ESET Mobile Security

User guide

[Click here to display the online version of this document]

Digital Security
Progress. Protected.

ESET Mobile Security was developed by ESET, spol. s r.o.

For more information visit https://www.eset.com.

Technical Support: https://support.eset.com

REV. 1/26/2024

Introduction

ESET Mobile Security is a complete security solution that safeguards your device from emerging threats and phishing pages 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 the ESET HOME portal
- Call Filter
- Security Audit
- Security Report
- Network Inspector
- App Lock
- Payment Protection

What's new

New features in ESET Mobile Security version 8:

Added

- Android 13 support
- Antismishing (SMS protection and Notification protection)
- Using wildcards in Call filter

Improved

- New home screen design
- New main menu design

Minimum system requirements

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

- Operating system: Android 6 (Marshmallow) or later

- Touchscreen resolution: minimum 240x320 px
- CPU: 500+ MHz ARM7+
- RAM: 512+ MB
- Internet connection

Support exclusions

- Dual SIM and rooted devices are not supported. The Anti-Theft and Call Filter features are not available on tablets that do not support calling or messaging.
- Android Go is not supported.
- ESET Mobile Security requires Google Play services to work correctly. ESET Mobile Security is not supported on devices without Google Play services, such as some Huawei devices.
- The Trusted SIM cards Anti-Theft feature is not available on CDMA devices.
- Some feature functionality is OS version dependent.

Installation

ESET Mobile Security is available for downloading here:

Amazon Appstore

Or visit our step by step installation guide (this article is not available in all languages).

For installation instructions, visit our Knowledgebase article (this article is not available in all languages).

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 is used, see the table in our Knowledgebase article (this article is not available in all languages).

Start-up wizard

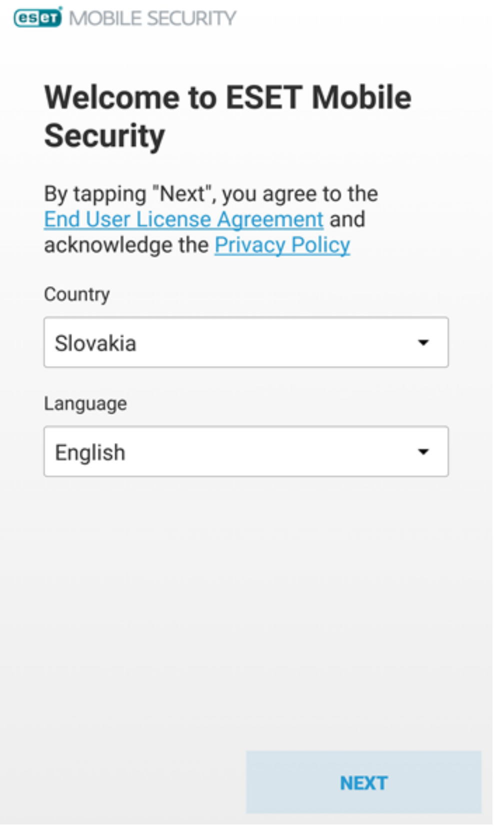
After installation, follow the on-screen prompts in the Start-up Wizard:

Enable permissions for ESET Mobile Security

This guide is based on stock Android settings. The permission-enabling process may differ based on your device manufacturer.

1. Tap **Country** and select the applicable country.
2. Tap **Language** and select the applicable language.

3. Tap **Next** and agree to the End User License Agreement and Privacy Policy.



Welcome to ESET Mobile Security

By tapping "Next", you agree to the End User License Agreement and acknowledge the Privacy Policy

Country: Slovakia

Language: English

4. If applicable, allow the following options and tap **Next**.

- **Allow ESET LiveGrid©**—To read more about **ESET LiveGrid©** feedback system, visit the Advanced settings section.
- **Allow analytics to help make our products better**—ESET Mobile Security will send anonymous application information (performance, operational statistics) that will help us improve our application and services. To read more about the information we collect, visit the Privacy Policy chapter.
- **Allow data usage for marketing purposes**

5. Review your activation details when you have installed ESET Mobile Security from the download link sent to your email address from the ESET HOME account. Tap **Continue**, and follow the instructions to activate ESET Mobile Security with the ESET HOME account. If you do not agree, tap **Decline** and follow the steps below.

6. Log in to your ESET HOME account to connect your mobile device to your account and activate ESET Mobile Security.

Continue with Google

a.Select your Google account.

b.If you are connecting for the first time to an existing ESET HOME account with your Google account, you will be prompted to type your ESET HOME password. Tap **Confirm password**.

Continue with Apple

a.Type your Apple ID and password.

b.Tap **Log in**.

c.Type the code sent to your Apple device.

d.Tap **Continue**.

e.If you trust your web browser, click **Trust**.

f.Tap **Continue** to access ESET HOME with your Apple ID.

g.Tap the **X** icon in the top left corner to return to ESET Mobile Security.

Scan QR code

This option requires another device with ESET HOME app.

a.Open the ESET HOME app on another device.

b.Tap the menu button ☰ > **Scan a QR code**.

c.Tap **Scan a QR code**. You might be prompted to allow ESET HOME to take pictures and record videos. Tap **While using the app** or **Only this time**.

d.Use your camera to scan the QR code.

e.Tap **Connect device**.

f.Tap **Finish** in your ESET Mobile Security.

Create account or log in

Create an ESET HOME account

a.Type your email address and password.

> ❗ **Password requirements**
> Password must contain at least ten characters and at least one lowercase, one uppercase character and one number.

b.Tap **Create account** to receive a confirmation link via email.

c.Create a nickname for your device and tap **Next**.

d.To properly work ESET Mobile Security, tap **Continue** to allow the All files access permission.

e.Tap the **Start first scan**.

f.To complete registration, tap the link in the confirmation email.

Log in to ESET HOME

a. Tap **Log in** under the **Create account** button.

b. Type in your email and password.

c. Tap **Log in**.

After logging in to your ESET HOME account, you must create a nickname for your device. It will help you identify this device in your ESET HOME account. Type in the nickname, and tap **Next**.

Skip

If you do not have a ESET HOME account, or you do not want to connect your mobile device to your ESET HOME account, tap **Skip**. You can log in to your ESET HOME account later in the ESET Mobile Security app.

If you skip this step, you will be prompted to select the email account that will receive ESET license registration and Technical Support emails. Tap **Select your email address** to display the list of available email accounts. Select the email from the list of accounts or tap **Add account** to add a new email account to your device. Tap **OK** to continue. To use a different email account without adding the account to your device, tap **Select your email address** > **Cancel**. Repeat this action twice. Type your email and tap **Select** to continue.

7. The last steps of the start-up wizard vary based on your device's Android version.

Android 6–10

a. To enable device scanning, ESET Mobile Security requires multiple permissions. Review the permissions for ESET Mobile Security in the **Allow access** screen and tap **Continue**.

b. Tap **Allow** to grant permission to ESET Mobile Security. If you tap **Skip**, ESET Mobile Security will not scan your device for threats until these permissions are allowed, and you will receive a Security risk notification.

Android 11 and later

a. Tap **Continue**.

b. Select ESET Mobile Security.

c. Enable the toggle next to ESET Mobile Security.

d. The Start-up Wizard is complete. Tap **Start first scan**.

Battery protector

Many device manufacturers introduced battery protectors or battery-saving options in Android 6 and later devices. When turned on, this feature turns off the Anti-Phishing functionality in ESET Mobile Security. On devices with this feature, you will need to create an exception to allow the ESET Mobile Security Anti-Phishing functionality to work with the battery-saving feature turned on. To create an exception, check your device manufacturer's documentation.

Free and Premium license features

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). The trial license is automatically activated the first time ESET Mobile Security is installed per Amazon ID.
- 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 detection modules		✔
App Lock		✔
Anti-Theft – SMS commands		✔
Anti-Theft – web portal		✔
Anti-Theft – SIM guard		✔
Network Inspector		✔
Anti-Phishing		✔
Call Filter		✔ (only for Android 5.1 and later)
Payment Protection		✔
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 specific activation method may vary depending on your country, as well as the means of distribution (ESET web page, Amazon Appstore).

- **Buy Premium** – select this option if you do not have a license and would like to buy one through Amazon Appstore.
- **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.

Activation

To unlock premium features on ESET Mobile Security, you need to activate a premium license.

If you do not have a license yet:

1. Tap the menu button ☰ to open the main menu.
2. Tap the **License**.
3. Tap **Buy premium**.
4. Follow the on-screen instructions to finish the purchase.

If you have an ESET license:

1. Tap the menu button ☰ to open the main menu.
2. Select **License**.
3. Tap **Enter a license key**.
4. Type in the license key you received with the ESET license.
5. Tap **Activate**.
6. Your license is now active.

Uninstallation

ESET Mobile Security can be uninstalled using the **Uninstall** wizard available from the main menu in ESET Mobile Security.

> **Note**
> Uninstalling the ESET Mobile Security product will free up one seat from your license.

1.Tap Menu ☰.

2.Tap **Settings**.

3.Tap **Uninstall**.

4.If Anti-Theft protection is activated, you will be prompted to enter your ESET Mobile Security security PIN/Pattern or your fingerprint.

5.Tap **Uninstall**.

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

Android 7 and later:

1.Go to Settings and tap **Manage apps** > **ESET Mobile Security** > **Uninstall**. If Anti-Theft protection is activated, you might be asked to deactivate Device administrator for ESET Mobile Security before uninstalling it.

Or

1.In the ESET Mobile Security, tap the main menu button ☰ to open the main menu.

2.Select **Settings**.

3.Tap **Uninstall**.

4.Tap **Uninstall** again to confirm you decision.

Android 6:

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 PIN/Pattern. You can skip this step if the application is no longer defined as a Device administrator.

2.Go back to **Settings** and tap **Manage apps** > **ESET Mobile Security** > **Uninstall**.

Connecting to ESET HOME

To use this feature, upgrade to ESET Mobile Security version 6.3 or later.

> **Activating ESET Mobile Security via ESET HOME**
> If you want to activate one device via ESET HOME a second time (for example, after reinstallation of ESET Mobile Security), you need to manually remove the device from the license in ESET HOME before you proceed. Otherwise, you will not be able to activate this device via ESET HOME.

Connect your device to an existing ESET HOME account

1. Tap the menu button ☰.

2. Tap **ESET HOME account**.

Continue with Google

a.Select your Google account.

b.If you are connecting for the first time to an existing ESET HOME account with your Google account, you will be prompted to type your ESET HOME password. Tap **Confirm password**.

Continue with Apple

a.Type your Apple ID and password.

b.Tap **Log in**.

c.Type the code sent to your Apple device.

d.Tap **Continue**.

e.If you trust your web browser, click **Trust**.

f.Tap **Continue** to access ESET HOME with your Apple ID.

g.Tap the **X** icon in the top left corner to return to ESET Mobile Security.

