eScan™

Mobile Security for Android

User Guide

24x7 FREE
Online Technical Support
support@escanav.com
https://forums.escanav.com

An ISO 27001 Certified Company

www.escanav.com

The software described in this guide is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Document Number: eANDROID/18/08/2021

Current Software Version: 7.X

Any technical documentation that is made available by MicroWorld is the copyrighted work of MicroWorld and is owned by MicroWorld.

NO WARRANTY: The technical documentation is being delivered to you AS-IS and MicroWorld makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user.

Documentation may include technical or other inaccuracies or typographical errors. MicroWorld reserves the right to make changes without prior notice. No part of this publication may be copied without the express written permission of MicroWorld.

Trademarks: The terms MicroWorld, MicroWorld Logo, eScan, eScan Logo, MWL, and MailScan are trademarks of MicroWorld.

Microsoft, MSN, Windows, and Windows Vista are trademarks of the Microsoft group of companies. All product names referenced herein are trademarks or registered trademarks of their respective companies. MicroWorld disclaims proprietary interest in the marks and names of others. Although MicroWorld makes every effort to ensure that this information is accurate, MicroWorld will not be liable for any errors or omission of facts contained herein. MicroWorld reserves the right to modify specifications cited in this document without prior notice.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of MicroWorld. Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Technical Support:	**support@escanav.com**
Sales	**: sales@escanav.com**
Forums	**: http://forums.escanav.com**
eScan Wiki	**: https://www.escanav.com/wiki**
Live Chat	**: https://www.escanav.com/english/livechat.asp**
Printed By	**: MicroWorld**
Date	**: August 2021**

Table of Contents

Introduction

eScan Mobile Security is a high-end Android security solution with a well-designed user interface for securing Android devices. eScan Mobile Security protects your Android devices against malicious activity, as well as allow users to track the location of your device and raise an alarm if it is lost or stolen. The parental control feature adds an extra layer of protection by restricting undesired websites.

User can identify the category of website embedded in QR code by using QR/Barcode scanner feature to prevent users to visit malicious websites. The call filter feature allows user to filter incoming calls based on backlist and whitelist created. User can take a backup of your contacts to your cloud or internal storage and restore it as per requirement. App usage feature gives detailed information regarding each application such as total data utilize, date and time, etc.

If your device is lost or stolen, all you must do is send an SMS command from any device to your lost or stolen device to lock, locate, wipe data, or scream (raise a loud alarm). If the unlock attempt fails more than twice, the lock watch feature of eScan Mobile Security will capture a picture using front camera. The captured image will be forwarded to the email address you specify and also stored in the lock watch gallery. Device booster feature allows you to boost your device, it will clean junk files.

User can use locate feature to find the device exact location, in case of lost or stolen. If the SIM card is replaced, the SIM watch feature will alert you. The scream feature will allow the device to a raise loud alarm, which can only be silenced by entering the correct secret code in case of device lost or stolen. User can use the app lock feature to lock applications on your device, if you don't want others to access them. eScan Mobile Security widget allows you quick access to multiple options.

To install eScan Mobile Security, ensure that you comply with the following requirements:

Pre-requisite

System Requirement

Pre-Requisition for Installation of eScan Mobile Android Security

Please check the pre-requisites before installing eScan Mobile Security on your device.

First Time Installation

- Ensure that you have Administrator Rights on the device where you wish to install eScan Mobile Android Security.
- Ensure that the System Requirements for installing eScan are met.
- Please uninstall all other similar applications like Antivirus, Anti-Spyware or Anti- Malware to avoid application conflict.
- Please ensure that sufficient space is available on your device for installation. Please check System Requirements for more details.
- We recommend that your device is connected to internet at the time of installation. This will ensure that eScan is updated with the entire recent virus signature from our Update Servers (eScan automatically checks and update the latest virus signature available on the update servers after installation).

Renewal and Upgrade

- **Renewal**: You need to have a License Key for renewing eScan, you can purchase the license key from any dealer nearby your place or you can purchase online from eScan at www.escanav.com.
- **Upgrade**: If a newer version is available, eScan can be upgraded by downloading and installing eScan from our website.

System Requirement

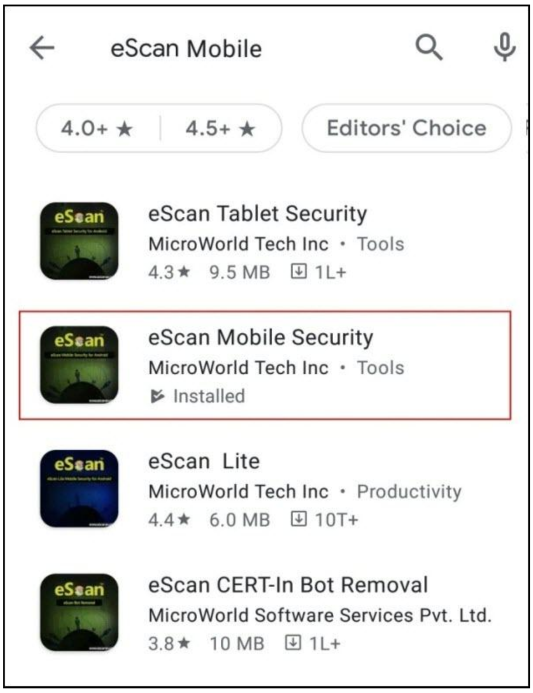
Prior to installation your device must meet the following criteria:

- **Operating System**: Android 5.0 and above
- **Minimum Space**: 40-50 MB
- **Others**: Internet connection

Download and Installation of eScan Mobile Security

Steps to follow for downloading and installing the eScan Mobile Security on your Android device:

1. Go to **Play Store.**
2. Search for **eScan Mobile Security** app in search box.



eScan Mobile

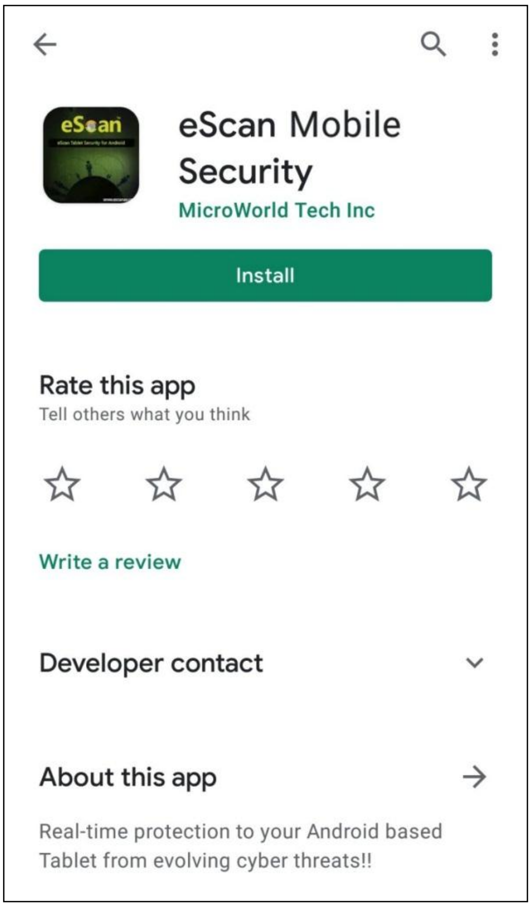
eScan Tablet Security
MicroWorld Tech Inc • Tools
4.3★ 9.5 MB 1L+

eScan Mobile Security
MicroWorld Tech Inc • Tools
Installed

eScan Lite
MicroWorld Tech Inc • Productivity
4.4★ 6.0 MB 10T+

eScan CERT-In Bot Removal
MicroWorld Software Services Pvt. Ltd.
3.8★ 10 MB 1L+

3. **Download** and **Install** the eScan Mobile Security application. eScan Mobile Security app is added to the applications list on your device.



eScan Mobile Security

MicroWorld Tech Inc

Install

Rate this app

Tell others what you think

☆ ☆ ☆ ☆ ☆

Write a review

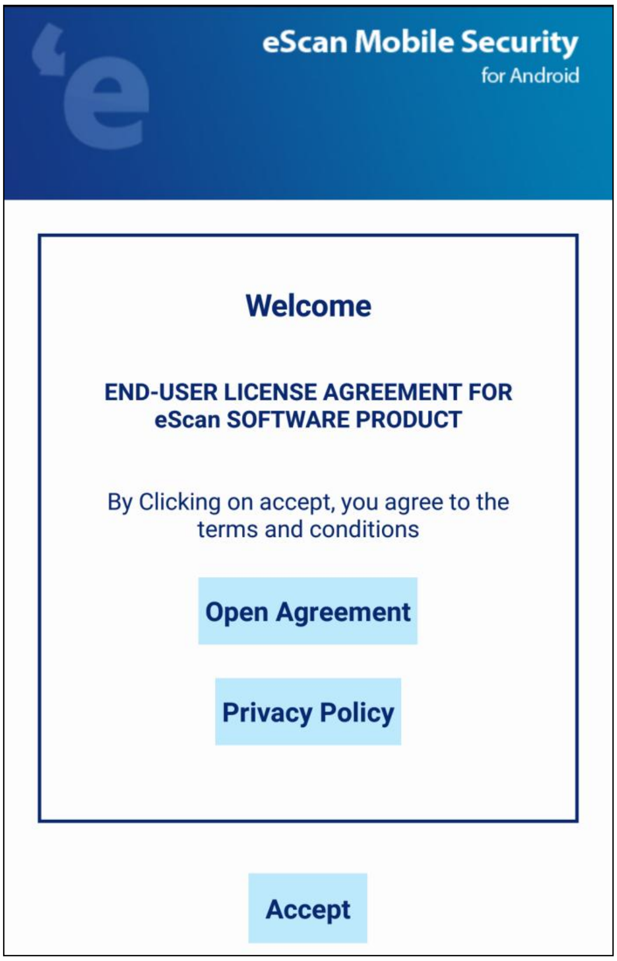
Developer contact

About this app

Real-time protection to your Android based Tablet from evolving cyber threats!!

4. To open the application on your device, go to the application list and tap on the eScan Mobile Security icon.

5. A License Agreement screen appears.



eScan Mobile Security
for Android

Welcome

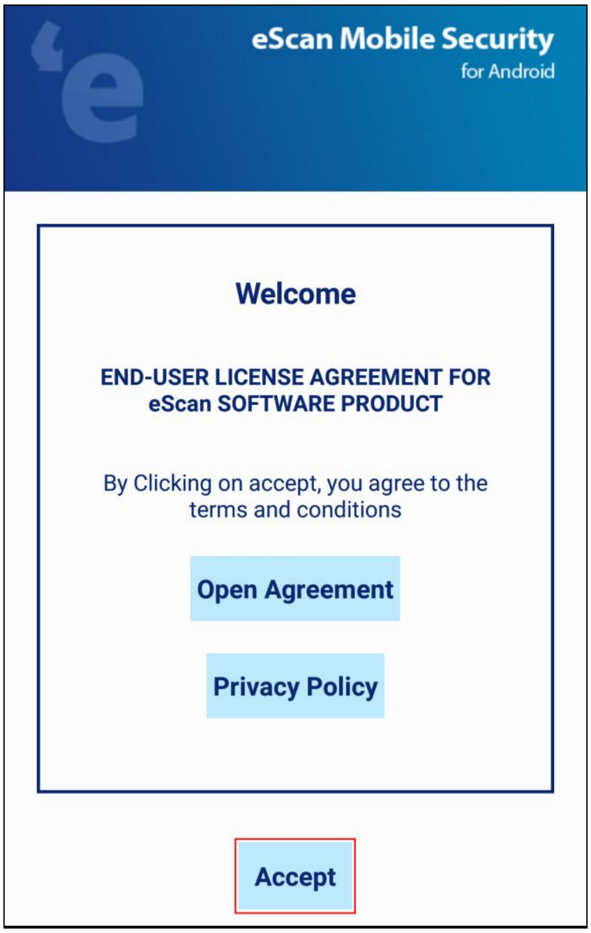
END-USER LICENSE AGREEMENT FOR eScan SOFTWARE PRODUCT

By Clicking on accept, you agree to the terms and conditions

6. Select **Open Agreement** option.

Read carefully End-User License Agreement and Privacy Policy.

