Kaspersky Security 10 for Mobile

Implementation Guide

Application version: 10.0 Service Pack 4
Dear User,

Thank you for trusting us. 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.

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.

This document uses registered trademarks and service marks which are the property of their respective owners.

Document revision date: 7/26/2018

© 2018 AO Kaspersky Lab. All Rights Reserved.

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

About this Guide ............................................................................................................................................. 6
In this document ............................................................................................................................................. 6
Document conventions ................................................................................................................................. 8
Sources of information about the application ............................................................................................. 9
Other sources of information about the application .................................................................................. 9
Discussing Kaspersky Lab applications on the Forum .............................................................................. 10
Kaspersky Security for Mobile .................................................................................................................. 11
  About Kaspersky Security for Mobile ..................................................................................................... 11
  About Kaspersky Endpoint Security for Android app ............................................................................ 12
  About Kaspersky Safe Browser mobile app. ............................................................................................. 14
  About iOS MDM profile .......................................................................................................................... 15
  About an Exchange mailbox ..................................................................................................................... 16
  About the Kaspersky Endpoint Security for Android administration plug-in .................................... 16
  About the Kaspersky Device Management for iOS administration plug-in ....................................... 17
Distribution kit ............................................................................................................................................ 17
Hardware and software requirements ....................................................................................................... 19
Application architecture ............................................................................................................................ 21
Common integrated solution deployment scenarios .................................................................................. 22
  Deployment scenarios for Kaspersky Endpoint Security for Android .................................................. 22
  Deployment scenarios for Kaspersky Safe Browser for iOS ................................................................ 24
  Deploying an iOS MDM profile ................................................................................................................ 24
Preparing the Administration Console for deployment of the integrated solution .................................. 26
  Configuring Administration Server settings for connection of mobile devices .................................... 26
  Displaying the Mobile Device Management folder in the Administration Console .......................... 27
  Creating an administration group ............................................................................................................ 27
  Creating a rule for device automatic allocating to administration groups ......................................... 28
  Creating a general certificate .................................................................................................................... 29
Install Kaspersky Endpoint Security for Android ..................................................................................... 30
Permissions ................................................................................................................................................ 30
Installing via Kaspersky Security Center .................................................................................................. 31
Installation from Self Service Portal ......................................................................................................... 33
Installation from Google Play .................................................................................................................... 34
Installing via KNOX Mobile Enrollment .................................................................................................. 35
  Creating a KNOX MDM profile ................................................................................................................. 35
  Adding devices in KNOX Mobile Enrollment ......................................................................................... 36
  Installing the app ..................................................................................................................................... 41
Creating an installation package ............................................................................................................... 41
Configuring installation package settings ................................................................................................. 42
Creating a standalone installation package .............................................................................................. 43
About this Guide

The Implementation Guide for the integrated solution Kaspersky Security 10.0 for Mobile (hereinafter referred to as "Kaspersky Security for Mobile") is intended for professionals who install and administer Kaspersky Security for Mobile. The Guide is also intended for professionals who provide technical support to organizations that use Kaspersky Security for Mobile.

You can use this guide to:

- Plan installation of Kaspersky Security for Mobile components (taking into account the operating principles of Kaspersky Security for Mobile, system requirements, common deployment scenarios, and specifics of Kaspersky Security for Mobile integration with other applications)
- Prepare the Kaspersky Endpoint Security and Kaspersky Safe Browser mobile apps for installation, install and configure them
- Configure the Kaspersky Endpoint Security and Kaspersky Safe Browser mobile apps after installation

This Guide also lists sources of information about the integrated solution and ways to get technical support.

In this section

<table>
<thead>
<tr>
<th>In this document</th>
<th>Document conventions</th>
</tr>
</thead>
<tbody>
<tr>
<td>............................................................</td>
<td>6</td>
</tr>
<tr>
<td>............................................................</td>
<td>8</td>
</tr>
</tbody>
</table>

In this document

This document comprises the following sections:

Sources of information on the application (see page 10)
This section lists the sources of information about the app.

Kaspersky Security for Mobile (see page 11)
This section describes the functions and components of Kaspersky Security for Mobile.

Hardware and software requirements (see page 19)
This section lists the hardware and software requirements.

Application architecture (see page 21)
This section describes the Kaspersky Security for Mobile components and their interaction.
Common integrated solution deployment scenarios (see page 22)
This section describes the common scenarios of Kaspersky Security for Mobile deployment on the corporate network.

Preparing the Administration Console for deployment of the integrated solution (see page 26)
This section provides instructions on preparing the Administration Console for deployment of the integrated solution.

Installing Kaspersky Endpoint Security for Android (see page 30)
This section describes the methods for deploying Kaspersky Endpoint Security for Android on a corporate network.

Installing Kaspersky Safe Browser for iOS (see page 45)
This section describes the methods of deploying Kaspersky Safe Browser for iOS on a corporate network.

Installing an iOS MDM profile (see page 49)
This section describes the methods of deploying iOS MDM profiles on a corporate network.

Installing administration plug-ins (see page 52)
This section describes the process of installing administration plug-ins of the Kaspersky Security for Mobile integrated solution on the administrator’s workstation.

Application licensing (see page 53)
This section provides information about the general terms related to licensing of Kaspersky Security for Mobile.

Updating a previous version of the application (see page 65)
This section contains step-by-step instructions on upgrading the version of Kaspersky Security for Mobile.

Uninstalling the application (see page 69)
This section contains step-by-step instructions on removing Kaspersky Security for Mobile.

Contacting the Technical Support service (see page 73)
This section describes the ways to get technical support and the terms on which it is available.

Glossary (see page 77)
This section contains a list of terms that are mentioned in the document and their definitions.

Kaspersky Lab AO (see page 79)
This section provides information about AO Kaspersky Lab.

Information about third-party code (see page 81)
This section provides information about the third-party code used in the application.
Trademark notifications (see page 82)
This section lists trademarks of third-party manufacturers that were used in the document.

Index (see page 88)
This section allows you to quickly find required information within the document.

Document conventions
This document uses the following conventions (see table below).

<table>
<thead>
<tr>
<th>Sample text</th>
<th>Description of document convention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note that ...</td>
<td>Warnings are highlighted in red and enclosed in frames. Warnings show information about actions that may have unwanted consequences.</td>
</tr>
<tr>
<td>We recommended that you use...</td>
<td>Notes are boxed. Notes provide additional and reference information.</td>
</tr>
<tr>
<td>Example:</td>
<td>Examples are given in blocks against a blue background under the heading &quot;Example&quot;.</td>
</tr>
<tr>
<td>Update means...</td>
<td>The following elements are italicized in the text:</td>
</tr>
<tr>
<td>The Databases are out of date</td>
<td>• New terms</td>
</tr>
<tr>
<td>event occurs.</td>
<td>• Names of application statuses and events.</td>
</tr>
<tr>
<td>Press ENTER.</td>
<td>The names of keyboard keys appear in bold and are capitalized.</td>
</tr>
<tr>
<td>Press ALT+F4.</td>
<td>Names of keys that are connected by a + (plus) sign indicate the use of a key combination. Those keys must be pressed simultaneously.</td>
</tr>
<tr>
<td>Click the Enable button.</td>
<td>Names of application interface elements, such as entry fields, menu items, and buttons, are in bold.</td>
</tr>
<tr>
<td>► To configure a task schedule:</td>
<td>Introductory phrases of instructions are italicized and are accompanied by the arrow sign.</td>
</tr>
<tr>
<td>In the command line, type help.</td>
<td>The following types of text content are set off with a special font:</td>
</tr>
<tr>
<td>The following message appears:</td>
<td>• Text in the command line</td>
</tr>
<tr>
<td>Specify the date in DD:MM:YY format.</td>
<td>• Text of messages that the application displays on the screen;</td>
</tr>
<tr>
<td>&lt;User name&gt;</td>
<td>• Data to be entered using the keyboard.</td>
</tr>
<tr>
<td></td>
<td>Variables are in angle brackets. It is required to replace each variable by the corresponding value, omitting angle brackets.</td>
</tr>
</tbody>
</table>

Table 1. Document conventions
Sources of information about the application

This section lists the sources of information about the app.

You can select the most suitable information source, depending on importance and urgency of the issue.

In this section

<table>
<thead>
<tr>
<th>Other sources of information about the application</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discussing Kaspersky Lab applications on the Forum</td>
<td>10</td>
</tr>
</tbody>
</table>

Other sources of information about the application

Web page of Kaspersky Security for Mobile on Kaspersky Lab website

On the Kaspersky Security for mobile page (http://www.kaspersky.com/business-security/mobile#tab=frame-1), you can find general information about the application, its features and operation parameters.

The web page of Kaspersky Security for Mobile provides a link to eStore. There you can purchase or renew the application.

Web page of Kaspersky Security for Mobile in Knowledge Base

Knowledge Base is a section on the Technical Support website.

On the Kaspersky Security for mobile page in the Knowledge Base (https://support.kaspersky.com/ks10mob), you can find articles that contain useful information, recommendations and answers to frequently asked questions on the application purchasing, installation, and use.

Knowledge Base articles can answer questions relating to not only Kaspersky Security for mobile but also to other Kaspersky Lab applications. Knowledge Base articles can also include Technical Support news.

Online help

The online help of the application comprises help files.

The context help of administration plug-ins for Kaspersky Security for Mobile provides information about the windows of Kaspersky Security Center: a description of Kaspersky Security for Mobile settings and links to descriptions of the tasks that use these settings.

Full help of the Kaspersky Endpoint Security and Kaspersky Safe Browser apps provides information on how to configure and use the mobile apps.
Discussing Kaspersky Lab applications on the Forum

If your question does not require an immediate answer, you can discuss it with Kaspersky Lab experts and other users in our forum (https://forum.kaspersky.com).

In this forum you can view existing topics, leave your comments, and create new discussion topics.
Kaspersky Security for Mobile

This section describes the features, components, and distribution kit of the Kaspersky Security for Mobile integrated solution, and contains a list of hardware and software requirements for Kaspersky Security for Mobile.

In this section

About Kaspersky Security for Mobile ........................................................................................................ 11
About Kaspersky Endpoint Security for Android app ............................................................................. 12
About Kaspersky Safe Browser mobile app ............................................................................................ 14
About iOS MDM profile .......................................................................................................................... 15
About an Exchange mailbox ................................................................................................................... 16
About the Kaspersky Endpoint Security for Android administration plug-in ........................................ 16
About the Kaspersky Device Management for iOS administration plug-in .............................................. 17
Distribution kit ........................................................................................................................................ 17

About Kaspersky Security for Mobile

Kaspersky Security 10.0 for Mobile Service Pack 4 (hereinafter referred to as "Kaspersky Security for Mobile") is an integrated solution for protecting and managing corporate mobile devices as well as personal mobile devices used by company employees for corporate purposes.

Kaspersky Security for Mobile includes the following components:

- Kaspersky Endpoint Security for Android mobile app.
  
  Kaspersky Endpoint Security for Android ensures protection of mobile devices against viruses and other applications that pose a threat, unwanted calls and SMS messages, and web threats.

- Kaspersky Safe Browser mobile app.
  
  Kaspersky Safe Browser is a browser that provides secure Internet access from devices running iOS operating system.

- Administration Plug-in for Kaspersky Endpoint Security for Android.
  
  The Administration Plug-in of Kaspersky Endpoint Security for Android provides the interface for managing mobile devices and mobile apps installed on them via the Administration Console of Kaspersky Security Center.
• Kaspersky Device Management for iOS administration plug-in.

The Kaspersky Device Management for iOS administration plug-in lets you define the configuration settings for devices connected to Kaspersky Security Center via the iOS MDM protocol (hereinafter referred to as "iOS MDM devices") and the Exchange ActiveSync protocol (hereinafter referred to as "EAS devices"), without using the iPhone Configuration Utility or the Exchange Management Console.

The Administration Plug-ins are integrated into the Kaspersky Security Center remote administration system. 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. After you connect mobile devices to the Administration Server, they become managed. The administrator can remotely monitor managed devices.

The Kaspersky Endpoint Security for Android and Kaspersky Safe Browser mobile apps may also operate as part of the Kaspersky Endpoint Security Cloud remote administration system. For more details on working with apps through Kaspersky Endpoint Security Cloud, please refer to Kaspersky Endpoint Security Cloud Online Help.

The Kaspersky Endpoint Security for Android mobile app can also operate as part of third-party EMM solutions of AppConfig Community participants.

About Kaspersky Endpoint Security for Android app

Kaspersky Endpoint Security for Android ensures protection of mobile devices against viruses and other applications that pose a threat, unwanted calls and SMS messages, and web threats.

Kaspersky Endpoint Security for Android 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.
  • Scan. It is started on demand for the entire file system, only for installed apps, or a selected file or folder.
  • Update. Update allows you to download new Anti-Virus databases for the application.
• Anti-Theft. This component protects information on the device against unauthorized access in case the device is lost or stolen. This component lets you use commands to lock the device, locate the device, sound an alarm, take a mugshot of its current user, or remotely wipe data from the device.
• Call & Text Filter. Depending on the selected mode of operation, the Call & Text Filter lets you block unwanted incoming calls and SMS messages. 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 SMS messages from all numbers on the device contact list or block incoming calls and SMS messages from all numbers that contain letters.
• Web Protection. This component blocks malicious sites designed to spread malicious code. Web Protection also blocks fake (phishing) websites 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. Web Protection 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 allows the administrator to restrict user access to certain categories of web pages (for example, web pages from the “Gambling, lotteries, sweepstakes” or “Internet communication” categories).

• Synchronization. Allows connecting a mobile device to the Administration Server. Synchronization makes it possible to configure remotely the settings of the app and the mobile device using group policies configured in the Administration Console of Kaspersky Security Center.

• 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. When the number of report entries exceeds 200, the component overwrites older entries with new ones.
About Kaspersky Safe Browser mobile app.

*Kaspersky Safe Browser* is a browser that provides secure Internet access from devices running iOS operating system.

Kaspersky Safe Browser includes the following components:

- **Web Protection.** This component blocks malicious sites designed to spread malicious code. Web Protection also blocks fake (phishing) websites 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. Web Protection 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 allows the administrator to restrict user access to certain categories of web pages (for example, web pages from the "Gambling, lotteries, sweepstakes" or "Internet communication" categories).