Scan QR code

This option requires another device with ESET HOME app.

a.Open the ESET HOME app on another device.

b.Tap the menu button ☰ > **Scan a QR code**.

c.Tap **Scan a QR code**. You might be prompted to allow ESET HOME to take pictures and record videos. Tap **While using the app** or **Only this time**.

d.Use your camera to scan the QR code.

e.Tap **Connect device**.

f.Tap **Finish** in your ESET Mobile Security.

Continue with email

a.Type your email and password.

b.Tap **Log in**.

3. If you are logging into your ESET HOME account for the first time with this device, create a nickname for your device to help identify the device in ESET HOME. Tap **Next**.

4. If you use a free or trial license and have an available license in ESET HOME, you will be offered to activate ESET Mobile Security.

   a.Select the applicable license.

   b.Tap **Activate**.

5. Tap **Finish**.

Create a ESET HOME account and connect your device

1. Tap the menu button ☰.
2. Tap **ESET HOME account**.
3. Tap **Create account**.
4. Type your email address and password.

> **Password requirements**
> Password must be at least ten characters and contain at least one lowercase, one uppercase character and one number.

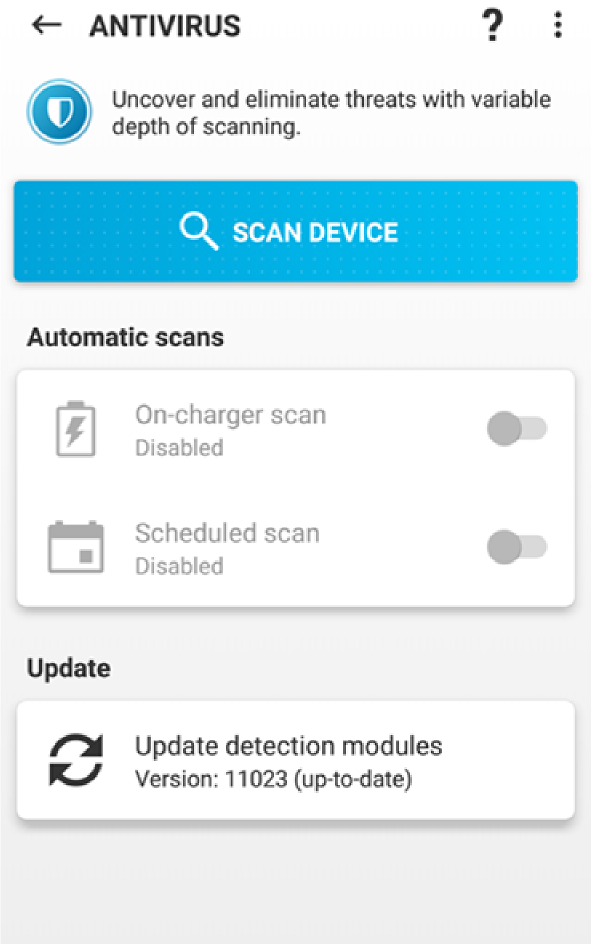
5. Tap **Create account** to receive a confirmation link via email.
6. Create a nickname for your device and tap **Next**.
7. To properly work ESET Mobile Security, tap **Continue** to allow the All files access permission.
8. Tap the **Start first scan**.
9. To complete registration, tap the link in the confirmation email.

Disconnect your device from ESET HOME

1. Tap the menu button ☰.
2. Tap **ESET HOME account**.
3. Tap **Disconnect device**. If your device is not connected to ESET HOME, this option is unavailable.
4. Use your fingerprint or type your PIN.
5. Tap **Disconnect**.

Antivirus

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


ANTIVIRUS

Uncover and eliminate threats with variable depth of scanning.

Automatic scans

On-charger scan
Disabled

Scheduled scan
Disabled

Update

Update detection modules
Version: 11023 (up-to-date)

Real-time protection

Real-time file system protection controls all files in download folders for malicious code when opened, created, or run.

By default, Real-time file system protection launches at system start-up and provides uninterrupted scanning. We do not recommend disabling enabled Real-time file system protection in the **Antivirus** section. If you need to go to the Real-time protection settings, tap the three dots ⋮ in the **Antivirus** section > **Advanced settings** > **Real-time protection**.

Scan device

You can perform an on-demand scan anytime by tapping the **Scan device** button in the **Antivirus** section. By default scan level is set to Smart scan. You can change the scan level in the antivirus **Advanced settings**. Tap the three dots ⋮ > **Advanced settings** > **Scan level**.

There are two 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 three nested archives and SD card content.
- **In-depth**—In-depth scans will scan all file types, regardless of their extension, in both internal memory and SD cards.

A brief scan summary is saved to a log file available in the **Scan Logs** section. If you want to abort a scan already in progress, tap **Cancel**. Scan outcomes and statistics are displayed during the scan in the **Antivirus** section.

> **Memory card scanning**
> ESET Mobile Security does not support memory card scanning on devices with Android 6.

Unresolved threats

After ESET Mobile Security detects a threat, this option will be available until you select a response action to the threat. The available response actions are to remove the threat or to ignore it.

Ignore threats

After you choose to Ignore a threat, the **Ignore threats** option will appear. This option will still allow you to remove an ignored threat later.

On-charger scan

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

Scheduled scan

The scheduled scan enables you to schedule a Device scan to run automatically at a pre-defined time. To schedule a scan, tap the switch next to **Scheduled scan** and specify the dates and times for the scan to launch.

Update detection modules

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

> **Data transfer charging**
> To prevent unnecessary bandwidth use, updates are issued as needed. 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:

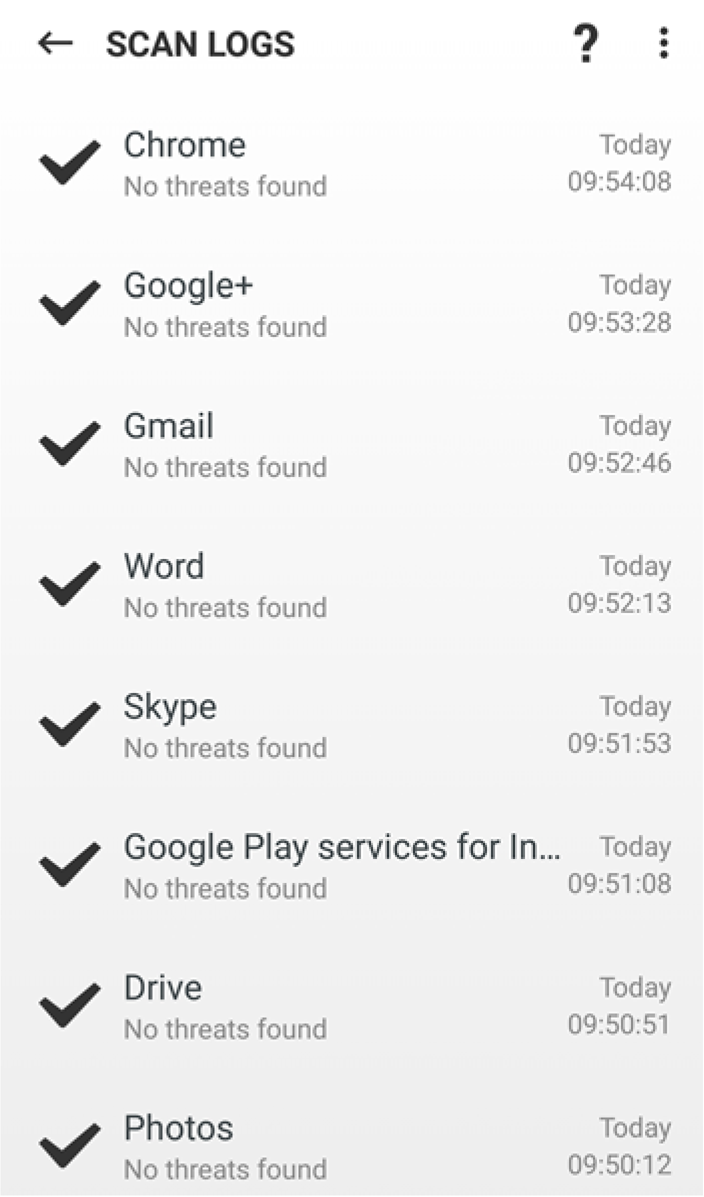
- Scan Logs
- Advanced settings

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
- Number of threats found and list of found threats



← SCAN LOGS ? ⋮

✓ Chrome
No threats found
Today 09:54:08

✓ Google+
No threats found
Today 09:53:28

✓ Gmail
No threats found
Today 09:52:46

✓ Word
No threats found
Today 09:52:13

✓ Skype
No threats found
Today 09:51:53

✓ Google Play services for In...
No threats found
Today 09:51:08

✓ Drive
No threats found
Today 09:50:51

✓ Photos
No threats found
Today 09:50:12

Advanced Settings

Open your ESET Mobile Security application, and tap menu icon ☰ > **Antivirus** > three dots in the upper right corner ⋮ > **Advanced settings**.

Scan level

There are two 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 three nested archives and SD card content.
- **In-depth**—In-depth scans will scan all file types, regardless of their extension, in both internal memory and SD cards.

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 LiveGrid© reputation system

ESET LiveGrid© is a preventative system 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. This enables us to offer better and more precise proactive protection and scanning speeds to all ESET users. We recommend that you enable this feature.

ESET LiveGrid© feedback system

This feedback system allows us to collect anonymous statistics, crash reports, and diagnostics data about suspicious objects, which we process automatically to create the detection mechanism in our cloud system.

Removable media

ESET Mobile Security scans all removable media connected to your device (USB Flash drives, External Hard drives, etc.).

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 may be some situations where you believe that the benefit provided by the potentially unwanted application outweighs the risks. For this reason, ESET assigns this category of applications a lower risk compared to malicious software.

Detect potentially unsafe applications

There are many legitimate applications whose function is to simplify the administration of networked devices. This classification includes programs such as remote access tools, password-cracking applications, and keyloggers. Potentially unsafe applications are a classification used for commercial, legitimate software. However, they can be misused for malicious purposes in the wrong hands. Enable the **Detect potentially unsafe applications** option to monitor this category of applications and block them if you prefer.

Update server

This option allows you to enable updates to 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 from early access to the latest detection methods and fixes. However, pre-release updates might not be completely stable at all times. To check the versions of the current program modules, tap the three dots ⋮ in the ESET Mobile Security main screen and tap **About** > **ESET Mobile Security**.We recommend that basic users leave the **Release server** option selected by default.

Adware Detector

Adware Detector is ESET's response to adware applications. Adware apps can be legitimate applications or applications that try to present themselves as legitimate (such as Calculator or torch). These apps then display full screen ads even when the application is closed. Therefore, the user cannot detect which application is displaying these screen ads.

Adware Detector helps you identify these adware applications. To use it, do the following after a screen ad is displayed:

1. Open ESET Mobile Security.
2. On the main ESET Mobile Security screen, tap **Antivirus**.
3. Tap ⋮ in the top right corner to display the menu.
4. Tap **Adware Detector** in the menu.
5. After Adware Detector displays a guide for detecting adware applications, Tap **Continue**.

