



Kaspersky Security Center 10

Web Console

User Guide

Dear User,

Thank you for your trust! We hope that this document will help you in your work and will provide answers regarding this software product.

Warning! This document is the property of Kaspersky Lab: All rights to this document are protected 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, is allowed only with the written permission of Kaspersky Lab.

This document, and graphic images related to it, may only be used for informational, non-commercial, and personal purposes.

This document may be amended without additional notification.

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

Document revision date: 12/7/2016

© 2017 AO Kaspersky Lab. All Rights Reserved.

<http://www.kaspersky.com>

<https://help.kaspersky.com>

<http://support.kaspersky.com>

Table of Contents

About this Guide.....	6
In this document.....	6
Document conventions	9
Kaspersky Security Center 10 Web Console.....	11
Software requirements.....	14
Application interface.....	15
Connect to Administration Server.....	17
Preparing to connect to Administration Server	17
Connecting to Administration Server	18
Network protection status	20
Viewing information about the statuses of devices	21
Viewing information about the protection status on devices	23
Viewing information about the status of security application databases	25
Manage devices	27
Managed devices and administration groups	27
Viewing a list of devices	28
Viewing device properties.....	30
Installing applications on networked devices	34
About installing applications	34
About installation packages.....	35
Remote installation of applications.....	36
Local installation mode	40
Publishing installation packages	41
Viewing the list of published installation packages	42
Canceling installation package publishing.....	43
Installing an app using a published installation package	44
Adding Android app files and app links from Google Play to the corporate Application Shop.....	45
Viewing the Application Shop	47
Editing the settings of an app and removing an app from the Application Shop ...	47


Installing apps from the Application Shop	49
Managing policies	50
Viewing a list of policies	51
Adding a policy.....	52
Managing policy profiles	54
About the policy profile	54
Adding a policy profile	56
Modifying a policy profile.....	57
Activating a policy	58
Modifying a policy	59
Applying an out-of-office policy	60
Deleting a policy.....	60
Managing mobile devices using an MDM policy.....	61
About the MDM policy	61
Configuring an MDM policy.....	63
Managing user accounts	66
Viewing the list of accounts	67
Filtering the list of user accounts.....	68
Viewing the user's details	69
Viewing the list of a user's mobile devices.....	70
Mobile Device Management	72
Viewing the list of mobile devices	73
Viewing mobile device settings	74
Viewing information about the owner of a mobile device	74
Commands for mobile device management	75
Sending commands to a mobile device	78
Viewing the commands log.....	78
Removing a mobile device from the list	79
Managing tasks	80
Viewing a list of tasks	80
Starting and stopping a task manually	82
Viewing task run results.....	82
Deleting tasks.....	83

Working with reports	84
About reports.....	84
Actions on reports	85
Viewing reports	86
Exporting reports.....	87
Configuring report delivery	88
Changing your account password	89
Exiting Kaspersky Security Center 10 Web Console.....	90
Glossary.....	91
AO Kaspersky Lab	97
Information about third-party code.....	99
Trademark notices	100
Index	101

About this Guide

This document provides information about Kaspersky Security Center 10 Web Console and instructions on proper use of the application.

This document is aimed at technical specialists (administrators) in organizations where a security system built on Kaspersky Lab solutions is used as a service (provided by a network protection service provider).

If you have any questions on how to use Kaspersky Security Center 10 Web Console, you can find answers in this User Guide and in the integrated Help system. To use Help for Kaspersky Security Center 10 Web Console, open the main application window and click the  icon.

In this section:

In this document	6
Document conventions	9

In this document

This document consists of sections with descriptions of features and instructions, glossary and index.

Kaspersky Security Center 10 Web Console (see page [11](#))

This section contains general information about Kaspersky Security Center 10 Web Console, its purpose, and its architecture.

Software requirements (see page [14](#))

This section lists the software that must be installed before you start using the application.

Application interface (see page [15](#))

This section describes the purpose of tabs and other interface elements located on the pages of the Kaspersky Security Center 10 Web Console web portal.

Connecting to Administration Server (see page [17](#))

This section provides instructions on how to get prepared for connection and how to connect to Administration Server using Kaspersky Security Center 10 Web Console.

Network protection status (see page [20](#))

This section provides instructions on how to find information on the status of the protection system covering networked devices that are managed by the Administration Server to which the application is connected.

Manage devices (see page [27](#))

This section provides information on how to view lists of devices in your network and their respective properties.

Installing applications on networked devices (see page [34](#))

This section provides instructions on how to install Kaspersky Lab applications and third-party applications on devices in your network in remote and local installation modes.

Managing policies (see page [50](#))

This section provides information about how to manage policies created for devices in your network.

Managing user accounts (see page [66](#))

This section provides information about how to manage accounts created for users on your network.

Mobile Device Management (see page [72](#))

This section provides information about how to manage mobile devices connected to Administration Server.

Managing tasks (see page [80](#))

This section provides information about how to manage tasks created for devices in your network.

Managing reports (see page [84](#))

This section provides instructions on how to view, print, and send by email reports of Administration Server to which the application has been connected, and how to save report data to a file.

Changing your account password (see page [89](#))

This section provides instructions on how to set a new password for your account.

Exiting Kaspersky Security Center 10 Web Console (see page [90](#))

This section provides instructions on how to exit the application.

Glossary

This section explains terms used in this document.

AO Kaspersky Lab (see page [97](#))

This section provides information about AO Kaspersky Lab.

Information about third-party code (see page [99](#))

This section provides information about the third-party code used in the application.

Trademark notices (see page [100](#))

This section provides information about trademarks used in the document and their respective owners.

Index

This section helps you find necessary data quickly.

Document conventions

Document conventions are used herein (see the table below).

Table 1. Document conventions

Sample text	Document conventions description
Note that...	Warnings are highlighted with red color and boxed. Warnings contain information about actions that may lead to some unwanted outcome.
We recommend that you use...	Notes are boxed. Notes contain additional and reference information.
Example: ...	Examples are given on a blue background under the heading "Example".
<i>Update</i> means... The <i>Databases are out of date</i> event occurs.	The following elements are italicized in the text: <ul style="list-style-type: none"> • New terms. • Names of application statuses and events.
Press ENTER . Press ALT+F4 .	Names of keyboard keys appear in bold and are capitalized. Names of keys that are connected by a + (plus) sign indicate the use of a key combination. Those keys must be pressed simultaneously.
Click the Enable button.	Names of application interface elements, such as entry fields, menu items, and buttons, are set off in bold.

Sample text	Document conventions description
<p>► <i>To configure task schedule:</i></p>	<p>Introductory phrases of instructions are italicized and accompanied by the arrow sign.</p>
<p>Enter <code>help</code> in the command line</p> <p>The following message then appears:</p> <pre>Specify the date in MM:DD:YY format.</pre>	<p>The following types of text content are set off with a special font:</p> <ul style="list-style-type: none"> • text in the command line; • text of messages displayed on the screen by the application; • data that the user have to enter from the keyboard.
<p><User name></p>	<p>Variables are enclosed in angle brackets. Instead of a variable, the corresponding value must be inserted, with angle brackets omitted.</p>

Kaspersky Security Center 10 Web Console

Kaspersky Security Center 10 Web Console is a web application designed to manage the status of the security system of an organization's network protected by Kaspersky Lab applications.

Using the application, you can do the following:

- Manage the status of your organization's security system (see page [20](#)).
- Install Kaspersky Lab applications on your networked devices and manage installed applications (see page [34](#)).
- Manage policies created for your networked devices (see page [50](#)).
- Manage user accounts (see page [66](#)).
- Manage mobile devices connected to the organization's server (see page [72](#)).
- Manage tasks for applications installed on your networked devices (see page [80](#)).
- View reports on the security system status (see page [84](#)).
- Manage the delivery of reports to interested parties: system administrators and other IT experts (see page [84](#)).

Kaspersky Security Center 10 Web Console runs on the side of the service provider that provides protection to your network. The protection service provider is responsible for application installation and maintenance. You do not have to install and run Kaspersky Security Center 10 Web Console on your device to use it. All you need is a browser (see section "Software requirements" on page [14](#)).

The figure below shows how Kaspersky Security Center 10 Web Console works.

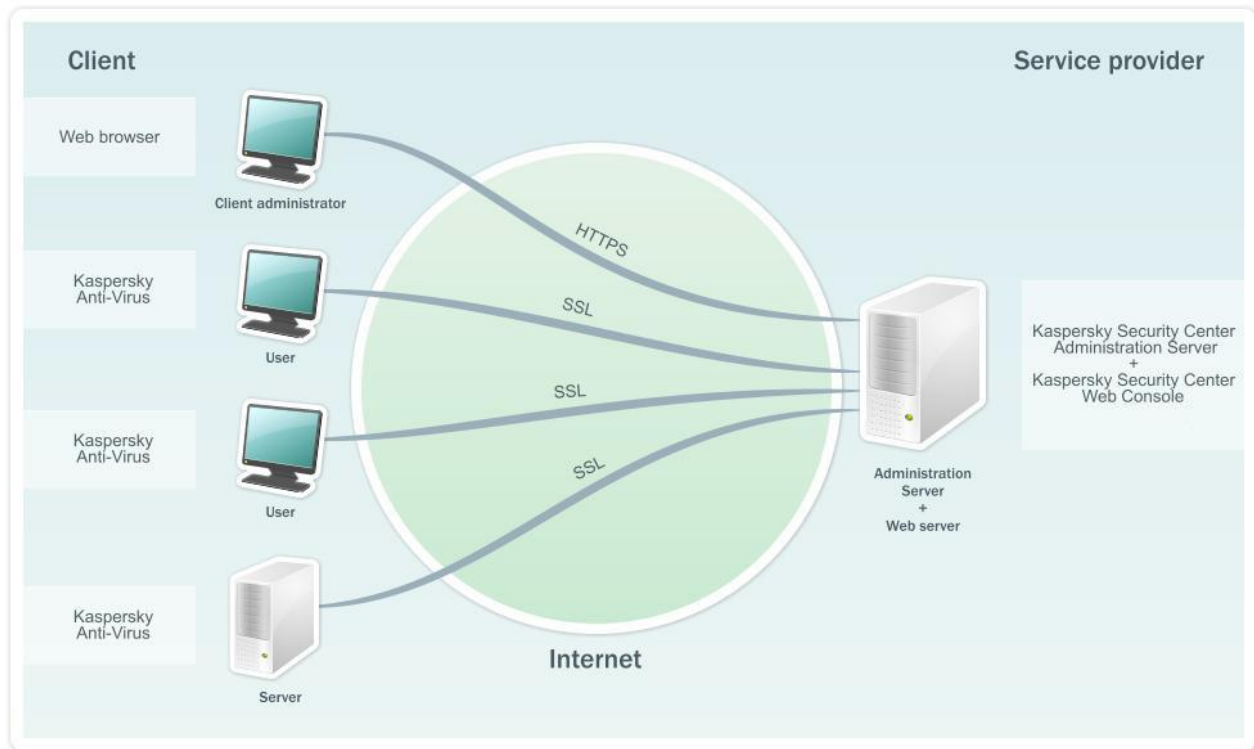


Figure 1. Operating layout

Kaspersky Security Center 10 Web Console interacts with Kaspersky Security Center Administration Server, which is located at the protection service provider. Administration Server is an application designed for managing Kaspersky Lab applications installed on devices in your network. Administration Server connects to devices in your network over channels protected with Secure Socket Layer (SSL).

Kaspersky Security Center 10 Web Console provides a web interface that ensures interaction between your computer and Administration Server over a browser. When you connect to Kaspersky Security Center 10 Web Console using your browser, the latter establishes an encrypted (HTTPS) connection with Kaspersky Security Center 10 Web Console.

Kaspersky Security Center 10 Web Console operates as follows:

1. Use a browser to connect to Kaspersky Security Center 10 Web Console, where the pages of the application web portal are displayed.
2. Use web portal controls to choose a command that you want to run. Kaspersky Security Center 10 Web Console performs the following operations:
 - If you select a command used for receiving information (for example, to view a list of devices), Kaspersky Security Center 10 Web Console generates a request for information to Administration Server, receives the necessary data, and sends it to the browser in an easy-to-view format.
 - If you have chosen a command used for management (for example, remote installation of an application), Kaspersky Security Center 10 Web Console receives the command from the browser and sends it to Administration Server. Then the application receives the result from Administration Server and sends it to the browser in an easy-to-view format.