- **Anti-Theft.** Lets you use commands to locate a mobile device that has been lost or stolen.

- **Synchronization.** Allows connecting a mobile device to the Administration Server. Synchronization makes it possible to configure remotely the settings of the app and the mobile device using group policies configured in the Administration Console of Kaspersky Security Center.
For more details on Kaspersky Safe Browser, please refer to the Kaspersky Safe Browser User Guide.

**About iOS MDM profile**

An *iOS MDM profile* is a profile that contains the settings for connecting mobile devices running iOS to Kaspersky Security Center. After installing an iOS MDM profile and synchronizing with Kaspersky Security Center, the device becomes a managed device. Mobile devices are managed through the Apple Push Notification service (APNs). For more details on installing an iOS MDM profile and working with APNs, please refer to the Kaspersky Security Center Implementation Guide in the section titled "Deploying mobile device management systems".

Using an iOS MDM profile, you can:

- Remotely configure the settings of iOS MDM devices using group policies.
- Send device lock and data wipe commands.
- Remotely install Kaspersky Lab apps and other third-party apps.
About an Exchange mailbox

An Exchange mailbox is a client app of the Exchange ActiveSync service. The app is intended to help corporate users work with mail, calendar, contacts, and tasks. An Exchange mailbox lets you connect a mobile device to a Microsoft Exchange server. For more details about the Exchange ActiveSync service, please visit the Microsoft Technical Support website https://technet.microsoft.com/.

To manage mobile devices via the Exchange ActiveSync protocol, Exchange Server must be deployed on the Microsoft Exchange server. For more details on installing an Exchange Server, please refer to the Kaspersky Security Center Deployment Guide in the section titled "Deploying mobile device management systems". No additional configuration is required on mobile devices.

Using an Exchange mailbox, you can remotely configure the settings of EAS devices by using group policies and send the data wipe command. The following operating systems support the Exchange ActiveSync protocol:

- Windows Mobile
- Windows CE
- Windows Phone
- Android
- Bada
- BlackBerry 10
- iOS
- Symbian

The contents of the set of management settings for an Exchange ActiveSync device depend on the operating system running on the mobile device. For details on the support features of the Exchange ActiveSync protocol for a specific operating system, please refer to the documentation on the specific operating system.

About the Kaspersky Endpoint Security for Android administration plug-in

The Administration Plug-in of Kaspersky Endpoint Security for Android provides the interface for managing mobile devices and mobile apps installed on them via the Administration Console of Kaspersky Security Center. The Administration Plug-in of Kaspersky Endpoint Security for Android can be used to:

- Create group security policies for mobile devices.
- Remotely configure the operating settings of the Kaspersky Endpoint Security for Android and Kaspersky Safe Browser apps on users' mobile devices.
- Receive reports and statistics on the operation of the Kaspersky Endpoint Security for Android and Kaspersky Safe Browser mobile apps on users' devices.

The Kaspersky Endpoint Security for Android administration plug-in is installed by default when deploying Kaspersky Security Center. The plug-in does not require individual installation.
About the Kaspersky Device Management for iOS administration plug-in

The administration plug-in of Kaspersky Device Management for iOS provides an interface for managing mobile devices connected via the iOS MDM and Exchange ActiveSync protocol via the Administration Console of Kaspersky Security Center. The Kaspersky Device Management for iOS administration plug-in can be used to:

- Create group security policies for mobile devices.
- Remotely define configuration settings of devices connected via the Exchange ActiveSync protocol (hereinafter referred to as "EAS devices").
- Remotely define configuration settings of devices connected via the iOS MDM protocol (hereinafter referred to as "iOS MDM devices").
- Receive reports and statistics on the operation of mobile devices of users.

For more details on connecting mobile devices to Kaspersky Security Center via the iOS MDM and Exchange ActiveSync protocols, please refer to the Kaspersky Security Center Implementation Guide in the section titled "Deploying mobile device management systems".

The Kaspersky Device Management for iOS administration plug-in is installed by default when deploying Kaspersky Security Center. The plug-in does not require individual installation.

Distribution kit

The Kaspersky Security for Mobile distribution kit includes the following components:

- The sc_package_xx self-unpacking archive containing setup files of mobile apps for all supported systems:
  - adb.exe, AdbWinApi.dll, AdbWinUsbApi.dll – a set of files needed to install Kaspersky Endpoint Security for Android.
  - installer.ini – is the configuration file that contain the Administration Server connection setting.
  - kmlisten.exe – the tool for delivering the application installation package via the workstation.
  - kmlisten.ini – the configuration file that contains the settings for the installation package delivery tool.
  - kmlisten.kpd – is the application description file.

- klcfginst_en.exe is the setup file of the Kaspersky Endpoint Security for Android plug-in for administering the application via the Kaspersky Security Center remote administration system.

- klmdminst.exe is the setup file of the Kaspersky Device Management for iOS administration plug-in for managing the application via the Kaspersky Security Center remote administration system.
- **KES10_xx_xx_xxx.apk** – a setup file for Kaspersky Endpoint Security for Android.

- **licutil.exe** is a utility for activating Kaspersky Endpoint Security for Android app if Kaspersky Security Center is not deployed in your organization.

- **SigningUtility.zip** – an archive that contains the utility for signing the distribution package of the mobile app and containers for iOS devices.

Documentation:

- Context Help for the Administration Plug-in of Kaspersky Endpoint Security for Android.
- Context-sensitive Help for the Kaspersky Device Management for iOS administration plug-in.
- Help for Kaspersky Endpoint Security for Android.
Hardware and software requirements

This section lists the hardware and software requirements for the administrator's computer that is used to deploy the apps on mobile devices, as well as the mobile device operating systems supported by Kaspersky Security for Mobile.

Hardware and software requirements for the administrator’s computer

To deploy the comprehensive solution Kaspersky Security for Mobile, the administrator’s computer must meet the hardware requirements of Kaspersky Security Center. For more details on using the hardware requirements of Kaspersky Security Center, see the Kaspersky Security Center Administrator’s Guide.

To work with the Administration Plug-in of Kaspersky Endpoint Security for Android, the Administration Console of Kaspersky Security Center version 10.0 must be installed on the administrator’s computer.

To work with the Kaspersky Device Management for iOS Administration Plug-in, the administrator’s computer must meet the following software requirements:

- Administration Console of Kaspersky Security Center 10 Service Pack 3
- Exchange Server component
- iOS MDM Server component
- Instruction set of version SSE2 or more recent version

To deploy the Kaspersky Endpoint Security for Android mobile app via the Administration Server, the administrator’s computer must meet the following software requirements:

- Kaspersky Security Center 10 Service Pack 3.
- Administration Plug-in for Kaspersky Endpoint Security for Android.

To support deployment of the Kaspersky Safe Browser for iOS mobile app via the iOS MDM Server, the administrator’s computer must meet the following software requirements:

- Kaspersky Security Center 10 Service Pack 3.
- Kaspersky Device Management for iOS administration plug-in.

There are no software requirements for the administrator’s computer when the Kaspersky Endpoint Security for Android, Kaspersky Safe Browser for iOS mobile apps are deployed from the relevant online stores.

Hardware and software requirements for the user’s mobile device to support installation of Kaspersky Endpoint Security for Android

Kaspersky Endpoint Security for Android has the following hardware and software requirements:

- Smartphone or tablet with a screen resolution of 320x480 pixels or higher
- 65 MB of free disk space in the main memory of the device
- Android operating system versions 4.2 – 9.0
- Processor architecture: Intel Atom x86, ARM5, ARM6 or ARM7
The app is installed to the main memory of the device only.

A SIM card should be inserted in the device to allow use of Call & Text Filter and SIM Watch functionality.

Hardware and software requirements for the user’s mobile device to support installation of iOS MDM profile

iOS MDM profile has the following hardware and software requirements.

- iOS operating system versions 9.0 – 11.4.1.
- Internet connection.

Hardware and software requirements for the user’s mobile device to support installation of Kaspersky Safe Browser for iOS

Kaspersky Safe Browser for iOS has the following hardware and software requirements.

- Device type: iPhone 4 or a later model.
- 35 MB of free disk space in the main memory of the device.
- iOS operating system versions 10.0 – 12.0.
- Internet connection.
Application architecture

Kaspersky Security for Mobile includes the following components:

- **Kaspersky Endpoint Security for Android mobile app.**
  
  Kaspersky Endpoint Security for Android ensures protection of mobile devices against viruses and other applications that pose a threat, unwanted calls and SMS messages, and web threats. It supports interaction between the mobile device and the Kaspersky Security Center Administration Server using Google Cloud Messaging.

- **Kaspersky Safe Browser mobile app.**
  
  *Kaspersky Safe Browser* is a browser that provides secure Internet access from devices running iOS operating system. It supports interaction between the mobile device and the Kaspersky Security Center Administration Server.

- **Administration Plug-in for Kaspersky Endpoint Security for Android.**
  
  The Administration Plug-in of Kaspersky Endpoint Security for Android provides the interface for managing mobile devices and mobile apps installed on them via the Administration Console of Kaspersky Security Center.

- **Kaspersky Device Management for iOS administration plug-in.**
  
  The administration plug-in of Kaspersky Device Management for iOS provides an interface for managing mobile devices connected via the iOS MDM and Exchange ActiveSync protocol via the Administration Console of Kaspersky Security Center.

The architecture of the Kaspersky Security for Mobile integrated solution is shown in the figure below.

![Figure 1. Architecture of Kaspersky Security for Mobile](image)

For details on the Administration Console, Administration Server, Exchange Server, and iOS MDM Server, please refer to the *Kaspersky Security Center Implementation Guide*. 
Common integrated solution deployment scenarios

This section covers the common deployment scenarios for the Kaspersky Security for Mobile integrated solution.

Different deployment scenarios can be used to deploy the integrated solution on Android devices and iOS devices. If the organization uses mobile devices running various operating systems, apps should be installed for each operating system separately by following the appropriate deployment scenario.

In this section

- Deployment scenarios for Kaspersky Endpoint Security for Android .......................................................... 22
- Deployment scenarios for Kaspersky Safe Browser for iOS ........................................................................... 24
- Deploying an iOS MDM profile .......................................................................................................................... 24

Deployment scenarios for Kaspersky Endpoint Security for Android

Kaspersky Endpoint Security for Android can be deployed on mobile devices within the corporate network in several ways. You can use the most suitable deployment scenario for your organization or combine several deployment scenarios.

For details on deploying Kaspersky Endpoint Security for Android in Kaspersky Endpoint Security Cloud, please refer to Kaspersky Endpoint Security Cloud Online Help, section “Device management”.

Deploying Kaspersky Endpoint Security for Android via Kaspersky Security Center

You can deploy Kaspersky Endpoint Security for Android via Kaspersky Security Center by using the following methods:

- Deliver messages with the Google Play link.
- Deliver messages with a link to the standalone app package.

Deployment of Kaspersky Endpoint Security for Android using Google Play consists in sending messages containing the Google Play link to users of devices from the Administration Console.
Deployment of Kaspersky Endpoint Security for Android via standalone package delivery consists of the following steps to be performed by the administrator:

1. Creating an app installation package. (see section "Creating an installation package" on page 41).
2. Configuring installation package settings. (see section "Configuring installation package settings" on page 42).
3. Creating a standalone installation package. (see section "Creating a standalone installation package" on page 43).
4. Sending messages with a link for downloading a standalone installation package to users of Android devices. Mass mailing is available. (see section "Installing via Kaspersky Security Center" see page 31).

The user installs Kaspersky Endpoint Security for Android on a mobile device after receiving a message with a Google Play link or a link for downloading the installation package from the Kaspersky Security Center Web Server. No additional preparations are needed to begin using the app.

Deploying Kaspersky Endpoint Security for Android via Self Service Portal

*Self Service Portal* is a web portal that lets the administrator delegate some of the mobile device management functions to users. For details on Self Service Portal, please refer to the *Kaspersky Security Center Implementation Guide*, section "Installing Self Service Portal" and the *Kaspersky Security Center Administrator's Guide*, section "Self Service Portal".

Users install Kaspersky Endpoint Security for Android on mobile devices on their own. After adding their mobile devices on Self Service Portal, users download the mobile app distribution package and install it to their device. No additional preparations are needed to begin using the app. To install the app via Self Service Portal, the user must be registered on Self Service Portal.

Deploying Kaspersky Endpoint Security for Android from Google Play

It is recommended to employ the Google Play deployment scenario if remote installation is not possible.

Kaspersky Endpoint Security for Android is installed from Google Play independently by the users of devices. Users download the mobile app distribution package from Google Play and install the app on devices. After the app has been installed on the device, you need to make additional preparations before you can begin using it: configure the settings of the connection to the Administration Server and install a general certificate (see section “Creating a general certificate” see page 29).

Deploying Kaspersky Endpoint Security for Android via KNOX Mobile Enrollment

Deployment via KNOX Mobile Enrollment is possible only for Samsung devices running Android version 5.0 or later. For the list of supported devices, visit the Samsung technical support website https://www.samsungknox.com/en/knox-platform/supported-devices/2.4+.
KNOX Mobile Enrollment (KME) is part of the Samsung KNOX mobile solution. Samsung KNOX is a mobile solution for configuring and protecting Samsung mobile devices running the Android operating system. For more details about Samsung KNOX, please visit the Samsung technical support website.

*KNOX Mobile Enrollment* is a cloud-based tool for automatic registration of devices in Samsung KNOX, quick deployment of enterprise apps on devices, and initial configuration of apps.

Deployment of Kaspersky Endpoint Security for Android consists of adding a KNOX MDM profile to mobile devices. The KNOX MDM profile contains a link to an app deployed on the Kaspersky Security Center Web Server or another server. After the app is installed on the mobile device, you must also install a general certificate (see section "Creating a general certificate" on page 29).

**Deployment scenarios for Kaspersky Safe Browser for iOS**

Kaspersky Safe Browser for iOS can be deployed on devices in a corporate network by using several different methods. You can use the most suitable deployment scenario for your organization or combine several deployment scenarios.

**Deploying Kaspersky Safe Browser for iOS via Kaspersky Security Center**

You can deploy Kaspersky Safe Browser for iOS via Kaspersky Security Center by using the following methods:

- Deliver messages with the App Store link.
- Use the command from the list of mobile devices, if the device is connected to Kaspersky Security Center.

