 'Password' field and enter your new password.
- Tap 'Password Reset Questions' if you want to reset the password reset Q&A and select the question.



○ Where were you born?

● Father's middle name?

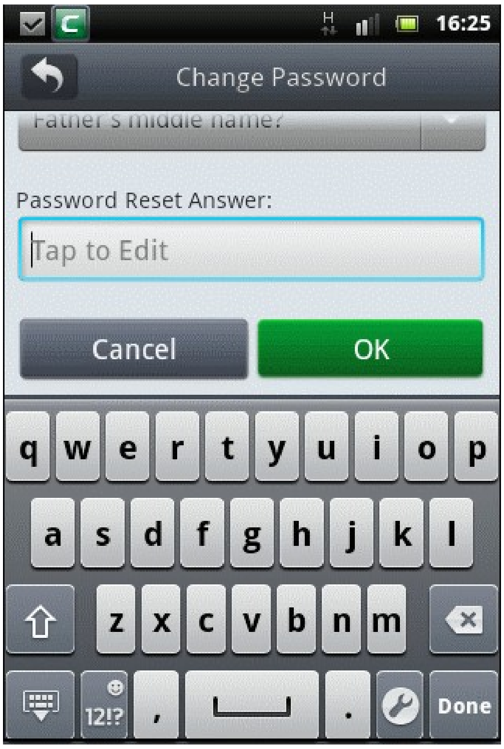
○ Mother's middle name?

○ Favorite food?

○ Favorite vacation location?

○ Name of your first pet?

- Enter the answer in the 'Password Reset Answer' field.



Father's middle name?

Password Reset Answer:

Tap to Edit

Cancel | OK

- Tap 'OK'.

That's it. Your new password for using the private space is set and enter it each time you want to access this feature.

How to encrypt your files / folders / images

The encryption feature in CMS encrypts images, files and folders thus safeguarding important contents even if your is device is hacked and files stolen. The encrypted items will not be available in the original path and will be stored as encrypted files in the Comodo folder. Decrypted items will be restored to its original location.

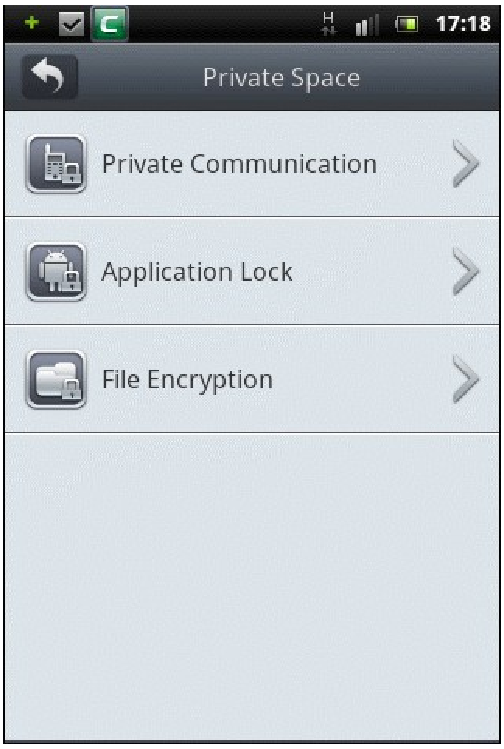
To encrypt files / folders

- Tap the CMS icon on your device.
- Tap 'Tool's tab located at the top or swipe to the left and tap 'Private Space'.

The 'Enter Password' screen will be displayed.

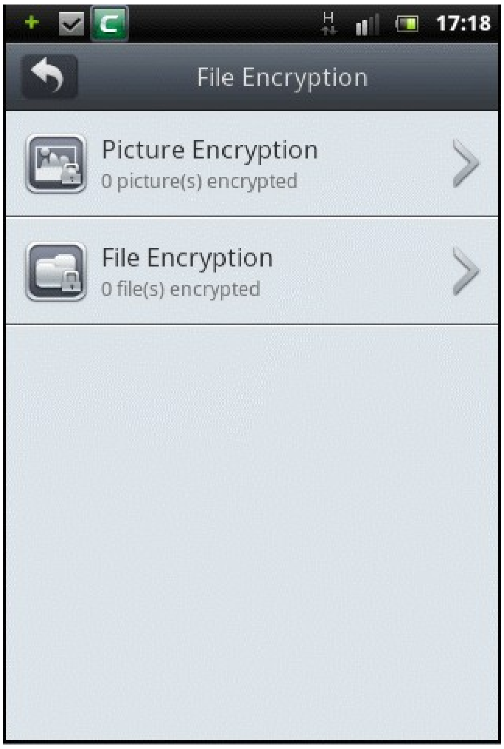
- Tap the 'Password' field and enter the password that you have set in this field.

The Private Space screen will be displayed.

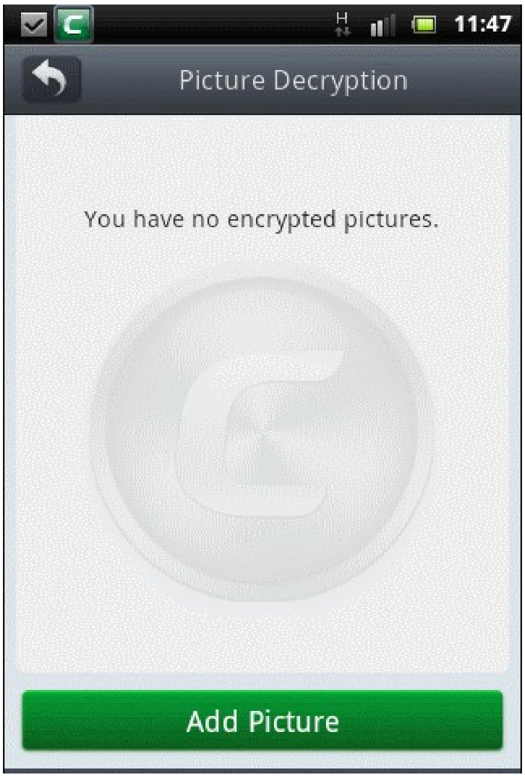


- Tap 'File Encryption'.

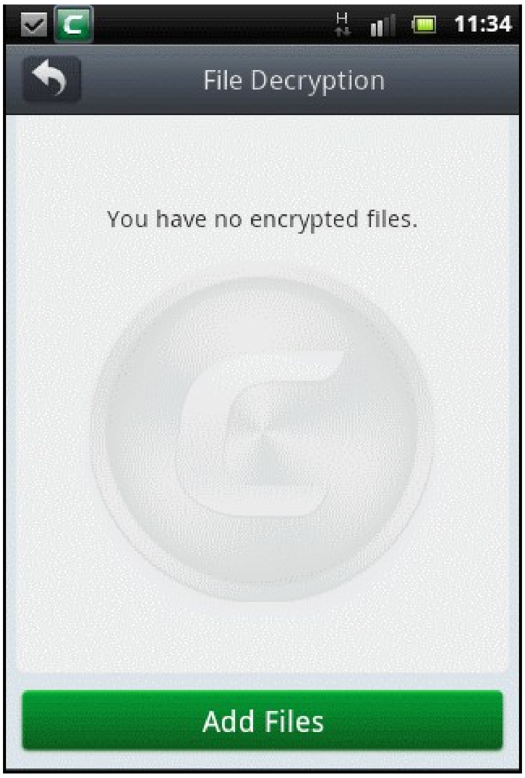
The 'File Encryption' screen will be displayed.



- Tap 'Picture Encryption' to encrypt only images or 'File Encryption' to encrypt all other files/folders.

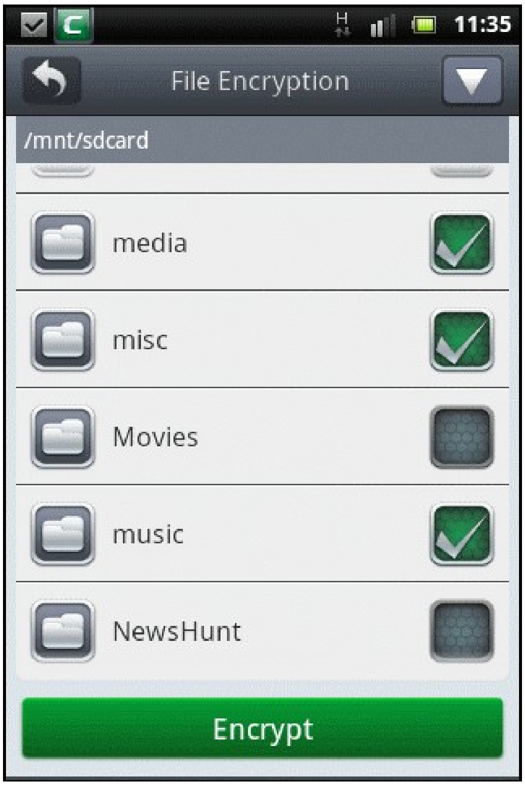


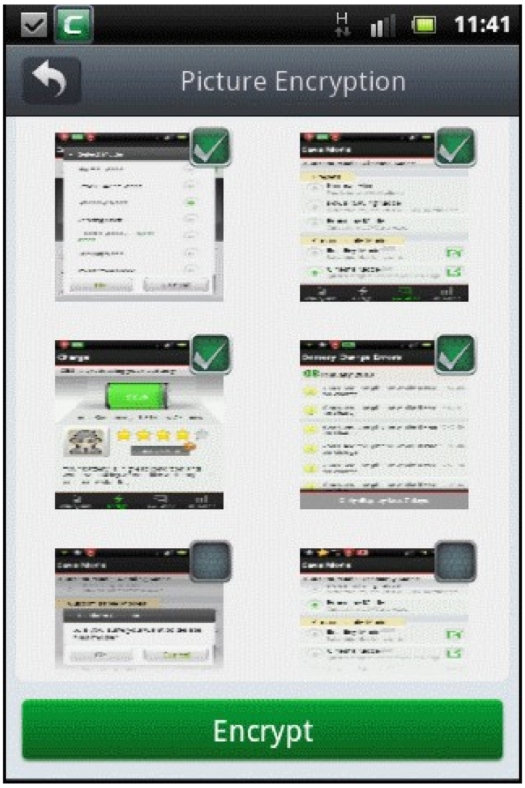
You have no encrypted pictures.



You have no encrypted files.

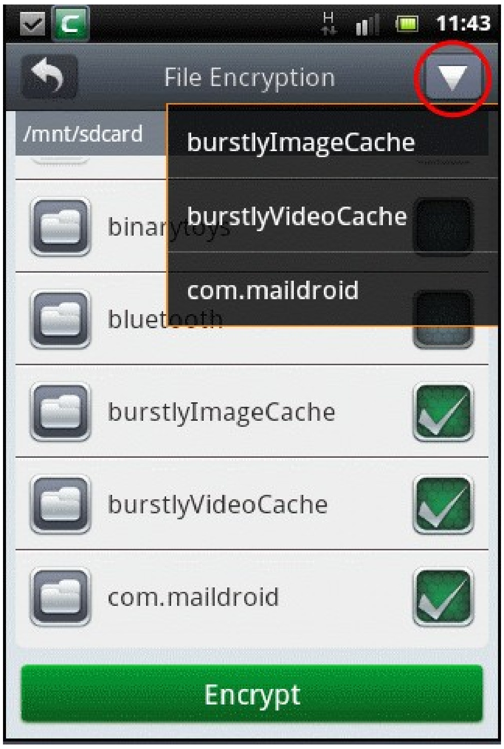
- Tap 'Add Picture' / Add Files' button.





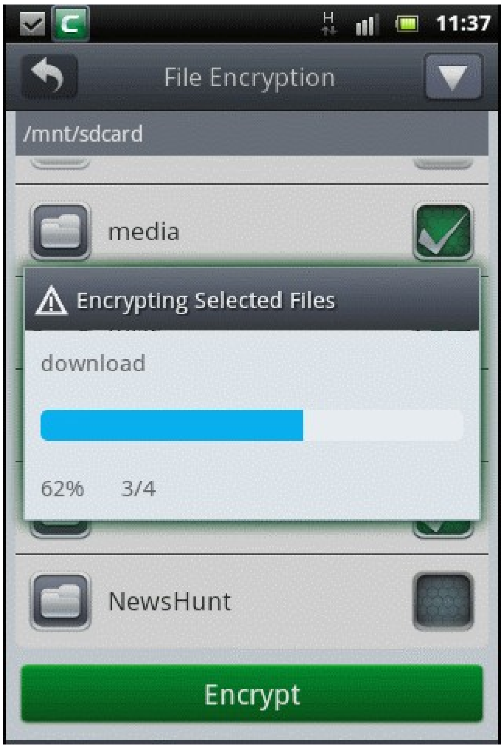
- Select the Files/Folders/Pictures that you want to encrypt.

- To deselect the selected items, tap on the respective selection box(es) or the inverted triangle at the top (for files only) and tap on the respective files from the drop-down.

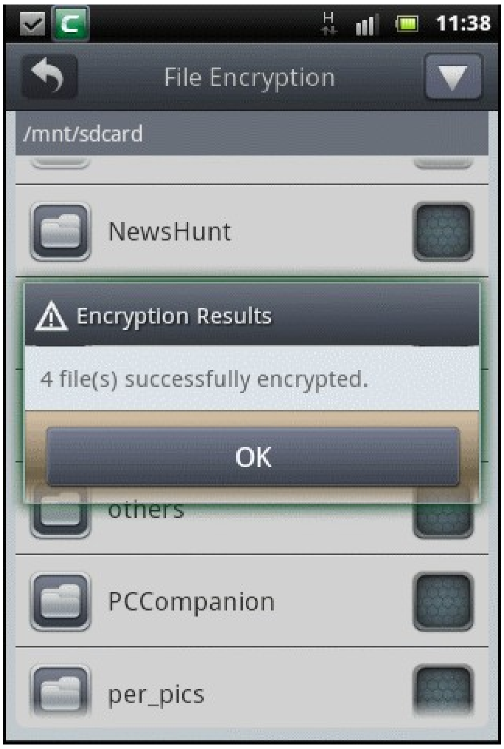


- Tap the 'Encrypt' button.

The encryption progress will be displayed...



...and on completion the result will be displayed.



Encryption Results

4 file(s) successfully encrypted.

OK

- Click 'OK' to return to the Encryption screen.

How to decrypt your files / folders / images

The CMS-encrypted items in your device can be decrypted and these items will be restored to the original location.

To decrypt files / folders / images

- Tap the CMS icon on your device.
- Tap 'Tool's tab located at the top or swipe to the left and tap 'Private Space'.

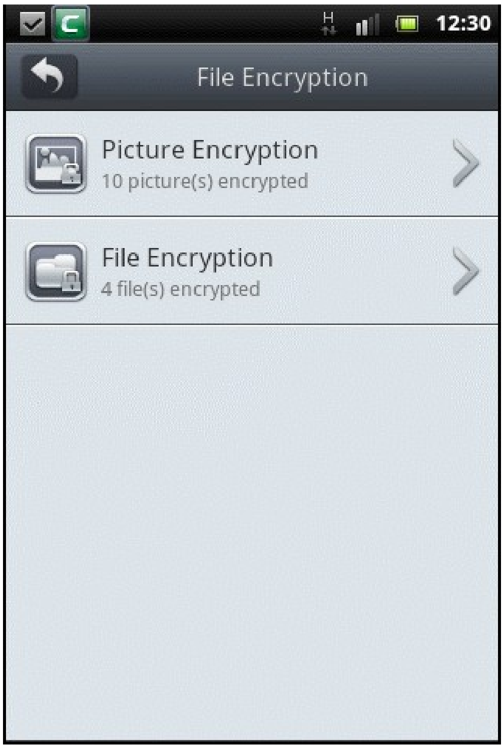
The 'Enter Password' screen will be displayed.

- Tap the 'Password' field and enter the password that you have set in this field.

The Private Space screen will be displayed.

- Tap 'File Encryption'.

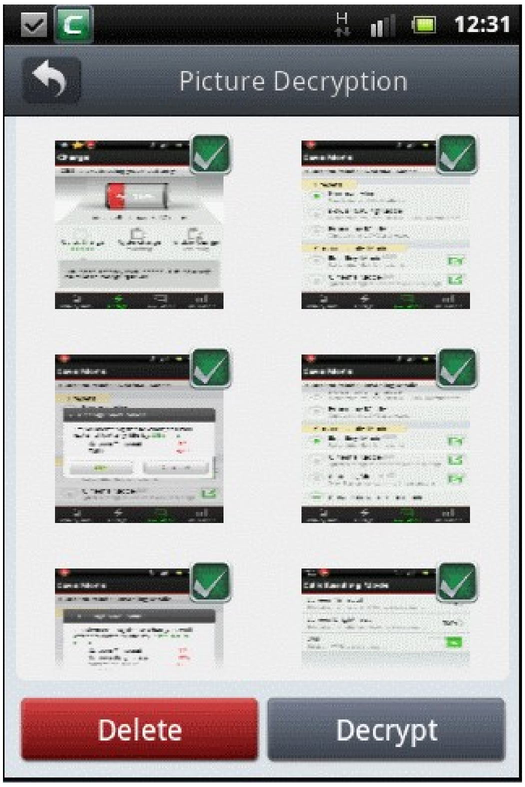
The 'File Encryption' screen will be displayed with the number of items that are encrypted for each category.

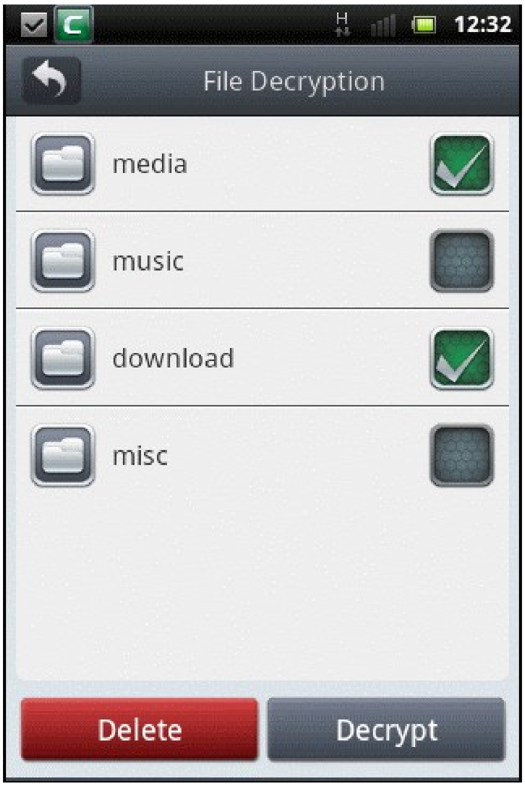


- Tap anywhere on the row of the item that you want to decrypt.

The encrypted images/files/folders will be displayed.

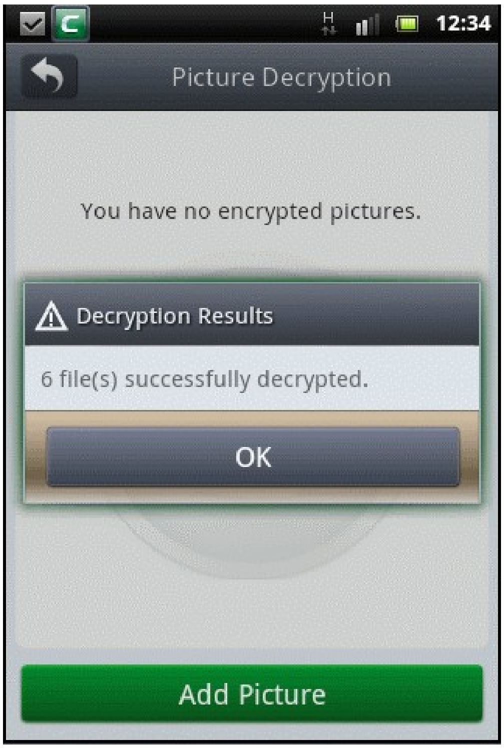
- To select encrypted files / folders, tap on the box beside the items.
- To select encrypted images, long-press on any of the item in the screen. The selection boxes will be displayed at the top right of each decrypted image. Tap on the images that you want to decrypt.





- Tap the 'Decrypt' button.

The selected item(s) will be decrypted and restored to its original location.



12:34

Picture Decryption

You have no encrypted pictures.

Decryption Results

6 file(s) successfully decrypted.

- Click 'OK' to return to the Encryption screen.
- Tap the 'Delete' button to removed the encrypted items.

Note: If you delete the encrypted items, they will no longer be available in the SD card.

8.Software Manager

The 'Software Manager' feature in CMS allows you to easily manage all the apps in your device. You can view the installed apps, take a backup or uninstall them. Restore uninstalled apps back to your device with a single tap. Software Manager provides a full list of apk files in your device SD card and you can choose either to install them or delete them.

Click the links below for help with common tasks:

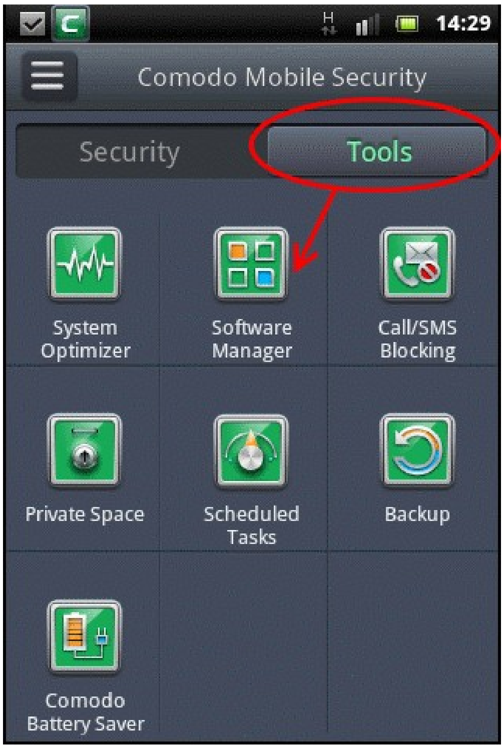
- **How to view the installed apps and take a backup or uninstall them**
- **How to restore or delete uninstalled apps**
- **How to view and manage all the apk files in your device**

How to view the installed apps and take a backup or uninstall them

You can view all the applications installed in your Android device and choose to take backup or uninstall any of the unwanted apps.

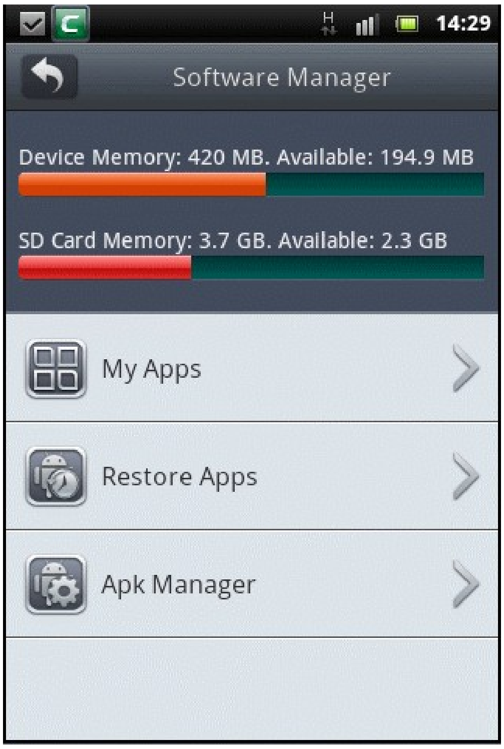
To view and take backup or uninstall applications

- Tap the CMS icon on your device.



- Tap 'Tool's tab located at the top or swipe to the left and tap 'Software Manager'.

The 'Software Manager' screen will be displayed. In the upper portion of the screen, the details of memory available in your Android device and in the SD card is displayed.

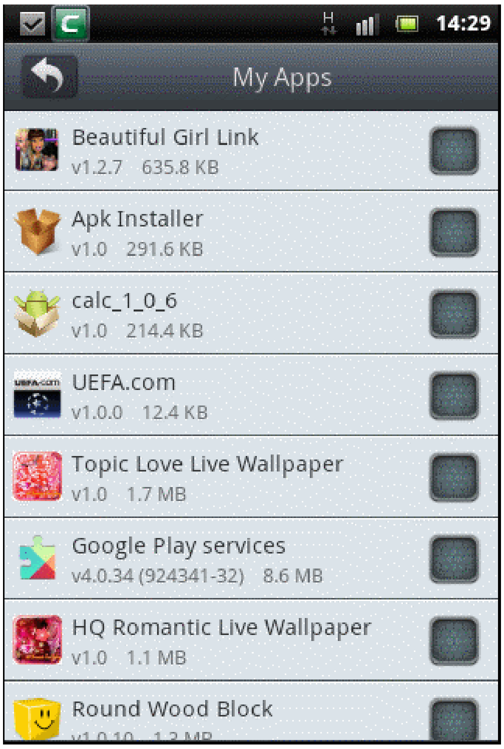


Device Memory: 420 MB. Available: 194.9 MB

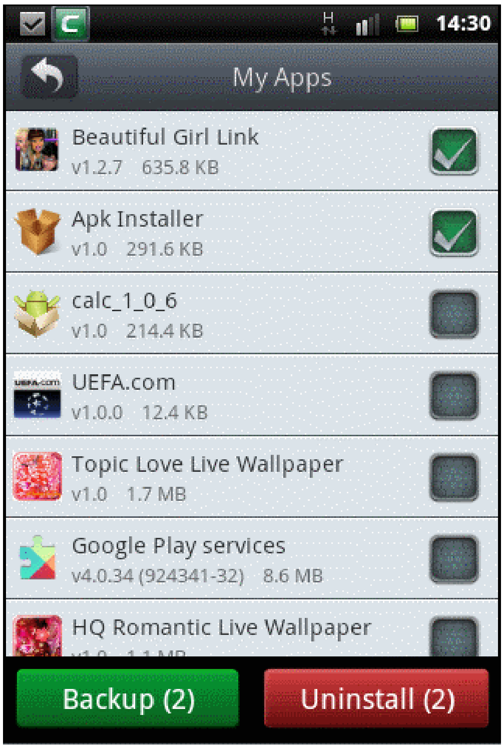
SD Card Memory: 3.7 GB. Available: 2.3 GB

- Tap anywhere on the 'My Apps' bar.

All the installed apps will be displayed in the 'My Apps' screen with details such as its version number and storage space it occupies.

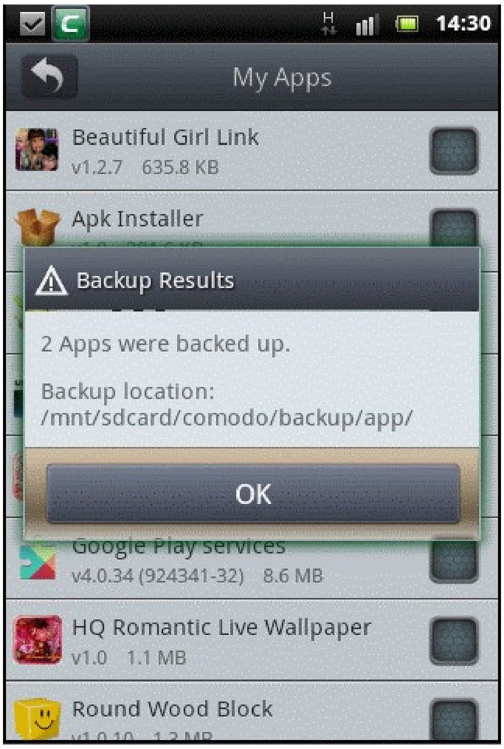


- Scroll up or down to view all the applications.
- Tap on the box beside the app(s) that you want to either backup or uninstall.