Software requirements

Use of Kaspersky Security Center 10 Web Console only requires a browser.

The hardware and software requirements to the device are identical to the requirements of the browser used with Kaspersky Security Center 10 Web Console.

Kaspersky Security Center 10 Web Console supports the following browsers:

- Internet Explorer®9 or later.
- Microsoft® Edge.
- Chrome™ 53 and later.
- Firefox™ 47 and later.
- Safari® 8 under Mac OS X® 10.10 (Yosemite).
- Safari 9 under Mac OS X 10.11 (El Capitan).

You can obtain information about the latest version of the hardware and software requirements from the Technical Support Service website on the application page of Kaspersky Security Center 10 Web Console in the System requirements section (<http://support.kaspersky.com/ksc10#requirements>).

Application interface

After you have established a connection to Administration Server, the main window of Kaspersky Security Center 10 Web Console opens in the browser (see the figure below).

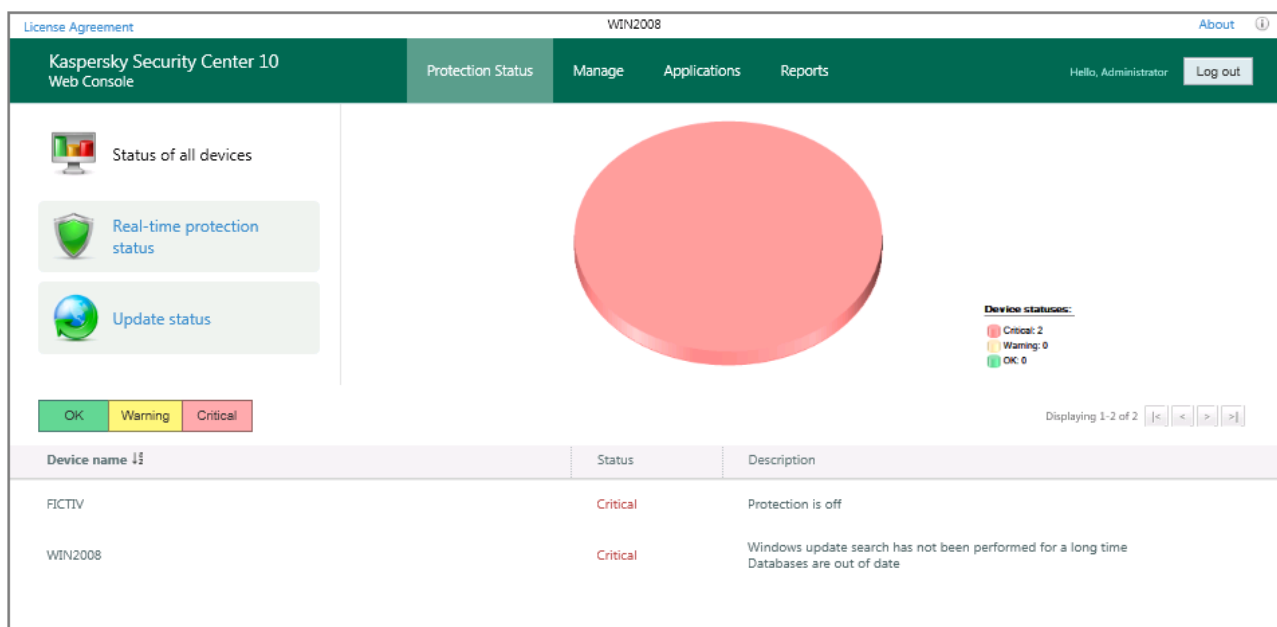


Figure 2. Main application window

The upper part of the main window contains the following interface elements:

- **Protection Status, Manage, Applications, and Reports** tabs provide access the main features of the application.
- Icon ⓘ – to get context-sensitive help.
- The **Change password** link changes the password of the user account.
- The **Log out** button exits the application.
- The **License Agreement** link takes you to the page with the License Agreement.
- The **Frequently Asked Questions** link takes you to the page with the frequently asked questions (FAQ).
- The **About** link takes you to the application info page.

Links can be modified by the service provider's administrator. Some links may be missing.

The informational area is the principal part of the main application window. The contents of the informational area vary according to the tab that is selected:

- **Protection status.** Provides information about the protection status of networked devices. In the upper part of the tab, you can select one of the following sections: **Status of all devices**, **Real-time protection status**, or **Update status**. After you select a section, a chart appears on the right showing statistics, while the bottom part of the tab displays a list with information about the statuses of devices.
- **Manage.** Designed for obtaining information about administration groups and devices, as well as policies and tasks created for them. The informational area of the tab is divided into two parts. The menu contains administration groups. The right part of the informational area contains three second-level tabs: **Policies**, **Tasks**, and **Devices**.
- **Applications.** Intended for publishing installation packages.
- **Reports.** Designed for viewing reports. The informational area of the tab is divided into two parts. The menu contains reports. The results pane displays the content of a selected report.

See also:

Connecting to Administration Server	17
Network protection status	20
Manage devices	27
Working with reports	84
Exiting Kaspersky Security Center 10 Web Console	90
Changing your account password	89

Connect to Administration Server

This section provides instructions on how to get prepared for connection and how to connect to Administration Server using Kaspersky Security Center 10 Web Console.

In this section:

Preparing to connect to Administration Server	17
Connecting to Administration Server	18

Preparing to connect to Administration Server

Before connecting to the Administration Server, you must perform the following preliminary actions: Prepare your browser for work and get the data required to establish the connection (an address to connect to the Administration Server and user account credentials: user name and password).

Preparing the browser

Before connecting to the Administration Server, make sure the following components are supported by your browser:

- JavaScript.
- Cookies.

If support of these components is disabled, enable it. You can find information in the browser Help about how to enable support of JavaScript and cookies in your browser.

Receiving data for the connection

To connect to Administration Server, you must have the following data:

- Web portal address in the form `https://<Domain_name>:<Port>`
- User name.
- Password.

You can get this information from the administrator of your service provider.

Connecting to Administration Server

► *To connect to Administration Server:*

1. Start the browser.
2. In the Address bar of the browser, enter the web portal address that you received from the service provider administrator (see section "Preparing to connect to Administration Server" on page [17](#)). Open this URL.

If you are connecting to Administration Server for the first time, the **License Agreement** window opens in the browser. If you have connected to Administration Server earlier, a window for entering the user name and password opens in the browser.

3. If you are connecting to Administration Server for the first time, perform the following operations in the **License Agreement** window:
 - a. Read through the License Agreement. If you accept all of its terms, select the **I accept the terms of the License Agreement** check box.
 - b. Click the **Continue** button.

In the browser a window opens, prompting you to enter your user name and password.

4. In the **User name** text box enter your account name.
5. In the **Password** text box, enter the password of your account.
6. In the **Administration Server** field enter the name of Administration Server to which you want to connect. Click the **Sign in** button.

The main application window opens (see section "Application interface" on page [15](#)).

If you have an error returned after attempting to connect to Administration Server, contact the service provider administrator to solve the issue.

Network protection status

Kaspersky Security Center 10 Web Console allows you to receive information about the status of the protection system covering networked devices that are managed by the Administration Server.

You can receive the following information about the status of your networked devices:

- Status of all devices—information about the status of devices in your network.

A device can have any of the three statuses:

- *OK*—The device is protected.
- *Warning*—The level of device protection has been reduced.
- *Critical*—The level of device protection has been reduced significantly.

The Administration Server assigns a status to the device on the basis of the condition of its protection. The *Warning* or *Critical* status is assigned if there are factors that lower the protection level of the device (such as inactivity of the security application, outdated databases, or a large number of objects that failed to be disinfected). The list of factors for *Warning* and *Critical* statuses is created by the service provider's administrator.

- The real-time protection status provides information about the status of the corresponding security application component in Kaspersky Lab applications installed on devices in your network.
- The update status provides information about the up-to-date status of the security application databases on devices in your network.

In this section:

Viewing information about the statuses of devices.....	21
Viewing information about the protection status on devices.....	23
Viewing information about the status of security application databases	25

Viewing information about the statuses of devices

► To view information about the status of your networked devices:

1. Open the main application window (see section "Application interface" on page [15](#)).
2. Select the **Protection status** tab.

The main application window displays the contents of the **Status of all devices** section (see figure below).

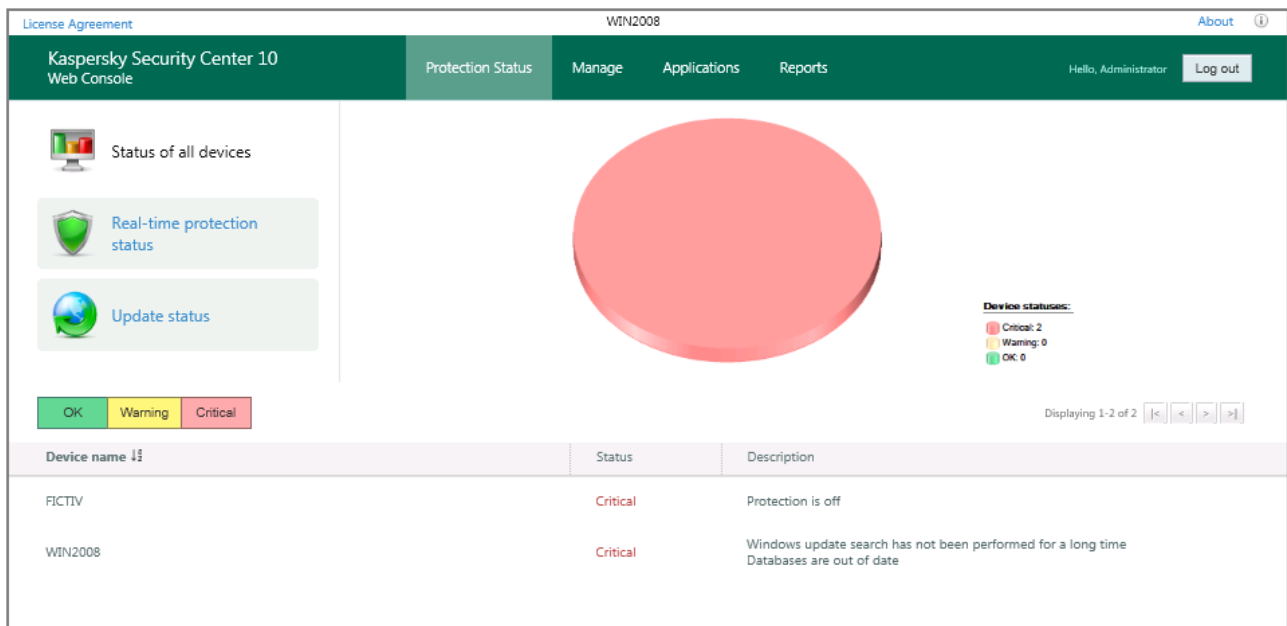




Figure 3. Status of all devices

The results pane displays a pie chart. It shows the number and percentage of devices with the *Critical*, *Warning*, and *OK* statuses, respectively.

The lower part of the section contains a list of devices. The list contains the following information about devices:

- **Device name.** Network name of the device.
- **Status** (*OK*, *Warning*, *Critical*). Information about the status of the device.
- **Description.** Messages that explain the causes of degraded security levels on devices with the *Warning* and *Critical* statuses (such as *Real-time protection is paused* or *The update task has not been started in more than 3 days*).

To view information about a specific device, use the following interface elements to locate that device in the list:

- The **Critical** button displays devices with the *Critical* status.
- The **Warning** button displays devices with the *Warning* status.
- The **OK** button displays devices with the *OK* status.
-  take you to the next/previous, first/last page of the list of devices.
-  sorts device names in the list of devices in ascending or descending order.

You can open the window with information about the properties of a device by clicking the string with the name of that device.

See also:

Managed devices and administration groups	27
Viewing the list of devices	28
Viewing the properties of a device	30

Viewing information about the protection status on devices

- To view information about the protection status of your networked devices:
1. Open the main application window (see section "Application interface" on page [15](#)).
 2. Select the **Protection status** tab.
 3. In the left part of the window, select the **Real-time protection status** section (see the figure below).

