Kaspersky Endpoint Security for Android

Instructions on activation using the licutil utility

Application version: 10.0

Dear User,

Thank you for choosing our product. We hope that you will find this documentation useful and that it will answer any questions that you may have.

Note: This document is the property of AO Kaspersky Lab (herein also referred to as Kaspersky Lab): all rights to this document are reserved by the copyright laws of the Russian Federation and by international treaties. Illegal reproduction or distribution of this document or parts hereof will result in civil, administrative, or criminal liability under applicable law.

Any type of reproduction or distribution of any materials, including translations, may be allowed only with written permission from Kaspersky Lab.

This document and related graphic images can be used for informational, non-commercial, or personal use exclusively.

This document may be amended without prior notice. You can find the latest version of this document at the Kaspersky Lab website, at http://www.kaspersky.com/docs.

Kaspersky Lab assumes no liability for the content, quality, relevance, or accuracy of any third-party materials used herein, or for any potential harm associated with the use of such materials.

Document revision date: 08/06/2016

http://www.kaspersky.com
https://help.kaspersky.com
http://support.kaspersky.com

Contents

Kaspersky Endpoint Security for Android

The mobile app Kaspersky Endpoint Security for Android (hereinafter also “Kaspersky Endpoint Security”) protects mobile devices running the Android™ operating system against viruses and malware, unwanted calls and texts, and web threats. Different app components provide protection against various threats.

Kaspersky Endpoint Security includes the following components:

- Anti-Virus. It allows you to detect and neutralize threats on your device by using the Anti-Virus databases and the Kaspersky Security Network cloud service. Anti-Virus includes the following components:
  - Protection. Detects threats in open files, scans new apps, and prevents device infection in real time.
  - Scanning. Scan is performed on demand for the entire file system, the random access memory, or a folder. Full Scan scans for the presence of malicious objects in the whole file system; Folder Scan scans a specific folder. Full Scan and Folder Scan detect threats in files that have been installed but not yet opened, as well as threats in files that are currently open. Memory Scan detects threats only in files that are currently open.
  - Update. Update allows you to download new Anti-Virus databases for the application.
- Call & Text Filter. Depending on the selected mode of operation, the Call & Text Filter lets you block unwanted incoming calls and texts. Incoming calls and texts are filtered using lists of allowed and blocked contacts. The Call & Text Filter can block or allow incoming calls and texts from blocked and allowed contacts. Depending on the mode selected, the Call & Text Filter can also allow incoming calls and texts from all numbers on the device contact list or block incoming calls and texts from all numbers that contain letters.
- Web Protection. This component blocks malicious sites designed to spread malicious code. The Call & Text Filter also blocks fake (phishing) website designed to steal confidential data of the user (for example, passwords to online banking or e-money systems) and access the user's financial info. The Call & Text Filter scans websites before you open them using the Kaspersky Security Network cloud service. After scanning, Web Protection allows trustworthy websites to load and blocks malicious websites. Web Protection also supports

website filtering by categories defined in Kaspersky Security Network cloud service. This lets the administrator restrict user access to certain categories (for example, web pages from the Gambling, lotteries, sweepstakes or Social networks categories).

- Quarantine. This component moves files detected during device scanning or during real-time protection to dedicated isolated storage. Quarantine stores files as archives, so they cannot harm the device. The Quarantine lets you delete or restore the files that were moved to isolated storage.
- Reports. This component lets you obtain information about the operation of Anti-Virus, Call&Text Filter, and Web Protection on the user's mobile device. The component groups reports chronologically. A report can contain up to 200 event entries. Once the number of report entries exceeds 200, the component overwrites older entries with new ones.
- Additional. This component lets you configure additional Kaspersky Endpoint Security settings: pop-up notifications with app events, sound notifications about app events. This component lets you remove Kaspersky Endpoint Security from the mobile device. The component also lets you receive license information about general information about Kaspersky Endpoint Security.