For more details on connecting iOS devices to Kaspersky Security Center, please refer to the *Kaspersky Security Center Implementation Guide* in the section titled "Deploying mobile device management systems”.

**Deploying Kaspersky Safe Browser for iOS from App Store**

It is recommended to employ the App Store deployment scenario if remote installation is not possible.

Users install Kaspersky Safe Browser on their mobile devices on their own. Users download the mobile app distribution package from App Store and install the app on devices. After the app has been installed on the device, you need to make additional preparations before you can begin using it: configure the settings of the connection to the Administration Server and install a general certificate (see section “Creating a general certificate” see page 29).

**Deploying an iOS MDM profile**

An iOS MDM profile can be deployed on mobile devices within the corporate network in several ways. You can use the most suitable deployment scenario for your organization or combine several deployment scenarios.

Before deploying an iOS MDM profile, the administrator must do the following:

1. Install an iOS MDM Server.
2. Obtain an Apple Push Notification Service certificate (APNs certificate).
3. Install an APNs certificate to the iOS MDM Server.

For more details on installing an iOS MDM Server and working with an APNs certificate, please refer to the Kaspersky Security Center Implementation Guide in the section titled "Deploying mobile device management systems".

For details on deploying an iOS MDM profile in Kaspersky Endpoint Security Cloud, please refer to Kaspersky Endpoint Security Cloud Online Help, section "Device management".

Deploying an iOS MDM profile via Kaspersky Security Center

Deployment of an iOS MDM profile via Kaspersky Security Center can be carried out by sending messages containing a link to download the iOS MDM profile. Mass mailing is available.

The user installs the iOS MDM profile to a mobile device after receiving the message with a link to the Kaspersky Security Center Web Server. No additional preparations for the iOS MDM profile are required.

For more details on creating an iOS MDM profile, please refer to the Kaspersky Security Center Implementation Guide in the section titled "Deploying mobile device management systems".

Deploying an iOS MDM profile via Self Service Portal

Self Service Portal is a web portal that lets the administrator delegate some of the mobile device management functions to users. For details on Self Service Portal, please refer to the Kaspersky Security Center Implementation Guide in the section titled "Installing Self Service Portal" RU&link=online_help&pid=Cloud&version=1.0&helpid=89534.htm, and the Kaspersky Security Center Administrator’s Guide, "Self Service Portal" section.

The user independently installs the iOS MDM profile to the mobile device. After adding the mobile device on Self Service Portal, the user downloads the iOS MDM profile and installs it to the device. No additional preparations are needed to begin using the app. To install an iOS MDM profile via Self Service Portal, the user must be registered on Self Service Portal.
Preparing the Administration Console for deployment of the integrated solution

This section provides instructions on preparing the Administration Console for deployment of the integrated solution.

In this section

- Configuring Administration Server settings for connection of mobile devices ........................................ 26
- Displaying the Mobile Device Management folder in the Administration Console ......................................... 27
- Creating an administration group .................................................................................................................. 27
- Creating a rule for device automatic allocating to administration groups ...................................................... 28
- Creating a general certificate .......................................................................................................................... 29

Configuring Administration Server settings for connection of mobile devices

In order for mobile devices to be able to connect to the Administration Server, before installing the Kaspersky Endpoint Security and Kaspersky Safe Browser mobile apps configure the mobile device connection settings in the Administration Server properties.

► To configure Administration Server settings for connecting mobile devices:

1. In the context menu of the Administration Server, select Properties.
   The Administration Server settings window opens.
2. Select Server connection settings → Additional ports.
3. Select the Open port for mobile devices check box.
4. In the Port for mobile devices field, specify the port through which mobile devices will connect to the Administration Server.
   Port 13292 is used by default. If the Open port for mobile devices check box is cleared or the wrong connection port is specified, mobile devices will not be able to connect to the Administration Server.
5. In the Port to activate mobile clients field, specify the port to be used by mobile devices to connect to the Administration Server for activation of the Kaspersky Endpoint Security for Android and Kaspersky Safe Browser apps. Port 17100 is used by default.
6. Click OK.
Displaying the Mobile Device Management folder in the Administration Console

By displaying the Mobile Device Management folder in the Administration Console, you can view the list of mobile devices managed by the Administration Server, configure the mobile device management settings, and install certificates on mobile devices of users.

To enable the display of the Mobile Device Management folder in the Administration Console:

1. In the context menu of the Administration Server, select View → Configuring interface.
2. In the window that opens, select the Display Mobile Device Management check box.
3. Click OK.

The Mobile Device Management folder is displayed in the Administration Console tree after the Administration Console is restarted.

Creating an administration group

To perform centralized configuration of the Kaspersky Endpoint Security for Android and Kaspersky Safe Browser apps installed on the users' mobile devices, the group policies must be applied to the devices.

To apply the policy to a device group, you are advised to create a separate group for these devices in the Managed devices prior to installing mobile apps on user devices.

After creating an administration group, you are advised to configure the option to allocate devices on which you want to install the apps to this group automatically (see section "Creating a rule for device automatic allocating to administration groups" on page 28). Then configure settings that are common to all devices using a group policy.

To create administration group, follow the steps below:

1. In the console tree, select the Managed devices folder.
2. In the workspace of the Managed devices folder or subfolder, select the Devices tab.
3. Click the Create group button.

   This opens the window in which you can create a new group.

4. In the Group name window type the group name and click OK.

A new administration group folder with the specified name appears in the console tree. For more detailed information on use of administration groups, see Kaspersky Security Center Administrator's Guide.
Creating a rule for device automatic allocating to administration groups

You can administer the settings of Kaspersky Endpoint Security for Android and Kaspersky Safe Browser apps installed on users' mobile devices centrally only if the devices belong to a previously created administration group for which a group policy has been configured (see section "Creating an administration group" on page 27).

If the rule to automatically allocate mobile devices detected on the network to the administration group is not configured, during the first synchronization of the device with the Administration Server, the device is automatically sent to the Administration Console in the Additional → Network poll → Domains → KES10 folder. A group policy does not apply to this device.

To create the rule for automatic allocating of mobile devices to administration group, follow the steps below:

1. In the console tree, select the Unassigned devices folder.
2. From the context menu of the Unassigned devices folder, select Properties.
   The Properties: Unassigned devices window appears.
3. In the Move devices section, click Add to start the process of creating a rule for automatically allocating devices to an administration group.
   The New rule window appears.
4. Type the rule name.
5. Specify the administration group to which mobile devices should be allocated after the Kaspersky Endpoint Security for Android or Kaspersky Safe Browser mobile apps have been installed on them. To do so, click Browse to the right of the Group to move devices to field and select the group in the window that appears.
6. In the Rule application section, select Run once for each device.
7. Select the Move only devices not added to administration groups check box to prevent allocating to the selected group the mobile devices that were allocated to other administration groups when applying the rule.
8. Select the Enable rule check box, so that the rule can be applied to newly detected devices.
9. Open the Apps section and do the following:
   a. Select the Operating system version check box.
   b. Select one or several types of operating systems of the devices to be allocated to the specified group: Android or iOS.
10. Click OK.

The newly created rule is displayed in the list of device allocation rules in the Move devices section in the properties window of the Unassigned devices folder.
Preparing the Administration Console for deployment of the integrated solution

According to the rule, Kaspersky Security Center allocates all devices that meet the specified requirements from the Unassigned devices folder to the selected group. The mobile devices which were earlier allocated to the Unassigned devices folder can also be allocated to the required administration group of the Managed devices folder manually. For more detailed information on administration groups management and actions with undistributed devices, see Kaspersky Security Center Administrator’s Guide.

Creating a general certificate

You have to create a general certificate in Administration Console for the purpose of identifying the user of a mobile device.

► To create a general certificate:

1. In the console tree, select the Mobile Device Management → Certificates folder.
2. In the workspace of the Certificates folder, click the Add certificate button to start the Certificate Installation Wizard.
3. In the Certificate type window of the Wizard, select the General certificate option.
4. In the User selection window of the Wizard, specify the users for whom you want to create a general certificate.
5. In the Certificate source window of the Wizard, select the method by which the general certificate is created.
   - To create a general certificate automatically using Administration Server tools, select Issue certificate through Administration Server tools.
   - To assign a previously created certificate to a user, select the Specify certificate file option. Click the Specify button to open the Certificate window and specify the certificate file in it.
     Clear the Publish certificate check box if you do not want to specify the type of mobile device and the method of notifying the user about certificate creation.
6. In the Method of user notification window of the Wizard, configure the settings of mobile device user notification about certificate creation using a text message or via email.
7. In the Generating the certificate window of the Wizard, click Done to finish the Certificate Installation Wizard.

As a result, the Certificate Creation Wizard creates a general certificate that the user can install on the mobile device. To get the certificate, start synchronization of the mobile device with the Administration Server. For more information about creating certificates and configuring rules for issuing them, please refer to the Kaspersky Security Center Administrator’s Guide.
Install Kaspersky Endpoint Security for Android

This section describes the methods for deploying Kaspersky Endpoint Security for Android on a corporate network.

In this section

Permissions.......................................................................................................................... 30
Installing via Kaspersky Security Center ................................................................. 31
Installation from Self Service Portal ........................................................................ 33
Installation from Google Play .......................................................... 34
Installing via KNOX Mobile Enrollment ............................................................ 35
Creating an installation package ........................................................................ 41
Configuring installation package settings ................................................................. 42
Creating a standalone installation package ............................................................... 43
Configuring synchronization settings ......................................................................... 44

Permissions

For all features of apps, Kaspersky Endpoint Security for Android prompts the user for the required permissions. Kaspersky Endpoint Security for Android prompts for the mandatory permissions while completing the Setup Wizard, as well as after installation prior to using individual features of apps. It is impossible to install Kaspersky Endpoint Security for Android without providing the mandatory permissions.

On certain devices (for example, Huawei, Meizu, and Xiaomi), you must manually add Kaspersky Endpoint Security for Android to the list of apps that are started when the operating system starts (Security → Permissions → Autorun). If the app is not added to the list, Kaspersky Endpoint Security for Android stops performing all of its functions after the mobile device is restarted.
Table 2. Permissions requested by Kaspersky Endpoint Security for Android

<table>
<thead>
<tr>
<th>Permission</th>
<th>App function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call management (mandatory)</td>
<td>Call &amp; Text Filter</td>
</tr>
<tr>
<td></td>
<td>Connect to Kaspersky Security Center (device ID)</td>
</tr>
<tr>
<td>Memory access (mandatory)</td>
<td>Anti-Virus</td>
</tr>
<tr>
<td>Device administrator (mandatory)</td>
<td>Anti-Theft – lock the device (only for Android 4.1 – 6.X)</td>
</tr>
<tr>
<td></td>
<td>Anti-Theft – take a mugshot of the thief</td>
</tr>
<tr>
<td></td>
<td>Anti-Theft – sound an alarm</td>
</tr>
<tr>
<td></td>
<td>Anti-Theft – full reset</td>
</tr>
<tr>
<td></td>
<td>Password protection</td>
</tr>
<tr>
<td></td>
<td>App removal protection</td>
</tr>
<tr>
<td></td>
<td>Install security certificate</td>
</tr>
<tr>
<td></td>
<td>App Control</td>
</tr>
<tr>
<td></td>
<td>Manage KNOX (only for Samsung devices)</td>
</tr>
<tr>
<td></td>
<td>Configure Wi-Fi</td>
</tr>
<tr>
<td></td>
<td>Configure Exchange ActiveSync</td>
</tr>
<tr>
<td></td>
<td>Restrict use of the camera, Bluetooth, and Wi-Fi</td>
</tr>
<tr>
<td>Camera access</td>
<td>Anti-Theft – take a mugshot of the thief</td>
</tr>
<tr>
<td>Locate</td>
<td>Anti-Theft – locate device</td>
</tr>
<tr>
<td>Manage SMS</td>
<td>SIM Watch</td>
</tr>
<tr>
<td></td>
<td>Call &amp; Text Filter</td>
</tr>
<tr>
<td>Accessibility</td>
<td>Anti-Theft – lock the device (only for Android 7.0 or later)</td>
</tr>
<tr>
<td></td>
<td>Web Protection (only for Android 5.0 or later)</td>
</tr>
<tr>
<td></td>
<td>App Control</td>
</tr>
<tr>
<td></td>
<td>App removal protection (only for Android 7.0 or later)</td>
</tr>
</tbody>
</table>

Installing via Kaspersky Security Center

Kaspersky Endpoint Security for Android is installed to the mobile devices of users whose user accounts have been added in Kaspersky Security Center. For more details about user accounts in Kaspersky Security Center, please refer to the Kaspersky Security Center Administrator’s Guide, section "Managing user accounts".
Kaspersky Security for Mobile lets you install the app via Kaspersky Security Center using the following methods:

- **Using a Google Play link**
  
  The user will receive a link to Google Play. In the link, the Kaspersky Security Center synchronization settings and general certificate are encrypted. The app can be installed by following the standard installation procedure of the Android platform. Additional configuration of Kaspersky Endpoint Security for Android after installation is not required.

- **Using a link to your own Web Server**
  
  This installation method is convenient if you want to install a specific version of Kaspersky Endpoint Security for Android.

To install Kaspersky Endpoint Security for Android using a link to your own web server:

1. Create an installation package (see section "Creating an installation package" on page 41).
   
   The *installation package* is a set of files created for remote installation of the Kaspersky Lab app via Kaspersky Security Center.

2. Configure the installation package settings (see section "Configuring installation package settings" on page 42).

3. Create a standalone installation package (see section "Creating a standalone installation package" on page 43).
   
   A *standalone installation package* is the installation file of a mobile app that contains the settings of the app connection to the Administration Server. It is created on the basis of the Kaspersky Endpoint Security for Android installation package. The standalone installation package is a special case of an installation package.

   The user will receive a link to the web server hosting the standalone installation package for Kaspersky Endpoint Security for Android. To install the app, the user must run the APK file. Additional configuration of Kaspersky Endpoint Security for Android after installation is not required.

To install Kaspersky Endpoint Security for Android using a link to your own web server, installation of apps from unknown sources must be allowed on the user’s mobile device (Android Settings → Security → Unknown sources).

- **To install Kaspersky Endpoint Security for Android via Kaspersky Security Center:**

  1. In the console tree, select the Mobile Device Management → Mobile devices folder.
  
  2. In the workspace of the Mobile devices folder, click the Add mobile device button.
     
     This starts the New Mobile Device Connection Wizard. Follow the instructions of the Wizard.
  
