ESET® MOBILE SECURITY for Android

User Guide

(intended for product version 3.5 and higher)

Click here to download the most recent version of this document

ESET MOBILE SECURITY

Customer Care: http://support.eset.com/

REV. 2/3/2017

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.

Major features include:

- Antivirus
- Anti-Theft
- Anti-Phishing
- Integration with My Eset portal
- SMS & Call Filter
- Security Audit
- Security Report

1.1 What's new in version 3.5

The following updates and improvements have been introduced in ESET Mobile Security version 3.5:

- Proactive protection
- Improved Anti-Phishing
- Security Report
- System permissions easily accessible from ESET Mobile Security
- Last known device location saved in ESET Anti-Theft before the device battery loses power

1.2 Minimum system requirements

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

- Operating system: Android 4 (Ice Cream Sandwich) or later
- Touchscreen resolution: minimum 480x800 px
- CPU: ARM with ARMv7+ instruction set, x86 Intel Atom
- RAM: 128 MB
- Internal storage free space: 20 MB
- Internet connection

NOTE: Dual SIM and rooted devices are not supported. Anti-Theft and SMS & Call Filter is not available on tablets that do not support calling or messaging.

2. Installation

ESET Mobile Security is available for downloading on these distribution channels:

Google play Google Play – this application receives regular updates via Google Play

eset ESET website – this application receives updates from the ESET version check update system

amazon Amazon Appstore

To protect your personal information and your Android device's resources, ESET Mobile Security will need to have access to your device's functions and in some cases have control over them. For detailed explanations of each permission type and how it's used, see the table in this Knowledgebase article:

http://support.eset.com/kb2711/#PrivacyPolicy
(The article is not available in all languages.)

2.1 Download from Google Play

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

Alternatively, follow the link or scan the QR code below using your mobile device and a QR scanning application:

Google play https://play.google.com/store/apps/details?id=com.eset.ems2.gp

2.2 Download from the ESET website

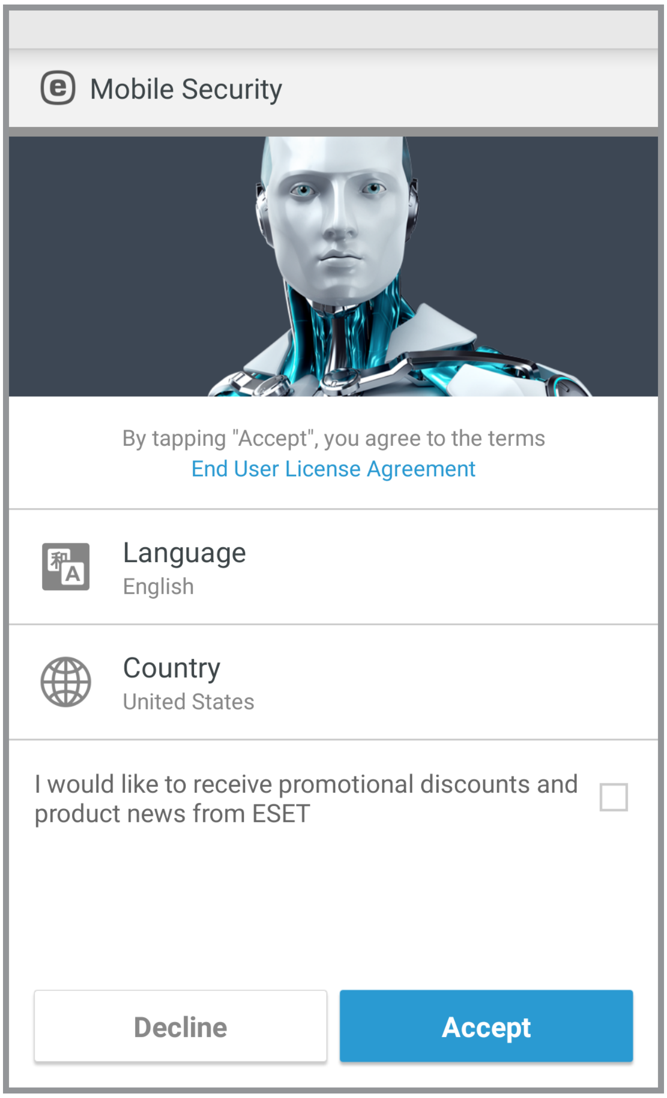
The availability of the web version varies depending on your region.

1. Download the APK installation file from the ESET website.
2. Make sure that applications from unknown sources are allowed on your device. To do so, tap the Launcher icon ▦ on the Android home screen (or navigate to Home > Menu). Tap **Settings** > **Security**. The check box next to **Unknown sources** must be selected.
3. Open the file from the Android notification area or locate it using a file browser. The file is usually saved to the Download folder.
4. Tap **Install** and then **Open**.

2.3 Start-up wizard

Once the application is installed, follow the on-screen prompts in the start-up wizard:

1. Tap **Language** to select the language you want to use in ESET Mobile Security. This can be changed later in the program's settings.



Mobile Security

By tapping "Accept", you agree to the terms End User License Agreement

Language: English

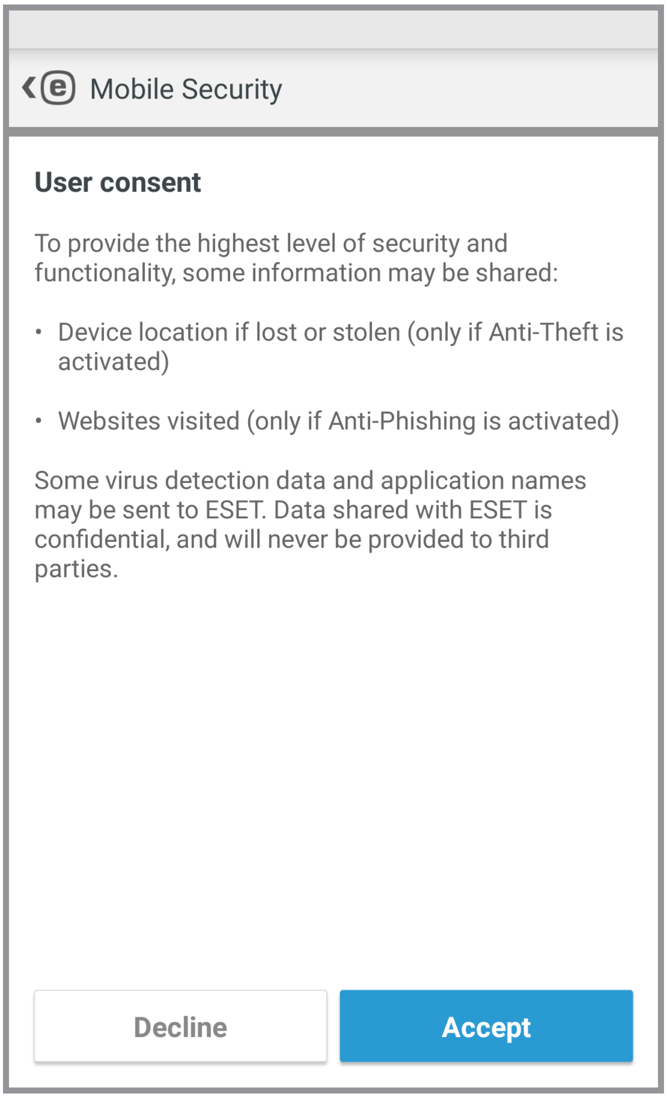
Country: United States

I would like to receive promotional discounts and product news from ESET □

2. Tap **Country** to select the country you currently reside in.

3. Tap **Accept** to agree with the End User License Agreement.

4. Tap **Accept** in the **User consent** screen. Some information like device location and visited websites may be shared with ESET.



