ESET Endpoint Security for Android

User guide

Click here to display the online version of this document

Digital Security
Progress. Protected.

ESET Endpoint Security for Android was developed by ESET, spol. s r.o.

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

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

REV. 4/12/2024

Introduction

The new generation of ESET Endpoint Security for Android (EESA) is designed to work with ESET PROTECT On-Prem and ESET PROTECT, the new management console which allows for remote management of all ESET security solutions.

There are ESET Endpoint Security for Android Google Play version and web version available.

ESET Endpoint Security for Android version 4 is compatible with:

- ESET PROTECT On-Prem
- ESET PROTECT.

ESET Endpoint Security for Android is designed to protect corporate mobile devices against the most recent malware threats and secure your data even if your device is lost or stolen. It also helps system administrators keep their devices compliant with company security policies.

ESET Endpoint Security for Android can be also applied in small-to-medium sized companies without the need of remote management via ESET PROTECT On-Prem. IT technician, system administrator or user can share his ESET Endpoint Security for Android configuration with colleagues. This process completely diminishes the need for product activation and manual setup of each product module that is otherwise required right after ESET Endpoint Security for Android is installed.

What's new in version 4

Added:

- Support for Android 14

Improved:

- Small visual enhancements of the ESET Endpoint Security for Android GUI

ESET Endpoint Security for Android versions

There are two versions of ESET Endpoint Security for Android available:

- **ESET Endpoint Security for Android**—Google Play version.
- **ESET Endpoint Security for Android**—web version with the Call filter feature.

Updates to the latest version

Updates of ESET Endpoint Security for Android differ based on your installed version:

Update your ESET Endpoint Security for Android Google Play version

If your mobile device is set to update Google Play apps automatically, the update will be performed automatically.

Update your ESET Endpoint Security for Android web version

Click the "Enable automatic application updates" toggle in ESET PROTECT or ESET PROTECT On-Prem to perform ESET Endpoint Security for Android app updates. After that, the end-user will automatically be prompted to update each time an update is available. For more information, visit our Knowledgebase article.

Minimum system requirements

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

- Operating system: Android 6 (Marshmallow) and later
- Touchscreen resolution: 480x800 px
- CPU: ARM with ARMv7 instruction set, x86 Intel Atom
- Free storage space: 20 MB
- Internet connection

Android Go and Fire OS are not supported.

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

Changelog

Users connecting to ESET PROTECT On-Prem and ESET PROTECT

ESET PROTECT On-Prem and ESET PROTECT are applications that allow you to manage ESET products in a networked environment from one central location. The ESET PROTECT On-Prem and ESET PROTECT task management system allows you to install ESET security solutions on remote computers and quickly respond to new problems and threats. ESET PROTECT On-Prem does not provide protection against malicious code on its own. It relies on the presence of an ESET security solution on each client.

ESET security solutions support networks that include multiple platform types. Your network can include a combination of current Microsoft, Linux-based, macOS, and operating systems that run on mobile devices (mobile phones and tablets).

ESET PROTECT On-Prem and ESET PROTECT are a new generation of a remote management system that differs significantly from previous versions of ESET Remote Administrator. You can check the compatibility with previous

versions of ESET security products here:

- ESET PROTECT On-Prem supported products
- ESET PROTECT supported products

You can find the differences between ESET PROTECT On-Prem and ESET PROTECT in our documentation.

For more information, see:
- ESET PROTECT On-Prem online documentation
- ESET PROTECT online documentation

Download the ESET Endpoint Security for Android

There are two ways how to download ESET Endpoint Security for Android:

Download ESET Endpoint Security for Android by scanning the QR code

Scan the QR code below using a QR scanning app on your mobile device:

Alternatively, you can download the ESET Endpoint Security for Android APK installation file from the ESET website:

1.Download the installation file from the ESET website.

2.Open the file from the Android notification area or locate it using a file browsing manager application. The file is usually saved to the Download folder.

3.Verify that applications from Unknown sources are allowed on your device. To do so, tap the Launcher icon on the Android home screen or go to **Home** > **Menu**. Tap **Settings** > **Security**. The **Unknown sources** option needs to be allowed.

4.After opening the file, tap **Install**.

ESET Endpoint Security for Android downloaded from the ESET website can only be upgraded by file downloaded from the ESET website or from inside the application. It cannot be upgraded using Google Play.

Download the ESET Endpoint Security for Android from Google Play

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

Alternatively, you can download the program by clicking the link or scanning the QR code below:

https://play.google.com/store/apps/details?id=com.eset.endpoint

Remote installation

Remote installation of ESET Endpoint Security for Android from ESET PROTECT On-Prem requires the following:

- Mobile Device Connector installation
- Mobile devices enrollment

ESET Endpoint Security for Android installation scenarios

- The administrator emails the enrollment link, installation APK file and an installation process to the end-users. The user taps the enrollment link and is redirected to their default Android internet browser. The device ESET Endpoint Security for Android is enrolled and connected to ESET PROTECT On-Prem. If ESET Endpoint Security for Android is not installed on the device, the user is redirected to the Google Play store to download the application. After the application is downloaded, a standard installation follows.

- The administrator emails the application settings file, installation APK file and an installation process to the end-users. After the installation, the user must open the application settings file. All the settings are imported, and the application is activated (provided the license information was included).

Enrollment of devices with limited input possibilities

ESET Endpoint Security for Android enables you to enroll devices without a camera, browser or email (for example, TVs, smart displays, advertisement displays, etc.) to ESET PROTECT. To enroll such devices, install ESET Endpoint Security for Android on the device via Google Play or the APK file. During the start-up wizard in the **Remote management** step, select **Yes, manage remotely** and tap **Limited-input device**.

In ESET PROTECT:

1. Click **Computers** > **Add device** > **Android or iOS/iPadOS** > **Customize enrollment**.

2.Select **Android devices with limited input options** and select your preferred distribution method. You can learn more about the distribution methods in the ESET PROTECT console.

3.Accept the End User License Agreement and acknowledge the Privacy Policy.

4.If this is a new device, click **Add**. Fill in all required information and click **Save**. If you are adding an existing device, select the applicable device.

5.You receive an enrollment link for the device. Click the link, and type the six-digit security code displayed in the **Remote management** section of the start-up wizard.

6.Click **Accept**.

The device is enrolled in ESET PROTECT.

Device re-enrollment

If your mobile device has stopped connecting, you can re-enroll it via email or QR code if you have physical access to device.

> **Device re-enrollment**
> For visual instructions on how to re-enroll your device, read our Knowledgebase article.

Local installation on the device

ESET Endpoint Security for Android provides administrators with an option to setup and manage Endpoint locally if they choose not to use ESET PROTECT On-Prem. All application settings are protected by Admin password so the application is under full administration control at all times.

If the administrator in a small company decides not to use ESET PROTECT On-Prem but he still wants to protect corporate devices and apply basic security policies, he has two options on how to manage the devices locally:

1.Physical access to each company device and a manual configuration of the settings.

2.Administrator can prepare desired configuration on his Android device (with ESET Endpoint Security for Android installed) and export these settings to a file – see the Import/Export settings section of this guide for more info). Administrator can share the exported file with the end-users (for example via email) – they can import the file to any device running ESET Endpoint Security for Android. When the user opens and accepts the received settings file, it will automatically import all the settings and activate the application (provided the license information was included). All the settings will be protected by Admin password.

Start-up wizard

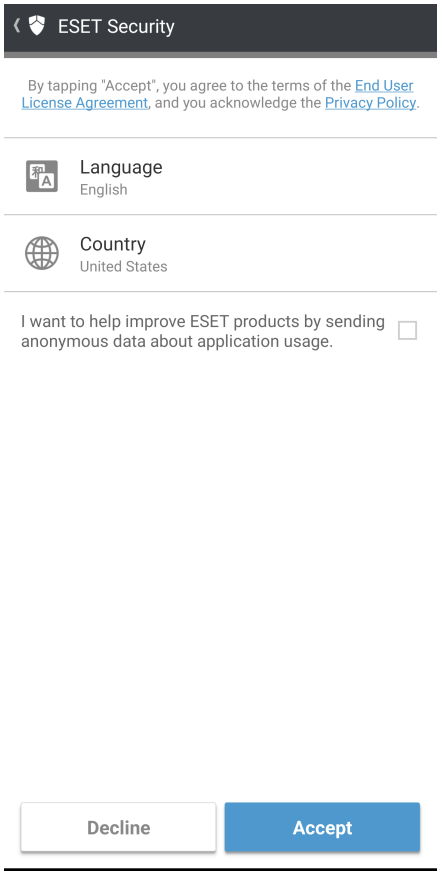
When the app is installed, tap **Admin setup** and follow the prompts from the start-up wizard. This procedure is intended for Administrators only:

1.Select the **Language** you want to use in ESET Endpoint Security for Android.

2.Select the **Country** you currently work or reside in.

3.If you want to help improve ESET products by sending anonymous data about app usage, select the check box.

4.Tap **Accept**. Tapping **Accept** indicates that you agree to the End User License Agreement.



5.Tap **Accept** to accept User consent.

6.Select **Yes, manage remotely** to connect ESET Endpoint Security for Android to ESET PROTECT On-Prem or perform a manual setup by tapping **No, just protect**.

7.A manual setup requires that the phone and storage permissions are enabled. Tap **Continue** and then tap **Allow** to enable each of the permissions.

8.Tap **Continue** to allow the Draw over other applications permission.

9.A manual setup requires product activation. You can activate ESET Endpoint Security for Android using a license key or an ESET Business Account (EBA).

10.Create an Admin password.

11.**Uninstall protection** restricts unauthorized users from uninstalling ESET Endpoint Security for Android. Tap **Enable** and then tap **Activate** in the **Activate Device admin app** prompt.

12.Enable Usage access to enable proper application functionality. Tap **Continue**, and then tap ESET Endpoint Security for Android to enable **Usage access**. Tap the back arrow twice to return to the start-up wizard.

13.Select the option to either **Allow** or **Decline** participation in the ESET LiveGrid® feedback system. To read more about ESET LiveGrid®, refer to this section.