7. Tap on **Accept** option.



eScan Mobile Security
for Android

Welcome

END-USER LICENSE AGREEMENT FOR
eScan SOFTWARE PRODUCT

By Clicking on accept, you agree to the
terms and conditions

8. You are redirected to the Activation screen to register your product. To know how to register your license, click here.

Uninstallation of eScan Mobile Security

For uninstallation of eScan Mobile Security application, follow the given methods:

- Do a **long press** on the eScan icon on your device main menu.
- The **recycle bin** image appears on the icon.
- **Drag** and **drop** the eScan icon into the bin.

OR

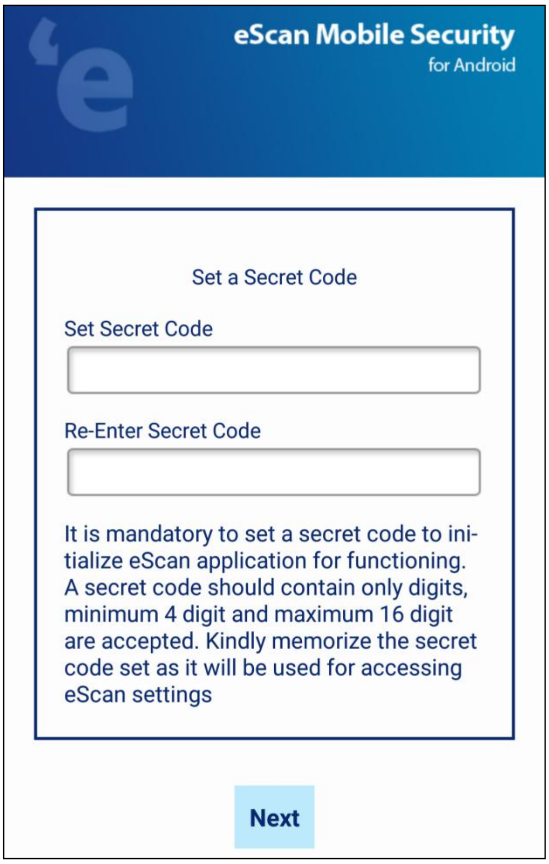
- Open eScan Mobile Security app.
- Tap on the **Additional** option.
- Tap on **Uninstall** option.

eScan Mobile Security application will be uninstalled from your device by confirming the uninstallation request.

Secret Code

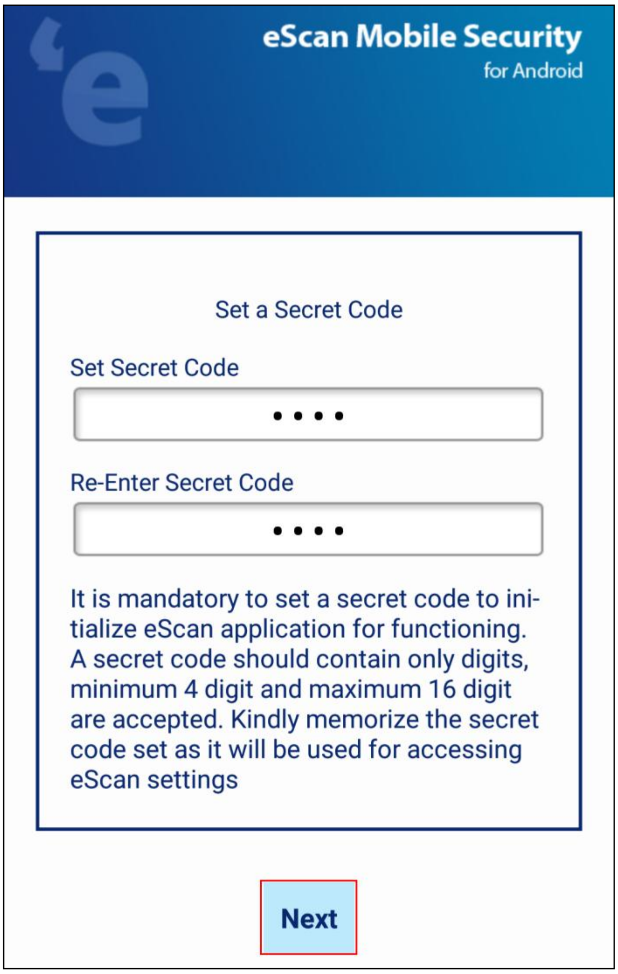
When you launch the eScan Mobile Security application for the first time on your device, it will prompt you to create a secret code. The secret code should be minimum 4 and maximum 16 digits long. The secret code should contain only digits (0-9).

NOTE	It is mandatory to set secret code, without secret code user cannot initialize eScan application for functioning.



It is mandatory to set a secret code to initialize eScan application for functioning. A secret code should contain only digits, minimum 4 digit and maximum 16 digit are accepted. Kindly memorize the secret code set as it will be used for accessing eScan settings

- **Enter** Secret Code. **Re-Enter** Secret code for confirmation.



Set a Secret Code

Set Secret Code

••••

Re-Enter Secret Code

••••

It is mandatory to set a secret code to initialize eScan application for functioning. A secret code should contain only digits, minimum 4 digit and maximum 16 digit are accepted. Kindly memorize the secret code set as it will be used for accessing eScan settings

- Tap on **Next** tab.

Recover the Secret Code

If you forget the secret code, you can recover it with eScan Mobile Security application. The recovery code will be sent to the registered Email Id, so provide a valid Email Id during registration and activation.

Registration and Activation

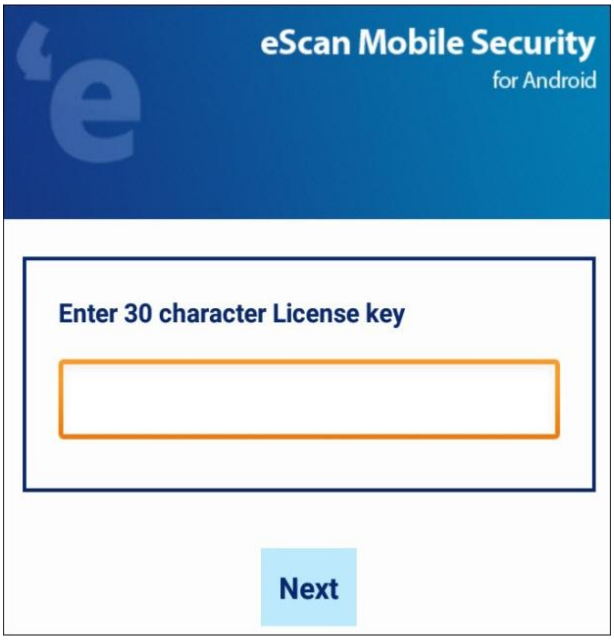
Once you purchase eScan Mobile Security, you have to enter a valid license key to activate the product. The license key will be mailed to your email address on purchasing the product online or if you have purchased a packet, the license key will be already included in it.

❗ NOTE	You can either choose internet mode or SMS mode for activation. Activation through the internet will be instant whereas activation through SMS will take 48 hours. One License Key can be activated only on single device.

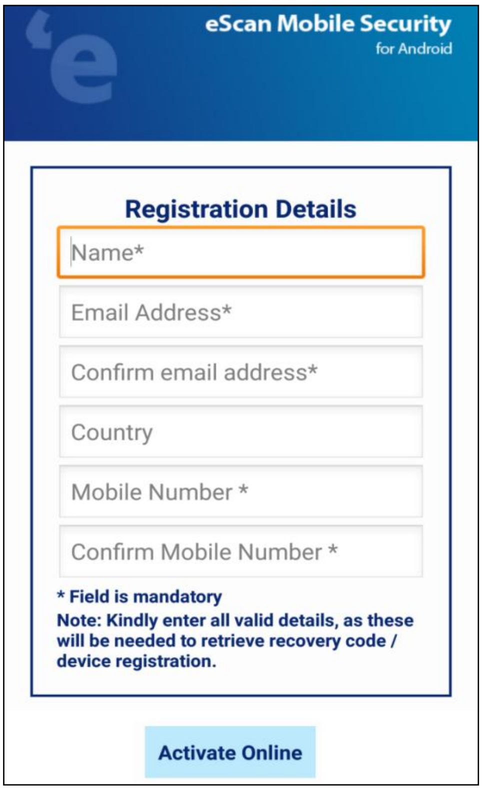
After you Open/Start the application for the first-time following screen appears with options as shown below:

Enter License Key: Tap on this to enter the license key that you received on your email id or included in the packet.

- Enter 30 characters **License Key**.



- Tap on **Next.**
- The **Registration Details** screen appears.



eScan Mobile Security
for Android

Registration Details

Name*

Email Address*

Confirm email address*

Country

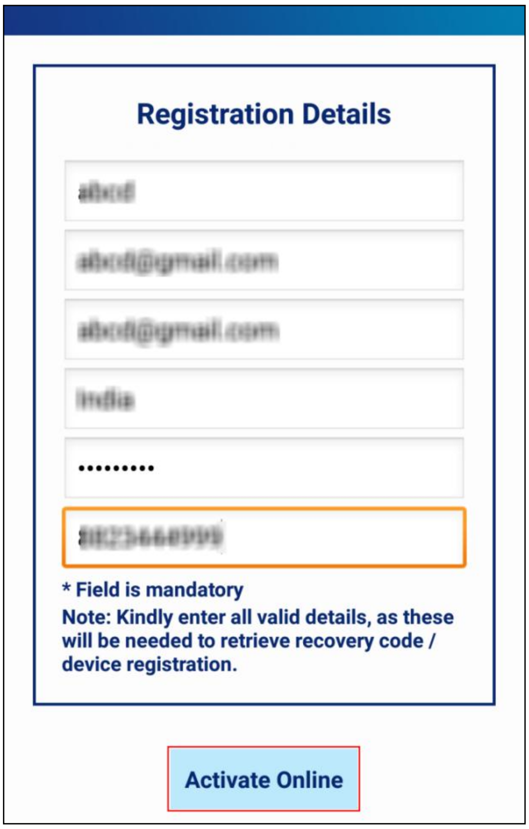
Mobile Number *

Confirm Mobile Number *

* Field is mandatory
Note: Kindly enter all valid details, as these will be needed to retrieve recovery code / device registration.

- Enter the following details:

Field	Description
Name*	Enter a name here. Your device will be registered by this name.
Email Address*	Enter a valid email address used for communication purpose.
Confirm Email Address*	Re-type the e-mail ID for confirmation.
Country	Enter the country name.
Mobile Number*	Enter a valid mobile number.
Confirm Mobile Number*	Re-type the mobile number for confirmation.



Registration Details

abcd

abcd@gmail.com

abcd@gmail.com

India

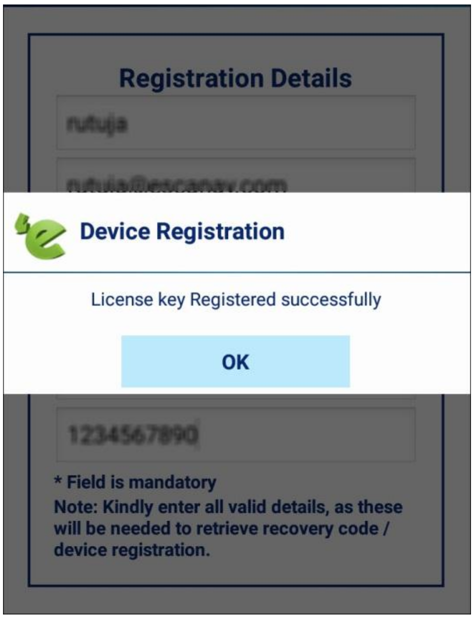
•••••••••

8823664999

* Field is mandatory

Note: Kindly enter all valid details, as these will be needed to retrieve recovery code / device registration.

- After entering all the required information, tap on **Activate Online**.
- **Device Registration** screen appear with message: “License Key Registered successfully”. Tap on **OK**.



Registration Details

rutuja

rutuja@escanav.com

Device Registration

License key Registered successfully

1234567890

* Field is mandatory

Note: Kindly enter all valid details, as these will be needed to retrieve recovery code / device registration.

Activate Free Trial: To use a trial version, tap on this option. From the day of activation, the trial version is available for duration of 29 days. Fill in all of the required information on the Registration Details screen, and then tap the Activate Online button to activate the account.