User consent

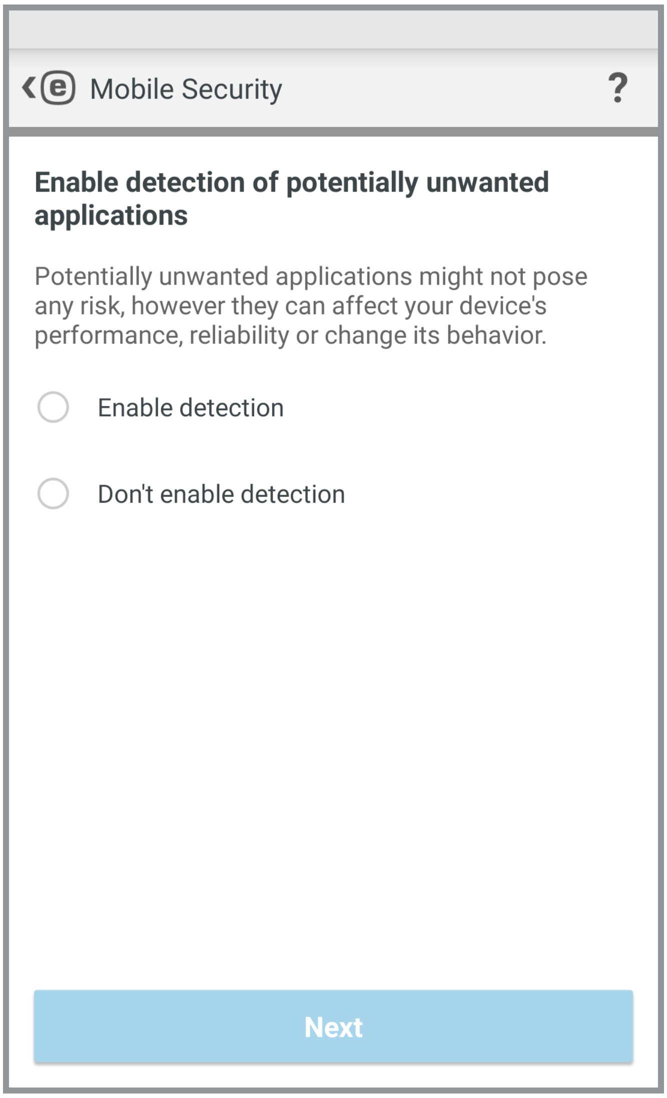
To provide the highest level of security and functionality, some information may be shared:

- Device location if lost or stolen (only if Anti-Theft is activated)
- Websites visited (only if Anti-Phishing is activated)

Some virus detection data and application names may be sent to ESET. Data shared with ESET is confidential, and will never be provided to third parties.

5. Tap **Next** if you want to participate in **ESET Live Grid**. This can be changed later in the program's settings. To read more, see this section.

6. Select either **Enable detection** or **Don't enable detection** to determine if ESET Mobile Security will detect Potentially unwanted applications (PUA's), then tap **Next**. This can be changed later in the program's settings. For more details about PUA's, see this section.



Enable detection of potentially unwanted applications

Potentially unwanted applications might not pose any risk, however they can affect your device's performance, reliability or change its behavior.

○ Enable detection

○ Don't enable detection

7. In the next step, you will see a list of all email accounts available on your device. Select the account you want ESET to use for communications about product license registration, security password reset information and ESET Customer Care communications. If there is no email account listed, tap **Add account** > **OK** > **Existing** to sign in to your existing email account or tap **New** to create a new one.

8. Tap **Activate** to activate the product's premium features or tap **Skip** to start using the free version.

3. Uninstallation

ESET Mobile Security can be uninstalled using the Uninstall wizard available in the program's main menu. Tap Menu ⋮ > **Settings** > **Uninstall**. You will be prompted to enter your Security Password.

Alternatively, follow the steps below to manually uninstall the product:

1. Tap the Launcher icon ▦ on the Android home screen (or navigate to Home > Menu) and tap **Settings** > **Security** > **Device administrators**. Select **ESET Mobile Security** and tap **Deactivate**. Tap **Unlock** and enter your Security Password. You can skip this step if the application is no longer defined as Device administrator.
2. Go back to **Settings** and tap **Manage apps** > **ESET Mobile Security** > **Uninstall**.

4. Product activation

ESET Mobile Security has three available versions:

- Free – basic features are free to use for unlimited time
- Trial – premium features are activated for a limited time (30 days by default)
- Premium – premium features are activated until your license expires

This table indicates which features are available in the Free, Trial and Premium versions:

	Free	**Trial and Premium**
Antivirus	✓	✓
Antivirus – automatic scans		✓
Automatic updates of virus database		✓
Anti-Theft – SMS commands	✓(except Wipe)	✓
Anti-Theft – web portal		✓
Anti-Theft – SIM guard		✓
Anti-Phishing		✓
SMS & Call Filter		✓
Security Audit		✓
Security Report	✓	✓

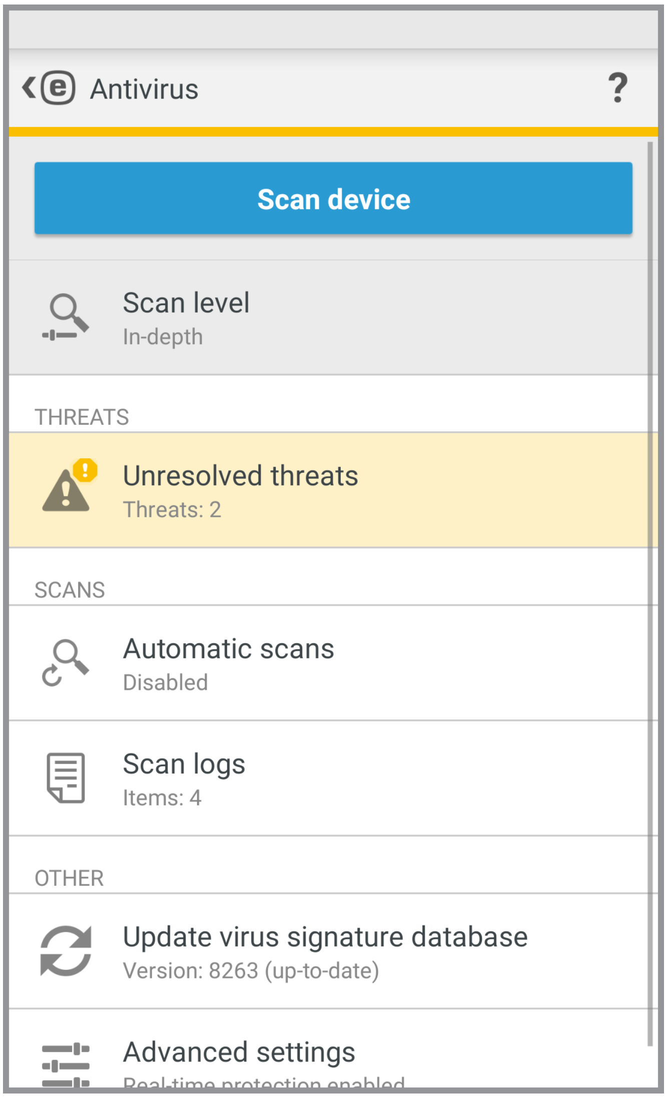
To activate ESET Mobile Security directly on your Android device, tap Menu ⋮ on the ESET Mobile Security main screen (or press the **MENU** button on your device) and tap **License**.