14.Select the option for ESET Endpoint Security for Android to either **Enable detection** or **Don't enable detection** of Potentially unwanted applications. More details about these applications can be found in this section. Tap **Next**.

15.Tap **Finish** to exit the start-up wizard and start your first device scan.

Uninstallation

You can uninstall the ESET Endpoint Security for Android manually by following these steps:

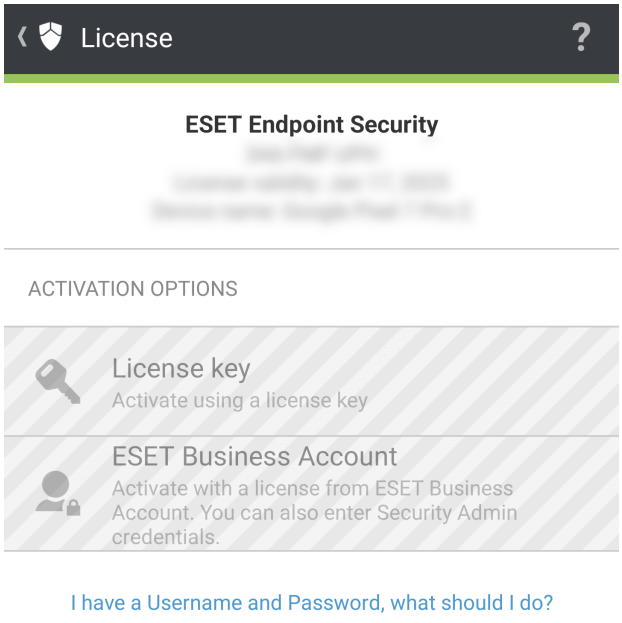
> Important
> This guide is based on stock Android settings. The uninstallation process may differ based on your device manufacturer.

1.On your Android device, go to **Settings** > **Biometrics and security** > **Other security settings** > **Device admin apps**. Deselect ESET Endpoint Security for Android and tap **Deactivate**. Tap **Unlock** and type the Admin Password. If you have not set ESET Endpoint Security for Android as the Device administrator, skip this step.

2.Go back to the **Settings** and tap **Apps** > **ESET Endpoint Security for Android** > **Uninstall** > **OK**.

Product activation

There are multiple ways to activate ESET Endpoint Security for Android. The availability of a specific activation method may vary depending on the country, as well as the means of distribution (ESET web page, etc.) for your product.



To activate ESET Endpoint Security for Android directly on the Android device, tap the **Menu** icon in the ESET Endpoint Security for Android main screen and tap **License**.

You can use any of the following methods to activate ESET Endpoint Security for Android:

- **License key**—A unique string in the format XXXX-XXXX-XXXX-XXXX-XXXX which is used for identification of the license owner and activation of the license.
- **ESET Business Account** - An account created on the ESET Business Account portal with credentials (email address and password). This method allows you to manage multiple licenses from one location.

ESET PROTECT On-Prem is able to activate client devices silently using licenses made available by the administrator.

Documentation for endpoints managed remotely

ESET business products and ESET Endpoint Security for Android can be managed remotely on client workstations, servers and mobile devices in a networked environment from one central location. System administrators who manage more than 10 client workstations should consider using an ESET remote management tool. ESET remote management tools can deploy ESET solutions, manage tasks, enforce security policies, monitor system statuses and quickly respond to problems or threats on remote computers from one central location.

ESET remote management tools

ESET Endpoint Security for Android can be managed remotely by either ESET PROTECT On-Prem or ESET PROTECT.

- Introduction to ESET PROTECT On-Prem
- Introduction to ESET PROTECT

> **Migration tool**
> ESET Endpoint Security for Android version 3.5 and later supports the Migration tool to migrate from ESET PROTECT On-Prem to ESET PROTECT.

Best practices

- Enroll a device using ESET PROTECT On-Prem
- Set up an admin password on connected client computers to avoid unauthorized modifications
- Apply a recommended policy to enforce available security features

How to guides

- How to use Override mode

Android device enrolled via Microsoft Intune

> When your device with Android 9 and later is enrolled via Microsoft Intune, ESET Endpoint Security for Android version 3.5 and later ignores the following settings when the corresponding policy is applied:
> - Device security
> - Application control
> - Anti-Theft

Introduction to ESET PROTECT On-Prem

ESET PROTECT On-Prem allows you to manage ESET products on workstations and servers in a networked environment from one central location.

Using the ESET PROTECT Web Console, you can deploy ESET solutions, manage tasks, enforce security policies, monitor system status and quickly respond to problems or detections on remote computers. See also ESET PROTECT On-Prem architecture and infrastructure elements overview, Getting started with ESET PROTECT Web

Console, and Supported Desktop Provisioning Environments.

ESET PROTECT On-Prem is made up of the following components:

- ESET PROTECT Server—ESET PROTECT Server can be installed on Windows as well as Linux servers and also comes as a Virtual Appliance. It handles communication with Agents and collects and stores application data in the database.

- ESET PROTECT Web Console—ESET PROTECT Web Console is the primary interface that allows you to manage client computers in your environment. It displays an overview of the status of clients on your network and allows you to deploy ESET solutions to unmanaged computers remotely. After you install ESET PROTECT Server, you can access the Web Console using your web browser. If you choose to make the web server available via the internet, you can use ESET PROTECT On-Prem from any place or device with an internet connection.

- ESET Management Agent—The ESET Management Agent facilitates communication between the ESET PROTECT Server and client computers. The Agent must be installed on client computer to establish communication between that computer and the ESET PROTECT Server. Because it is located on the client computer and can store multiple security scenarios, use of the ESET Management Agent significantly lowers reaction time to new detections. Using ESET PROTECT Web Console, you can deploy the ESET Management Agent to unmanaged computers identified by Active Directory or ESET RD Sensor. You can also manually install the ESET Management Agent on client computers if necessary.

- Rogue Detection Sensor—The ESET PROTECT On-Prem Rogue Detection (RD) Sensor detects unmanaged computers present on your network and sends their information to the ESET PROTECT Server. This allows you to add new client computers to your secured network easily. The RD Sensor remembers computers that have been discovered and will not send the same information twice.

- ESET Bridge (HTTP Proxy)— You can use ESET Bridge with ESET PROTECT On-Prem as a Proxy service to:

  - Distribute updates to client computers and installation packages to the ESET Management Agent.

  - Forward communication from ESET Management Agents to the ESET PROTECT Server.

- ESET PROTECT Virtual Appliance—The ESET PROTECT On-Prem VA is intended for users who want to run ESET PROTECT On-Prem in a virtualized environment.

- Mirror Tool—The Mirror Tool is necessary for offline module updates. If your client computers do not have an internet connection, you can use the Mirror Tool to download update files from ESET update servers and store them locally.

- ESET Remote Deployment Tool—This tool serves to deploy All-in-one packages created in the ESET PROTECT Web Console. It is a convenient way to distribute ESET Management Agent with an ESET product on computers over a network.

- ESET Business Account—The licensing portal for ESET business products allows you to manage licenses. See the ESET Business Account section of this document for instructions to activate your product, or see the ESET Business Account User Guide for more information about using the ESET Business Account.

- ESET Enterprise Inspector—A comprehensive Endpoint Detection and Response system that includes features such as: incident detection, incident management and response, data collection, indicators of compromise detection, anomaly detection, behavior detection and policy violations.

Using the ESET PROTECT Web Console, you can deploy ESET solutions, manage tasks, enforce security policies, monitor system status and quickly respond to problems or threats on remote computers.

For more information, please see the ESET PROTECT On-Prem Online user guide.

Introduction to ESET PROTECT

ESET PROTECT allows you to manage ESET products on workstations and servers in a networked environment from one central location without the requirement to have a physical or virtual server like for ESET PROTECT On-Prem. Using the ESET PROTECT Web Console, you can deploy ESET solutions, manage tasks, enforce security policies, monitor system status and quickly respond to problems or threats on remote computers.

- Read more about this in the ESET PROTECT Online user guide

Policies

The administrator can push specific configurations to ESET products running on client devices using policies from the ESET PROTECT On-Prem Web Console. A policy can be applied directly to individual devices or to groups of devices. You can also assign multiple policies to a device or a group.

A user must have the following permissions to create a new policy: **Read** permission to read the list of policies, **Use** permission to assign policies to target computers and **Write** permission to create, modify or edit policies.

Policies are applied in the order that Static Groups are arranged. This is not true for Dynamic Groups, where policies are applied to child Dynamic Groups first. This allows you to apply policies with greater impact to the top of the Group tree and apply more specific policies to subgroups. Using flags, an ESET Endpoint Security for Android user with access to groups located higher in the tree can override the policies of lower groups. The algorithm is explained in ESET PROTECT On-Prem Online user guide.

Setting policies on the device disables the option to change the policy-controlled settings locally. These settings are locked against changes even in Admin mode. You can allow temporary changes to be made by creating an Override mode policy.

Setting certain policies may require you to grant additional permission to ESET Endpoint Security for Android locally on the affected device.

We recommend that you assign more generic policies (for example, the update server policy) to groups that are higher within the group tree. More specific policies (for example, device control settings) should be assigned deeper in the group tree. The lower policy usually overrides the settings of the upper policies when merged (unless defined otherwise using policy flags).

Default policies for ESET Endpoint Security for Android

Policy name	Policy description
General - Maximum protection	ESET Endpoint Security for Android uses all options to secure maximum protection for the device.
General - Balanced setup	ESET Endpoint Security for Android uses the configuration recommended for most setups.

Policy name	Policy description
General - Maximum performance	ESET Endpoint Security for Android combines threat protection and minimal impact on everyday tasks and device performance.

Apply policies

After connecting ESET Endpoint Security for Android to the ESET management console, the best practice is to apply a recommended or custom policy.

There are several built-in policies for ESET Endpoint Security for Android:

Policy name	Policy description
General - Maximum protection	ESET Endpoint Security for Android uses all options to secure maximum protection for the device.
General - Balanced setup	ESET Endpoint Security for Android uses the configuration recommended for most of the setups.
General - Maximum performance	ESET Endpoint Security for Android combines threat protection and minimal impact on everyday tasks and device performance.