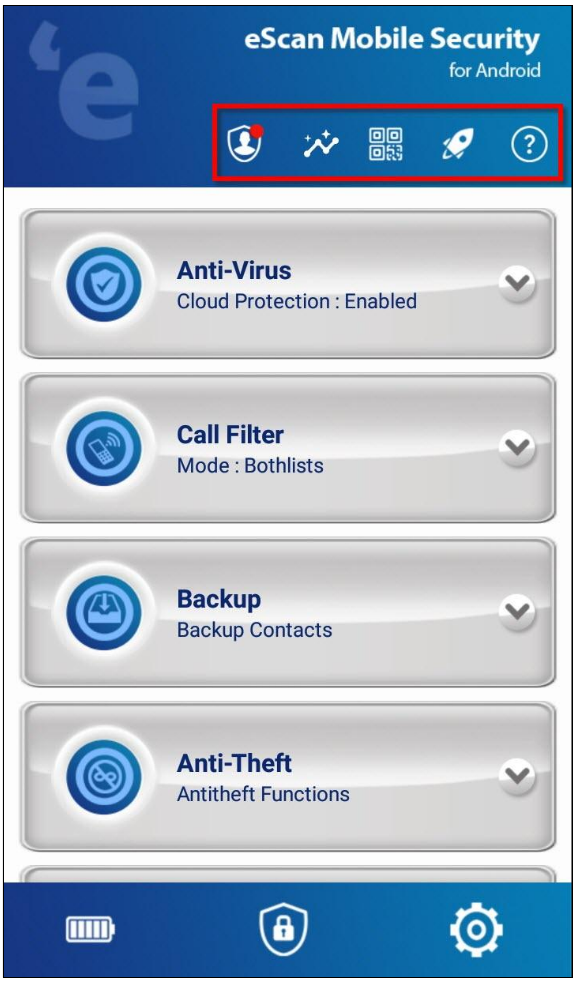
❗ NOTE	To activate the trial version of eScan Mobile Security, no license key is required.

Purchase Online: To purchase the product online, tap the link. You can get it through the Play Store or the eScan website at https://www.escanav.com. You can activate it via the internet after downloading it.

Additional Features

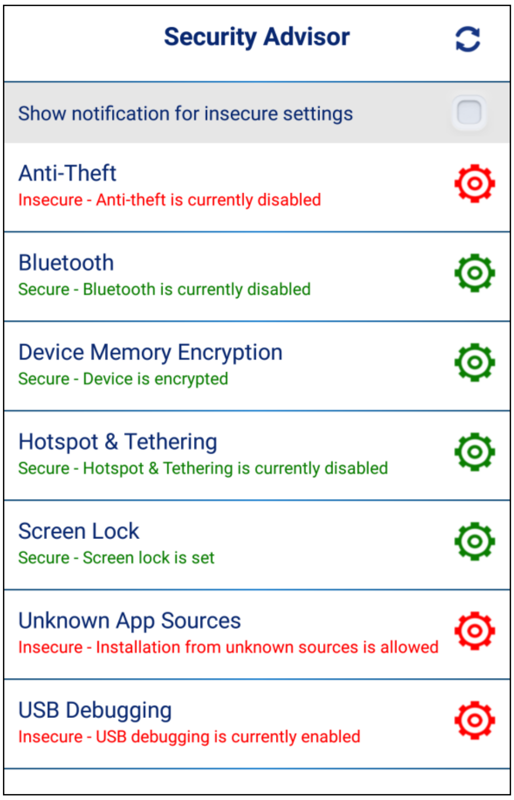
The eScan Mobile Security dashboard gives quick access to the following features:

- Security Advisor
- App Usage
- QR/Barcode Scanner
- Device Booster
- Help



Security Advisor

The Security Advisor warns you about vulnerable settings and lets you to check for potential vulnerabilities on your device. User can update the security settings to avoid such attempts to exploit vulnerabilities. It will improve the overall device security. By selecting check box, it will show a notification for insecure settings.



Security Advisor

Show notification for insecure settings □

Anti-Theft
Insecure - Anti-theft is currently disabled

Bluetooth
Secure - Bluetooth is currently disabled

Device Memory Encryption
Secure - Device is encrypted

Hotspot & Tethering
Secure - Hotspot & Tethering is currently disabled

Screen Lock
Secure - Screen lock is set

Unknown App Sources
Insecure - Installation from unknown sources is allowed

USB Debugging
Insecure - USB debugging is currently enabled

NOTE	⚙ : This setting icon shows unsecure settings.
	⚙ : This setting icon shows secure settings.

Insecure settings: If eScan Mobile Security detects vulnerable settings at that moment, a notification is displayed. For unsafe setting of notification alerts for such events, you can enable or disable this feature. For the insecure setup of notification alerts, it is suggested that you enable this option.

Secure Settings: You can increase the security level by using this setting icon. When you tap the setting icon, you will be redirected to the individual security features, where you can configure them.

The Security Advisor includes following setting options for configuration:

- **Anti-Theft**: The Anti-Theft feature provides security and ensures complete protection to your device from any unauthorized access in case of device is lost or stolen.

- **Bluetooth**: It is used to transfer files and data. It may endanger to your device and data. Simply switch off the Bluetooth option if it is not in use.

- **Device Memory Encryption**: You have the option of encrypting the data of your device, which safeguards your information from unauthorized access. As a result, it is preferable to enable this setting to secure your device from illegal access.

- **Hotspot & Tethering**: Data sharing via Wi-Fi Hotspot, USB, and Bluetooth Tethering put your device at risk of being hacked. If it is not in use, simply turn it off.

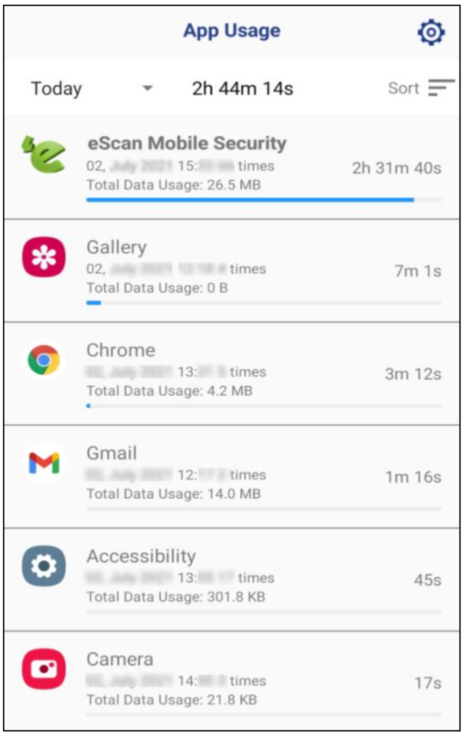
- **Screen Lock**: To prevent the misuse of your device data and personal information, Setting a Pattern, PIN, Password, or Finger Print as a screen lock is preferable.

- **Unknown App Sources**: It prevents unknown applications from being installed on your device. If you enable this option, every time when you try to install an application, it will prompt you to allow installation.

- **USB Debugging**: The device is not as secure when connected to a computer to transfer data through USB. So, it is preferable to disable this setting.

App Usage

Detailed information can be captured with regards to the total usage of the application based on Today, Yesterday, This Week, or This Month along with date, time, and total data usage. It will help users to monitor number of times the particular application is used by the user. User can also monitor how much data is utilized by the each application.



App Usage

Today 2h 44m 14s Sort

eScan Mobile Security
02, [redacted] 15:[redacted] times
Total Data Usage: 26.5 MB
2h 31m 40s

Gallery
02, [redacted] times
Total Data Usage: 0 B
7m 1s

Chrome
[redacted] 13:[redacted] times
Total Data Usage: 4.2 MB
3m 12s

Gmail
[redacted] 12:[redacted] times
Total Data Usage: 14.0 MB
1m 16s

Accessibility
[redacted] 13:[redacted] times
Total Data Usage: 301.8 KB
45s

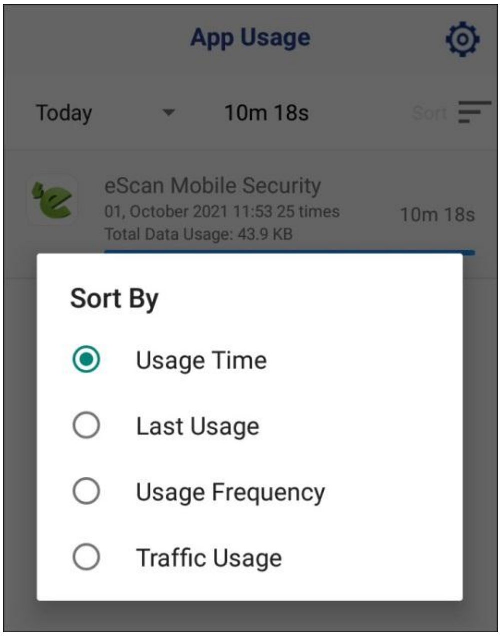
Camera
[redacted] 14:[redacted] times
Total Data Usage: 21.8 KB
17s

App Usage has following options to configure:

- Sort
- Settings

Sort: Using this option, user can sort the applications as per requirements. User can sort application based on following criteria:

- Usage Time: It will sort applications according to total time utilized.
- Last Usage: it will sort applications according to time.
- Usage Frequency: it will sort applications based on number of time app used.
- Traffic Usage: It will sort applications based on data usage.



App Usage

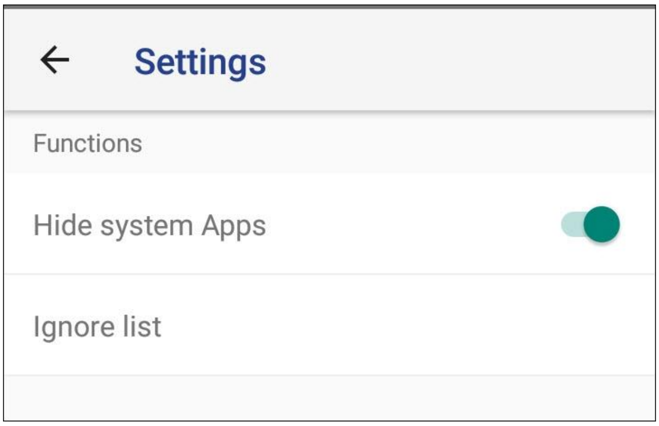
Today ▾ 10m 18s Sort

eScan Mobile Security
01, October 2021 11:53 25 times
Total Data Usage: 43.9 KB
10m 18s

Sort By

● Usage Time
○ Last Usage
○ Usage Frequency
○ Traffic Usage

Settings: This option can be used to Hide System Apps and to see Ignore list of apps.



← Settings

Functions

Hide system Apps ●

Ignore list

Settings has following options:

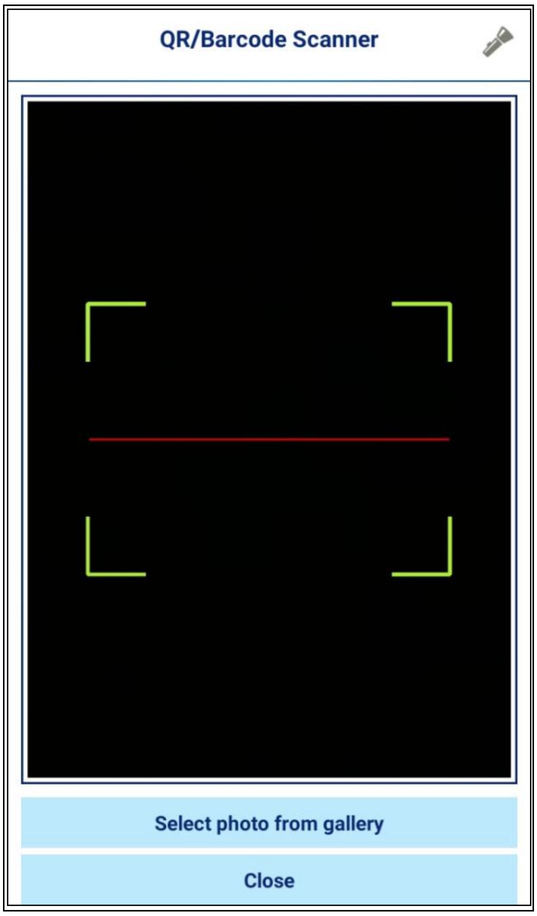
- Hide System Apps: Enable this option to hide system apps.
- Ignore list: It will show the list of applications ignored by the users. User can remove the application from the ignore list.