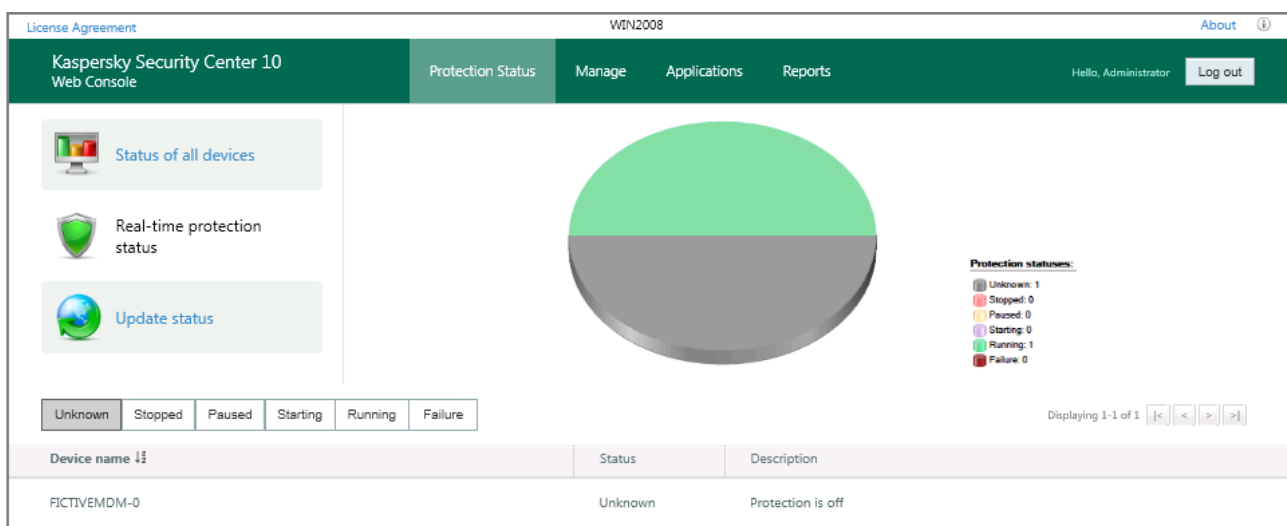


Figure 4. Real-time protection status

The results pane displays a pie chart. It contains information about the status of the protection component in applications installed on your networked devices.

The chart displays the number and the percentage of devices on which the protection component has the following statuses, respectively:



- *Unknown.*
- *Stopped.*
- *Paused.*
- *Starting.*

- *Running*.
- *Failure*.

The lower part of the section contains a list of devices. The list of devices provides the following details:

- **Device name.** Network name of the device.
- **Status** (*OK*, *Warning*, *Critical*). Information about the status of the device.
- **Description.** Messages that explain the causes of degraded security levels on devices with the *Warning* and *Critical* statuses (such as *Number of non-disinfected objects is too large* or *License term expired*).

To view information about a specific device, use the following interface elements to locate that device in the list:

- The **Unknown** button displays devices with the *Unknown* protection status.
- The **Stopped** button displays devices with the *Stopped* protection status.
- The **Paused** button displays devices with the *Paused* protection status.
- The **Starting** button displays devices with the *Starting* protection status.
- The **Running** button displays devices with the *Running* protection status.
- The **Failure** button displays devices with the *Failure* protection status.
-  take you to the next/previous, first/last page of the list of devices.
-  sorts device names on the list of devices in alphabetical order.

You can open the window with information about the properties of a device by clicking the string with the name of that device.

See also:

Managed devices and administration groups	27
Viewing the properties of a device	30

Viewing information about the status of security application databases

- ▶ To view information about the protection status of your networked devices:
 1. Open the main application window (see section "Application interface" on page [15](#)).
 2. Select the **Protection status** tab.
 3. In the left part of the window, select the **Update status** section (see the figure below).

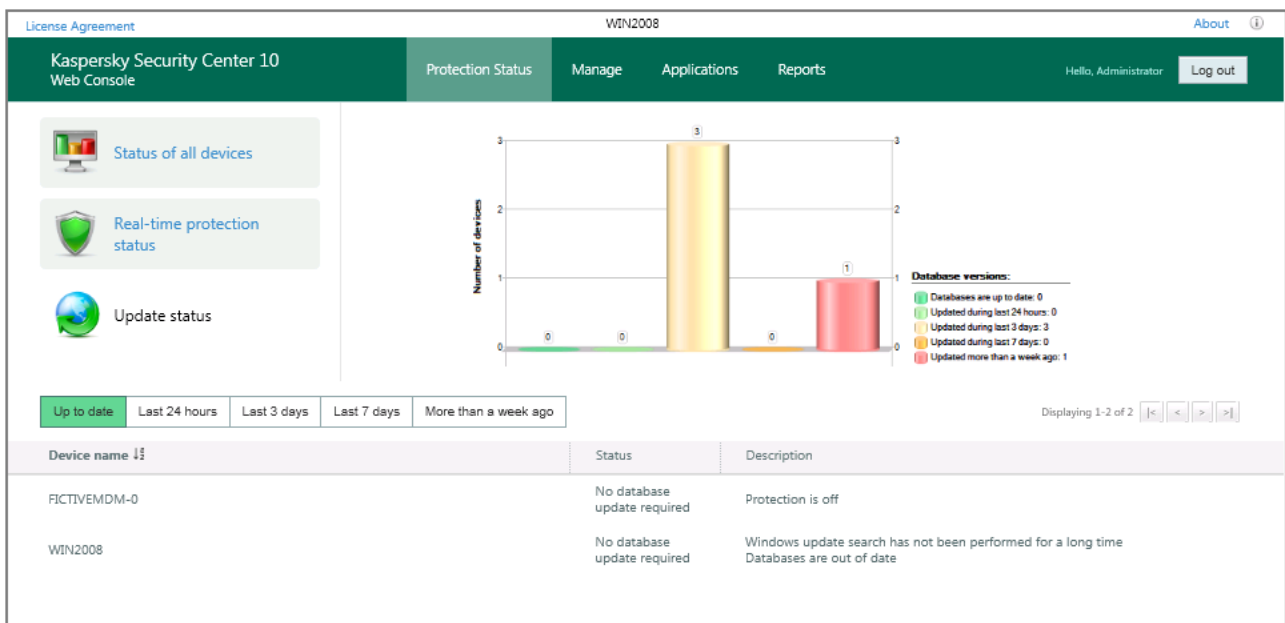


Figure 5. Update status

The upper part of the section displays a bar chart. It provides information about the status of the security application databases on your networked devices.

The chart displays the number of devices on which the security application databases have the following statuses:

- *Up to date*—Databases are up to date.
- *Last 24 hours*—Databases were updated within the last 24 hours.
- *Last 3 days*—Databases were updated within the last 3 days.

- *Last 7 days*—Databases were updated within the last 7 days.
- *More than a week ago* – Databases were updated more than a week ago.

The lower part of the section contains a list of devices. The list of devices provides the following details:

- **Device name.** Network name of the device.
- **Status** (*OK, Warning, Critical*). Information about the status of the device.
- **Description.** Messages that explain the causes of degraded security levels on devices with the *Warning* and *Critical* statuses, such as *Real-time protection is paused* or *The update task has not been started in more than 3 days*.

To view information about a specific device, use the following interface elements to locate that device in the list:

- The **Up to date** button displays devices with the *Up to date* status.
- The **Last 24 hours** button displays devices with the *Last 24 hours* status.
- The **Last 3 days** button displays devices with the *Last 3 days* status.
- The **Last 7 days** button displays devices with the *Last 7 days* status.
- The **More than a week ago** button displays devices with the *More than a week ago* status.

-  take you to the next/previous, first/last page of the list of devices.

-  sorts device names on the list in ascending or descending alphabetical order.

You can open the window with information about the properties of a device by clicking the string with the name of that device.

See also:

Managed devices and administration groups	27
Viewing the properties of a device	30

Manage devices

This section provides information about devices in your network and administration groups, as well as instructions on how to view lists and properties of devices.

In this section:

Managed devices and administration groups	27
Viewing the list of devices	28
Viewing the properties of a device	30

Managed devices and administration groups

The security status of devices in your network is managed by the Administration Server of your protection service provider.

All your networked devices with Kaspersky Lab applications installed are distributed among administration groups. Administration groups are sets of devices grouped by their functions and by Kaspersky Lab applications installed.

Devices included in an administration group are referred to as *managed devices*. After Kaspersky Lab applications are installed on devices in your network, the Administration Server automatically adds those devices to the **Managed devices** administration group. The service provider's administrator can create other administration groups and distribute devices among these groups. An administration group can contain other administration groups.

Using Kaspersky Security Center 10 Web Console, you can receive information about managed devices from the Administration Server by viewing the list of devices and the properties of managed devices.

See also:

| Installing applications on networked devices [34](#)

Viewing a list of devices

You can view lists of your networked devices managed by the Administration Server. You can also view lists of managed devices in each of the administration groups separately.

► *To view a list of devices:*

1. Open the main application window (see section "Application interface" on page [15](#)).
2. Select the **Manage** tab.
3. In the window that opens, select the **Devices** tab.
4. In the left part of the window, select the administration group in which you want to view the list of devices:
 - If you want to view the list of all managed devices, select the **Managed devices** group.
 - If you want to view the list of managed devices in some particular administration subgroup, click an administration group in the group tree located in the relevant subfolder of the **Managed devices** administration group.

The list of devices in the selected administration group is displayed on the screen (see figure below).

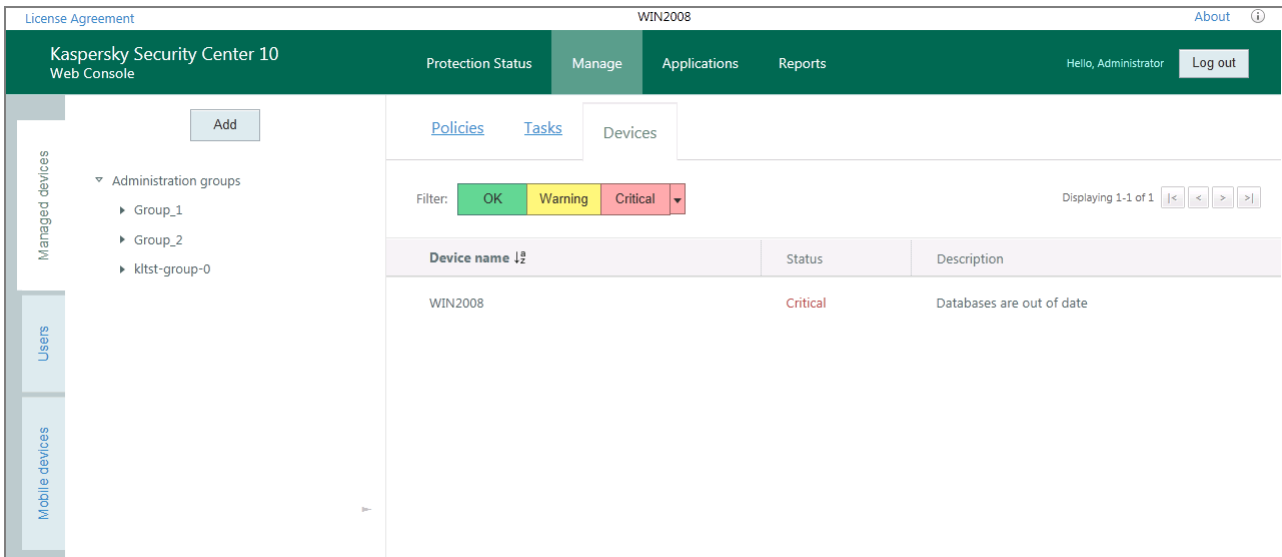




Figure 6. Viewing the list of devices

The list contains the following information about devices:

- **Device name.** Network name of the device.
- **Status.** Status of the device.
- **Description.** Messages that explain the causes of lowered security levels on devices with the *Warning* and *Critical* statuses (such as *Real-time protection paused* or *Update task has not been started in more than 3 days*).

To view information about a specific device, use the following interface elements to locate that device in the list:

- The **Critical** button displays devices with the *Critical* status.
- The **Warning** button displays devices with the *Warning* status.
- The **OK** button displays devices with the *OK* status.
-  take you to the next/previous, first/last page of the list of devices.
-  sorts device names in the list of devices in ascending or descending order.

You can open the window with information about the properties of a device by clicking the string with the name of that device.

See also:

Managed devices and administration groups	27
Network protection status	20

Viewing device properties

► To view the properties of a device:

1. Open the main application window (see section "Application interface" on page [15](#)).
2. Select the **Devices** tab.
3. In the left part of the window, in the list of administration groups, select the administration group, which contains the relevant device.