- Tap the 'Backup' button if you want to backup the selected apps.

The Backup Results dialog will be displayed with details of the backup location. The backed up apps will be available in '**Restore Apps**'.



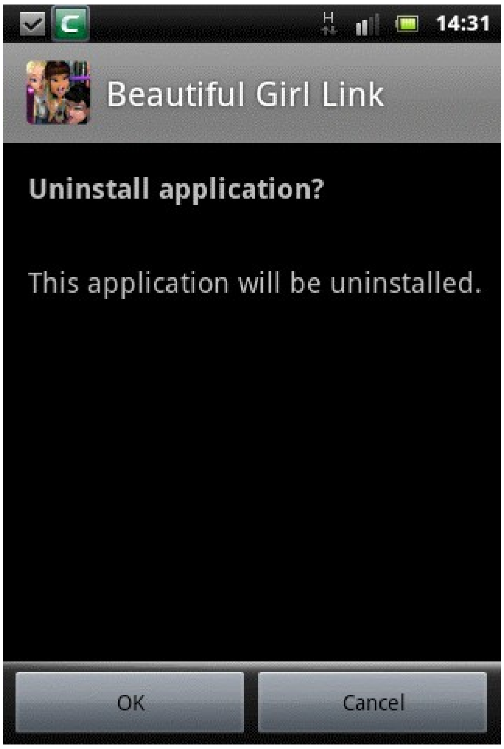
Backup Results

2 Apps were backed up.

Backup location:
/mnt/sdcard/comodo/backup/app/

OK

- Tap 'OK' to return to the 'My Apps' screen.
- Tap the 'Uninstall' button if you want to uninstall the selected app(s).



Beautiful Girl Link

Uninstall application?

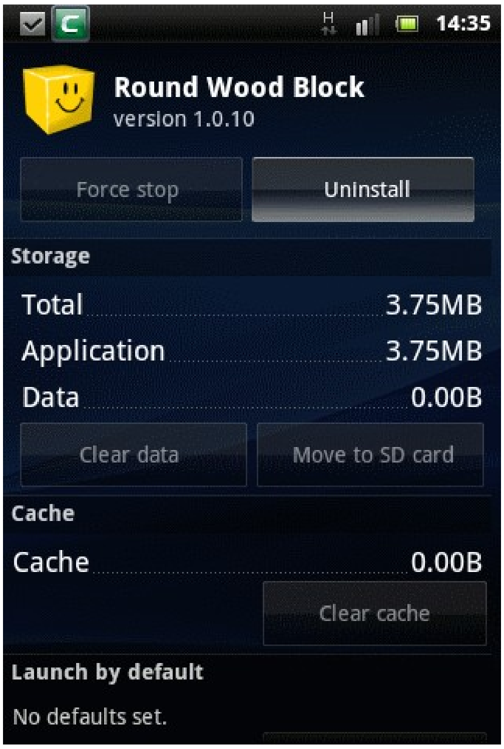
This application will be uninstalled.

OK Cancel

- Tap 'OK' to confirm the action or tap 'Cancel'.

You can re-install the uninstalled apps from the 'Restore Apps' screen or from the 'Apk Manager' screen if the apk files are available in your SD card. Refer to '**How to restore or delete uninstalled apps**' and '**How to view and manage all the apk files in your device**' for more details.

Tapping anywhere on an app bar, you can force stop, uninstall, move to SD card, clear data or clear cache. An example of the 'Manage Applications' screen is shown below:



Round Wood Block
version 1.0.10

Storage

Total 3.75MB
Application 3.75MB
Data 0.00B

Cache

Cache 0.00B

Launch by default

No defaults set.

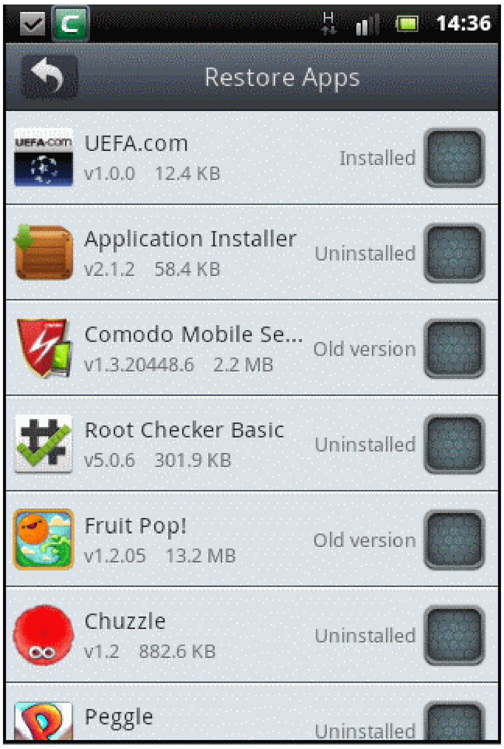
How to restore or delete uninstalled apps

All the uninstalled and backed up apps can be accessed in the 'Restore Apps' screen. You can choose to either install them again or delete them altogether from the device.

To restore or delete uninstalled apps

- Tap the CMS icon on your device.
- Tap 'Tool's tab located at the top or swipe to the left and tap 'Software Manager'.
- In the 'Software Manager' screen, tap 'Restore Apps'.

All the uninstalled apps will be displayed. If the status of an app is shown as installed, it means that it has been restored again after uninstallation. The uninstalled apps will be continue to remain in this screen even after they have been restored until it is deleted.



14:36

Restore Apps

UEFA.com
v1.0.0 12.4 KB
Installed

Application Installer
v2.1.2 58.4 KB
Uninstalled

Comodo Mobile Se...
v1.3.20448.6 2.2 MB
Old version

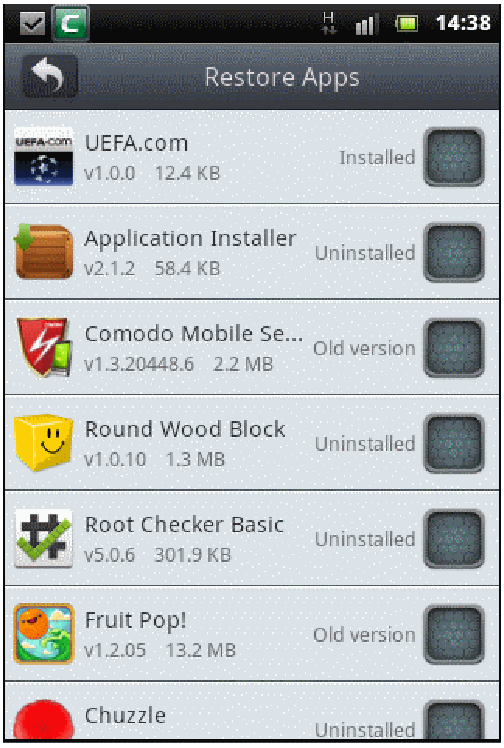
Root Checker Basic
v5.0.6 301.9 KB
Uninstalled

Fruit Pop!
v1.2.05 13.2 MB
Old version

Chuzzle
v1.2 882.6 KB
Uninstalled

Peggle
Uninstalled

- Tap on the box beside the uninstalled app(s) that you want to restore or delete.



14:38

Restore Apps

UEFA.com
v1.0.0 12.4 KB
Installed

Application Installer
v2.1.2 58.4 KB
Uninstalled

Comodo Mobile Se...
v1.3.20448.6 2.2 MB
Old version

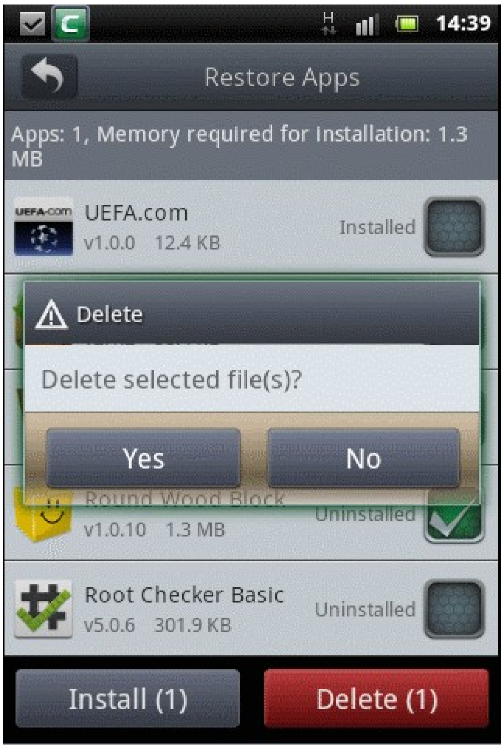
Round Wood Block
v1.0.10 1.3 MB
Uninstalled

Root Checker Basic
v5.0.6 301.9 KB
Uninstalled

Fruit Pop!
v1.2.05 13.2 MB
Old version

Chuzzle
Uninstalled

- Tap the 'Install' button if you want to restore the application to your device. The selected app(s) will be installed.
- Tap the 'Delete' button if you want to remove the app from your device and confirm it in the 'Delete' dialog screen.



The selected app(s) will be deleted from your device.

Note: You can also re-install the uninstalled apps from the 'Apk Manager' screen if the apk files are available in the SD of your device. Refer to '**How to view and manage all the apk files in your device**' for more details.

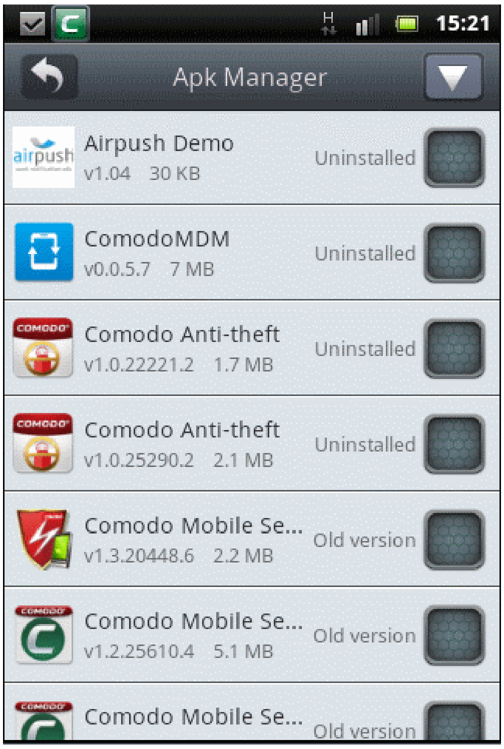
How to view and manage all the apk files in your device

The applications in your device are installed by using the apk files. The extension of an application installation file is .apk. Using the Apk Manager feature in CMS you can view all the apk files stored in your SD card. You can use the filter option to view all apk files, installed apk files, uninstalled apk files or only older versions.

To view and manage apk files

- Tap the CMS icon on your device.
- Tap 'Tool's tab located at the top or swipe to the left and tap 'Software Manager'.
- In the 'Software Manager' screen, tap 'Apk Manager'.

The 'Apk Manager' screen will be displayed.



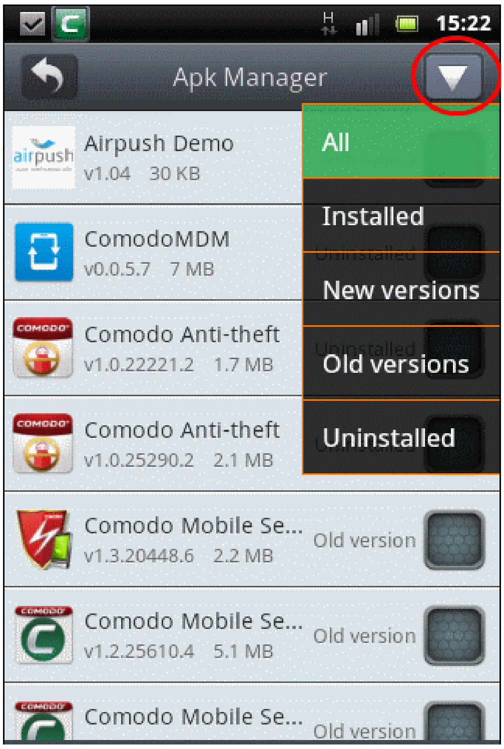
15:21

Apk Manager

Airpush Demo v1.04 30 KB	Uninstalled	
ComodoMDM v0.0.5.7 7 MB	Uninstalled	
Comodo Anti-theft v1.0.22221.2 1.7 MB	Uninstalled	
Comodo Anti-theft v1.0.25290.2 2.1 MB	Uninstalled	
Comodo Mobile Se... v1.3.20448.6 2.2 MB	Old version	
Comodo Mobile Se... v1.2.25610.4 5.1 MB	Old version	
Comodo Mobile Se...	Old version	

The screen displays all the versions including which are installed and uninstalled. You can use the filter option to view and manage any one of the type of apk files.

To use the filter option, tap the drop-down button located at the top right.



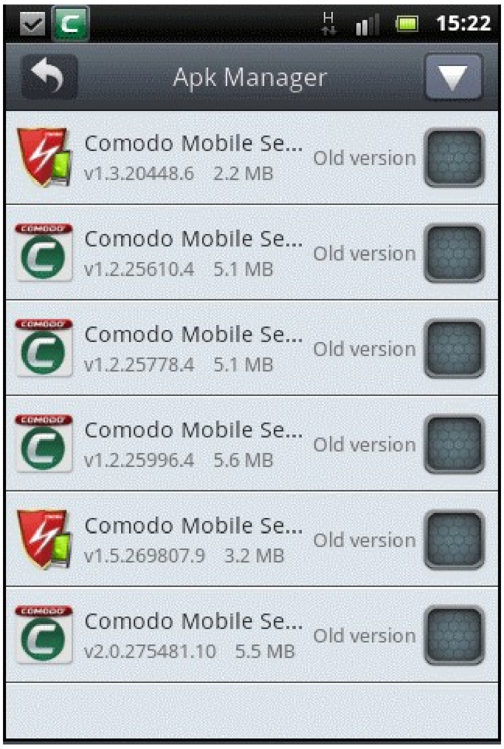
15:22

Apk Manager

- All
- Installed
- New versions
- Old versions
- Uninstalled

Airpush Demo v1.04 30 KB	
ComodoMDM v0.0.5.7 7 MB	
Comodo Anti-theft v1.0.22221.2 1.7 MB	
Comodo Anti-theft v1.0.25290.2 2.1 MB	
Comodo Mobile Se... v1.3.20448.6 2.2 MB	Old version
Comodo Mobile Se... v1.2.25610.4 5.1 MB	Old version
Comodo Mobile Se...	Old version

Tap on the option that you wish to filter the apk files. For example if you tap on 'Old versions', all the old versions of the apk files will be displayed.

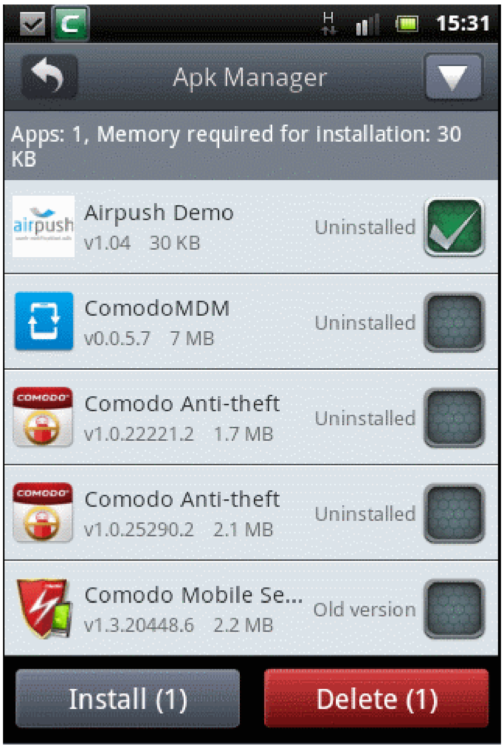


15:22

Apk Manager

Comodo Mobile Se... v1.3.20448.6 2.2 MB	Old version	□
Comodo Mobile Se... v1.2.25610.4 5.1 MB	Old version	□
Comodo Mobile Se... v1.2.25778.4 5.1 MB	Old version	□
Comodo Mobile Se... v1.2.25996.4 5.6 MB	Old version	□
Comodo Mobile Se... v1.5.269807.9 3.2 MB	Old version	□
Comodo Mobile Se... v2.0.275481.10 5.5 MB	Old version	□

To install an app, tap anywhere on the respective apk file.



15:31

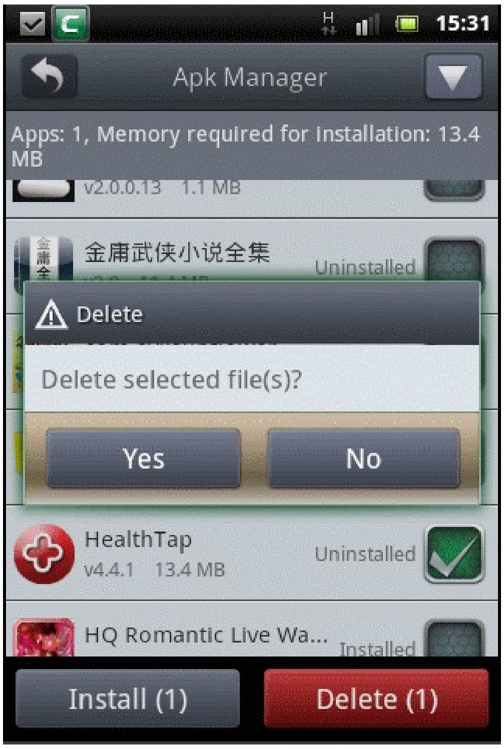
Apk Manager

Apps: 1, Memory required for installation: 30 KB

Airpush Demo v1.04 30 KB	Uninstalled	☑
ComodoMDM v0.0.5.7 7 MB	Uninstalled	□
Comodo Anti-theft v1.0.22221.2 1.7 MB	Uninstalled	□
Comodo Anti-theft v1.0.25290.2 2.1 MB	Uninstalled	□
Comodo Mobile Se... v1.3.20448.6 2.2 MB	Old version	□

The details of such as how many apk file(s) are selected and how much memory is required for its installation are displayed at the top.

- Tap the 'Install' button to proceed with the installation.
- To remove apk files from your device, select them and tap the 'Delete' button.



Apps: 1, Memory required for installation: 13.4 MB

Delete

Delete selected file(s)?

- Tap 'Yes' to confirm the deletion.

9.Call & SMS Blocking

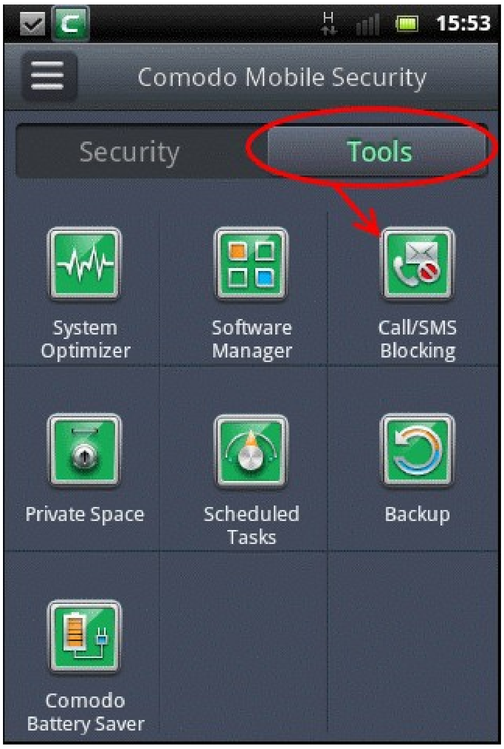
The Call & SMS blocking feature in CMS allows you to block unwanted messages or calls. Calls from unknown can be also added to the blocked list. You can view blocked messages (and unblock callers if desired) from the view screen. You can also add known contacts to your personal whitelist and blacklist.

Click the links below for help with common tasks:

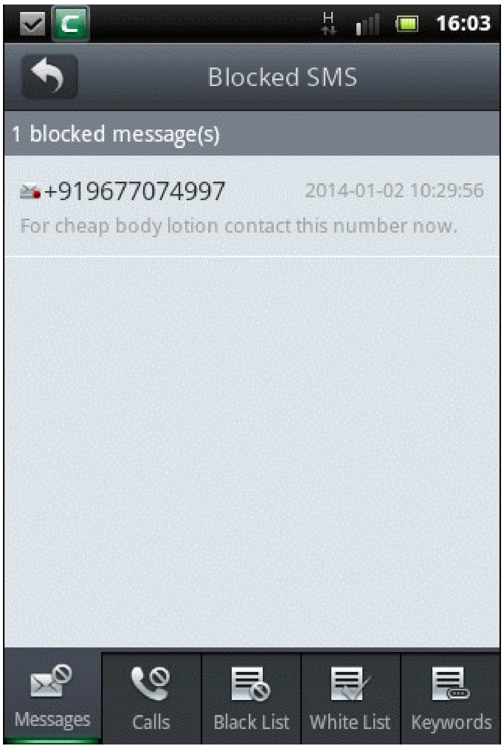
- **How to block messages**
- **How to view blocked messages**
- **How to add phone numbers to whitelist**
- **How to add phone numbers to blacklist**
- **How to view blocked call list**

How to block messages

- Tap the CMS icon on your device.
- Tap 'Tool's tab located at the top or swipe to the left and tap 'Call/SMS Blocking'.



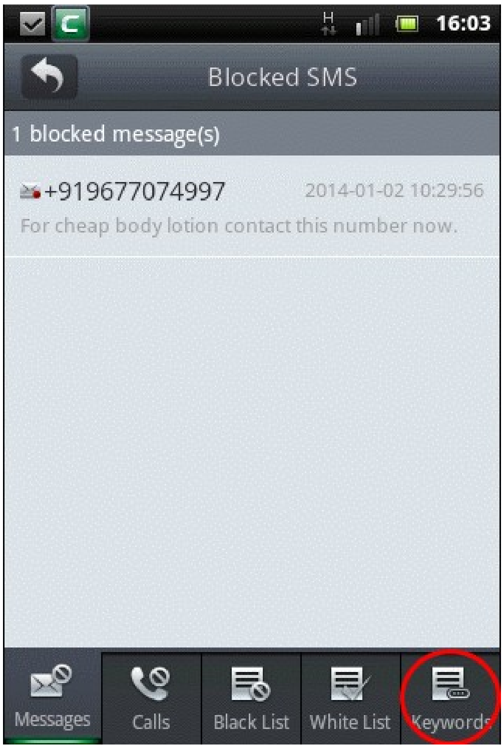
By default, the blocked SMS messages list will be displayed.



1 blocked message(s)

+919677074997 2014-01-02 10:29:56
For cheap body lotion contact this number now.

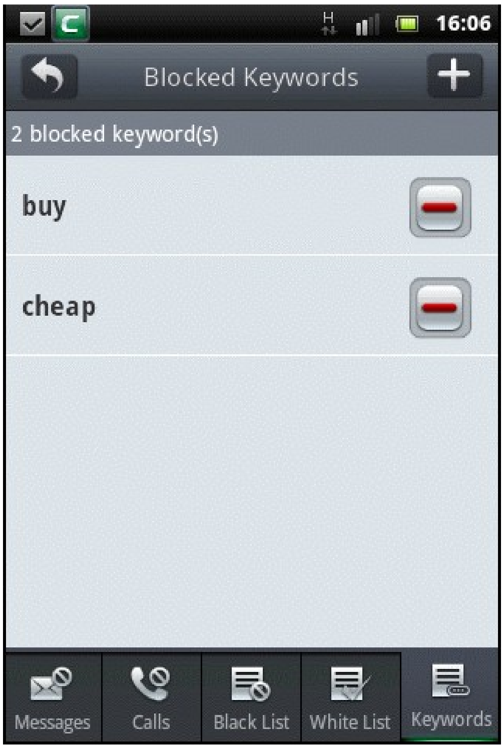
- Tap the 'Keywords' icon located at the bottom of the screen.


Blocked SMS

1 blocked message(s)

+919677074997 2014-01-02 10:29:56
For cheap body lotion contact this number now.

The 'Blocked Keywords' list will be displayed if keywords were already added to the list.


Blocked Keywords

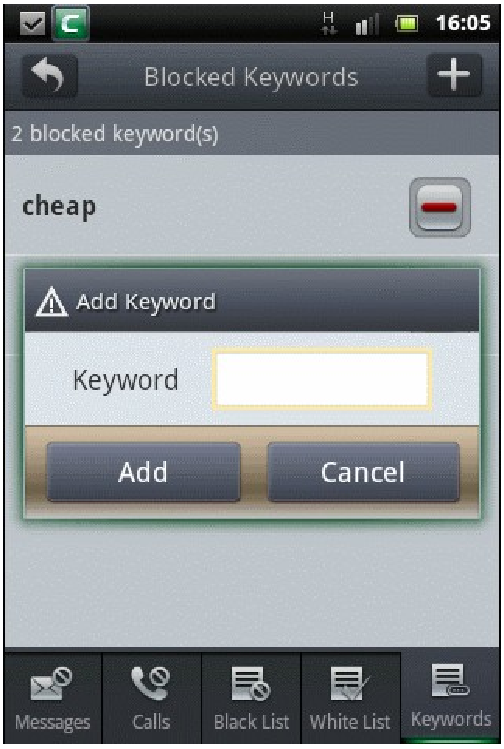
2 blocked keyword(s)

buy

cheap

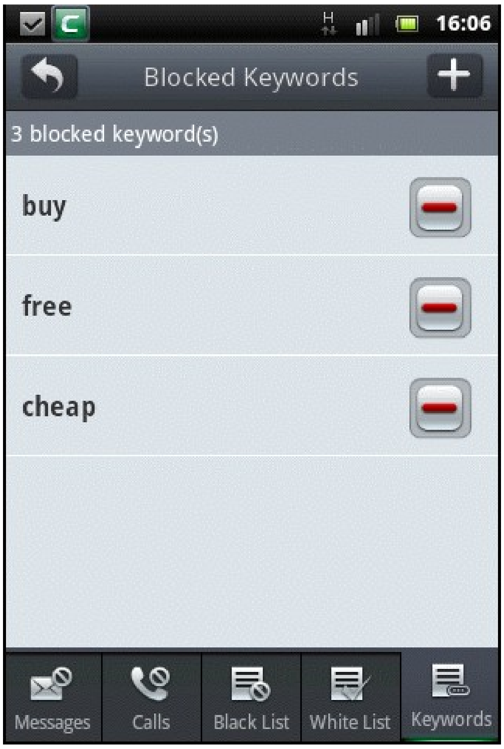
- Tap + button located at the top right to add keywords.

The 'Add Keyword' dialog will be displayed.



- Tap in the 'Keyword' field and fill in the word that CMS should search and automatically block the SMS message.
- Add as many keywords as you desire.