Add application in the Igonre list:

- Open eScan Mobile Security application. Tap on **App Usage**.
- Press and hold on application user want to add ignore list.
- List of option will appear.Tap on **Ignore this app** option.

QR/Barcode Scanner

This function allows user to scan QR/Barcode and verify target URLs for malware and internet risks. In addition, user can scan QR/Barcodes with a photo from device gallery. It will prevent user from visiting any malicious website. Scanning result show you content of QR/Barcode with its category.



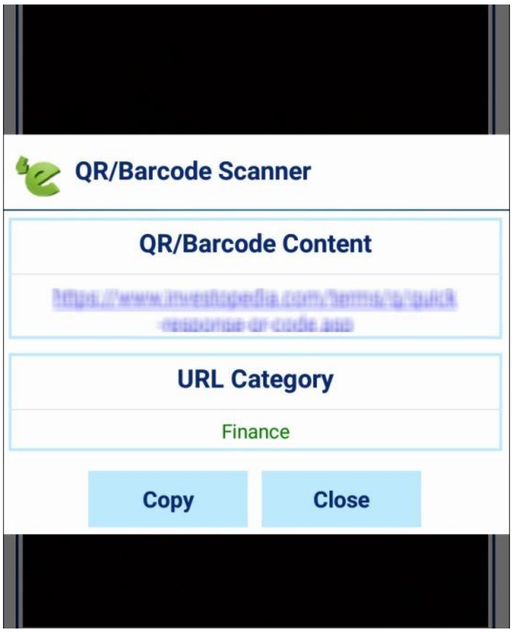
To scan QR/Barcode:

- Hold your device over a QR/Barcode to scan. After scanning result will appear.

OR

- You can select image from your gallery. Tap on **Select Photo from gallery** option.
- **Select** image.

After scanning result screen appear as shown below.



QR/Barcode Scanner

QR/Barcode Content

[redacted]

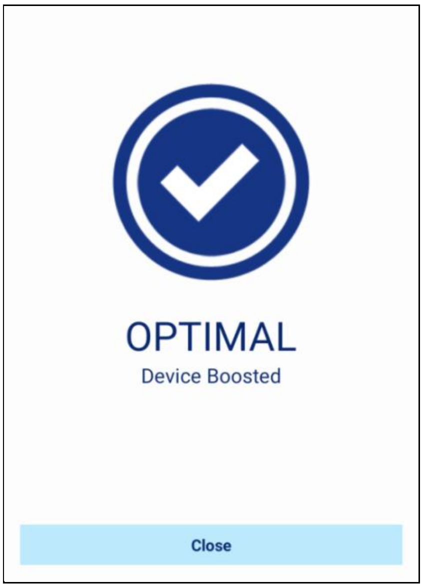
URL Category

Finance

- **QR/Barcode Content-** This option shows the content of scanned QR/Barcode.
- **URL Category-** This option shows the category of scanned QR/Barcode.

Device Booster

It optimizes your device and improves performance. This feature will help you to free up the storage by removing junk files, cache files running in background. Tap on device booster icon, it will start boosting your device.



OPTIMAL

Device Boosted

Help

It helps user to understand each function, tab, toolbar option, or other elements within the user interface. It explains you in detail information about eScan Mobile Security application features with its functioning.

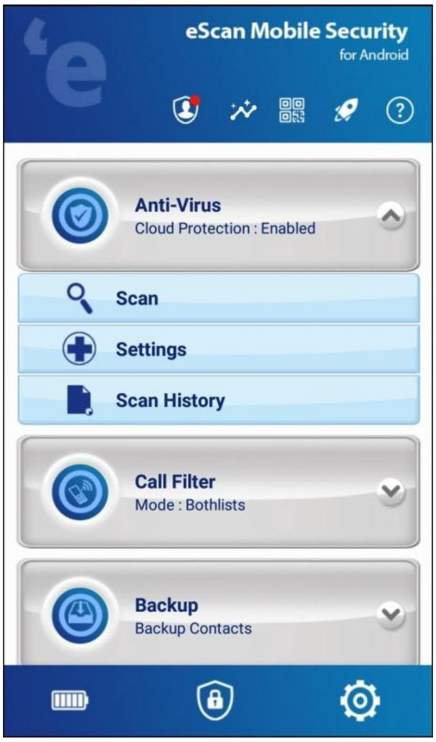
Modules

eScan Mobile Security application provide users following modules:

- Anti-Virus
- Call Filter
- Backup
- Anti-Theft
- Parental Control
- App Lock

Anti-Virus

For Android-based devices, eScan Anti-Virus provides protection against Malware, Trojans, and other viruses. It will scan your device in real time when you install or download a new application, to protect your device from all types of infections/attacks. It allows users to define the scan setting for automatic or scheduled scanning. User can also select whether you want to scan the full files, folders directory or just the executable files. It provides you scanning history.



Anti-Virus module has following options to configure:

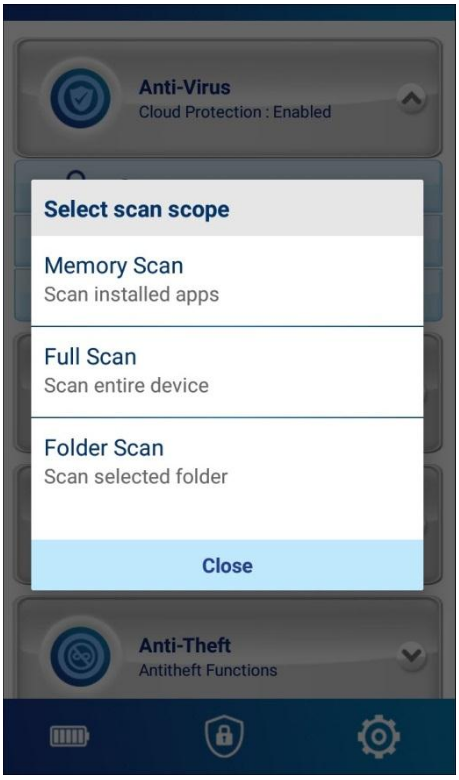
- Scan
- Settings
- Scan History

NOTE	Check and see that your smartphone is connected to the internet. The scan process will not begin if your device is not connected to the internet.

Scan

This tab is used to scan your device for the potential vulnerabilities and privacy violations. It will scan your device as per user requirement for scanning.

As you tap on **Scan,** it displays the following options for scanning:



Anti-Virus
Cloud Protection : Enabled

Select scan scope

Memory Scan
Scan installed apps

Full Scan
Scan entire device

Folder Scan
Scan selected folder

Close

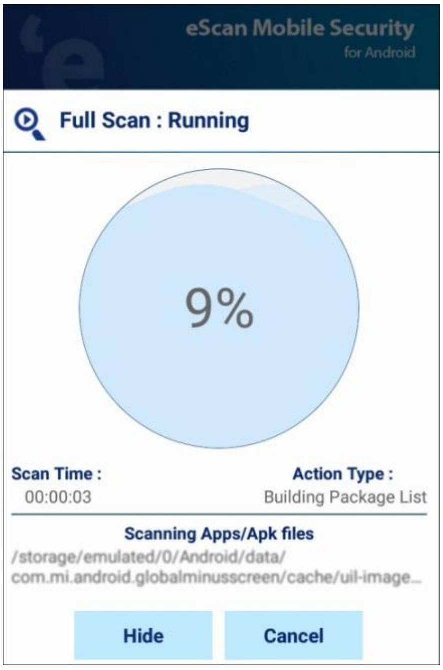
Anti-Theft
Antitheft Functions

Choose an appropriate option for scanning.

- **Memory Scan**: To scan all the apps/apk files of all the applications of the device, tap on this option. The message Memory Scan: Finished will be displayed, along with scan details such as the number of apps/apk files scanned, threats detected, threats deleted, threats skipped, and the total scan time.
- **Full Scan**: Select this option to scan all the apps/apk files available on your device as well as your memory card. When the scan is finished, a report will appear with the details apps/apk files scanned, threats identified, threats eliminated, skipped, and total scan time.

- **Folder Scan**: Select this option to scan only the apps/apk files within particular folder you want. Folder Scan: Finished will appear in a report, along with other scan details such as file scanned, threats found, threats removed, skipped, and scan time.

Tap on **Cancel** to close and tap on **Hide** to send the scanning process to background.



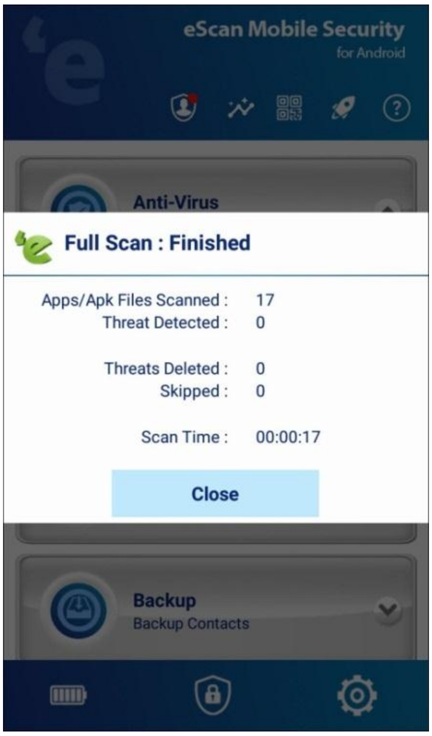
Scan Time : 00:00:03

Action Type : Building Package List

Scanning Apps/Apk files

/storage/emulated/0/Android/data/com.mi.android.globalminusscreen/cache/uil-image...

After completing scanning, Result screen appear with details as shown below.



Full Scan : Finished

Apps/Apk Files Scanned : 17
Threat Detected : 0

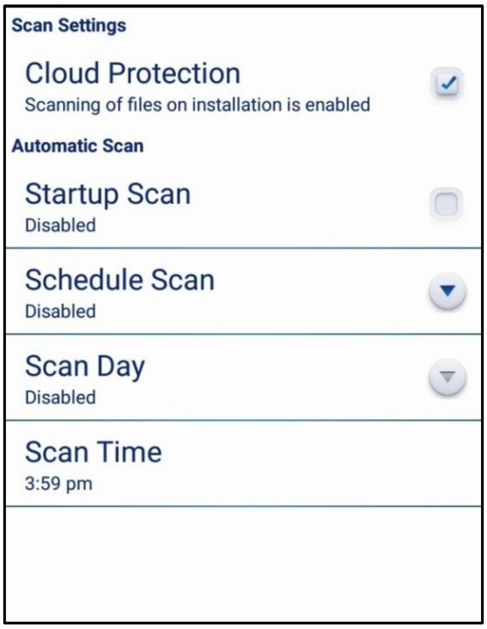
Threats Deleted : 0
Skipped : 0

Scan Time : 00:00:17

Settings ✚

This tab used to configure a setting for scanning and allow users to schedule scan. User has to enter a secret code to access the administration mode, which help users to configure the settings for the Anti-Virus module for the following option:

- Scan Settings
- Automatic Scan



Scan Settings

Cloud Protection ☑
Scanning of files on installation is enabled

Automatic Scan

Startup Scan □
Disabled

Schedule Scan ▼
Disabled

Scan Day ▼
Disabled

Scan Time
3:59 pm

Scan Settings

- **Cloud Protection:** This option is activated by default, and it ensures that all newly downloaded application files are scanned.