The right part of the window displays the list of devices of the selected administration group.

4. In this list, select the device whose properties you want to view, and click the string with the device name to open the window containing information about the device properties (see figure below).

The screenshot shows a window titled "Device Info" with a dark green header and a close button (X) in the top right corner. The main content area is divided into sections:

- Device Info** (light blue header):
 - Last update: 11/07/2016 12:15:09
 - Last visible time: 11/07/2016 12:15:09
 - Last connection to Server: 11/07/2016 12:15:09
 - IP address: _____
 - Connection IP address: _____
 - Domain: **FICTIV**
 - Network name: **FICTIV**
 - Domain name: **fictiv**
 - Operating system (OS): Windows NT/2000/XP/Server 2003/Vista/7/Server 2008/8/Ser...
 - Group: Managed devices
 - Real-time protection status: Unknown
- Protection is off** (red background bar)
- Applications** (light blue header):
 - Application name: _____
 - iOS Mobile Device Management** (expanded):
 - Databases version: Unknown
 - Security application version: _____
 - Viruses detected: 0
 - Last updated on: 11/07/2016 12:15:09
 - Last scanned on: Unknown
 - Real-time protection status: Unknown

Figure 7. Viewing the properties of devices

The device properties window comprises two different parts.

The upper part of the window provides information about the following properties of the device:

- **Last update.** Date of the last update of Kaspersky Lab applications or Kaspersky Lab anti-virus databases on the device.
- **Last visible time.** Date and time the device became visible in the network.
- **Last connection to Server.** Date and time the device last connected to the Administration Server.
- **IP address.** Network address of the device.
- **Connection IP address.** Network address under which the device connects to the Administration Server. For example, if you connect to Administration Server via a proxy server, the address of the proxy server is displayed.
- **Domain.** Name of the network domain in which the device is registered.
- **Network name.** Network name of the device. It is same as the device name displayed in the left part of the window.
- **Domain name.** Full domain name of the device, in <Computer_name>.<Domain_name> format.
- **Operating system (OS).** Type of the operating system installed on the device.
- **Group.** Name of the administration group to which the device belongs.
- **Real-time protection status.** Status of the device's real-time protection.
- Warnings that contain information about the causes of degraded anti-virus protection on the device, such as outdated anti-virus databases, or a large number of objects that the application failed to disinfect. Those warnings are displayed if the device status is *Warning* or *Critical*.



The lower part of the window contains the **Applications** section providing information about Kaspersky Lab applications installed on the device.

The **Applications** section is only displayed if any Kaspersky Lab applications have been installed on the device.

The **Applications** section contains the following information:

- **Application name.** Full name of the application.
- Application properties, such as the application version or the date of the last update. The list of application properties is displayed after the app name. Each application has its own set of properties.

To view the properties of an application, you can use the following interface elements:

- Icon  – opens the information section that contains the properties of an application.
- Icon  – closes the information section that contains the properties of an application.

See also:

Managed devices and administration groups	27
Viewing the list of devices	28

Installing applications on networked devices

This section provides instructions for local and remote installation of Kaspersky Lab applications and third-party applications on your networked devices.

In this section:

About installing applications	34
About installation packages	35
Remote installation of applications.....	36
Local installation mode.....	40

About installing applications

Using Kaspersky Security Center 10 Web Console, you can install Kaspersky Lab applications on your networked devices. The list of applications available for installation is created by your service provider's administrator.

There are two ways of installing an application:

- *Remote installation* (referred to as remote installation mode). Remote installation allows you to install an application on multiple networked devices at once. You can run and control remote installation through the application web portal.
- *Local installation* (referred to as local installation mode). Local installation is required, for example, in case remote installation fails. You can allow enterprise network users to perform unassisted local installation of applications on their devices.

Applications that are available for installation are stored on Administration Server as installation packages (see section "About installation packages" on page [35](#)).

See also:

Local installation mode.....	40
Remote installation of applications.....	36

About installation packages

Installation package is a dedicated executable file intended for installation of an application on client devices. An installation package is created based on files included in the application distribution package; it contains a collection of settings required to install the application and ensure its proper functioning immediately after the installation. Parameter values correspond to application defaults.

Installation packages are created and distributed by the service provider administrator.

Installation packages are used for remote installation of Kaspersky Lab applications and third-party applications on client devices through a remote management system provided by Kaspersky Security Center 10 Web Console.

You can install Kaspersky Lab applications and third-party applications on your networked devices in local installation mode (see section "Local installation mode" on page [40](#)), as well as allow your network users to perform unassisted installation of applications on their devices. To do this, you can use Kaspersky Security Center 10 Web Console to publish installation packages of applications.

See also:

Canceling installation package publishing	43
Viewing the list of published installation packages	42
Publishing installation packages	41

Remote installation of applications

The remote installation mode allows you to install Kaspersky Lab applications and third-party applications on multiple devices in your network simultaneously.

Kaspersky Security Center 10 Web Console performs remote installation of applications in background mode. During remote installation, you can use other features of the application, as well as view information about the status of remote installation for each of the devices on which remote installation is running.

► *To install an application on your networked devices in remote installation mode:*

1. Open the main application window (see section "Application interface" on page [15](#)).
2. Select the **Manage** tab.
3. On the **Manage** tab, select the **Managed devices** section.
4. In the **Managed devices** section, select the **Devices** tab.
5. In the left part of the window, click the **Add** button.

The Application Setup Wizard opens, showing the Welcome page.

6. Click the **Install to one or more networked devices using installation package** button.

The **Select installation package** window opens.

7. In the list, select the installation package of an application that you want to install, and click the **Next** button.

A window opens, showing a list of devices in your network on which you can install the application.

8. Select the check boxes for the devices on which you want to install the application. If you want to install the application on all devices listed, select the **Device name** check box. Click **Next**.

The **Adding accounts** window opens (see the figure below).

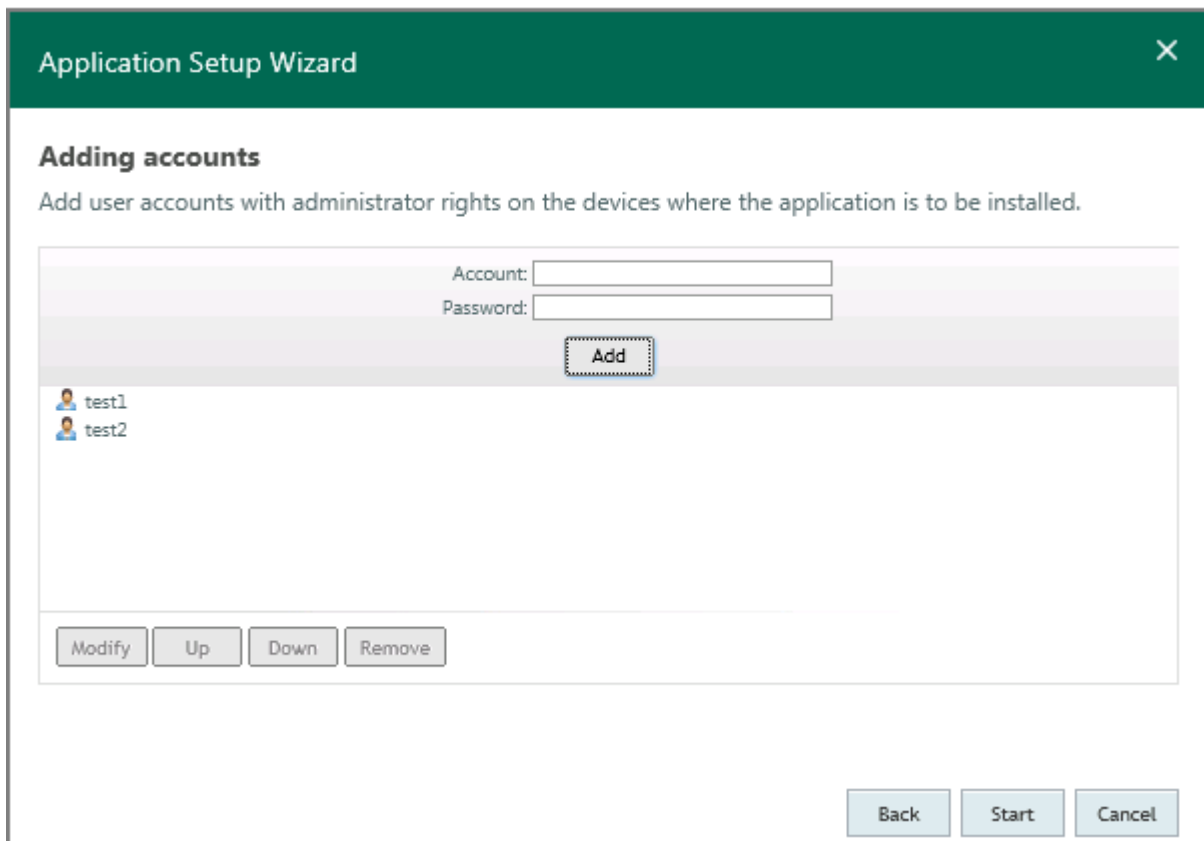


Figure 8. Application Setup Wizard. Adding accounts

9. Create a list of user accounts that have administrator privileges on the devices selected for installation (see figure below).

- To add accounts, for each account do the following:
 - a. In the **Account** text box, enter the account name.
 - b. In the **Password** text box, enter the password for the account.
 - c. Click **Add**.

The added account appears on the list of accounts in the lower part of the window.

- To modify account settings:
 - a. In the list, select the user account that you need to modify and click the **Modify** button.
 - b. Edit the account name in the **Account** text box.

- c. Change the account password in the **Password** text box.
- d. Click the **Save changes** button (see the figure below).

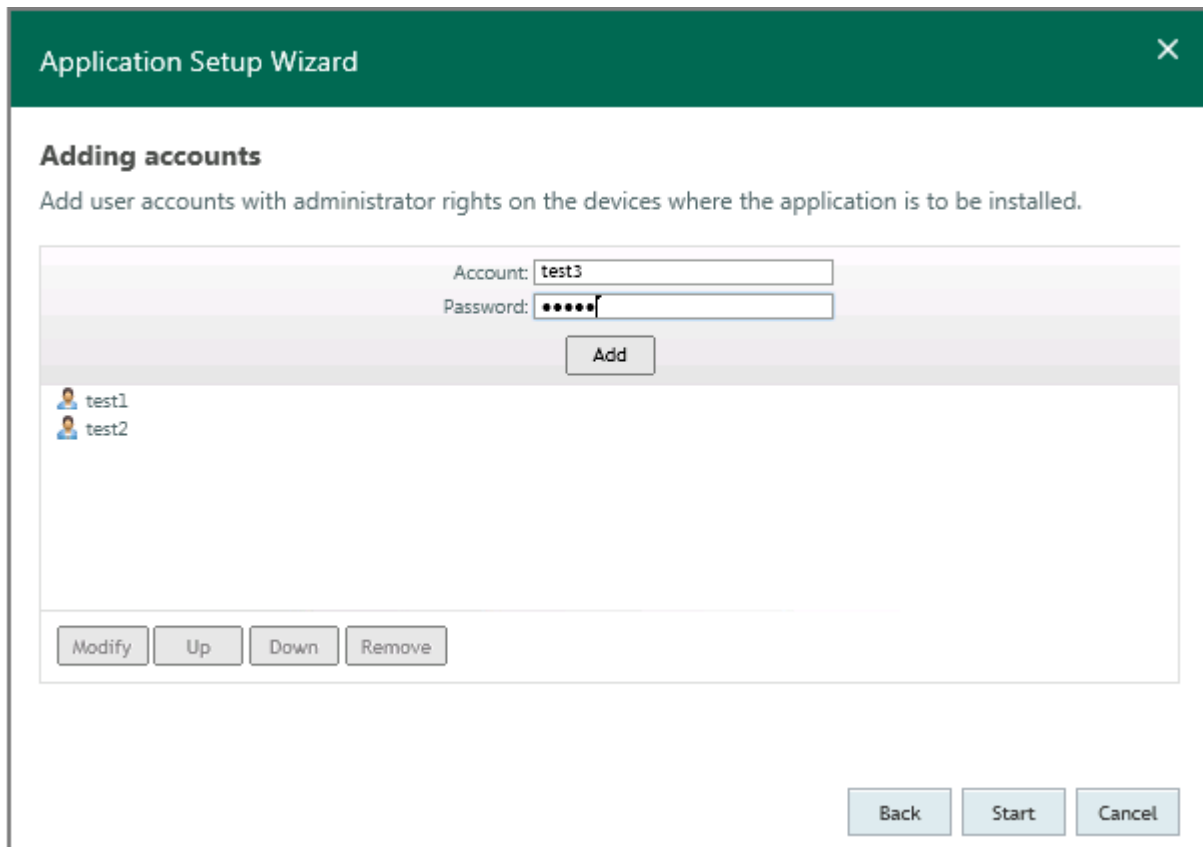


Figure 9. Application Setup Wizard. Modifying an account




The new name and password of the selected account will be saved.