Adware Detector displays applications that were open in the last five minutes. Identify suspicious applications, and tap **Remove** to remove them from your device. A suspicious application is usually one that you were not supposed to open or that you were not using at the moment.

Security Report

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

If some of the information are not present, it means that zero occurrences happened.

Antivirus

- App scans
- Threats found
- Database updates

- Detection occurred
- Files scanned
- Apps updated

App Lock

- Number of protected applications
- Number of successful application unlocks
- Number of unsuccessful unlock attempts

Anti-Phishing

- Scanned links
- Scanned notifications
- Detected threats

Call Filter

- Outgoing calls
- Received calls
- Blocked calls

Payment Protection

- Number of protected applications
- Number of scans of protected applications
- Number of issues found
- Number of how many times you launched banking or payment app from Safe launcher

Security Audit

- Roaming alerts represents number of times you were alerted of being connected to a roaming network
- Open WIFI warnings

Network Inspector

- Network scans
- Devices found

- Vulnerabilities found

ESET Mobile Security will display a brief monthly report message in the Android notification bar every month. If you do not want to receive these notifications, enable the **Don't show monthly report notification** option.

Activity log

Activity Log displays the daily activities of ESET Mobile Security on the main screen of the ESET Mobile Security application. The Activity Log contains information about the websites scanned by ESET Mobile Security, ESET Mobile Security updates, application updates, applications installed, ESET Mobile Security scans and more.

To display the full Activity Log history, tap the **>** icon next to the Activity Log. In the Activity Log full report, you can use **Filters** to filter activities by status or ESET Mobile Security feature. For example: Warning, Risk, Anti-Theft, and License. You can also filter the activities by the date of occurrence by newest or by the oldest.

To clear the Activity Log history:

1. Open ESET Mobile Security.
2. Swipe home screen down.
3. Tap the **>** icon next to the **Activity Log**.
4. Tap the menu icon ⋮.
5. Tap **Clear all**.

To remove individual records from the Activity Log history:

1. Open ESET Mobile Security.
2. Swipe home screen up.
3. Tap the **>** icon next to the **Activity Log**.
4. Swipe the appropriate record to the left.
5. Tap **Remove**.

Anti-Theft

The ESET Anti-Theft feature protects your mobile device from unauthorized access, enables you to monitor foreign activity, and tracks your device's location. You can also display a message to the finder if your device is lost.

ESET Anti-Theft requires the following permissions:

- Camera access to take an intruder's pictures.
- Edit files access to delete sensitive data remotely.
- Location data access to track your device if it goes missing.
- Physical activity access to recognize when your device is moved.
- Background location access to track your device if it goes missing, even when ESET Mobile Security is closed or not in use. When granting this permission, select **Allow all the time** to ensure full protection.
- Usage access to allow receiving calls on your device if it gets locked.
- Device admin access to prevent unauthorized ESET Mobile Security uninstallation. After activating the device admin, you will be prompted to create a PIN to protect important settings in ESET Mobile Security.
- Read phone information to detect SIM card removal. Your device will lock when the SIM card is removed.

Visit our Set up Anti-Theft protection in ESET Mobile Security for Android Knowledgebase article to set up Anti-Theft protection in ESET Mobile Security (Knowledgebase articles are not available in all languages).

Auto-lock device

In addition to locking your device from the ESET HOME portal, you can set up ESET Mobile Security to automatically lock your device when one of the following actions is performed:

- **SIM card is removed**—If the trusted SIM card is removed from your device, your device will lock. To remove and inspect trusted SIM cards, tap **Manage trusted SIM cards**, select the SIM card you want to remove, and then tap the bin icon 🗑. To add a trusted SIM card, insert the SIM card. If Auto-lock is enabled, you will have to unlock the device. ESET Mobile Security will ask you to confirm the newly added SIM card as trusted.

⚠ Auto-lock on the SIM card removal support

- Auto-lock on the SIM card removal feature is unavailable on CDMA, WCDMA, and Wi-Fi-only devices.

- **After [X] unlock attempts**—When enabled, your device locks after a set number of unsuccessful unlock attempts. You can set the number of unsuccessful unlock attempts before locking the device in the Anti-Theft settings. If your unsuccessful attempt was caused by mistake, you can correct it in 30 seconds, and it will not be counted as an unsuccessful attempt. You can change the time for a correction in the Anti-Theft settings in the **Time for correction** option. You can also disable the time for correction, and your device will lock immediately after the set number of unsuccessful attempts.

When your device is locked, you can display information to contact the device owner. You can also enable your device to take pictures with both cameras to get photos of the person that tries to unlock your device.

After the device is locked

You can set the following to happen after your device is locked:

- The **Show contact details** option displays the **Contact owner** details when an incorrect screen lock code is entered. Tap **Edit contact details** to type your contact details to display when your device is lost. Your ESET HOME email is typed by default.

- The **Take a photo** option saves the rear and front camera photos to your device Gallery and the Anti-Theft portal in case of a failed unlock attempt or a SIM card removal.

How to unlock my mobile device

If you locked your mobile device via the ESET Anti-Theft portal or ESET Mobile Security for Android has locked your mobile device, you will need access to your ESET HOME password.

> Unlock your device managed by someone else
> If your ESET Mobile Security for Android is managed by someone else's ESET HOME account, type the password for that account to unlock your device.

For visual instructions on unlocking your mobile device, read the following ESET Knowledgebase article (available in English and several other languages).

Anti-Theft Settings

Lock after failed attempts

Select the number of failed unlock attempts permitted before the device will lock. To set up number of unlock attempts tap ⋮ on the Anti-Theft screen, select **Settings**, tap **Lock after failed attempts**, and select the number of failed attempts you want.

Time for correction

If you enabled Lock after failed attempts, your device will lock after the number of unsuccessful attempts you set. Disable Time for correction to lock the device immediately after reaching the set number of failed attempts, or set a length of time to unlock your device successfully before it locks after reaching the set number of failed attempts.

> Example
> **Lock after failed attempts** is enabled, and the number of failed attempts is set to three.
> **Time for correction** is set to 15 seconds.
> After entering the wrong unlock pattern on the device three times, you have 15 seconds to enter the correct unlock pattern to prevent ESET Mobile Security from locking the device.

Edit contact details

If you mark your device as missing on ESET Anti-Theft, or after a selected number of failed unlock attempts, the information from **Contact Details** will be displayed on your locked device's screen so that the person who finds it will be able to contact you.

This information can include:

- Message displayed (optional)
- Your name (optional)
- Phone number (other than your own)

- Email address (optional)

Manage trusted SIM cards

This option allows you to delete or rename the inserted SIM card. To add a new trusted SIM card, insert the SIM card in the device. The device will lock. Unlock the device with your security code. You will be prompted to add the newly inserted SIM card to the list of trusted SIM cards. If you do not add this SIM card to the list, SIM guard will stay disabled.

Change lock type

Select a way to unlock ESET Anti-Theft. PIN code is set as a default option during the Anti-Theft setup. You can change this to a pattern unlock option.

Use fingerprint

When enabled, you can use the fingerprint saved in the device to unlock the Anti-Theft option.

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, 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 ESET HOME 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, theESET Anti-Theft functions managed from ESET HOME will be limited.

Web Portal

ESET Mobile Security integrates completely with ESET Anti-Theft protection through the new ESET HOME portal. From the ESET Anti-Theft web portal, you are 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 ESET HOME account, tap **Create new account** and fill out the registration form. Check your email for the account confirmation and click the link inside to activate your account. After the account activation, you can remotely manage the ESET Anti-Theft security feature of the connected devices through the ESET HOME portal. If you already have a ESET HOME account, tap **Sign in** and type your email and password. When these steps are complete, you can associate the device with your ESET HOME account.

For further guidance on how to use ESET Anti-Theft features, refer to the Anti-Theft user guide or tap **Help** icon in the top right corner of the ESET HOME portal.

ESET HOME password

Change your forgotten password:

1.Visit https://login.eset.com/LostPassword.

2.Type the email address you used to register with ESET HOME and click **Send**.

3.Log in to your email account, open the **Account password change request - ESET HOME** email and click the link in the email.

4.Type and confirm a new password and click **Confirm Change**.

5.Type the new password on your device and tap **Unlock** to unlock your device.

Change your ESET HOME password:

1.Go to ESET HOME website.

2.Sign in using your email address and current password.
3.Click your email next to the down-facing arrow ⍰ in the top right corner.
4.Click **Change password**.

5.Type in your current password.

6.Type in your new password and confirm it.

7.Click **Save changes**.

Anti-Phishing

Phishing describes a criminal activity involving manipulating users into providing confidential information on a website that appears genuine but is not. This type of manipulation is known as social engineering. Phishing is often used to gain access to sensitive data such as bank account numbers, payment card numbers, PINs or usernames, and passwords.

Anti-Phishing in ESET Mobile Security protects against websites deemed malicious or dangerous.

We recommend that you keep **Anti-Phishing** enabled. When 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 and social network apps 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 because they do not provide sufficient integration for Anti-Phishing. To fully utilize the Anti-Phishing functionality, we recommend not using unsupported web browsers.

> For proper Anti-Phishing integration with web browsers, we recommend using Android 6 (Marshmallow) or later.

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 support 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)**.

To disable the Anti-Phishing, tap the three dots ⋮ in the Anti-Phishing section, and tap **Disable**.

Accessibility permission on ESET Mobile Security installed from the .APK file on Android 13

> Note
> For security reasons, Android 13 restricts accessibility permission to apps installed from .apk files to prevent uninformed access to these permissions.
> **How ESET Mobile Security uses this permission**
> We use this permission to access the URLs of websites you visit. We analyze these websites for malicious intent, such as phishing, malware or other dangerous activities.
> The website is blocked when a threat is detected to protect your sensitive data.
> Data accessed via accessibility permission are not shared with any third parties.

To solve the accessibility issue:

> Allow accessibility permission
> For the illustrated instructions, read our Knowledgebase article (it may only be available in English).

1. Open **Settings** > **Accessibility** > **Downloaded apps**, and the ESET Mobile Security is unavailable.

2. Tap the ESET Mobile Security app, and the **Restricted setting** dialog opens.

3. Tap **OK**.

4. Go to **Settings** > **Apps** > ESET Mobile Security to open the **App info**.

5. Tap the three-dot menu icon ⋮ in the upper right corner > **Allow restricted settings**.

Restricted settings are now allowed, and you can start using the application securely.

Anti-Phishing on Samsung DeX

Anti-Phishing is not supported on devices connected to the Samsung DeX station.