  3. In the Operating system window of the Wizard, select Android.
  
  4. In the Kaspersky Endpoint Security for Android installation method, select the app installation method:
     
     - Using a Google Play link.
• By using a link from Web Server.

5. In the Select users window of the Wizard, select one or several users for installation of Kaspersky Endpoint Security for Android to their mobile devices.

   If the user is not in the list, you can add a new user account without exiting the New Mobile Device Connection Wizard.

6. In the Certificate source window of the Wizard, select the source of the certificate for protection of data transfer between Kaspersky Endpoint Security for Android and Kaspersky Security Center:

   • Issue certificate through Administration Server tools. In this case, the certificate will be created automatically.

   • Specify certificate file. In this case, your own certificate must be prepared ahead of time and then selected in the window of the Wizard. This option cannot be used if you want to install Kaspersky Endpoint Security for Android to several mobile devices. A separate certificate must be created for each user.

7. In the User notification method window of the Wizard, select the channel used to forward the app installation link:

   • To send the link by email, select Send link to Kaspersky Endpoint Security and configure the settings in the By email section. Make sure that the email address is specified in the settings of user accounts.

   • To send the link by SMS message, select Send link to Kaspersky Endpoint Security and configure the settings in the By SMS section. Make sure that the phone number is specified in the settings of user accounts.

   • To install Kaspersky Endpoint Security for Android using a QR code, select Show link to installation package and scan the QR code using the camera of the mobile device.

   • If none of the listed methods are suitable for you, select Show link to installation package → Copy to copy the link for installing Kaspersky Endpoint Security for Android to the clipboard. Use any available method to deliver the app installation link.

8. Finish the New Mobile Device Connection Wizard.

After installing Kaspersky Endpoint Security for Android to users’ mobile devices, you will be able to configure the settings for devices and apps by using group policies. You will also be able to send commands to mobile devices for data protection in case devices are lost or stolen.

**Installation from Self Service Portal**

Kaspersky Endpoint Security for Android is installed from Self Service Portal manually by the device user. After adding their mobile devices to the Self Service Portal, users download the Kaspersky Endpoint Security for Android installation package to devices. The package includes the Kaspersky Endpoint Security for Android distribution package, a general certificate, and the Administration Server connection settings. Users use their own Self Service Portal accounts to install the app.
After Kaspersky Endpoint Security for Android has been installed on the mobile device, the app is prepared for operation automatically.

For detailed information on adding a mobile device to Self Service Portal and on the Kaspersky Endpoint Security for Android installation procedure, please refer to the Kaspersky Security Center Administrator's Guide, section "Self Service Portal".

Installation from Google Play

Kaspersky Endpoint Security for Android is installed from Google Play by users manually. The app can be installed by following the standard installation procedure of the Android platform. Users use their own Google accounts to install the application.

For details on the procedure of installing Kaspersky Endpoint Security for Android from Google Play, see the Google technical support website http://support.google.com/googleplay/.

After installing Kaspersky Endpoint Security for Android from Google Play, you must prepare the app for use. The process of preparing the app for use includes the following steps:

1. The administrator sends the settings of mobile device synchronization with the Administration Server (server address and port number) using any available method (for example, by sending an email message).

2. The user can configure the settings of mobile device synchronization with the Administration Server during operation of the Initial Configuration Wizard or in the Kaspersky Endpoint Security for Android settings.

3. The administrator creates a general certificate (see section "Creating a general certificate" on page 29) for a mobile device user.

4. The user receives an automatic notification with a prompt to install the general certificate. When installation is confirmed, the general certificate is installed on the mobile device.

Internet access should be enabled on the mobile device for synchronization with the Administration Server.

See the Kaspersky Endpoint Security for Android Help for details on how to configure the settings of mobile device synchronization with the Administration Server and receive a general certificate.

During the next synchronization of the mobile device with Administration Server, the user's mobile device on which Kaspersky Endpoint Security for Android is installed is moved to the Additional → Network poll → Domains folder in the administration group that was specified during installation of the application (the default group is KES10). You can move a mobile device to the administration group you created in the Managed devices folder either manually or using automatic allocation rules (see section Creating a rule for device automatic allocating to administration groups on page 28).
Installing via KNOX Mobile Enrollment

KNOX Mobile Enrollment (KME) is part of the Samsung KNOX mobile solution. Samsung KNOX is a mobile solution for configuring and protecting Samsung mobile devices running the Android operating system. For more details about Samsung KNOX, please visit the Samsung technical support website.

KNOX Mobile Enrollment is a cloud-based tool for automatic registration of devices in Samsung KNOX, quick deployment of enterprise apps on devices, and initial configuration of apps. KNOX Mobile Enrollment is used for batch installation and initial configuration of apps on new Samsung devices purchased from official vendors.

Installation of the Kaspersky Endpoint Security for Android app via KNOX Mobile Enrollment consists of the following steps:

a. Creating a KNOX MDM profile with the Kaspersky Endpoint Security for Android app. (see section "Creating a KNOX MDM profile" on page 35)

b. Adding devices in KNOX Mobile Enrollment. (see section "Installing the app" on page 41)

c. Installing the Kaspersky Endpoint Security for Android app on the user's mobile devices. (see section "Installing the app" on page 41)

For more details about working with KNOX Mobile Enrollment, please refer to the KNOX Mobile Enrollment User Guide https://docs.samsungknox.com/KME-Getting-Started/Content/about-kme.htm.

Deployment via KNOX Mobile Enrollment is possible only for Samsung devices running Android version 5.0 or later. For the list of supported devices, visit the Samsung technical support website https://www.samsungknox.com/en/knox-platform/supported-devices/2.4+.

In this section

Creating a KNOX MDM profile ............................................................................................................................ 35
Adding devices in KNOX Mobile Enrollment ..................................................................................................... 36
Installing the app .............................................................................................................................................. 41

Creating a KNOX MDM profile

A KNOX MDM profile is a profile that contains links to apps for their quick deployment and initial configuration on mobile devices.

► To create a KNOX MDM profile:

2. Select the MDM profiles section.
3. Click Add. 
   The New KNOX MDM Profile Wizard starts.

4. At the MDM server connection step, select Server URI is not required for my MDM service and click Next.

5. At the MDM profile info step:
   a. Enter general information about the KNOX MDM profile: Profile name and Description.
   b. Click the Add MDM apps button and enter the path to the APK installation file.
      The installation file for Kaspersky Endpoint Security for Android is included in the Kaspersky Security for Mobile distribution kit (see section "Distribution kit" on page 17). Beforehand, place the APK installation file on the Kaspersky Security Center Web Server or on another server that is accessible for downloading from the device.
   c. Enter the settings for connecting the device to Kaspersky Security Center in the JSON user data field in the following format: 
      "serverAddress":"ksc.server.com","serverPort":"12345","groupName":"MOBILE GROUP".
      The device must be connected to Kaspersky Security Center to activate the app (see section "Activating the application" on page 61), configure the device, and send commands.
   d. Select the Add Knox agreements check box.
      To install Kaspersky Endpoint Security for Android via KNOX Mobile Enrollment, the mobile device user must accept the terms of the Samsung License Agreement. You can view the terms of the Samsung License Agreement in the section named End User License Agreements, Terms of Service, and User Agreements. You can also add other legal documents of your company that are necessary for deploying a KNOX MDM profile by clicking the Add user agreement button.
   e. Clear the Bind Knox license to this profile check box.
      Samsung KNOX license information is delivered to the mobile device together with the policy when the device is synchronized with Kaspersky Security Center.

6. Click the Save button.
   As a result, the new KNOX MDM profile with the Kaspersky Endpoint Security for Android app will be added to the list in the KME console.

Adding devices in KNOX Mobile Enrollment

Devices can be added in the KNOX Mobile Enrollment (KME) console in the following ways:

- The vendor automatically adds devices in the KME console after the devices are purchased. Select this method if your organization is working with an official vendor of Samsung devices.
- The administrator installs the KNOX Deployment app from Google Play on their mobile device and migrates the KNOX MDM profile to users’ devices through Bluetooth or NFC (Near Field Communication). After deployment of the KNOX MDM profile, the device will be automatically added in the KME console.
Select this method if the Samsung devices were not purchased from an official vendor.

Adding a device through the vendor

An official vendor of Samsung devices is registered in Samsung KNOX. For the list of official vendors, visit the Samsung technical support website [https://www2.samsungknox.com/support](https://www2.samsungknox.com/support). The vendor automatically adds devices in the KME console for your Samsung account immediately after the devices are purchased. To have the devices added by the vendor, you must register the vendor in the KME console for your Samsung account. You will need a reseller ID to add the vendor of Samsung devices in the KME console. To receive the reseller ID, you must send a request to the vendor. In the request, specify your KNOX client ID.

► To view your KNOX client ID:

2. Select the Resellers section.
3. Your ID is displayed in the KNOX client ID field.

After you receive a response from the vendor with the reseller ID, register the vendor in the KME console. Prior to registering the vendor, you can create a KNOX MDM profile so that the profile can be automatically deployed when adding new devices.

► To register an official vendor in the KME console:

2. Select the Resellers section.
3. Click the Register reseller button.

   This opens a window for registering the device vendor.
4. In the Reseller ID field, enter the ID received from the official vendor of Samsung devices.
5. If you created a KNOX MDM profile (see section "Creating a KNOX MDM profile" on page 35), select the KNOX MDM profile in the vendor registration window.

   When you add new devices, the KNOX MDM profile is automatically installed.
6. In the Preferred download confirmation method list, select a method for confirming the addition of a device for a vendor.
   - **All downloads must be confirmed.** When a device is added by the vendor, you will need to confirm the operation.
   - **Automatically confirm all downloads of this reseller.** Devices of the vendor will be automatically added in the KME console.
7. Click OK.

The vendor of Samsung devices will be added to the list of vendors in the KME console.
After new devices are purchased from the official vendor, the Kaspersky Endpoint Security for Android app will be automatically installed to the devices after the devices are connected to the Internet. For more details about working with KNOX Mobile Enrollment, please refer to the KNOX Mobile Enrollment User Guide https://docs.samsungknox.com/KME-Getting-Started/Content/about-kme.htm. If you already have a list of devices in the KME console, add the KNOX MDM profile with the KNOX MDM app to the device.

► To deliver a KNOX MDM profile to devices:

2. Select Devices → All devices.
3. Select the devices on which you want to install the KNOX MDM profile.
4. Click the Configure button.
   The Device info window opens.
5. In the MDM profile list, select the KNOX MDM profile with the Kaspersky Endpoint Security for Android app.
6. In the Tags field, enter tags for grouping and labeling devices, and for search optimization in the KME console.
7. Enter the user account credentials of the device into the UserID and Password fields.
   Account credentials are required for receiving a general certificate. The user ID and password must match the user account credentials in Kaspersky Security Center (Full name and Password in user account properties).
8. Select the KNOX MDM profile for the remaining devices.
9. Click the Save button.
   After the device is connected to the Internet, the user will be prompted to install the KNOX MDM profile.

Adding a device through the KNOX Deployment app

If you did not purchase your Samsung device from an official vendor, you can add the device to KNOX Mobile Enrollment through Bluetooth or NFC. This will require the administrator's mobile device that will be used to deliver KNOX MDM profiles to users' mobile devices.

To add devices using the KNOX Deployment app, the following conditions must be met:

- Depending on the selected delivery mode, Bluetooth or NFC modules must be enabled on the mobile devices.
- The mobile devices must be connected to the Internet.
To deliver a KNOX MDM profile using the KNOX Deployment app:

1. Install the KNOX Deployment app from Google Play
   on the administrator’s mobile device.
2. Start the KNOX Deployment app.
3. Enter your Samsung account credentials.
4. In the KNOX Deployment window, configure the settings for deploying a KNOX MDM profile:
   - Select the KNOX MDM profile (see section "Creating a KNOX MDM profile" on page 35).
   - Select the deployment mode: Bluetooth or NFC.
     When using Bluetooth, you can add a KNOX MDM profile to several devices at the same time.
5. Click Start deployment:
     This starts the Samsung KNOX Device Registration Wizard. Follow the instructions on the screen.
     After the KNOX MDM profile is installed, the new device with the Bluetooth tag will be added in the KME console.
   - NFC. Bring the administrator’s mobile device close to the user’s mobile device and transfer the KNOX MDM profile (see the figure below).
On the user’s mobile device, there will be a prompt to install the KNOX MDM profile. The new device with the NFC tag will be added in the KME console.

Figure 2. KNOX Deployment app
Installing the app

Prior to installing the Kaspersky Endpoint Security for Android app, issue a general certificate for mobile device users in the Kaspersky Security Center Administration Console (see section "Creating a general certificate" on page 29). A general certificate is required for identifying the mobile device user in the Kaspersky Security Center Administration Console.

After deployment of the KNOX MDM profile is started, the APK installation file will be automatically downloaded on the mobile device. Installation of the Kaspersky Endpoint Security for Android app is started automatically. The user must accept the Samsung KNOX License Agreement and the Kaspersky Endpoint Security for Android License Agreement. No additional configuration of the app is required. After the app is installed, synchronization with Kaspersky Security Center will be performed automatically. The mobile device will be added to the Kaspersky Security Center Administration Console to the administration group specified in the KNOX MDM profile settings (see section "Creating a KNOX MDM profile" on page 35) (groupName).

Creating an installation package

The Kaspersky Endpoint Security for Android installation package is the ak_package.exe self-extracting archive. The archive includes files required for installing mobile app on devices:

- adb.exe, AdbWinApi.dll, AdbWinUsbApi.dll – a set of files needed to install Kaspersky Endpoint Security for Android.
- installer.ini – is the configuration file that contain the Administration Server connection setting.
- kmlisten.exe – the tool for delivering the application installation package via the workstation.
- kmlisten.ini – the configuration file that contains the settings for the installation package delivery tool.
- kmlisten.kpd – is the application description file.

To create the Kaspersky Endpoint Security for Android installation package:

1. In the console tree, select the Advanced ➔ Remote installation ➔ Installation packages folder.
2. In the workspace of the Installation packages folder, click the Create installation package button.
   The Installation Package Creation Wizard starts. Follow the instructions of the Wizard.
3. In the Select installation package type window of the Wizard, click the Create installation package for Kaspersky Lab application button.
4. In the Defining installation package name window of the Wizard, enter the installation package name that will be displayed in the workspace of the Installation packages folder.
5. In the **Select application installation package for installation** window of the Wizard, select the **ak_package.exe** self-extracting archive included in the distribution kit.