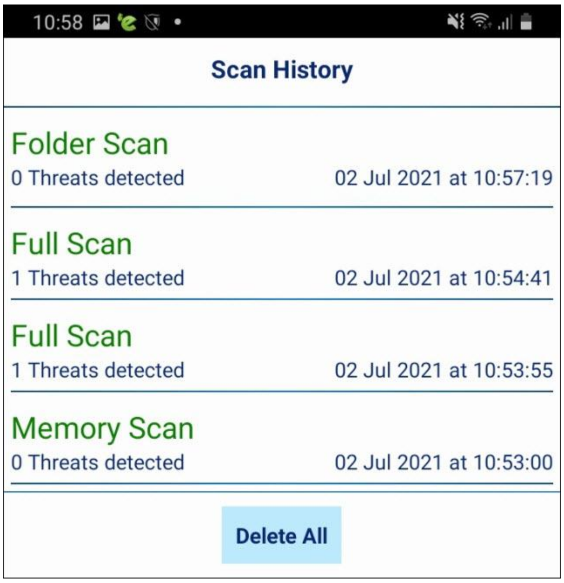
Automatic Scan

It comprises of following configuration:

- **Startup Scan**: This setting is disabled by default. It lets you scan your device whenever you start or reboot your device. Tap on this option to turn on or off the startup scan as per your requirement.
- **Schedule Scan**: This option allows you to schedule a scan on a Weekly or Daily basis. By default it is disabled. From the drop-down Schedule Scan screen, choose an appropriate option to schedule scan.
    - Weekly: It allows user to schedule a weekly scan on a particular day.
    - Daily: It allows user to schedule a daily scan at predefined time.
    - Disabled: It allows user to disable the schedule scan.
- **Scan Day**: By default, this option is turned off. The Scan Day setting is activated after the Weekly scan option is selected in Schedule Scan. You can schedule the scan for a specific day of the week.
- **Scan Time**: By default, this option is turned off. This option is enabled after you select the Schedule Scan option as Weekly or Daily. This option allows you to set the scan time.

Scan History

This tab displays records of all previously performed scans on the device with scan type, total threats detected, date, and time. It lets you see all the details of scan attempted for each target.



Scan History

Folder Scan
0 Threats detected 02 Jul 2021 at 10:57:19

Full Scan
1 Threats detected 02 Jul 2021 at 10:54:41

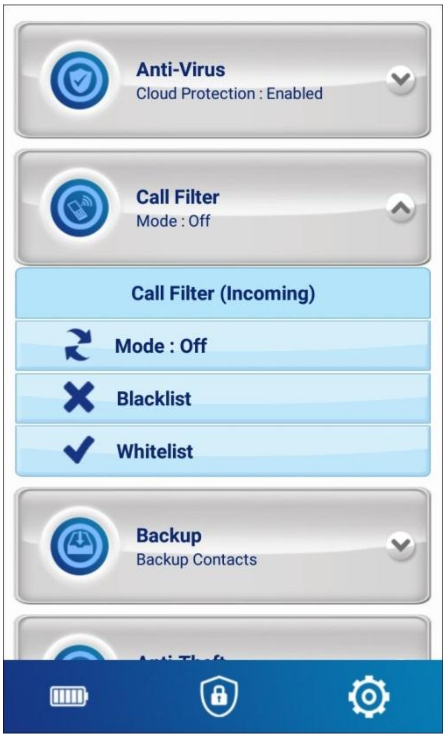
Full Scan
1 Threats detected 02 Jul 2021 at 10:53:55

Memory Scan
0 Threats detected 02 Jul 2021 at 10:53:00

Tap on **Delete All**, the scan history will be erase. It will prompt you for confirmation.

Call Filter

This tab lets you filter the all incoming calls. User can designate numbers, phrases, words, and keywords to be whitelisted and blacklisted. It will filter incoming calls on the basis of blacklist and whitelist created by user. Filtering can be controlled using the following options as shown in the below screen.



Anti-Virus
Cloud Protection : Enabled

Call Filter
Mode : Off

Call Filter (Incoming)

Mode : Off

Blacklist

Whitelist

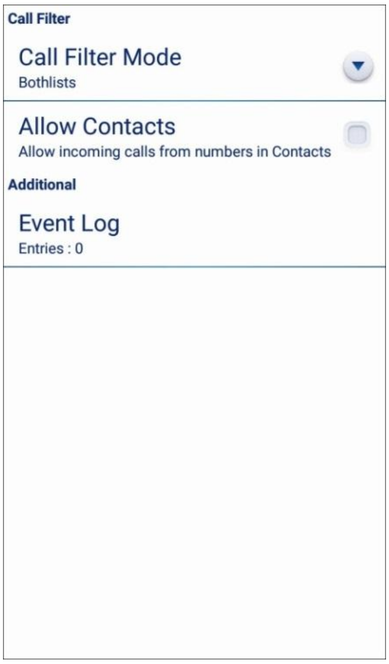
Backup
Backup Contacts

Call Filter module has following options to configure:

- Mode
- Blacklist
- Whitelist

Mode

Using this option user can set the filter mode as per requirement. By default filter mode is off. User can set mode as Blacklist, Whitelist and Bothlists. It will provide you call log with details of the calls blocked.



Call Filter

Call Filter Mode
Bothlists

Allow Contacts
Allow incoming calls from numbers in Contacts ☐

Additional

Event Log
Entries : 0

Call Filter

- **Call Filter Mode**: As you tap on this option, a drop-down list appears with options Off, Whitelist, Blacklist and Bothlists. It will filter incoming calls based on your selection. By default call filter mode is off.
  1. Off: Disable all call filters.
  2. Blacklist: Block all calls from blacklist numbers.
  3. Whitelist: Allow all calls from whitelist numbers.
  4. Bothlists: Blocks all calls from blacklist, allow calls from whitelist and contact list (in case Allow Contact option is selected).

Allow Contacts

If you enable this option, you will only receive calls from numbers in your contact list.

Additional

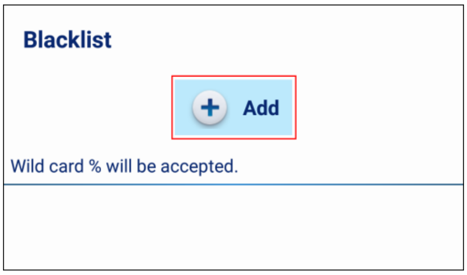
- **Event Log:** It will display the records of the calls blocked.

Blacklist ☒

This feature allows you to add contact numbers to blacklist and blocks incoming calls from those numbers. You can also add % wild card characters to block incoming calls from particular series. This will only applicable when call filter mode is set as Blacklist or Bothlists.

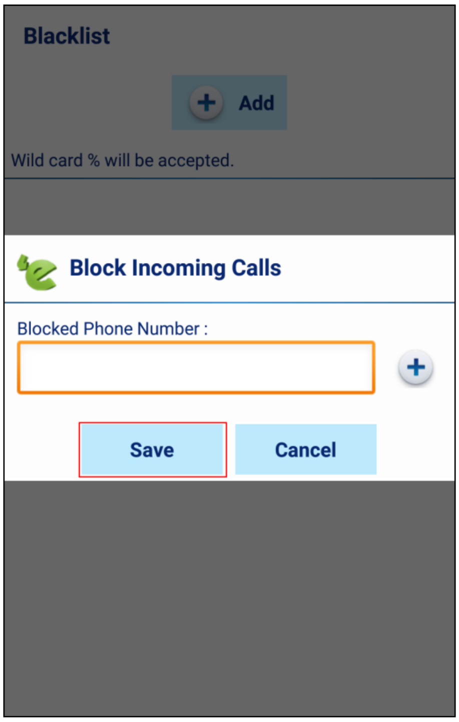
To add contact numbers in Blacklist follow the given steps:

- Tap on **Blacklist** option.
- Tap on **Add**.



Wild card % will be accepted.

- Enter the contact number you want to blacklist and tap on **Save**. It will block all the calls coming from that specified number. Additionally, you can also add contact from device contact list.

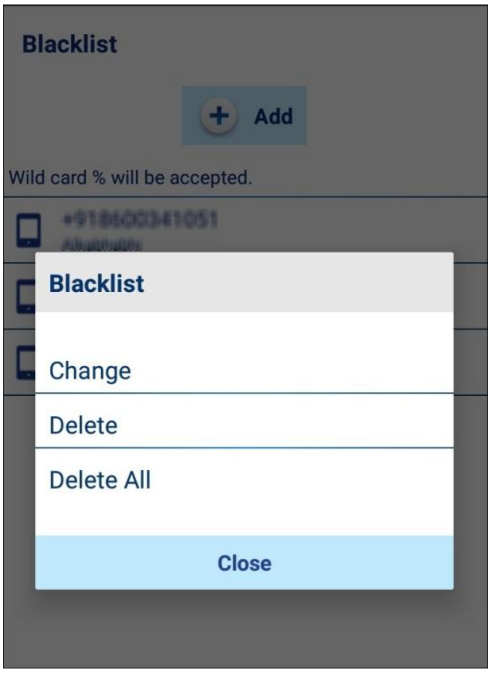


Wild card % will be accepted.

Blocked Phone Number :

To edit and delete contacts/numbers from the Blacklist you created:

- Tap on particular number/contact you want delete or edit.
- Following options will appear:
    1. Change: Allow you to make changes in existing contact.
    2. Delete: It will delete selected contact/number from blacklist.
    3. Delete All: All contacts will delete from the blacklist.



Blacklist

Wild card % will be accepted.

[redacted]

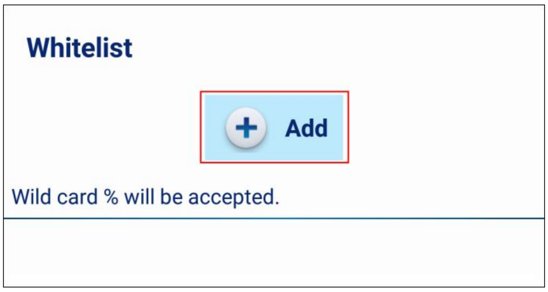
- Choose an appropriate option. It will prompt you for confirmation.

Whitelist ✓

This option allows calls from the contact numbers added in the whitelist. % wild card characters can be added to the whitelist. It is applicable, when call filter mode is set as Whitelist or Bothlists.

To add contact numbers in Whitelist follow the below given steps:

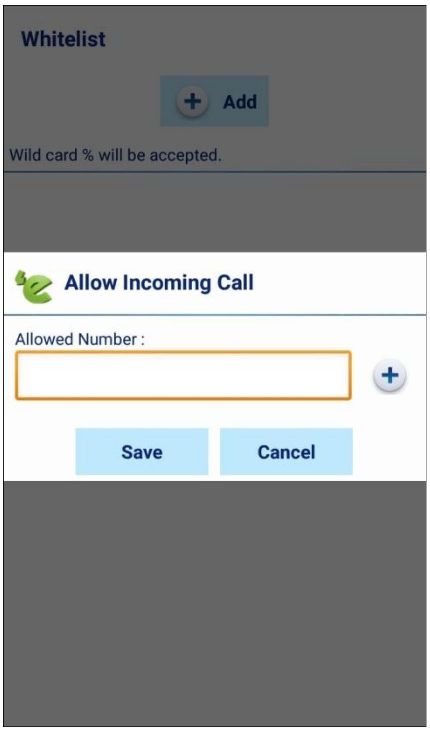
- Tap on **Whitelist** option.
- Tap on **Add**.



Whitelist

Wild card % will be accepted.

- Enter the phone number you want to whitelist and tap on **Save**. It will allow all the calls from that specified numbers. Additionally, you can also add contact from device contact list.



Whitelist

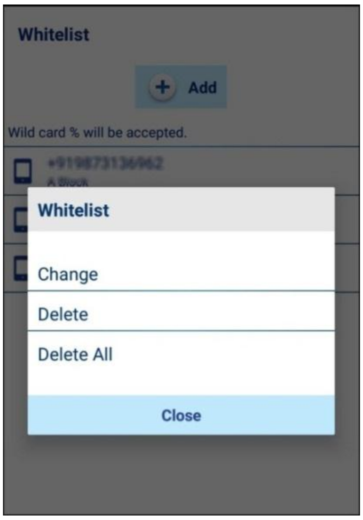
Wild card % will be accepted.

Allow Incoming Call

Allowed Number :

To edit and delete contacts/numbers from the whitelist you created:

- **Tap** on particular number/contact you want delete or edit.
- Following options will appear
  1. Change: Allow you to make changes in existing contact.
  2. Delete: It will delete selected contact/number from whitelist.
  3. Delete All: All contacts will delete from the whitelist.



Whitelist

Wild card % will be accepted.