For more information on policies, refer to the following topics:

- ESET PROTECT On-Prem policies
- ESET PROTECT policies
- Apply a recommended or pre-defined policy for ESET Endpoint Security for Android using ESET PROTECT On-Prem

Flags

The policy that is applied to a client computer is usually the result of multiple policies being merged into one final policy. When merging policies, you can adjust the expected behavior of the final policy, due to the order of applied policies, by using policy flags. Flags define how the policy will handle a specific setting.

For each setting, you can select one of the following flags:

Not apply	Any setting with this flag is not set by the policy. Since the setting is not set by the policy, it can be changed by other policies applied later.
Apply	Settings with the **Apply** flag will be applied to the client computer. However, when merging policies, it can be overwritten by other policies applied later. When a policy is sent to a client computer containing settings marked with this flag, those settings will change the local configuration of the client computer. Since the setting is not forced, it can still be changed by other policies applied later.
Force	Settings with the **Force** flag have priority and cannot be overwritten by any policy applied later (even if it also has a **Force** flag). This assures that other policies applied later will not be able to change this setting during merging. When a policy is sent to a client computer containing settings marked with this flag, those settings will change the local configuration of the client computer.

Scenario: The *Administrator* wants to allow user *John* to create or edit policies in his home group and see all policies created by the *Administrator* including Policies that have Force flags. The *Administrator* wants *John* to be able to see all policies, but not edit existing policies created by *Administrator*. *John* can only create or edit policies within his Home Group, San Diego.
Solution: *Administrator* has to follow these steps:
Create custom static groups and permission sets
1. Create a new Static Group called *San Diego*.
2. Create a new Permission set called *Policy - All John* with access to the Static Group *All* and with **Read** permission for **Policies**.
3. Create a new Permission set called *Policy John* with access to Static Group *San Diego*, with functionality access **Write** permission for **Group & Computers** and **Policies**. This permission set allows *John* to create or edit policies in his Home Group *San Diego*.
4. Create a new user *John* and in the **Permission Sets** section select *Policy - All John* and *Policy John*.
Create policies
5. Create a new policy *All- Enable Firewall*, expand the **Settings** section, select **ESET Endpoint for Windows**, navigate to **Personal Firewall** > **Basic** and apply all settings by **Force** flag. Expand the **Assign** section and select the Static Group *All*.
6. Create a new policy *John Group- Enable Firewall*, expand the **Setting** section, select **ESET Endpoint for Windows**, navigate to **Personal Firewall** > **Basic** and apply all settings by **Apply** flag. Expand the **Assign** section and select Static Group *San Diego*.
Result
The Policies created by *Administrator* will be applied first since **Force** flags were applied to the policy settings. Settings with the Force flag applied have priority and cannot be overwritten by another policy applied later. The policies that are created by user *John* will be applied after the policies created by the Administrator.
To see the final policy order, navigate to **More** > **Groups** > **San Diego**. Select the computer and select **Show details**. In the **Configuration** section, click **Applied policies**.

Use Override mode

Users with ESET Endpoint Security for Android (version 2.1 and later) installed on their machine can use the Override feature. Override mode enables users on the client-device level to change settings in the installed ESET product for a set time, even if a policy is applied over these settings. After the set time, settings are reverted back to settings set by policies.

By default policy settings, ESET Endpoint Security for Android scans the device after the override session has ended. You can change this with the **Scan device after override session**.

- To change settings locally on the device while in Override mode, you must type in the ESET Endpoint Security for Android admin password.
- Override mode cannot be stopped from the ESET Web Console after it is enabled. Override mode will be disabled automatically when the override time expires.
- The user using the Override mode needs to have ESET Endpoint Security for Android admin password. Otherwise, the user cannot access the settings of ESET Endpoint Security for Android. You can create a temporary admin override password for each policy.

To set **Override mode**:

1. Click **Polices** > **New Policy**.

2. In the **Basic** section, type a **Name** and **Description** for the policy.

3.In the **Settings** section, select **ESET Endpoint Security for Android**.

4.In the policy options, click **Settings**.

5.Expand **Override mode settings** and configure rules for override mode.

6.In the **Assign** section, select the applicable devices.

7.Review the settings in the **Summary** section and click Finish.

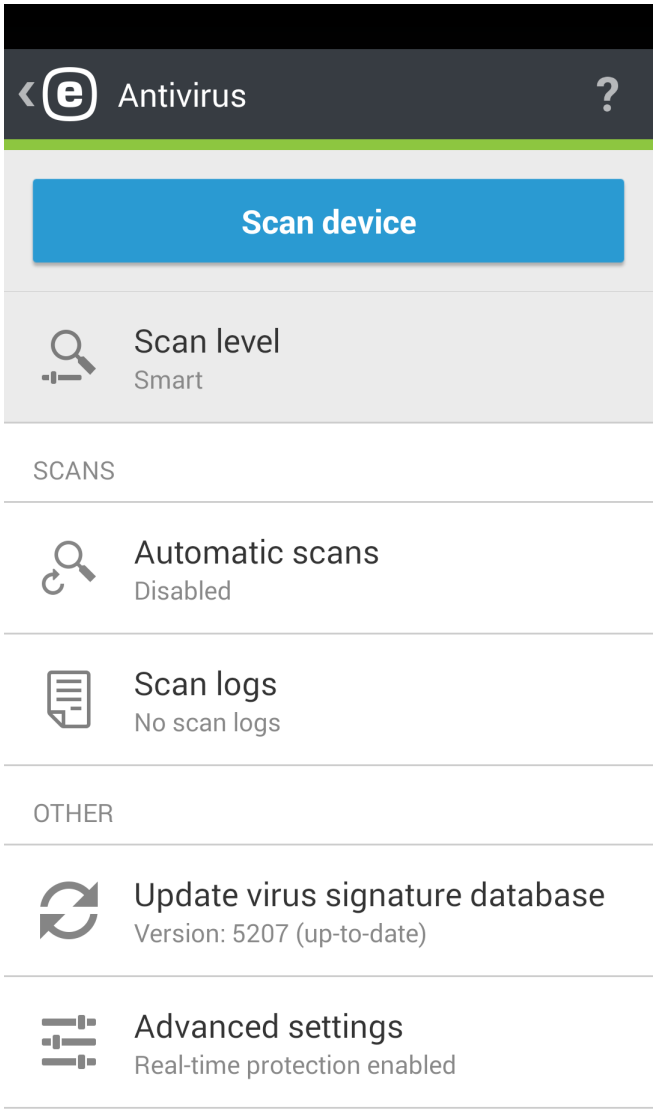
If *John* has a problem with his endpoint settings blocking an important functionality or web access on his device, the Administrator can allow *John* to override his existing endpoint policy and tweak the settings manually on his device. Afterward, these new settings can be requested by ESET PROTECT so the Administrator can create a new policy out of them.
To do so, follow the steps below:
1.Click **Policies** > **New Policy**.
2.Complete the **Name** and **Description** fields. In the **Settings** section, select **ESET Endpoint Security for Android**.
3.Click **Settings** in the policy options.
4.Expand the **Override mode** settings and enable the override mode for one hour.
5.Click **Set** in the Override credentials to create a temporary admin password for John. Type in the password (for example, 12345) twice and click **OK**.
6.Assign the policy to *John's smartphone* and click **Finish** to save the policy.
7.*John* has to type in the admin password to enable the **Override mode** on his ESET Endpoint Security for Android and change the settings manually on his device.
8.In the ESET PROTECT Web Console, click **Computers**, select *John's smartphone* and click **Show Details**.
9.To schedule a client task to get the configuration from the client, in the **Configuration** section, click **Request configuration**.
10.The new configuration appears. Select the applicable product and then click **Open Configuration**.
11.Review the settings and then click **Convert to policy**.
12.Complete the **Name** and **Description** fields.
13.In the **Settings** section, modify the settings if needed.
14.In the **Assign** section, assign this policy to *John's smartphone* (or others).
15.Click **Finish**. Do not forget to remove the override policy after it is no longer needed.

Override password

This option enables you to create a temporary administrator password to enable users to alter the settings on the client device without having access to the actual administrator password. Click **Set** next to the policy to insert the override password.

Antivirus

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



Scan Device

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

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

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

Scan Level

There are 2 different scan levels to choose from:

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

Automatic Scans

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

Scan Logs

The Scan Logs section contains comprehensive data about completed scans in the form of log files. See the Antivirus Scan Logs section of this document for more information.

Update detection modules

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

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

Detailed descriptions of the Antivirus Advanced settings can be found in the Advanced settings section of this document.

Automatic Scans

Scan Level

There are 2 different scan levels to choose from. This setting will apply to both On-Charger Scan and Scheduled Scan:

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

On-Charger Scan

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

Scheduled Scan

Scheduled Scan allows you to run a Device scan automatically at a pre-defined time. To schedule a scan, tap  next to **Scheduled Scan** and specify the dates and times for the scan to be launched. By default, Monday 4 am is selected.

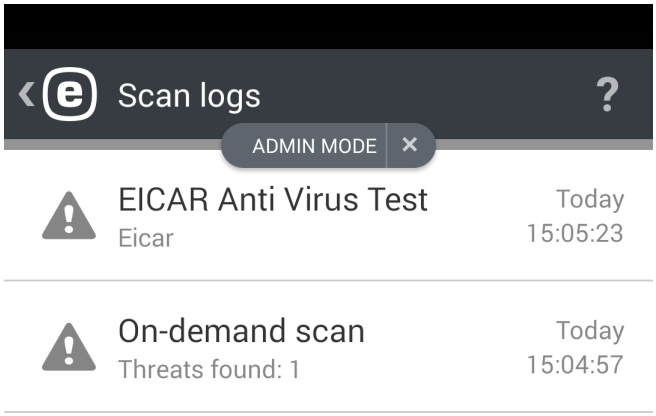
Scan Logs

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

Each log contains:

- date and time of the event

- duration of the scan
- number of scanned files
- scan result or errors encountered during the scan



Ignore rules

If you manage ESET Endpoint Security for Android remotely from ESET PROTECT On-Prem, you have the option to define files that will not be reported as malicious. Files added to **Ignore rules** will be ignored in future scans. To create a rule, you must specify the following:

- a filename with a proper "apk" extension
- an application package name, e.g. uk.co.extorian.EICARAntiVirusTest
- the name of the threat as detected by antivirus programs, e.g. Android/MobileTX.A (this field is mandatory)

This feature is not available in the ESET Endpoint Security for Android app.