- To delete an account from the list, in the list of accounts select an account that you want to delete and click the **Remove** button.
- To change the order in which the Setup Wizard applies the user accounts when starting remote installation on devices:
 - To move the account up in the list, select an account and click the **Move up** button.
 - To move the account down in the list, select an account and click the **Move down** button.

10. Start remote installation of the application by clicking the **Start** button.

Remote installation starts on the devices that you selected. The **Installing <App name>** window opens, displaying a list of application installation tasks for the selected networked devices.

You can view the list of installation tasks using the following interface elements:

- —Sorts the list of installation tasks by the selected field in ascending or descending alphabetical order.
- —Opens the section of information about the selected device.
- —Closes the section of information about the selected device.

The section of information about the device on which remote installation of the application has been started provides the following details:

- **Device name.** Network name of the device.
- **Status.** Application installation status. After remote installation is started, the status changes to *Installation in progress*.
- **IP address.** Network address of the device.
- **Domain.** Name of the network domain in which the device is registered.

11. To exit the Application Setup Wizard, click the **Close** button. The installation tasks keep on running.

If remote installation on devices has completed successfully, those devices are automatically added to the **Managed devices** administration group.

Remote installation of the application may return an error: for example, if another instance of the same application has already been installed on the device. Installation tasks that have returned an error, are displayed on the list of tasks with the *Installation error* status. If remote installation of the application on one or multiple devices returns an error, you can install the application locally.

You can run only one remote installation task at once. If you run one more remote installation task before the current remote installation completes, the latter will be stopped.

See also:

About installing applications	34
-------------------------------------	--------------------

Local installation mode

You can install Kaspersky Lab applications and third-party applications on your networked computers and Android™ devices in local installation mode. Kaspersky Security Center 10 Web Console provides two options for local installation of applications:

- Local installation through installation packages. To make an application available for local installation, you must publish the installation package of that application. Published installation packages are shown in the main application window, on the **Applications** tab. After publishing, Kaspersky Security Center 10 Web Console generates a link to the published installation package. Click this link to download the published installation package to the device and run it. After you run the installation package on the device, the application is installed automatically. You can allow network users to perform unassisted installation of applications on their devices, using published installation packages. To do this, users need links to published installation packages (for example, sent by email).
- Local installation from the Application Shop. The Application Shop is a component of Kaspersky Security Center 10 Web Console that is implemented in the interface as an individual tab. The Application Shop is intended for publishing Android apps and links to those apps in Google Play™ with the purpose of further installation on Android devices. To make apps available for local installation, you must add apk files or links to those apps in Google Play to the corporate Application Shop. Apps in the Application Shop are shown in the main application window on the **Applications** tab.

In this section:

Publishing installation packages	41
Viewing the list of published installation packages	42
Canceling installation package publishing	43
Installing an app using a published installation package	44
Adding Android app files and app links from Google Play to the corporate Application Shop	45
Viewing the Application Shop	47
Editing the settings of an app and removing an app from the Application Shop	47
Installing apps from the Application Shop	49

Publishing installation packages

► *To publish installation packages:*

1. Open the main application window (see section "Application interface" on page [15](#)).
2. Select the **Applications** tab.
3. In the left part of the window, select the **Published packages** tab.
4. In the left part of the window, click the **Add** button to open the **Package Addition Wizard** window.

A window opens, showing a list of installation packages that are available for publishing.

5. Select the check boxes for installation packages that you want to publish. To publish all installation packages on the list, select the check box next to the **Installation package name** header.

6. Click the **Publish** button.

The statuses of the installation packages that you have selected changes to *Publishing*. Publishing of the selected installation packages starts.

7. Click the **Close** button to close the **Adding packages** window.

Publishing of installation packages continues in automatic mode. After the publishing is complete, the installation packages will be added to the list of published installation packages on the **Published packages** tab.

Published installation packages are stored on the Administration Server. Kaspersky Security Center 10 Web Console provides links for downloading published installation packages. You can send those links to users in your network.

See also:

About installation packages	35
Canceling installation package publishing	43
Viewing the list of published installation packages	42

Viewing the list of published installation packages

► *To view a list of published installation packages:*

1. Open the main application window (see section "Application interface" on page [15](#)).
2. Select the **Applications** tab.
3. In the left part of the window, select the **Published packages** tab.

A window opens showing a list of published installation packages.

The list contains the following information about published installation packages:

- **Installation package name.** The name of the published installation package.
- **Permanent link to installation package.** A link used to download the published installation package from the local network.

If a newer version of the installation package is available on Administration Server, you can update the package by clicking the **Upgrade** button located next to the installation package.

You can send links to published installation packages to users of your network (for example, by email). Network users can use them to download published installation packages to their devices and to install applications.

See also:

About installation packages	35
-----------------------------------	--------------------

Canceling installation package publishing

You can cancel publishing of an installation package (for example, if its version has gone out of date).

► *To cancel publishing of an installation package:*

1. Open the main application window (see section "Application interface" on page [15](#)).
2. Select the **Applications** tab.
3. In the left part of the window, select the **Published packages** tab.

A window opens showing a list of published installation packages.

4. On the list, find the installation package for which you want to cancel publishing, and click the **Close access** button in the corresponding line.

The text *package deleted, access blocked* appears in the line. Publishing of the selected installation package will be canceled. The package becomes unavailable for download.

After publishing is canceled, the installation package is deleted from Administration Server and becomes unavailable for download. The link to the installation package becomes inactive.

See also:

About installation packages [35](#)

Installing an app using a published installation package

► *To install an app using a published installation package:*

1. Download a published installation package to the device on which you want the app installed. To do this, use the link received after publishing of the installation package.

To find the link that you should click to download the published installation package from the local network, open the list of published packages (see section "Viewing the list of published installation packages" on page [42](#)).

2. Start the published installation package. After you have run it, the installation will be performed automatically.
3. Wait until the app installation is complete.

See also:

Connecting to Administration Server [18](#)

Viewing the list of devices [28](#)

About installing applications [34](#)

Adding Android app files and app links from Google Play to the corporate Application Shop

The Application Shop allows you to add apk files and app links in Google Play.

► *To add an apk file:*

1. Open the main application window (see section "Application interface" on page [15](#)).
2. Select the **Applications** tab.
3. In the left part of the window, select the **Application Shop** tab.

The **List of Android applications** appears.

4. Click the **Add app package** button above the list.

The **New App Package Wizard for Android devices** window opens.

5. Click the **Browse** button and select an apk file from the list.
6. Click the **Next** button.
7. Enter the app name and description in the corresponding entry fields.

You can enter up to 256 characters in the **App name** field and up to 2,048 characters in the **Application description** field.

8. Click **Apply**.

The apk file that has been added will appear on the **List of Android applications** list. The number of apps added is shown in brackets after the list header (see the figure below).

► *To add an app link from Google Play:*

1. Open the main application window (see section "Application interface" on page [15](#)).
2. Select the **Applications** tab.
3. In the left part of the window, select the **Application Shop** tab.

The **List of Android applications** appears.

4. Click the **Add link to Google Play application** button over the list.

The **Link to Google Play application** window opens.

5. Enter the link in the **Specify link to application here** entry field.

The link must start with the `https://` network protocol name.

6. Click the **Next** button.
7. Enter the app name and description in the corresponding entry fields.

You can enter up to 256 characters in the **App name** field and up to 2,048 characters in the **Application description** field.

8. Click **Apply**.

The link that has been added appears on the **List of Android applications** list (see the figure below).

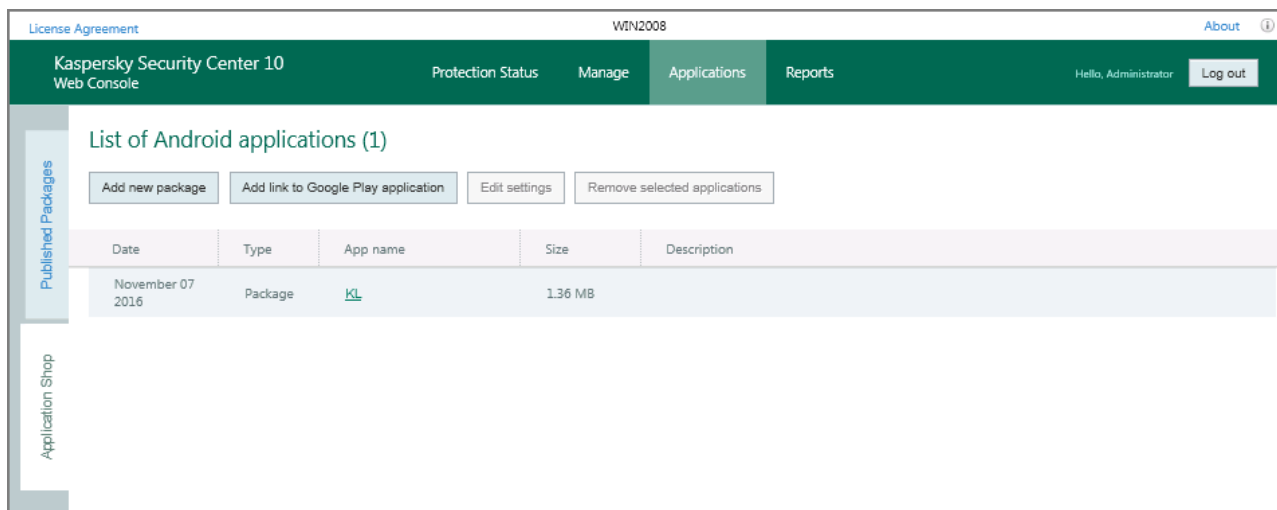


Figure 10. Apps and links to apps in Google Play in the Application Shop

Viewing the Application Shop

► *To view the list of Android apps in the Application Shop:*

1. Open the main application window (see section "Application interface" on page [15](#)).
2. Select the **Applications** tab.
3. In the left part of the window, select the **Application Shop** tab.

The **Application Shop** tab contains a list of Android apps that have been added to the Shop (apk files and app links from Google Play).

The list contains the following information about Android apps:

- **Date.** The date the package or the app link was added to the list.
- **Type.** The type of the app added: **Package** or **Link**.
- **App name.** The app name is a link. Clicking the link to an app belonging to the **Package** type causes Kaspersky Security Center 10 Web Console to download the app file to the device that you are currently using. Clicking an app belonging to the **Link** type causes Kaspersky Security Center 10 Web Console to proceed to the page of that app in Google Play.
- **Size.** The size of the package in Megabytes. It is specified for the **Package** app type only.
- **Description.** The description of the app.

Editing the settings of an app and removing an app from the Application Shop

► *To edit the settings of an app in the Application Shop:*

1. Open the main application window (see section "Application interface" on page [15](#)).
2. Select the **Applications** tab.
3. In the left part of the window, select the **Application Shop** tab.

The **List of Android applications** appears.

4. Select an app from the list and click the **Edit settings** button over the list.

If you have selected an app belonging to the **Package** type on the list, the **Application package** window opens. In this window, you can select the apk file of an app, as well as edit the app name and description.

If you have selected an app belonging to the **Link** type on the list, the **Link to Google Play application** window opens. In this window, you can specify the link to the app, as well as edit the app name and description.

5. Make the required changes and click the **Apply** button.

As a result, the newly edited app settings will be displayed in the Application Shop.

► *To remove an app from the Application Shop:*

1. Open the main application window (see section "Application interface" on page [15](#)).
2. Select the **Applications** tab.
3. In the left part of the window, select the **Application Shop** tab.

The **List of Android applications** appears.

4. Select an app from the list.

You can select multiple apps on the list.

5. Click the **Remove selected applications** button over the list.

The **Remove** window opens.

6. Click the **Remove** button.

As a result, the selected app will be removed from the Application Shop.

