ESET MOBILE SECURITY

FOR ANDROID

User Guide

(intended for product version 3.0 and higher)

Click here to download the most recent version of this document

ESET **MOBILE SECURITY**

Customer Care: www.eset.com/support

REV. 22. 10. 2014

Contents

1. Introduction

ESET Mobile Security is a complete security solution that safeguards your device from emerging threats and phishing pages, filters unwanted calls and messages and allows you to take control of your device remotely in the event of loss or theft.

1.1 What's New

The following updates and improvements have been introduced in ESET Mobile Security version 3:

- Integration of ESET Anti-Theft into the my.eset.com portal
- Location tracking – device location is now displayed on a map
- Camera pictures – front and rear camera snapshots are now taken automatically when the device is marked as missing
- On-screen message – ability to send a custom message to the device finder
- Automatic lock – device will be locked when suspicious activity is detected or the device is marked as missing
- Device low on battery – when your device is near critical battery level, ESET Mobile Security sends its latest location to my.eset.com
- Play siren – trigger a loud siren remotely from my.eset.com if you think your device is nearby
- Security password change – ability to change your Security password from my.eset.com in case you forget it
- Remote wipe – wipe all important data on your device from my.eset.com
- Ignored Threats – a list of threats that will be ignored in future scans
- On-Charger Scan – a scan will start automatically when the device is in an idle state and connected to a charger

1.2 System Requirements

To install ESET Mobile Security, your Android device must meet the following minimum system requirements:

Operating system: Android 2.3 (Gingerbread) and later
Touchscreen resolution: minimum 240x320 px, recommended 320x480 px
CPU: 500 MHz (ARM7+)
RAM: 128 MB
Free internal storage space: 20 MB
Internet connection

NOTE: Dual SIM and rooted devices are not supported. Some features (for example, Anti-Theft and SMS & Call Filter) are not available on tablets that do not support calling and messaging.

2. Installation

To install ESET Mobile Security, use one of the following methods.

NOTE: If you already have an active Username and Password or Activation key issued by ESET, please download ESET Mobile Security from the ESET website.

2.1 Installation from ESET website

Download ESET Mobile Security by scanning the QR code below using your mobile device and an application such as QR Droid or Barcode Scanner:

Alternatively, you can download the ESET Mobile Security installation APK file on your computer:

1. Download the file from the ESET website.
2. Copy the file to your device via Bluetooth or USB.
3. Tap the Launcher icon on the Android home screen, or go to **Home** > **Menu** and tap **Settings** > **Applications**. Make sure that applications from **Unknown sources** are allowed on your device.
4. Locate the APK file using a file browsing application such as ASTRO File Manager or ES File Explorer.
5. Open the file and tap **Install**. Once the application is installed, tap **Open**.

2.2 Installation from Google Play

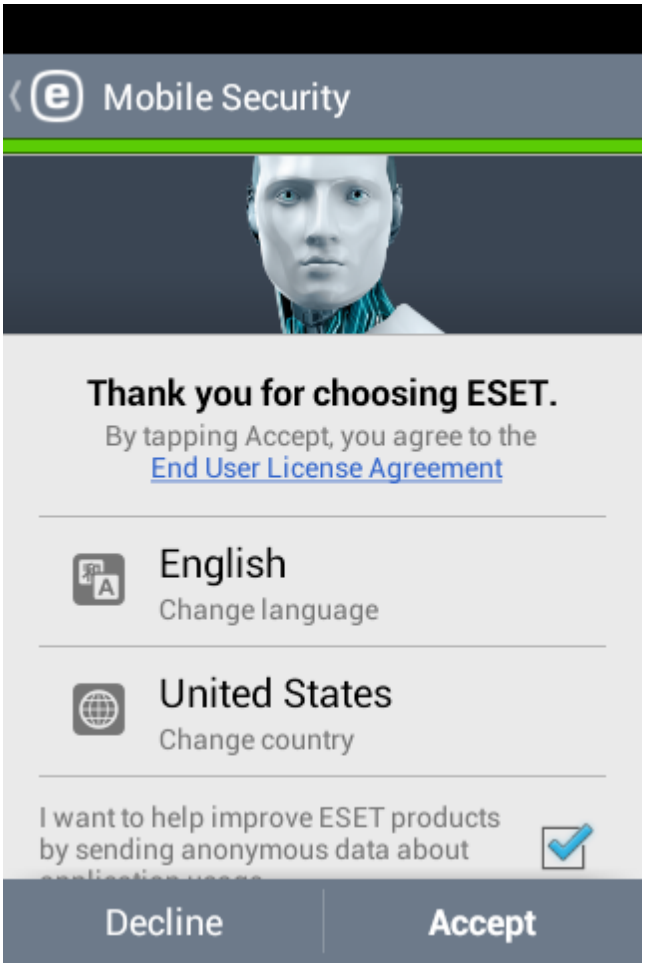
Open the Google Play Store application on your Android device and search for ESET Mobile Security (or just Eset).

Alternatively, you can install the program by scanning the QR code below using your mobile device and an application such as QR Droid or Barcode Scanner:

2.3 Installation from Amazon

Open the Amazon application on your Android device and search for ESET Mobile Security (or just Eset).