Advanced settings

Real-time protection

This option allows you to enable and disable the Real-time scanner. This scanner launches automatically at system startup and scans the files you interact with. After it is mounted, it automatically scans the Download folder, APK installation files and all files on the SD card.

ESET LiveGrid® reputation system

ESET LiveGrid® is a preventative system designed to provide your device with additional security. It constantly monitors your system's running programs and processes against the latest intelligence collected from millions of ESET users worldwide. This allows us to offer all ESET users better and more precise proactive protection and scanning speeds. We recommend that you enable this feature. We recommend that you enable this feature.

ESET LiveGrid® feedback system

The 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.

Detect potentially unwanted applications

An unwanted app is a program that contains adware, installs toolbars, traces your search results or has other unclear objectives. In some situations, you may believe that the benefits of the unwanted app outweigh the risks. For this reason, ESET assigns these applications to a lower-risk category compared to other types of malicious software.

Detect potentially unsafe applications

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

Block unresolved threats

This setting determines the action that will be performed after the scan is complete and threats are found. If you enable this option, ESET Endpoint Security for Android will block access to files categorized as threats.

Removable media

You can choose an action after removable media is inserted into the device:

- **Always scan**—removable media will always be scanned
- **Do not scan**—removable media will not be scanned
- **Show me options**—option to scan a removable media will be shown after the media is inserted

Detection modules database updates

This option allows you to set the time interval for the frequency that threat database updates are automatically downloaded. These updates are issued as needed when a new threat is added to the database. We recommend leaving this set to the default value (Every day).

Custom max database age

This setting defines the time between threat database updates, after which you will be notified to update ESET Endpoint Security for Android.

Update server

Using this option, you can choose to update your device from the **Pre-release server**. Pre-release updates have gone through thorough internal testing and will be available to the general public soon. You can benefit from enabling pre-release updates by accessing to the most recent detection methods and fixes. However, pre-release updates might not be stable enough at all times. The list of current modules can be found in the **About** section: tap the Menu icon  in the ESET Endpoint Security for Android main screen and tap **About** > **ESET Endpoint Security for Android**. We recommended that basic users leave the **Release server** option selected by default.

ESET Endpoint Security for Android allows you to create copies of update files that can be used to update other devices on the network. The use of a Local mirror—a copy of the update files in the LAN environment—is convenient because the update files do not need to be repeatedly downloaded from the vendor update server by each mobile device. Detailed information on how to configure the mirror server using ESET Endpoint products for Windows can be found in this document.

To create offline mirror, use Mirror tool with ESET Endpoint Security for Android update server parameter.

Anti-Theft

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

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

Trusted SIM cards feature is not available on devices with Android 10 and later.

Anti-Theft features help administrators protect and locate a missing device. Actions may be triggered from ESET PROTECT On-Prem.

When executing commands from ESET PROTECT On-Prem, the administrator receives a confirmation in ESET PROTECT On-Prem.

When receiving location info (**Find** command), the administrator using ESET PROTECT On-Prem receives the location information in the form of GPS coordinates.

All Anti-Theft commands can be performed from ESET PROTECT On-Prem. New mobile device management

functionality allows the administrators to perform the Anti-Theft commands just by few clicks. Tasks are immediately submitted for executions via a new push-commands processing component (Mobile Device Connector) that is now a part of ESET PROTECT On-Prem infrastructure.

Administrator contacts

This is the List of administrator phone numbers protected by the admin password. These numbers are also used for notifications related to Anti-Theft actions.

How to add administrator contact

A name of the administrator and the phone number is supposed to be typed during the Anti-Theft start-up wizard. If the contact contains more than one phone number, all associated numbers will be taken into account.

Admin contacts can be added or modified in the **Anti-Theft** > **Admin contacts** section.

Lock screen info

The administrator is able to define custom information (company name, email address, message) which will be displayed when the device is locked, with the option to call one of the pre-defined admin contacts.

This information includes:

- Company name (optional)
- Email address (optional)
- A custom message

Trusted SIM cards

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

To add a new SIM card, tap the ➕ icon. Type a **Name** for the SIM card (for example, Home, Work) and its IMSI (International Mobile Subscriber Identity) number. IMSI is usually presented as a 15-digit long number printed on your SIM card. In some instances, it may be shorter.

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

⚠ Trusted SIM cards feature is not available on devices with Android 10 and later.

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

Remote commands

Remote commands can be triggered directly from ESET PROTECT On-Prem Console:

Find device

You will receive a text message with the GPS coordinates of the target device, including a link to its location on Google maps. The device will send a new SMS if a more precise location is available after 10 minutes.

Lock device

This will lock the device—you will be able to unlock it using the Admin password or the Unlock remote command.

Unlock locked device

The device will be unlocked and the SIM card currently in the device will be saved as a Trusted SIM.

Siren/Lost Mode sound

The device will be locked and it will play a very loud sound for 5 minutes (or until unlocked). A loud siren will play even if the device is set to mute.

Enhanced factory reset

This will reset the device to its factory settings. All accessible data will be erased and file headers will be removed. The process can take several minutes.

Device lock feature is only available for devices managed by ESET PROTECT.

Application Control

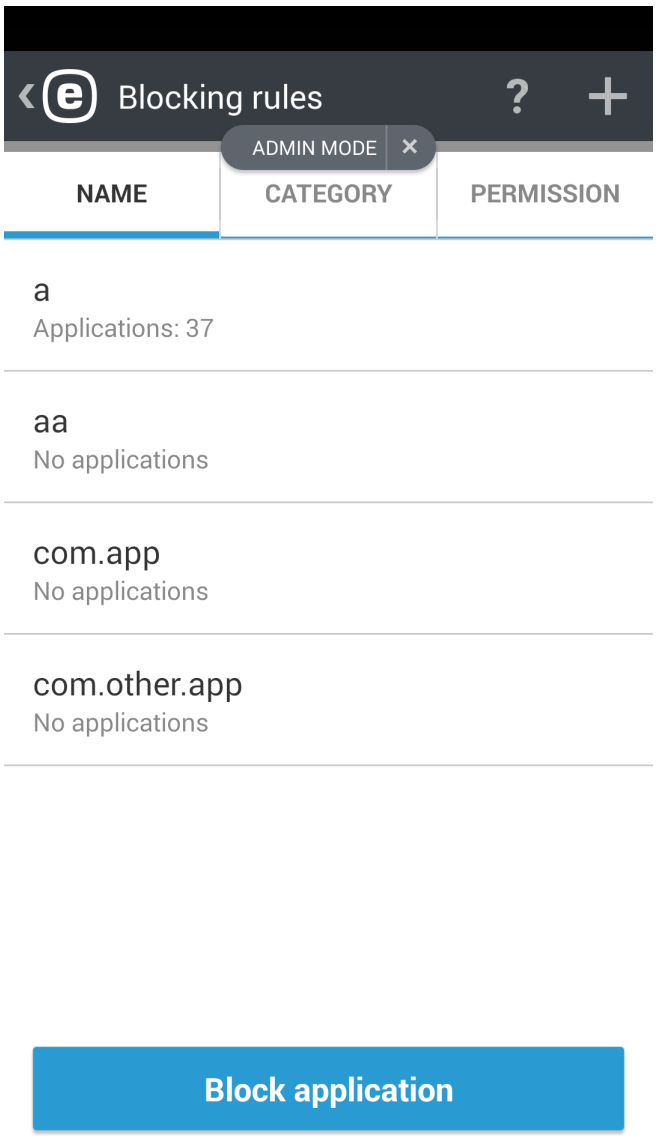
The **Application Control** feature offers administrators the option to monitor installed applications, block access to defined applications, and lower the risk of exposure by prompting the users to uninstall certain applications. The administrator can select from several filtering methods for applications:

- Manually define applications that should be blocked
- Category-based blocking (for example, games or social)
- Permission-based blocking (for example, applications that track location)
- Blocking by source (for example, applications installed from sources other than the Google Play store)

Blocking Rules

In the **Application Control** > **Blocking** > **Blocking rules** section, you can create the application blocking rules based on the following criteria:

- application name or package name
- category
- permissions



Blocking by application name

ESET Endpoint Security for Android gives administrators the option to block an application according to its name or the package name. The **Blocking rules** section provides an overview of the created rules and the list of blocked applications.

To modify an existing rule, touch and hold the rule and then tap **Edit** . To remove rule entries from the list,

touch and hold one of the entries, select the ones you want to remove and then tap **Remove**  . To clear the entire list, tap **SELECT ALL** and then tap Remove  .

When you block an application by name, ESET Endpoint Security for Android will look for the exact match with a name of launched application. If you change the ESET Endpoint Security for Android GUI to a different language, you must reenter the application name in that language to continue blocking it.

To avoid any issues with localized application names, we recommend that you block such applications by their package names—a unique application identifier that cannot be changed during runtime or reused by another application.

In the case of a local administrator, a user can find the application package name in **Application Control** > **Monitoring** > **Allowed applications**. After tapping the application, the **Detail** screen will display the application package name. To block the application, follow these steps.

How to block an application by its name

1.Tap **Application Control** > **Blocking** > **Block application** > **Block by name**.

2.Choose whether to block the application according to its name or the name of the package.

3.Type the words based on which the application will be blocked. To divide multiple words, use a comma (,) as a delimiter.

For example, a word "*poker*" in the **Application name** field will block all applications containing "*poker*" in their name. If you type "*com.poker.game*" into the **Package name** field, ESET Endpoint Security for Android will block just one application.