Installing apps from the Application Shop

► *To install an app from the Application Shop on an Android device using an apk file:*

1. Open the main application window (see section "Application interface" on page [15](#)).
2. Select the **Applications** tab.
3. In the left part of the window, select the **Application Shop** tab.

The **List of Android applications** appears.

4. Select an app belonging to the **Package** type from the list.
5. Click the link with the app name to download the apk file from the Application Shop to the device that you are currently using.
6. Move the apk file from the computer to the Android device using any convenient method.
7. Start the app installation from the apk file on the device.

To install the app, check if the device settings allow installation of apps from unknown sources. Installation of the app from the apk file is performed in a standard way adopted for Android devices.

► *To install an app using a Google Play link:*

1. Open the main application window (see section "Application interface" on page [15](#)).
2. Select the **Applications** tab.
3. In the left part of the window, select the **Application Shop** tab.

The **List of Android applications** appears.

4. Select an app belonging to the **Link** type from the list.
5. Click the link with the app name to open the app page on Google Play.

The app page on Google Play opens on a new browser tab.

6. Click the **Install** button on the app page.

The app prompts you to allow installation. Installation of the app from Google Play is performed in a standard way adopted for Android devices.

Managing policies

Policy is a collection of application settings defined for an administration group. By using policies, you can specify common values for the application settings in a centralized manner for all client devices in an administration group, as well as forbid any changes in the settings to be made locally through the application interface. The policy does not define all application settings.

Multiple policies with different values can be defined for a single application. However, there can be only one active policy for an application at a time. There is an option of activating an inactive policy when a specified event occurs. This, for example, allows you to define stricter anti-virus protection settings during virus outbreaks.

An application can run under different settings for different administration groups. Each group can have its own policy for an application.

Also, out-of-office policies can be created. If the connection between Administration Server and a client device is interrupted, the client device starts running under the out-of-office policy (if it is defined), or the policy keeps running under the applied settings until the connection is re-established.

After a policy is deleted or revoked, the application continues working with the settings specified in the policy. Those settings can be subsequently modified manually.

In this section:

Viewing a list of policies	51
Adding a policy	52
Managing policy profiles	54
Activating a policy	58
Modifying a policy	59
Applying an out-of-office policy	60
Deleting a policy	60
Managing mobile devices using an MDM policy.....	60

Viewing a list of policies

You can view the list of policies created for your networked devices that are managed by Administration Server. You can view the lists of policies for each administration group separately.

► *To view a list of policies:*

1. Open the main application window (see section "Application interface" on page [15](#)).
2. Select the **Manage** tab.
3. In the window that opens, select the **Policies** tab.
4. In the left part of the window select an administration group for which you want to view a list of policies:

A list of policies for the selected administration group is displayed on the screen (see the figure below).

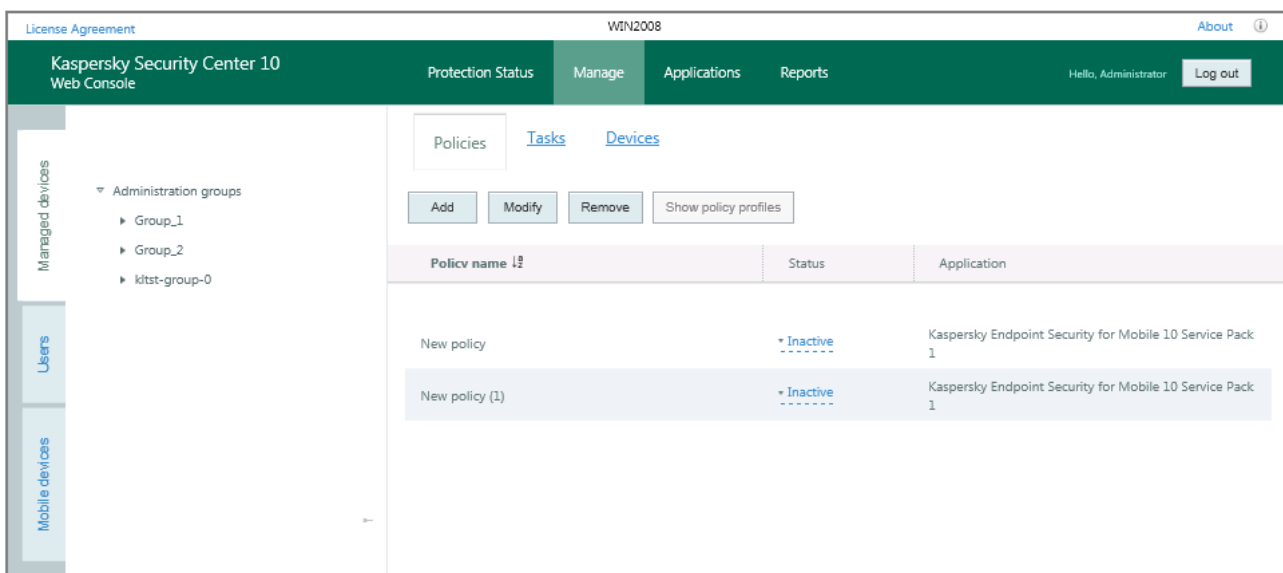




Figure 11. Viewing a list of policies

The list of policies contains the following information:

- Policy name.
- Policy status (active, inactive, for offline users).
- Name of the application for which the policy has been created.

To view information about a specific policy, use the following interface elements to find it on the list:

- Buttons  – Moves to the next / previous, first / last page of the list of policies.
- Icon  in the column header – Sorts entries in the list of policies by column value in ascending or descending alphabetical order.

Adding a policy

► *To add a policy:*

1. Open the main application window (see section "Application interface" on page [15](#)).
2. Select the **Manage** tab.
3. On the **Manage** tab, select the **Managed devices** section.
4. In the **Managed devices** section, select the **Policies** tab.
5. In the left part of the window, select the administration group for which you want to add a policy.
6. Click **Add**.

The New Policy Wizard opens, showing the Welcome page.

7. Click the **Create a policy** button.
8. In the **Select an application for which you want to create a group policy** window of the Wizard, select the application for which you want to create a policy and click the **Next** button.

With Kaspersky Security Center 10 Web Console, you can create policies for Kaspersky Mobile Device Management 10 Service Pack 1 and Kaspersky Endpoint Security 10 Service Pack 1 for Mobile. To create policies for other Kaspersky Lab applications, please use Administration Server.

A window opens for entering the name of the new group policy.

9. In the **Policy name** field, enter a name for the group policy being created.

10. Click the **Start** button to close the New Policy Wizard.

The new policy created by the Wizard will be added to the list of policies on the **Policies** tab (see section "**Viewing the list of policies**" on page [51](#)). By default, the newly created policy is assigned the *Inactive* status. You can change the policy's status in the **Status** column of the list of policies.

You can create several policies for one application from the group, but only one policy can be active at a time. When you create new active policy, the previous active policy becomes inactive.

When creating a policy, you can specify a minimum set of parameters required for the application to function properly. All other values are set to the default values applied during the local installation of the application. You can change the policy after it is created.

Settings of Kaspersky Lab applications changed after policies are applied are described in details in their respective Guides.

After the policy is created, the settings locked from editing (🔒 lock is set) take effect on client devices regardless of which settings had been previously specified for the application.

Managing policy profiles

This section provides information about *policy profiles* that are used for effective management of groups of devices. The advantages of policy profiles are described, as well as ways of applying them.

In this section:

About the policy profile	54
Adding a policy profile	56
Modifying a policy profile	57

About the policy profile

Policy profile is a named set of variable settings of a policy that is activated on a client device (computer or mobile device) when specific conditions are met. Activation of a profile modifies the policy settings that had been active on the device before the profile was activated.

Those settings take values that have been specified in the profile.

Profiles are only supported by the following policies:

- Policies of Kaspersky Endpoint Security 10 Service Pack 1 for Windows or later.
- Policies of Kaspersky Endpoint Security 10 Service Pack 1 for Mac.
- Policies of plug-in of Kaspersky Mobile Device Management 10 Service Pack 1 or later.

Advantages of policy profiles

Policy profiles simplify the management of client devices through policies:

- Profiles contain only settings that differ from the basic policy.
- You do not have to maintain and manually apply several instances of a single policy that differ only by a few settings.

- You do not have to allocate an individual out-of-office policy.
- New policy profiles are easy to create since export and import of profiles are supported, as well as creation of new profiles based on existing ones by copying.
- Several policy profiles can be active on a single client device simultaneously.
- The hierarchy of policies is supported.

Profile activation rules. Priorities of profiles

A policy profile is activated on a client device when an activation rule triggers. An activation rule can contain the following conditions:

- Network Agent on a client device connects to the Server with a specified set of connection parameters, such as Server address, port number, etc.
- The client device is offline.
- The client device has been assigned specified tags.
- The client device is located in a specific unit of Active Directory®, the device or its owner is located in a security group of Active Directory.
- The client device belongs to a specified owner, or the owner of the device is included in an internal security group of Kaspersky Security Center 10 Web Console.

Profiles that have been created for a policy are sorted in descending order of priority. If the *X* profile precedes the *Y* profile on the list of profiles, this means that *X* has a higher priority than *Y*. The priorities of profiles are necessary because several profiles may be active simultaneously on a client device.

Policies in the hierarchy of administration groups

While policies influence each other in accordance with the hierarchy of administration groups, profiles with identical names merge. Profiles of a 'higher' policy have a higher priority. For example, in administration group *A*, policy *P(A)* has profiles *X1*, *X2*, and *X3* (in descending order of priority). In administration group *B*, which is a subgroup of group *A*, policy *P(B)* has been created with profiles *X2*, *X4*, *X5*. Then policy *P(B)* will be modified with policy *P(A)* so that the list of profiles

in policy $P(B)$ will look as: $X1, X2, X3, X4, X5$ (in descending order of priority). The priority of profile $X2$ will depend on the initial state of $X2$ of policy $P(B)$ and $X2$ of policy $P(A)$.

The active policy is the sum of the master policy and all active profiles of that policy, i.e., profiles for which the activation rules are triggered. The active policy is recalculated when you run Network Agent, enable and disable offline mode, or edit the list of tags assigned for the client device.

Properties and restrictions of policy profiles

Profiles have the following properties:

- Profiles of an inactive policy have no impact on client devices.
- If a policy is active in offline mode, profiles of that policy will also be applied in offline mode only.
- Profiles do not support static analysis of access to executable files.
- A policy cannot contain notification settings.
- If UDP port 15000 is used for connecting a device to Administration Server, you must activate the corresponding policy profile within one minute when assigning a tag to the device.
- You can use rules of connection between Network Agent and Administration Server when creating profile activation rules.

Adding a policy profile

► *To add a policy profile:*

1. Open the main application window (see section "Application interface" on page [15](#)).
2. Select the **Manage** tab.
3. On the **Manage** tab, select the **Managed devices** section.
4. In the **Managed devices** section, select the **Policies** tab.
5. In the left part of the window, select an administration group.

6. In the list of policies, select the policy for which you want to add a profile.

7. Click the **Show policy profiles** button.

The list of policy profiles opens.

8. Click **Add**.

The New Policy Profile Wizard opens, showing the Welcome page.

9. Click the **Create policy profile** button.

A window opens for entering the policy profile settings.

10. In the upper entry field, specify the name of a policy profile. The name of a profile cannot include more than 100 characters.

11. In the **Activation rules** list, click the **Add** button to create a rule by which the policy profile will be activated.

12. Select the **Enable profile** check box to allow client devices or managed devices to use the policy profile.

13. Click the **Start** button to close the New Policy Profile Wizard.

The new policy profile that has been created by the Wizard will be added to the list of policy profiles. You can view the list of policy profiles on the **Policies** tab by clicking the **Show policy profiles** button. You can define the settings for the newly created policy profile on the **Policies** tab by clicking **Edit** (see section "**Modifying a policy profile**" on page [57](#)).

Modifying a policy profile

You can edit the settings of a policy profile for Kaspersky Lab applications after the policy profile is created.

► *To modify a policy profile:*

1. Open the main application window (see section "Application interface" on page [15](#)).

2. Select the **Manage** tab.

3. In the left part of the window, select an administration group.
4. In the list of policies, select the one for which you want to edit the profile settings.
5. Click the **Show policy profiles** button.

In the lower part of the window, a list of policy profiles opens.

6. Select the profile of which you want to edit the settings.
7. Click **Change**.

The group policy properties window appears on the screen.