There are multiple ways to activate ESET Mobile Security. The availability of a particular activation method may vary depending on your country, as well as the means of distribution (ESET web page, Google Play, Amazon Appstore).

- **Buy Premium** – select this option if you do not have a license and would like to buy one through Google Play.
- **Enter a License Key** – select this option if you already have a license key. A license key is a unique string formatted: XXXX-XXXX-XXXX-XXXX-XXXX which is used to identify the license owner. You can find it in the email received from ESET or on the license card included in the purchased box.
- **Activate Free Trial** – select this option if you want to evaluate ESET Mobile Security before making a purchase. This can be only done once per Google account.
- **I have a Username and password, what should I do?** – select this option to convert your Username and password to a License Key at https://my.eset.com/convert

5. Antivirus

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



Antivirus

Scan device

Scan level
In-depth

THREATS

Unresolved threats
Threats: 2

SCANS

Automatic scans
Disabled

Scan logs
Items: 4

OTHER

Update virus signature database
Version: 8263 (up-to-date)

Advanced settings
Real-time protection enabled

Scan device

Certain predefined file types are scanned by default. A device scan checks 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 ☒.

Scan level

There are 2 scan levels to choose from:

- **Smart** — Smart Scan will scan installed applications, DEX files (executable files for Android OS), SO files (libraries), archives with a maximum scanning depth of 3 nested archives and SD card content.
- **In-depth** — In-depth scan will scan all file types regardless of their extension in both internal memory and SD card.

Update virus signature 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 virus signature database**.

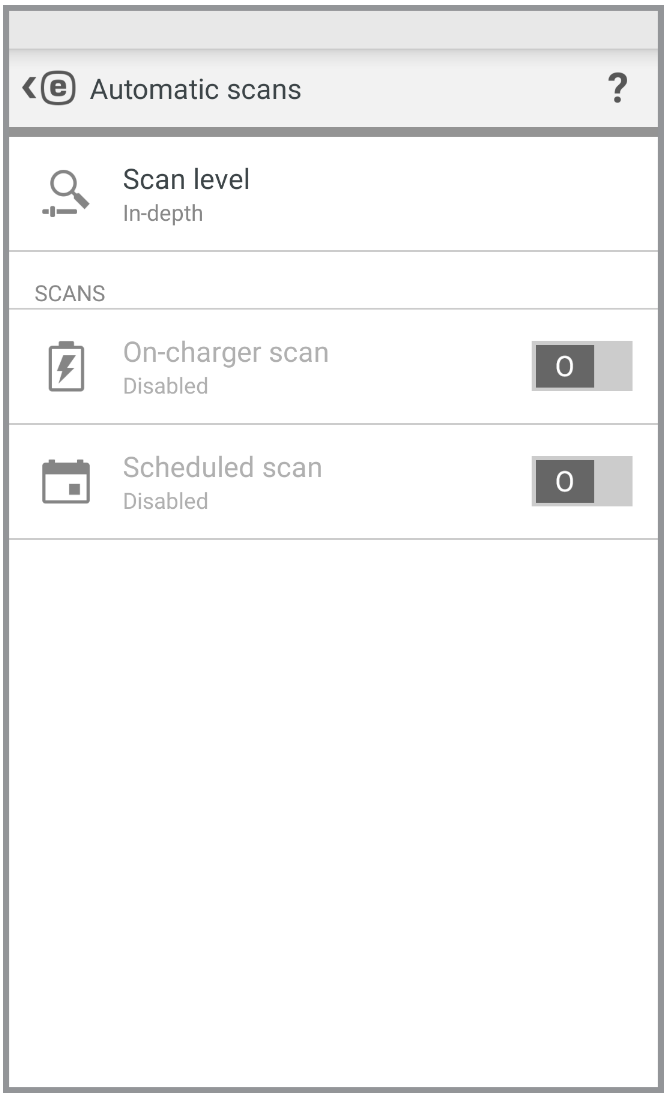
NOTE: To prevent unnecessary bandwidth usage, updates are issued as needed when a new threat is added. Updates are free, although you may be charged by your mobile service provider for data transfers.

For more information about scans, see the following links:

- Automatic Scans
- Scan Logs
- Advanced settings

5.1 Automatic Scans

In addition to the manually triggered Device scan, ESET Mobile Security also offers automatic scans.



Automatic scans

Scan level
In-depth

SCANS

On-charger scan
Disabled

Scheduled scan
Disabled

Scan level

There are 2 scan levels to choose from. This setting will apply to both the On-charger scan and the Scheduled scan:

- **Smart** — Smart scan will scan installed applications, DEX files (executable files for Android OS), SO files (libraries), archives with a maximum scanning depth of 3 nested archives and SD card content.
- **In-depth** — In-depth scan will scan all file types regardless of their extension in both internal memory and SD card.

On-charger scan

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

Scheduled scan

Scheduled scan allows you to schedule a Device scan to run automatically at a predefined time. To schedule a scan, tap the switch next to **Scheduled scan** and specify the dates and times for the scan to be launched.