   If you have already unpacked the archive, choose the application description file, **kmlisten.kpd**. The application name and the version number appear in the entry field.

   After the wizard finishes, the created installation package appears in the **Installation packages** folder workspace. The installation packages are stored in the **Packages** folder, in the public shared folder on the Administration Server.

### Configuring installation package settings

**To configure the installation package settings:**

1. In the console tree, select the **Additional > Remote installation > Installation packages** folder.

2. In the context menu of the Kaspersky Endpoint Security for Android installation package, select **Properties**.

3. On the **Settings** tab, specify the Administration Server connection settings for mobile devices and the name of the administration group to which the mobile devices will be added automatically after the first synchronization with the Administration Server. Follow the steps below:

   - In the **Connection to the Administration Server** section, in the **Server address** field, type the name of the Administration Server for mobile devices in the format that was used for installing **Mobile devices support** during the Administration Server deployment.

     Depending on the Administration Server name format for the **Mobile devices support** component, specify the DNS name or the IP address of the Administration Server. In the **SSL port number** field, specify the number of the port open on the Administration Server for connecting mobile devices. Port 13292 is used by default.

   - In the **Allocation of computers to groups** section, in the **Group name** field, type the name of the group to which mobile devices will be added after the first synchronization with the Administration Server (**KES10** is used by default).

     The specified group will be automatically created in the **Additional → Network poll → Domains** folder.

   - In the **Actions during installation** section, select the **Request email address** check box if you want the app to ask users to provide their corporate email address when the app is started for the first time.

     The user’s email address is used to form the name of the mobile device when it is added to the administration group.

4. To apply the specified settings, click **Apply**.
Creating a standalone installation package

To create a standalone installation package, follow the steps below:

1. In the console tree, select the Advanced → Remote installation → Installation packages folder.
2. Choose the installation package of Kaspersky Endpoint Security for Android.
3. In the context menu of the installation package, select Create a standalone installation package. The wizard that creates the standalone installation package will be started. Follow the instructions of the Wizard.
4. Configure ways in which the standalone installation package is distributed:
   - To distribute the path to the created standalone installation package among users via email, in the Further actions section click the link Send the link to the standalone installation package by email.
     The message editor window opens, and the text in the window contains the path to the shared folder with the standalone installation package.
   - To post the link to the created standalone installation package on your corporate website, click the link Sample HTML code for posting link on website.
     A tmp file containing HTML_RJL links opens.
5. To publish the created standalone installation package on the Kaspersky Security Center Web Server and view the entire list of standalone packages for the selected installation package, in the Standalone installation package wizard completed successfully window select the Open the stand-alone packages list check box.

After the wizard closes, the window List of standalone packages for the installation package <Installation package name> opens.

The List of standalone packages for the installation package <Installation package name> window contains the following information:

- A list of standalone installation packages.
- The network path to the shared folder in the Path field.
- The address of the standalone package on the Kaspersky Security Center Web Server in the URL field.

When sending email notifications, you can specify either the address in the URL field or the path in the Path field as a resource from which users can download the setup file of the app. When sending text message notifications to users, you have to specify the download link appearing in the URL field.

You are advised to copy the address of the created standalone package to clipboard and then paste the link to the required installation package into the email or text message notification for users.
Configuring synchronization settings

To manage mobile devices and receive reports or statistics from mobile devices of users, you must configure the synchronization settings. Mobile device synchronization with Kaspersky Security Center may be performed in the following ways:

- **By schedule.** Synchronization by schedule is performed using the HTTP protocol. You can configure the synchronization schedule in the group policy settings. Modifications to group policy settings, commands and tasks will be performed when the device is synchronizing with Kaspersky Security Center according to the schedule, i.e. with a delay. By default, mobile devices are synchronized with the Kaspersky Security Center automatically every 6 hours.

- **Forced.** Forced synchronization is performed using push notifications of the GSM service (Google Cloud Messaging). Forced synchronization is primarily intended for timely delivery of commands to a mobile device. If you want to use forced synchronization, make sure that the GSM settings are configured in Kaspersky Security Center.

► To configure the settings of mobile device synchronization with the Kaspersky Security Center:

1. In the console tree, in the **Managed devices** folder, select the administration group to which the Android devices belong.
2. In the workspace of the group, select the **Policies** tab.
3. Open the policy properties window by double-clicking.
4. In the policy **Properties** window, select the **Synchronization** section.
5. Select the frequency of synchronization in the **Synchronize** drop-down list.
6. To disable synchronization of a device with Kaspersky Security Center while roaming, select the **Do not synchronize while roaming** check box.

   The device user can manually perform synchronization in the app settings (*→ Settings → Synchronization → Synchronize*).

7. To hide synchronization settings (server address, port and administration group) from the user in the app settings, clear the **Show synchronization settings on device** check box. It is impossible to modify hidden settings.
8. Click the **Apply** button to save the changes you have made.

Mobile device settings are configured after the next device synchronization with the Kaspersky Security Center. You can manually synchronize the mobile device by using a special command. To learn more about working with commands for mobile devices, please refer to the *Kaspersky Security Center Administrator’s Guide in the section “Mobile Device Management”*. 
Installing Kaspersky Safe Browser for iOS

This section describes the methods of deploying Kaspersky Safe Browser for iOS on a corporate network.

In this section

- Installing via Kaspersky Security Center .......................................................... 45
- Installation from App Store .................................................................................. 47
- Configuring synchronization settings .................................................................... 48

Installing via Kaspersky Security Center

Kaspersky Safe Browser for iOS is installed to the mobile devices of users whose user accounts have been added in Kaspersky Security Center. For more details about user accounts in Kaspersky Security Center, please refer to the Kaspersky Security Center Administrator’s Guide, section "Managing user accounts".

Kaspersky Security for Mobile lets you install the app via Kaspersky Security Center using the following methods:

- **Using the App Store link**
  The user will receive a link to App Store. In the link, the Kaspersky Security Center synchronization settings and general certificate are encrypted. The app can be installed by following the standard installation procedure of the iOS platform. Additional configuration of Kaspersky Safe Browser for iOS after installation is not required.

- **Using a special command**
  To install Kaspersky Safe Browser for iOS using a special command, the mobile devices must be connected to the iOS MDM Server. For this, an iOS MDM profile must be installed on the mobile device (see section "Installing an iOS MDM profile" on page 49). For more details on connecting mobile devices to the iOS MDM Server, please refer to the Kaspersky Security Center Implementation Guide in the section titled "Deploying mobile device management systems".

  The user will receive a link to App Store. In the link, the Kaspersky Security Center synchronization settings are encrypted. The app can be installed by following the standard installation procedure of the iOS platform. Additional configuration of Kaspersky Safe Browser for iOS after installation is not required.

- To install Kaspersky Safe Browser for iOS via Kaspersky Security Center:
  1. In the console tree, select the **Mobile Device Management** → **Mobile devices** folder.
  2. In the workspace of the **Mobile devices** folder, click the **Add mobile device** button.

     This starts the New Mobile Device Connection Wizard. Follow the instructions of the Wizard.
3. In the **Operating system** window of the Wizard, select iOS.

4. In the **iOS MDM device protection method** window of the Wizard, select **Install Kaspersky Safe Browser by using the App Store link**.

5. In the **Select users** window of the Wizard, select one or several users for installation of Kaspersky Safe Browser for iOS to their mobile devices.

   If the user is not in the list, you can add a new user account without exiting the New Mobile Device Connection Wizard.

6. In the **Certificate source** window of the Wizard, select the source of the certificate for protection of data transfer between Kaspersky Safe Browser for iOS and Kaspersky Security Center:

   - **Issue certificate through Administration Server tools.** In this case, the certificate will be created automatically.

   - **Specify certificate file.** In this case, your own certificate must be prepared ahead of time and then selected in the window of the Wizard. This option cannot be used if you want to install Kaspersky Safe Browser for iOS to several mobile devices. A separate certificate must be created for each user.

7. In the **User notification method** window of the Wizard, select the channel used to forward the app installation link:

   - To send the link by email, select **Send link to Kaspersky Safe Browser** and configure the settings in the **By email** section. Make sure that the email address is specified in the settings of user accounts.

   - To send the link by SMS message, select **Send link to Kaspersky Safe Browser** and configure the settings in the **By SMS** section. Make sure that the phone number is specified in the settings of user accounts.

   - To install Kaspersky Safe Browser for iOS using a QR code, select **Show link to installation package** and scan the QR code using the camera of the mobile device.

   - If none of the listed methods are suitable for you, select **Show link to installation package → Copy** to copy the link for installing Kaspersky Safe Browser for iOS to the clipboard. Use any available method to deliver the app installation link.

8. Finish the New Mobile Device Connection Wizard.

   After installing Kaspersky Safe Browser for iOS to users' mobile devices, you will be able to configure app settings by using group policies. You will also be able to send commands to mobile devices for data protection in case devices are lost or stolen.

   You can also install Kaspersky Safe Browser for iOS using a special command if the mobile devices are connected to the iOS MDM Server. For this, an iOS MDM profile must be installed on the mobile device (see section "Installing an iOS MDM profile" on page 49). For more details on connecting mobile devices to the iOS MDM Server, please refer to the **Kaspersky Security Center Implementation Guide in the section titled "Deploying mobile device management systems"**.

   **To install Kaspersky Safe Browser using a command:**

   1. In the console tree, select the **Mobile Device Management → Mobile devices folder**.
2. In the list of mobile devices, select the device to which you want to install Kaspersky Safe Browser after making sure that the device is connected via the iOS MDM protocol.

3. In the context menu of the mobile device, select **All commands → Install Kaspersky Safe Browser**.

   The Kaspersky Safe Browser installation command will be sent to the mobile device. The user receives a notification containing a prompt to install Kaspersky Safe Browser. After the user confirms installation, the app is installed to the mobile device. You can track the progress of command execution in the command log.

### Installation from App Store

Kaspersky Safe Browser [https://itunes.apple.com/ru/app/kaspersky-safe-browser/id723879672](https://itunes.apple.com/ru/app/kaspersky-safe-browser/id723879672) can be installed from App Store by the user. The app can be installed by following the standard installation procedure of the iOS platform. The user uses a personal Apple ID to install the app.

For details on Kaspersky Safe Browser installation from App Store, see the *User Guide for Kaspersky Safe Browser*.

After installing Kaspersky Safe Browser from App Store, you must prepare the app for use. The process of preparing the app for use includes the following steps:

1. The administrator sends the settings of mobile device synchronization with the Administration Server (server address and port number) using any available method (for example, by sending an email message).

2. The user can configure the settings of mobile device synchronization with the Administration Server during operation of the Initial Configuration Wizard or in the Kaspersky Safe Browser settings.

   See the *User Guide for Kaspersky Safe Browser* for details on how to configure the settings of mobile device synchronization with the Administration Server and receive a general certificate.

3. The administrator creates a general certificate for a mobile device user (see section "Creating a general certificate" on page 29).

4. The user receives a notification with a prompt to install the general certificate. When the user confirms installation, the general certificate is installed on the mobile device.

   Internet access should be enabled on the mobile device for synchronization with the Administration Server.
During the next synchronization of the mobile device with Administration Server, the user’s mobile device on which Kaspersky Safe Browser is installed is moved to the **Additional → Network poll → Domains** folder in the administration group that was specified during installation of the application (the default group is **KES10**). You can move a mobile device to the group you created in the **Managed computers** folder either manually or using automatic allocation rules (see section Creating a rule for device automatic allocating to administration groups on page **28**).

**Configuring synchronization settings**

To apply a group policy on mobile devices of users, you should configure the frequency of starting synchronization with Kaspersky Security Center.

By default, mobile devices are synchronized with the Kaspersky Security Center automatically every 6 hours. Automatic synchronization is enabled for when the device is roaming.

---

**To configure the settings of mobile device synchronization with the Kaspersky Security Center:**

1. In the console tree, in the **Managed devices** folder, select the administration group containing devices with the Kaspersky Safe Browser app installed.

   A Kaspersky Endpoint Security for Android policy is used to manage devices that have the Kaspersky Safe Browser app installed.

2. In the workspace of the group, select the **Policies** tab.

3. Open the policy properties window by double-clicking.

4. In the policy **Properties** window, select the **Synchronization** section.

5. Select the frequency of synchronization in the **Synchronize** drop-down list.

6. To disable synchronization of a device with Kaspersky Security Center while roaming, select the **Do not synchronize while roaming** check box.

   The device user can manually perform synchronization in the app settings (**→ Settings → Synchronization → Synchronize**).

   a. To hide synchronization settings (server address, port and administration group) from the user in the app settings, clear the **Show synchronization settings on device** check box. It is impossible to modify hidden settings.

   b. To block automatic synchronization with the Administration Server when the device is roaming, select the **Do not synchronize while roaming** check box.

7. Click the **Apply** button to save the changes you have made.

Mobile device settings are configured after the next device synchronization with the Kaspersky Security Center.
Installing an iOS MDM profile

This section describes the methods of deploying iOS MDM profiles on a corporate network.

Before deploying an iOS MDM profile, the administrator must do the following:

1. Install an iOS MDM Server.
2. Obtain an Apple Push Notification Service certificate (APNs certificate).
3. Install an APNs certificate to the iOS MDM Server.

For more details on installing an iOS MDM Server and working with an APNs certificate, please refer to the Kaspersky Security Center Implementation Guide in the section titled “Deploying mobile device management systems”.

For details on deploying an iOS MDM profile in Kaspersky Endpoint Security Cloud, please refer to Kaspersky Endpoint Security Cloud Online Help, section “Device management”.

In this section

<table>
<thead>
<tr>
<th>About iOS device management modes</th>
<th>49</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installing via Kaspersky Security Center</td>
<td>50</td>
</tr>
<tr>
<td>Installation from Self Service Portal</td>
<td>51</td>
</tr>
</tbody>
</table>

About iOS device management modes

You can deploy an iOS device management system in several different ways. The management mode depends on the owner of the mobile device (personal or corporate) and corporate security requirements. You can choose the management mode that is most suitable for the company, and use several modes at the same time.