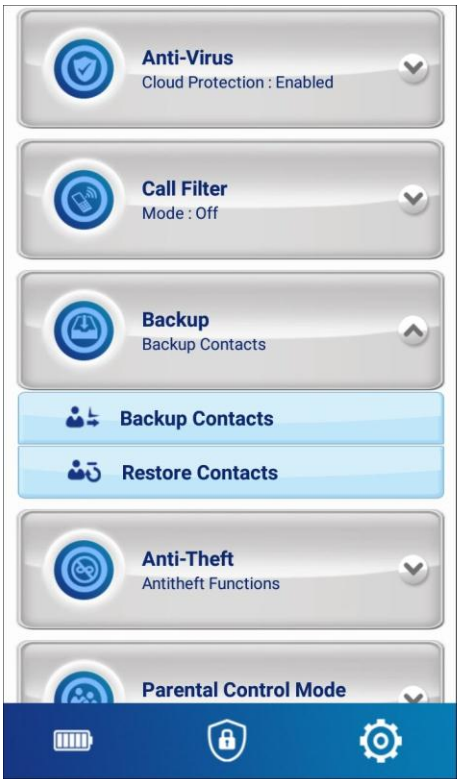
[redacted]

Whitelist

- Choose an appropriate option. It will prompt you for confirmation.

Backup

This module lets you take a backup of all your contacts to cloud (Google Drive) or internal storage. When necessary, the backed-up data can simply restore to the device. The contacts are saved in .vcf file format after back up.

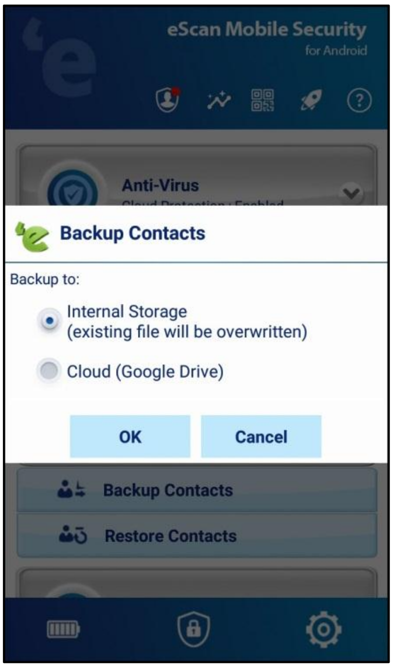


Backup module has following options to configure:

- Backup Contacts
- Restore Contacts

Backup Contacts

This tab lets you save all your contacts to the Internal Storage or Cloud (Google Drive).



Backup Contacts

Backup to:

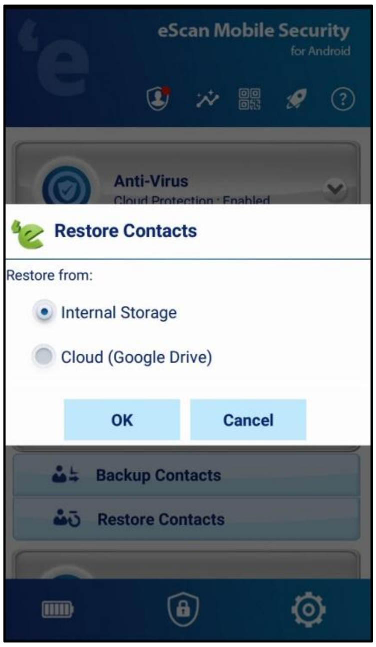
● Internal Storage
(existing file will be overwritten)

○ Cloud (Google Drive)

- Select an appropriate option to backup of contacts.

Restore Contacts

Tap on **Restore Contacts** to recover all your contacts from a backup file as per requirement.



Restore Contacts

Restore from:

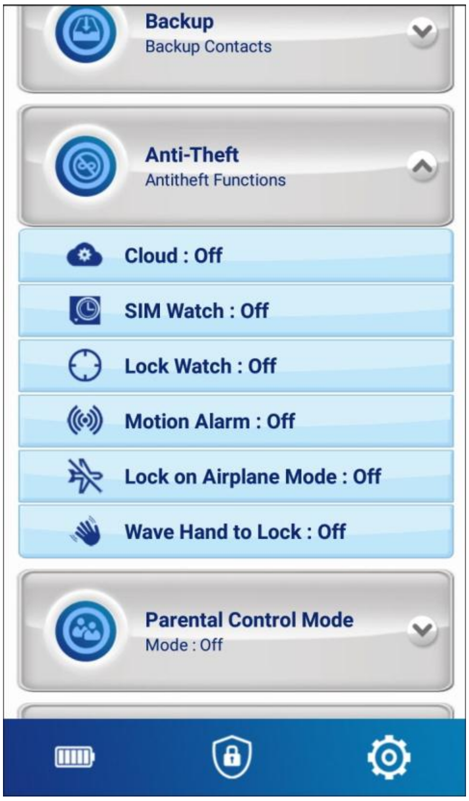
● Internal Storage

○ Cloud (Google Drive)

- Select an appropriate option to restore contacts.

Anti-Theft

The Anti-Theft feature provides security and total protection to your device from any unauthorized access, in case your device is lost or stolen. Anti-Theft module allows users to Lock, Locate or Wipe Data of your Android device. You can access and use anti-theft features through our Anti-Theft Portal. To use Anti-Theft portal user need to have an account on anti-theft portal and android device linked to it. The features Lock, Data Wipe, Locate and Scream can be activated via Cloud portal (only if they are enabled on the device).



Backup
Backup Contacts

Anti-Theft
Antitheft Functions

Cloud : Off
SIM Watch : Off
Lock Watch : Off
Motion Alarm : Off
Lock on Airplane Mode : Off
Wave Hand to Lock : Off

Parental Control Mode
Mode : Off

Anti-Theft module has following options to configure:

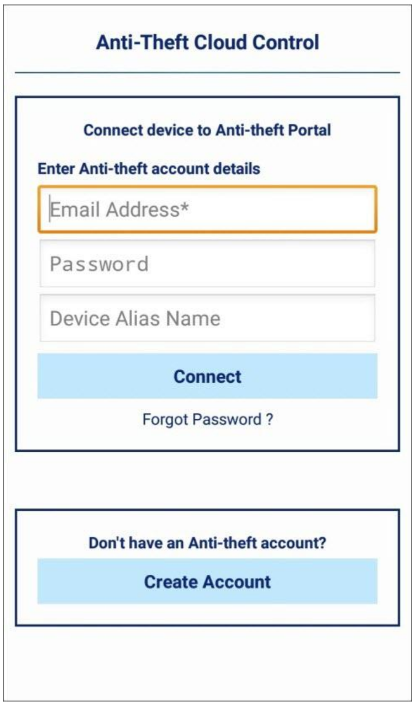
- Cloud
- SIM Watch
- Lock Watch
- Motion Alarm
- Lock on Airplane Mode
- Wave Hand to Lock

Cloud

This tab helps users to protect the device if it gets lost or stolen. User can create an Anti-Theft account to protect your device, which will allow users to use the Anti-Theft console with various features remotely.

For Anti-Theft login follow the below given steps:

- Tap on the **Cloud** option. Anti-Theft Cloud Control screen appear.



Anti-Theft Cloud Control

Connect device to Anti-theft Portal

Enter Anti-theft account details

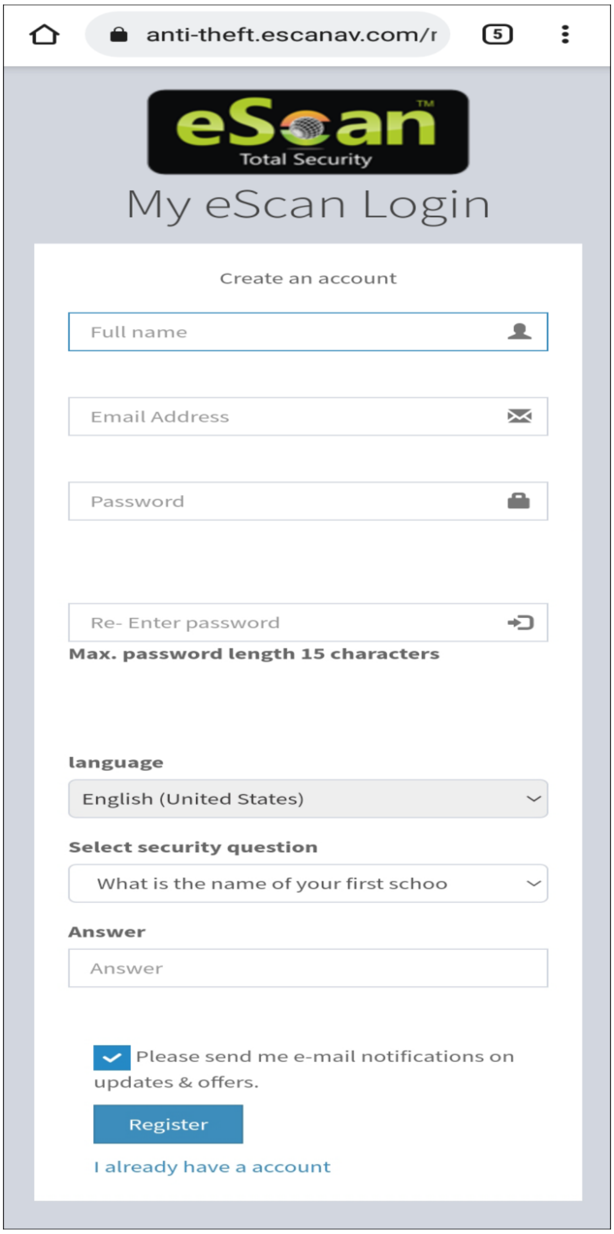
Email Address*

Password

Device Alias Name

Don't have an Anti-theft account?

- **Enter** your **Login Details,** if you are an existing user
- Tap on **Create Account,** if you are new user. You will be redirected to the Anti-Theft portal login screen. Register here by providing the required details.



anti-theft.escanav.com/r

eScan™ Total Security

My eScan Login

Create an account

Full name

Email Address

Password

Re- Enter password

Max. password length 15 characters

language

English (United States)

Select security question

What is the name of your first schoo

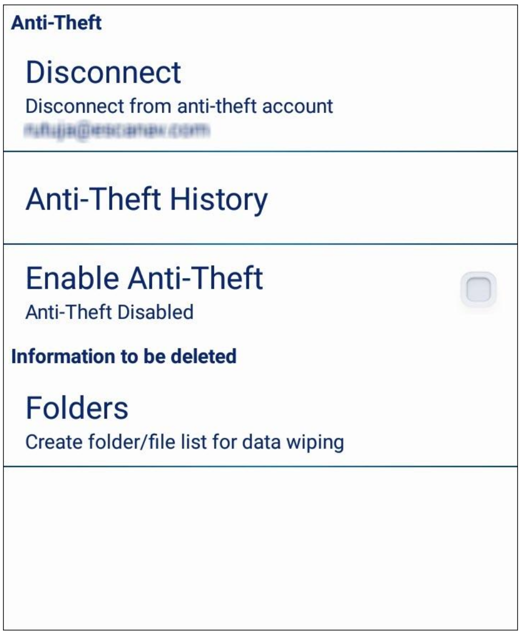
Answer

Answer

☑ Please send me e-mail notifications on updates & offers.

- Tap on **Register.**
- Login with your credential email address, password and device name.
- Tap on **Connect.** This will add your device to the Anti-Theft portal from where you can send the anti-theft command for Wipe Data, Device lock, Locate Device, and Scream.

NOTE	Password is case sensitive. Please make sure that you are entering it in proper case and Caps Lock is OFF. If you have forgotten your password, click the 'Forgot Password?' link below the Login button. In the 'Forget Password ', enter the email address specified as your account username and click 'SEND'. A mail with a 'Reset Password' link will be sent to your email address. Clicking the link from the email will enable you to create a new password for your account.



Anti-Theft

Disconnect
Disconnect from anti-theft account
[redacted]

Anti-Theft History

Enable Anti-Theft ☐
Anti-Theft Disabled

Information to be deleted

Folders
Create folder/file list for data wiping

Anti-Theft cloud consists of following options:

- **Disconnect** - Using this option user can disconnect their device from Anti-Theft account.
- **Anti-Theft History** – It shows Anti-Theft summary/history of last 30 days by default. In the same option user can delete and filter summary as per requirement.
- **Enable Anti-Theft** - Enable the anti-theft feature on the device so the commands sent from the anti-theft portal are received by the device.
- **Folders** – Using this option user can select folder/file list for data wiping.

SIM Watch

If the SIM has been changed after the device lost or stolen, the SIM Watch feature will send an SMS and email with the new SIM details and location.