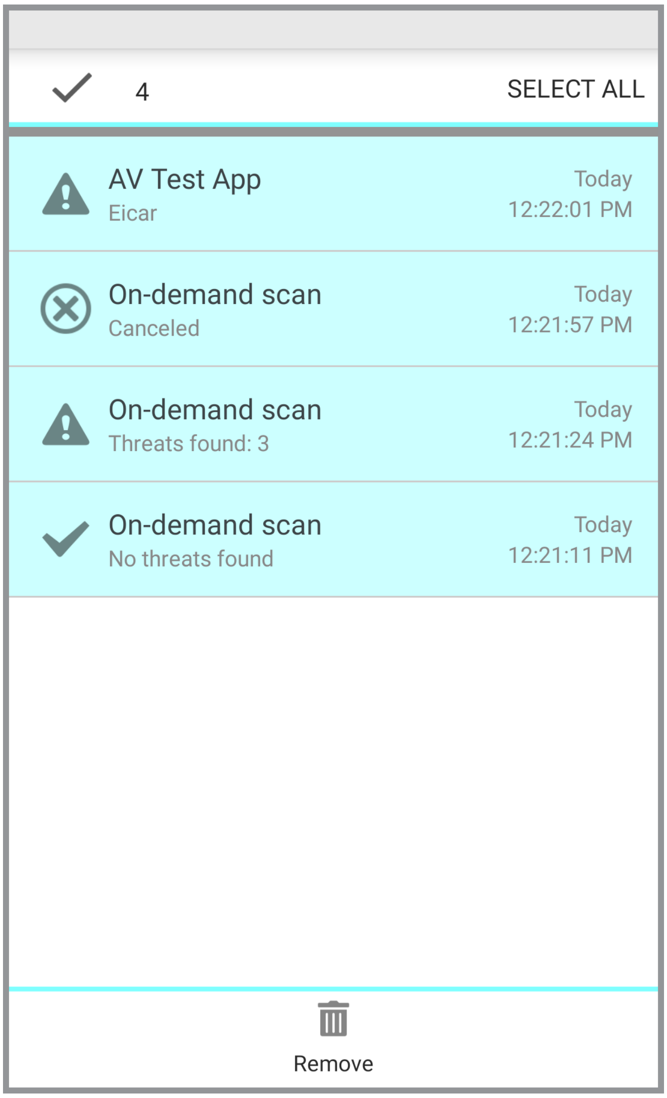
5.2 Scan Logs

The Scan logs section contains comprehensive data about each Scheduled scan or manually triggered Device scan.

Each log contains:

- Date and time of the scan
- Scan level (Smart or In-depth)
- Duration of the scan
- Number of scanned files
- Scan result or errors encountered during the scan

To remove a log from the list, touch and hold the log to select it and tap Remove 🗑 .



✓ 4 SELECT ALL

⚠ AV Test App
Eicar
Today
12:22:01 PM

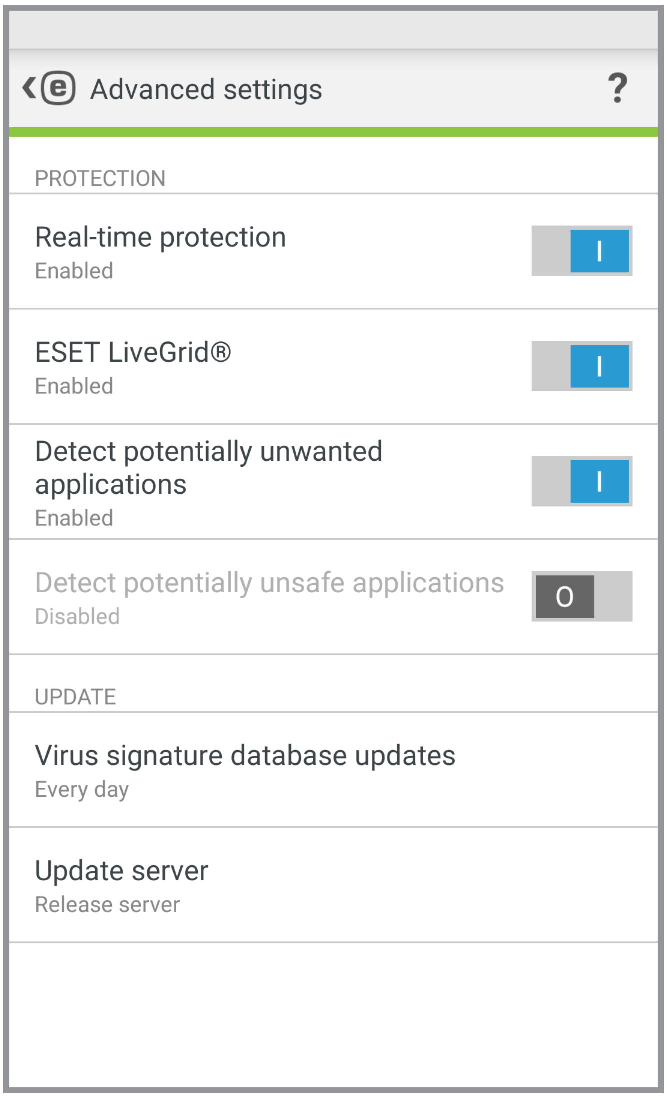
⊗ On-demand scan
Canceled
Today
12:21:57 PM

⚠ On-demand scan
Threats found: 3
Today
12:21:24 PM

✓ On-demand scan
No threats found
Today
12:21:11 PM

🗑 Remove

5.3 Advanced Settings



Advanced settings

PROTECTION

Real-time protection
Enabled

ESET LiveGrid®
Enabled

Detect potentially unwanted applications
Enabled

Detect potentially unsafe applications
Disabled

UPDATE

Virus signature database updates
Every day

Update server
Release server

Real-time protection

Real-time scanner launches automatically at system startup and scans the files that you interact with. It automatically scans the *Download* folder and installed or updated applications.

ESET Live Grid

Built on the *ThreatSense.Net* advanced early warning system, ESET Live Grid is designed to provide your device with an additional level of security. 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 better proactive protection and scanning speed to all ESET users. We recommend that you enable this feature. Thank you for your support.

Detect potentially unwanted applications

A potentially 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 potentially 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. Enable the **Detect potentially unsafe applications** option to monitor these types of applications and block them if you prefer. 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.

Virus signature database updates

This option allows you to set the time interval for automatic threat database downloads. These updates are issued as needed when a new threat is added to the database. We recommend that you leave this set to the default value (daily).

Update server

This option allows you to choose to update your device 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 by having access to the most recent detection methods and fixes. However, pre-release updates might not be stable enough at all times. To check the versions of the current program modules, tap Menu ⋮ in the ESET Mobile Security main screen and tap **About** > **ESET Mobile Security**. It is recommended that basic users leave the **Release server** option selected by default.

6. Anti-Theft

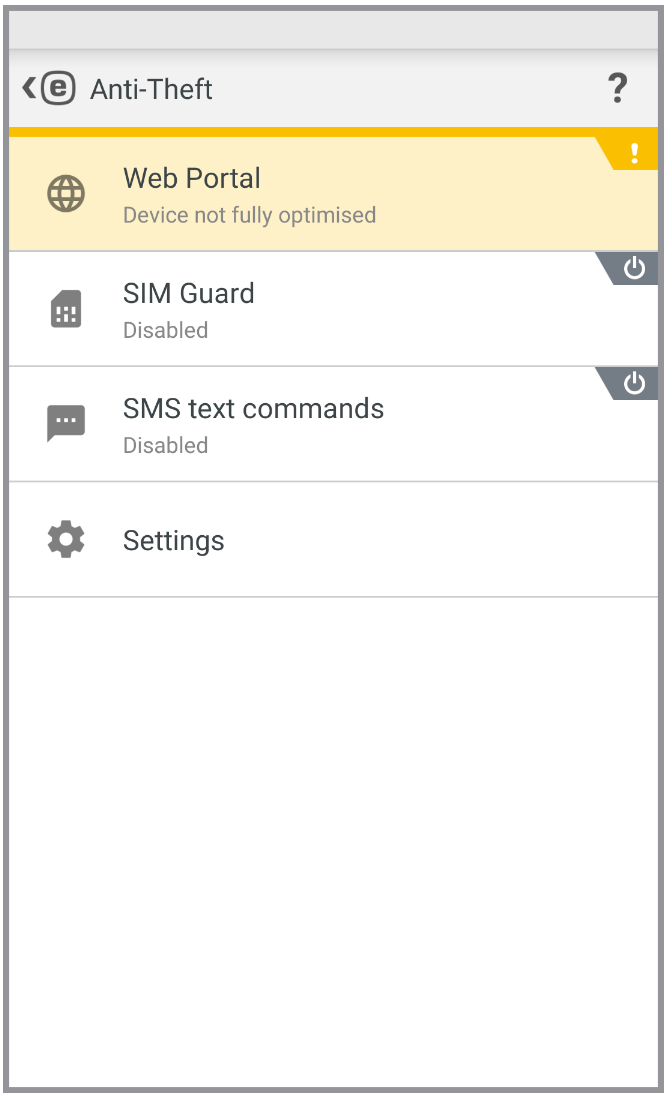
The **Anti-Theft** feature protects your mobile device from unauthorized access.