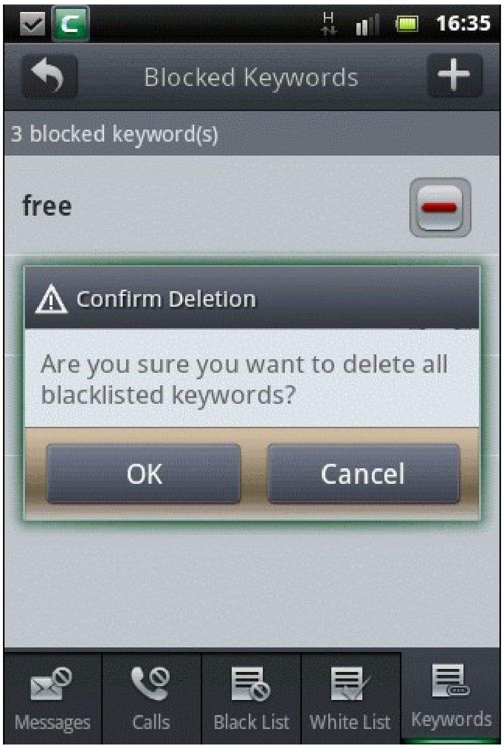
The added keywords will be displayed in the list and messages that contain any of the keywords will be automatically blocked.



- To remove a keyword from the list, tap the ⊖ button beside the keyword that you want to remove and confirm it in the 'Confirm Deletion' dialog.
- To remove all the keywords, tap or press the menu key.

The 'Delete All' button will be displayed.

- Tap 'Delete All' if you want to delete all the keywords.



16:35

Blocked Keywords

3 blocked keyword(s)

free

Confirm Deletion

Are you sure you want to delete all blacklisted keywords?

- Tap 'OK' to confirm the deletion or tap 'Cancel' to cancel the deletion.

Note: Messages sent from whitelisted numbers will not be blocked. Refer '**How to add phone numbers whitelist**' for more details.

How to view blocked messages

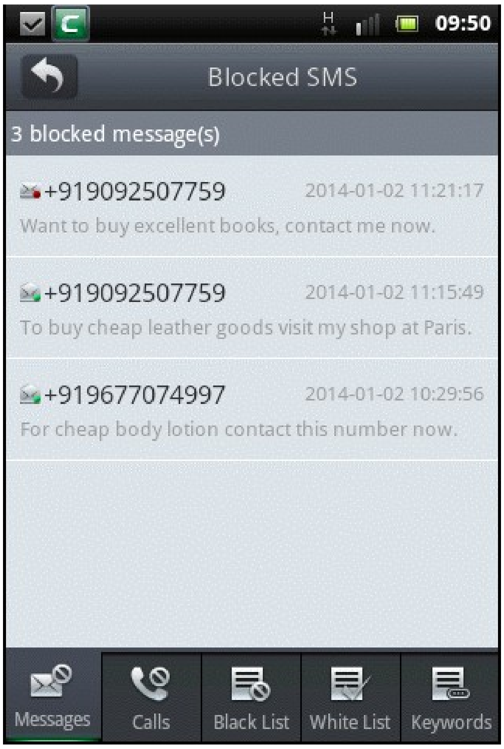
In the blocked messages screen, you can view the list of messages that are blocked and choose to do the following tasks:

- Delete
- Call Back
- Add to Blacklist
- Add to Whitelist
- Export to System SMS

To view blocked messages

- Tap the CMS icon on your device.
- Tap 'Tool's tab located at the top or swipe to the left and tap 'Call/SMS Blocking'.

By default, the blocked SMS messages list will be displayed.



3 blocked message(s)

+919092507759 2014-01-02 11:21:17
Want to buy excellent books, contact me now.

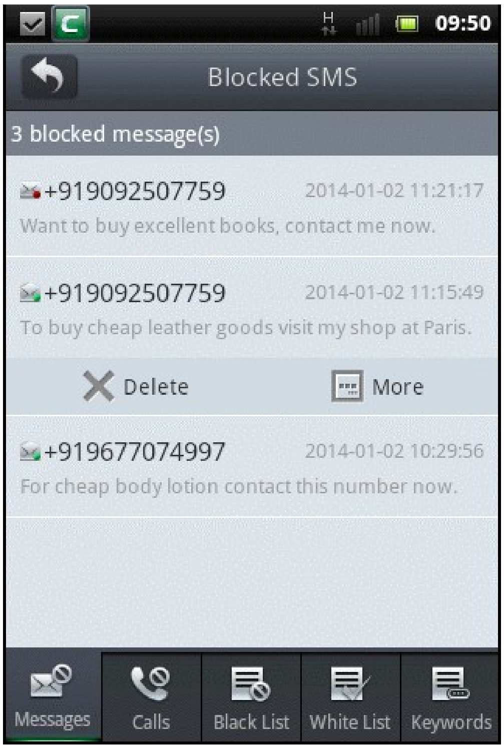
+919092507759 2014-01-02 11:15:49
To buy cheap leather goods visit my shop at Paris.

+919677074997 2014-01-02 10:29:56
For cheap body lotion contact this number now.

The red dot on the message indicates that it has not been viewed and the green dot indicates that the messages have been viewed.

- Tap anywhere on the message bar that you want to view the message.

You can view the full blocked message in the screen.



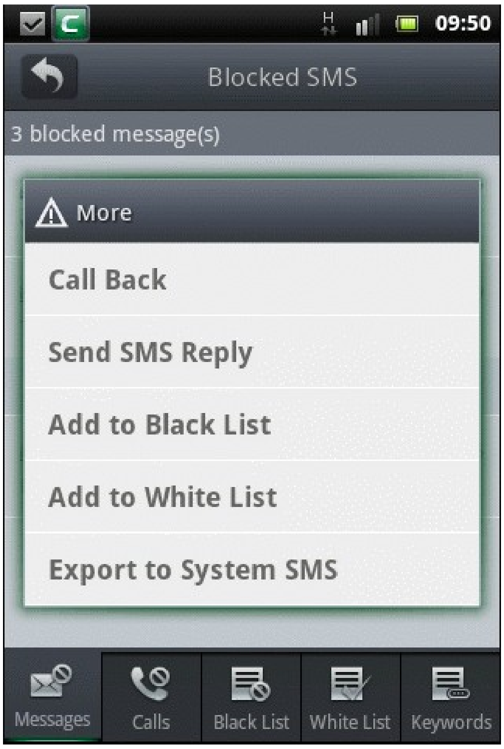
3 blocked message(s)

+919092507759 2014-01-02 11:21:17
Want to buy excellent books, contact me now.

+919092507759 2014-01-02 11:15:49
To buy cheap leather goods visit my shop at Paris.

+919677074997 2014-01-02 10:29:56
For cheap body lotion contact this number now.

- Tap 'Delete' to remove the message from your device and tap 'Yes' in the Confirm Dialog screen.
- Tap 'More'. The following options are available:



- **Call Back** - Tap this bar to contact the sender of the message.
- **Send SMS Reply** - Tap this bar to send a reply message.
- **Add to Black List** - Tap this bar to add the number to blacklist.

Note: Messages sent from blacklisted numbers will be blocked automatically irrespective of whether they contain keywords or not. Refer the sections '**How to block messages**' and '**How to add phone numbers to blacklist**' for more details.

- **Add to White List** - Tap this bar to add the number to whitelist.

Note: Messages sent from whitelisted numbers will not be blocked irrespective of whether they contain keywords or not. Refer the sections '**How to block messages**' and '**How to add phone numbers to whitelist**' for more details.

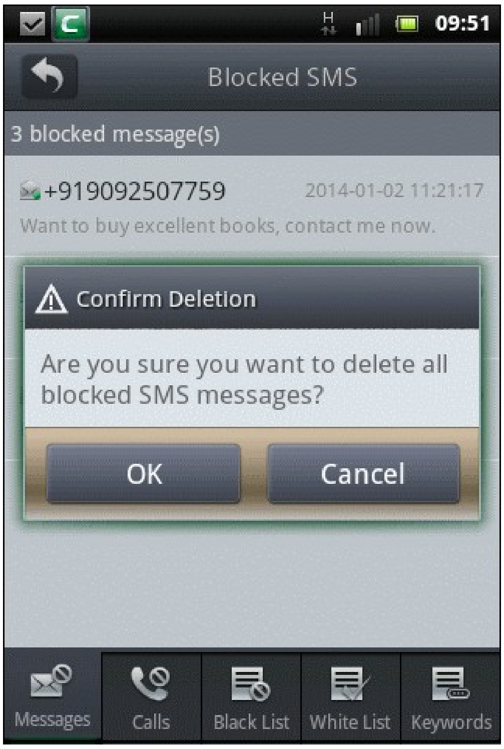
- **Export to System SMS -** Tap this bar to export the message to your device's message box.

CMS allows you to delete all messages or bulk delete some messages.

- In the Blocked SMS screen, tap or press the menu key of your device.

The 'Delete All' and 'Delete Selection' buttons will be displayed.

- Tap 'Delete All' if you want to delete all blocked messages.



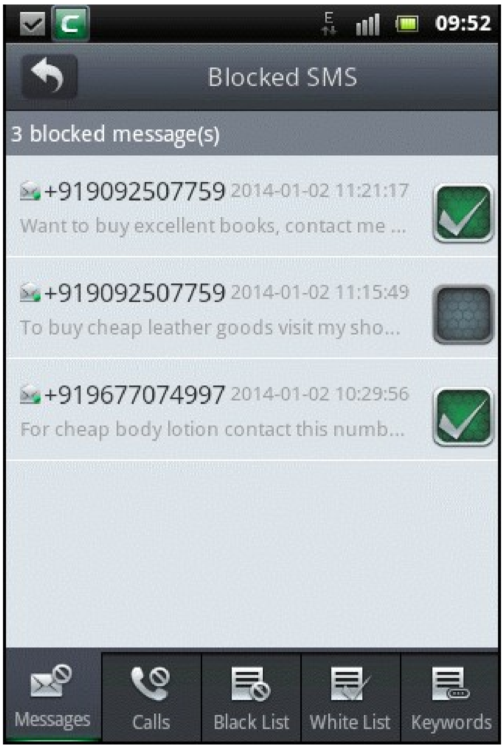
Are you sure you want to delete all blocked SMS messages?

- Tap 'OK' to confirm the deletion.

To bulk delete some messages:

- Tap 'Delete Selection'.

At the right side of each message bar, a selection box will be displayed.



Blocked SMS

3 blocked message(s)

+919092507759 2014-01-02 11:21:17 ☑
Want to buy excellent books, contact me ...

+919092507759 2014-01-02 11:15:49 □
To buy cheap leather goods visit my sho...

+919677074997 2014-01-02 10:29:56 ☑
For cheap body lotion contact this numb...

- Tap the menu key on your phone again and the 'Delete Selected' and 'Select All' button will be displayed.
- Tap 'Select All' if you want to select all blocked messages.
- Tap 'Delete Selected' to delete all the selected blocked messages.

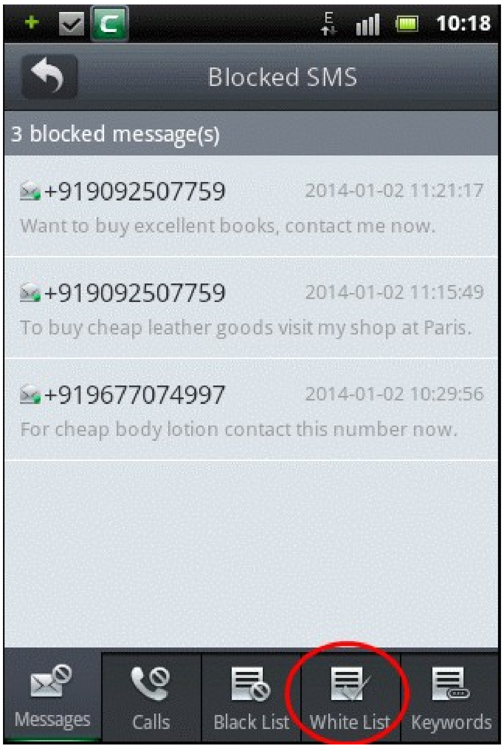
How to add phone numbers to whitelist

CMS will not apply its filters to messages and calls from whitelisted numbers and no messages or calls will be blocked from these numbers.

To add phone numbers to whitelist

- Tap the CMS icon on your device.
- Tap 'Tool's tab located at the top or swipe to the left and tap 'Call/SMS Blocking'.

By default, the blocked SMS messages list will be displayed.



Blocked SMS

3 blocked message(s)

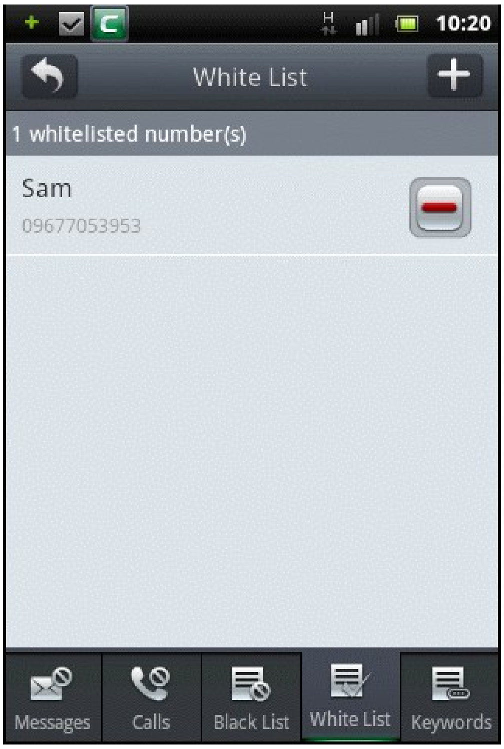
+919092507759 2014-01-02 11:21:17
Want to buy excellent books, contact me now.

+919092507759 2014-01-02 11:15:49
To buy cheap leather goods visit my shop at Paris.

+919677074997 2014-01-02 10:29:56
For cheap body lotion contact this number now.

- Tap 'White List' to add numbers.

The list of phone numbers in whitelist will be displayed if they are already added.



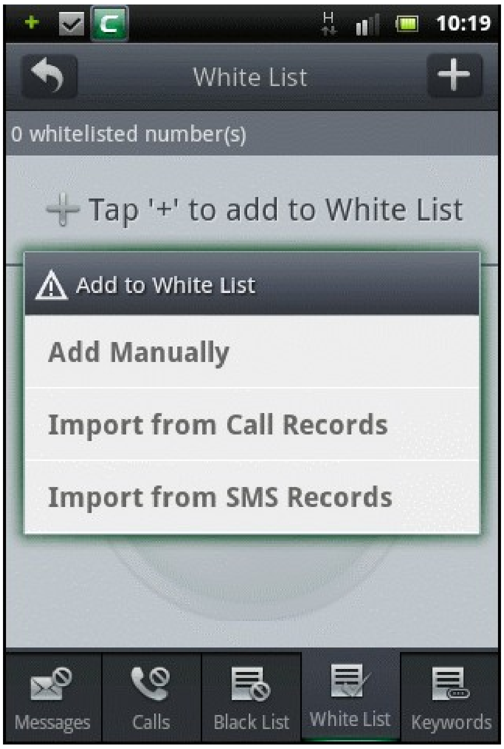
White List

1 whitelisted number(s)

Sam
09677053953

- Tap + to add phone numbers to whitelist.

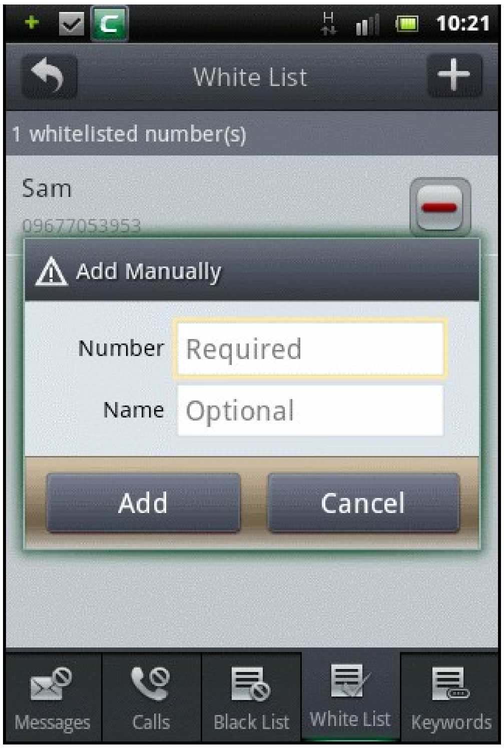
You can add phone numbers to whitelist by three methods:



- **Add Manually** - Tap this bar to add phone numbers manually.
- **Import from Call Records** - Tap this bar to add phone numbers that are in your call records.
- **Import from SMS Records** - Tap this bar to add phone numbers from SMS messages record in your device.

Add Manually

- Tap this bar to add phone numbers manually.



- Tap the Number field and enter the phone number.
- Tap the Name field and enter the name. This is optional.
- Tap 'Add' to confirm the addition of the number to whitelist.

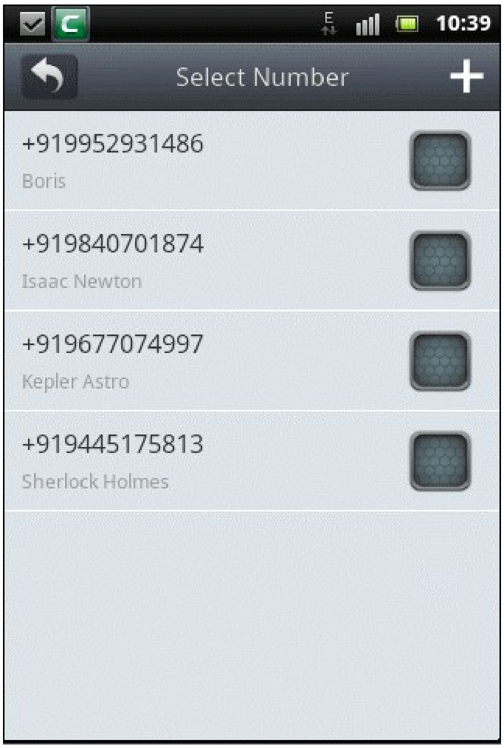
The number will be added to whitelist.

Note: If you add numbers that are already blacklisted, a 'Duplicate Number' alert will be displayed and provide an option to move it to whitelist.

Import from Call / SMS Records

- Tap this bar to add phone numbers that are in your call / SMS records.

The numbers in your call / SMS records will be displayed.



+919952931486
Boris

+919840701874
Isaac Newton

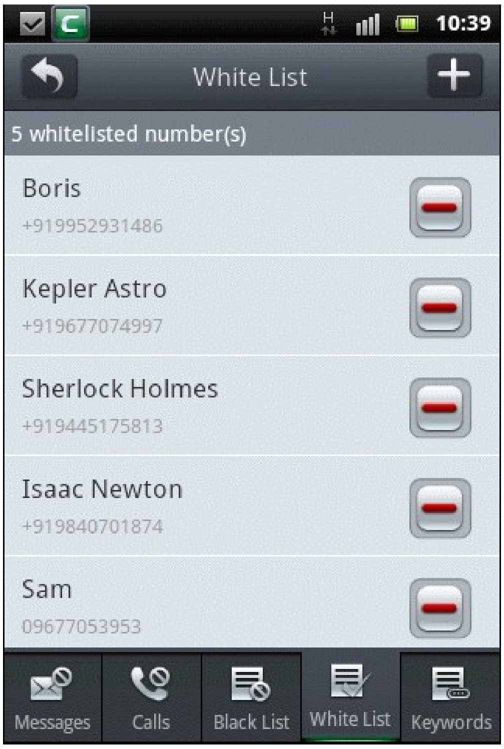
+919677074997
Kepler Astro

+919445175813
Sherlock Holmes

Note: Numbers that are already blacklisted will not be listed in the screen.

- Tap on the box beside the number that you want to add to whitelist.
- After selecting the number(s), tap the + button at the top.

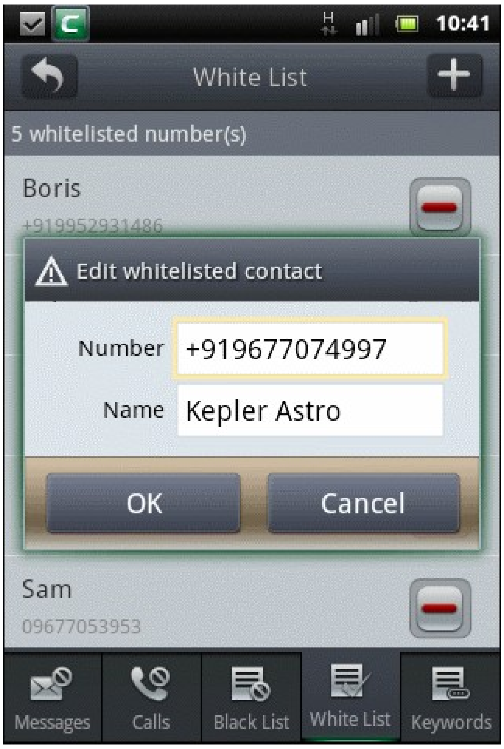
The added number(s) / names will be displayed in whitelist.



5 whitelisted number(s)

Boris	+919952931486
Kepler Astro	+919677074997
Sherlock Holmes	+919445175813
Isaac Newton	+919840701874
Sam	09677053953

- Tap the ⊖ icon beside a number to delete it and tap 'Yes' in the 'Confirm Deletion' screen.
- Tap anywhere on a whitelisted number bar to edit the number and / or the name and tap 'OK'.



5 whitelisted number(s)

Boris +919952931486

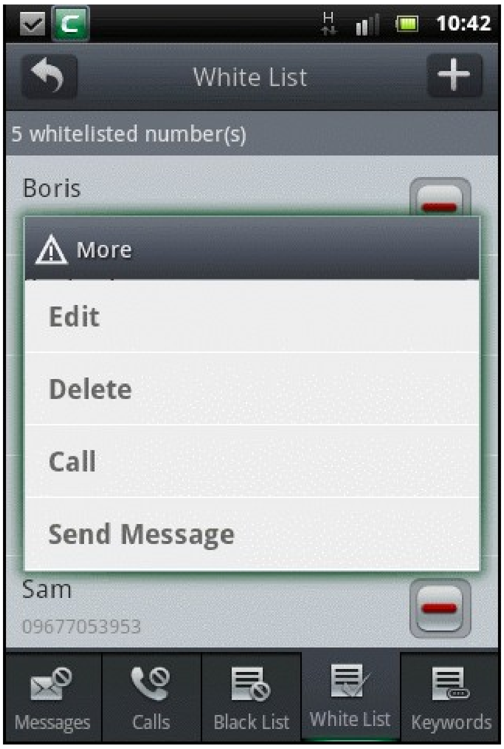
Edit whitelisted contact

Number: +919677074997

Name: Kepler Astro

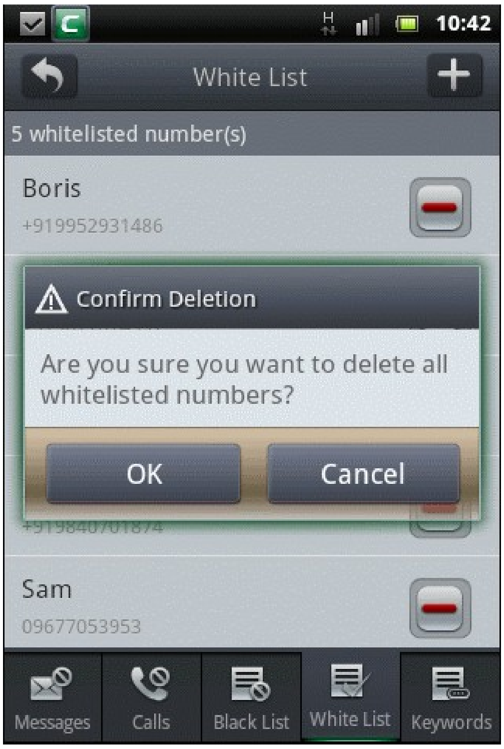
Sam 09677053953

- Tap and hold briefly anywhere on a whitelisted number bar to edit, delete, call or send a SMS message.



CMS allows you to delete all whitelisted numbers.

- Tap or press the menu key in your phone to display the 'Delete All' button.
- Tap 'Delete All' if you want to delete all the whitelisted numbers.



Are you sure you want to delete all whitelisted numbers?

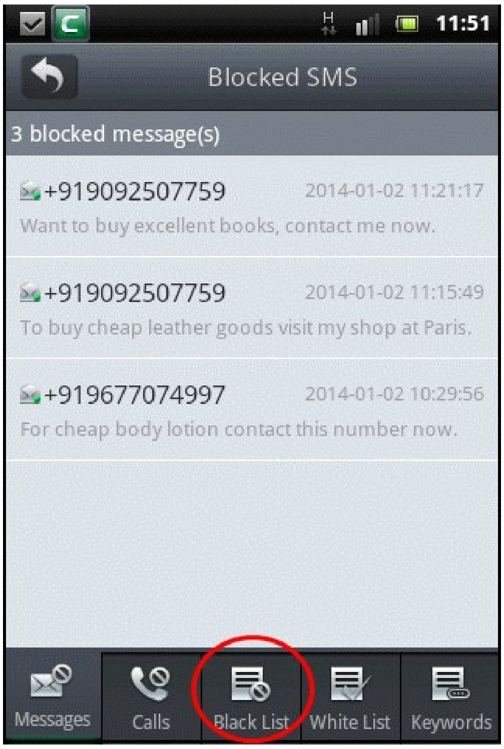
- Tap 'OK' to confirm the deletion.

How to add phone numbers to blacklist

- Tap the CMS icon on your device.

- Tap 'Tool's tab located at the top or swipe to the left and tap 'Call/SMS Blocking'.

By default, the blocked SMS messages list will be displayed.



Blocked SMS

3 blocked message(s)

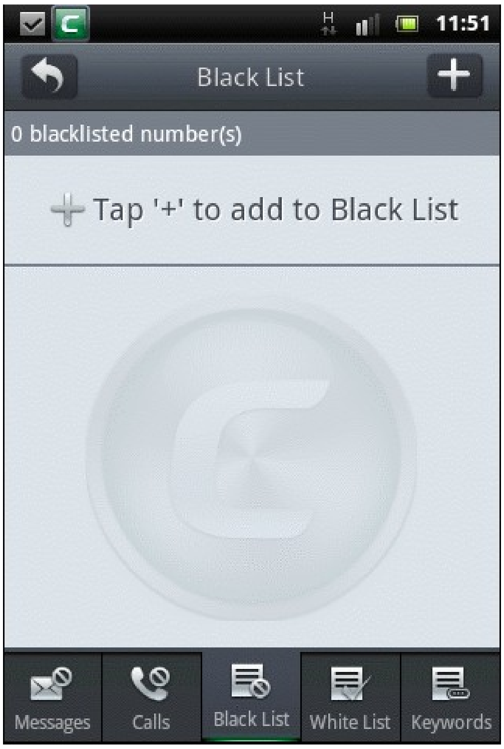
+919092507759 2014-01-02 11:21:17
Want to buy excellent books, contact me now.

+919092507759 2014-01-02 11:15:49
To buy cheap leather goods visit my shop at Paris.

+919677074997 2014-01-02 10:29:56
For cheap body lotion contact this number now.

- Tap 'Black List' to add numbers.

The list of phone numbers in blacklist will be displayed if they are already added.