Blocking by application category

ESET Endpoint Security for Android gives admin the option to block the application according to pre-defined application categories. The **Blocking rules** section provides you with an overview of the created rules and the list of blocked applications.

If you want to modify the existing rule, touch and hold the rule and tap **Edit**  .

To remove some rule entries from the list, touch and hold one of the entries, select the ones you want to remove and tap **Remove**  . To clear the entire list, tap **SELECT ALL**.

How to block an application based on its category

1.Tap **Application Control** > **Blocking** > **Block application** > **Block by category**.

2.Select the pre-defined categories using check-boxes and tap **Block**.

Blocking by application permissions

ESET Endpoint Security for Android gives admin the option to block the application according to its permissions. The **Blocking rules** section provides you with an overview of the created rules and the list of blocked applications.

If you want to modify the existing rule, touch and hold the rule and tap **Edit** .

To remove some rule entries from the list, touch and hold one of the entries, select the ones you want to remove and tap **Remove** . To clear the entire list, tap **SELECT ALL**.

How to block an application by its permissions

1.Tap **Application Control** > **Blocking** > **Block application** > **Block by permission**.

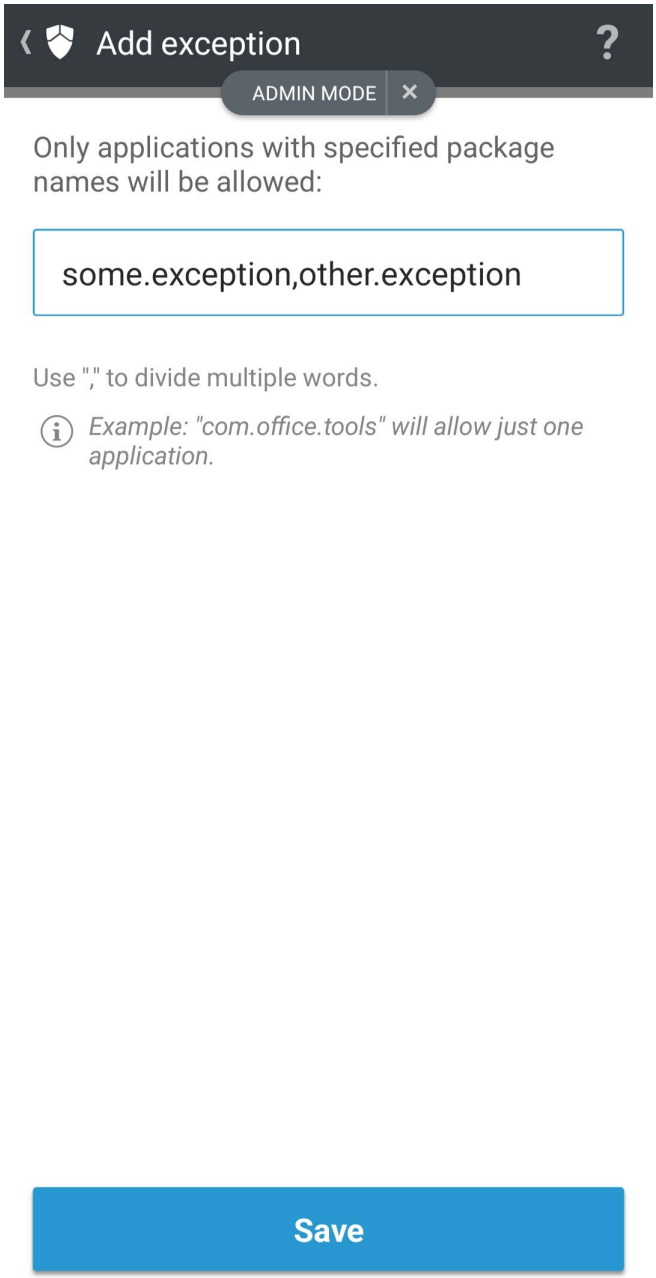
2.Select the permissions using check-boxes and tap **Block**.

Block unknown sources

By default, ESET Endpoint Security for Android does not block the applications obtained from the internet or any source other than the Google Play store. The **Blocked applications** section provides you with an overview of blocked applications (package name, rule applied) and the option to uninstall the application or add it to the whitelist—**Exceptions** section.

Exceptions

Tap **Application Control** > **Blocking** > **Exceptions** > **Add exception**, and you can create exceptions to exclude a specific application from the list of blocked applications. Administrators managing ESET Endpoint Security for Android remotely can use this new feature to determine whether a specific device is in compliance with the company policy regarding installed applications.



How to add exceptions

Apart from adding the new exception (entering the application package name), applications can be also whitelisted by exempting them from the list of **Blocked applications:**

1. In your ESET Endpoint Security for Android application, tap **Application Control**.
2. Tap **Blocking** > **Blocked applications**.
3. Select the application you want to whitelist.
4. Tap the three dots icon in the upper- right corner, and tap **Add exception**.
5. Type the admin password, and tap **Enter**.

Required applications

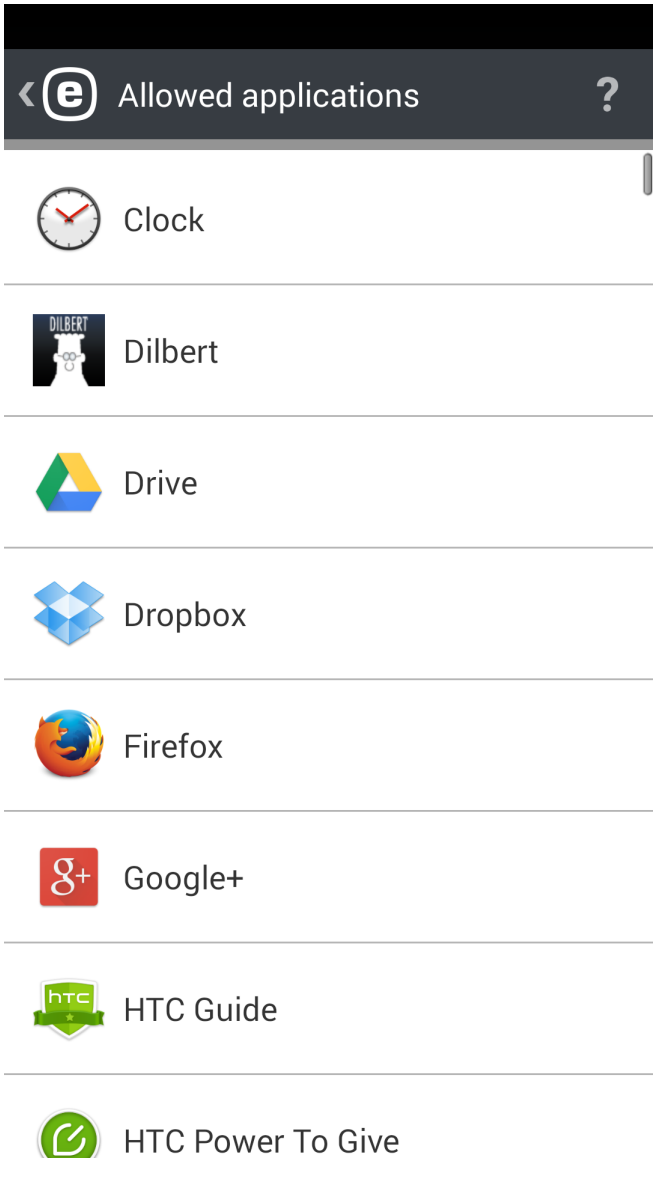
If you manage ESET Endpoint Security for Android remotely from ESET PROTECT On-Prem, you have the option to define which applications must be installed on the target device(s). The following information is required:

- name of the application visible to the user
- unique application package name, e.g. *com.eset.ems2.gp*
- URL where a user can find a download link. You can also use Google Play links, e.g. https://play.google.com/store/apps/details?id=com.eset.ems2.gp

This feature is not available in the ESET Endpoint Security for Android app.

Allowed applications

This section provides you with an overview of installed applications that are not blocked by blocking rules.

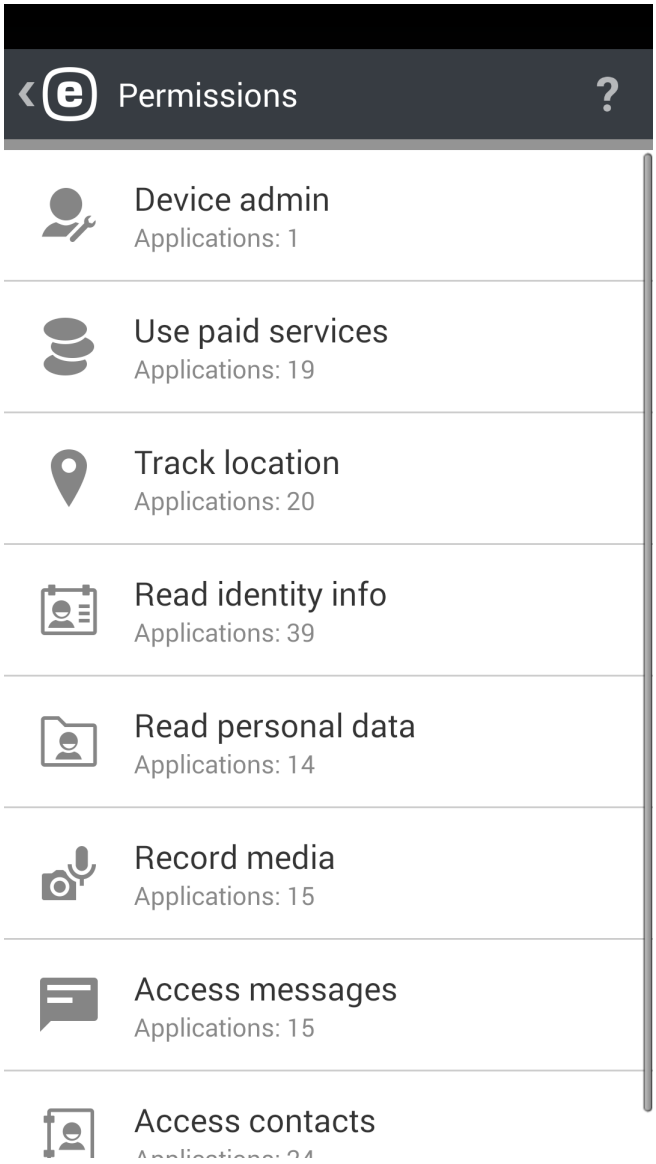


Permissions

This feature tracks the behavior of applications with access to personal or company data, and allows the administrator to monitor application access based on pre-defined permissions categories.