You can use Kaspersky Endpoint Security for Android as part of Kaspersky Security for Mobile. *Kaspersky Security for Mobile* is an integrated solution for protecting and managing corporate mobile devices and also personal mobile devices used by company employees for corporate purposes (hereinafter "the app"). Kaspersky Security for Mobile is integrated into the *Kaspersky Security Center remote administration system* (see the *Kaspersky Security for Mobile Deployment Guide*). The administrator can use a single Administration Console of Kaspersky Security Center to manage all mobile device on the corporate network as well as client computers and virtual systems (see the *Kaspersky Security Center Administrator's Guide*). After deploying Kaspersky Security for Mobile, you can connect mobile devices to the Administration Server of the organization and configure their security policies (see the *Administrator's Guide for Kaspersky Security for Mobile*). After you connect mobile devices to the Administration Server, they become managed. You can remotely monitor managed devices. The table below lists the functions of Kaspersky Endpoint Security for Android when used with Kaspersky Security Center and without Kaspersky Security Center.

> Kaspersky Endpoint Security for Android can be used with Kaspersky Security Center only as part of the commercial version of Kaspersky Security for Mobile.

Table 1. Comparison of Kaspersky Endpoint Security for Android functions when used with and without Kaspersky Security Center.

Functions	Kaspersky Endpoint Security for Android used without Kaspersky Security Center	Kaspersky Endpoint Security for Android used with Kaspersky Security Center
Anti-Virus protection	✓	✓
Anti-Theft protection		✓
Call & Text Filter	✓	✓
Protection against malicious websites	✓	✓
Web browsing control		✓
Remote activation of Kaspersky Endpoint Security	✓	✓
Usage of containers		✓
App Control		✓
Remote configuration of hardware functions of the device: camera, Bluetooth, Wi-Fi		✓
Configuring the system password strength		✓
Remote configuration of the TouchDown email client		✓
Managing Samsung KNOX devices		✓
Remote removal of Kaspersky Endpoint Security		✓

App activation

The app can be activated in the following ways:

- By adding an activation code to the app installation package before distributing it among users.
- By adding an activation code to the Google Play™ link for downloading the app before sending the link to users.

After the app has been installed on the user's mobile device, activation of the app is performed automatically.

The licutil utility is used to add an activation code to the app installation package or to the Google Play link. The licutil utility is included in the Kaspersky Endpoint Security distribution kit.

> If the Kaspersky Security Center remote administration system is deployed at your organization, you can connect mobile devices with Kaspersky Endpoint Security installed to the Administration Server and remotely manage mobile devices via the Administration Console of Kaspersky Security Center. This requires activating the app using a key from the Kaspersky Security Center storage. If you have activated the app by sending an installation package or a Google Play link with an activation code added, replace the active key with a key from the Kaspersky Security Center storage (see the *Administrator's Guide for Kaspersky Security for Mobile*). You can add the key that has been freed up as a result of active key replacement on a different device where it can be used until the relevant license expires.

In this section

Adding an activation code to the Google Play link

► *To add an activation code to the link for downloading the app from Google Play using the licutil utility,*

run the following command in the command line: `<path to distribution kit>/licutil.exe -c <activation code>`.

Example:

```
C:\Users\Admin\Distrib\KSM\licutil.exe –c A1234-B5678-C9012-D3456
```

This starts the licutil utility. A link for downloading the app from Google Play with the activation code added appears in the command line.

You can send the link for downloading the app from Google Play to a mobile device user using any available method (for example, via email or text message). You should mention in the accompanying message that the user should skip the Administration Server connection settings configuration step in the Initial Configuration Wizard of the app. After the user downloads the app from Google Play and installs it on the mobile device, app activation is performed automatically.

The activation code is confidential information. To prevent unauthorized access to the activation code or a potential leak of the activation code, you have to personally protect the message with the Google Play link with the activation code added while it is being delivered to users.

The following conditions must be satisfied to install the app from Google Play:

- The mobile device user must have a Google™ account.
- The mobile device must be linked to the Google account.
- The mobile device must be connected to the Internet.

For more details on creating a Google account, linking the device to the Google account, or using Google Play, see Google's technical support website at http://support.google.com/googleplay/.

Adding an activation code to the app installation package

► *To add an activation code to the app installation package using the licutil utility,*

run the following command in the command line: `<path to the distribution kit>/licutil.exe -s <path to the Kaspersky Endpoint Security installation package from the distribution kit> -t <path to the installation package with the added key> -c <activation code>`.