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 (Trusted SIM cards and SMS Text Commands) are not available on devices that do not support text messaging.

6.1 Web Portal

Version 3 of ESET Mobile Security integrates completely with ESET Anti-Theft protection through My Eset portal. From the portal you will be able to monitor your device activity, lock the device, send custom messages to the device finder, trigger a loud siren or wipe device data remotely.



To create a My ESET account, tap **Create new account** and fill out the registration form. Check your email inbox for the account confirmation and click the link inside to activate your account. Now you can enjoy managing the Anti-Theft security features from my.eset.com. If you already have a My ESET account, tap **Sign in** and enter your email and password. Once these steps are complete, you can associate the device with your My ESET account.

For further guidance on how to use Anti-Theft features in My ESET portal, refer to the Anti-Theft online help or tap **Help** in the top right corner of the screen.

Last known location – this feature saves the device location in ESET Anti-Theft before the device battery loses power.

6.1.1 Optimization

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

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**.

- **Location services turned off** – to turn on, navigate to Android settings > **Location services** and select **Use Wireless networks**
- **GPS Satellites not used** – access this setting in Android settings > **Location** > **Mode** > **High accuracy**
- **Screen Lock not secured** – to secure your device with a screen lock code, password, PIN or pattern, navigate to Android settings > **Lock screen** > **Screen lock** and select one of the available options. Most Android devices offer Swipe, Motion, Face unlock, Face and voice, Pattern, PIN or Password. If someone tries to unlock your device using an incorrect code, ESET Anti-Theft will notify you about the suspicious activity in the My Eset portal.
- **Mobile data not enabled** – access this setting in Android settings > **Wireless & Networks** > **Mobile networks** > **Data**.
- **Google Play Services not present** – ESET Anti-Theft uses Google Play Services to deliver commands to your device in real-time and display push notifications. If these services are disabled or missing on your device, the ESET Anti-Theft functions managed from My Eset will be limited. In this situation, we recommend using SMS commands rather than the My Eset portal.

6.1.2 Proactive Protection

This feature allows you to adjust the warnings and activities triggered by Suspicious mode. ESET Mobile Security regularly saves the device location, camera photos and WiFi IP addresses. You can define the following:

- **Activate when unlock attempt failed** – enabled by default; displays **Contact owner** option when an incorrect screen lock code is entered
- **Max number of failed unlock attempts** – number of failed unlock attempts permitted
- **Time for correction** – by default, you have 15 seconds to enter the correct unlock code
- **Save photos to device** – saves the rear and front camera photos to your device Gallery and the Anti-Theft portal in the event of a failed unlock attempt or a SIM card removal

6.2 SIM Guard

To start using SIM Guard, tap **Anti-Theft** > **SIM Guard** in the main program menu and then tap the switch ○ to enable the feature. A simple wizard will guide you through the setup. These steps can be also accessed through the SMS text commands setup wizard:

- Enter a Security password
- Add Contact details
- Enable Uninstall protection
- Save a current SIM card as trusted
- Add a Trusted friend

6.2.1 Trusted SIM cards

The **Trusted SIM cards** section shows the list of 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 the Trusted Friends.

To add a new SIM card, tap + . Enter a **SIM CARD NAME** (for example, Home or Work) and its **IMSI** (International Mobile Subscriber Identity) number. The IMSI is usually presented as a 15-digit long number printed on your SIM card. In some instances, it may be shorter.

To remove a SIM card from the list, select the SIM card and tap 🗑 .

NOTE: The Trusted SIM cards feature is not available on CDMA, WCDMA and WiFi-only devices.

6.2.2 Trusted Friends

In the **Trusted friends** section, you can add or remove the phone numbers of your friends and family members that will be able to:

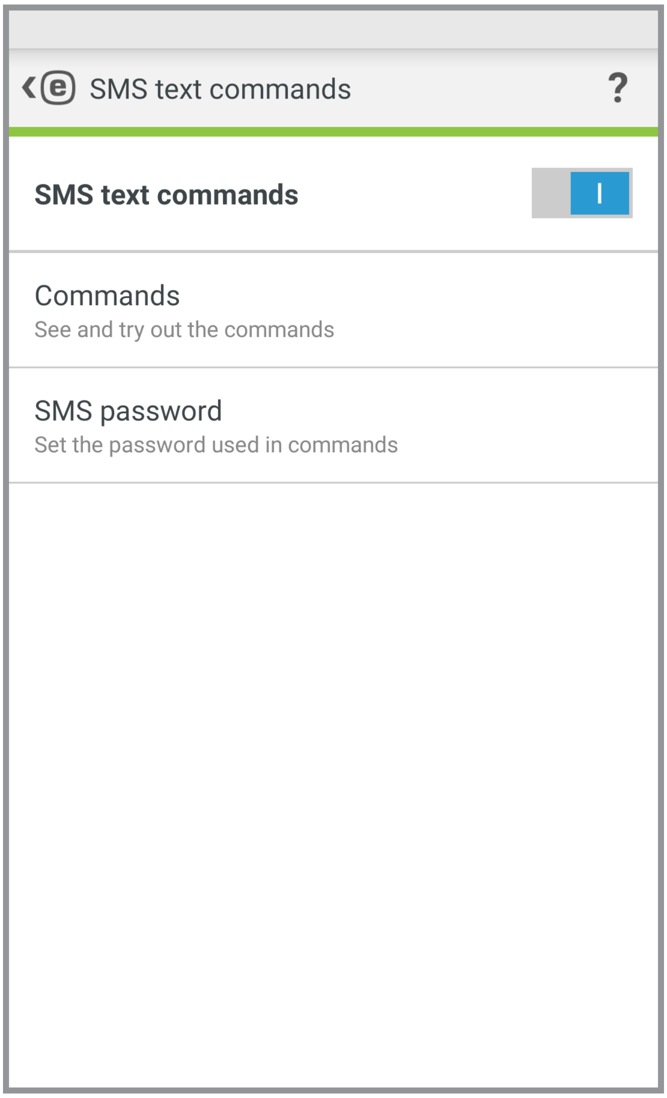
- Receive an alert SMS after detecting unauthorized SIM card in your device
- Reset your Security password (provided the **Allow remote Security password reset** option is enabled for this contact)

To add a new Trusted friend, tap + and enter the friend's name and mobile number or tap 👤 to select a contact from your phone's Contact list. To remove a Trusted friend, select the entry and tap Remove 🗑.