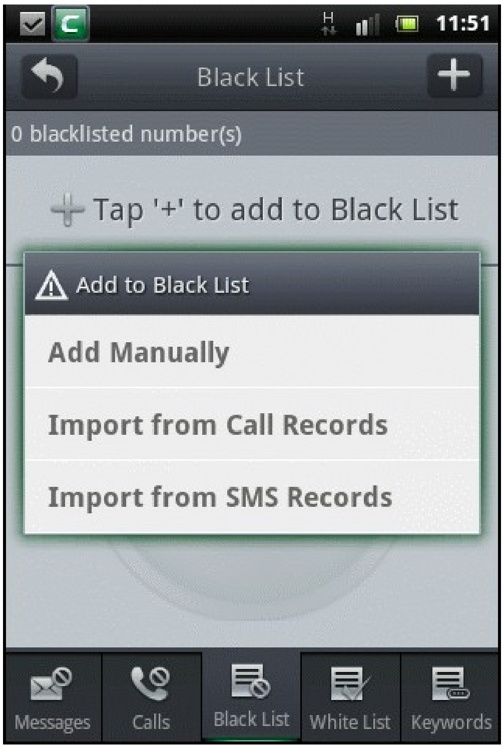
Black List

0 blacklisted number(s)

Tap '+' to add to Black List

- Tap + to add phone numbers to blacklist.

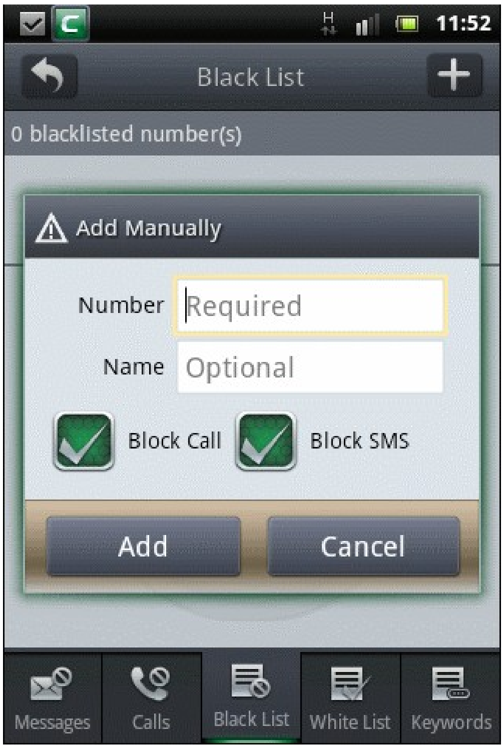
You can add phone numbers to blacklist by three methods:



- **Add Manually** - Tap this bar to add phone numbers manually.
- **Import from Call Records** - Tap this bar to add phone numbers that are in your call records.
- **Import from SMS Records** - Tap this bar to add phone numbers from SMS messages record in your device.

Add Manually

- Tap this bar to add phone numbers manually.



- Tap the Number field and enter the phone number.
- Tap the Name field and enter the name. This is optional.
- Select whether you want block only calls or only messages or both from the 'Block Call and 'Block SMS' options and tap 'Add'.

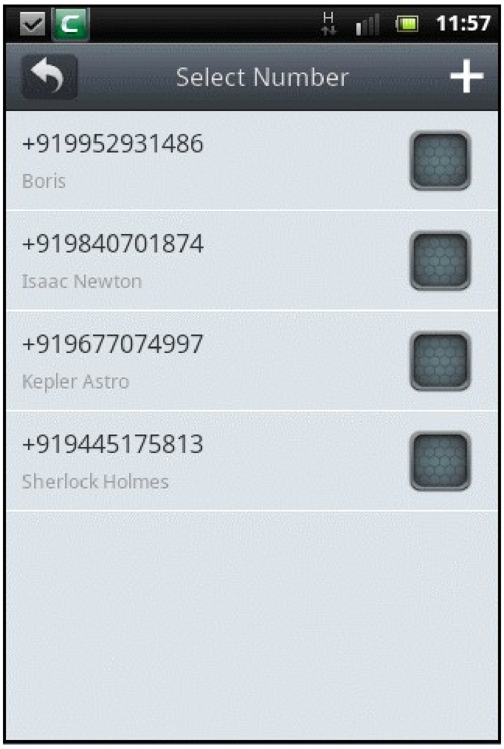
The number will be added to blacklist.

Note: If you add numbers that are already whitelisted, a 'Duplicate Number' alert will be displayed and provide an option to move it to blacklist.

Import from Call / SMS Records

- Tap this bar to add phone numbers that are in your call / SMS records.

The numbers in your call / SMS records will be displayed.



11:57

Select Number

+919952931486
Boris

+919840701874
Isaac Newton

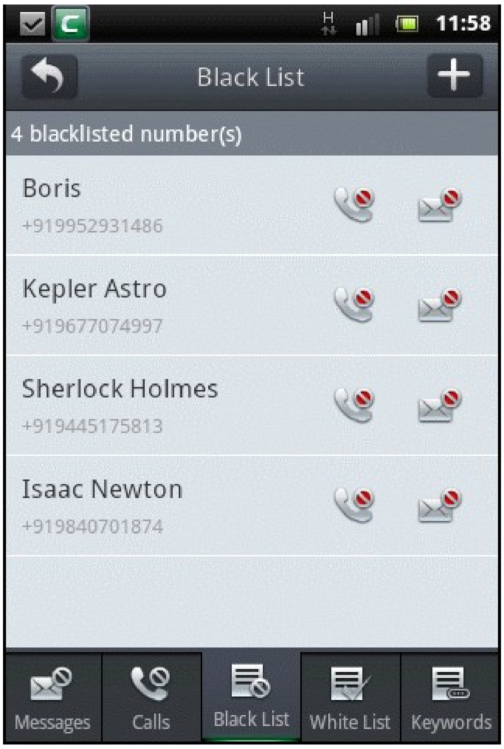
+919677074997
Kepler Astro

+919445175813
Sherlock Holmes

Note: Numbers that are already whitelisted will not be listed in the screen.

- Tap on the box beside the number that you want to add to blacklist.
- After selecting the number(s), tap the + button at the top.

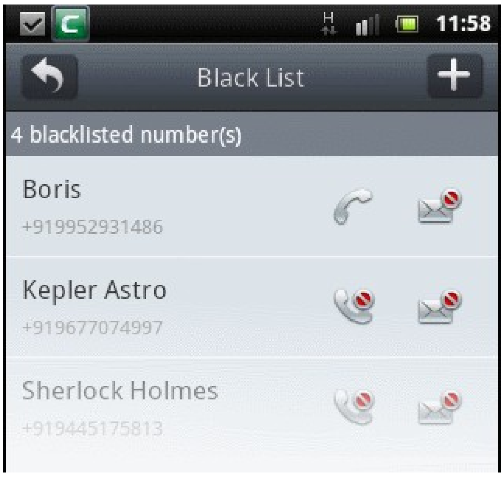
The added number(s) / names will be displayed in blacklist.



4 blacklisted number(s)

Boris	+919952931486
Kepler Astro	+919677074997
Sherlock Holmes	+919445175813
Isaac Newton	+919840701874

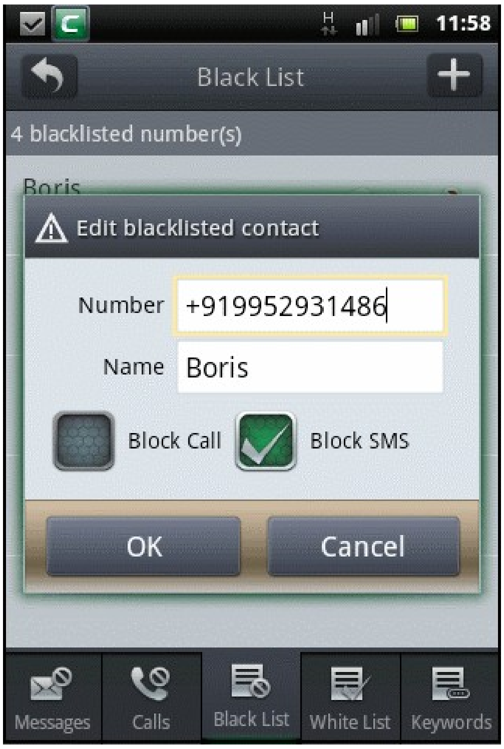
The icons ☎ and ✉ beside a blacklisted number indicate that both calls and messages are blocked. If you want to allow calls only, tap on the phone icon. Its status will change to allow. Similarly you can enable messages for the blacklisted number.



4 blacklisted number(s)

Boris	+919952931486
Kepler Astro	+919677074997
Sherlock Holmes	+919445175813

- Tap anywhere on a blacklisted number bar to edit the number and / or the name, allow calls / SMS and tap 'OK'.



Black List

4 blacklisted number(s)

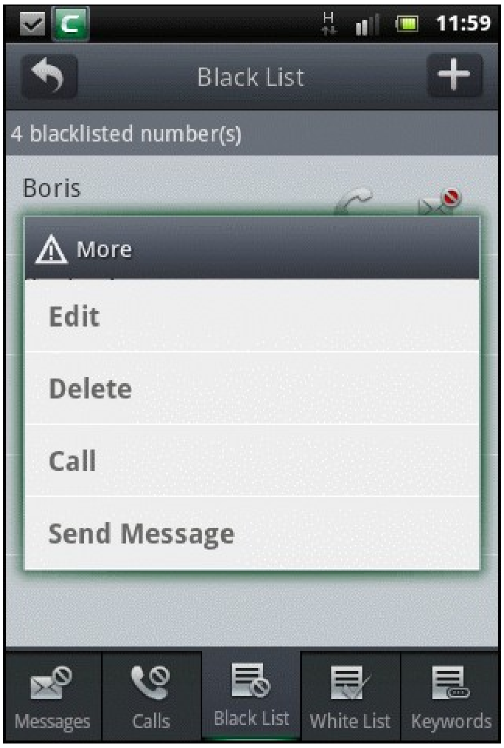
Edit blacklisted contact

Number: +919952931486

Name: Boris

□ Block Call ☑ Block SMS

- Tap and hold briefly anywhere on a blacklisted number bar to edit, delete, call or send a SMS message.



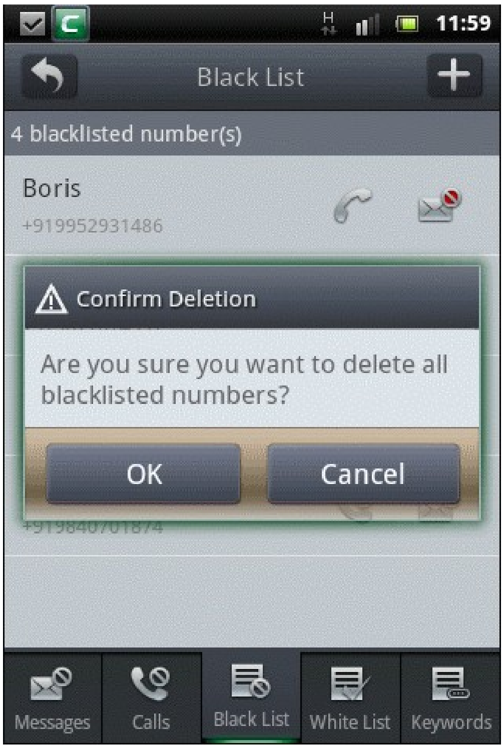
Black List

4 blacklisted number(s)

Boris

CMS allows you to delete all blacklisted numbers.

- Tap or press the menu key in your phone to display the 'Delete All' button.
- Tap 'Delete All' if you want to delete all the blacklisted numbers.



Are you sure you want to delete all blacklisted numbers?

- Tap 'OK' to confirm the deletion.

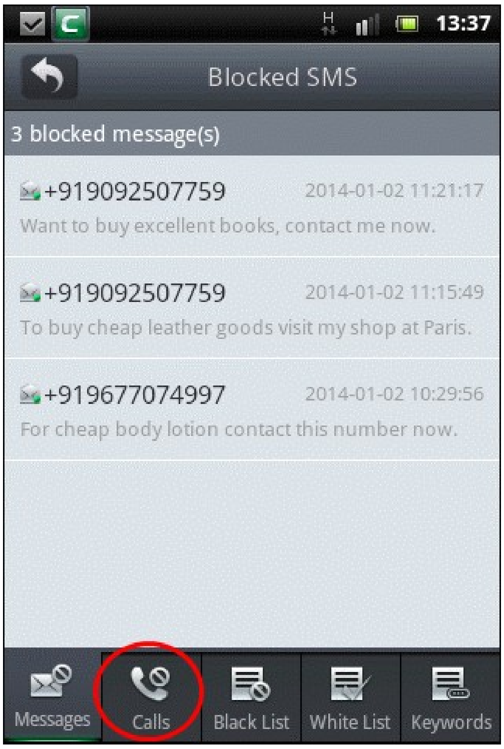
How to view blocked call list

The blocked call list screen allows you to view the list of blocked calls and edit a selected item such as adding it to the blacklist or whitelist, sending a message or call the number. Please note that an incoming call with a single ring will be displayed in the blocked call list.

To view blocked calls

- Tap the CMS icon on your device.
- Tap 'Tool's tab located at the top or swipe to the left and tap 'Call/SMS Blocking'.

By default, the blocked SMS messages list will be displayed.



13:37

Blocked SMS

3 blocked message(s)

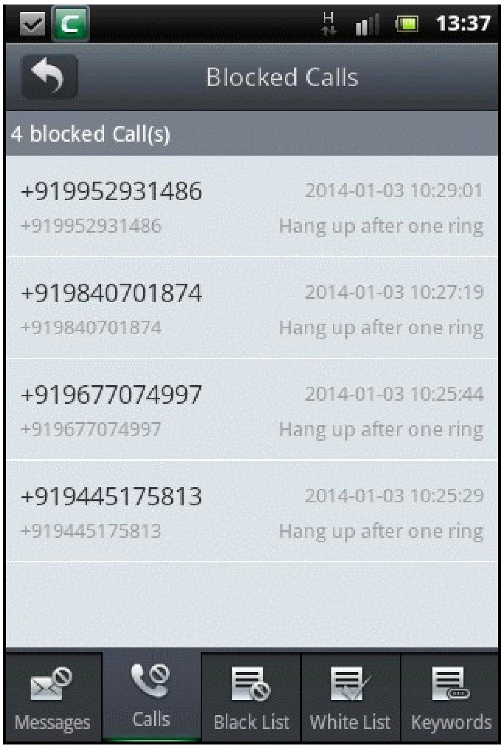
+919092507759 2014-01-02 11:21:17
Want to buy excellent books, contact me now.

+919092507759 2014-01-02 11:15:49
To buy cheap leather goods visit my shop at Paris.

+919677074997 2014-01-02 10:29:56
For cheap body lotion contact this number now.

- Tap 'Calls' to view the list of blocked calls.

The list of blocked calls will be displayed.



13:37

Blocked Calls

4 blocked Call(s)

+919952931486 2014-01-03 10:29:01
+919952931486 Hang up after one ring

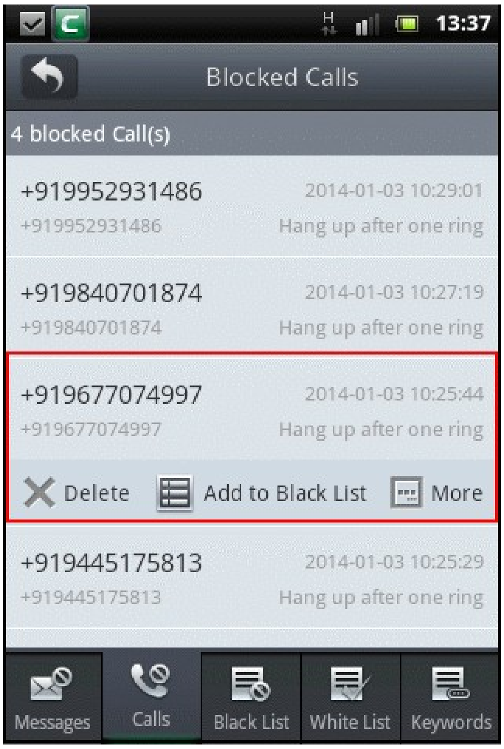
+919840701874 2014-01-03 10:27:19
+919840701874 Hang up after one ring

+919677074997 2014-01-03 10:25:44
+919677074997 Hang up after one ring

+919445175813 2014-01-03 10:25:29
+919445175813 Hang up after one ring

Note: An incoming call that rings only once will be displayed in the Blocked Calls list. This number then can be added to blacklist, whitelist or deleted.

- Tap anywhere on a blocked call number bar.



Blocked Calls

4 blocked Call(s)

+919952931486 2014-01-03 10:29:01
+919952931486 Hang up after one ring

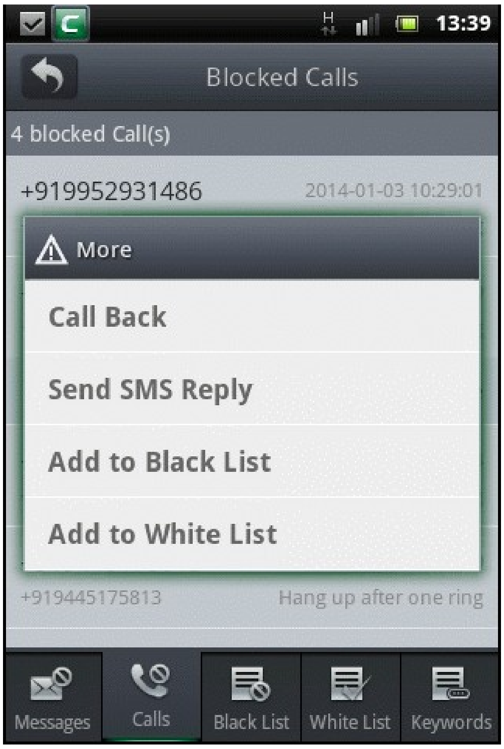
+919840701874 2014-01-03 10:27:19
+919840701874 Hang up after one ring

+919677074997 2014-01-03 10:25:44
+919677074997 Hang up after one ring

+919445175813 2014-01-03 10:25:29
+919445175813 Hang up after one ring

- Tap 'Delete' to remove the selected item from your device.
- Tap 'Add to Black List' to add the selected item to the list of blacklisted numbers and confirm your choice in the subsequent screens.
- Tap 'More'.

The following options are available:



Blocked Calls

4 blocked Call(s)

+919952931486 2014-01-03 10:29:01

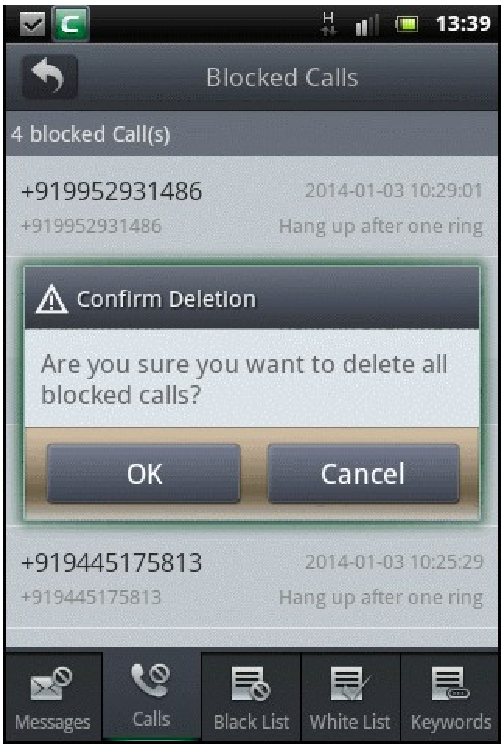
+919445175813 Hang up after one ring

- **Call Back** - Tap this bar to contact the caller.
- **Send SMS Reply** - Tap this bar to send a message to the caller.
- **Add to Black List** - Tap this bar to add the number to blacklist.

- **Add to White List** - Tap this bar to add the number to whitelist.

CMS allows you to delete all calls or bulk delete some calls.

- Tap or press the menu key on your phone to display the 'Delete All' and 'Delete Selection' button.
- Tap 'Delete All' if you want to delete all blocked calls.



Blocked Calls

4 blocked Call(s)

+919952931486 2014-01-03 10:29:01
+919952931486 Hang up after one ring

Confirm Deletion

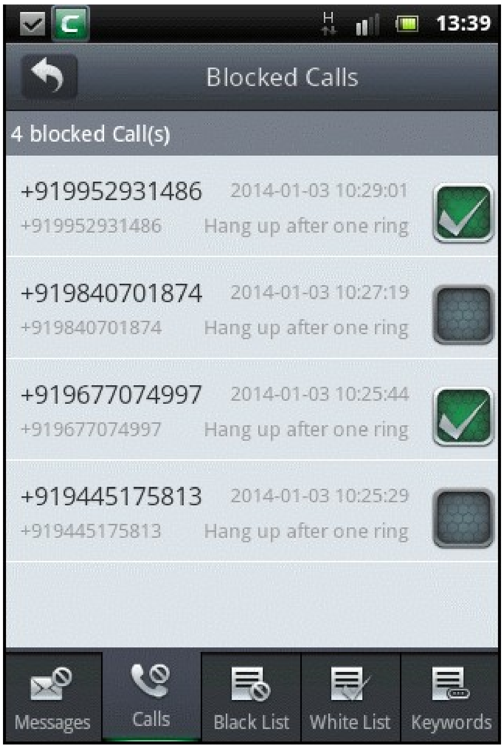
Are you sure you want to delete all blocked calls?

+919445175813 2014-01-03 10:25:29
+919445175813 Hang up after one ring

- Tap 'OK' to confirm the deletion.

To bulk delete some calls:

- Tap 'Delete Selection'.
- Tap on the box beside the blocked call(s) that you want to delete.



Blocked Calls

4 blocked Call(s)

+919952931486 2014-01-03 10:29:01 ☑
+919952931486 Hang up after one ring

+919840701874 2014-01-03 10:27:19 □
+919840701874 Hang up after one ring

+919677074997 2014-01-03 10:25:44 ☑
+919677074997 Hang up after one ring

+919445175813 2014-01-03 10:25:29 □
+919445175813 Hang up after one ring

- Tap the menu key again to display the 'Delete Selected' and 'Select All' button.
- Tap 'Select All' if you want to select all blocked calls.
- Tap 'Delete Selected' to delete all the selected blocked calls.

The selected blocked call(s) will be deleted from the list.

10. Backup

The Backup feature in CMS allows you to back up important data such as:

- Contacts stored in your device
- Text messages
- Contacts, messages and call registers in your Private Space
- CMS configuration

> **Note**: The applications in your device can be backed up by using the **Software Manager** feature. For more details refer to '**How to view the installed apps and take a backup or uninstall them**' section.

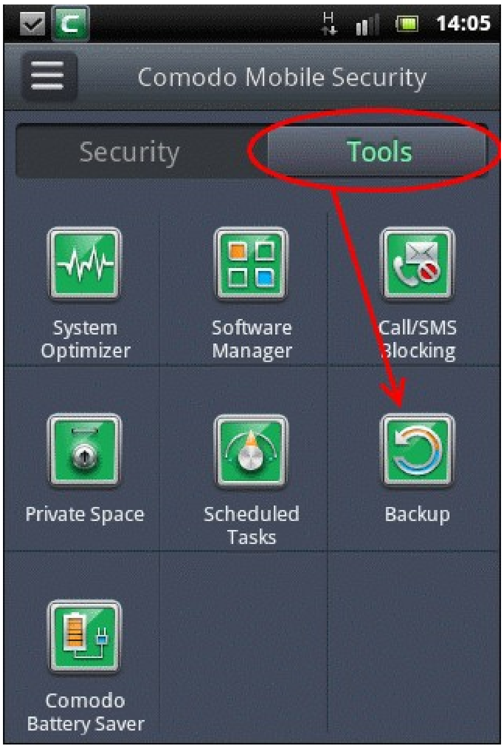
All the backup files are stored in your SD card. In the case of data loss or apps uninstalled accidentally, you can easily restore the backed up data instantly. You can view the details of logs of backup and restore operations in the History screen.

Click the following links for help with specific backup tasks:

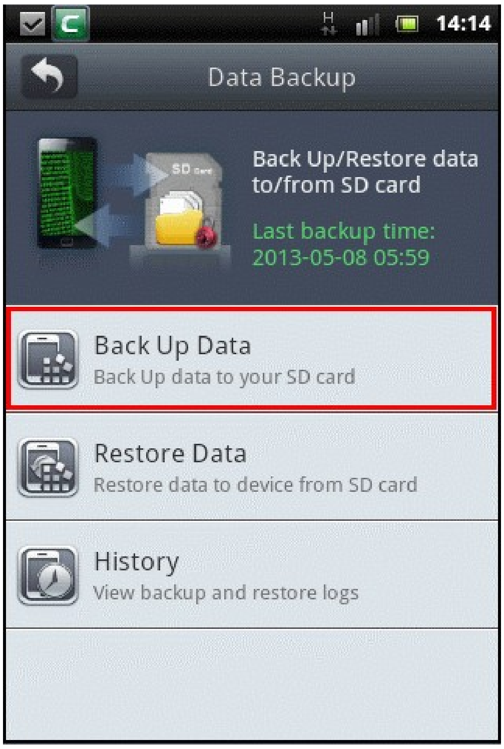
- **How to backup your data**
- **How to restore your data**
- **How to view data backup and restore logs**

How to backup your data

- Tap the CMS icon C on your device.
- Tap 'Tool's tab located at the top or swipe to the left and tap 'Backup'.



The Data Backup screen will be displayed.



Back Up/Restore data to/from SD card

Last backup time: 2013-05-08 05:59

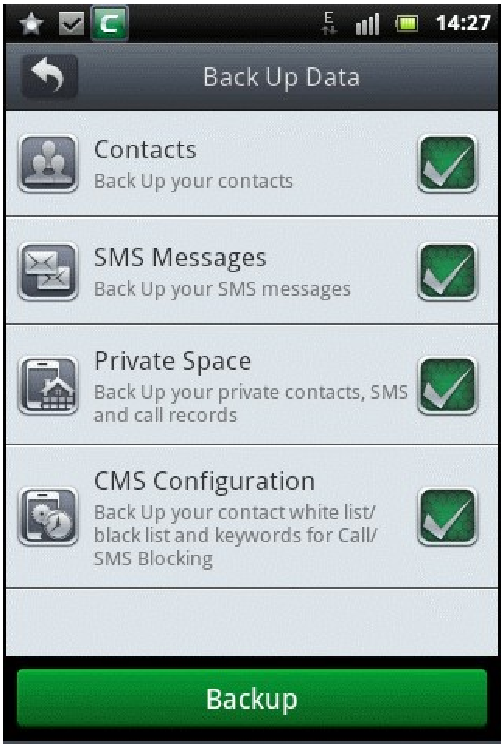
Back Up Data
Back Up data to your SD card

Restore Data
Restore data to device from SD card

History
View backup and restore logs

- Tap 'Backup Data'.

The list of items to be backed up will be displayed.