- **SIM Watch Enable**: Enable this option, to start monitoring the activity of SIM. It will allow to send the details of new SIM and blocking the device, in case SIM card is replaced.
- **Block**: Tap on this to allow your device to block if a new SIM is inserted, in case of lost or stolen. User need to enter a valid secret code to unlock the device.

NOTE	This feature works on devices with Android 9 or below versions.

Lock Watch

This feature allows you to capture image of the person who tries to unlock your device more than twice and fails, using front camera of device, in case of device lost or stolen.

- **Lock Watch Enable**: Tap on this option, it will capture a picture from your device front camera whenever a device unlocks attempt fails more than twice.
- **Lock Watch Gallery**: The Lock Watch Gallery feature stores the captured picture, when the unlock device attempts fails more than twice. Captured image is sent to email Id specified under the alternate contact details.

Motion Alarm

Enable this feature to sound an alarm in case the device is moved from the place you have kept. To enable this feature, tap on Motion Alarm and then tap on Activate.

Lock on Airplane Mode

This feature blocks your device if airplane or flight mode is enabled on device. It provides security to your device if it is lost or stolen.

Wave Hand to Lock

This feature allows you to lock your device with a simple hand gesture over the display screen. To enable this option, select the Wave Hand to Lock option and tap on Activate tab.

Following features are available on Anti-Theft Portal.

Locate

This option will allow you to locate your device in case of loss or theft. This function is activated via Cloud portal. A location map viewed along with the last located date and time of the device on the Anti-Theft portal.

Lock

This option will allow you to lock the device remotely via Cloud portal. Device will only unlock by entering secret code. To lock device in case of lost or stolen, send Lock command from Anti-Theft portal.

Scream

This option will raise a loud alarm on the device when given a scream command via Cloud portal. You can stop the screaming by entering the secret code.

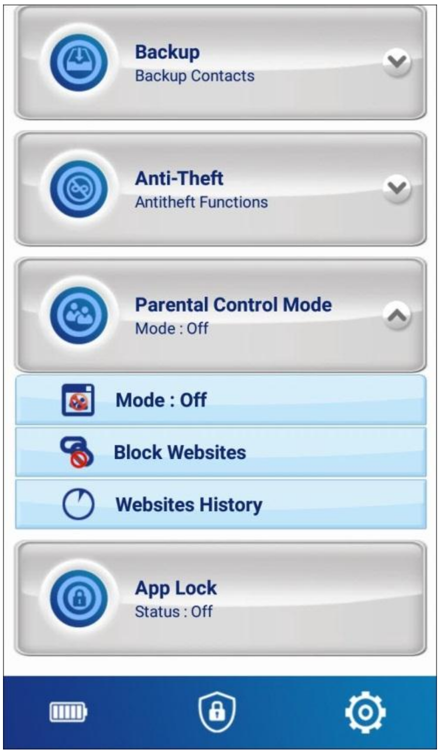
Data wipe

This option will allow you to delete all your Contacts and Selected data from the device via Cloud portal.

Refer to https://anti-theft.escanav.com for more details.

Parental Control Mode

This feature protects your device by restricting access to unauthenticated website. This module provides an extra layer of protection to your device by blocking access to specific category of websites. Through SafeSearch feature you can filter out explicit content in Google's search results page. For the first time it will ask you for the secret code to configure this option as per user requirement.

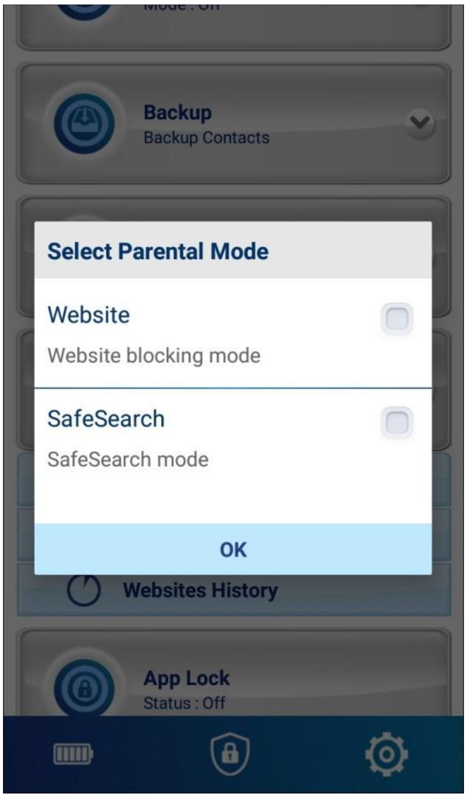


Parental Control Mode module has following options to configure:

- Mode
- Block Websites
- Websites History

Mode

It comprises of following options:



Select Parental Mode

Website □
Website blocking mode

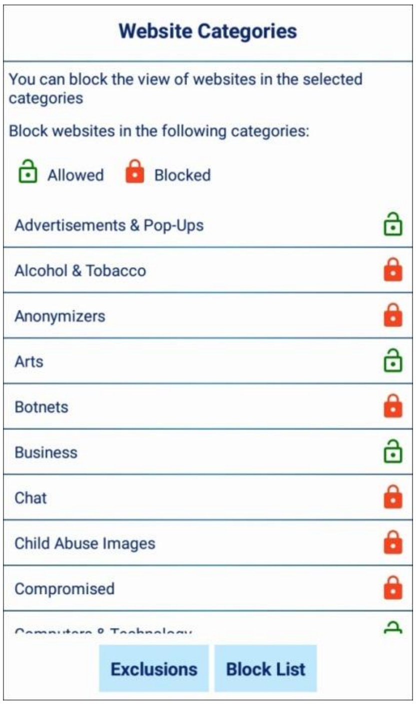
SafeSearch □
SafeSearch mode

OK

- **Website**: This mode allows you to block the websites categories based on the configuration made in the Block Websites tab.
- **SafeSearch**: It sets the chrome browser to the safesearch mode, and helps to filter out explicit content in Google search results.

Block Websites

It displays the list of pre-defined categories of websites that are blocked and also display the categories of the websites that are allowed. The website blocking feature is only supported while using the default Android browser and Chrome Browser. Block Website settings will be applied only when Parental Control Mode is set as Website.



Website Categories

You can block the view of websites in the selected categories

Block websites in the following categories:

🔓 Allowed 🔒 Blocked

Advertisements & Pop-Ups	🔓
Alcohol & Tobacco	🔒
Anonymizers	🔒
Arts	🔓
Botnets	🔒
Business	🔓
Chat	🔒
Child Abuse Images	🔒
Compromised	🔒
Computers & Technology	🔓

NOTE	🔒: This indicates that website is blocked
	🔓: This indicates that website is allowed

Exclusions

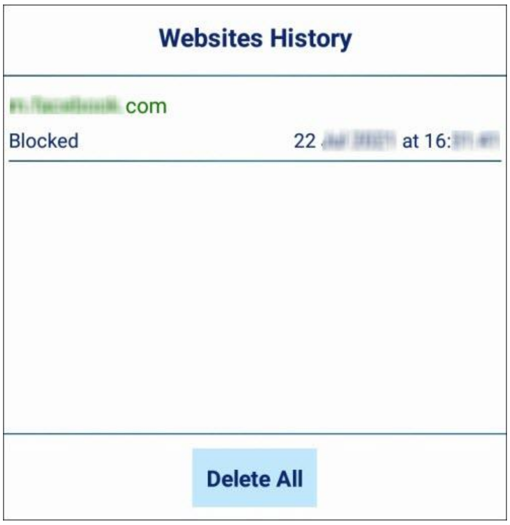
- This option allows users to exclude few specific website or webpages from view by adding them to exclusions list.
- To add website in Exclusion list, follow the below steps:
    1. Tap on **Exclusions**. Tap on **Add**.
    2. Enter the website address and tap on **Save**.
- The specified website will be allowed to view even if it is in the block category.

Block List

- This option lets you block the particular websites and webpages by adding them in the block list.
- To add websites or webpages in Block List follow the below steps:
    1. Tap on **Block List**. Tap on **Add**.
    2. Enter the website address and tap on **Save**.
- Access to the added website will be restricted.

Websites History

This option displays a list of blocked and allowed websites, along with the date and time.



Websites History

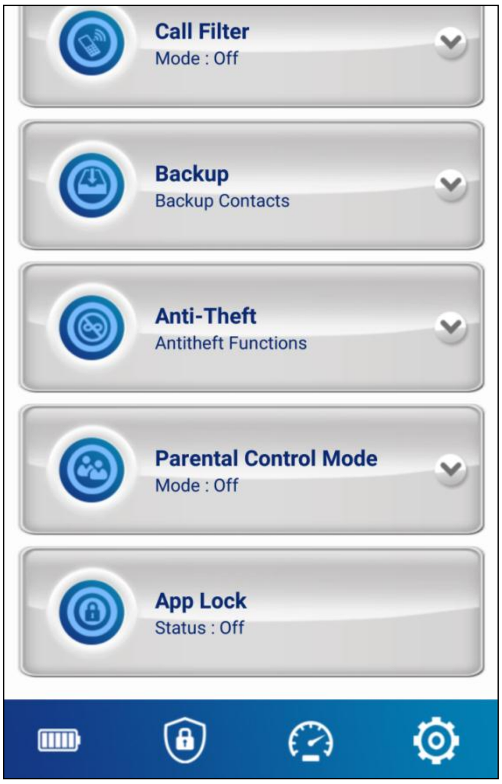
[redacted].com

Blocked 22 [redacted] at 16:[redacted]

To delete website history, tap on **Website History** > **Delete All**.

App Lock

This feature allows user to lock the application which contain confidential data on their device. Locked application will ask for password to open it. To get admin rights on App Lock module it will ask you secret code. To enable this option select the checkbox of App Lock Status.



Call Filter
Mode : Off

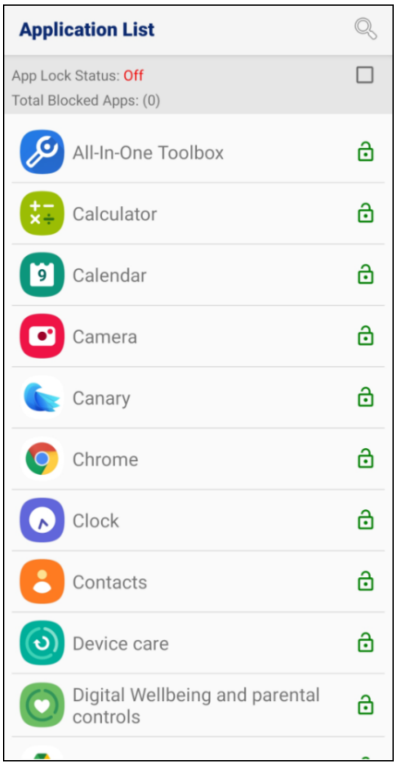
Backup
Backup Contacts

Anti-Theft
Antitheft Functions

Parental Control Mode
Mode : Off

App Lock
Status : Off

Tap on **App Lock**. Following screen appear.



Application List

App Lock Status: Off □
Total Blocked Apps: (0)

- All-In-One Toolbox 🔓
- Calculator 🔓
- Calendar 🔓
- Camera 🔓
- Canary 🔓
- Chrome 🔓
- Clock 🔓
- Contacts 🔓
- Device care 🔓
- Digital Wellbeing and parental controls 🔓

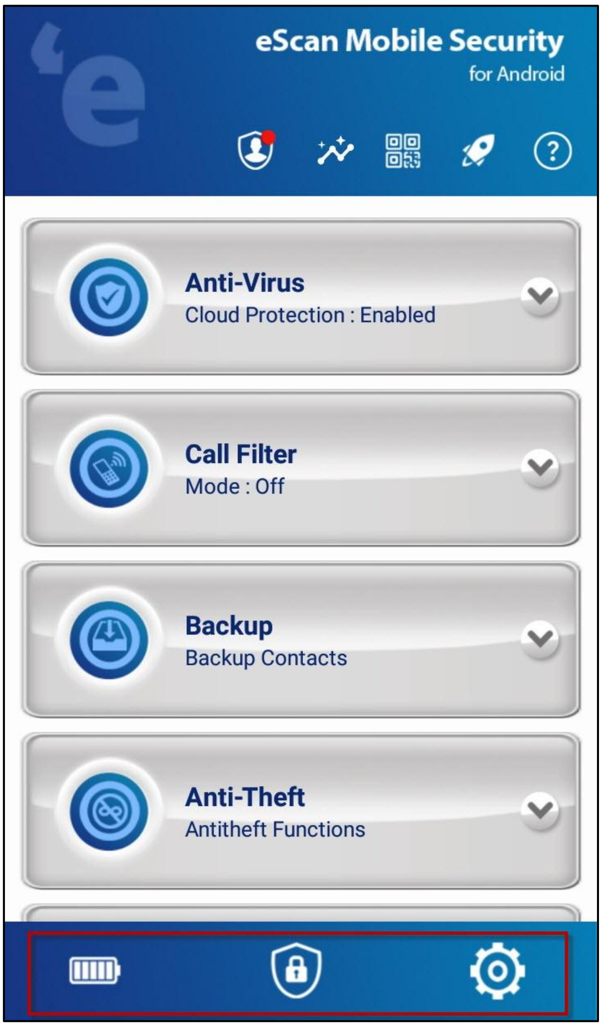
NOTE	🔒: This indicates that application is locked
	🔓: This indicates that application in unlocked

By default, the App Lock feature is Off. To enable this feature simply select the checkbox of **App Lock Status**. User can unlock the application by entering valid PIN. At the top, it displays the number of blocked apps.