Example:

```
C:\Users\Admin\Distrib\KSM\licutil.exe -s
C:\Users\Admin\Distrib\KSM\KES10.apk -t
C:\Users\Admin\Distrib\KSM\KES10key.apk -c A1234-B5678-C9012-D3456
```

This starts the licutil utility. An app installation package with the activation code added is created in this folder.

You can deliver the installation package to the user's mobile device using any available method (for example, by copying the installation package to the user's workstation to be later transferred to the mobile device). You should mention in the accompanying message that the user should skip the Administration Server connection settings configuration step in the Initial Configuration Wizard of the app. After the user receives the app installation package and installs the app on the mobile device, app activation is performed automatically.

> The activation code is confidential information. To prevent unauthorized access to the activation code or a potential leak of the activation code, you have to personally protect the installation package with the activation code added while it is being delivered to users.

To be able to install the app from the installation package, installation of apps received other than from Google Play must be allowed on the user's mobile device.

AO Kaspersky Lab

Kaspersky Lab is a world-renowned vendor of systems protecting computers against various threats, including viruses and other malware, unsolicited email (spam), network and hacking attacks.

In 2008, Kaspersky Lab was rated among the world's top four leading vendors of information security software solutions for end users (IDC Worldwide Endpoint Security Revenue by Vendor). Kaspersky Lab is the preferred vendor of computer protection systems for home users in Russia ("IDC Endpoint Tracker 2014").

Kaspersky Lab was founded in Russia in 1997. It has since grown into an international group of companies with 34 offices in 31 countries. The company employs more than 3000 qualified specialists.

PRODUCTS. Kaspersky Lab's products provide protection for all systems—from home computers to large corporate networks.

The personal product range includes security applications for desktop, laptop, and tablet computers, smartphones and other mobile devices.

The company offers protection and control solutions and technologies for workstations and mobile devices, virtual machines, file and web servers, mail gateways, and firewalls. The company's portfolio also features specialized products providing protection against DDoS attacks, protection for industrial control systems, and prevention of financial fraud. Used in conjunction with Kaspersky Lab's centralized management system, these solutions ensure effective automated protection for companies and organizations of any size against computer threats. Kaspersky Lab's products are certified by the major test laboratories, are compatible with the software of many suppliers of computer applications, and are optimized to run on many hardware platforms.

Kaspersky Lab's virus analysts work around the clock. Every day they uncover hundreds of thousands of new computer threats, create tools to detect and disinfect them, and include them in databases used by Kaspersky Lab applications.

TECHNOLOGIES. Many technologies that are now part and parcel of modern anti-virus tools were originally developed by Kaspersky Lab. It is no coincidence that many other developers use the

Kaspersky Anti-Virus kernel in their products, including: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, General Dynamics, Facebook, Juniper Networks, Lenovo, H3C, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, ZyXEL. Many of the company's innovative technologies are patented.

ACHIEVEMENTS. Over the years, Kaspersky Lab has won hundreds of awards for its services in combating computer threats. Following tests and research conducted by the reputed Austrian test laboratory AV-Comparatives in 2014, Kaspersky Lab ranked among the top two vendors by the number of Advanced+ certificates earned and was eventually awarded the Top Rated certificate. But Kaspersky Lab's main achievement is the loyalty of its users worldwide. The company's products and technologies protect more than 400 million users, and its corporate clients' number is more than 270,000.

Kaspersky Lab's website:	http://www.kaspersky.com
Virus encyclopedia:	http://www.securelist.com
Virus Lab:	http://newvirus.kaspersky.com (for scanning suspicious files and websites)
Kaspersky Lab's web forum:	http://forum.kaspersky.com

Information about third-party code

Information about third-party code is contained in the **About** section in the app settings.

Trademark notifications

Registered trademarks and service marks are the property of their respective owners.

Android, Google, and Google Play are trademarks of Google, Inc.

The word mark Bluetooth and its logo are the property of Bluetooth SIG, Inc.

Samsung and KNOX are trademarks of SAMSUNG in the United States of America and elsewhere.