2.4 Start-up wizard

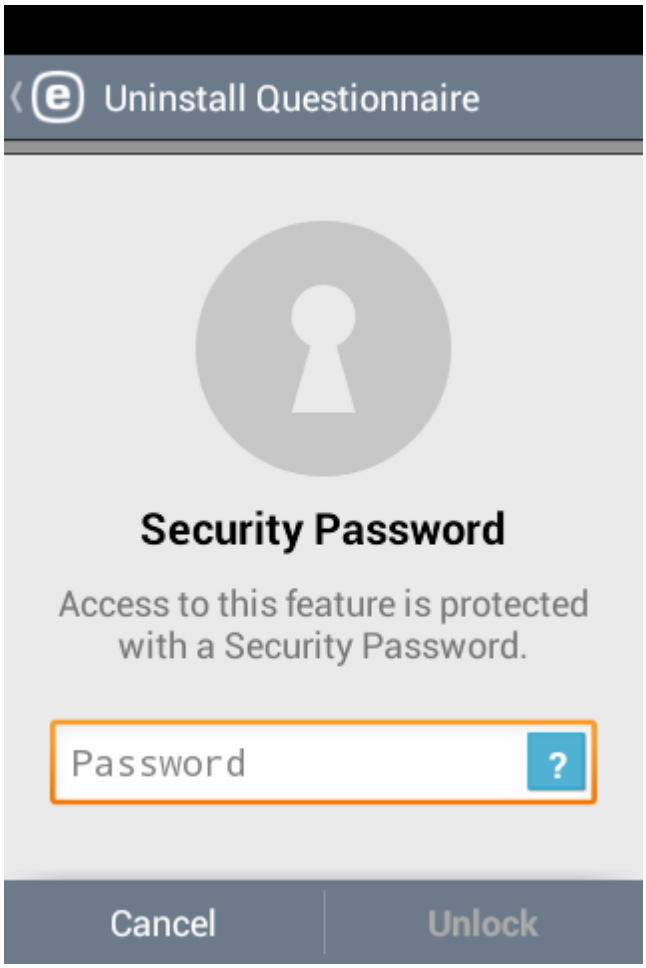


Once the application is installed on your device, follow the prompts from the start-up wizard:

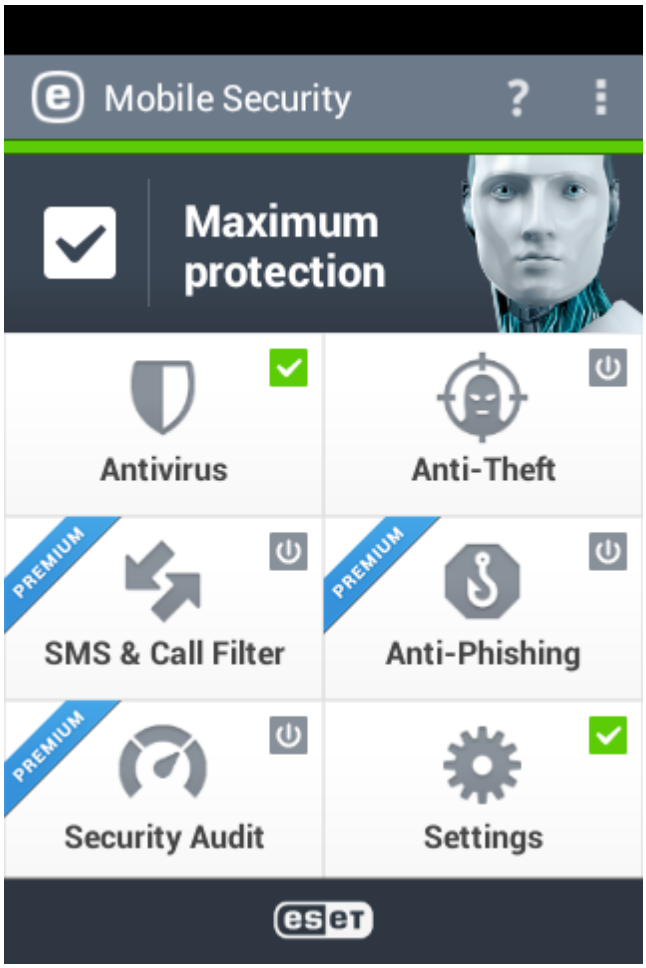
1. Select the language you want to use in ESET Mobile Security.
2. Select the country you currently reside in.
3. If you want to help improve ESET products by sending anonymous data about application usage, select the appropriate option.
4. Tap **Accept**. By doing this, you agree to the End User License Agreement.
5. Choose if you want to participate in ESET Live Grid. To read more about ESET Live Grid, see this section 8.
6. Tap **Next**.
7. Choose whether you want ESET Mobile Security to detect Potentially unwanted applications. More details about such applications can be found in this section 8.
8. Tap **Next**.
9. Tap **Finish**.

2.5 Uninstallation

If you want to uninstall ESET Mobile Security, use the Uninstall wizard available in the ESET Mobile Security main menu under **Settings** > **Uninstall**. If you enabled Uninstall protection, you will be asked to enter your Security Password.



3. License



After a successful installation, ESET Mobile Security must be activated. To open the **License** section, tap the Menu icon in the ESET Mobile Security main screen (or press the **MENU** button on your device) and tap **License**.

Activation methods vary depending on whether you downloaded ESET Mobile Security from the ESET website, Amazon or Google Play.