If a Trusted friend entry contains more than one phone number, the alert SMS and password reset will work with all associated numbers.

NOTE: If you are abroad, enter all phone numbers into the list with the international dialing code followed by the actual number (e.g., +1610100100).

6.3 SMS text commands



SMS text commands

SMS text commands I

Commands
See and try out the commands

SMS password
Set the password used in commands

To start using SMS text commands, tap **Anti-Theft** > **SMS text commands** in the main program menu and then tap the switch ○ to enable the feature. If you already completed the SIM Guard wizard, this setup will only prompt you to enter one additional parameter – the SMS password. The Security password can be used for this purpose, however It is not recommended to do so, since the SMS password will be visible on the mobile screen in incoming messages.

The following SMS commands can be sent:

Unlock

```
eset remote reset
```

Send this command from a trusted friend's device to unlock your device's screen.

Lock

```
eset lock password
```

This will lock the device—you will be able to unlock it using the Security password.

Siren

```
eset siren password
```

A loud siren will play even if the device is set to mute.

Find

```
eset find password
```

You will receive a text message with the GPS coordinates of the target device, including a link to its location on Google Maps. The device will send a new SMS if a more precise location is available after certain time.

Wipe

```
eset wipe password
```

All contacts, messages, emails, accounts, SD card content, pictures, music and videos stored in default folders will be permanently erased from your device. ESET Mobile Security will remain installed.

NOTE: Although the SMS commands are not case sensitive, the password needs to be typed in exactly as you defined it in the Anti-Theft setup wizard.

6.4 Settings

In the Anti-Theft Settings section, access the following:

- Security Password
- Contact Details

6.4.1 Security Password

Your **Security Password** is required to unlock your device, access Anti-Theft, uninstall ESET Mobile Security or send SMS text commands (provided that you enabled this option when creating an SMS password).

If you forget the Security password, try the following options:

- Send a text message from a Trusted Friend's mobile number to your number. The message must be in the form: eset remote reset
- If your device is connected to the Internet, request a password reset code by tapping **Email** on your locked device. An email containing the verification code will be delivered to the Google email account defined during the installation. Enter the verification code and a new password on your locked screen.
- Reset the password from My Eset portal. After logging in, select your device, click **Settings** and enter a new password.
- If your device is not connected to the Internet, fill out the form in this Knowledgebase article.
- Contact ESET Customer Care if you are not able to send the aforementioned data.

IMPORTANT: To create a secure password that will be harder to guess, use a combination of lowercase letters, uppercase letters and numbers.

6.4.2 Contact Details

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

This information may include:

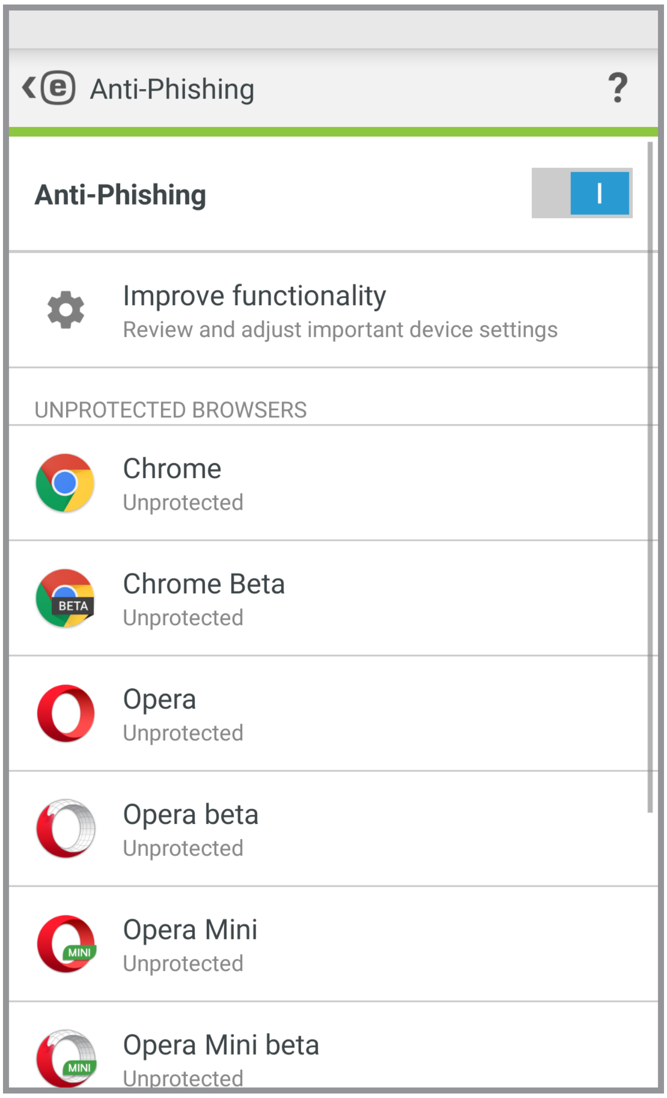
- Your name (optional)
- Backup mobile number of a family member or a friend
- Device description (optional)
- Email address (optional)

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 attempted attack.

Anti-Phishing integrates with the most common web browsers available on Android OS – Chrome and stock browsers that come as pre-installed on Android devices (usually called *Internet* or *Browser*). Other browsers may be listed as Unprotected since they do not provide sufficient integration for Anti-Phishing. To fully utilize the Anti-Phishing functionality, we recommend that you do not use unsupported web browsers.



Anti-Phishing ?

Anti-Phishing I

Improve functionality
Review and adjust important device settings

UNPROTECTED BROWSERS

Chrome
Unprotected

Chrome Beta
Unprotected

Opera
Unprotected

Opera beta
Unprotected

Opera Mini
Unprotected

Opera Mini beta
Unprotected

Improve functionality – ESET Mobile Security warns you if Anti-Phishing protection requires additional permissions to be granted by the Android OS. Tap **Allow** to open the system's Accessibility settings and consider the available options to provide support for more browsers and enable protection when browsing in private (incognito) mode. If you do not want this issue to be reported as a problem, tap **Ignore this issue (not recommended)**.