Protected Browsers

- Chrome
- Chrome Beta
- Firefox
- Firefox Beta
- Opera
- Opera Beta
- Opera Mini
- Opera Mini Beta
- Opera TV browser
- Samsung Internet
- Mint
- Yandex browser
- DuckDuckGo (in ESET Mobile Security version 6.1 and later)
- Kiwi browser
- Edge
- Silk in Amazon devices
- Mi browser
- Xiaomi Mi browser
- Vewd in Android TV

Protected social network apps

- Facebook
- Facebook Lite
- Messenger
- Messenger Lite

- Instagram
- Social network apps that use protected browser components for web view are also protected.

SMS and Notification protection

SMS and Notification protections protect you against smishing.

Smishing comes from combining the words phishing and SMS (Short Message Service). That is why it might sometimes be referred to as SMS phishing. Attackers use SMS messages, as people tend to trust messages more than email.

SMS protection guards you against smishing spread from the SMS message. But the threat could be spread also from any messaging platform. That is where Notification protection steps in. When you receive an SMS or a notification (for example, after receiving a message from Whatsapp), ESET Mobile Security analyses the link. Based on the analysis, there are three possible outcomes:

- No threat is found.
- Potentially unwanted content is found. The content of the message or notification might not pose any direct risk. The intent is not as unequivocally malicious as other types of malware, such as viruses or trojans. It may, however, install additional unwanted software, change the behavior of the digital device, or perform activities not approved or expected by the user.
- Dangerous content found. This message or notification contains dangerous or phishing links. We recommend you do not open the content and delete the message or notification.

> **Deleting messages and notifications**
> For security reasons, ESET Mobile Security cannot delete messages and notifications for you. You must delete the dangerous content manually.

How smishing works

1. An attacker sends you a message containing a link to a website.
2. The link usually leads to a phishing website that might lure you into providing your personal information. These can be used, for example, to steal money from you or commit further fraud. The link could also lead to a malicious website that contains malware or tries to trick you into downloading it.

Signs of smishing

- A suspicious phone number, for example, a foreign number or a number with a nonstandard length.
- The message contains unknown files or links.
- Smishing messages usually have an urgent tone.
- Smishing messages often pose as a prize or winning information.

App Lock

Use App Lock to secure access to selected applications (emails, messages, calendar, etc.) with a PIN code or fingerprint. App Lock prevents unauthorized access to selected applications even when the device is unlocked.

> Recommendation
>
> Turn on **Overlay** (**Apps that can appear on top**) permissions for ESET Mobile Security for better functionality.

To set up App Lock on your device:

1. Tap **App Lock** on the ESET Mobile Security main screen.

2. Tap **Enable**.

3. Allow Usage access permission, and click **Continue**.

4. Type your PIN, which unlocks applications.

5. Confirm your PIN by typing it again.

6. Tap an application to lock or unlock it.

Configure App Lock Settings

To access the App Lock settings, open the ⋮ menu in the top right corner, and click **Settings**:

- **Lock new apps** — With App Lock enabled, after installing a new application on your device, you are asked if you want to lock the new application.

- **Re-lock app** — You can set App Lock to lock an application immediately after it closes, after the screen turns off, or after a minute has passed.

- **Lock type** — You can lock your application using a PIN or a pattern.

- **Unlock with fingerprint** — This option is only available if a verified fingerprint is saved to your device. When this setting is enabled, you can unlock applications using the fingerprint saved to your device. You will still be able to unlock the application using the PIN. To do so, tap **Use PIN** when opening a locked application.

- **Intruder alert** — After a series of unsuccessful unlock attempts, ESET Mobile Security photographs the intruder. The photo is shown after the next successful unlock of the application.

Disable App Lock

1. Go to the App Lock feature in ESET Mobile Security.

2. Type your App Lock PIN.

3. Tap the menu ⋮ in the top right corner.

4. Tap **Disable**.

Activate Night mode

You can activate Night mode on your App Lock screen to make it easier for your eyes by tapping the night mode icon in the upper right corner.

I forgot my App Lock PIN

If you forget your App Lock PIN and do not have a fingerprint saved to your device, you have two options for unlocking a locked application, depending on your Anti-Theft settings:

- If you activated the Anti-Theft feature in ESET Mobile Security:

  1. Open ESET Mobile Security.
  2. Go to the App Lock feature.
  3. Type your PIN. **Tap Forgot your PIN?** in the middle of the screen.
  4. If the Anti-Theft feature is active, you are prompted to type your ESET HOME password. Type the password into the **Password** field and tap **Enter**.
  5. Type your new PIN and tap ⍰ to confirm it.
  6. Type the same PIN again to confirm it. Tap ⍰ when you are finished.

- If you did not activate the Anti-Theft feature, uninstall ESET Mobile Security and install it again.

Payment Protection

Payment Protection is an additional layer designed to protect your financial data on Android devices against advanced phishing and other threats. Payment Protection prevents other applications from noticing the launch of your protected applications and prevents them from replacing information or reading on-screen information from your protected application. Payment Protection scans every application that is in its list of protected applications. After activating Payment Protection, it will automatically add some banking and payment applications to the list of protected applications.

Add a new application to the list of protected applications

1. Open Payment Protection in the Apps menu or in the ESET Mobile Security.
2. Tap **Manage**.
3. Select applications you want to protect by Payment Protection.
4. Tap **OK** to confirm your selection.

Open a banking and payment application using Payment Protection

To ensure the highest protection of your banking and payment applications, open these applications from Safe Launcher. Safe Launcher provides an additional layer of protection compared with standard protection from the Payment Protection feature when opening application outside of the Safe launcher.
Safe Launcher is automatically created when Payment Protection is enabled. Safe Launcher contains all the applications that are protected by Payment Protection. Once you select the desired payment application, a quick Payment Protection scan is initiated and you get a notification with results of the scan.

What is Safe Launcher, and how can I access it?

You can find Safe Launcher in your applications list or in ESET Mobile Security > Payment Protection .

> **Access Safe Launcher**
> For quicker and easier access to your banking and payment applications, you can add Safe Launcher to your home screen. To add Safe Launcher to your home screen, long-press the Safe Launcher icon and drag it to your home screen.

Call Filter

Call Filter blocks incoming or outgoing calls based on rules that you set.

Call notifications will not be displayed when an incoming call is blocked. View the **Call log** to check for calls that may have been blocked by mistake.

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

Rules

To create a new rule, tap the + icon. See the next chapter for more information.

To modify an existing rule, tap the rule entry in the list of rules . To remove an entry from the **Rules** list, select the entry and tap **Remove**.

Call log

The **Call log** section displays the log of all calls blocked by the Call Filter. Each log contains the name of the call, corresponding phone number, and date and time of the event.

> **Devices without SIM card**
> **Call Filter** does not work on devices that do not support calling and messaging.

> **Outgoing calls**
> Call filter is not blocking outgoing call in ESET Mobile Security downloaded from Google Play.

> **Android support**
> Call Filter is available only on devices with Android 6 or later.

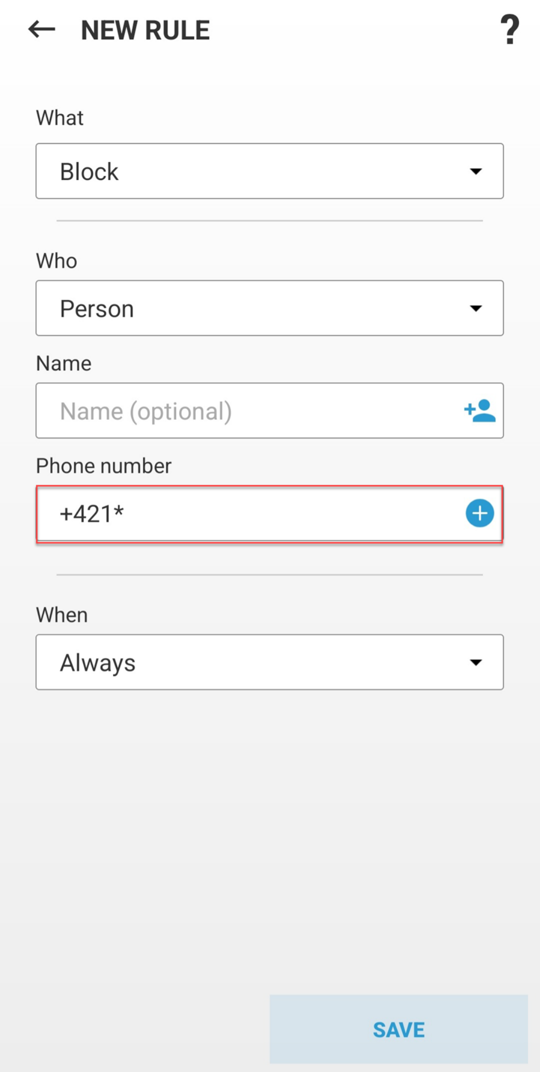
Block phone numbers using wildcards

You can block a range of numbers via wildcards described in the table below:

Wildcard	Description
*	represents multiple characters
?	represents a single character

✓ **Example**

If you do not want to receive calls from a specific country, type the country code and * wildcard character into the **Phone number** field, and all incoming calls from the country starting with this number pattern get blocked. When you decide to exclude some phone number from that country, add a new rule with the action **Allow**. The image below shows how to block all calls from Slovakia.



What: Block

Who: Person

Name: Name (optional)

Phone number: +421*

When: Always

Add a new rule

To create a new rule, tap the **+** icon.

1. In the **What** section, select either **Block** or **Allow** to specify the rule type for calls and messages. Select the calls direction to be blocked (Incoming is selected by default).

2.In the **Who** section, select an option to specify the phone numbers that will be affected by the rule.

- **Person** - Select a person from your contact list, or add the name and the numbers manually. You can assign more phone numbers to one name by clicking the **+** button in the **Phone number** section.
- **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.
- **All numbers** will block all incoming calls.
- **Hidden numbers** will apply to callers that have their phone number intentionally hidden via the Calling Line Identification Restriction (CLIR).

3.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.

Visit this Knowledgebase article for illustrated instructions.

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

Network Inspector

Network Inspector allows you to scan your network for devices connected to your router and to check for vulnerabilities. Network Inspector scans your network in two steps.

First Network Inspector scans your network for connected devices. If a new device is discovered, you will see a notification, and the device will be marked with the star symbol. Discover devices on your network manually, by tapping **Scan Network**. You can also discover devices automatically. To use this option, tap the menu icon ⋮ > **Settings** and allow the **Discover devices automatically** option.

In the second step of the scan, Network Inspector tests the connected devices for vulnerabilities by connecting to them and checking for safety issues such as open ports, weak router username, and password, router firmware problem, etc. These vulnerabilities can be leveraged by attackers to gain control of your router and other devices connected to it. Routers and devices that are controlled by attackers can then be used to collect information about you, or even participate in distributed denial-of-service attacks (DDoS), etc.

Network Inspector also provides you with a comprehensive list of devices connected to your network to keep you informed about who is connected to your network. Based on this information, you can manage or deny access these devices have to your network from your router's web interface. You can access your router's web interface directly from Network Inspector by selecting your router and tapping the **Open web interface** option.