- **Free Trial** - select this option if you do not have a license and would like to evaluate ESET Mobile Security before making a purchase. Fill in your **Email Address** to activate ESET Mobile Security for a limited time. You will receive a confirmation email after successfully activating the product. You can only activate a trial license once per device.
- **Activate Application Using your Username and Password** - if you purchased your product from an ESET distributor, you received a Username and Password with your purchase. Enter the information you received in the **Username** and **Password** fields.
- **Activate Application Using your Activation Key** - if you acquired your program with a new device (or as a boxed product), you received an Activation key with your purchase. Enter the information you received in the **Activation Key** field and then enter your current email address in the **Email Address** field. Your new authentication data (Username and Password) will automatically replace the Activation key and will be sent to the email address you specified.
- **Purchase License** - select this option if you do not have a license and would like to buy one. You will be redirected to the webpage of your local ESET distributor.

Each license is valid for a fixed period of time. After the license expires, you will be asked to renew it (the program will notify you in advance).

NOTE: During activation, the device must be connected to the Internet. A small amount of data will be downloaded.

4. Antivirus

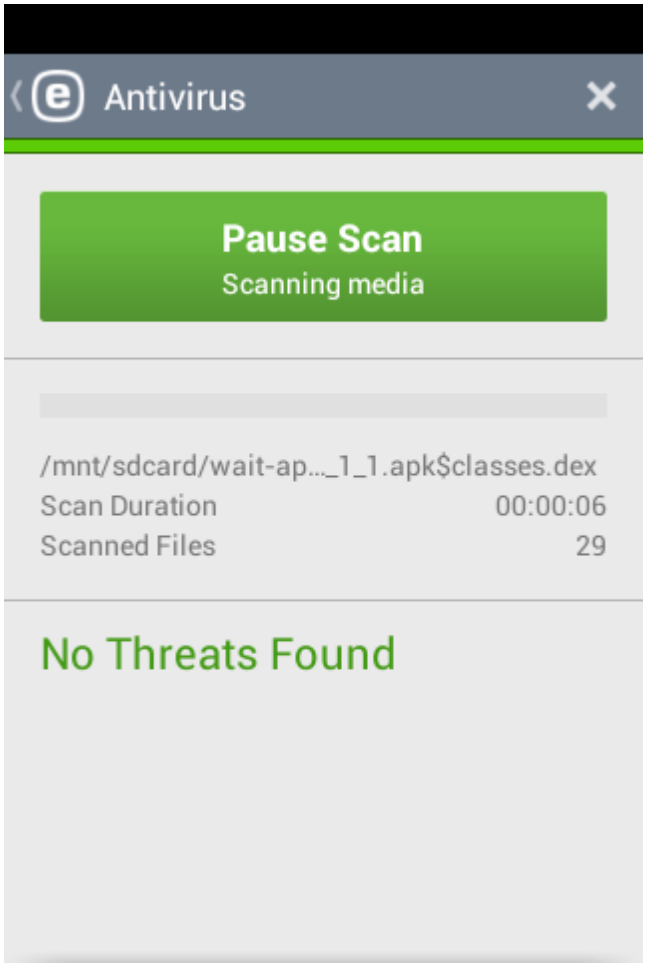
The Antivirus module safeguards your device against malicious code by blocking threats and then cleaning or quarantining them.

Scan Device

Scan Device can be used to check your device for infiltrations.

Certain predefined file types are scanned by default.
A complete device scan checks the memory, running processes and their dependent dynamic link libraries as well as files that are part of internal and removable storage. A brief summary of the scan will be saved to a log file available in the **Scan Logs** section.

If you want to abort a scan already in progress, tap the icon.



Scan Level

There are 3 different scan levels to choose from:

- **Quick** - if you select this, ESET Mobile Security will only scan installed applications, DEX files (executable files for Android OS), SO files (libraries) and ZIP files with a maximum scanning depth of 3 nested archives.
- **Smart** - Smart scan will scan SD card content in addition to the file types scanned by the quick scan.
- **Deep** - all file types regardless of their extension will be scanned both in internal memory and SD card.

Automatic Scans

In addition to On-demand device scan, ESET Mobile Security also offers automatic scans. To learn how to use On-Charger Scan and Scheduled Scan, read this section 7.

Quarantine

The main purpose of the quarantine is to safely store infected files. To read more, see the Quarantine 8 section.

Ignored Threats

To learn about this feature, see this section 8.

Scan Logs

The **Scan Logs** section contains comprehensive data about completed scans in the form of log files. More information can be found in this chapter 8.

Update Threat Database

By default, ESET Mobile Security includes an update task to ensure that the program is updated regularly. To run the update manually, tap **Update Threat Database**.

NOTE: To prevent unnecessary bandwidth usage, updates are issued as needed when a new threat is added. While updates are free with your active license, you may be charged by your mobile service provider for data transfers.

Detailed descriptions of the Antivirus **Advanced Settings** can be found in the Advanced Settings 8 section.

4.1 Automatic Scans

Scan Level

There are 3 different scan levels to choose from. This setting will apply to On-Charger Scan and Scheduled Scan:

- **Quick** - if you select this option, ESET Mobile Security will only scan installed applications, DEX files (executable files for Android OS), SO files (libraries) and ZIP files with a maximum scanning depth of 3 nested archives.
- **Smart** - Smart scan will scan SD card content in addition to the file types scanned by the quick scan.
- **Deep** - all file types regardless of their extension will be scanned both in internal memory and SD card.

On-Charger Scan

When this is selected, scan will start automatically when device is in the idle state, fully charged and connected to a charger.

Scheduled Scan

Scheduled Scan allows you to run the Device scan automatically at a predefined time. To schedule a scan, tap the button next to **Scheduled Scan** and specify the dates and times for the scan to be launched. By default, all days of the week are selected.