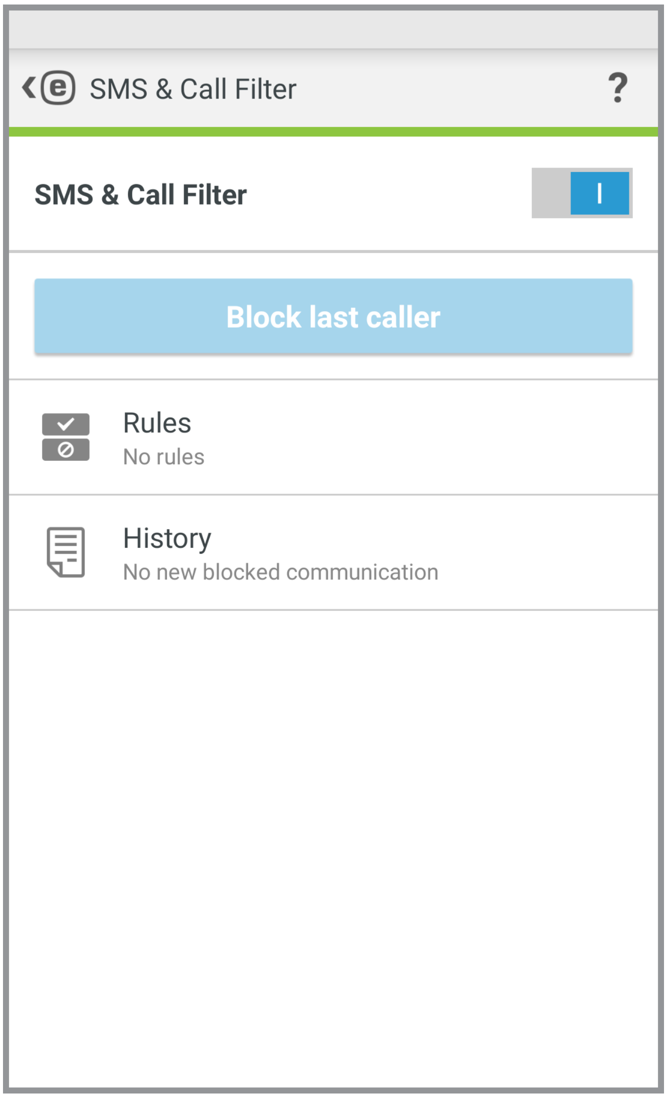
8. SMS & Call Filter

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

Unsolicited messages usually include advertisements from mobile phone service providers or messages from unknown or unspecified users. Notifications will not be displayed when an incoming message or call is blocked. View the History section to check for calls or 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/MMS filtering is not available on Android OS 4.4 and later versions and will be disabled on devices where Google Hangouts is set as the primary application for SMS.

8.1 Rules



SMS & Call Filter

SMS & Call Filter I

Block last caller

Rules
No rules

History
No new blocked communication

Block last caller – tap to block incoming calls from the last received phone number. This will create a new rule.

To create a new rule, tap **Rules** > **Add rule**. See the next chapter for more information.

To modify an existing rule, select it and tap **Edit** ✎ . To remove an entry from the **Rules** list, select the entry and tap **Remove** 🗑 .

8.1.1 Add a new rule

1. In the **Action** section, select either **Block** or **Allow** to specify the rule type for calls and messages.
2. In the **Who** section, select an option to specify the phone numbers that will be affected by the rule.
   - **Person**
   - **Group** – ESET Mobile Security will recognize the contact groups saved in your Contacts (for example, Family, Friends or Co-workers).
   - **All unknown numbers** will include all phone numbers not saved in your contact list. Use this option to block unwelcome phone calls (for example, "cold calls") or to prevent kids from dialing unknown numbers.
   - **All known numbers** will include 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).
3. In the **What** section, select the call or text type that should be blocked or allowed:

   ☎ outgoing calls
   ☎ incoming calls
   ✉ incoming text messages (SMS) or
   ✉ incoming multimedia messages (MMS)
4. In the **When** section, select either **Always** or **Custom** to specify the time interval and the days of the week that the rule will be in effect. By default, Saturday and Sunday are selected.

NOTE: If you are abroad, enter all phone numbers into the list with the international dialing code followed by the actual number (for example, +1610100100).

8.2 History

The **History** section displays the log of all calls and messages blocked 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.

To remove an entry from the list, select it and tap Remove 🗑 .

9. Security Audit

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

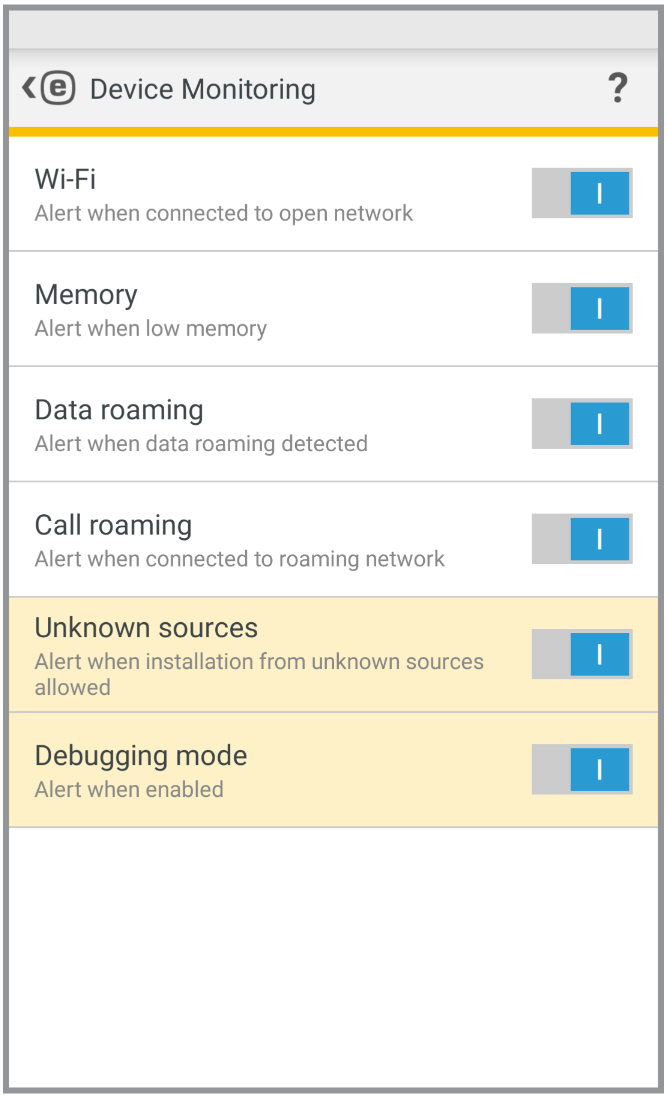
To enable or disable Security Audit and its specific components, tap ○.

- Device monitoring
- Application Audit

9.1 Device Monitoring

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

Tap each option to view its detailed description and current status. In the **Unknown Sources** and **Debug Mode** options, tap **Open settings** to change the settings in Android OS Settings.