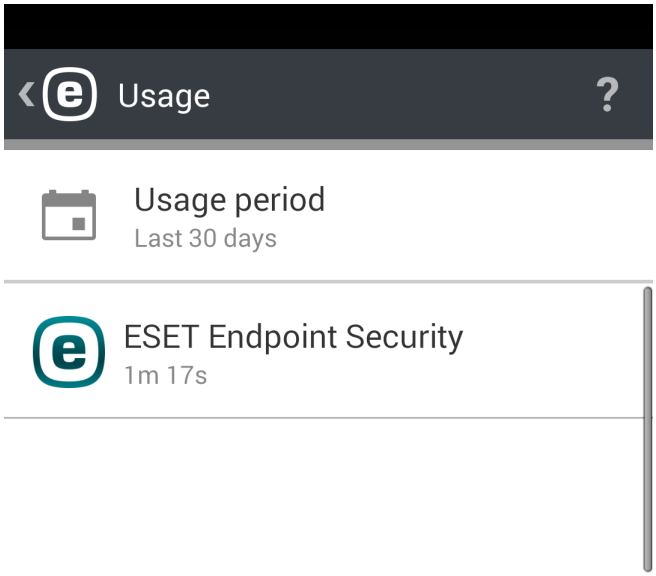
Some applications installed on your device might have access to services that cost you money, track your location or read your identity info, contacts or text messages. ESET Endpoint Security for Android provides an audit of these applications.

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



Usage

In this section, the administrator can monitor the amount of time a user spends using specific applications. To filter the overview by its usage period, use the **Interval** option.

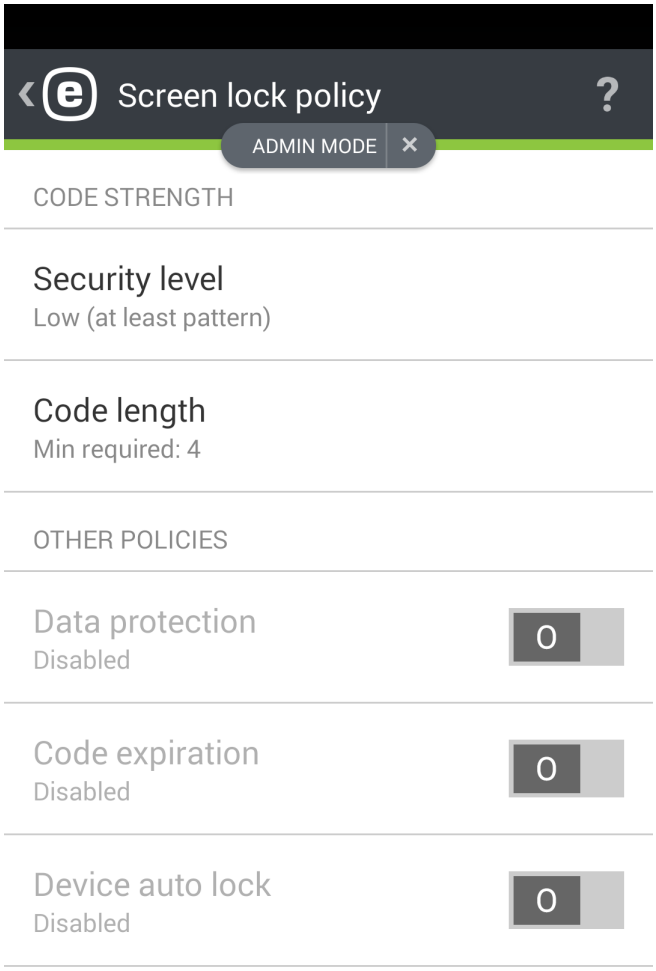


Device Security

Device security provides administrators with options to perform the following:

- execute basic security policies across mobile devices and define policies for important device settings
- specify the required screen lock strength
- restrict built-in camera usage

Screen lock policy



In this section, the administrator is able to:

- set a minimum security level (pattern, PIN, password) for the system screen lock code, and define the complexity of the code (for example, minimum code length)
- set the maximum number of failed unlock attempts (or the device will go to factory defaults)
- set maximum screen lock code age
- set the lock screen timer

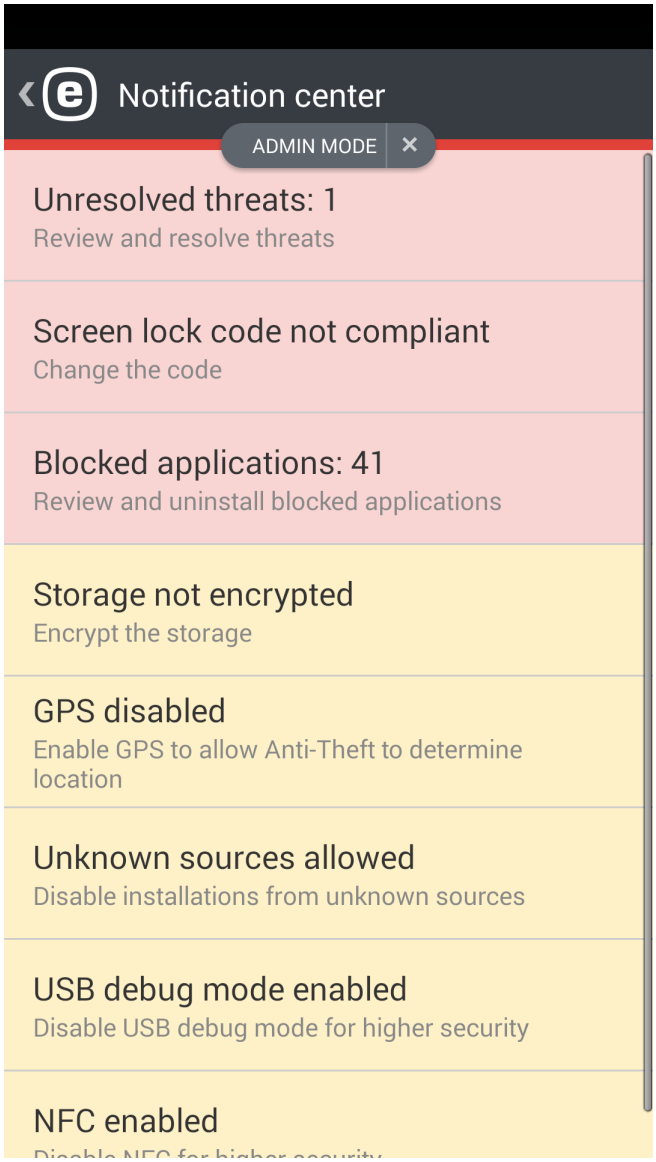
ESET Endpoint Security for Android automatically notifies the user and the administrator if the current device settings are in compliance with corporate security policies. If a device is out of compliance, the application will automatically suggest to the user what should be changed to be compliant again.

Device settings policy

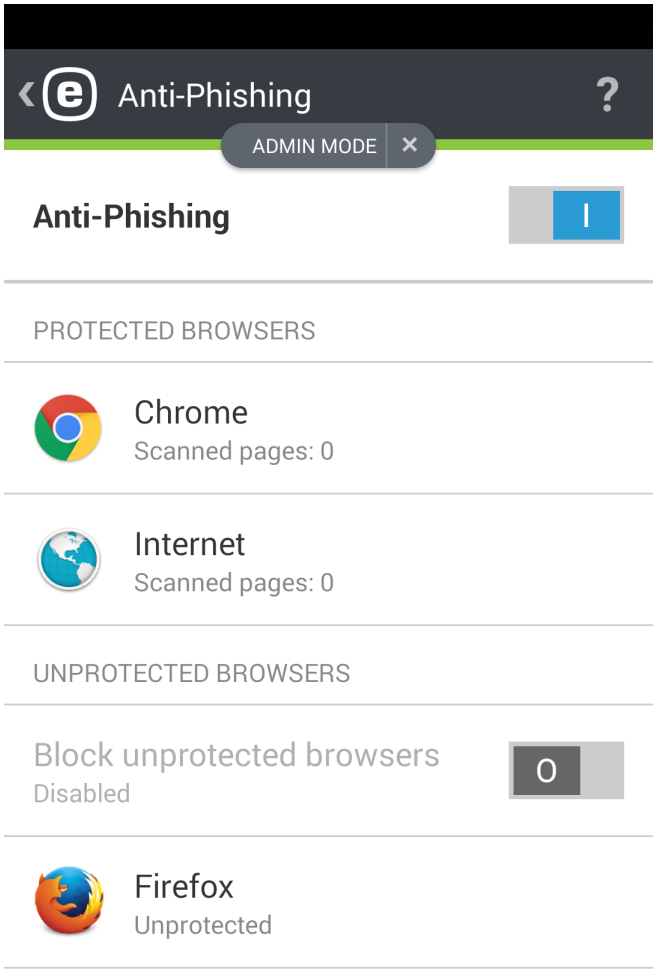
Device Security also includes your **Device Settings Policy** (previously a part of the **Security audit** functionality) which gives the system administrator the option to monitor pre-defined device settings to determine if they are in the recommended state.

Device settings include:

- Wi-Fi
- GPS satellites
- Location services
- Memory
- Data roaming
- Call roaming
- Unknown sources
- Debug mode
- NFC
- Storage encryption
- Rooted device



Anti-Phishing



Phishing is a criminal activity that uses social engineering (manipulating users to obtain confidential information). Phishing is often used to gain access to sensitive data such as bank account numbers, credit card numbers, PIN numbers or usernames and passwords.