4.2 Quarantine

Files should be quarantined if they cannot be cleaned, if it is not safe or advisable to delete them or if they are being falsely detected by ESET Mobile Security.

Files stored in the quarantine can be viewed in a log that displays the name and original location of the infected file along with the date and time that it was quarantined.

If you want to restore a quarantined file to its original location, tap the file and then tap the icon. We do not recommend that you regularly restore quarantined files.

To permanently remove a quarantined file from your device, tap the file and then tap the icon.

NOTE: If you quarantine a suspicious application but later choose install it, the application will automatically be removed from the quarantine.

4.3 Ignored Threats

During the scan, you can add a new threat to the whitelist. This will cause that threat to be ignored in future scans.

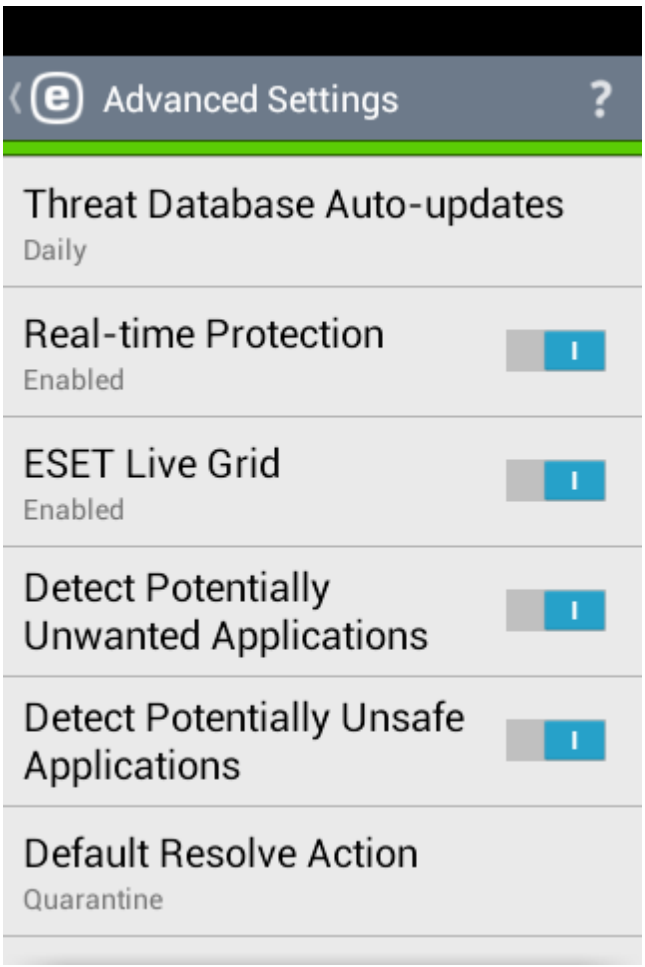
4.4 Scan Logs

Scan Logs are created after each Scheduled scan or manually triggered Device scan.

Each log contains:

- date and time of the event
- duration of the scan
- number of scanned files
- scan result or errors encountered during the scan

4.5 Advanced Settings



Threat Database Auto-updates
This option allows you to set the time interval on which threat database updates are automatically downloaded. These updates are issued as needed when a new threat is added to the database. We recommend that you leave this setting at the default value (daily).

Real-time Protection
This option allows you to enable/disable the Real-time scanner. This scanner launches automatically at system startup and scans files that you interact with. It automatically scans the *Download* folder, all *.apk* installation files and all files on the SD card after it is mounted.

ESET Live Grid
Built on the ThreatSense.Net advanced early warning system, **ESET Live Grid** is designed to provide additional levels of security to your device. It constantly monitors your system's running programs and processes against the latest intelligence collected from millions of ESET users worldwide. Additionally, your scans are processed faster and more precisely as the ESET Live Grid database grows over time. This allows us to offer greater proactive protection and scanning speed to all ESET users. We recommend that you activate this feature. Thank you for your support.

Detect Potentially Unwanted Applications
An unwanted application is a program that contains adware, installs toolbars, traces your search results or has other unclear objectives. There are some situations where you may feel that the benefits of the unwanted application outweigh the risks. For this reason, ESET assigns such applications a lower-risk category compared to other types of malicious software.

Detect Potentially Unsafe Applications
There are many legitimate applications whose function is to simplify the administration of networked devices. However, in the wrong hands, they may be misused for malicious purposes. The **Detect Potentially Unsafe Applications** option allows you to uncover such threats. “Potentially unsafe applications” is the classification used for commercial, legitimate software. This classification includes programs such as remote access tools, password-cracking applications and keyloggers.

Default Resolve Action
This setting determines the action that will be performed after the scan is complete and threats are found. If you select **Remove**, the infected file will be removed. If you select **Quarantine**, the infected file will be moved to the Quarantine 8.

Update server
In this option, you can switch to update threat database from the **Pre-release server**. Pre-release updates have gone through thorough internal testing and will be available to the general public soon. You can benefit from enabling pre-release updates by having access to the most recent detection methods and fixes. However, pre-release updates might not be stable enough at all times. The list of current modules can be found in the About section: tap the Menu icon  in the ESET Mobile Security main screen (or press the **MENU** button on your device) and tap **About** > **Application version**. It is recommended that basic users leave the **Release server** option selected by default.

5. Anti-Theft

The Anti-Theft feature protects your mobile device from unauthorized access.