Device Monitoring

Wi-Fi
Alert when connected to open network

Memory
Alert when low memory

Data roaming
Alert when data roaming detected

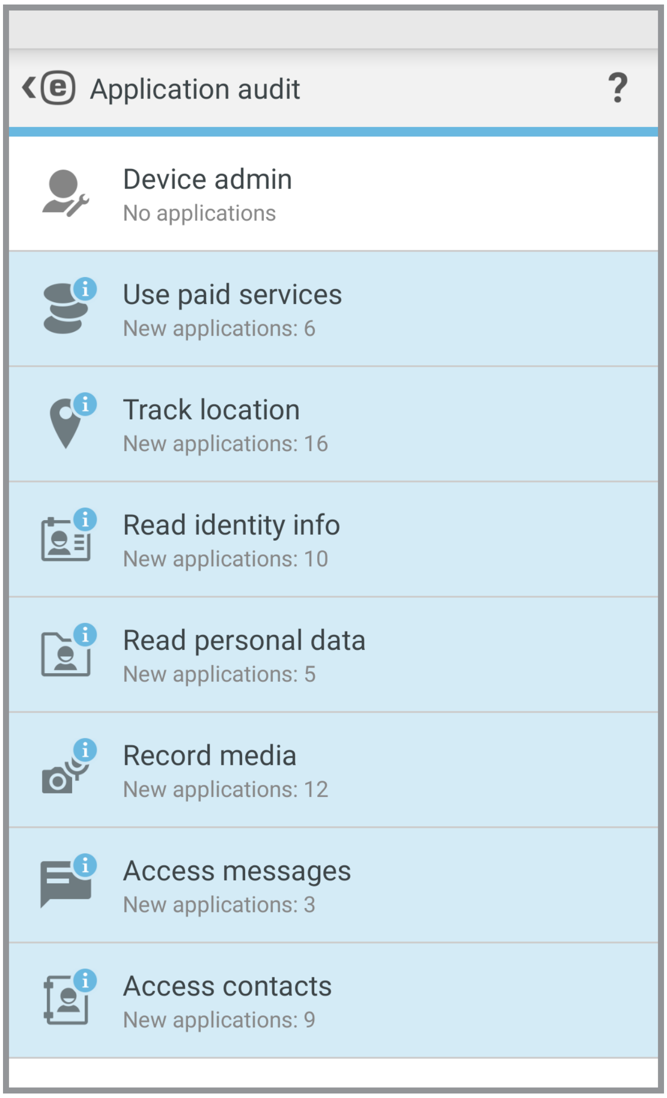
Call roaming
Alert when connected to roaming network

Unknown sources
Alert when installation from unknown sources allowed

Debugging mode
Alert when enabled

9.2 Application Audit

Application Audit performs an audit of the applications installed on your device that might have access to services that cost you money, track your location or read your identity information, contacts or text messages. ESET Mobile Security provides a list of these applications sorted by categories. Tap each category to see its detailed description. Tap an application to view its permissions details.



Application audit

Device admin
No applications

Use paid services
New applications: 6

Track location
New applications: 16

Read identity info
New applications: 10

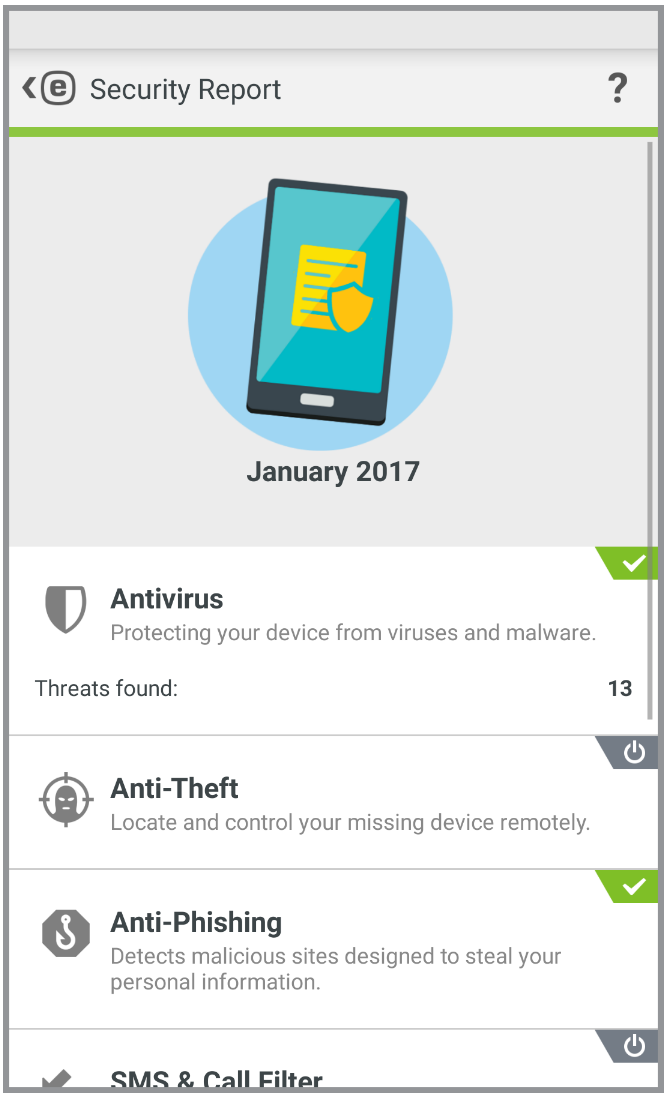
Read personal data
New applications: 5

Record media
New applications: 12

Access messages
New applications: 3

Access contacts
New applications: 9

10. Security Report



Security Report

January 2017

Antivirus
Protecting your device from viruses and malware.

Threats found: 13

Anti-Theft
Locate and control your missing device remotely.

Anti-Phishing
Detects malicious sites designed to steal your personal information.

SMS & Call Filter

Security Report provides a comprehensive overview of each program module and its respective status and statistics. You can also enable the modules that are currently not in use from the Security Report screen. Each program module section contains the following information.

Antivirus:

- Installed applications
- Updated applications
- Scanned applications
- Detected threats
- Virus signature database updates

Anti-Theft

Anti-Phishing:

- Scanned websites
- Detected threats

SMS & Call Filter:

- Outgoing calls
- Received calls
- Blocked calls

Security Audit:

- Roaming alerts
- Open WiFi warnings

Enable the **Monthly report notification** option to display a brief message in the Android notification bar. Tap the notification to open the **Security Report** window.

11. Settings

To access the program's settings, tap Menu ⋮ in the ESET Mobile Security main screen (or press the Menu button on your device) and tap **Settings**.

Language

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

Permanent notification

The ESET Mobile Security icon ⓔ will be displayed in the top left corner of the screen (Android status bar). If you do not want this icon to be displayed, deselect **Permanent notification** and tap **Turn off**.

Special offers

You will receive the in-product news and latest offers from ESET.

Update

For maximum protection, it is important to use the latest version of ESET Mobile Security. Tap **Update** to see if there is a newer version available for download from the ESET website. This option is not available if you downloaded ESET Mobile Security from Google Play – in this case, the product is updated from Google Play.

Uninstall

Running the Uninstall wizard will permanently remove ESET Mobile Security from the device. If Uninstall protection was enabled, you will be asked to enter your Security Password. To uninstall the product manually, follow the steps described in this section.

12. 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 contact ESET Customer Care, follow this link.

To send a support request directly from your device, tap Menu ⋮ in the ESET Mobile Security main screen (or press the Menu button on your device), tap **Customer Care** > **Customer Care** and fill in all 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 **Submit application log** is selected (default). Tap **Submit** to send your request. An ESET Customer Care specialist will contact you at the email address you provided.