14:27

Back Up Data

Contacts
Back Up your contacts ☑

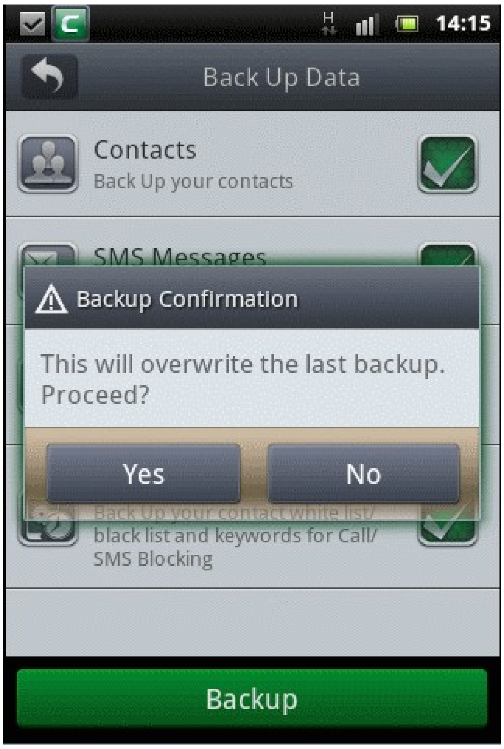
SMS Messages
Back Up your SMS messages ☑

Private Space
Back Up your private contacts, SMS and call records ☑

CMS Configuration
Back Up your contact white list/ black list and keywords for Call/ SMS Blocking ☑

- Select the items you want to backup, from Contacts stored in your device, Text messages, Private Space and CMS configuration by tapping the check box beside the item. Tap once again to deselect an item.
- Tap 'Backup'.

If you have taken backups earlier, the current backup will overwrite the last backup and an alert will be displayed to confirm it.



14:15

Back Up Data

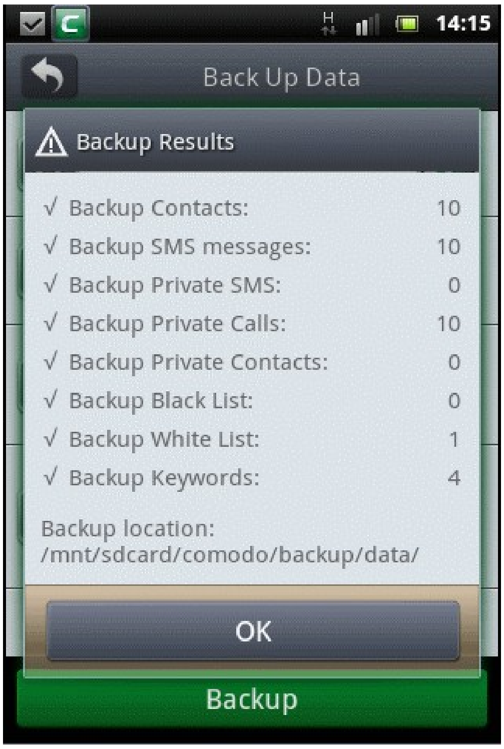
Backup Confirmation

This will overwrite the last backup. Proceed?

- Tap 'Yes' to allow the current backup to overwrite the last backup.

Tip: If you want to preserve the last backup, before starting the backup process, navigate to the folder comodo/backup/data in your SD Card through a third party File Manager App and store a copy of the backup file to a safe location. If you want to restore your data from the previous backup file, simply replace the existing backup file at the location comodo/backup/data with the previous backup file and restore your data. For more details on restoring your data, refer to '**How to restore your data**'.

The selected items will be backed up to the location SD Card/comodo/backup/data and on completion, the results will be displayed.



Backup Results

√ Backup Contacts:	10
√ Backup SMS messages:	10
√ Backup Private SMS:	0
√ Backup Private Calls:	10
√ Backup Private Contacts:	0
√ Backup Black List:	0
√ Backup White List:	1
√ Backup Keywords:	4

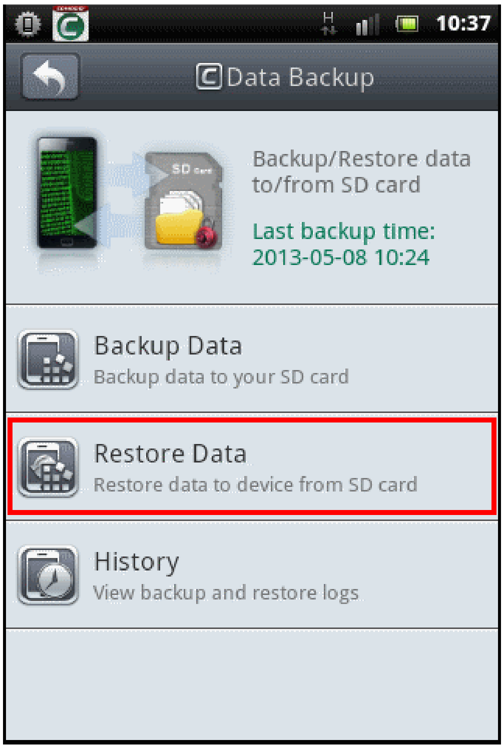
Backup location:
/mnt/sdcard/comodo/backup/data/

- Tap 'OK'.

How to restore your data

- Tap the CMS icon on your device.
- Tap 'Tool's tab located at the top or swipe to the left and tap 'Backup'.

The Data Backup screen will be displayed.



10:37

Data Backup

Backup/Restore data to/from SD card

Last backup time: 2013-05-08 10:24

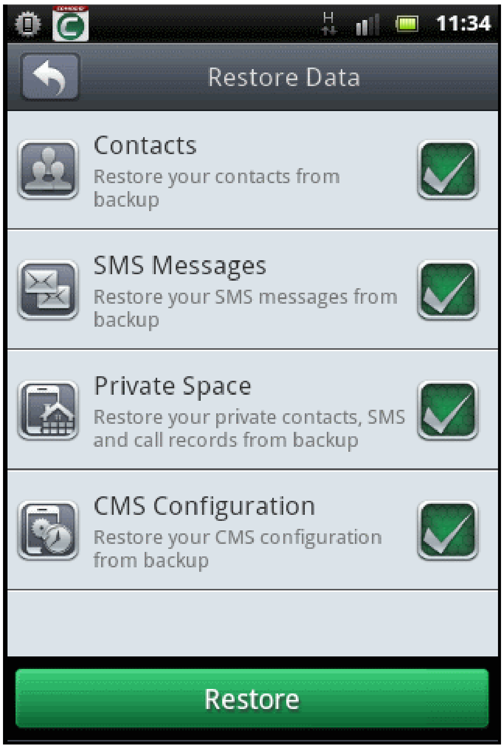
Backup Data
Backup data to your SD card

Restore Data
Restore data to device from SD card

History
View backup and restore logs

- Tap 'Restore Data'.

The list of items to be restored will be displayed.



11:34

Restore Data

Contacts
Restore your contacts from backup ☑

SMS Messages
Restore your SMS messages from backup ☑

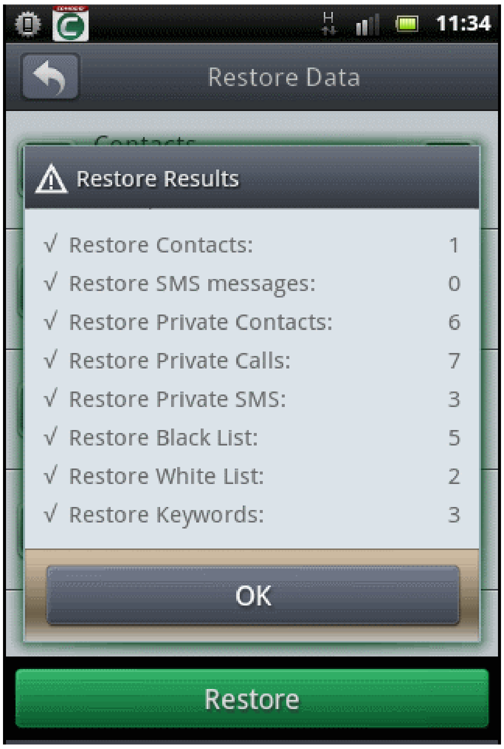
Private Space
Restore your private contacts, SMS and call records from backup ☑

CMS Configuration
Restore your CMS configuration from backup ☑

Restore

- Select the items you want to restore by tapping the check box beside the item. Tap once again to deselect an item.
- Tap 'Restore'.

The selected items will be restored to your device from the SD Card and on completion, the results will be displayed.



11:34

Restore Data

Restore Results

√ Restore Contacts: 1

√ Restore SMS messages: 0

√ Restore Private Contacts: 6

√ Restore Private Calls: 7

√ Restore Private SMS: 3

√ Restore Black List: 5

√ Restore White List: 2

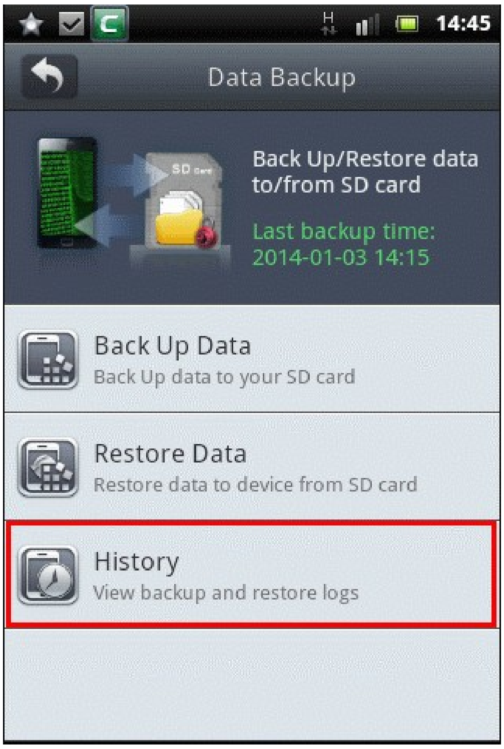
√ Restore Keywords: 3

- Tap 'OK'.

How to view data backup and restore logs

- Tap the CMS icon on your device.
- Tap 'Tool's tab located at the top or swipe to the left and tap 'Backup'.

The Data Backup screen will be displayed.



14:45

Data Backup

Back Up/Restore data to/from SD card

Last backup time: 2014-01-03 14:15

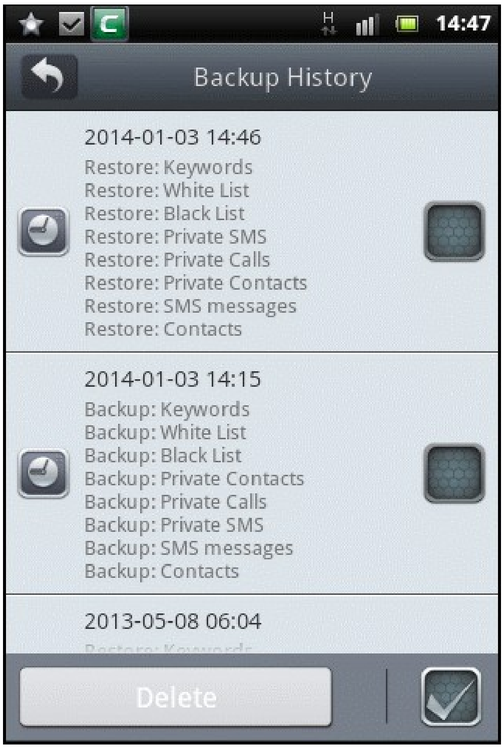
Back Up Data
Back Up data to your SD card

Restore Data
Restore data to device from SD card

History
View backup and restore logs

- Tap 'History'.

The Backup/Restore logs will be displayed.

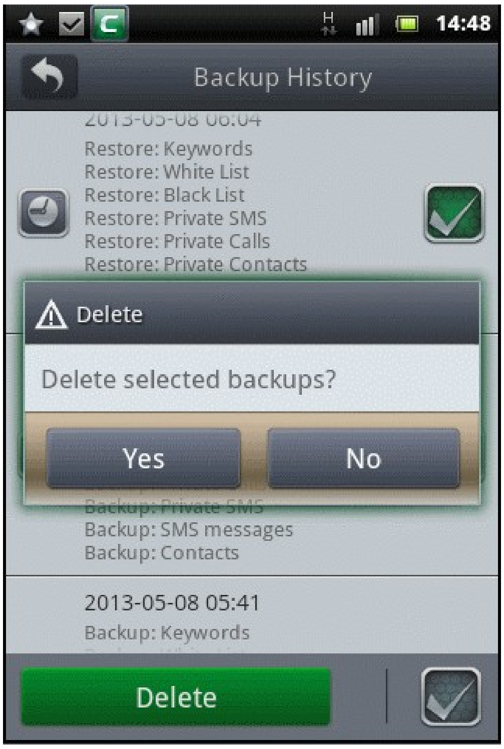


2014-01-03 14:46
Restore: Keywords
Restore: White List
Restore: Black List
Restore: Private SMS
Restore: Private Calls
Restore: Private Contacts
Restore: SMS messages
Restore: Contacts

2014-01-03 14:15
Backup: Keywords
Backup: White List
Backup: Black List
Backup: Private Contacts
Backup: Private Calls
Backup: Private SMS
Backup: SMS messages
Backup: Contacts

2013-05-08 06:04

- Scroll up or down to view the full list of logs.
- Tap the selection box beside 'Delete' at the bottom to select all the logs.
- If you want to delete only some log(s), tap the check box beside them.
- Tap the 'Delete' button after you have selected the log entries.



2013-05-08 06:04
Restore: Keywords
Restore: White List
Restore: Black List
Restore: Private SMS
Restore: Private Calls
Restore: Private Contacts

Delete

Delete selected backups?

Backup: Private SMS
Backup: SMS messages
Backup: Contacts

2013-05-08 05:41
Backup: Keywords

- In the 'Delete' confirmation dialog, tap 'Yes' to confirm the deletion of selected log entries.

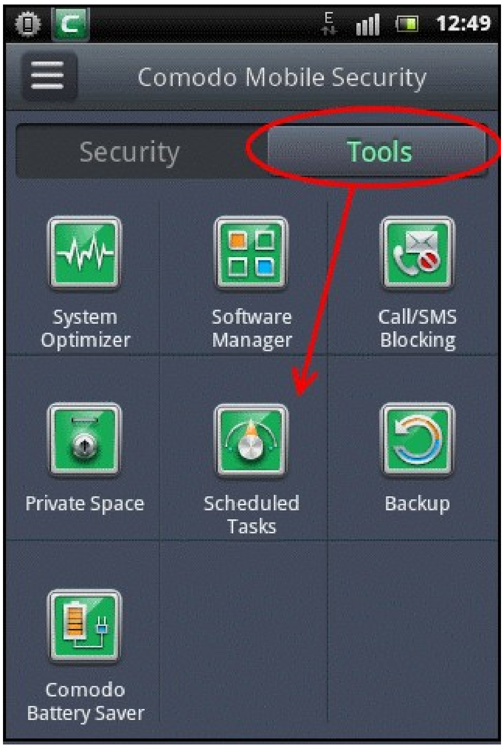
The selected log entries will be deleted from the list.

11. Scheduled Tasks

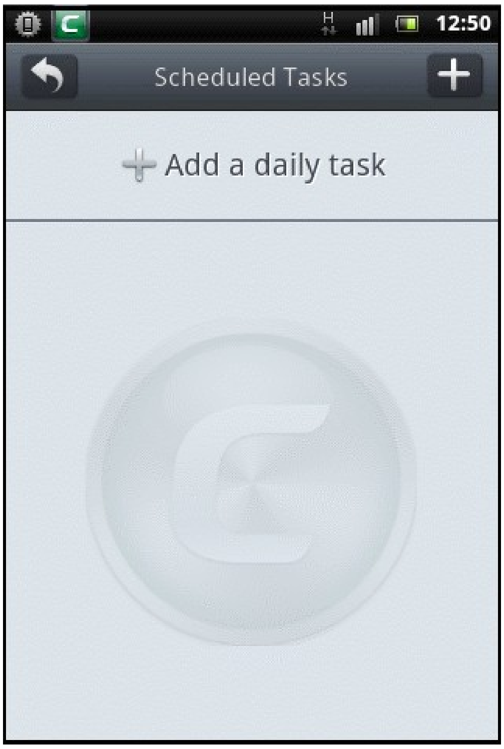
The Task Scheduler feature in CMS allows you to automate the antivirus scanning process. You can choose to run the scan on any day or all days at a preset time. You can also set schedules for 'Enter Flight Mode' and 'Leave Flight Mode' on your device.

How to schedule a task

- Tap the CMS icon on your device.
- Tap 'Tool's tab located at the top or swipe to the left and tap 'Scheduled Tasks'.

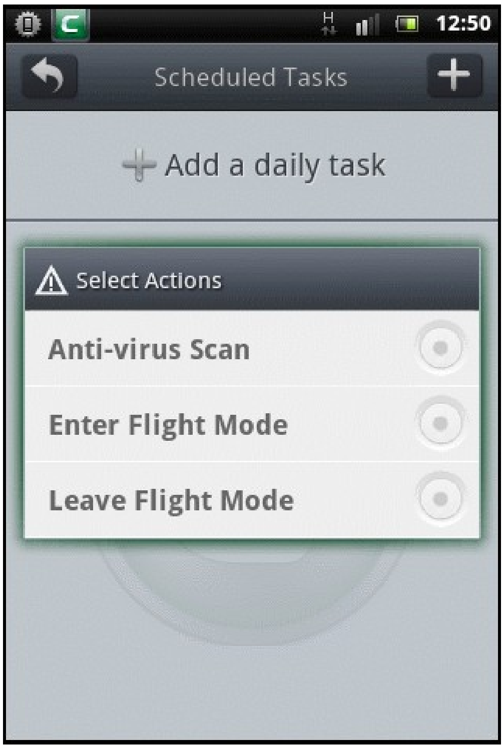


The Scheduled Tasks screen will be displayed.



- Tap the '+' button at the top or anywhere on the 'Add a daily task' row to add a new task.

The Select Actions dialog will be displayed.

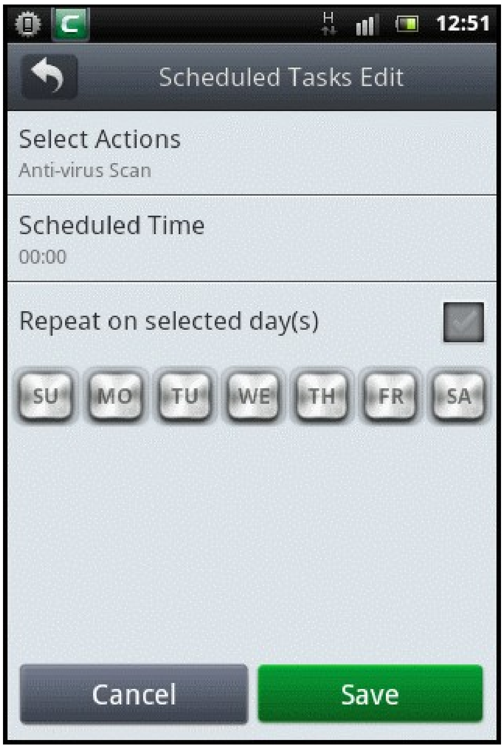


The following tasks can be scheduled.

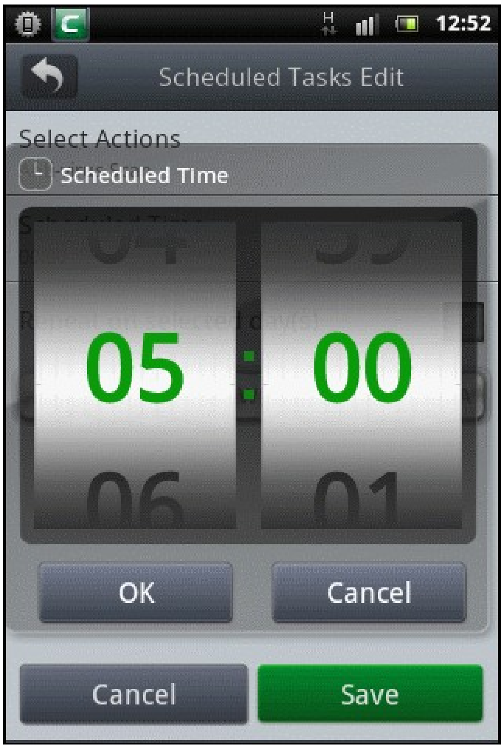
- Anti-virus Scan
- Enter Flight Mode
- Leave Flight Mode

From the options, select any of the actions.

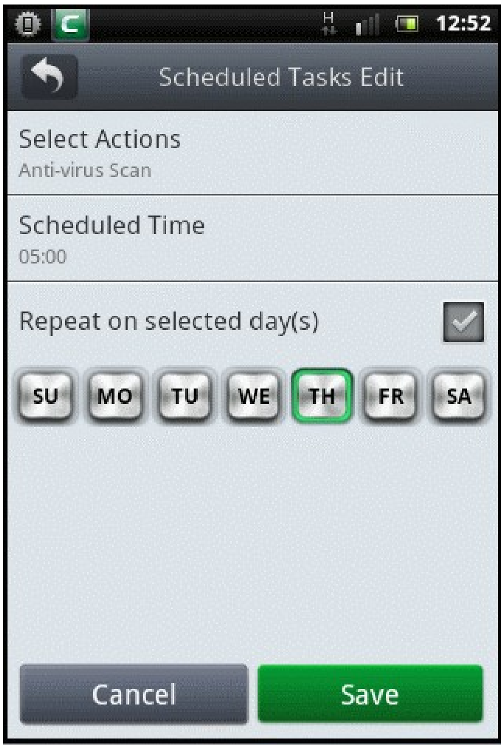
The 'Select Actions' bar will display the selected action in the Scheduled Tasks Edit screen. For example, Anti-virus Scan.



- Tap anywhere on the 'Scheduled Time' bar.



- Select the time at which the task should start.
- Tap 'OK' after selecting the time.
- Tap 'Repeat on selected day(s)' to select the day on which the task should run.



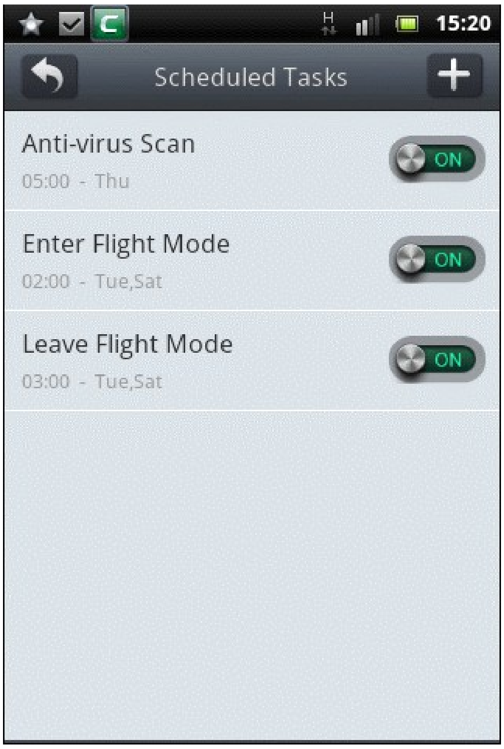
Select Actions
Anti-virus Scan

Scheduled Time
05:00

Repeat on selected day(s) ☑

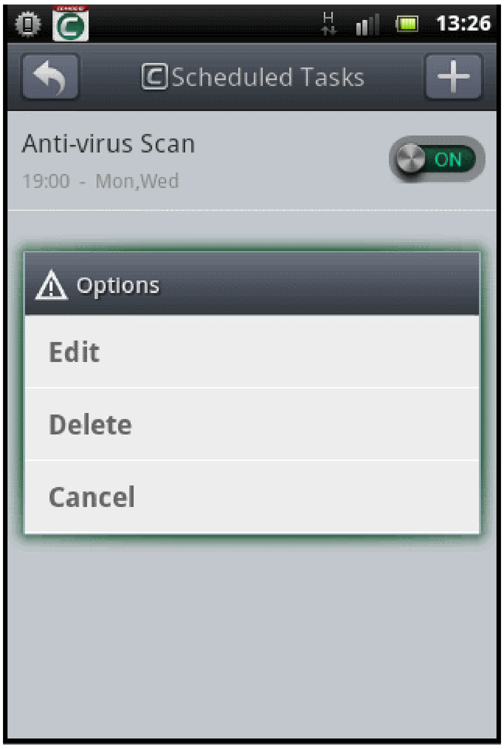
- Select the day on which the task should run and tap the 'Save' button.
- Repeat the procedure to add as many scheduled tasks as you require in the same manner described above.

The list of scheduled tasks will be displayed.



Anti-virus Scan 05:00 - Thu	ON
Enter Flight Mode 02:00 - Tue,Sat	ON
Leave Flight Mode 03:00 - Tue,Sat	ON

- To disable a scheduled task, tap on the toggle switch to display 'OFF' condition. To enable it again, tap on it again.
- To edit a scheduled task, tap on the task and edit the required details.
- To edit or delete a scheduled task from your device, tap and hold briefly on the task.



- Tap 'Edit' and edit the task.
- Tap 'Delete' to remove the task.

12. Anti Theft

The Anti Theft feature in CMS enables you to recover your device easily if it is mislaid, lost or even stolen. The feature allows you to remotely:

- Sound a loud alarm on your device in order to identify its location
- Get the location of your device in Google maps
- Send an text message to your buddy's phone if someone changes the SIM card
- Remotely lock the device to prevent unauthorized access
- Wipe off all your private and confidential data including text messages, Contacts, Browser Bookmarks, even the pictures, music/video and other files stored in its SD card
- Take a photograph from your missing or stolen device and receive it at your email to identify the possessor

Anti-Theft Text Codes

(txt to your missing device)

- locate#yourpassword
- alarm#yourpassword
- lock#yourpassword
- wipe#yourpassword
- takephoto#yourpassword

All the above can be done remotely, just by sending commands as SMS messages from your any other phone.

You need to activate Anti Theft to get the full benefits of the feature. Click the links below for the help with the Anti Theft tasks.

- **How to view the demo of Anti theft feature**
- **How to activate Anti theft**
- **How to make your device to sound an alarm**
- **How to get the location of your device**
- **How to remotely lock your device**

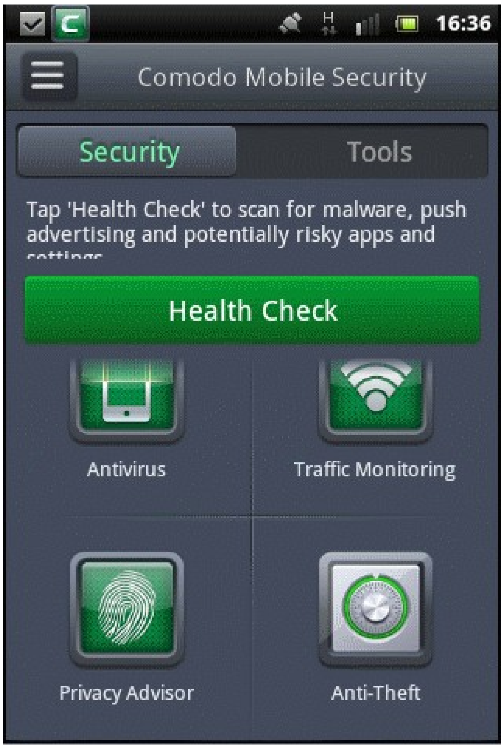
- **How to remotely wipe all your confidential data from your device**
- **How to remotely take a photograph**
- **How to configure Anti theft Settings**

You can watch the demonstration of each feature at anytime by accessing the Anti theft screen and tapping on the respective feature.