If you lose your device or someone steals it and replaces your SIM card with a new (untrusted) one, the device will automatically be locked by ESET Mobile Security and an alert SMS will be sent to user-defined phone number(s). This message will include the phone number of the currently inserted SIM card, the IMSI (International Mobile Subscriber Identity) number and the phone's IMEI (International Mobile Equipment Identity) number. The unauthorized user will not be aware that this message has been sent because it will automatically be deleted from your device's messaging threads. You can also request the GPS coordinates of your lost mobile device or remotely erase all data stored on the device.

NOTE: Certain Anti-Theft features (SIM Guard, Trusted Friends and SMS Text Commands) are not available on tablets that do not support messaging.

Version 3 of ESET Mobile Security integrates completely with ESET Anti-Theft protection through my.eset.com. This allows you to monitor your device activity from the ESET Anti-Theft online portal, lock the device, send custom messages to the device finder, trigger a loud siren or wipe device data remotely.

To start using Anti-Theft protection, tap **Anti-Theft** in the main program menu. A simple wizard will guide you through creating your Security password, enabling Uninstall protection, adding your SIM card as trusted, adding a Trusted friend, entering your contact details and enabling SMS text commands. Once these steps are complete, you can associate your device with your my.eset.com account.

5.1 my.eset.com

If you already have a my.eset.com account, tap **Already have an account?** and enter your email and password to sign in.

If you do not have a my.eset.com account, tap **Register** and fill out the registration form. Check your inbox for email confirmation and click the link to activate your account. Now you can enjoy the Anti-Theft security features managed from my.eset.com.

For further guidance on how to use Anti-Theft at my.eset.com, refer to online help - click **Help** in the top right corner of the screen.

5.2 Optimization

ESET Anti-Theft optimization is a measurable technical assessment of the security state of your device. ESET Anti-Theft protection will examine your system for the following issues:

- Location services turned off
- GPS satellites not used
- Screen lock not secured
- Mobile data not enabled
- Google Play Services not present

For each security issue, you can tap **Change settings** to navigate to the screen where you can resolve that specific issue. If you do not want ESET Mobile Security to report an issue as a problem, tap **Ignore this issue**.

5.3 SIM Guard

The **SIM Guard** section shows the list of trusted SIM cards that will be accepted by ESET Mobile Security. If you insert a SIM card not defined in this list, the screen will be locked and an alert SMS will be sent to your **Trusted friends**.

To add a new SIM card, tap the  icon. To read more, see this section 10.

To remove a SIM card from the list, touch and hold the entry and tap the  icon.

NOTE: SIM Guard is not available on certain CDMA and WCDMA mobile devices.

5.3.1 Adding a New Trusted SIM

Enter a **Name for the SIM card** (e.g. Home, Work) and its **IMSI** (International Mobile Subscriber Identity) number. IMSI is usually presented as a 15-digit long number printed on your SIM card. In some instances, it may be shorter.

5.4 Trusted Friends

In the **Trusted Friends** list, you can add or remove the phone numbers that will receive an alert SMS after an untrusted SIM card is inserted into your device. To add a new trusted friend, tap **Add from Contacts** and select a contact from your contact list.

If the person is not included in your contact list, tap the  icon. To read more, see this section 10.

To remove a contact from the list, touch and hold the contact and tap the  icon.

NOTE: If you are abroad, all phone numbers entered in the list must include the international dialing code followed by the actual number (e.g., +1610100100).

5.4.1 Adding a New Trusted Friend

Enter a friend's name and his/her phone number. If the contact contains more than one phone number, alert SMS will be sent to all associated numbers. If you want to allow this friend to reset your password in case you forget it, select the **Allow remote reset of the password** option.

5.5 SMS Text Commands

Remote SMS commands (lock, siren, find and wipe) will only work if **SMS Text Commands** are enabled.

If you lose your device and would like to lock it, send a Remote lock SMS from any mobile device to your phone number in the following form:
eset lock password
Replace *password* with your Security password. Once your device is locked, an unauthorized user will be required to enter your password to unlock it.

To lock your device and trigger a siren, send an SMS to your

mobile number in the following form:
eset siren password
The siren will start even if your device is set to mute.

If you want to request the GPS coordinates of your mobile device, send a text message to your mobile number or the unauthorized user's mobile number (if the SIM card was already replaced) in the following form:
eset find password
You will receive a text message with the GPS coordinates of your lost device including a link to that location on Google maps.

If you want to erase all data stored on your device and all currently inserted removable media, send a Remote wipe SMS to your device in the following form:
eset wipe password
All contacts, messages, emails, accounts, applications, SD card content, pictures, music and videos stored in the Android default folders will be permanently erased from your device.