You can view the connected devices as a list or as a visual:

- ☰ List view - Connected devices are displayed in a standard list view with the router on top followed by the online devices and ending with the history of previously connected devices.

- ◉ Sonar view - devices are displayed as a visual in a half-circle with the router in the center. In the second layer from the center are displayed devices that are online at the moment. In the third layer is displayed a history of previously connected devices. You can move between devices by tapping the arrow buttons or scroll in the circle direction.

For easier device management, assign a category to the device (such as Smartphone, TV, Gaming console, Computer, etc.), rename the devices from the standard manufacturers' names, or its IP address to more recognizable names (for example SM-G955F to Sam's phone, 192.168.1.52 to Jane's computer, etc.).

To rename the devices in Network Inspector, tap the device icon in Network Inspector > tap the pencil icon in the top right, select the device category, type in the device's name, and then tap **OK**.

Security Audit

Security Audit helps you monitor and change important device settings. Review the permissions given to each application installed on your device to prevent security risks.

To enable or disable Security Audit and its specific components, tap the menu button ⋮ and tap **Disable Device Monitoring** or **Disable Application Audit**.

- Device Monitoring
- Application Audit

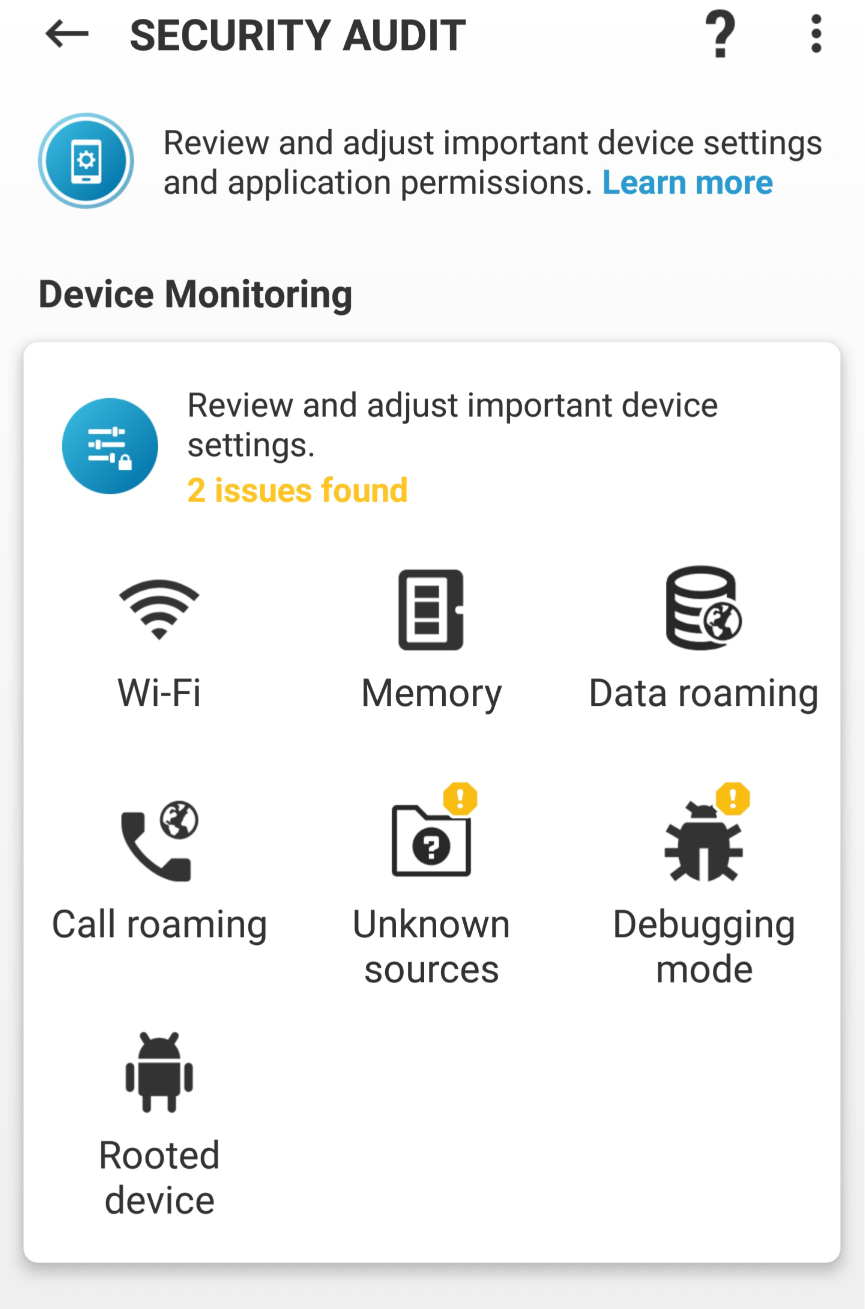
Device Monitoring

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**.

You can disable each component.

1. Tap the component you want to disable.
2. Tap the menu icon ⋮ .
3. Tap **Disable**.


SECURITY AUDIT

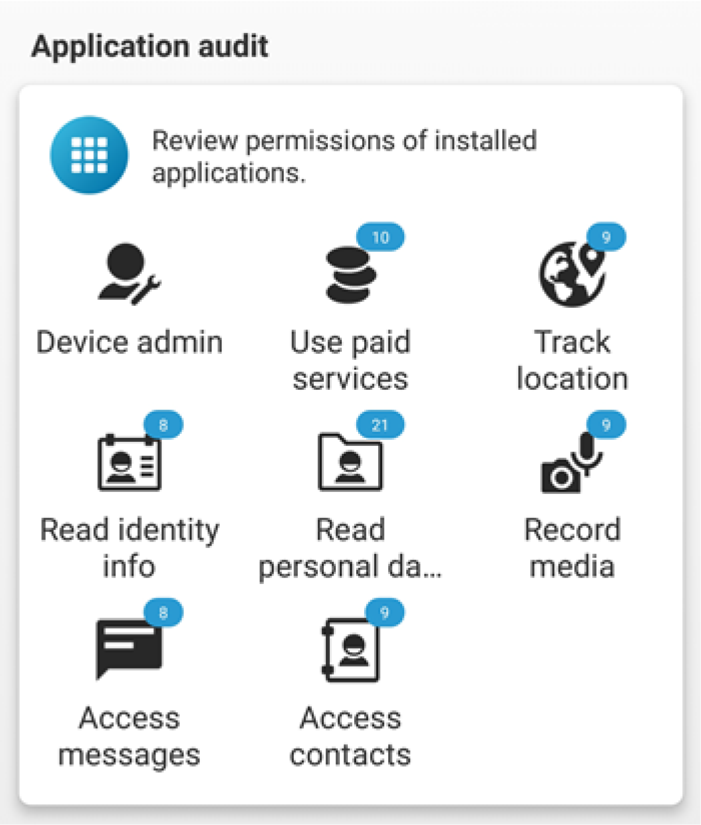
Review and adjust important device settings and application permissions. Learn more

Device Monitoring

Review and adjust important device settings.
2 issues found

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.



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**.

Backup & Restore

ESET Mobile Security allows you to create a backup file containing your ESET Mobile Security settings. You can download this file to an external device and use it to restore your ESET Mobile Security settings.

Language

By default, ESET Mobile Security is installed in the language set as the 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

(This option is available only for Android 7 and earlier)

ESET Mobile Security will display a notification on the bottom part of the Android notification bar. If you do not want the notification to be displayed, deselect Permanent notification and tap Turn off.

User consent

- **Allow ESET LiveGrid©**—To read more about **ESET LiveGrid©** feedback system, visit the Advanced settings section.

- **Allow analytics to help make our products better**—ESET Mobile Security will send anonymous application information (performance, operational statistics) that will help us improve our application and services. To read more about the information we collect, visit the Privacy Policy chapter.
- **Allow data usage for marketing purposes**

Update

For maximum protection, it is important to use the latest version of ESET Mobile Security. Tap **Update** to see if there is a later 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 Anti-Theft protection is activated, you will be prompted to enter your ESET Mobile Security security PIN/Pattern or your fingerprint. To uninstall the product manually, follow the steps described in this section.

> **Uninstall protection**
> Uninstall protection is not active in Android versions 7.0 and later.

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.

Contact ESET Customer Care

To send a support request directly from your device:

1. Tap Menu ☰ in the ESET Mobile Security main screen (or press the Menu button on your device).

2. Tap **Customer Care**.

3. Tap **Customer Care** to create a request for technical support.

4. Fill in all required fields. ESET Mobile Security includes advanced logging functionality to help diagnose potential technical issues.

5. To provide ESET with a detailed application log, make sure that **Submit application log** is selected (default).

6. Tap **Submit** to send your request.

7. An ESET Customer Care specialist will contact you at the email address you provided.

The diagnostic logs were deleted if you uninstalled and reinstalled ESET Mobile Security as part of troubleshooting. We recommend replicating the problem again and sending the logs afterward.

Application is unable to open or is not responding

To submit support request to ESET if ESET Mobile Security is not responding or you are unable to open it, go to **Settings** > **Applications** > **ESET Mobile Security** > **Storage** > **Manage Storage**. Click **Customer care** and fill in all required fields.

End User License Agreement

Effective as of October 19, 2021.

IMPORTANT: Please read the terms and conditions of product application set out below carefully prior to download, installation, copy or use. **THROUGH DOWNLOADING, INSTALLING, COPYING OR USING THE SOFTWARE YOU ARE EXPRESSING YOUR CONSENT TO THESE TERMS AND CONDITIONS AND YOU ACKNOWLEDGE PRIVACY POLICY.**

End User License Agreement

Under the terms of this End User License Agreement ("Agreement") executed by and between ESET, spol. s r. o., having its registered office at Einsteinova 24, 85101 Bratislava, Slovak Republic, registered in the Commercial Register administered by Bratislava I District Court, Section Sro, Entry No 3586/B, Business Registration Number: 31333532 ("ESET" or "Provider") and you, a physical person or legal entity ("You" or "End User"), You are entitled to use the Software defined in Article 1 of this Agreement. The Software defined in Article 1 of this Agreement can be stored on a data carrier, sent via electronic mail, downloaded from the Internet, downloaded from the Provider's servers or obtained from other sources, subject to the terms and conditions specified below.

THIS IS AN AGREEMENT ON END USER RIGHTS AND NOT AN AGREEMENT FOR SALE. The Provider continues to own the copy of the Software and the physical media contained in the sales package and any other copies that the End User is authorized to make pursuant to this Agreement.

By clicking on "I Accept" or "I Accept…" while installing, downloading, copying or using the Software, You agree to the terms and conditions of this Agreement and acknowledge the Privacy Policy. If You do not agree to all of the terms and conditions of this Agreement and/or Privacy Policy, immediately click on the canceling option, cancel the installation or download, or destroy or return the Software, installation media, accompanying documentation and sales receipt to the Provider or the outlet from which You acquired the Software.

YOU AGREE THAT YOUR USE OF THE SOFTWARE ACKNOWLEDGES THAT YOU HAVE READ THIS AGREEMENT, UNDERSTAND IT AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS.