Unsupervised devices

Unsupervised iOS devices are employees' personal devices that are connected to Kaspersky Security Center. In this mode, the user is allowed to use a personal Apple ID, work with any apps, and store personal data on the device. You can use a Kaspersky Device Management for iOS group policy to configure access to corporate resources, security settings, and other settings. By default, all iOS devices are unsupervised.
Supervised devices

Supervised iOS devices are corporate devices that are connected to Kaspersky Security Center. Initial configuration of the mobile device is performed in Apple Configurator. Apple Configurator is an application designed to prepare and configure iOS devices. Apple Configurator is installed on a computer running OS X. For more details about working with Apple Configurator, please refer to the Apple Technical Support website https://support.apple.com. You can use a Kaspersky Device Management for iOS group policy for further configuration. On supervised devices, you can access an extended selection of settings. For example, you can configure Global HTTP Proxy and additional restrictions (for example, blocked use of iMessage and Game Center), and you can block user account modifications.

To work with supervised and unsupervised iOS devices, the iOS MDM Server must have an APNs certificate installed, and an iOS MDM profile must be installed on the mobile devices of users. If you do not have an APNs certificate, you can use Kaspersky Safe Browser (see section "About Kaspersky Safe Browser app" on page 14). If this is the case, you cannot configure the iOS device settings, except for controlling access to web resources in Kaspersky Safe Browser, Internet protection, and sending commands to mobile devices from Kaspersky Security Center. You can also use Kaspersky Safe Browser together with supervised and unsupervised devices.

Installing via Kaspersky Security Center

The iOS MDM profile is installed to the mobile devices of users whose user accounts have been added in Kaspersky Security Center. For more details about user accounts in Kaspersky Security Center, please refer to the Kaspersky Security Center Administrator’s Guide, section "Managing user accounts".

To install an iOS MDM profile:

1. In the console tree, select the Mobile Device Management → Mobile devices folder.
2. In the workspace of the Mobile devices folder, click the Add mobile device button.
   
   This starts the New Mobile Device Connection Wizard. Follow the instructions of the Wizard.

3. In the Operating system window of the Wizard, select iOS.

4. In the iOS MDM device protection method window of the Wizard, select Use iOS MDM profile of iOS MDM Server and specify the iOS MDM profile from the list.

5. In the Select users window of the Wizard, select one or several users for installation of the iOS MDM profile to their mobile devices.
   
   If the user is not in the list, you can add a new user account without exiting the New Mobile Device Connection Wizard.

6. In the Certificate source window of the Wizard, select the source of the certificate for protection of data transfer between the mobile device and Kaspersky Security Center:
   
   • Issue certificate through Administration Server tools. In this case, the certificate will be created automatically.

Installing an iOS MDM profile
• **Specify certificate file.** In this case, your own certificate must be prepared ahead of time and then selected in the window of the Wizard. This option cannot be used if you want to install the iOS MDM profile to several mobile devices. A separate certificate must be created for each user.

7. In the **User notification method** window of the Wizard, select the channel used to forward the app installation link:

   • To send the link by email, select **Send link to iOS MDM profile** and configure the settings in the **By email** section. Make sure that the email address is specified in the settings of user accounts.
   
   • To send the link by SMS message, select **Send link to iOS MDM profile** and configure the settings in the **By SMS** section. Make sure that the phone number is specified in the settings of user accounts.
   
   • To install the iOS MDM profile using a QR code, select **Show link to installation package** and scan the QR code using the camera of the mobile device.
   
   • If none of the listed methods are suitable for you, select **Show link to installation package → Copy** to copy the iOS MDM profile installation link to the clipboard. Use any available method to deliver the app installation link.

8. Finish the New Mobile Device Connection Wizard.

After installing the iOS MDM profile to users’ mobile devices, you will be able to configure the app settings by using group policies. You will also be able to send commands to mobile devices for data protection in case devices are lost or stolen.

**Installation from Self Service Portal**

The iOS MDM profile is installed from Self Service Portal manually by the user. After adding their mobile devices to Self Service Portal, users download the iOS MDM profile to their devices. The iOS MDM profile also includes a general certificate and the Administration Server connection settings. Users use their own Self Service Portal accounts to install the iOS MDM profile.

For detailed information on adding a mobile device to Self Service Portal and on the iOS MDM profile installation procedure, please refer to the *Kaspersky Security Center Administrator's Guide*, section "Self Service Portal".
Installing administration plug-ins

To manage mobile devices, the following administration plug-ins must be installed to the administrator’s workstation:

- The Administration Plug-in of Kaspersky Endpoint Security for Android provides the interface for managing mobile devices and mobile apps installed on them via the Administration Console of Kaspersky Security Center.

- The administration plug-in of Kaspersky Device Management for iOS provides an interface for managing mobile devices connected via the iOS MDM and Exchange ActiveSync protocol via the Administration Console of Kaspersky Security Center.

► To install the Kaspersky Endpoint Security Administration Plug-in,

copy the plug-in installation file klcfinst.exe from the integrated solution distribution package and run it on the administrator's workstation.

The installation is performed by the wizard, and you do not need to configure the settings.

► To install the Kaspersky Device Management for iOS administration plug-in:

copy the plug-in installation file klmdminst.exe from the integrated solution distribution package and run it on the administrator's workstation.

Plug-in installation is performed by the wizard, and you do not need to configure the settings.

You can make sure that the administration plug-ins are installed by viewing the list of installed app administration plug-ins in the properties window of the Administration Server in the Additional → Information about the installed application administration plug-ins section.
Application licensing

This section provides information about the general terms related to licensing of Kaspersky Security for Mobile.

In this section

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About the End User License Agreement</td>
<td>53</td>
</tr>
<tr>
<td>About the license</td>
<td>54</td>
</tr>
<tr>
<td>About the subscription</td>
<td>55</td>
</tr>
<tr>
<td>About the key</td>
<td>55</td>
</tr>
<tr>
<td>About the activation code</td>
<td>56</td>
</tr>
<tr>
<td>About the key file</td>
<td>56</td>
</tr>
<tr>
<td>About data provision</td>
<td>56</td>
</tr>
<tr>
<td>Activating the application</td>
<td>61</td>
</tr>
</tbody>
</table>

About the End User License Agreement

The End User License Agreement is a binding agreement between you and Kaspersky Lab AO, stipulating the terms on which you may use Kaspersky Security for Mobile.

We recommend carefully reading the terms of the License Agreement before using Kaspersky Security for Mobile.

You can view the terms of the License Agreement in the following ways:

- During installation of components of Kaspersky Security for Mobile.
- By reading the license.txt file. This file is included in the distribution kit of Kaspersky Security for Mobile.
- In the About the app section in Kaspersky Endpoint Security for Android and Kaspersky Safe Browser.

By confirming that you agree with the End User License Agreement when installing the components of Kaspersky Security for Mobile, you signify your acceptance of the terms of the End User License Agreement. If you do not accept the terms of the End User License Agreement, you should abort installation of Kaspersky Security for Mobile components and refrain from using them.
About the license

The license is a time-limited right to use the integrated solution Kaspersky Security for Mobile provided to you on the terms of the End User License Agreement.

A current license entitles you to the following kinds of services:

- Use apps on mobile devices in accordance with the terms of the End User License Agreement.
- Receive technical support.

The scope of available services and the app usage term depend on the type of license under which the app has been activated.

The following license types are provided:

- **Trial** – a free license intended for trying out the Kaspersky Security for Mobile.
  
  The trial license is valid for 30 days. When the trial license expires, the Kaspersky Endpoint Security for Android mobile app stops performing all its functions except for synchronization with the Administration Server. To continue using the app, you must purchase a commercial license.

- **A commercial license** is a pay-for license provided when you purchase Kaspersky Security for Mobile.

  When the commercial license expires, the mobile app continues to work, but with limited functionality. In limited functionality mode, the following components are available in the Kaspersky Endpoint Security for Android app:

  - **Anti-Virus**: Real-time Protection and Virus Scan of the device, but anti-virus database updates are not available.
  - **Anti-Theft**: Capability to send commands to the mobile device, and SIM Watch.
  - **Synchronization with the Administration Server**.

  The remaining components of the Kaspersky Endpoint Security for Android app are not available to the device user. The administrator can use group policies to manage these components in limited functionality mode. You cannot use group policies to configure the other components of the app.

Kaspersky Endpoint Security for Android stops exchanging information with Kaspersky Security Network and Google Analytics if the Kaspersky Lab key is blocked (see section "About the key" on page 55), if the trial license expires, or if a license is missing (the activation code is removed from the group policy).

To continue using the app in fully functional mode, you must renew your commercial license (see section "Activating the application" on page 61). We recommend renewing the license term or buying a new license before the current one expires in order to ensure maximum protection of your computer against all security threats.
About the subscription

*Subscription for Kaspersky Security for Mobile* is an order for using the mobile app with the selected parameters (subscription expiry date, number of mobile devices protected). You can order subscription for Kaspersky Security for Mobile from your service provider (such as your ISP). Subscription can be renewed manually or automatically, or you may cancel your subscription. You can manage your subscription on the website of the service provider.

Subscription can be limited (for example, one-year) or unlimited (with no expiration date). To keep Kaspersky Security for Mobile working after expiry of the limited subscription term, you have to renew your subscription. Unlimited subscription is renewed automatically provided a prepayment to the service provider was timely.

If the subscription is limited, when it expires you may be offered a grace period for renewing the subscription, during which time the apps will retain their functionality. The availability and duration of such grace period are at the discretion of the service provider.

To use Kaspersky Security for Mobile under subscription, you have to apply the activation code received from the service provider. After the activation code is applied, the key is installed for the license for using the application under subscription.

The possible subscription management options may vary with each service provider. The service provider may not offer a subscription renewal grace period during which the apps will retain their functionality.

Activation codes purchased under subscription cannot be used for activating earlier versions of Kaspersky Security for Mobile.

About the key

A *key* is a sequence of bits that you can apply to activate and then use the integrated solution Kaspersky Security for Mobile in accordance with the terms of the End User License Agreement. Keys are generated by Kaspersky Lab specialists.

You can add a mobile app key using a key file or activation code:

- If you organization has deployed the Kaspersky Security Center software suite, you have to apply the key file and distribute it to mobile apps (see section “Activating apps in Kaspersky Security Center” on page 61). They key is displayed in the interface of Kaspersky Security Center and the interface of the mobile app as a unique alphanumeric sequence.
- If your organization does not use the Kaspersky Security Center software suite, you have to add an activation code to the distribution package of the mobile app. (See section "Activating Kaspersky Endpoint Security for Android without Kaspersky Security Center" on page 62). The key is displayed in the mobile app interface as a unique alphanumeric sequence after you add it to the app.

After adding keys, you can replace them with other keys.
The key may be blocked by Kaspersky Lab if, for example, the terms of the End User License Agreement have been violated. If the key is blocked, the Kaspersky Endpoint Security for Android mobile app stops performing all its functions except for synchronization with the Administration Server. To continue using the app, you need to add a different key.

### About the activation code

*Activation code* is a unique sequence of 20 alphanumeric characters. You enter an activation code to add a key that activates Kaspersky Endpoint Security for Android. You receive the activation code at the email address that you have specified after purchasing the integrated solution Kaspersky Security for Mobile or after ordering the trial version of Kaspersky Security for Mobile.

To activate the mobile app with an activation code, you need Internet access to connect to Kaspersky Lab activation servers.

If you have lost your activation code after you activated the app, it can be restored. You may need your activation code, e.g., to register with Kaspersky CompanyAccount. To restore your activation code, send a request to Kaspersky Lab Technical Support (see section "Contacting Technical Support" on page 73).

### About the key file

A *key file* is a file with the .key extension that you receive from Kaspersky Lab. The purpose of a key file is to add a key that activates the mobile app.

You receive the key file at the email address that you have specified after purchasing the integrated solution Kaspersky Security for Mobile or after ordering the trial version of Kaspersky Security for Mobile.

You do not need to connect to Kaspersky Lab activation servers in order to activate the application with a key file.

You can recover a key file if it has been accidentally deleted. You may need a key file to register a Kaspersky CompanyAccount, for example.

To recover a key file, do one of the following:

- Contact Kaspersky Lab Technical Support (see section "Contacting Technical Support" on page 73).

### About data provision

Kaspersky Security for Mobile complies with the General Data Protection Regulations (GDPR).
To install the app, the user must accept the terms of the End User License Agreement. In addition, the Installation Wizard will prompt the user to accept the following Statements regarding the processing of the user’s personal data:

- Statement regarding data processing for marketing purposes.

The user may accept the terms of a Statement or decline them at any time in the About the app section in the settings of Kaspersky Endpoint Security for Android or Kaspersky Safe Browser.

Data provision under the End User License Agreement

To improve real-time protection, Kaspersky Security for Mobile uses the Kaspersky Security Network cloud service for the operation of the following components:

- **Anti-Virus.** The app runs a scan of installed apps before they are started for the first time. The scan is performed for threats whose information has not yet been added to Anti-Virus databases but is already available in KSN. Kaspersky Security Network cloud service provides full operation of Antivirus and reduces the likelihood of false alarms.

- **Web Protection.** The app uses data received from KSN to run scan of websites before they are opened. The app also determines the website category to control Internet access to users based on lists of allowed and blocked categories (for example, the "Internet communication" category).

- **App Control.** The app determines the app category to restrict the startup of apps that do not meet corporate security requirements based on lists of allowed and blocked categories (for example, the "Games" category).

Information on the type of data submitted to Kaspersky Lab when using KSN during operation of the Kaspersky Endpoint Security for Android and Kaspersky Safe Browser mobile apps is available in the End User License Agreement. By accepting the terms and conditions of the License Agreement, you agree to transfer the following information.

Where the Activation Code is used to activate the Software, in order to verify legitimate use of the Software, the End User agrees to periodically provide the Rightholder the following information: the type, version and localization of the installed Software, versions of the installed Updates, the identifier of the Computer and the identifier of the Software installation on the Computer, the activation code and the unique identifier of activation of the current license, activation date and time, the type, version and word size of the operating system, the name of the virtual environment when the Software is installed in the virtual environment, and identifiers of the Software components that are active at the time the information is provided, URL and IP address of activation service, certificate hash sum, certificate type and certificate contents of activation service.