8. Configure the policy profile and the Kaspersky Lab application in the respective sections.

The settings of Kaspersky Lab applications are described in detail in the respective Guides.

9. Click the **OK** button to complete the editing of the profile settings.

The settings that you have modified will be applied either after the device is synchronized with the Administration Server (if the policy profile is active), or after the activation rule is triggered (if the policy profile is inactive).

Activating a policy

► *To make a policy active for a selected administration group:*

1. In the main application window (see section "Application interface" on page [15](#)), on the **Manage** tab, select the **Policies** tab.
2. From the list select a policy that you want to activate.
3. In the drop-down list, in the **Status** column, select the **Active** value.

As a result, the policy becomes active for the selected administration group.

When a policy is applied to a large number of client devices, both the load on the Administration Server and the network traffic amount increase significantly for some time.

Modifying a policy

You can edit the settings of group policies for Kaspersky Lab applications after they are created.

► *To edit a policy:*

1. Open the main application window (see section "Application interface" on page [15](#)).
2. Select the **Manage** tab.
3. On the **Manage** tab, select the **Managed devices** section.
4. In the **Managed devices** section, select the **Policies** tab.
5. In the left part of the window, select the administration group for which you want to edit the policy.
6. In the list of policies, select the one of which you want to edit the settings.
7. Click **Change**.

The group policy properties window appears on the screen.

8. Define the settings of the Kaspersky Lab application.

The settings of Kaspersky Lab applications are described in detail in the respective Guides.

9. Click the **OK** button to complete the editing of the policy settings. To apply the settings, click the **Apply** button. To abort the policy editing, click the **Cancel** button. In this case, all changes of the policy settings will be discarded.

Applying an out-of-office policy

An out-of-office policy takes effect on a device in case it is disconnected from the corporate network.

- ▶ *To apply the selected out-of-office policy,*
 1. In the main application window (see section "Application interface" on page [15](#)), on the **Manage** tab, select the **Policies** tab.
 2. From the list, select a policy that you want to apply to offline users.
 3. In the drop-down list, in the **Status** column, select the **Out-of-office** value.

As a result, the policy is applied to the devices if they are disconnected from the corporate network.

Deleting a policy

- ▶ *To delete a policy:*
 1. In the main application window (see section "Application interface" on page [15](#)), on the **Manage** tab, select the **Policies** tab.
 2. From the list select the policy that you want to delete.
 3. Click the **Remove** button.
 4. In the window that opens, confirm the operation by clicking the **Yes** button.

As a result, the policy will be deleted from the list.

Managing mobile devices using an MDM policy

This section provides information about how to handle the policy for Kaspersky Mobile Device Management 10 Service Pack 1.

In this section:

About the MDM policy	61
Configuring an MDM policy.....	63

About the MDM policy

To manage iOS MDM and EAS devices (EAS devices are connected to the Administration Server over Exchange ActiveSync®), you can use the Kaspersky Mobile Device Management 10 Service Pack 1 management plug-in, which is included in the Kaspersky Security Center distribution kit. Kaspersky Mobile Device Management lets you create group policies for specifying the configuration settings of iOS MDM and EAS devices. A group policy that allows viewing and defining the configuration settings of iOS MDM devices and EAS devices, is called an MDM policy.

An MDM policy provides the administrator with the following options:

- For managing EAS devices:
 - Configuring the device unlocking password.
 - Configuring the data storage on the device in encrypted form.
 - Configuring the synchronization of the corporate mail.
 - Configuring the hardware features of mobile devices, such as the use of removable drives, the use of the camera, or the use of Bluetooth®.
 - Configuring restrictions on the use of mobile applications on the device.

- For managing iOS MDM devices:
 - Configuring device password security settings.
 - Configuring restrictions on the use of hardware features of the device and restrictions on installation and removal of mobile apps.
 - Configuring restrictions on the use of pre-installed mobile apps, such as YouTube™, iTunes® Store, Safari.
 - Configuring restrictions on media content viewed (such as movies and TV shows) by region where the device is located.
 - Configuring settings of device connection to the Internet via the proxy server (Global HTTP proxy).
 - Configuring the settings of the account using which the user can access corporate apps and services (Single Sign On technology).
 - Monitoring Internet usage (visits to websites) on mobile devices.
 - Configuring settings of wireless networks (Wi-Fi), access points (APN), and virtual private networks (VPN) that use different authentication mechanisms and network protocols.
 - Configuring settings of the connection to AirPlay® devices for streaming photos, music, and videos.
 - Configuring settings of the connection to AirPrint® printers for wireless printing of documents from the device.
 - Configuring settings of synchronization with the Microsoft Exchange server and user accounts for using corporate email on devices.
 - Configuring user credentials for synchronization with the LDAP directory service.
 - Configuring user credentials for connecting to CalDAV and CardDAV services that give users access to corporate calendars and contact lists.
 - Configuring settings of the iOS® interface on the user's device, such as fonts or icons for favorite websites.

- Adding new security certificates on devices.
- Configuring settings of the SCEP server for automatic retrieval of certificates by the device from the Certification Center.
- Adding custom settings for operation of mobile apps.

The general operating principles of an MDM policy do not differ from the operating principles of policies created for managing other apps. An MDM policy is special in that it is assigned to an administration group that includes the iOS MDM Server and the Microsoft Exchange Mobile Devices Server (hereinafter referred to as "mobile device servers"). All settings specified in an MDM policy are first applied to mobile device servers and then to mobile devices managed by those servers. In the case of a hierarchical structure of administration groups, slave mobile device servers receive MDM policy settings from master mobile device servers and distribute them to mobile devices.

For detailed information about how to use the MDM policy in the Administration Console of Kaspersky Security Center, please refer to the Administrator's Guide for Kaspersky Security for Mobile Integrated Solution.

Configuring an MDM policy

Using an MDM policy, you can define the configuration settings of EAS devices and iOS MDM devices. You can define the settings of EAS devices in the MDM policy properties window, in the **Settings of EAS devices** section. You can define the settings of iOS MDM devices by means of third-party utilities, such as iPhone® Configuration Utility or Apple® Configurator, and then import the settings to the MDM policy. Using such utilities as iPhone Configuration Utility or Apple Configurator, you can also export the settings of iOS MDM devices to a file for further viewing and editing.

► *To import the configuration settings of iOS MDM devices from a file:*

1. Open the main application window (see section "Application interface" on page [15](#)).
2. Select the **Manage** tab.
3. On the **Manage** tab, select the **Managed devices** section.

4. In the **Managed devices** section, select the **Policies** tab.
5. In the left part of the window, select the administration group for which you want to import an MDM policy.
6. In the list of policies, select the MDM policy of which you want to import the settings.
7. Click **Change**.

The MDM policy properties window opens.

8. In the MDM policy properties window, select the **Import / Export settings** tab.
9. Click the **Import** button.
10. In the window that opens, select the file with the `mobileconfig` extension.

This results in the configuration settings of iOS MDM devices being imported from the selected file to the MDM policy.

► *To export the configuration settings of iOS MDM devices to a file:*

1. Open the main application window (see section "Application interface" on page [15](#)).
2. Select the **Manage** tab.
3. On the **Manage** tab, select the **Managed devices** section.
4. In the **Managed devices** section, select the **Policies** tab.
5. In the left part of the window, select the administration group for which you want to export an MDM policy.
6. In the list of policies, select the MDM policy of which you want to export the settings.
7. Click **Change**.

The MDM policy properties window opens.

8. In the MDM policy properties window, select the **Export / Import settings** tab.

9. Click the **Export** button.

This results in the configuration settings of iOS MDM devices being exported to a file with the `mobileconfig` extension. You can open that file with iPhone Configuration Utility or Apple Configurator.

Managing user accounts

Kaspersky Security Center 10 Web Console lets you manage user accounts and user groups.

The application supports two types of accounts:

- Accounts of organization employees. Administration Server retrieves data of the accounts of those users when polling the organization's network.
- Internal user accounts. Those are applied when handling virtual Administration Servers. The accounts of internal users are created and used only within Kaspersky Security Center 10 Web Console.

You can view all user accounts in the **Users** section (see page [67](#)).

You can perform the following actions on user accounts and user groups:

- Filter the list of user accounts (see page [68](#)).
- View the user details (see page [69](#)).
- View the list of the user's mobile devices (see page [70](#)).

In this section:

Viewing the list of accounts	67
Filtering the list of user accounts.....	68
Viewing the user's details	69
Viewing the list of a user's mobile devices.....	70



Viewing the list of accounts

When managing accounts, you can view a list of user accounts and user groups created on the Administration Server.

► *To view the list of accounts:*


1. Open the main application window (see section "Application interface" on page [15](#)).
2. Select the **Manage** tab.
3. On the **Manage** tab, select the **Users** section.


The **Users** section displays a list of user accounts (see the figure below). By default, the list of user accounts contains the following information about users:

- An icon for the account type. If the icon looks like , the account has been created for a single user. If the icon looks like , the account has been created for a group of users.
- User name. The name of an account or group of accounts.

You can add columns with additional information about an account to the list by clicking the **Show user details** button.

4. View the list of accounts by using the following interface elements:

- The  buttons to move to the next / previous, first / last page of the list of accounts.

- The  icon in the column header signifies the sorting of accounts in the list in alphabetical order.

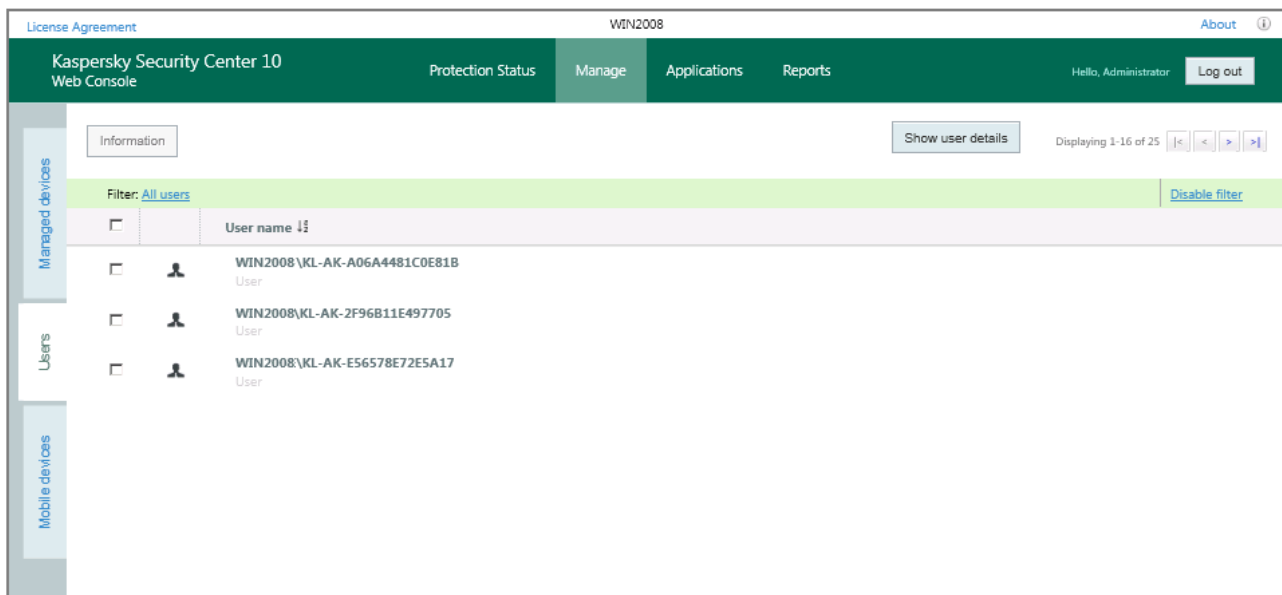


Figure 12. List of user accounts

Filtering the list of user accounts

For convenient management of the list of user accounts, you can filter it based on specified settings.

► *To filter the list of user accounts:*

1. Open the main application window (see section "Application interface" on page [15](#)).
2. Select the **Manage** tab.
3. On the **Manage** tab, select the **Users** section.

A list of user accounts appears on the screen.

4. Click the link next to the **Filter** marking in the upper part of the window to open the filter settings window.

5. In the **Filter: Users** window that opens, configure the filtering of the list of accounts:
 - By specific text contained in user account data.
 - By user account details, such as name, user type, organization name, email address, and so forth.
6. Click the **OK** button to filter the list of accounts.