1. **Software**. As used in this Agreement the term "Software" means: (i) computer program accompanied by this Agreement and all components thereof; (ii) all the contents of the disks, CD-ROMs, DVDs, e-mails and any attachments, or other media with which this Agreement is provided, including the object code form of the Software supplied on a data carrier, via electronic mail or downloaded via the Internet; (iii) any related explanatory written materials and any other possible documentation related to the Software, above all any description of the Software, its specifications, any description of the Software properties or operation, any description of the operating environment in which the Software is used, instructions for use or installation of the Software or any description of how to use the Software ("Documentation"); (iv) copies of the Software, patches for possible errors in the Software, additions to the Software, extensions to the Software, modified versions of the Software and updates of Software components, if any, licensed to You by the Provider pursuant to Article 3 of this Agreement. The Software shall be provided exclusively in the form of executable object code.

2. **Installation, Computer and a License key**. Software supplied on a data carrier, sent via electronic mail, downloaded from the Internet, downloaded from the Provider's servers or obtained from other sources requires

installation. You must install the Software on a correctly configured Computer, complying at least with requirements set out in the Documentation. The installation methodology is described in the Documentation. No computer programs or hardware which could have an adverse effect on the Software may be installed on the Computer on which You install the Software. Computer means hardware, including but not limited to personal computers, laptops, workstations, palmtop computers, smartphones, hand-held electronic devices, or other electronic devices for which the Software is designed, on which it will be installed and/or used. License key means the unique sequence of symbols, letters, numbers or special signs provided to the End User in order to allow the legal use of the Software, its specific version or extension of the term of the License in compliance with this Agreement.

3. **License**. Subject to the condition that You have agreed to the terms of this Agreement and You comply with all the terms and conditions stipulated herein, the Provider shall grant You the following rights ("License"):

a) **Installation and use**. You shall have the non-exclusive, non-transferable right to install the Software on the hard disk of a Computer or other permanent medium for data storage, installation and storage of the Software in the memory of a computer system and to implement, store and display the Software.

b) **Stipulation of the number of licenses.** The right to use the Software shall be bound by the number of End Users. One End User shall be taken to refer to the following: (i) installation of the Software on one Computer; or (ii) if the extent of a license is bound to the number of mailboxes, then one End User shall be taken to refer to a Computer user who accepts electronic mail via a Mail User Agent ("MUA"). If MUA accepts electronic mail and subsequently distributes it automatically to several users, then the number of End Users shall be determined according to the actual number of users for whom the electronic mail is distributed. If a mail server performs the function of a mail gate, the number of End Users shall equal the number of mail server users for which the said gate provides services. If an unspecified number of electronic mail addresses are directed to and accepted by one user (e.g., through aliases) and messages are not automatically distributed by the client to a larger number of users, a License for one computer shall be required. You must not use the same License at the same time on more than one Computer. The End User is entitled to enter the License key to the Software only to the extent to which the End User has the right to use the Software in accordance with the limitation arising from the number of Licenses granted by Provider. The License key is deemed confidential, You must not share the License with third parties or allow third parties to use the License key unless permitted by this Agreement or Provider. If your License key is compromised, notify Provider immediately.

c) **Home/Business Edition.** A Home Edition version of the Software shall be used exclusively in private and/or non-commercial environments for home and family use only. A Business Edition version of the Software must be obtained for use in a commercial environment as well as to use the Software on mail servers, mail relays, mail gateways, or Internet gateways.

d) **Term of the License.** Your right to use the Software shall be time-limited.

e) **OEM Software.** Software classified as "OEM" shall be limited to the Computer You obtained it with. It cannot be transferred to a different Computer.

f) **NFR, TRIAL Software.** Software classified as "Not-for-resale", NFR or TRIAL cannot be assigned for payment and must only be used for demonstration or testing the Software's features.

g) **Termination of the License.** The License shall terminate automatically at the end of the period for which granted. If You fail to comply with any of the provisions of this Agreement, the Provider shall be entitled to withdraw from the Agreement, without prejudice to any entitlement or legal remedy open to the Provider in such eventualities. In the event of cancellation of the License, You must immediately delete, destroy or return at your own cost, the Software and all backup copies to ESET or to the outlet from which You obtained the Software. Upon termination of the License, the Provider shall also be entitled to cancel the End User's entitlement to use the functions of the Software, which require connection to the Provider's servers or third-party servers.

4. **Functions with data collection and internet connection requirements.** To operate correctly, the Software requires connection to the Internet and must connect at regular intervals to the Provider's servers or third-party servers and applicable data collection in compliance with Privacy Policy. Connection to the Internet and applicable data collection is necessary for the following functions of the Software:

a) **Updates to the Software.** The Provider shall be entitled from time to issue updates or upgrades to the Software ("Updates"), but shall not be obliged to provide Updates. This function is enabled under the Software's standard settings and Updates are therefore installed automatically, unless the End User has disabled the automatic installation of Updates. For provisioning of Updates, License authenticity verification is required, including information about Computer and/or the platform on which the Software is installed in compliance with Privacy Policy.

Provision of any Updates may be subject to End of Life Policy ("EOL Policy"), which is available on https://go.eset.com/eol_home. No Updates will be provided after the Software or any of its features reaches the End of Life date as defined in the EOL Policy.

b) **Forwarding of infiltrations and information to the Provider.** The Software contains functions which collect samples of computer viruses and other malicious computer programs and suspicious, problematic, potentially unwanted or potentially unsafe objects such as files, URLs, IP packets and ethernet frames ("Infiltrations") and then send them to the Provider, including but not limited to information about the installation process, the Computer and/or the platform on which the Software is installed and, information about the operations and functionality of the Software ("Information"). The Information and Infiltrations may contain data (including randomly or accidentally obtained personal data) about the End User or other users of the Computer on which the Software is installed, and files affected by Infiltrations with associated metadata.

Information and Infiltrations may be collected by following functions of Software:

i. LiveGrid Reputation System function includes collection and sending of one-way hashes related to Infiltrations to Provider. This function is enabled under the Software's standard settings.

ii. LiveGrid Feedback System function includes collection and sending of Infiltrations with associated metadata and Information to Provider. This function may be activated by End User during the process of installation of the Software.

The Provider shall only use Information and Infiltrations received for the purpose of analysis and research of Infiltrations, improvement of Software and License authenticity verification and shall take appropriate measures to ensure that Infiltrations and Information received remain secure. By activating this function of the Software, Infiltrations and Information may be collected and processed by the Provider as specified in Privacy Policy and in compliance with relevant legal regulations. You can deactivate these functions at any time.

For the purpose of this Agreement, it is necessary to collect, process and store data enabling the Provider to identify You in compliance with Privacy Policy. You hereby acknowledge that the Provider checks using its own means whether You are using the Software in accordance with the provisions of this Agreement. You hereby acknowledge that for the purpose of this Agreement it is necessary for your data to be transferred, during communication between the Software and the Provider's computer systems or those of its business partners as part of Provider’s distribution and support network to ensure functionality of Software and authorization to use the Software and to protection of the Provider’s rights.

Following conclusion of this Agreement, the Provider or any of its business partners as part of Provider’s distribution and support network shall be entitled to transfer, process and store essential data identifying You for billing purposes, performance of this Agreement and transmitting notifications on your Computer.

Details about privacy, personal data protection and Your rights as a data subject can be found in Privacy Policy which is available on Provider’s website and accessible directly from the installation process. You can also visit it from Software’s help section.

5. **Exercising End User rights**. You must exercise End User rights in person or via your employees. You are only entitled to use the Software to safeguard your operations and protect those Computers or computers systems for which You have obtained a License.

6. **Restrictions to rights.** You may not copy, distribute, extract components or make derivative works of the Software. When using the Software, You are required to comply with the following restrictions:

a) You may make one copy of the Software on a permanent storage medium as an archival backup copy, provided your archival back-up copy is not installed or used on any Computer. Any other copies You make of the Software shall constitute a breach of this Agreement.

b) You may not use, modify, translate or reproduce the Software or transfer rights to use the Software or copies of the Software in any manner other than as provided for in this Agreement.

c) You may not sell, sub-license, lease or rent or borrow the Software or use the Software for the provision of commercial services.

d) You may not reverse engineer, reverse compile or disassemble the Software or otherwise attempt to discover the source code of the Software, except to the extent that this restriction is expressly prohibited by law.

e) You agree that You will only use the Software in a manner that complies with all applicable laws in the jurisdiction in which You use the Software, including, but not limited to, applicable restrictions concerning copyright and other intellectual property rights.

f) You agree that You will only use the Software and its functions in a way which does not limit the possibilities of other End Users to access these services. The Provider reserves the right to limit the scope of services provided to individual End Users, to enable use of the services by the highest possible number of End Users. Limiting the scope of services shall also mean complete termination of the possibility to use any of the functions of the Software and deletion of Data and information on the Provider's servers or third-party servers relating to a specific function of the Software.

g) You agree not to exercise any activities involving use the License key, contrary to the terms of this Agreement or leading to provide License key to any person who is not entitled to use the Software, such as the transfer of used or unused License key in any form, as well as the unauthorized reproduction, or distribution of duplicated or generated License keys or using the Software as a result of the use of a License key obtained from the source other than the Provider.

7. **Copyright**. The Software and all rights, without limitation including proprietary rights and intellectual property rights thereto are owned by ESET and/or its licensors. They are protected by international treaty provisions and by all other applicable national laws of the country in which the Software is being used. The structure, organization and code of the Software are the valuable trade secrets and confidential information of ESET and/or its licensors. You must not copy the Software, except as set forth in Article 6(a). Any copies which You are permitted to make pursuant to this Agreement must contain the same copyright and other proprietary notices that appear on the Software. If You reverse engineer, reverse compile, disassemble or otherwise attempt to discover the source code of the Software, in breach of the provisions of this Agreement, You hereby agree that any information thereby obtained shall automatically and irrevocably be deemed to be transferred to and owned by the Provider in full, from the moment such information comes into being, notwithstanding the Provider's rights in relation to breach of this Agreement.

8. **Reservation of rights**. The Provider hereby reserves all rights to the Software, with the exception of rights expressly granted under the terms of this Agreement to You as the End User of the Software.

9. **Multiple language versions, dual media software, multiple copies**. In the event that the Software supports multiple platforms or languages, or if You receive multiple copies of the Software, You may only use the Software for the number of computer systems and for the versions for which You obtained a License. You may not sell, rent, lease, sub-license, lend or transfer versions or copies of the Software which You do not use.

10. **Commencement and termination of the Agreement.** This Agreement shall be effective from the date You agree to the terms of this Agreement. You may terminate this Agreement at any time by permanently uninstalling, destroying and returning, at your own cost, the Software, all backup copies and all related materials provided by the Provider or its business partners. Your right to use Software and any of its features may be subject to EOL Policy. After the Software or any of its features reaches the End of Life date defined in the EOL Policy, your right to use the Software will terminate. Irrespective of the manner of termination of this Agreement, the provisions of Articles 7, 8, 11, 13, 19 and 21 shall continue to apply for an unlimited time.