To view the demo

- Tap the CMS icon on your device.

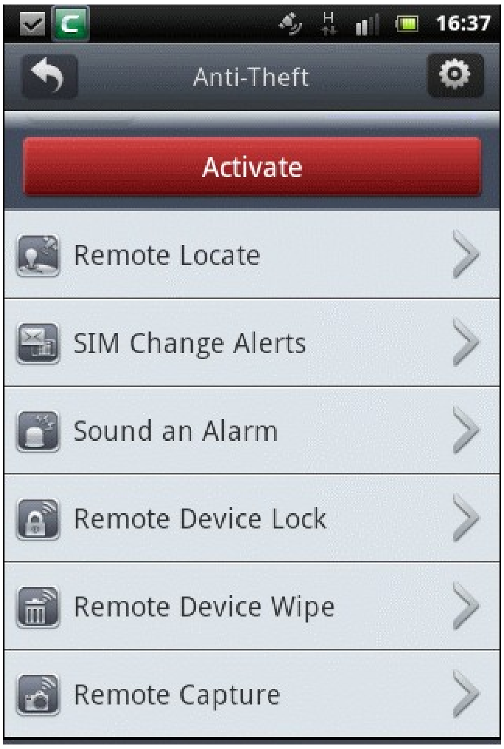
The home page of CMS under Security tab will open.



Tap 'Health Check' to scan for malware, push advertising and potentially risky apps and settings

- Tap 'Anti Theft'.

The Anti Theft screen will be displayed.



- Tap on the feature for which you wish to watch the demo.

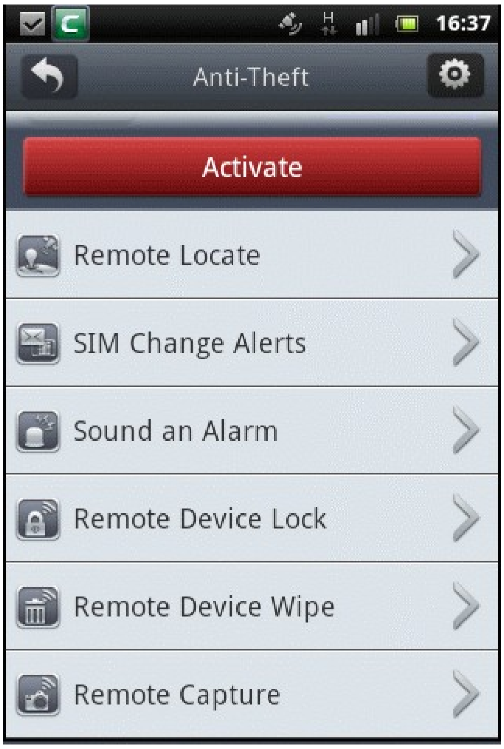
To activate Anti Theft

- Tap the CMS icon on your device.

The home page of CMS under Security tab will open.

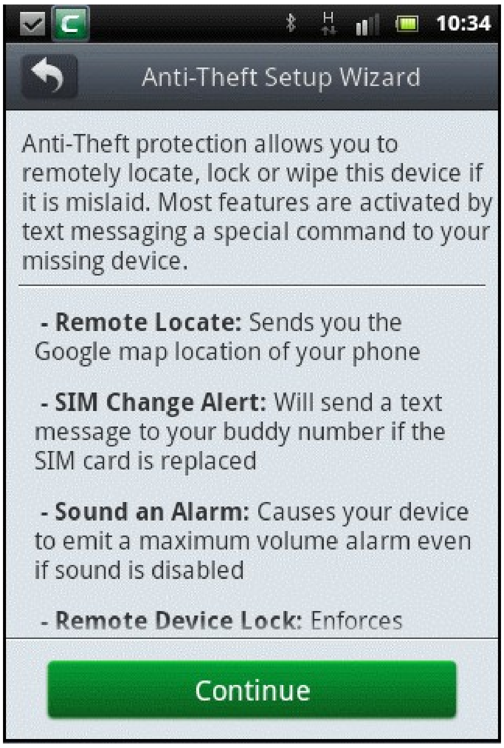
- Tap 'Anti Theft'.

The Anti Theft screen will be displayed.



- Tap 'Activate'.

The Anti Theft Setup Wizard will start.



Anti-Theft protection allows you to remotely locate, lock or wipe this device if it is mislaid. Most features are activated by text messaging a special command to your missing device.

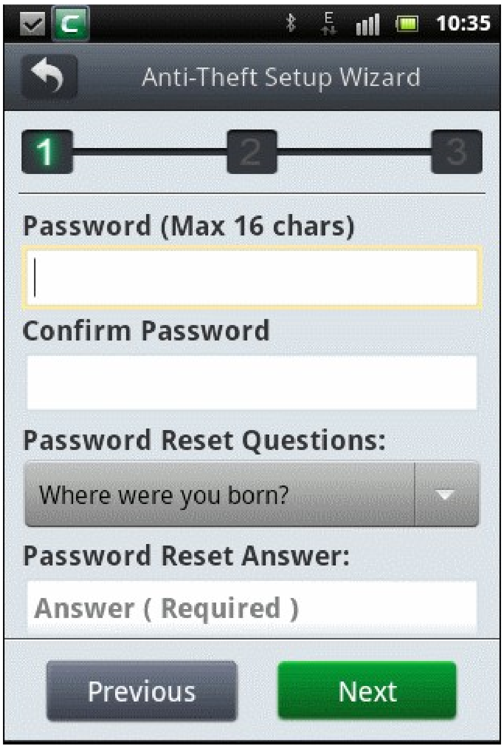
- **Remote Locate:** Sends you the Google map location of your phone

- **SIM Change Alert:** Will send a text message to your buddy number if the SIM card is replaced

- **Sound an Alarm:** Causes your device to emit a maximum volume alarm even if sound is disabled

- **Remote Device Lock:** Enforces

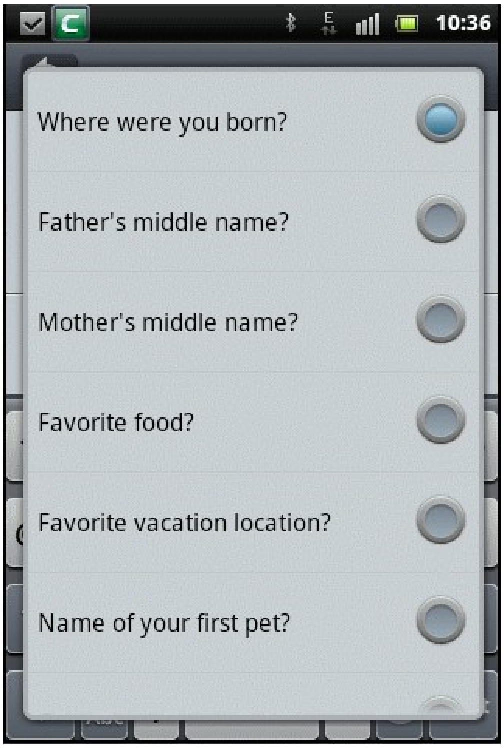
- Tap 'Continue'. You will be taken to Step 1 of the wizard.



Step 1:

You have to set a password and set password reset security question and answer in step 1.

- Enter a password for Anti Theft in the 'Password' field. This password is required for:
  - Sending remote commands to your device via SMS from another phone if your device is mislaid, lost or stolen
  - Unlock your device, if locked by remote command
  - Opening Anti Theft Settings, if you want to re-configure the settings
- Re-enter the password in the 'Confirm Password' field
- Select a Password Reset Question from the Password Reset Questions drop-down

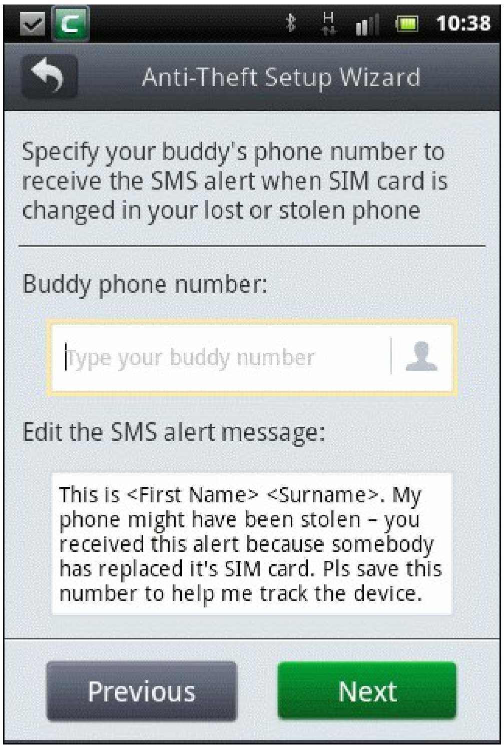


- ● Where were you born?
- ○ Father's middle name?
- ○ Mother's middle name?
- ○ Favorite food?
- ○ Favorite vacation location?
- ○ Name of your first pet?

- Enter the answer to Password Reset Security Question in the Password Reset Answer field. This answer is required for:
  - Resetting your password, if you have forgotten your password
  - Unlocking the device if locked by remote command
- Tap 'Next' You will be taken to Step 2 of the Wizard

Step2:

The next step is configuring your device to send an automated SMS to your friend's phone, if it is lost or stolen and someone changes its SIM card. Your friend can store the new number and you can send remote commands to locate the missing device, lock it or wipe off your private and confidential data in it, to prevent miss-handling.



Anti-Theft Setup Wizard

Specify your buddy's phone number to receive the SMS alert when SIM card is changed in your lost or stolen phone

Buddy phone number:

Type your buddy number

Edit the SMS alert message:

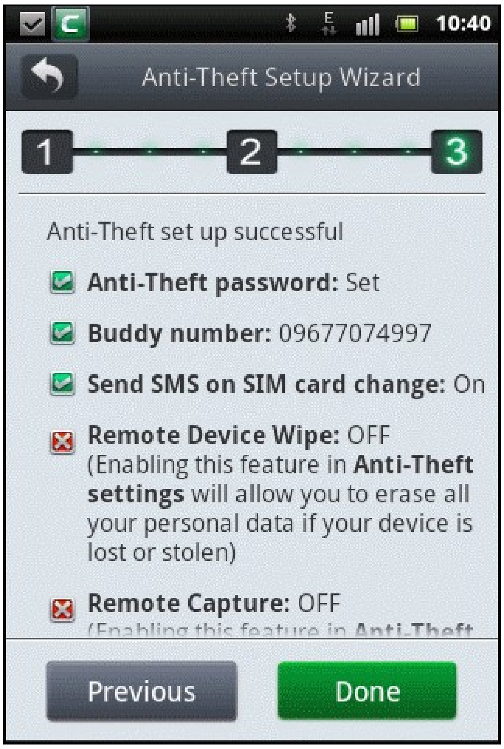
This is <First Name> <Surname>. My phone might have been stolen – you received this alert because somebody has replaced it's SIM card. Pls save this number to help me track the device.

- Enter the phone number of your friend to whom you wish the automated SMS to be sent from the new number if the SIM card is changed, in the 'Buddy phone number' field. You can even add a phone number from your contacts by tapping the contact icon in the right hand side end of the field and selecting the contact.
- Edit the message to be sent to your friend's phone from the new number in the 'Edit the SMS alert message' field.
- Tap 'Next'. You will be taken to Step 3.

Step3:

Step 3 allows you to confirm the choices you made in the previous steps and complete the wizard.

- To reconfigure the settings made in the previous steps, click 'Previous' and re-configure the settings



Anti-Theft set up successful

✓ **Anti-Theft password:** Set

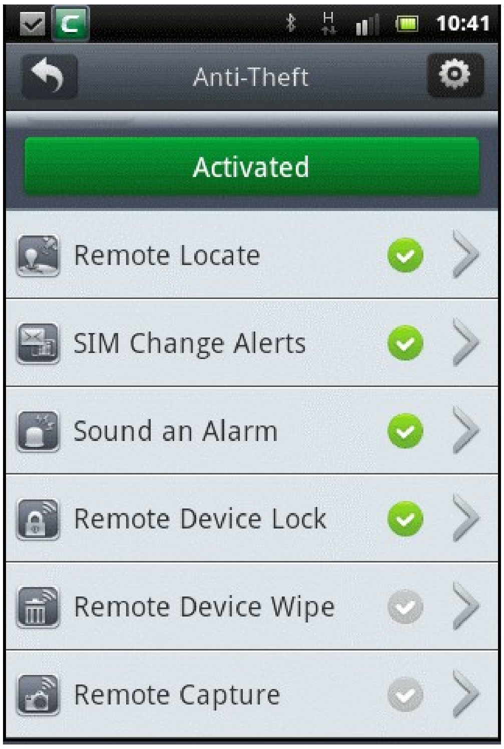
✓ **Buddy number:** 09677074997

✓ **Send SMS on SIM card change:** On

☒ **Remote Device Wipe:** OFF (Enabling this feature in **Anti-Theft settings** will allow you to erase all your personal data if your device is lost or stolen)

☒ **Remote Capture:** OFF (Enabling this feature in **Anti-Theft**

- To complete the wizard, tap 'Done'. The Anti Theft will be activated.



Remote Locate ✓

SIM Change Alerts ✓

Sound an Alarm ✓

Remote Device Lock ✓

Remote Device Wipe

Remote Capture

Important Note: Upon activation of Anti Theft, all the Anti Theft features will be enabled except Remote Device Wipe and Remote Capture. You can manually enable these features through Anti Theft Settings. Refer to **Configuring Anti Theft Settings** for more details.

To make your device to sound an alarm

- Send an SMS with the following text message to your device from another phone.

  alarm#[your Anti Theft password]

Note: Replace [your Anti Theft password] with the password that you specified in Step 1 during Anti Theft activation correctly

Upon receiving the SMS your device will emit a loud alarm at full volume, even if it is in silent mode. You will also get a confirmation text message to the device from which the alarm was sent. Your device will also be locked. Once you get the device back, you can unlock it by entering your Anti Theft password or the answer for your password reset security question.

If the device is stolen and somebody has changed its SIM card, the automated SIM card change alert SMS will be sent to your friend's phone registered as Buddy number in the setup wizard. Now you can send the SMS to this new number to make the device sound an alarm.

To get the location of your device

If your device is mislaid, lost or stolen, you can get the location of your device with Google map location by sending a remote command.

- Send an SMS with the following text message to your device from another phone.

  locate#[your Anti Theft password]

Note: Replace [your Anti Theft password] with the password that you specified in Step 1 during Anti Theft activation correctly

You will receive a reply SMS in the same phone with the location and a link to Google Maps, showing the location of your device in Google Maps.

If the device is stolen and somebody has changed its SIM card, the automated SIM card change alert SMS will be sent to your friend's phone registered as Buddy number in the setup wizard. Now you can send the SMS to this new number to make the device send its location.

To remotely lock your device

If your device is mislaid, lost or stolen, you can lock the device by sending a remote command, to prevent it being miss-handled. Once you get the device back, you can unlock it by entering the Anti Theft password or the answer for the password reset question.

- Send an SMS with the following text message to your device from another phone.

  lock#[your Anti Theft password]

Note: Replace [your Anti Theft password] with the password that you specified in Step 1 during Anti Theft activation correctly

If the device is stolen and somebody has changed its SIM card, the automated SIM card change alert SMS will be sent to your friend's phone registered as Buddy number in the setup wizard. Now you can send the SMS to this new number to lock the device remotely.

Your device will be locked and once you get back the device, you can unlock it by entering your Anti Theft password. If you have forgotten the password, you can unlock it by entering the answer to your password reset question. Tap the 'Unlock by answering password reset security question link', enter the answer and tap 'OK'.

To remotely wipe all your confidential data from your device

You can remotely erase all the confidential data including stored messages, contacts, call history, browser bookmarks and all the files stored in your SD card including pictures, music, video etc. The Remote Wipe feature is not activated by default upon activating Anti Theft.

Important Note: The Remote Wipe feature is not enabled by default on activating Anti Theft. You need to manually enable the feature through Anti Theft Settings. Refer to **Configuring Anti Theft Settings** for more details.

- Send an SMS with the following text message to your device from another phone.

  wipe#[your Anti Theft password]

Note: Replace [your Anti Theft password] with the password that you specified in Step 1 during Anti Theft activation correctly

If the device is stolen and somebody has changed its SIM card, the automated SIM card change alert SMS will be sent to your friend's phone registered as Buddy number in the setup wizard. Now you can send the SMS to this new number to wipe the data in the device remotely.

All the confidential data in your device will be erased.

To remotely take a picture from your device

The Remote Capture feature allows you to remotely take photograph from your missing or stolen device and receive it at your email, in order to identify the possessor of your device. On sending this remote command, your device will alert the possessor as if a message has been received, in order to lure him/her to look at the screen. Once the possessor taps the 'Read' button to view the message, the front camera in your device will be activated to take a photograph of the possessor. If your device does not have a front camera, the photograph will be taken from the back camera. The picked-up photograph will immediately be sent to your email address registered in Anti Theft Settings.

Important Note:The Remote Capture feature is not enabled by default on activating Anti Theft. You need to manually enable the feature through Anti Theft Settings. Refer to **Configuring Anti Theft Settings** for more details.

- Send an SMS with the following text message to your device from another phone.

  takephoto#[your Anti Theft password]

Note: Replace [your Anti Theft password] with the password that you specified in Step 1 during Anti Theft activation correctly

If the device is stolen and somebody has changed its SIM card, the automated SIM card change alert SMS will be sent to your friend's phone registered as Buddy number in the setup wizard. Now you can send the SMS to this new number to take a picture of the possessor.

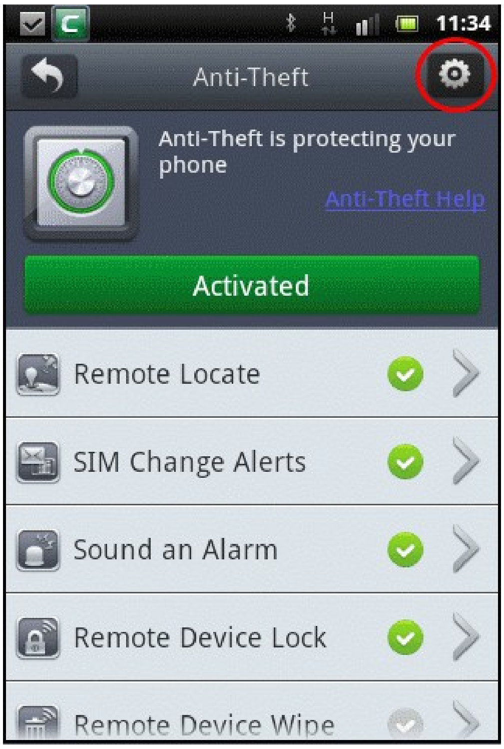
You will receive an email containing the photograph picked up from your device.

To configure Anti Theft Settings

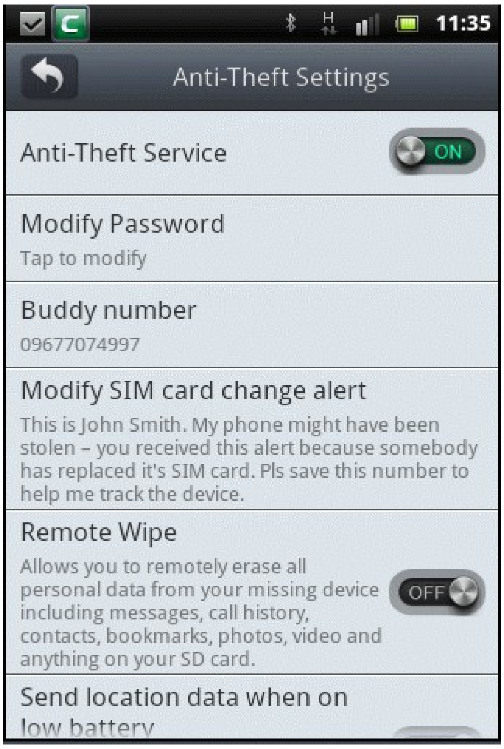
The Anti Theft Settings screen allows you to:

- **Enable/disable Anti Theft**
- **Change your Anti Theft password**
- **Re-configure SIM card change alert settings**
- **Enable/disable the 'Remote Wipe' feature**
- **Automatically receive an email when your battery is running low**
- **Configure Remote Capture feature**
- **Change your email settings**

To open the Settings screen, tap Settings icon at the top right of the Anti Theft screen.



The Settings screen will open.



Anti-Theft Service: ON

Modify Password
Tap to modify

Buddy number
09677074997

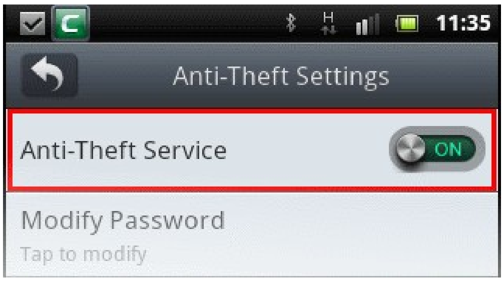
Modify SIM card change alert
This is John Smith. My phone might have been stolen – you received this alert because somebody has replaced it's SIM card. Pls save this number to help me track the device.

Remote Wipe: OFF
Allows you to remotely erase all personal data from your missing device including messages, call history, contacts, bookmarks, photos, video and anything on your SD card.

Send location data when on low battery

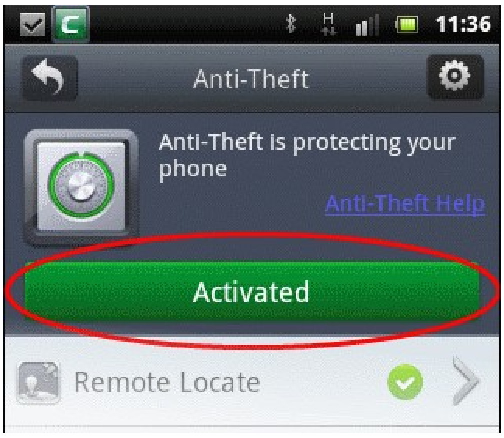
Enabling / Disabling Anti Theft

- To enable or disable the Anti Theft feature, tap anywhere on the 'Anti-theft service' bar to toggle between 'ON' and 'OFF' status.

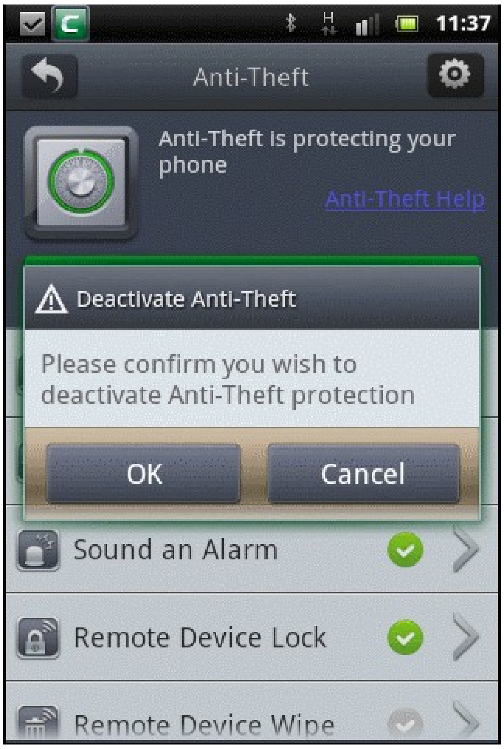


OR

- Tap on the Activated button in the Anti Theft screen to disable the anti theft feature...

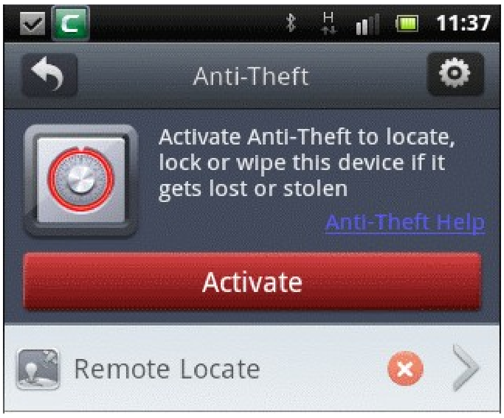


...and confirm in the Deactivate Anti-Theft dialog.



Please confirm you wish to deactivate Anti-Theft protection

The green color 'Activated' button in the Anti Theft will now be red color 'Activate' button indicating Anti Theft feature's disabled status.

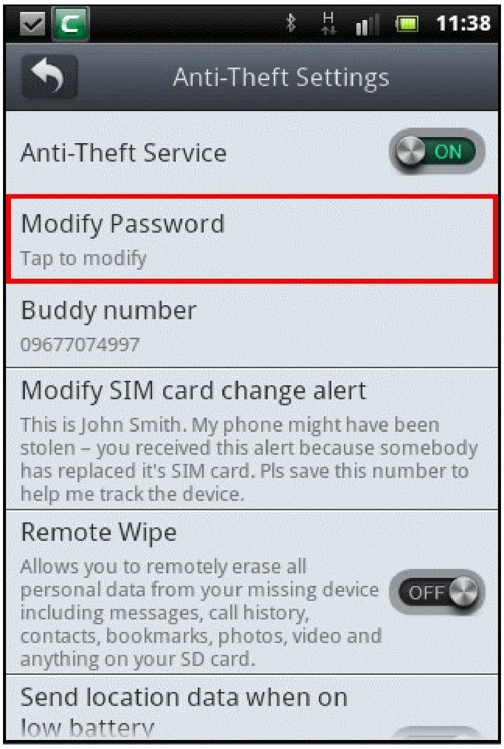


11:37
Anti-Theft
Activate Anti-Theft to locate, lock or wipe this device if it gets lost or stolen
Anti-Theft Help
Activate
Remote Locate

- Tap on the 'Activate' button to enable the feature again.

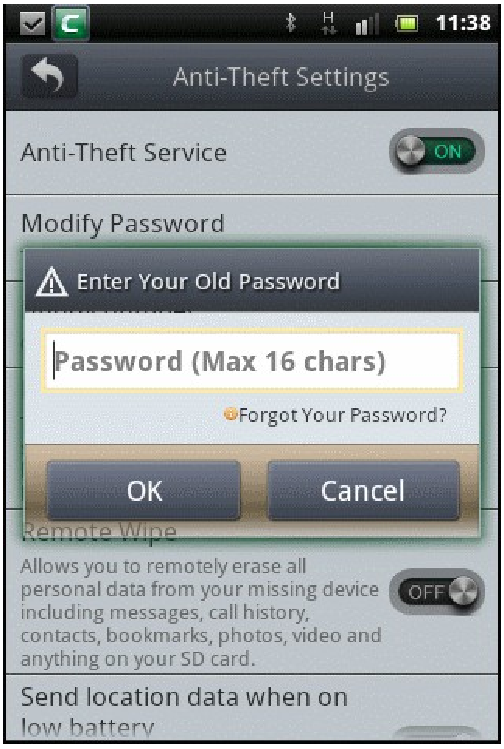
Changing your Anti Theft Password

- Tap the Modify Password bar.



11:38
Anti-Theft Settings
Anti-Theft Service
ON
Modify Password
Tap to modify
Buddy number
09677074997
Modify SIM card change alert
This is John Smith. My phone might have been stolen – you received this alert because somebody has replaced it's SIM card. Pls save this number to help me track the device.
Remote Wipe
Allows you to remotely erase all personal data from your missing device including messages, call history, contacts, bookmarks, photos, video and anything on your SD card.
OFF
Send location data when on low battery

- Type your existing password in the Enter Your Old Password dialog and tap OK.