We recommend that you keep **Anti-Phishing** enabled. ESET Endpoint Security for Android scans the URL addresses—all potential phishing attacks coming from websites or domains listed in the ESET malware database will be blocked, and a warning notification will be displayed informing you of the attack.

IMPORTANT: Anti-Phishing integrates with the most common web browsers available on Android OS. In general, Anti-Phishing protection is available for Chrome, Firefox, Opera, Opera Mini, Dolphin, Samsung and stock browsers that come pre-installed on Android devices. Other browsers will be listed as unprotected, and access to them can be blocked by the O toggle .

You must enable **Accessibility** in Android system settings for ESET Anti-Phishing to function properly.

Allow accessibility permission on ESET Endpoint Security for Android installed from the .APK file on Android 13

Note

For security reasons, Android 13 restricts accessibility permission to apps installed from .apk files. This prevents uninformed access to these permissions.

How ESET Endpoint Security for Android 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 information.
Data accessed via accessibility permission is not shared with any third parties.

To solve the accessibility issue:

1. Open **Settings** > **Accessibility** > **Downloaded apps**, and the ESET Endpoint Security for Android is greyed out.
2. Tap on the ESET Endpoint Security for Android app, and the **Restricted setting** dialog opens.
3. Tap **OK**.
4. Go to **Settings** > **Apps** > ESET Endpoint Security for Android to open the **App info**.
5. Tap the three dots ⋮ icon in the upper right corner > **Allow restricted settings**.

Accessibility permission is now allowed, and you can start using the application.

Web control

Use Web control settings to protect your company from the risk of legal liability. For instance, Web control can regulate access to websites that violate intellectual property rights. The goal is to prevent employees from accessing pages with inappropriate or harmful content or pages that negatively impact productivity.

Employers or system administrators can prohibit access to more than 27 pre-defined website categories and over 140 subcategories and log these visits.

Web control is a managed feature. All settings are controlled from ESET PROTECT.

For Web control to function, a managed device must meet the following requirements:
- ESET Endpoint Security for Android version 3 or later.
- Android version 8 or later.
- Enrolled in ESET PROTECT with device administrator permissions.

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
- Kiwi browser
- Edge
- Silk in Amazon devices
- Mi browser
- Xiaomi Mi browser
- Vewd in Android TV
- Apps that use protected browser components for web view are also protected.

Call Filter

> **Important**
> Call Filter feature is available only in the ESET Endpoint Security for Android web version.

Call Filter blocks incoming/outgoing calls based on user-defined rules.

No notification is displayed when an incoming call is blocked. The advantage of this is that you will not be bothered by unsolicited information, but can always check the logs for calls that may have been blocked by mistake.

> Call Filter does not work on tablets that do not support calling.

To block calls from the last received phone number, tap **Block Last Caller**. This will create a new rule.

Block phone numbers using wildcards

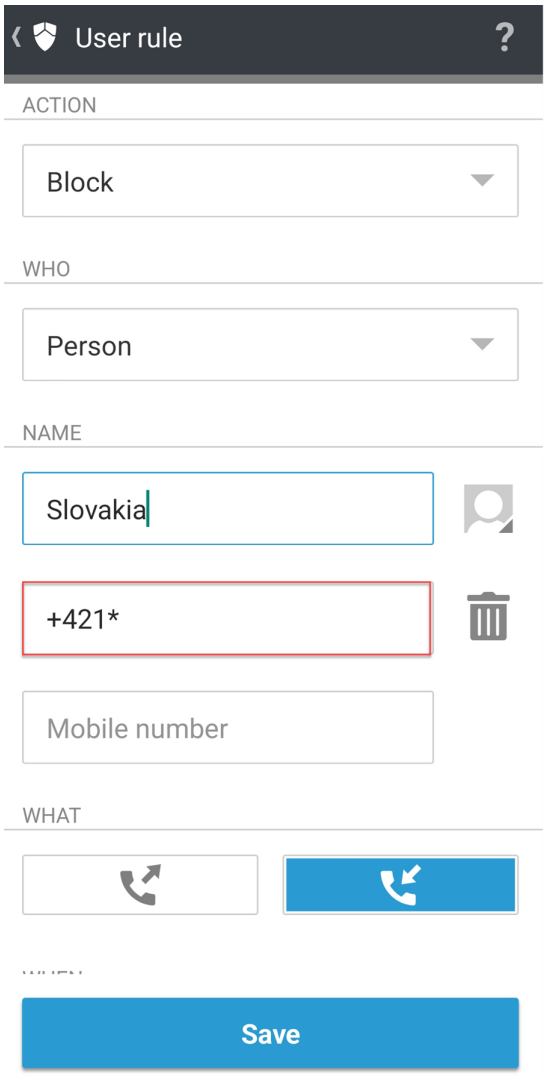
You can block a range of numbers via wildcards described in the table below:

Wildcard	Description
*	represents multiple characters

Wildcard	Description
?	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 **Mobile 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.



Rules

As a user, you can create user rules without a need of entering Admin password. Admin rules can be created only in Admin mode. Admin rules will overwrite any user rules.

More information about creating a new rule can be found in this section.

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

How to add a new rule

To add a new rule, tap **Add rule** or tap the  icon in the top right corner of the **Rules** screen.

Specify a person or a group of phone numbers. ESET Endpoint Security for Android will recognize the contact groups saved in your Contacts (for example, Family, Friends or Coworkers). **All unknown numbers** will include the phone numbers not saved in your contact list. You can use this option to block unwelcome phone calls (for example, "cold calls") or to prevent employees from dialing unknown numbers. The **All known numbers** option refers to all phone numbers saved in your contact list. **Hidden numbers** will apply to callers that have their phone number intentionally hidden via the Calling Line Identification Restriction (CLIR).

Specify which should be blocked or allowed:

-  outgoing calls
-  incoming calls

To apply the rule for a specified time only, tap **Always** > **Custom** and select the days of the week and a time interval for which you want to apply the rule. By default, Saturday and Sunday are selected. This functionality might come in handy if you do not want to be disturbed during meetings, business trips, night or during the weekend.

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

History

In the **History** section, you can see the calls and messages blocked or allowed by the Call Filter. Each log contains the name of the event, corresponding phone number, date and time of the event.

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

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

Settings

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

Country—Select the country, where you currently work or reside.

Update—For maximum protection, it is important to use the latest version of ESET Endpoint Security for Android. Tap Update to see if a later version is available for download from the ESET website.

Device ID—Set or change your device identification name for the administrator if the device is stolen or lost.

Remote management—Connect your device to ESET PROTECT On-Prem.

Advanced settings

Click **Advanced settings** to open the Advanced settings section.

Permission notifications—Refer to the Permission management section.

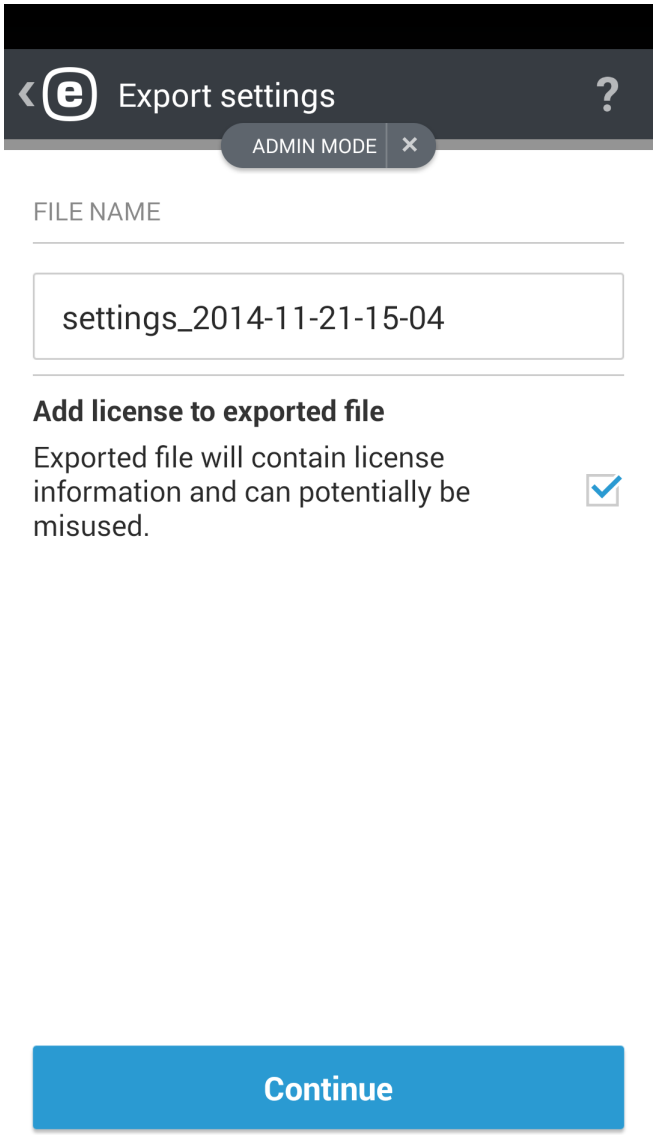
Send usage data—This option helps improve ESET products by sending anonymous data about app usage. Sensitive information will not be sent. If you did not enable this option during the installation start-up wizard, you can do so in the Settings > Advanced settings section.

Admin Password—This option allows you to set a new Admin password or change the existing one. To read more, refer to the Admin Password section of this document.

Import/Export settings—Import or export settings from or to ESET Endpoint app.

Import/Export settings

To easily share settings from one mobile device with another if the devices are not managed by ESET PROTECT On-Prem, ESET Endpoint Security for Android includes the option to export and import program settings. The administrator can manually export device settings to a file which can then be shared (for example, via email) and imported to any device running the client application. When the user accepts the received settings file, it automatically defines all settings and activates the application (provided the license information was included). All settings will be protected by the administrator password.



Export settings

To export the current settings of ESET Endpoint Security for Android, specify the settings filename – the current date and time will be automatically filled in. You can also add the license information (License key or Security admin account email address and password) to the exported file but beware that this information will not be encrypted and can be misused.