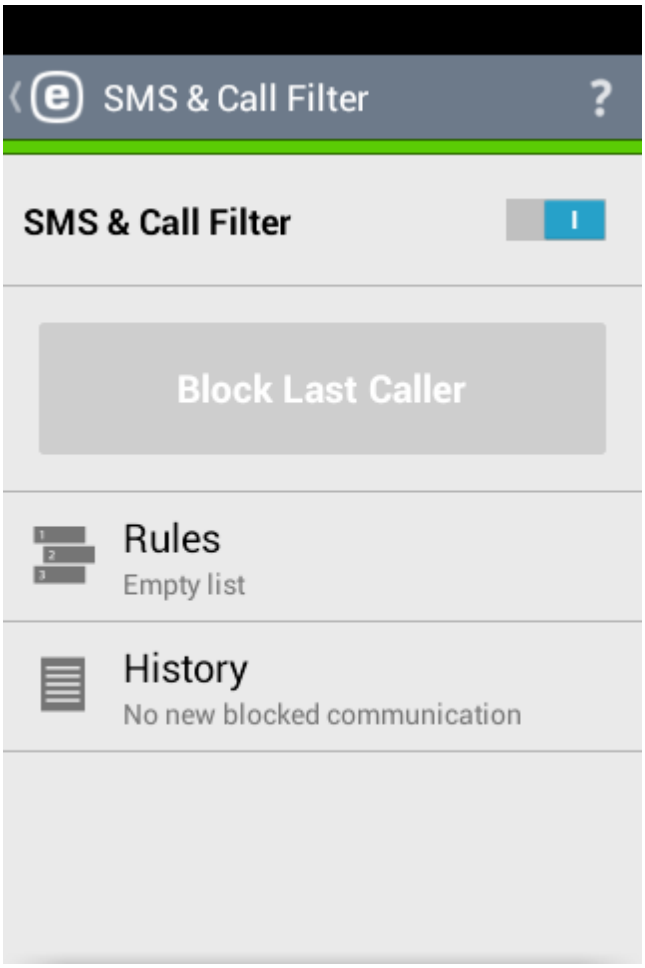
NOTE: Your password is case sensitive. Please make sure to enter the password exactly as you defined it during the Anti-Theft setup wizard.

5.6 My Contact Details

If you mark your device as missing on my.eset.com, the information from **My Contact Details** will be displayed on your locked device's screen to help the finder contact you.

Enter your name, device description, alternative contact number (for example, home or work phone number) or your email address.

6. SMS & Call Filter



SMS & Call Filter blocks incoming SMS/MMS messages and incoming/outgoing calls based on your rules.

Unsolicited messages usually include advertisements from mobile phone service providers or messages from unknown or unspecified users. The term *block message* refers to moving an incoming message to the **History** section automatically. No notification is displayed when an incoming message is blocked. The advantage of this is that you will not be bothered by unsolicited information, but can always check the logs for messages that may have been blocked by mistake.

NOTE: SMS & Call Filter does not work on tablets that do not support calling and messaging. SMS & Call Filter is not available for Android OS 4.4 (KitKat) devices, and will be disabled on devices where Google Hangouts is set as the primary application for SMS.

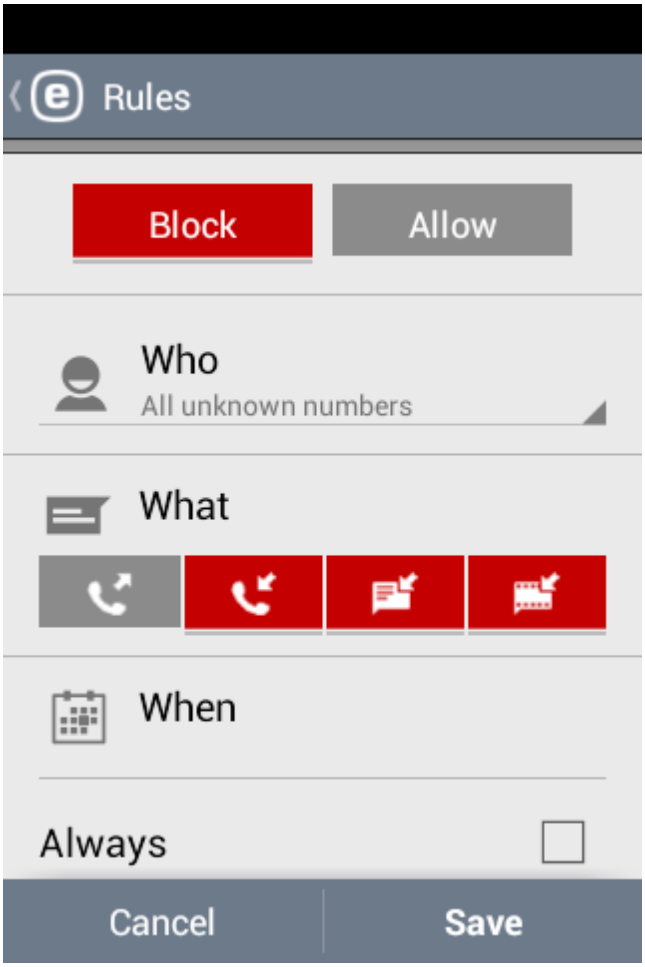
To block calls and messages from the last received phone number, tap **Block Last Caller**. This will create a new SMS & Call Filter rule.

6.1 Rules

To add a new rule, tap the + icon. More information about creating a new rule can be found in this section 12.

If you want to remove an existing rule entry from the **Rules** list, touch and hold the entry and tap the icon.

6.1.1 Adding a New Rule



Specify a group of phone numbers or a person. **All unknown numbers** will include the phone numbers not saved in your contact list. You can use this option to block unwelcome phone calls (e.g. "cold calls") or to prevent kids from dialing unknown numbers. The **All known numbers** option refers to all phone numbers saved in your contact list. **Hidden numbers** will apply to callers that have their phone number intentionally hidden via the Calling Line Identification Restriction (CLIR).

Specify which should be blocked or allowed:

- outgoing calls
- incoming calls
- incoming text messages (SMS) or
- incoming multimedia messages (MMS)

To apply the rule for a specified time only, deselect **Always** at the bottom and select the dates and times for which you want to apply the rule. By default, all days of the week are selected. This functionality might come handy if you do not want to be disturbed during the night or during the weekend.