Anti-Theft Settings

Anti-Theft Service ON

Modify Password

Enter Your Old Password

Password (Max 16 chars)

Forgot Your Password?

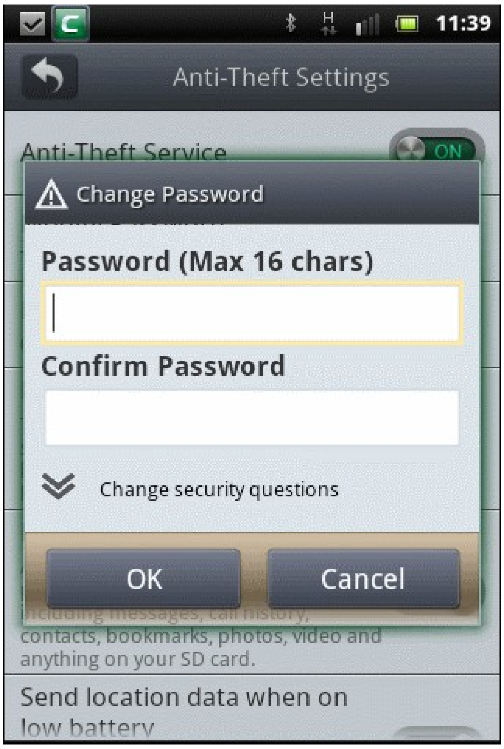
OK Cancel

Remote Wipe

Allows you to remotely erase all personal data from your missing device including messages, call history, contacts, bookmarks, photos, video and anything on your SD card. OFF

Send location data when on low battery

- Type your new password in the Password field and re-enter the password in the Confirm Password field.



Anti-Theft Settings

Anti-Theft Service ON

Change Password

Password (Max 16 chars)

Confirm Password

Change security questions

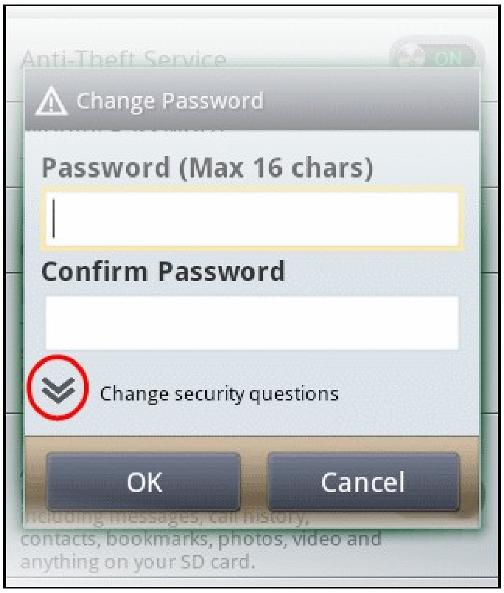
OK Cancel

contacts, bookmarks, photos, video and anything on your SD card.

Send location data when on low battery

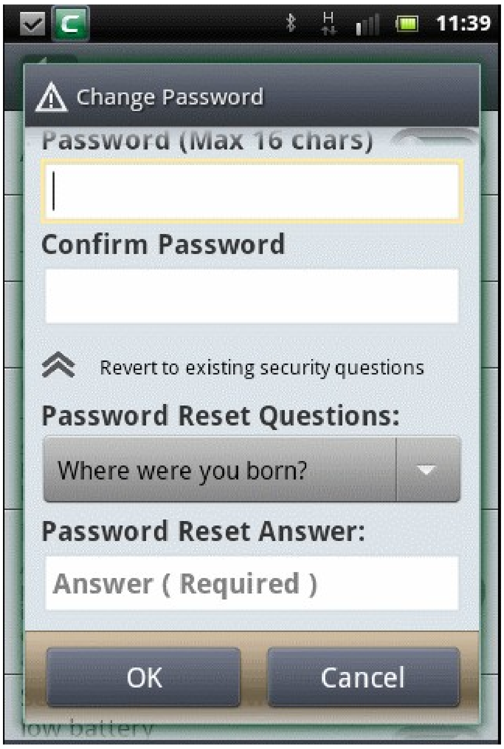
- Tap 'OK'.

If you want to change the security question and password, tap on the double down arrow in the 'Change Password' dialog.



Anti-Theft Service
ON
Change Password
Password (Max 16 chars)
Confirm Password
Change security questions
OK
Cancel
including messages, call history,
contacts, bookmarks, photos, video and
anything on your SD card.

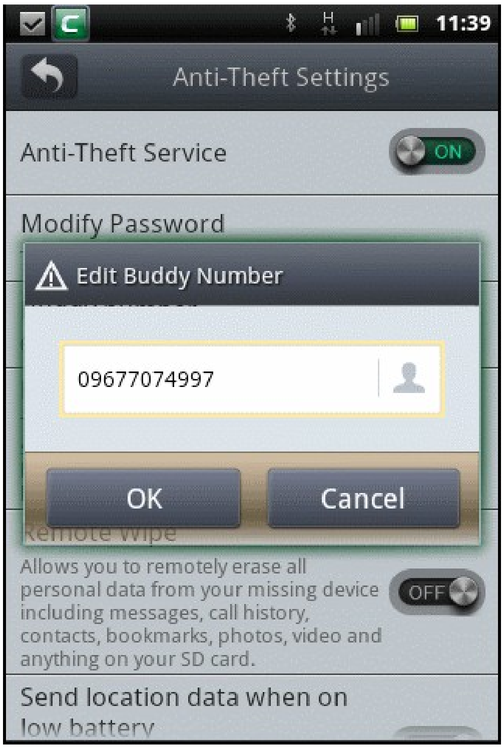
- Select the new Password Reset Questions from the drop-down button and enter the new password reset answer.



- Tap 'OK' when done.

Re-configuring SIM card alert settings

- To change your friend's phone number to whom the alert message has to be sent, tap on the 'Buddy number' band in the Anti Theft settings screen.

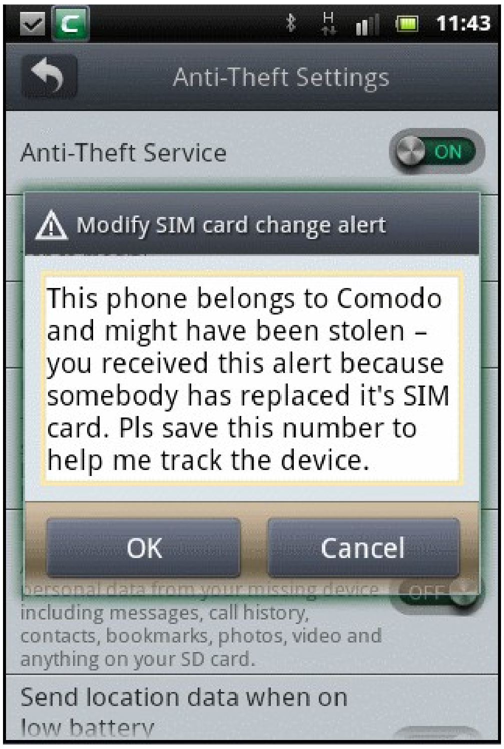


09677074997

Allows you to remotely erase all personal data from your missing device including messages, call history, contacts, bookmarks, photos, video and anything on your SD card.

- Change the phone number and tap OK.

- To alter the SIM card change alert message sent as SMS to your friend's phone, tap 'Modify SIM card change Alert' band in the Anti Theft settings screen.


11:43
Anti-Theft Settings
Anti-Theft Service
ON
Modify SIM card change alert
OK
Cancel
OFF
Send location data when on low battery

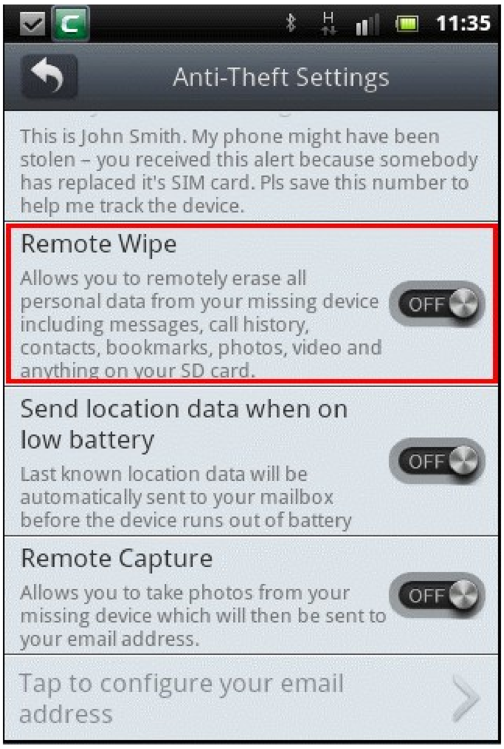
This phone belongs to Comodo and might have been stolen – you received this alert because somebody has replaced it's SIM card. Pls save this number to help me track the device.

personal data from your missing device including messages, call history, contacts, bookmarks, photos, video and anything on your SD card.

- Tap in the text field, edit the message and tap OK.

Enabling / Disabling Remote Wipe

- To enable / disable Remote Wipe feature, tap anywhere on the bar to toggle between 'ON' and 'OFF' states.



11:35

Anti-Theft Settings

This is John Smith. My phone might have been stolen – you received this alert because somebody has replaced it's SIM card. Pls save this number to help me track the device.

Remote Wipe
Allows you to remotely erase all personal data from your missing device including messages, call history, contacts, bookmarks, photos, video and anything on your SD card. OFF

Send location data when on low battery
Last known location data will be automatically sent to your mailbox before the device runs out of battery OFF

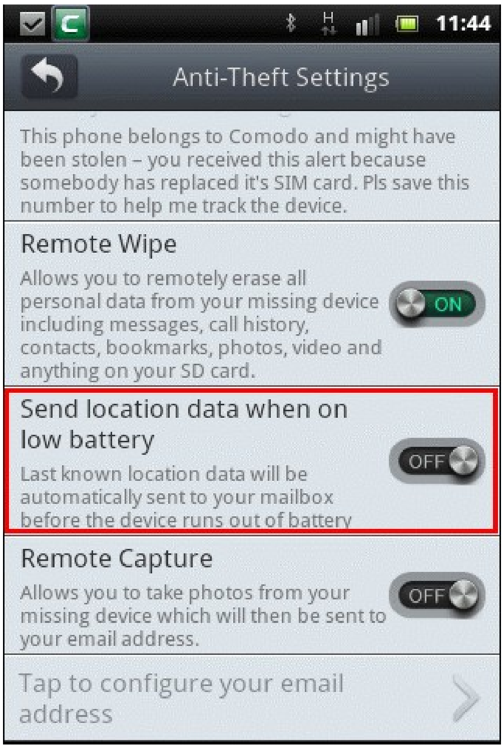
Remote Capture
Allows you to take photos from your missing device which will then be sent to your email address. OFF

Tap to configure your email address

Automatically Receive An Email When Your Battery Is Running Low

If enabled, you will automatically receive an email when your battery is running low. This email contains the last known location of the device which can be helpful if the device has been lost or stolen.

- To enable 'Send location data when on low battery' feature, tap anywhere on the bar to toggle between 'ON' and 'OFF' states.



11:44

Anti-Theft Settings

This phone belongs to Comodo and might have been stolen – you received this alert because somebody has replaced it's SIM card. Pls save this number to help me track the device.

Remote Wipe
Allows you to remotely erase all personal data from your missing device including messages, call history, contacts, bookmarks, photos, video and anything on your SD card. ON

Send location data when on low battery
Last known location data will be automatically sent to your mailbox before the device runs out of battery OFF

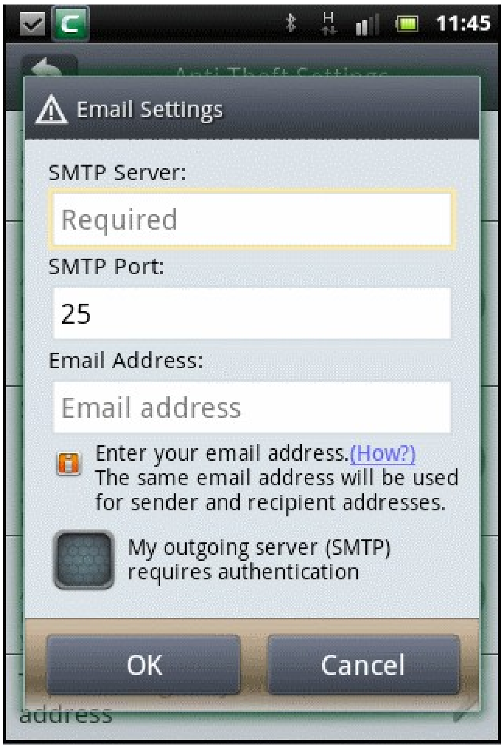
Remote Capture
Allows you to take photos from your missing device which will then be sent to your email address. OFF

Tap to configure your email address

On enabling the feature, an email settings screen will appear to configure the email accounts for sending the photographs taken on successful execution of Send location data when on low battery command.

Note: If the email settings has been configured in **Configuring Remote Capture feature** or **Configuring Email Settings**, then

the email settings screen will not appear.



Email Settings

SMTP Server:

Required

SMTP Port:

25

Email Address:

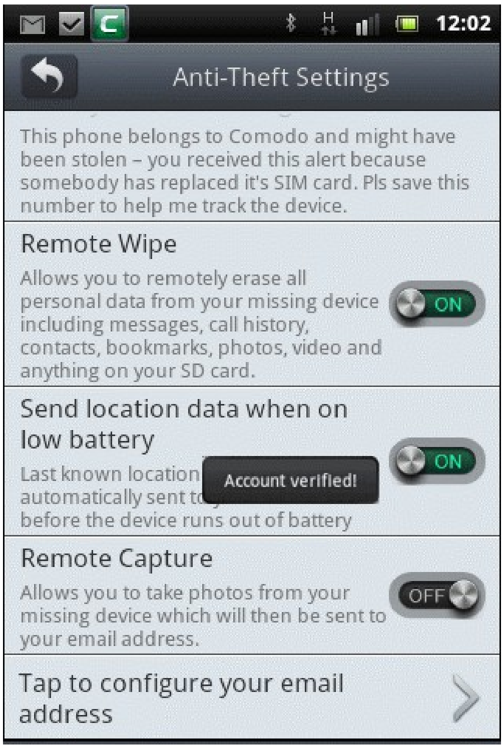
Email address

Enter your email address.(How?)
The same email address will be used for sender and recipient addresses.

My outgoing server (SMTP) requires authentication

- Enter the required data in the fields. For more details on the settings to the **table** in the **Configuring Remote Capture feature** section.

- Click OK to save your settings. CMS will verify your account settings and send a confirmation mail to your mail account.



Anti-Theft Settings

This phone belongs to Comodo and might have been stolen – you received this alert because somebody has replaced it's SIM card. Pls save this number to help me track the device.

Remote Wipe
Allows you to remotely erase all personal data from your missing device including messages, call history, contacts, bookmarks, photos, video and anything on your SD card. ON

Send location data when on low battery
Last known location automatically sent t... before the device runs out of battery ON

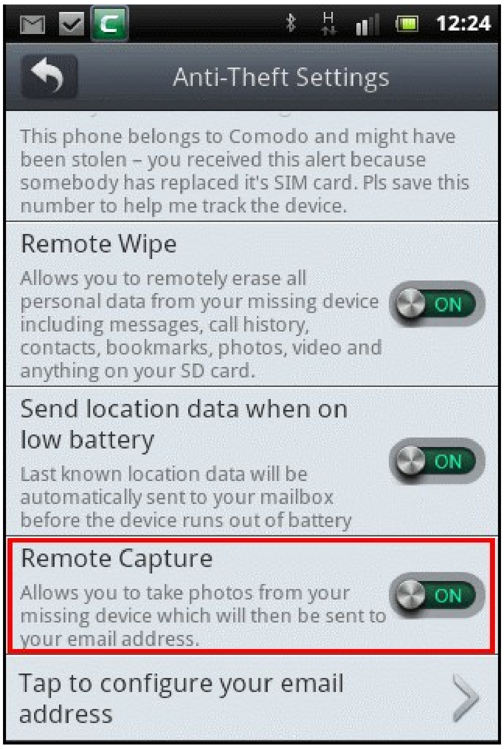
Account verified!

Remote Capture
Allows you to take photos from your missing device which will then be sent to your email address. OFF

Tap to configure your email address

Configuring Remote Capture Feature

- To enable the Remote Capture feature, tap anywhere in the 'Remote Capture' bar and ensure the slider switch shows 'ON'.



Anti-Theft Settings

This phone belongs to Comodo and might have been stolen – you received this alert because somebody has replaced it's SIM card. Pls save this number to help me track the device.

Remote Wipe
Allows you to remotely erase all personal data from your missing device including messages, call history, contacts, bookmarks, photos, video and anything on your SD card. ON

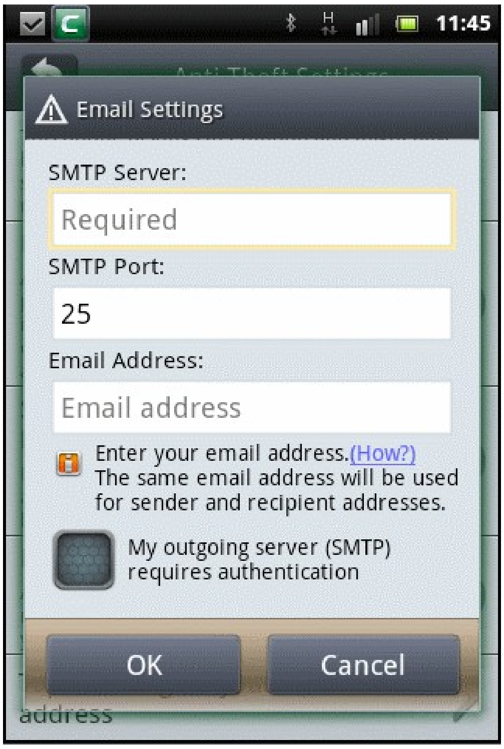
Send location data when on low battery
Last known location data will be automatically sent to your mailbox before the device runs out of battery ON

Remote Capture
Allows you to take photos from your missing device which will then be sent to your email address. ON

Tap to configure your email address

On enabling the feature, an email settings screen will appear to configure the email accounts for sending the photographs taken on successful execution of Remote Capture command.

Note: If the email settings has been configured to **receive an email when your battery is running low** or in **Configuring Email Settings**, then the email settings screen will not appear.



Email Settings

SMTP Server: Required

SMTP Port: 25

Email Address: Email address

Enter your email address.(How?) The same email address will be used for sender and recipient addresses.

My outgoing server (SMTP) requires authentication

OK Cancel

- Enter the SMTP server name of your email service provider, SMTP Port and your email address in the respective fields. The same email address will be used for both sender and recipient address for sending the photograph taken by your device.
- If your SMTP server requires user authentication for sending mails, select the check box 'My outgoing server (SMTP) requires authentication' and enter your username and email password in the respective fields.

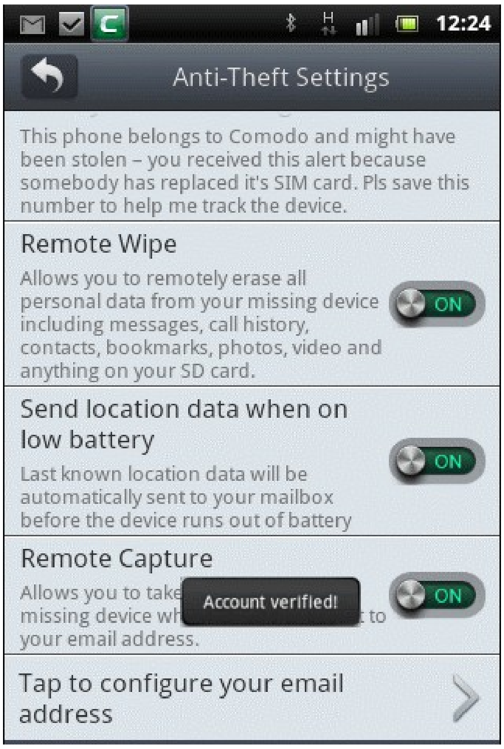
Tip: In most of the cases, your username would be the string that comes before @ in your email address. If your email address is yourname@example.com, your username is 'yourname'. It may differ depending on the configuration of the mail server.

The table below provides the SMTP server and port for popular mail account types:

Mail Account	SMTP Server	SMTP Port	Requires SMTP Authentication?
Hotmail	smtp.live.com	25	Yes
Gmail	smtp.gmail.com	587	Yes
Yahoo	smtp.mail.yahoo.com	25	Yes
MSN	smtp.email.msn.com	25	Yes
163	smtp.163.com	25	Yes
QQ	smtp.qq.com	25	Yes

If your mail account is not listed, then you will need to request this information from your ISP/email service provider. You can get the SMTP address/port by sending an email request their support department. Alternatively, if you visit your ISP's website and type 'SMTP Address' in their search box it will often lead right to the info you need.

- Click OK to save your settings. CMS will verify your account settings and send a confirmation mail to your mail account.



This phone belongs to Comodo and might have been stolen – you received this alert because somebody has replaced it's SIM card. Pls save this number to help me track the device.

Remote Wipe
Allows you to remotely erase all personal data from your missing device including messages, call history, contacts, bookmarks, photos, video and anything on your SD card. ON

Send location data when on low battery
Last known location data will be automatically sent to your mailbox before the device runs out of battery ON

Remote Capture
Allows you to take missing device wh to your email address. ON

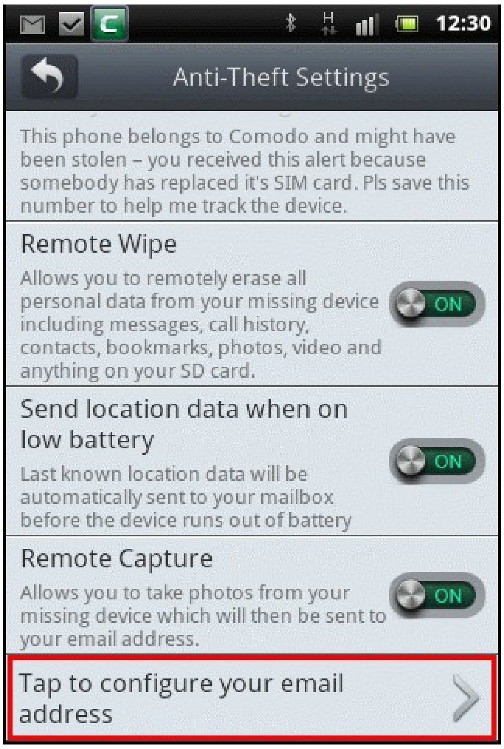
Account verified!

Tap to configure your email address

Configuring your Email Address

If you have not configured your email address in **Automatically Receive An Email When Your Battery Is Running Low** or **Configuring Remote Capture Feature**, you can do so by tapping the 'Tap to configure your email address' bar. If the email has been configured, you edit the details in this screen.

- To configure or edit email settings, tap anywhere on the 'Tap to configure your email address' bar.



This phone belongs to Comodo and might have been stolen – you received this alert because somebody has replaced it's SIM card. Pls save this number to help me track the device.

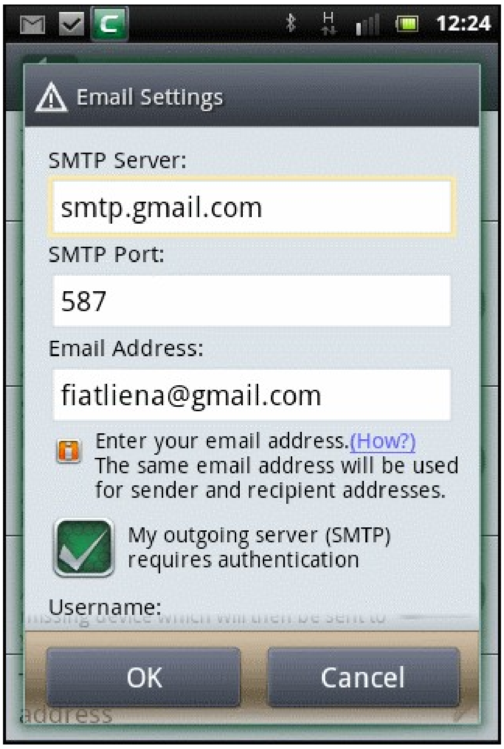
Remote Wipe
Allows you to remotely erase all personal data from your missing device including messages, call history, contacts, bookmarks, photos, video and anything on your SD card. ON

Send location data when on low battery
Last known location data will be automatically sent to your mailbox before the device runs out of battery ON

Remote Capture
Allows you to take photos from your missing device which will then be sent to your email address. ON

Tap to configure your email address

The Email Settings screen will be displayed. If it has been configured the details will be displayed and you can edit it if required.



SMTP Server: smtp.gmail.com

SMTP Port: 587

Email Address: fiatliena@gmail.com

Enter your email address.(How?) The same email address will be used for sender and recipient addresses.

☑ My outgoing server (SMTP) requires authentication

Username:

If the settings has not been configured, enter the details in the fields. For more details on the settings refer to the **table** in the **Configuring Remote Capture feature** section.

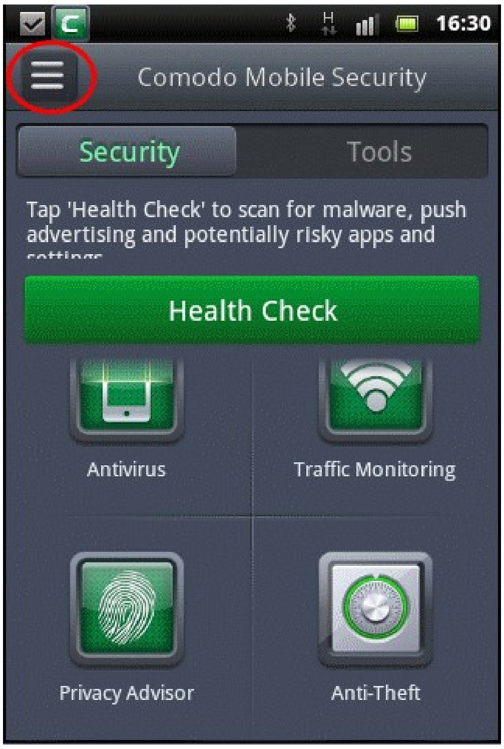
13. CMS Settings and More

In the 'More List' screen you can configure settings such as notifications on blocked calls/SMS, enabling security service and enabling automatically check the updates using non-wifi internet. You can also update the virus database as well as CMS suite in this screen manually. Leave a feedback and find out about the CMS version in this screen.