In order to protect the Computer against information security threats, the End User agrees to periodically provide the Rightholder the following information:

- URL address of the page, port number, URL protocol, URL, which refers to the requested information;
- name of the detected object (file), MD5 hash sum of the detected object (APK file);
- name of the detected object according to the Kaspersky Lab classification, verdict type, database release date and time, Identifier of the anti-virus database record on which the verdict is based;
- application package name, name of store from which the application was downloaded, public key and hash sum of certificate used to sign the APK file.

The received information is protected by Kaspersky Lab in accordance with the requirements established by law. The original received information is stored in encrypted form and is destroyed as it is accumulated (twice per year) or at the request of the User. General statistics are stored indefinitely.

**Data provision under the Kaspersky Security Network Statement**

Use of the KSN could lead to increase the effectiveness of protection provided by the Software, against information and network security threats.

During use of the KSN, the Rightholder will automatically receive and process the following data:

- Information about the checksums of processed files (MD5 and SHA256)
- Name of the scanned file, size of the file (in bytes), and the file format
- Indicator of a portable executable (PE) file
- Reason for scanning the file: optimization of scan methods or categorization
- Full path to the file and path template code
- Name of the threat according to the Rightholder's classification
- ID of the detected threat in the threats database
- Information about updates of databases (database ID, database release date, and last update date and time)
- Data on the software and hardware configuration of the mobile device (OS type and version, model name, device ID, firmware version and build number, manufacturer name)
- Information about whether the user has obtained root/jailbreak privileges
- Information about executable files that were used to download detected threats (checksum (MD5), name and size of the file)
- Statistical data on detected adware and riskware (the web address of the page from which the transition was made to load the object, the size, name, and checksum (MD5) of the executable file that sent the request to the website, the web address of the link source from the HTTP request, the IP address of the server to which the connection was established, the version of the server operating system)
- The web address at which the object is loaded and the web address of the page from which the object is loaded
- IPv4 address of the host of the blocked object
• Settings of the Wi-Fi access point in use (the SSID, the checksum (MD5, SHA256) of the BSSID, whether the DNS domain, the checksum of a combination of identifiers: a device ID, the installation ID, and Wi-Fi network ID, a list of available wireless networks and access points (SSID and BSSID), category, security and publicity wireless network product, the settings DHCP, signal strength, wireless network, control the amount of given local IP addresses (IPv4 and IPv6), the local time start and of the disconnection, connection types, supported by the wireless access point, information about the authentication Protocol to be used and other technical information)

• Statistical data on detected adware adware (date of adware display, size of the advertisement window, data on the adware distribution package, the name of the application package, the name of the application installer (APK) and the path to it, the checksums (MD5) of the application installer (APK) and the DEX file)

• Statistical data on the distribution package of the affected app (the name of the application package, the name of the application installer (APK) and the path to it, the checksums (MD5) of the application installer (APK) and the DEX file)

• Device screen resolution

• App information: version, type, app ID, installation ID, checksum (MD5) of the application

• Information about scanned objects (MD5 hash sum of the DEX file, MD5 hash sum of the APK file, name of the APK file, name and application version from AndroidManifest.xml, product version, serial number of the certificate that was used to sign the APK file, issuer of the certificate that was used to sign the APK file, public key and hash sum of the certificate used to sign the APK file, date and time of signing, flag indicating whether the application has Device Administrator, Accessibility and other rights, flag indicating whether the application is a default SMS messenger, flag indicating whether the application is in the system catalog, information about enabling SafetyNet Attestation service, SafetyNet Attestation category and SHA256 hash sum of the scanned with SafetyNet Attestation object)

• The version of the statistics package (service information)

Also, in order to achieve the declared purpose of increasing the effectiveness of protection provided by the Software, the Rightholder may receive objects that could be exploited by intruders to harm the Computer and create information security threats.

The Rightholder uses third-party information systems to process data. Their data processing is governed by the privacy statements of such third-party information systems. The following are the third-party information systems that the Rightholder uses and the data they process:

During the use of the Software, the following data will be sent to Google Analytics automatically and on a regular basis in order to achieve the declared purpose: a part of the app code, information about the necessary permissions to the application, the path to the quarantined file.

Data is transferred to the Google Analytics services via a secure connection.

Providing the above information to the KSN is voluntary. You can opt out of participating in Kaspersky Security Network at any time.
Data provision under the Statement regarding data processing for marketing purposes

The Rightholder uses third-party information systems to process data. Their data processing is governed by the privacy statements of such third-party information systems. The following are the services that the Rightholder uses and the data they process:

- Google Analytics
- SafetyNet Attestation

During the use of the Software, the following data will be sent to Google Analytics automatically and on a regular basis in order to achieve the declared purpose:

- App info, including the app version, app ID, and the ID of the app in the Google Analytics service.
- ID of app installation on the device and method of installation on the device.
- About the region and language localization.
- About the device screen resolution.
- Information about the user obtaining root privileges
- Diagnostic data on the device from the SafetyNet Attestation service.
- Information about setting Kaspersky Endpoint Security for Android as an Accessibility feature.
- About navigation between app icons.
- About the protocol used to submit data to the Google Analytics service, its version, and ID of the data submission method used.
- Details on the type and parameters of the event for which the data is submitted.
- About the app license, its availability, the number of devices.
- Information about the intervals of anti-virus database updates and synchronization with the Administration Server.
- About the Administration Console (Kaspersky Security Center or third-party EMM systems).

Data is transferred to the Google Analytics services via a secure connection. Information about how data is processed in Google Analytics is published at: www.google.com/policies/privacy/partners/.

During the use of the Software, the following data will be sent to SafetyNet automatically and on a regular basis in order to achieve the declared purpose:

- device check time
- information about the software, name and data about the software certificates
- device check results
- random ID checks to verify the results of the check device

Data is forwarded to SafetyNet over a secure channel. Information about how data is processed in SafetyNet is published at: https://policies.google.com/privacy.
Providing the above information for processing for marketing purposes is voluntary.

Activating the application

In Kaspersky Security Center, the license can cover various groups of features. To ensure that Kaspersky Security for Mobile is fully functional, the Kaspersky Security Center license purchased by the organization must provide for Mobile Device Management functionality. The Mobile Device Management functionality is intended for connecting mobile devices to Kaspersky Security Center and managing them.

For detailed information about licensing of Kaspersky Security Center and licensing options, please refer to the Kaspersky Security Center Administrator’s Guide in the section titled “Licensing the application”.

When Kaspersky Endpoint Security for Android and Kaspersky Safe Browser are activated, license information is delivered to the mobile device together with the policy when the device is synchronized with Kaspersky Security Center.

If app activation is not completed within 30 days from the time of installation on the mobile device, the app is automatically switched to the limited functionality mode. In this mode, most of the app components are not operational. When switched to limited functionality mode, the app stops performing automatic synchronization with Kaspersky Security Center. Therefore, if for some reason the activation of the application has not been completed within 30 days after the installation, the user must synchronize the device with the Kaspersky Security Center manually.

If Kaspersky Security Center is not deployed in your organization, you can activate Kaspersky Endpoint Security for Android using the special licutil utility. In this case, activation of Kaspersky Safe Browser is not required.

In this section

Activating apps in Kaspersky Security Center ........................................................................................................................................................................ 61
Activating Kaspersky Endpoint Security for Android without Kaspersky Security Center .......................................................... 62

Activating apps in Kaspersky Security Center

To activate the Kaspersky Endpoint Security for Android and Kaspersky Safe Browser app:

1. In the console tree, in the Managed devices folder, select the administration group to which the Android devices belong.
2. In the workspace of the group, select the Policies tab.
3. Open the policy properties window by double-clicking.
4. In the policy Properties window, select the Licensing section.
5. In the License section, open the Key drop-down list and select the required application activation key from the key storage of the Kaspersky Security Center Administration Server.
The details of the app for which the license has been purchased are displayed in the field below.

6. Select the **Activate with a key from Kaspersky Security Center storage** check box.
   
   If the app was activated without a key stored in the Kaspersky Security Center storage, Kaspersky Security for Mobile replaces this key with the activation key selected in the **Key** list.

7. To activate the app on the user’s mobile device, block changes to settings.

8. Click the **Apply** button to save the changes you have made.

Mobile device settings are configured after the next device synchronization with the Kaspersky Security Center.

### Activating Kaspersky Endpoint Security for Android without Kaspersky Security Center

Activation of Kaspersky Endpoint Security for Android without using Kaspersky Security Center is recommended only when Kaspersky Security Center is not deployed at your organization.

You can activate the app by using the following methods:

- Add an activation code to the app distribution package before distributing it among users.
- Add 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 distribution package or to the Google Play link. The licutil utility is included in the distribution kit of Kaspersky Security for Mobile.

If the Kaspersky Security Center remote administration system is deployed at your organization, you can connect mobile devices installed with Kaspersky Endpoint Security for Android to Kaspersky Security Center and remotely manage mobile devices via the Administration Console. This requires activating the app using a key from the Kaspersky Security Center storage. If you have activated the app by sending a distribution package or a Google Play link with an activation code added, replace the active key with a key from the Kaspersky Security Center storage. After replacing the key, you can use the newly available key on another device. The term for using this key is limited by the term of its corresponding license.

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

**Example:**

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

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 text 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/](http://support.google.com/googleplay/).