In the next step, select the way you want to share the file through:

- Wi-Fi network
- Bluetooth
- Email
- Gmail
- file browsing application (for example, ASTRO File Manager or ES File Explorer)

Import settings

To import settings from a file located on the device, use a file browsing application to locate the settings file and select ESET Endpoint Security for Android.

Settings can be also imported by selecting a file in the **History** section.

History

History section provides you with the list of imported settings files and allows you to share, import or remove them.

Admin Password

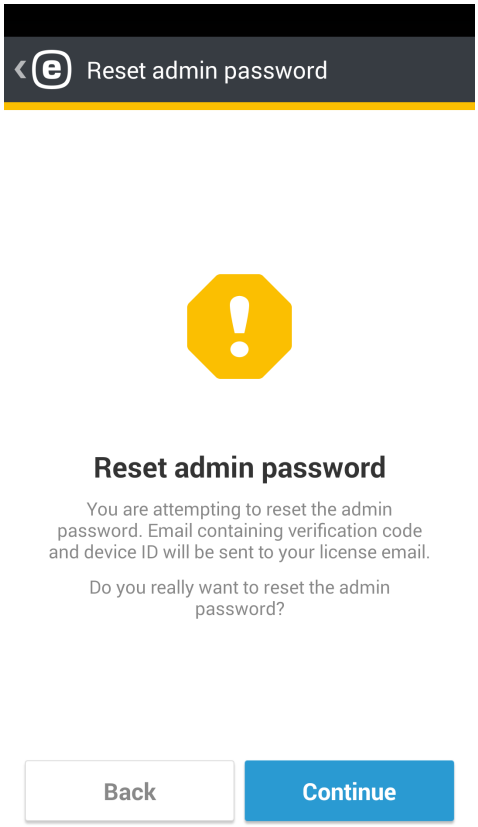
The **Admin password** is required to unlock a device, send Anti-Theft commands, access password-protected features and uninstall ESET Endpoint Security for Android.

Creating **Admin password** blocks users from changing the ESET Endpoint Security for Android settings.

Choose the password carefully. To increase security, use a combination of small letters, capital letters and numbers.

To reset the Admin password on a device with a locked screen:

1. Tap **Forgotten password?** > **Continue** > **Request verification code**. If the device is not connected to the internet, tap the **choose offline reset** link instead and contact ESET Technical Support.



2. An email containing the verification code and device ID will be sent to the email address associated with the ESET license. The verification code will be active for seven days. Type the verification code and a new password on your device's locked screen.

Remote management

ESET PROTECT On-Prem allows you to manage ESET Endpoint Security for Android in a network environment from one central location.

Using ESET PROTECT On-Prem not only increases your level of security, but also provides ease-of-use in the administration of all ESET products installed on client workstations and mobile devices. Devices with ESET Endpoint Security for Android can connect to ESET PROTECT On-Prem using any type of internet connection—WiFi, LAN, WLAN, Cellular Network (3G, 4G LTE, HSDPA, GPRS), etc.—as long as it is a regular internet connection (without a proxy or firewall) and both endpoints are configured correctly.

When connecting to ESET PROTECT On-Prem over a cellular network, a successful connection depends on the mobile network provider and requires a full-featured internet connection.

To connect a device to ESET PROTECT On-Prem, add the device to the Computers list in ESET PROTECT On-Prem Web Console, enroll the device using the **Device Enrollment** task and type the **MDC Server Address**.

The enrollment link (MDC Server Address) uses the standard format `https://MDCserver:port/token` in ESET PROTECT On-Prem. The link contains the following values:

- **MDCserver**—The full DNS name or public IP address of the server running Mobile Device Connector (MDC). Hostname can only be used if you are connecting through an internal Wi-Fi network.
- **Port**—The port number used to connect to Mobile Device Connector
- **Token**—The string of characters generated by admin in ESET PROTECT On-Prem Web Console

To learn more about how to manage your network using ESET PROTECT On-Prem, refer to the following online help topics:

- How to manage policies
- How to create client tasks
- Learn about reports

Device ID

Device ID helps the admin to identify your device when it is lost or stolen.

Permission management

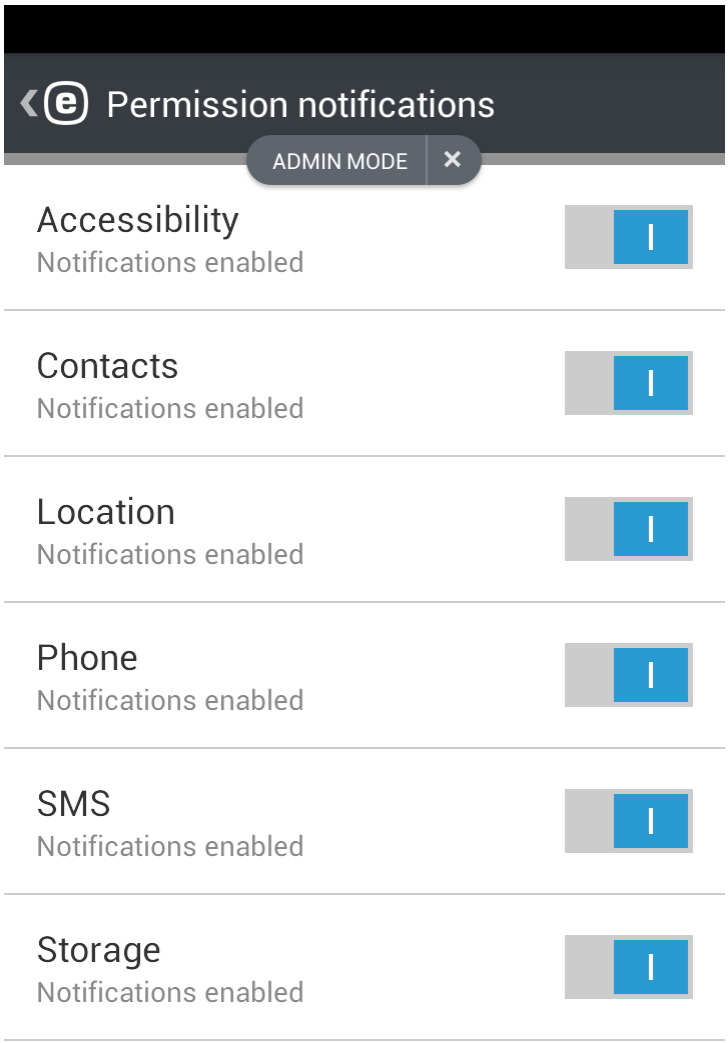
In Android 6 (Marshmallow), Google introduced a new Permission Management system and ESET Endpoint Security for Android is compatible with it. Apps designed for Android 6.0 will ask for permissions when you start using them. Instead of giving an app access during installation, you'll be prompted the first time the app wants to

access a specific device function.

ESET Endpoint Security for Android requires access to the following functions:

- **Accessibility**—required for the proper functionality of ESET Anti-Phishing
- **Contacts**—required for Anti-Theft and Call Filter
- **Location**—Anti-Theft
- **Phone**—Anti-Theft and Call Filter
- **SMS**—Anti-Theft and Call Filter
- **Storage**—Antivirus and Anti-Theft

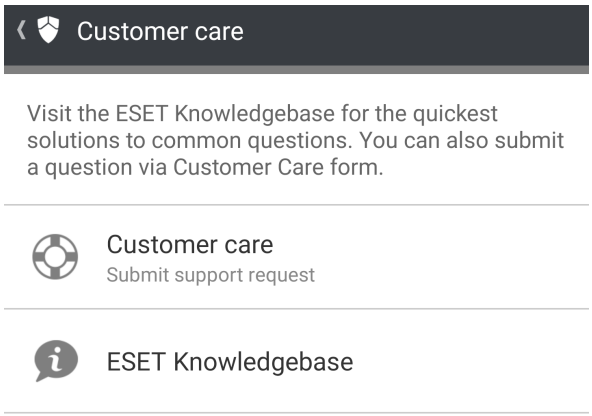
Admin is allowed to disable monitoring of these permissions in **Settings** > **Permission notifications**.



Customer Care

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

To send a support request directly from your device, tap the Menu icon in the ESET Endpoint Security for Android main screen, tap **Customer care** > **Customer care** and fill in all required fields.



ESET Endpoint Security for Android includes advanced logging functionality to help diagnose potential technical issues. To provide ESET with a detailed application log, verify that **Submit application log** is selected (default). Tap **Submit** to send your request. An ESET Customer Care specialist will contact you at the email address you provided.

Customer Experience Improvement Program

By joining the Customer Experience Improvement Program you provide ESET with anonymous information relating to the use of our products. More information on data processing is available in our Privacy Policy.

Your consent

Participation in the Program is voluntary and based on your consent. After joining in, the participation is passive, which means you do not need to take any further action. You may revoke your consent by changing the product settings at any time. Doing so will bar us from further processing of your anonymous data.

What types of information do we collect?

Data about interaction with the product

This information tells us more about how our products are used. Thanks to this we know, for example, which functionalities are used often, what settings users modify or how much time they spend using the product.

Data about devices

We collect this information to understand where and what devices our products are used on. Typical examples are device model, country, version and name of the operating system.

Error diagnostics data

Information about error and crash situations is also collected. For example, what error has occurred and which actions led to it.

Why do we collect this information?

This anonymous information lets us improve our products for you, our user. It helps us to make them the most relevant, easy-to-use and faultless as possible.

Who controls this information?

ESET, spol. s r.o. is the sole controller of data collected in the Program. This information is not shared with third parties.

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_business. 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.

EULAID: EULA-PRODUCT-LG; 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, 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.

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:

- Update and other statistics covering 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.
- One-way hashes related to infiltrations as part 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.
- Suspicious samples and metadata from the wild 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 about devices in local network such as type, vendor, model and/or name of device;

- 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 your 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.

- Licensing information such as license ID and personal data such as name, surname, address, email address is required for billing purposes, license genuineness verification and provision of our services.
- Contact 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.

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 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 or your objection processing, 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. 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.

Right to Restriction of Processing. 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.

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