NOTE: If you are abroad, all phone numbers entered in the list must include the international dialing code followed by the actual number (e.g., +1610100100).

6.2 History

In the **History** section, you can see the calls and messages blocked or allowed by the SMS & Call Filter. Each log contains the name of the event, corresponding phone number, date and time of the event. SMS and MMS message logs also contain the message body.

If you want to modify a rule related to the phone number or a contact that was blocked, select the entry from the list by tapping it and tap the  icon.

To remove the entry from the list, select it and tap the  icon. To remove more entries, touch and hold one of the entries, select the ones you want to remove and tap the  icon.

7. Anti-Phishing

The term *phishing* defines a criminal activity that uses social engineering (the manipulation of users in order to obtain confidential information). Phishing is often used to gain access to sensitive data such as bank account numbers, credit card numbers, PIN numbers or usernames and passwords.

We recommend that you keep **Anti-Phishing** enabled. All potential phishing attacks coming from websites or domains listed in the ESET malware database will be blocked and a warning notification will be displayed informing you of the attack.

Anti-Phishing integrates with the most common web browsers available on Android OS (e.g. Chrome or default Android web browser).

NOTE: Anti-Phishing will not protect you while browsing in private (incognito) mode.

7.1 History

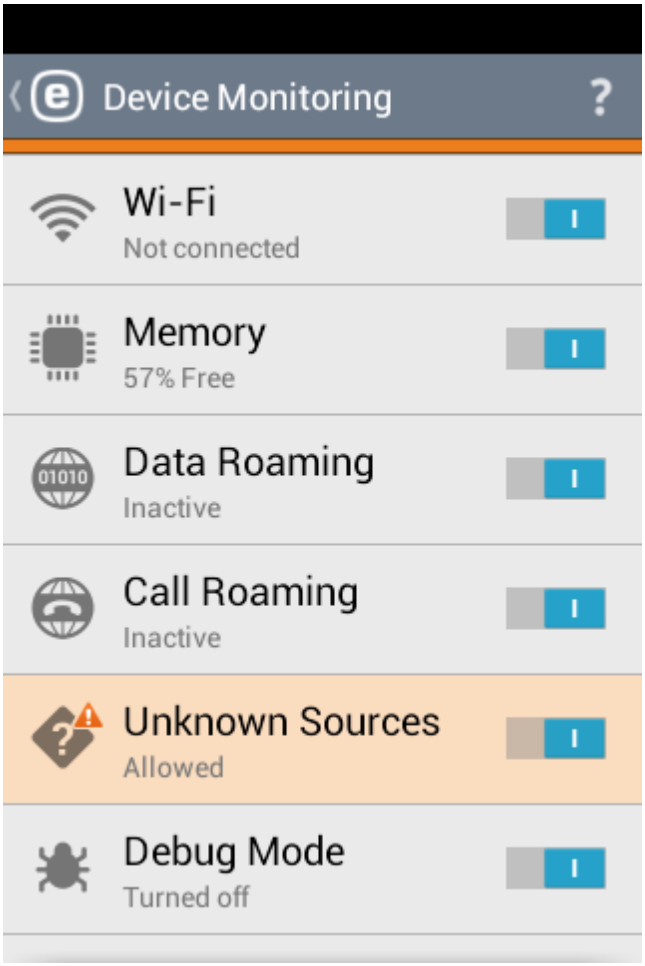
In the **History** section, you can see a list of all phishing attacks blocked by ESET Mobile Security.

8. Security Audit

Security Audit helps you monitor and change important device settings and permissions of installed applications to prevent security risks.

To turn on/off Security Audit and its specific components, use these buttons: 

8.1 Device Monitoring

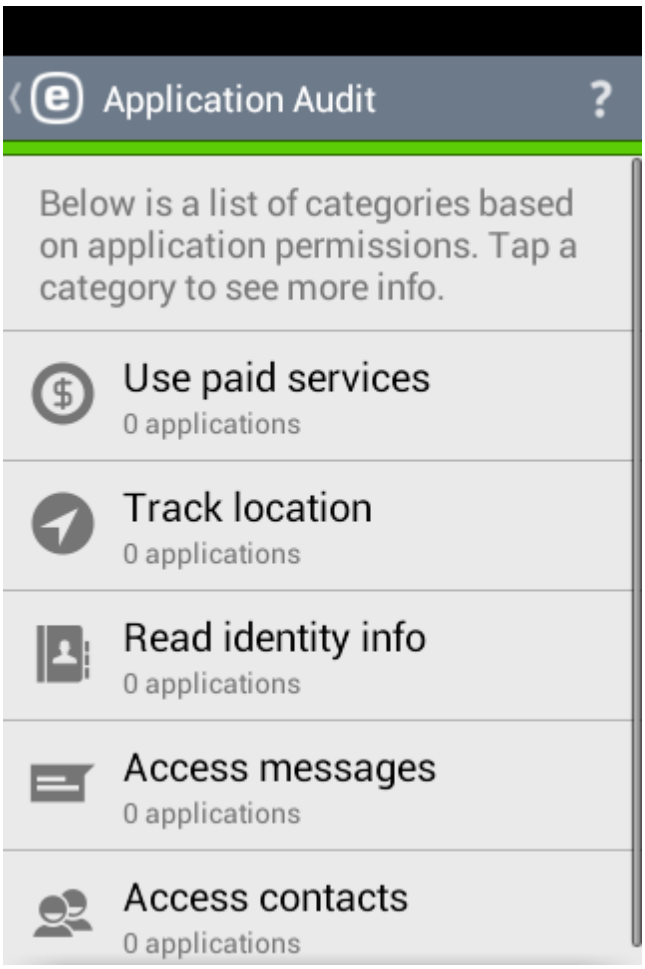


In the **Device Monitoring** section, you can define which device components will be monitored by ESET Mobile Security.