To add an activation code to the app distribution 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 for Android installation package from the distribution kit> -t <path to the installation package with the added key> -c <activation code>.
```

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

You can deliver the distribution package to the user’s mobile device using any available method (for example, by copying the distribution 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 distribution 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.
Updating a previous version of the application

This section contains step-by-step instructions on upgrading the version of Kaspersky Security for Mobile.

In this section

Application upgrade requirements ........................................................................................................... 65
Upgrading the previous version of Kaspersky Endpoint Security for Android ........................................... 66
Upgrading the previous version of Kaspersky Safe Browser ...................................................................... 68
Upgrading previous versions of administration plug-ins.......................................................................... 68

Application upgrade requirements

The application upgrade must meet the following requirements:

- The version of the Kaspersky Endpoint Security administration plug-in and the version of the Kaspersky
  Endpoint Security for Android mobile app must match.
  You can view the build numbers of the versions of the administration plug-in and mobile app in the

- Make sure that Kaspersky Security Center satisfies the software requirements of Kaspersky Security for Mobile. (See section "Hardware and software requirements" on page 19).

- The administration plug-ins of Kaspersky Endpoint Security 10.0 Service Pack 2 (Build 10.6.0.1801) and
  Kaspersky Device Management for iOS 10.0 Service Pack 2 (Build 10.6.0.1767) and later versions can be
  automatically upgraded to the current version. Upgrades of earlier versions of administration plug-ins are not supported.
  To upgrade administration plug-ins of earlier versions, you must remove the installed administration
  plug-ins and group policies that were created with them. Then install the new versions of the administration plug-ins. For details on removing administration plug-ins, please visit the Kaspersky Lab Technical Support website
  http://support.kaspersky.com/9303.

- Use the same version of Kaspersky Endpoint Security for Android on all mobile devices of the organization.

The terms and conditions of technical support for Kaspersky Security for Mobile versions are available on
the Kaspersky Lab Technical Support website http://support.kaspersky.com/support/lifecycle#b2b.block0.ks10mob.
To view the version and build number of administration plug-ins:

1. In the console tree in the context menu of the Administration Server, select Properties.
2. In the Administration Server properties window, select Additional → Information about the installed application administration plug-ins.

The workspace displays information about installed administration plug-ins in the format <Plug-in name> <Version> <Build>.

You can view the version and build number of the Kaspersky Endpoint Security for Android app by using the following methods:

- If Kaspersky Endpoint Security for Android was installed with a standalone installation package (see page “Installing via Kaspersky Security Center” on page 31), you can view the version and build number of the app in the package properties.
- If Kaspersky Endpoint Security for Android was installed through Google Play (see section “Installing via Kaspersky Security Center” on page 31), you can view the build number in the app settings (≡ → Settings → Additional → About the app).

Upgrading the previous version of Kaspersky Endpoint Security for Android

Kaspersky Endpoint Security for Android can be updated in the following ways:

- Using Google Play. The mobile device user downloads the new version of the app from Google Play and installs it on the device.
- Using Kaspersky Security Center. You can remotely update the version of the app on the device using the Kaspersky Security Center remote administration system.

You can select the app update method that is most suitable for your organization. You can use only one update method.

Updating the app from Google Play

The app can be updated from Google Play by following the standard update procedure of the Android platform. The following conditions must be met in order for the app to be updated:

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

You can update through Google Play if Kaspersky Endpoint Security for Android was installed from Google Play. If the app was installed using another method, you cannot update through Google Play.
Updating a previous version of the application

One way to update a previous version of the application is to use Kaspersky Security Center. After applying a group policy, you can select the Kaspersky Endpoint Security for Android standalone installation package of the version that meets the corporate security requirements.

You can update through Kaspersky Security Center if Kaspersky Endpoint Security for Android was installed through Kaspersky Security Center or was installed from the Self Service Portal. If the app was installed from Google Play, you cannot update the app through Kaspersky Security Center.

To upgrade Kaspersky Endpoint Security for Android using a standalone installation package, installation of apps from unknown sources must be allowed on the user’s mobile device (Android Settings → Security → Unknown sources).

To update the version of the app:

1. In the console tree, in the Managed devices folder, select the administration group to which the Android devices belong.

2. In the workspace of the group, select the Policies tab.

3. Open the policy properties window by double-clicking.

4. In the policy Properties window, select the Additional section.

5. In the Upgrading Kaspersky Endpoint Security for Android section, click the Select button.

   This opens the Upgrading Kaspersky Endpoint Security for Android window.

6. In the list of Kaspersky Endpoint Security standalone installation packages, select the package whose version meets the corporate security requirements.

   You can upgrade Kaspersky Endpoint Security only to a more recent application version. Kaspersky Endpoint Security cannot be upgraded to an older application version.

7. Click OK.

   A description of the selected standalone installation package is displayed in the Upgrading Kaspersky Endpoint Security for Android section.

8. Click the Apply button to save the changes you have made.

Mobile device settings are configured after the next device synchronization with the Kaspersky Security Center. The mobile device user is prompted to install the new version of the app. After the user gives consent, the new app version is installed on the mobile device.
Upgrading the previous version of Kaspersky Safe Browser

The user can upgrade Kaspersky Safe Browser on his or her mobile device using the standard method for the relevant operating system. The user uses a personal Apple ID to update the app.

For detailed information on upgrading the app, please refer to the User Guide for Kaspersky Safe Browser.

Upgrading previous versions of administration plug-ins

To upgrade the administration plug-ins of Kaspersky Endpoint Security and Kaspersky Device Management for iOS, you need to download the latest version of the application from the Kaspersky Security for Mobile page (http://www.kaspersky.com/business-security/mobile#tab=frame-1) and run the Installation Wizard for each of the plug-ins (see section "Distribution kit" on page 17). Previous versions of plug-ins are removed automatically during operation of the Installation Wizard.

When administration plug-ins are updated, the existing administration groups in the Managed devices folder and rules for the automatic allocation of devices from the Unassigned devices folder to these groups are saved. The existing group policies for mobile devices are also saved. New policy settings that implement the new functions of the Kaspersky Security for Mobile integrated solution will be added to the existing policies and will have the default values.
Uninstalling the application

This section contains step-by-step instructions on removing Kaspersky Security for Mobile.

In this section

<table>
<thead>
<tr>
<th>Removal of Kaspersky Endpoint Security for Android</th>
<th>Removing Kaspersky Safe Browser</th>
</tr>
</thead>
<tbody>
<tr>
<td>........................................................................</td>
<td>................................</td>
</tr>
</tbody>
</table>

Removal of Kaspersky Endpoint Security for Android

Kaspersky Endpoint Security for Android can be removed in the following ways:

1. App removal by the user.
   The user removes Kaspersky Endpoint Security for Android manually using the app interface. In order for users to be able to remove the app, app removal should be allowed in the policy applied to the device.

2. App removal by the administrator.
   The administrator removes the app remotely using the Administration Console of Kaspersky Security Center. The app can be removed from a separate device or from several devices at once.

In this section

<table>
<thead>
<tr>
<th>Remote app removal</th>
<th>Permitting users to remove the app</th>
<th>App removal by the user</th>
</tr>
</thead>
<tbody>
<tr>
<td>..........................................................</td>
<td>.......................................</td>
<td>................................</td>
</tr>
</tbody>
</table>

Remote app removal

You can remove Kaspersky Endpoint Security for Android from users’ mobile devices remotely in the following ways:

- Using a group policy. This method is convenient if you want to remove the app from several devices at once.
- By configuring local app settings. This method is convenient if you want to remove the app from a separate device.
To remove the app by applying a group policy:

1. In the console tree, in the Managed devices folder, select the administration group to which the Android devices belong.
2. In the workspace of the group, select the Policies tab.
3. Open the policy properties window by double-clicking.
4. In the policy Properties window, select the Additional section.
5. In the Removal of Kaspersky Endpoint Security for Android section, select the Remove Kaspersky Endpoint Security for Android from device check box.
6. Click the Apply button to save the changes you have made.

As a result, Kaspersky Endpoint Security for Android is removed from mobile devices after synchronization with the Administration Server. Users of mobile devices receive a notification that the app has been removed.

To remove the app by configuring local settings:

1. In the console tree, select Mobile Device Management → Mobile devices.
2. In the list of devices, select the device on which you want to remove the app.
3. Open the device properties window double-clicking.
5. Open the Kaspersky Endpoint Security properties window by double-clicking.
6. Select the Additional section.
7. In the Uninstall the Kaspersky Endpoint Security for Android app section, select the Remove Kaspersky Endpoint Security for Android from device check box.
8. Click the Apply button to save the changes you have made.

As a result, Kaspersky Endpoint Security for Android is removed from mobile device after synchronization with the Administration Server. The mobile device user receives a notification that the app has been removed.

Permitting users to remove the app

To protect the app from removal on devices running Android 7.0 or later, Kaspersky Endpoint Security for Android must be set as an Accessibility feature. When the Initial Configuration Wizard is running, Kaspersky Endpoint Security for Android prompts the user to grant the application all required permissions. The user can skip these steps or disable these permissions in the device settings at a later time. If this is the case, the app is not protected from removal.
You can allow users to remove Kaspersky Endpoint Security for Android from their mobile devices in the following ways:

- Using a group policy. This method is convenient if you want to allow users to remove the app from several devices at once.
- Using local app settings. This method is convenient if you want to allow the user of a separate device to remove the app.

**To allow removal of the app in a group policy:**

1. In the console tree, in the Managed devices folder, select the administration group to which the Android devices belong.
2. In the workspace of the group, select the Policies tab.
3. Open the policy properties window by double-clicking.
4. In the policy Properties window, select the Additional section.
6. Click the Apply button to save the changes you have made.

As a result, removal of the app by users is allowed on mobile devices after synchronization with the Administration Server. The app removal button becomes available in the Kaspersky Endpoint Security for Android settings.

**To allow removal of the app in the local app settings:**

1. In the console tree, select Additional → Mobile Device Management → Mobile devices.
2. In the list of devices, select the device from which you want to allow app removal by the user.
3. Open the device properties window double-clicking.
5. Open the Kaspersky Endpoint Security properties window by double-clicking.
6. Select the Additional section.
8. Click the Apply button to save the changes you have made.

As a result, removal of the app by the user is allowed on the mobile device after synchronization with the Administration Server. The app removal button becomes available in the Kaspersky Endpoint Security for Android settings.
App removal by the user

To independently remove Kaspersky Endpoint Security for Android from a mobile device, the user must do the following:

1. In the main window of Kaspersky Endpoint Security for Android, tap → Uninstall the app.
   
   A confirmation prompt appears on the screen.
   
   If the Remove app button is missing, this means that the administrator enabled protection against removal of Kaspersky Endpoint Security for Android.


   The Kaspersky Endpoint Security for Android app will be removed from the user’s mobile device.

Removing Kaspersky Safe Browser

The user can remove Kaspersky Safe Browser from his or her mobile device using the standard acceptable method for the relevant operating system.

See the User Guide for Kaspersky Safe Browser for details on how to remove the app.
Contacting the Technical Support service

This section describes the ways to get technical support and the terms on which it is available.

In this section

- How to get technical support .......................................................... 73
- Technical support by phone ............................................................ 73
- Technical Support via Kaspersky CompanyAccount ........................................ 74

How to get technical support

If you could not find a solution to your problem in the documentation or in one of the sources of information about the application (see the section "Sources of information about the application" on page 9), we recommend that you contact Technical Support. Technical Support specialists will answer your questions about installing and using the application.

Before contacting Technical Support, please read the support rules (https://support.kaspersky.com/support/rules).

You can contact Technical Support in one of the following ways:

- By calling Technical Support (https://support.kaspersky.com/b2c).
- By sending a request to Kaspersky Lab Technical Support through the Kaspersky CompanyAccount portal (https://companyaccount.kaspersky.com).

Technical support by phone

You can call Technical Support representatives in most regions of the world. You can find information on ways to receive technical support in your region and contacts for Technical Support on the website of Kaspersky Lab Technical Support (https://support.kaspersky.com/b2c).

Before contacting Technical Support, please read the support rules (https://support.kaspersky.com/support/rules).
Technical Support via Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) is a portal for organizations that use Kaspersky Lab applications. The Kaspersky CompanyAccount portal is designed to facilitate interaction between users and Kaspersky Lab experts through online requests. Kaspersky CompanyAccount lets you monitor the progress of electronic request processing by Kaspersky Lab experts and store a history of electronic requests.

You can register all of your organization's employees under a single account on Kaspersky CompanyAccount. A single account lets you centrally manage electronic requests from registered employees to Kaspersky Lab and also manage the privileges of these employees via Kaspersky CompanyAccount.

The Kaspersky CompanyAccount portal is available in the following languages:

- English
- Spanish
- Italian
- German
- Polish
- Portuguese
- Russian
- French
- Japanese

To learn more about Kaspersky CompanyAccount, please visit the Technical Support website (https://support.kaspersky.com/faq/companyaccount_help).
Glossary

A

Administrator’s workstation
The computer hosting the Administration Console of Kaspersky Security Center. If the application administration plug-in is installed on the administrator’s workstation, the administrator can manage Kaspersky Endpoint Security mobile apps deployed on user devices.

Administration group
A set of managed devices, such as mobile devices grouped according to the functions they perform and the set of apps installed on them. Managed devices are grouped so that they can be managed as a single whole. For example, mobile devices running the same operating system can be combined into an administration group. A group may include other administration groups. It is possible to create group policies and group tasks for group devices.

Administration Server
A component of Kaspersky Security Center that centrally stores information about all Kaspersky Lab applications that are installed within the corporate network. It can also be used to manage these applications.

Apple Push Notification service (APNs) certificate
A certificate signed by Apple that lets you use the functionality of the Apple Push Notification service. An iOS MDM Server can use the Apple Push Notification service to manage iOS devices.

Application administration plug-in
A dedicated component that provides the interface for managing Kaspersky Lab applications through Administration Console. Each application that can be managed through Kaspersky Security Center SPE has its own administration plug-in. The administration plug-in is included in all Kaspersky Lab applications that can be managed via Kaspersky Security Center.

C

Certificate Signing Request
A file with Administration Server settings that, once confirmed by Kaspersky Lab, is sent to Apple for purposes of getting the APNs certificate.
Container
A special-purpose shell for mobile apps that makes it possible to control the activity of a containerized app. A container protects personal and corporate data on the mobile device. A container used on an iOS device is signed by the same certificate that is used to sign Kaspersky Safe Browser for iOS devices.

Device administrator
A set of app rights on an Android device that enables the app to use device management policies. It is necessary to implement full functionality of Kaspersky Endpoint Security on Android devices.

EAS device
A mobile device connected to Administration Server via Exchange ActiveSync protocol.

Exchange Server
A Kaspersky Endpoint Security component that makes it possible to connect Exchange ActiveSync mobile devices to the Administration Server. It is installed on the client device.

Group task
A task intended for an administration group and performed on all managed devices included in the group.

Installation package
A set of files created for remote installation of a Kaspersky Lab application by using the remote administration system. The installation package is created from special files included in the app distribution package. The installation package contains a range of settings needed to install the app and get it running immediately after installation. The values of settings in the distribution kit correspond to default values of application settings.

iOS MDM device
An iOS mobile device controlled by the iOS MDM Server.
iOS MDM mobile device server
A component of the Kaspersky Security Center administration system that makes it possible to connect iOS mobile devices to the Administration Server and control them using iOS MDM profiles.

iOS MDM profile
A profile that contains a set of settings for connecting iOS mobile devices to the Administration Server. An iOS MDM profile makes it possible to distribute iOS configuration profiles in background mode using the iOS MDM Server, and also receive extended diagnostic information about mobile devices. A link to the iOS MDM profile needs to be sent to a user in order to enable the iOS MDM Server to discover and connect the user’s iOS mobile device.

K
Kaspersky Security Center Web Server
A component of Kaspersky Security Center that is installed with Administration Server. The web server is intended for transferring standalone installation packages, iOS MDM profiles, and files from the shared folder over the network.

Kaspersky Security Network (KSN)
An infrastructure of cloud services that provides access to the online Knowledge Base of Kaspersky Lab which contains information about the reputation of files, web resources, and software. The use of data from Kaspersky Security Network ensures faster responses by Kaspersky Lab applications to threats, improves the performance of some protection components, and reduces the likelihood of false alarms.

Kaspersky SMS Broadcasting utility
A utility for sending text messages to Android devices of users. This utility is installed on the administrator’s Android device.

M
Manifest file
A file in PLIST format containing a link to the app file (ipa file) located on a web server. It is used by iOS devices to locate, download, and install apps from a web server.
P

Packages of mobile apps
An installation file for the Android operating system (file with the .apk extension) uploaded to the Administration Server. Mobile app packages are stored on the Kaspersky Security Center web server or in the public folder of the Kaspersky Security Center administrator. Mobile app packages can be created for apps of third-party publishers. When creating a mobile app package, one can specify that the app will be containerized.

Policy
A set of settings of the application and Kaspersky Endpoint Security mobile apps applied to devices in administration groups or to individual devices. Different policies can be applied to different administration groups. A policy includes the configured settings of all functions of Kaspersky Endpoint Security mobile apps.

Provisioning profile
A set of parameters that apps need to work on iOS mobile devices. A provisioning profile includes license information and is linked to a specific app.

S

Standalone installation package
An installation file of Kaspersky Endpoint Security for the Android operating system, which contains the settings of application connection to the Administration Server. It is created on the basis of the installation package of this application and is a particular case of mobile app package.
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 38 offices in 33 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 signatures of these threats 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, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, 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 website: [https://www.kaspersky.com](https://www.kaspersky.com)

Virus encyclopedia: [https://securelist.com/](https://securelist.com/)

Virus Lab: [https://virusdesk.kaspersky.com/](https://virusdesk.kaspersky.com/) (for scanning suspicious files and websites)

Kaspersky Lab’s web forum: [https://forum.kaspersky.com](https://forum.kaspersky.com)
Information about third-party code

Information about third-party code is contained in the legal_notices.txt file located in the installation folder of the Kaspersky Security for Mobile integrated solution.

On Android devices, information about third-party code is available in the Kaspersky Endpoint Security for Android app by clicking the → About the app button.

On iOS devices, information about third-party code is available in the settings of Kaspersky Safe Browser in the About the app section.
Trademark notifications

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

Apple, App Store, Keychain, iPhone, iPad, Mac OS, OS X, and Safari are trademarks of Apple Inc., registered in the USA and elsewhere.

IOS is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the United States and other countries.

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

Active Directory, ActiveSync, Microsoft, Windows, Windows Phone are trademarks owned by Microsoft Corporation and registered in the United States of America and elsewhere.

ARM is a trademark or registered trademark of ARM Ltd. or its subsidiaries.

The BlackBerry trademark is owned by Research In Motion Limited and is registered in the United States and may be pending or registered in other countries.

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

SAMSUNG is a trademark of SAMSUNG in the United States and elsewhere.

Symbian is a trademark owned by Symbian Foundation Ltd.

Intel and Atom are trademarks of Intel Corporation in the U.S. and/or other countries.
Index

A
Activating the application................................................................. 67
Administration Console....................................................................... 32
Administration plug-in........................................................................ 22
App Store............................................................................................... 52, 73

C
Certificate
  general................................................................................................... 34

G
Google Play............................................................................................ 39

M
Mobile device administration plug-in.................................................. 22

S
Standalone installation package.......................................................... 48
Standalone package
  creating ............................................................................................ 48
Synchronization.................................................................................... 49