Quick Tools

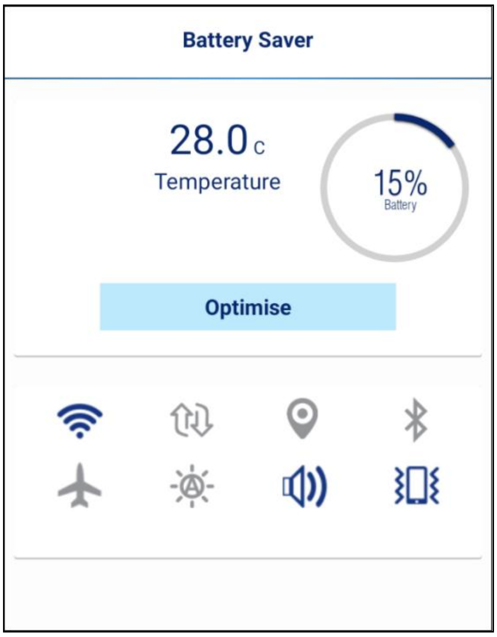
The eScan Mobile security dashboard gives quick access to the following tools present at bottom of the screen:

- Battery Saver
- Privacy Advisor
- Additional Setting



Battery Saver

The Battery Saver feature helps to preserve power of device. Battery Saver option displays the status of Wi-Fi, Mobile Data, Location, Bluetooth, etc. User can optimize the battery by disabling the device features to save battery.



Battery Saver

28.0 c Temperature

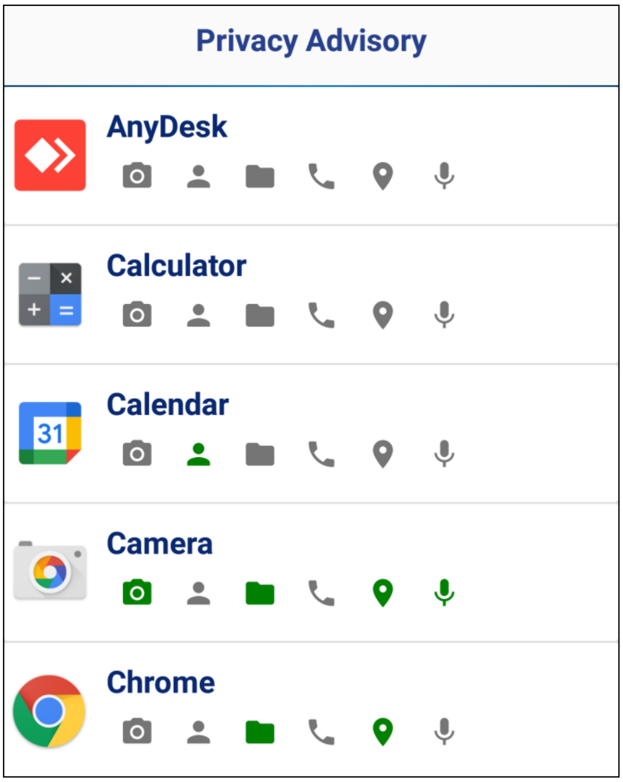
15% Battery

The percentage of battery and temperature of battery are indicated. It also enables you to configure following options in the Battery Saver:

- Wi-Fi
- Mobile Data
- Location
- Bluetooth
- Airplane Mode
- Auto-Brightness
- Device Volume
- Vibration Mode

Privacy Advisory

This feature helps in keeping track of permission enabled for the application installed in your device. It lets you monitor the security level of the applications. User can change permissions for a single app or by permission type using device settings. Tap on any permission category, it will show you list of applications using those permission. Further you can also tap on particular application to see list of permissions used by that application.



Privacy Advisory

AnyDesk

Calculator

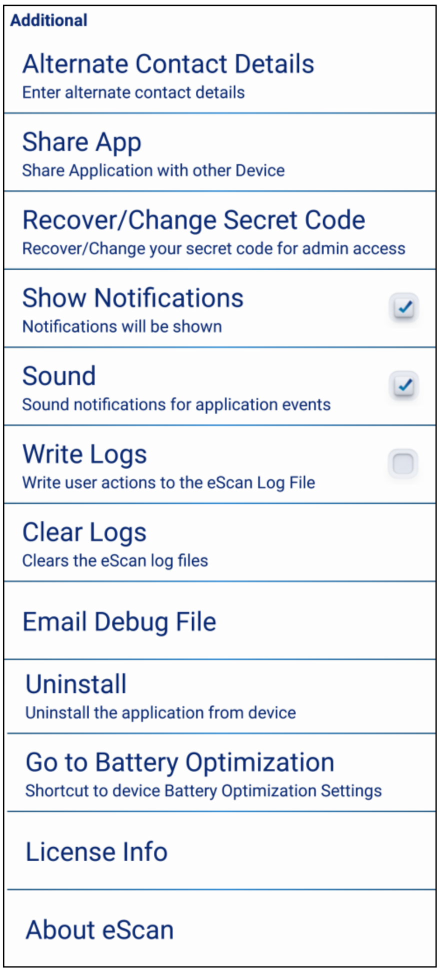
Calendar

Camera

Chrome

Additional Settings

This section contains information about the additional settings available in eScan Mobile Security application, such as changing the secret code, sharing eScan app, clear logs, activating and deactivating notifications, and sound notifications. User can configure the following settings as per their requirement.



Additional

Alternate Contact Details
Enter alternate contact details

Share App
Share Application with other Device

Recover/Change Secret Code
Recover/Change your secret code for admin access

Show Notifications ☑
Notifications will be shown

Sound ☑
Sound notifications for application events

Write Logs □
Write user actions to the eScan Log File

Clear Logs
Clears the eScan log files

Email Debug File

Uninstall
Uninstall the application from device

Go to Battery Optimization
Shortcut to device Battery Optimization Settings

License Info

About eScan

Alternate Contact Details

Enter a valid email address. This email address is used by SIM Watch and Lock Watch feature to send mail.

Share App

eScan Mobile Security allows users to share eScan application installed on their device with other nearby devices through various mediums.

Recover/Change Secret Code

It lets you recover or change secret code. You can change the secret code that you have set at the time of installing eScan Mobile Security application on your device.

Show Notifications

Notifications help you to view the eScan Mobile Security status icon on the status bar and eScan Mobile Security protection status under notification bar.

NOTE	☑: It indicates notification is in enabled mode, eScan Mobile Security Notification will be displayed. ☐: It indicates notification is in disabled mode, eScan Mobile Security Notification will not be displayed.

Sound

A sound will play, whenever notification is raised for threats or malware detection by eScan Mobile Security. User can enable or disable the option to play sound for notification alerts for such events. It is recommended that you enable this option to play sound notification alerts.

NOTE	☑: It indicates sound notification is in enable mode, eScan Mobile Security Notification will be played sound whenever threat detected. ☐: It indicates sound notification is in disabled mode. No sound notification will be played whenever any threats are detected.

Write Logs

It enables you to create logs on usage, infections and scanning, these logs are stored in the eScan_Mobile/YYYY-MMDD (Date wise folders). Logs will be created in date-wise folders and saved for 7 days and will be cleared as FIFO (First In First Out) basis.

NOTE	☑: It indicates the Write logs is in enable mode, eScan will create log. ☐: It indicates the Write logs is in disable mode. eScan will not create any log.

Clear Logs

It enables you to clear all the log files generated by the application. Before deleting it will prompt you for confirmation.

Email Debug File

This option is enabled by default. It lets you share the debug file through e-mail to eScan support team, if you face any kind of issue in the application.

Uninstall

This option lets you uninstall the eScan application. It will ask you for the confirmation before uninstallation take place.

Go to Battery Optimization

This selection will take you direct to the battery optimization setting, where you can configure it as per requirement.

License Info

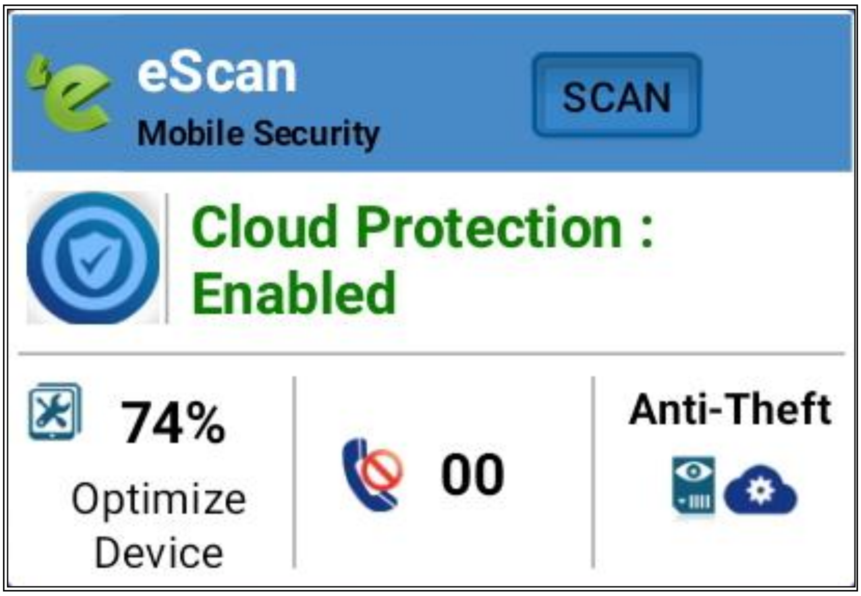
This option gives you information of App version, IMEI number, Android ID, MAC address, Install/Expiry Date, and License Key. After the expiry of the current key you can register new license key here. For more details of registration, click here.

About eScan

Tap this option to view eScan information, which includes the current version number of the product. It also provides an e-mail address for contacting eScan and copyright information.

eScan Widget

eScan Widgets are installed automatically in widgets on installing eScan Mobile Security app on device. It gives quick access to the scan and update options for virus scanning and downloading eScan antivirus signature updates. Furthermore, it displays the device optimization status in percentage. It also provides protection status and Anti-theft status (Enable or Disable).



To view the eScan widgets on your device, follow the below given steps:

- Press and hold on Home screen of your device.
- Tap on the widget icon which appears on the home screen.
- Tap on the eScan widget icon present in the widget.
- Drag and drop the eScan widget to home screen of your device for quick access.

Contact Us

We offer 24/7 free online technical support to our customers through email and live chat. We also provide 24/7 free telephonic service to customers. Before you contact technical support team, ensure that your system meets all the requirements and you have Administrator access on it. Also, ensure that a qualified person is available at the system in case it becomes necessary to replicate the error/situation.

Chat Support

The eScan Technical Support team is available round the clock to assist you with your queries. You can contact our support team via Live Chat by clicking here.

Forum Support

You can even join the MicroWorld Forum to discuss eScan related problems with eScan experts by clicking here.

Email Support

If you have any queries, suggestions and comments regarding our products or for this User Guide, please write to us at support@escanav.com.

Sales Enquiry

The eScan Sales Enquiry team helps you out from any type of query regarding product or this User guide, Please write to us at sales@escanav.com.

eScan Wikipedia/help

You will get more detailed information about the product from eScan Wikipedia/help page by clicking it: https://www.escanav.com/wiki