- **How to configure CMS settings**
- **How to enable / disable security service**
- **How to leave feedback**
- **How to know the CMS and virus database versions in your device**
- **How to update CMS and virus database**

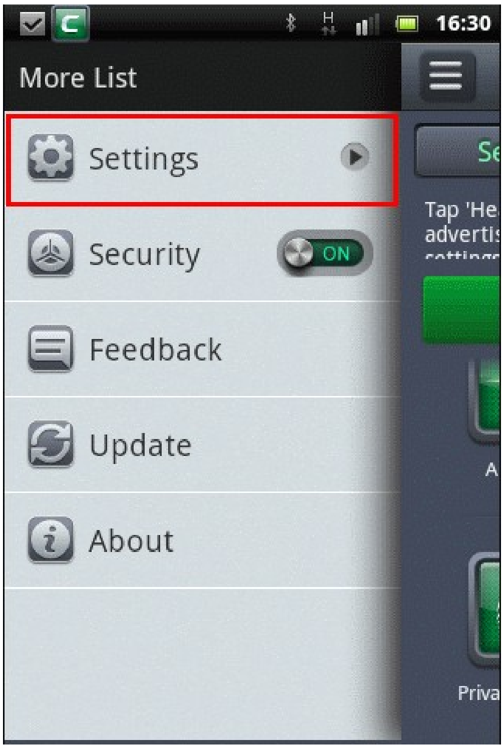
How to configure CMS settings

- Tap the CMS icon on your device.
- Tap the 'Menu' button located at the top left of the screen.



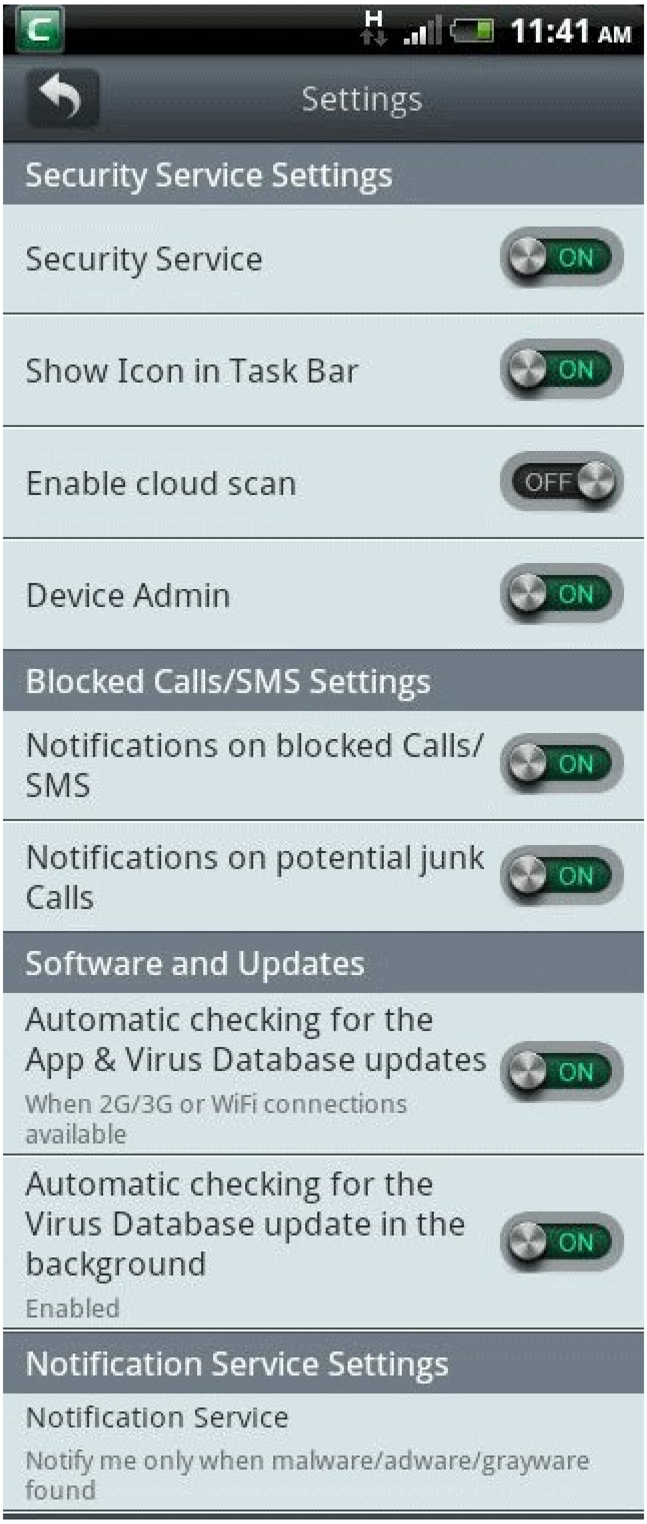
Tap 'Health Check' to scan for malware, push advertising and potentially risky apps and settings

The 'More List' screen will be displayed.



- Tap anywhere on the Settings bar.

The 'Settings' screen will be displayed.



11:41 AM

Settings

Security Service Settings

Security Service ON

Show Icon in Task Bar ON

Enable cloud scan OFF

Device Admin ON

Blocked Calls/SMS Settings

Notifications on blocked Calls/SMS ON

Notifications on potential junk Calls ON

Software and Updates

Automatic checking for the App & Virus Database updates ON
When 2G/3G or WiFi connections available

Automatic checking for the Virus Database update in the background ON
Enabled

Notification Service Settings

Notification Service
Notify me only when malware/adware/grayware found

- Tap anywhere on a setting bar to toggle an option between 'On' and 'Off' states.

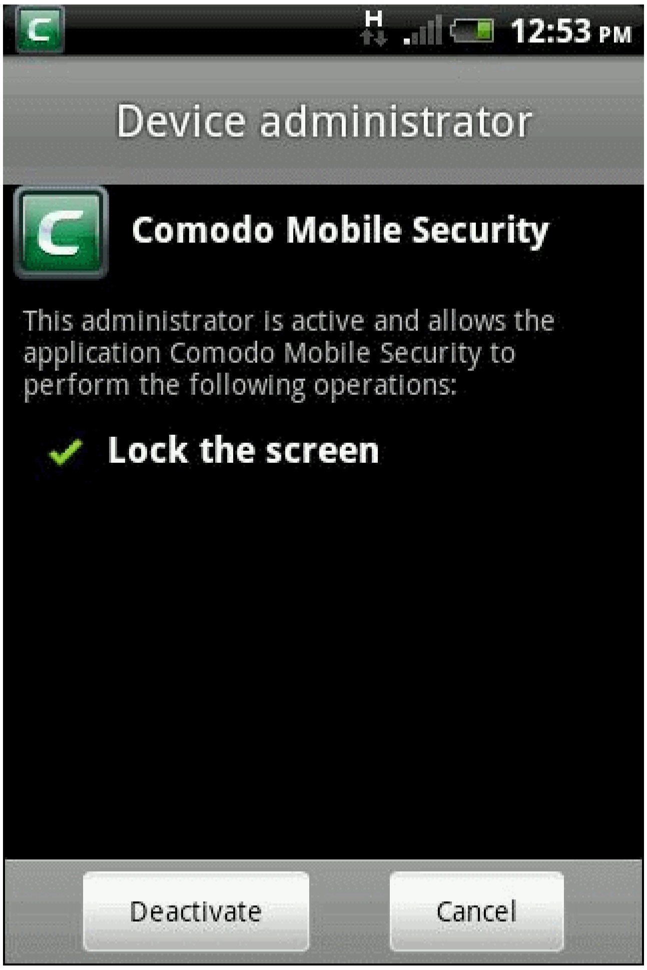
The following options are available in the settings screen:

Security Service Settings

- **Security Service** - Enables or disables the full CMS protection for your device.
- **Show Icon on Task Bar** - Displays or hides the CMS icon on the task bar in your device.
- **Enable cloud scan** - If the device is connected to the Internet via WiFi, then the hash values of .apk files will be sent to Comodo's File Lookup Service (FLS) one by one for detailed analysis of the application. This is applicable to only .apk files and not other files in your device. If there is no WiFi connection, the results will be displayed according to the

local scan.

- **Device Admin** - CMS requires administrative privileges on your device to activate its security policies and prevent it being uninstalled by any third-party application.
  - Tap anywhere in the Device Admin tap to activate/deactivate the policies.



Device administrator

Comodo Mobile Security

This administrator is active and allows the application Comodo Mobile Security to perform the following operations:

✓ Lock the screen

Blocked Calls/SMS Settings

- **Notifications on blocked Calls / SMS** - Alerts you when you receive calls or SMS messages from a blacklisted number if this setting is enabled.
- **Notifications on potential junk Calls** - Alerts you when you receive potential junk calls.

Software and Updates

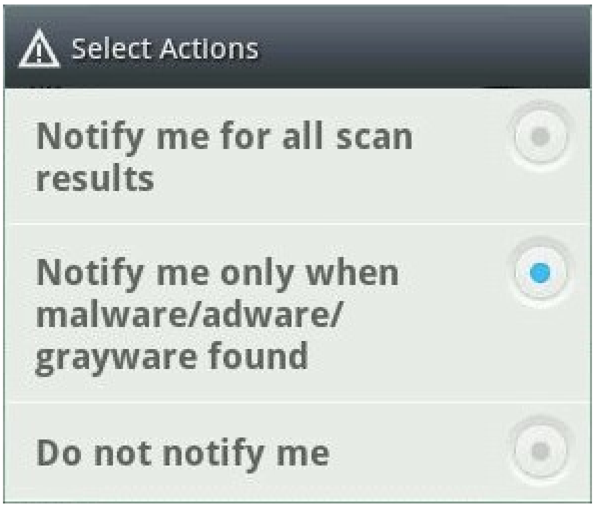
- **Automatic checking for App & Virus Database updates** - Enables or disables to check for updates when using non-wifi internet. If the setting is on, CMS will check for udpates (both databases and CMS version) regardless of whether you are using wifi or non-wifi internet (such as 3G or GPRS). If the button is off, CMS will only check for updates when you are using wifi.
- **Automatic checking for the Virus Database update in the background** - Enables or disables automatic virus database updates. If the settings is on, CMS will update virus database automatically in 2G/3G network. If the button is off, CMS will only update when you are using wifi.

Notification Service Settings

CMS can generate alerts on real time, on-demand or scheduled Antivirus scans. You can configure the Antivirus scan events for which you wish to receive the alerts.

To configure the notification alerts

- Tap on the 'Notification Service' bar. The 'Select Actions' dialog will appear.



Select Actions

○ Notify me for all scan results

● Notify me only when malware/adware/grayware found

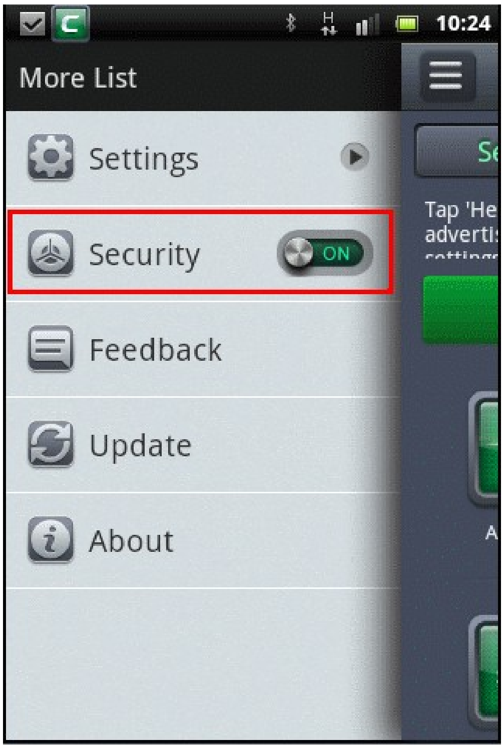
○ Do not notify me

- Choose the event for which you wish to be notified
    - **Notify me for all scan results** - The notification alert will be displayed in the notification area of your device on every scan irrespective of the results
    - **Notify me only when malware/adware/grayware found** - The notification alert will be displayed in the notification area only when malware is found on a scan
    - **Do not notify me** - The scan notification alert is disabled

How to enable / disable security service

- Tap the CMS icon on your device.
- Tap the 'Menu' button located at the top left of the screen.

In the 'More List' screen, tap the Security bar to toggle between 'ON' and 'OFF' state.



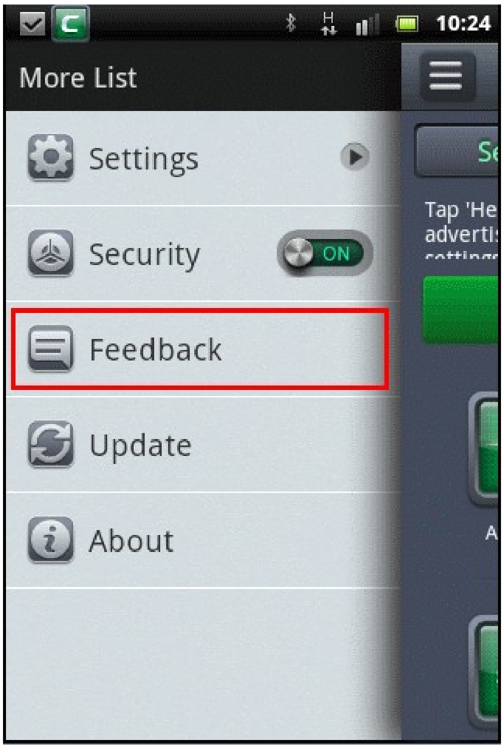
This is same as the '**Security Service**' in the '**Settings**' screen and is a shortcut to enable or disable the full CMS protection for your device.

How to leave feedback

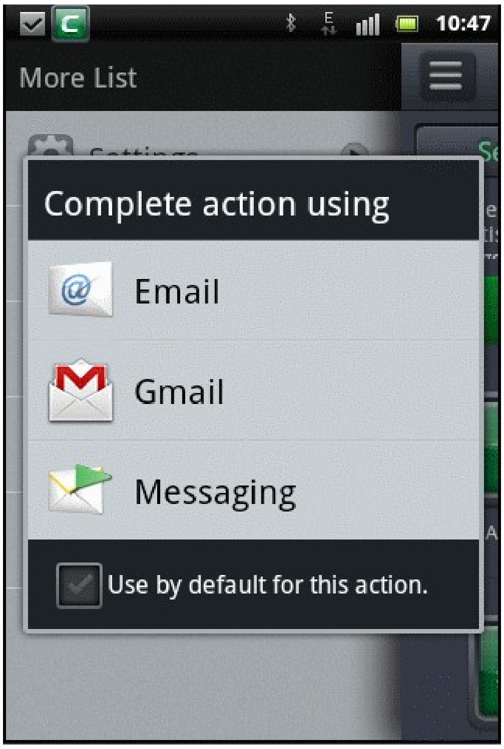
Comodo would like to have your feedback, comments and suggestions about the software. CMS allows you to provide feedback via email or as text message.

- Tap the CMS icon on your device.
- Tap the 'Menu' button located at the top left of the screen.

In the 'More List' screen, tap the Feed Back bar.



- Select the mode for providing feedback from the 'Complete action using' screen.

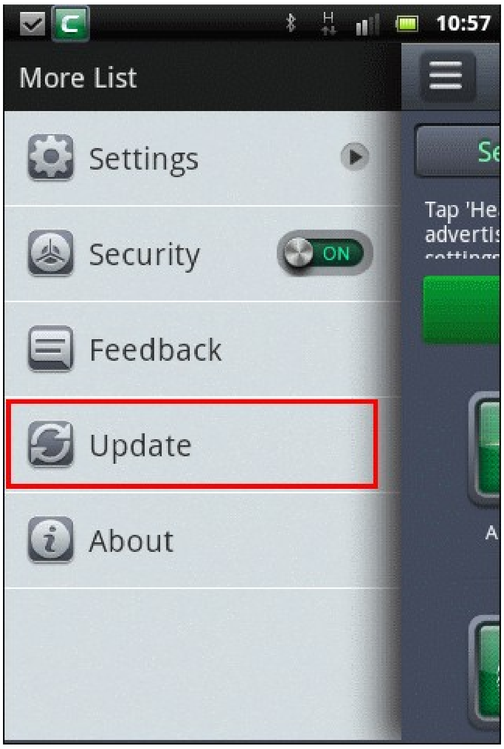


Your feedback and impression about the software is valuable to us.

How to update CMS and virus database

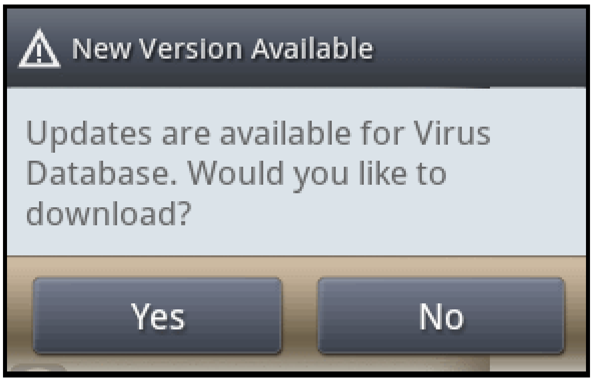
CMS allows you to check if the latest version of the software and the virus database is available.

- Tap the CMS icon on your device.
- Tap the 'Menu' button located at the top left of the screen.

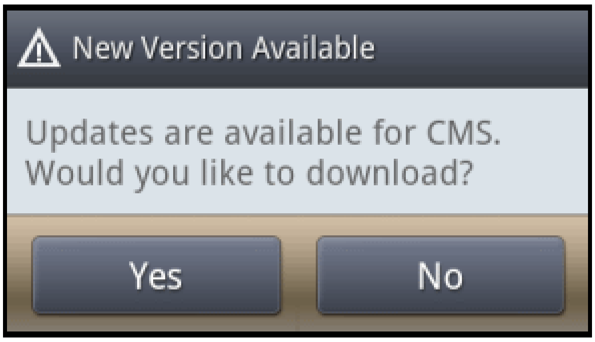


- Tap anywhere on the 'Update' bar.

CMS will check and if any new version of software and / or virus database is available, the New Version Available dialog will be displayed.


New Version Available

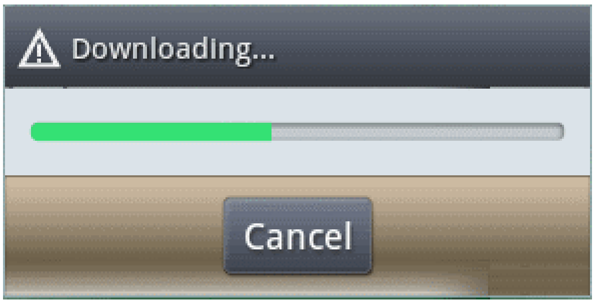
Updates are available for Virus Database. Would you like to download?


New Version Available

Updates are available for CMS. Would you like to download?

- Click 'Yes' to download the software or virus database.

The progress of the download will be displayed….

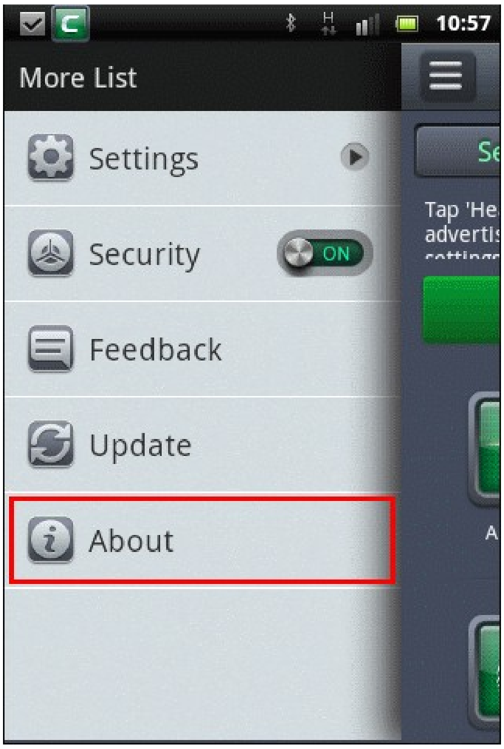

Downloading...

...and on successful completion, the successfully updated screen will be displayed.

If the current CMS and virus database versions in your device are the latest, then 'Software is up to date' and 'Database is up to date' screens will be displayed respectively.

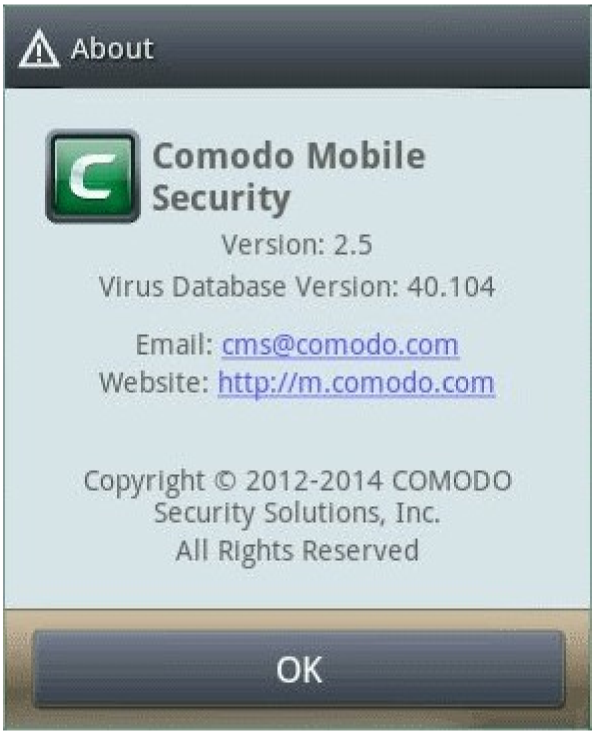
How to know the CMS and virus database versions in your device

- Tap the CMS icon on your device.
- Tap the 'Menu' button located at the top left of the screen.



- Tap anywhere on the 'About' bar.

The 'About' screen will be displayed.



Comodo Mobile Security

Version: 2.5

Virus Database Version: 40.104

Email: cms@comodo.com
Website: http://m.comodo.com

Copyright © 2012-2014 COMODO Security Solutions, Inc.
All Rights Reserved

The details of the CMS and virus database version in your device will be displayed in the screen. You can also send an email or visit our website by tapping the appropriate links.

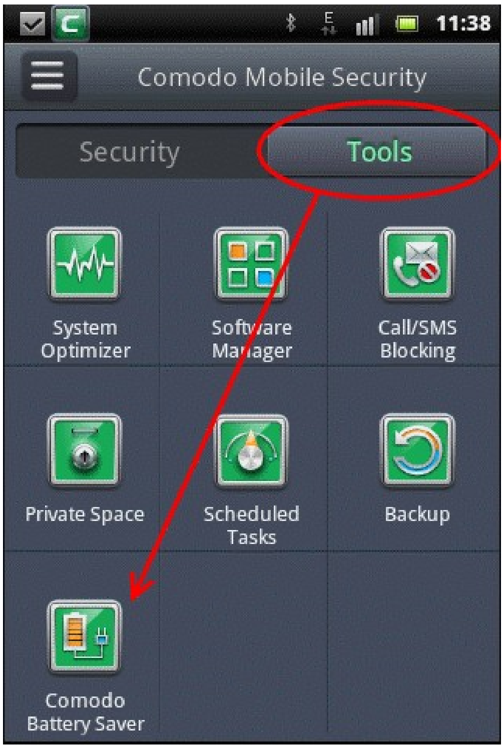
14. Comodo Battery Saver

Comodo Battery Saver (CBS) makes your Android device last a whole lot longer and slashes how often you need to put it on charge. The app lets you quickly switch between preset and user customized power saving modes while its intelligent optimization feature automatically applies energy saving tweaks as your battery moves towards exhaustion. CBS also lets you disable power-hungry applications with a single tap, generates alerts when the battery needs to be unplugged and gives you a detailed breakdown of exactly which applications are using the most power.

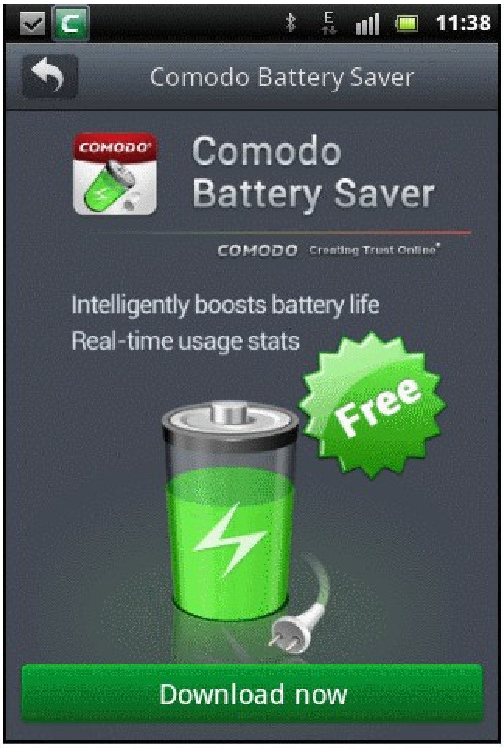
CBS can be launched from Comodo Mobile Security screen and for the first time the CBS app will be downloaded and installed in your device.

To launch Comodo Battery Saver from CMS

- Tap the CMS icon on your device.
- Tap 'Tool's tab located at the top or swipe to the left and tap 'Comodo Battery Saver'.



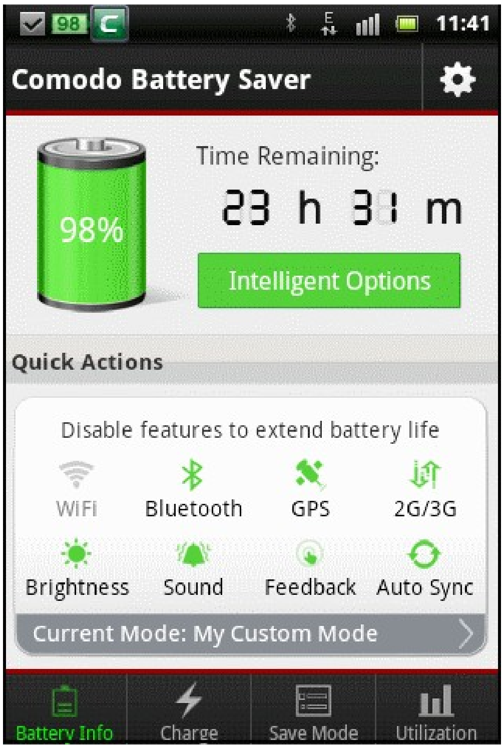
If CBS is not installed in your device, the download screen will be displayed.



- Download the application and install it in your device.

Next time you tap the CBS icon in the CMS screen, the application will be launched.

Note: CBS is a separate application and its icon will be available in your device after installation. CBS can also be launched by tapping the icon in your device.



For detailed explanation and help on Comodo Battery Saver, refer to our online guide at **http://help.comodo.com/product-174-Comodo-Battery-Saver.html**.

About Comodo

The Comodo companies are leading global providers of Security, Identity and Trust Assurance services on the Internet. Comodo CA offers a comprehensive array of PKI Digital Certificates and Management Services, Identity and Content Authentication (Two-Factor - Multi-Factor) software, and Network Vulnerability Scanning and PCI compliance solutions. In addition, with over 10,000,000 installations of its threat prevention products, Comodo Security Solutions maintains an extensive suite of endpoint security software and services for businesses and consumers.

Continual innovation, a core competence in PKI and a commitment to reversing the growth of Internet-crime distinguish the Comodo companies as vital players in the Internet's ongoing development. Comodo, with offices in the US, UK, China, India, Romania and the Ukraine, secures and authenticates the online transactions and communications for over 200,000 business customers and millions of consumers, providing the intelligent security, authentication and assurance services necessary for trust in on-line transactions.

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**.