11. **END USER DECLARATIONS**. AS THE END USER YOU ACKNOWLEDGE THAT THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW. NEITHER THE PROVIDER, ITS LICENSORS OR AFFILIATES, NOR THE COPYRIGHT HOLDERS MAKE ANY REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR THAT THE SOFTWARE WILL NOT INFRINGE ANY THIRD-PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. THERE IS NO WARRANTY BY THE PROVIDER OR BY ANY OTHER PARTY THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE. YOU ASSUME ALL RESPONSIBILITY AND RISK FOR THE SELECTION OF THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS AND FOR THE INSTALLATION, USE AND RESULTS OBTAINED FROM IT.

12. **No other obligations**. This Agreement creates no obligations on the part of the Provider and its licensors other than as specifically set forth herein.

13. **LIMITATION OF LIABILITY**. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE PROVIDER, ITS EMPLOYEES OR LICENSORS BE LIABLE FOR ANY LOST PROFITS, REVENUE, SALES, DATA OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, PROPERTY DAMAGE, PERSONAL INJURY, INTERRUPTION OF BUSINESS, LOSS OF BUSINESS INFORMATION OR FOR ANY SPECIAL, DIRECT, INDIRECT, INCIDENTAL, ECONOMIC, COVER, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND WHETHER ARISING UNDER CONTRACT, TORT, NEGLIGENCE OR OTHER THEORY OF LIABILITY, ARISING OUT OF THE INSTALLATION, THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF THE PROVIDER OR ITS LICENSORS OR AFFILIATES ARE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME COUNTRIES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF LIABILITY, BUT MAY ALLOW LIABILITY TO BE LIMITED, IN SUCH CASES, THE LIABILITY OF THE PROVIDER, ITS EMPLOYEES OR LICENSORS OR AFFILIATES SHALL BE LIMITED TO THE SUM THAT YOU PAID FOR THE LICENSE.

14. Nothing contained in this Agreement shall prejudice the statutory rights of any party dealing as a consumer if running contrary thereto.

15. **Technical support**. ESET or third parties commissioned by ESET shall provide technical support at their own discretion, without any guarantees or declarations. No technical support will be provided after the Software or any of its features reaches the End of Life date defined in the EOL Policy. The End User shall be required to back up all existing data, software and program facilities prior to the provision of technical support. ESET and/or third parties commissioned by ESET cannot accept liability for damage or loss of data, property, software or hardware or loss of profits due to the provision of technical support. ESET and/or third parties commissioned by ESET reserve the right to decide that resolving the problem is beyond the scope of technical support. ESET reserves the

right to refuse, suspend or terminate the provision of technical support at its own discretion. License information, Information and other data in compliance with Privacy Policy may be required for the purpose of technical support provision.

16. **Transfer of the License**. The Software can be transferred from one Computer to another, unless contrary to the terms of the Agreement. If not contrary to the terms of the Agreement, the End User shall only be entitled to permanently transfer the License and all rights ensuing from this Agreement to another End User with the Provider's consent, subject to the condition that (i) the original End User does not retain any copies of the Software; (ii) the transfer of rights must be direct, i.e. from the original End User to the new End User; (iii) the new End User must assume all the rights and obligations incumbent on the original End User under the terms of this Agreement; (iv) the original End User has to provide the new End User with documentation enabling verification of the genuineness of the Software as specified under Article 17.

17. **Verification of the genuineness of the Software.** The End User may demonstrate entitlement to use the Software in one of the following ways: (i) through a license certificate issued by the Provider or a third party appointed by the Provider; (ii) through a written license agreement, if such an agreement was concluded; (iii) through the submission of an e-mail sent by the Provider containing licensing details (user name and password). License information and End User identification data in compliance with Privacy Policy may be required for the purpose of Software genuineness verification.

18. **Licensing for public authorities and the US Government**. The Software shall be provided to public authorities, including the United States Government, with the license rights and restrictions described in this Agreement.

19. **Trade control compliance**.

a) You will not, directly or indirectly, export, re-export, transfer or otherwise make available the Software to any person, or use it in any manner, or be involved in any activity, that could result in ESET or its holding companies, its subsidiaries, and the subsidiaries of any of its holding companies, as well as entities controlled by its holding companies ("Affiliates") being in violation of, or being subject to, negative consequences under trade control laws which include:

i. any laws that control, restrict, or impose licensing requirements on export, re-export or transfer of goods, software, technology, or services, issued or adopted by any government, state or regulatory authority of the United States of America, Singapore, the United Kingdom, the European Union or any of its Member States, or any country in which obligations under the Agreement are to be performed, or in which ESET or any of its Affiliates are incorporated or operate, and

ii. any economic, financial, trade or other, sanction, restriction, embargo, import or export ban, prohibition on transfer of funds or assets or on performing services, or equivalent measure imposed by any government, state or regulatory authority of the United States of America, Singapore, the United Kingdom, the European Union or any of its Member States, or any country in which obligations under the Agreement are to be performed, or in which ESET or any of its Affiliates are incorporated or operate.

(legal acts referred to in points i, and ii. above together as "Trade Control Laws").

b) ESET shall have the right to suspend its obligations under, or terminate, these Terms with immediate effect in the event that:

i. ESET determines that, in its reasonable opinion, the User has breached or is likely to breach provision of Article 19 a) of the Agreement; or

ii. the End User and/or the Software become subject to Trade Control Laws and, as a result, ESET determines that, in its reasonable opinion, the continued performance of its obligations under the Agreement could result in ESET or its Affiliates being in violation of, or being subject to negative consequences under, Trade Control Laws.

c) Nothing in the Agreement is intended, and nothing should be interpreted or construed, to induce or require either party to act or refrain from acting (or to agree to act or refrain from acting) in any manner which is inconsistent with, penalized, or prohibited under any applicable Trade Control Laws.

20. **Notices**. All notices and returns of the Software and Documentation must be delivered to: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, without prejudice to ESET's right to communicate to You any changes to this Agreement, Privacy Policies, EOL Policy and Documentation in accordance with art. 22 of the Agreement. ESET may send You emails, in-app notifications via Software or post the communication on our website. You agree to receive legal communications from ESET in electronic form, including any communications on change in Terms, Special Terms or Privacy Policies, any contract proposal/acceptance or invitations to treat, notices or other legal communications. Such electronic communication shall be deemed as received in writing, unless applicable laws specifically require a different form of communication.

21. **Applicable law**. This Agreement shall be governed by and construed in accordance with the laws of the Slovak Republic. The End User and the Provider hereby agree that the principles of the conflict of laws and the United Nations Convention on Contracts for the International Sale of Goods shall not apply. You expressly agree that any disputes or claims ensuing from this Agreement with respect to the Provider or any disputes or claims relating to use of the Software shall be settled by Bratislava I District Court and You expressly agree to the said court exercising jurisdiction.

22. **General provisions**. Should any of the provisions of this Agreement be invalid or unenforceable, this shall not affect the validity of the other provisions of the Agreement, which shall remain valid and enforceable under the conditions stipulated therein. This Agreement has been executed in English. In case any translation of the Agreement is prepared for the convenience or any other purpose or in any case of a discrepancy between language versions of this Agreement, the English version shall prevail.

ESET reserves the right to make changes to the Software as well as to revise terms of this Agreement, its Annexes, Addendums, Privacy Policy, EOL Policy and Documentation or any part thereof at any time by updating the relevant document (i) to reflect changes to the Software or to how ESET does business, (ii) for legal, regulatory or security reasons, or (iii) to prevent abuse or harm. You will be notified about any revision of the Agreement by email, in-app notification or by other electronic means. If You disagree with the proposed changes to the Agreement, You may terminate it in accordance with Art. 10 within 30 days after receiving a notice of the change. Unless You terminate the Agreement within this time limit, the proposed changes will be deemed accepted and become effective towards You as of the date You received a notice of the change.

This is the entire Agreement between the Provider and You relating to the Software and it supersedes any prior representations, discussions, undertakings, communications or advertising relating to the Software.

ADDENDUM TO THE AGREEMENT

Network Connected Devices Security Assessment. Additional provisions apply to the Network Connected Devices Security Assessment as follows:

The Software contains a function for checking the security of End User's local network and security of devices in local network which requires local network name and information about devices in local network such as presence, type, name, IP address and MAC address of device in local network in connection with license information. The information also includes wireless security type and wireless encryption type for router devices. This function may also provide information concerning availability of security software solution to secure devices in local network.

Protection Against Misuse of Data. Additional provisions apply to the Protection Against Misuse of Data as follows:

The Software contains a function that prevents loss or misuse of critical data in direct connection with theft of a Computer. This function is switched off under the default settings of the Software. The ESET HOME Account needs to be created for it to be activated, through which the function activates data collection in the event of computer theft. If you chose to activate this function of the Software, data about the stolen Computer will be collected and sent to the Provider, which can include data about the Computer's network location, data about the content displayed on the Computer screen, data about the configuration of the Computer and/or data recorded by a camera connected to the Computer (hereinafter referred to as "Data"). The End User shall be entitled to use Data obtained by this function and provided via ESET HOME Account exclusively for rectifying an adverse situation caused by theft of a Computer. For the sole purpose of this function, Provider process Data as specified in Privacy Policy and in compliance with relevant legal regulations. The Provider shall allow End User to access the Data for the period required to achieve the purpose for which the data was obtained which shall not exceed retention period specified in Privacy Policy. Protection against misuse of data shall be used exclusively with Computers and accounts End User have legitimate access to. Any illegal use will be reported to competent authority. Provider will comply with relevant laws and assist law enforcement authorities in case of the misuse. You agree and acknowledge that You are responsible for safeguarding the password to access ESET HOME Account and you agree that You shall not disclose your password to any third party. End User is responsible for any activity using Protection Against Misuse of Data function and ESET HOME Account, authorized or not. If ESET HOME Account is compromised, notify Provider immediately.

Codes. Additional provisions apply to the Codes as follows:

ESET may create and provide referral code and/or other code for promotional or marketing purposes (hereinafter referred to as "Code") at its own discretion. You may redeem the Code to prolong term of license in compliance with this Agreement. ESET reserves the right to disable the Code at any time when the Code is obtained or used in manner not compliant with this Agreement and/or in case of reasonable believe that error, fraud or illegal activity is involved. You are required to comply with the following restrictions:

i. You may not redeem the Code more than one time.

ii. You may not sell, lease or rent the Code or use the Code for the provision of commercial services.

iii. You agree that ESET may disable provision and/or use of the Code at any time without any liability to ESET.

iv. You agree that Code is not valid for cash or any other compensation.

v. You agree that the Code and/or Code usage may be subject to special terms provided by ESET for the specific referral, promotional and/or marketing campaign.