Tap each option to view a detailed description of the option and its current status.

Certain options like **Unknown Sources** and **Debug Mode** can be changed by tapping **Change Settings**. This will redirect you to the Android OS settings screen.

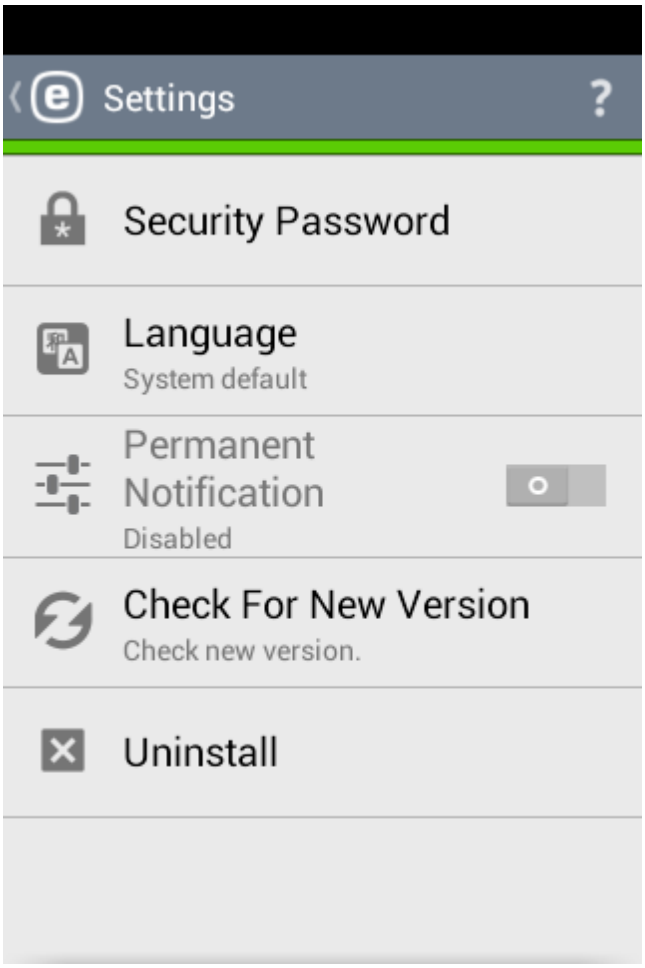
8.2 Application Audit



Some applications installed on your device might have access to services that cost you money, track your location or read your identity info, contacts or text messages. ESET Mobile Security provides an audit of these applications.

In the **Application Audit** section, you can see the list of applications sorted by categories. Tap each category to see its detailed description. Permissions details of each application can be accessed by tapping a particular application.

9. Settings



Security Password
This option allows you to set a new security password or change the existing one. To read more, see the Security Password 16 section.

Language
By default, ESET Mobile Security is installed in the language which is set on your device as a system locale (in the Language and keyboard settings of Android OS). To change the language of the application user interface, tap **Language** and select the language of your choice.

Permanent Notification

ESET Mobile Security displays its notification icon in the top left corner of the screen (Android status bar). If you do not want this icon to be displayed, deselect **Permanent Notification**.

Check for New Version
For maximum protection, it is important to use the latest version of ESET Mobile Security. Tap **Check for New Version** to see if there is a newer version available for download.

Uninstall
If you want to uninstall ESET Mobile Security, use the **Uninstall** wizard. The ESET Mobile Security and quarantine folders will be permanently deleted.

9.1 Security Password

Your **Security Password** is required to unlock your device, access password protected features (for example, Anti-Theft) and uninstall ESET Mobile Security. The **Reminder phrase** (if set) displays a hint to help you remember your password.

If you forget your password, you can send an SMS from the mobile number saved in your Trusted Friends 10 list to your mobile number. This SMS must be in the following form:
eset remote reset
Your password will be reset and you will be prompted to define a new password.

If you did not have a Trusted Friend defined prior to locking your device, you can send a password reset request. This option will become active on your locked screen after 2 unsuccessful attempts to unlock your device. You will receive an email containing an unlock code at your Google account email address or an email address defined during the purchase or activation of ESET product. Enter the unlock code on your locked screen. Once your device is unlocked, define a new security password in **Settings** > **Password**.

Additionally, you can change your Security password at my.eset.com. After logging in, select your device, click **Settings** and type a new password.

IMPORTANT: Please choose your password carefully. To increase security and make your password harder for others to guess, use a combination of small letters, capital letters and numbers.

10. Customer Care

ESET Customer Care specialists are available to provide administrative assistance or technical support related to ESET Mobile Security or any other ESET product.

To send a support request directly from your device, tap the Menu icon  in the ESET Mobile Security main screen (or press the **MENU** button on your device) and tap **Customer Care** > **Customer Care**. Fill in all the required fields.

ESET Mobile Security includes advanced logging functionality to help diagnose potential technical issues. To provide ESET with a detailed application log, make sure that **Application log** is selected (default). Send your request by tapping **Submit**. ESET Customer Care specialists will contact you at the email address you provided.