EULAID: EULA-PRODUCT-LG-EMS; 3537.0

Privacy Policy

The protection of personal data is of particular importance to ESET, spol. s r. o., having its registered office at Einsteinova 24, 851 01 Bratislava, Slovak Republic, registered in the Commercial Register administered by Bratislava I District Court, Section Sro, Entry No 3586/B, Business Registration Number: 31333532 as a Data Controller ("ESET" or "We"). We want to comply with the transparency requirement as legally standardized under the EU General Data Protection Regulation ("GDPR"). To achieve this goal, We are publishing this Privacy Policy with the sole purpose of informing our customer ("End User" or "You") as a data subject about following personal data protection topics:

- Legal Basis of Personal Data Processing,
- Data Sharing and Confidentiality,
- Data Security,
- Your Rights as a Data Subject,
- Processing of Your Personal Data
- Contact Information.

Legal Basis of Personal Data Processing

There are a few legal bases for data processing which We use according to the applicable legislative framework related to protection of personal data. The processing of personal data at ESET is mainly necessary for the performance of the End User License Agreement ("EULA") with End User (Art. 6 (1) (b) GDPR), which is applicable for the provision of ESET products or services, unless explicitly stated otherwise, e.g.:

- Legitimate interest legal basis (Art. 6 (1) (f) GDPR), that enables us to process data on how our customers use our Services and their satisfaction to provide our users with the best protection, support and experience We can offer. Even marketing is recognized by applicable legislation as a legitimate interest, therefore We usually rely on it for marketing communication with our customers.
- Consent (Art. 6 (1) (a) GDPR), which We may request from You in specific situations when we deem this legal basis as the most suitable one or if it is required by law.
- Compliance with a legal obligation (Art. 6 (1) (c) GDPR), e.g. stipulating requirements for electronic communication, retention for invoicing or billing documents.

Data Sharing and Confidentiality

We do not share your data with third parties. However, ESET is a company that operates globally through affiliated companies or partners as part of our sales, service and support network. Licensing, billing and technical support information processed by ESET may be transferred to and from affiliates or partners for the purpose of fulfilling the EULA, such as providing services or support.

ESET prefers to process its data in the European Union (EU). However, depending on your location (use of our products and/or services outside the EU) and/or the service you choose, it may be necessary to transfer your data to a country outside the EU. For example, we use third-party services in connection with cloud computing. In these cases, we carefully select our service providers and ensure an appropriate level of data protection through contractual as well as technical and organizational measures. As a rule, we agree on the EU standard contractual clauses, if necessary, with supplementary contractual regulations.

For some countries outside the EU, such as the United Kingdom and Switzerland, the EU has already determined a comparable level of data protection. Due to the comparable level of data protection, the transfer of data to these countries does not require any special authorization or agreement.

Data Security

ESET implements appropriate technical and organizational measures to ensure a level of security which is appropriate to potential risks. We are doing our best to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services. However, in case of data breach resulting in a risk to your rights and freedoms, We are ready to notify the relevant supervisory authority as well as affected End Users as data subjects.

Data Subject’s Rights

The rights of every End User matter and We would like to inform you that all End Users (from any EU or any non-EU country) have the following rights guaranteed at ESET. To exercise your data subject’s rights, you can contact us via support form or by e-mail at dpo@eset.sk. For identification purposes, we ask you for the following information: Name, e-mail address and - if available - license key or customer number and company affiliation. Please refrain from sending us any other personal data, such as the date of birth. We would like to point out that to be able to process your request, as well as for identification purposes, we will process your personal data.

Right to Withdraw the Consent. Right to withdraw the consent is applicable in case of processing based on consent only. If We process your personal data on the basis of your consent, you have the right to withdraw the consent at any time without giving reasons. The withdrawal of your consent is only effective for the future and does not affect the legality of the data processed before the withdrawal.

Right to Object. Right to object the processing is applicable in case of processing based on the legitimate interest of ESET or third party. If We process your personal data to protect a legitimate interest, You as the data subject have the right to object to the legitimate interest named by us and the processing of your personal data at any time. Your objection is only effective for the future and does not affect the lawfulness of the data processed before the objection. If we process your personal data for direct marketing purposes, it is not necessary to give reasons for your objection. This also applies to profiling, insofar as it is connected with such direct marketing. In all other cases, we ask you to briefly inform us about your complaints against the legitimate interest of ESET to process your personal data.

Please note that in some cases, despite your consent withdrawal, we are entitled to further process your personal data on the basis of another legal basis, for example, for the performance of a contract.

Right of Access. As a data subject, you have the right to obtain information about your data stored by ESET free of charge at any time.

Right to Rectification. If we inadvertently process incorrect personal data about you, you have the right to have this corrected.

Right to Erasure and Right to Restriction of Processing. As a data subject, you have the right to request the deletion or restriction of the processing of your personal data. If we process your personal data, for example, with your consent, you withdraw it and there is no other legal basis, for example, a contract, We delete your personal data immediately. Your personal data will also be deleted as soon as they are no longer required for the purposes stated for them at the end of our retention period.

If we use your personal data for the sole purpose of direct marketing and you have revoked your consent or objected to the underlying legitimate interest of ESET, We will restrict the processing of your personal data to the extent that we include your contact data in our internal black list in order to avoid unsolicited contact. Otherwise, your personal data will be deleted.

Please note that We may be required to store your data until the expiry of the retention obligations and periods issued by the legislator or supervisory authorities. Retention obligations and periods may also result from the Slovak legislation. Thereafter, the corresponding data will be routinely deleted.

Right to Data Portability. We are happy to provide You, as a data subject, with the personal data processed by ESET in the xls format.

Right to Lodge a Complaint. As a data subject, You have a right to lodge a complaint with a supervisory authority at any time. ESET is subject to the regulation of Slovak laws and We are bound by data protection legislation as part of the European Union. The relevant data supervisory authority is The Office for Personal Data Protection of the Slovak Republic, located at Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Processing of Your Personal Data

Services provided by ESET implemented in our product are provided under the terms of EULA, but some of them might require specific attention. We would like to provide You with more details on data collection connected with the provision of our services. We render various services described in the EULA and the product documentation. To make it all work, We need to collect the following information:

Licensing and Billing Data. The name, e-mail address, license key and (if applicable) address, company affiliation and payment data are collected and processed by ESET in order to facilitate the activation of license, license key delivery, reminders on expiration, support requests, license genuineness verification, provision of our service sand other notifications including marketing messages in line with applicable legislation or Your consent. ESET is legally obliged to keep the billing information for the period of 10 years, however the licensing information will be anonymized no later than 12 months after the expiration of license.

Update and Other Statistics. The processed information includes information concerning installation process and your computer including platform on which our product is installed and information about the operations and functionality of our products such as operation system, hardware information, installation IDs, license IDs, IP address, MAC address, configuration settings of product are processed for the purpose of provision update and upgrade services and for the purpose of maintenance, security and improvement of our backend infrastructure.

This information is kept apart from the identification information required for the licensing and billing purposes since it does not require the identification of End User. The retention period is up to 4 years.

ESET LiveGrid® Reputation System. One-way hashes related to infiltration are processed for the purpose of ESET LiveGrid® Reputation System which improves the efficiency of our anti-malware solutions by comparing scanned files to a database of whitelisted and blacklisted items in the cloud. The End User is not identified during this process.

ESET LiveGrid® Feedback System. Suspicious samples and metadata from the wild are collected as part of ESET LiveGrid® Feedback System which enables ESET to react immediately to needs of our end users and keep us responsive to the latest threats providing. We are dependent on You sending us

- Infiltrations such as potential samples of viruses and other malicious programs and suspicious; problematic, potentially unwanted or potentially unsafe objects such as executable files, email messages reported by You as spam or flagged by our product;
- Information concerning the use of internet such as IP address and geographic information, IP packets, URLs and ethernet frames;
- Crash dump files and information contained.

We do not desire to collect your data outside of this scope but sometimes it is impossible to prevent it. Accidentally collected data may be included in malware itself (collected without our knowledge or approval) or as part of filenames or URLs and We do not intend it to form part of our systems or process it for the purpose declared in this Privacy Policy.

All information obtained and processed through the ESET LiveGrid® Feedback System are meant to be used without the identification of End User.

Network Connected Devices Security Assessment. To provide the security assessment function, We process the local network name and information about devices in your local network, such as presence, type, name, IP address and MAC address of the device in your local network in connection with license information. The information also includes wireless security type and wireless encryption type for router devices. The license information identifying the End User will be anonymized no later than 12 months after the expiration of the license.

Technical Support. The contact and licensing information and data contained in your support requests may be required for service of support. Based on the channel You choose to contact us, We may collect your email address, phone number, license information, product details and description of your support case. You may be asked to provide us with other information to facilitate service of support. The data processed for technical support is stored for 4 years.

Protection Against Misuse of Data. If You create the ESET HOME Account on https://home.eset.com and mark your device as missing via the Anti-theft function, the following information will be collected and processed: the location data, screenshots, data about the configuration of a computer and data recorded by a computer's camera. The collected data is stored on our servers or our service providers' servers with a retention period of 3 months.

Usage and Crash Analytics. Based on your opt-in consent, we will collect and analyze data relating to the use of our products to test their performance and improve them for our users. Collected data may include various user actions and events happening in the product (for example, launching the app, app update, session duration, in-app purchase), information on a used device, platform or operating system, as well as data related to your age, gender, location and interests, that may be associated with various identifiers (for example installation IDs). Moreover, we will process technical data related to the application crashes (such as device information, installation identifier, crash traces, crash minidump) to get insight into the crashes, learn about their causes and ensure our product is fully operational. To collect and analyze those data, We use our Customer Experience Improvement Program (where only anonymous telemetry data is processed) and Google services to obtain more in-depth insight. To learn more about the processing of your data by Google, refer to the relevant Google Privacy Policy.

Processing for Marketing Purposes. If you choose to grant us your consent for marketing purposes, We and our marketing partners will use data about your usage of our product to evaluate the performance of our online marketing activities, understand your interests better and show You online advertisements that should be more relevant for you. Collected data may include various user actions and events happening in the product (for example, launching the app, app update, session duration, in-app purchase), information on a used device, platform or operating system, as well as data related to your age, gender, location and interests, that may be associated with various identifiers (installation IDs, mobile ad ID). We use Google to collect and analyze those data for us. To learn more about the processing of your data by Google, refer to the relevant Google Privacy Policy.

Please note that if the person using our products and services is not the End User who has purchased the product or service and concluded the EULA with Us, (e.g. an employee of the End User, a family member or a person otherwise authorized to use the product or service by the End User in compliance with EULA, the processing of the data is carried out in the legitimate interest of ESET within the meaning of Art. 6 (1) f) GDPR to enable the user authorized by End User to use the products and services provided by Us in accordance with EULA.

Contact Information

If You would like to exercise your right as a data subject or You have a question or concern, send us a message at:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24

85101 Bratislava
Slovak Republic
dpo@eset.sk