You can click the **Disable filter** link in the upper part of the **Users** section to cancel filtering of the list of user accounts.

Viewing the user's details

► *To view the details of a user:*

1. Open the main application window (see section "Application interface" on page [15](#)).
2. Select the **Manage** tab.
3. On the **Manage** tab, select the **Users** section.

The **Users** section displays a list of user accounts.

4. In the list, select the account of a user or group of users of which you want to view the details.
5. At the top of the section, click the **Information** button.
6. In the **User information** window that opens, select the **User data** section.

The user's details appear on the screen (see the figure below).

The screenshot shows a 'User information' dialog box with a dark green header and a close button (X) in the top right corner. The dialog is divided into two main sections: 'User data' and 'User devices'. The 'User data' section contains a list of fields with corresponding input fields or values:

Field	Value
SAM name:	FakeUser_1
Full name:	FakeUser_1
Company:	
Department:	
SAM domain:	
Domain:	
User or group:	User
Local user account:	No
Kaspersky Security Center 10 internal user:	Yes
Email 1:	
Email 2:	
Phone 1:	
Phone 2:	
Mobile:	

A 'Close' button is located in the bottom right corner of the dialog box.

Figure 13. User data

Viewing the list of a user's mobile devices

► To view the list of a user's mobile devices:

1. Open the main application window (see section "Application interface" on page [15](#)).
2. Select the **Manage** tab.
3. On the **Manage** tab, select the **Users** section.

A list of user accounts appears on the screen.

4. In the list, select the user account whose list of mobile devices you want to view.
5. At the top of the section, click the **Information** button.
6. In the **User information** window that opens, select the **User devices** section.

A list of the user's mobile devices connected to the Administration Server appears on the screen (see the figure below).

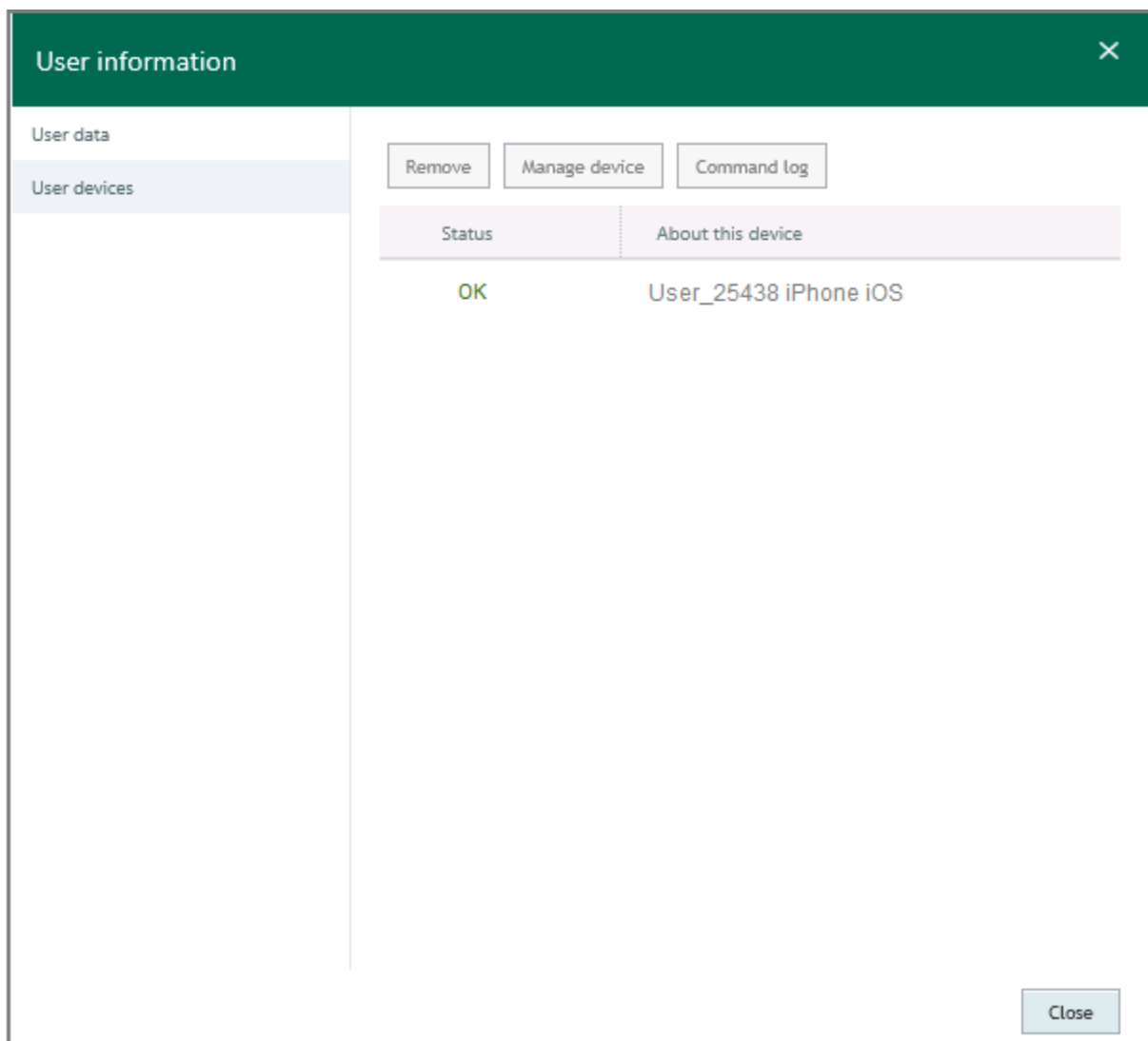


Figure 14. List of the user's mobile devices

In the **User devices** section, you can view information about each device of the user, as well as send a command to a selected device, track the status of its execution in the command log, or remove the device from the list.

Mobile Device Management

Kaspersky Security Center 10 Web Console allows managing users' mobile devices that have been connected to Kaspersky Security Center Administration Server. Such mobile devices are called *managed mobile devices*.

The list of all managed mobile devices is displayed in the **Mobile devices** section, on the **Manage** tab of the main application window.

You can take the following actions on users' mobile devices:

- View information about a mobile device (see page [74](#)).
- View information about the owner of a mobile device (see page [74](#)).
- Send commands to a mobile device (see page [78](#)).
- View the commands execution log (see page [78](#)).
- Remove mobile devices from the list (see page [79](#)).

In this section:

Viewing the list of mobile devices.....	73
Viewing mobile device settings	74
Viewing information about the owner of a mobile device	74
Commands for mobile device management.....	75
Sending commands to a mobile device	78
Viewing the commands log.....	78
Removing a mobile device from the list.....	79

Viewing the list of mobile devices


You can view a list of all mobile devices managed by the Administration Server.

► *To view the list of mobile devices:*

1. Open the main application window (see section "Application interface" on page [15](#)).
2. Select the **Manage** tab.
3. On the **Manage** tab, select the **Mobile devices** section.

The **Mobile devices** section displays a list of managed mobile devices (see the figure below). By default, the list contains the following information about devices:

- **Status:** Information about the connection status and the operation of the mobile device.
- **About this device.** General information about the device: name of the mobile device in Kaspersky Security Center, names of the company and department, name and version of the operating system, phone number.

4. View the list of mobile devices by using the  buttons to jump to the next / previous, first / last page of the list of mobile devices.

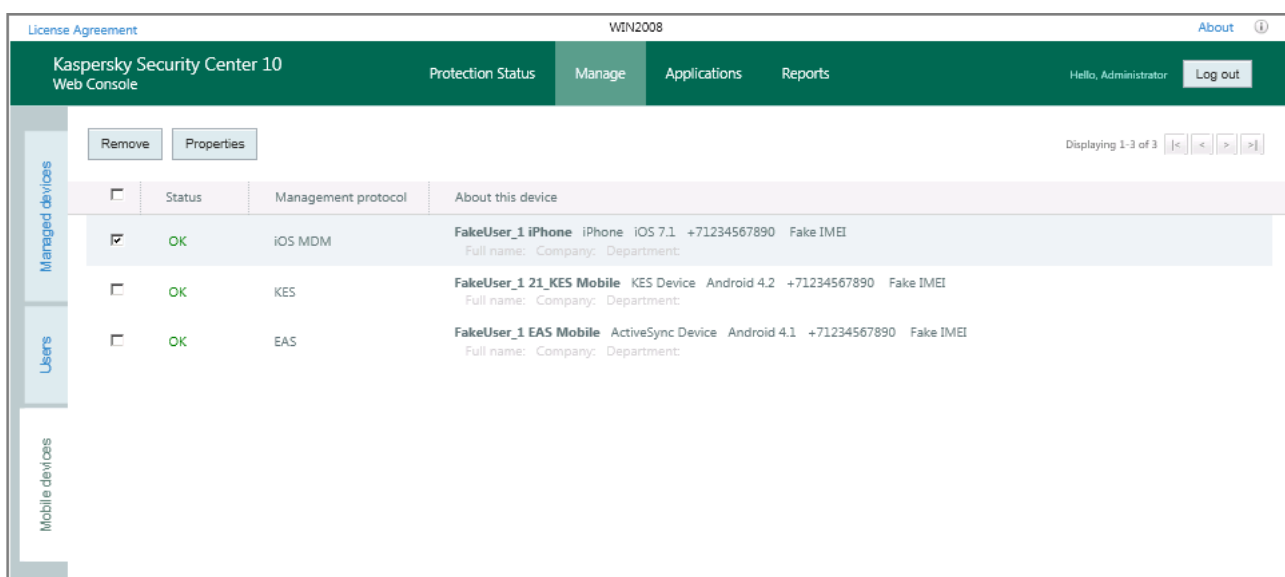


Figure 15. List of managed mobile devices

Viewing mobile device settings

► *To view the settings of a mobile device:*

1. Open the main application window (see section "Application interface" on page [15](#)).
2. Select the **Manage** tab.
3. On the **Manage** tab, select the **Mobile devices** section.

The **Mobile devices** section displays a list of managed mobile devices

4. In the list, select a mobile device whose settings you want to view.
5. At the top of the section, click the **Properties** button.
6. In the **About this device** window that opens, select the **Device data** section.

Information about the mobile device (operating system version of the operating system, model, phone number on the SIM card, etc.) appears on the screen.

To view the settings required for the operation of the device management protocol, select the **Settings <protocol name>** or the **Advanced settings <protocol name>** section, or **Kaspersky Endpoint Security**.

Viewing information about the owner of a mobile device

► *To view information about the user of a mobile device:*

1. Open the main application window (see section "Application interface" on page [15](#)).
2. Select the **Manage** tab.
3. On the **Manage** tab, select the **Mobile devices** section.

The **Mobile devices** section displays a list of managed mobile devices

4. In the list of mobile devices, select the one about which you want to view information.

5. At the top of the section, click the **Properties** button.

6. In the **About this device** window that opens, select the **Owner** section.

The details of the user account under which the mobile device has been connected to Administration Server appear on the screen (full name of the account, organization name, account domain, email address, etc.).

Commands for mobile device management

Kaspersky Security Center 10 Web Console supports commands for mobile device management.

Such commands are used for remote mobile device management. For example, in case your mobile device is lost, you can delete corporate data from the device by using a command.

You can use commands for the following types of managed mobile devices:

- iOS MDM devices.
- KES devices.
- EAS devices.

Each device type supports a dedicated set of commands. The following table shows sets of commands for each of the device types.

For all types of devices, if the **Reset settings to factory values** command is successfully executed, all data is deleted from the device, and the device settings are rolled back to their factory values.

After successful execution of the **Delete corporate data** command on an iOS MDM device, all installed configuration profiles, provisioning profiles, the iOS MDM profile, and applications for which the **Remove together with iOS MDM profile** check box has been selected, are removed from the device.

If the **Delete corporate data** command is successfully executed on a KES device, all corporate data, entries in Contacts, the SMS history, the call log, the calendar, the Internet connection settings, and the user accounts, except for the Google™ account, will be deleted from the device. For a KES device, all data from the memory card will also be deleted.

Table 2. List of supported commands

Mobile device type	Commands	Command execution result
iOS MDM device	Lock	The mobile device is locked.
	Unlock	Mobile device locking with a PIN code is disabled. The previously specified PIN code has been reset.
	Reset settings to factory values	All data is deleted from the mobile device and the settings are rolled back to their factory values.
	Delete corporate data	All installed configuration profiles, provisioning profiles, the iOS MDM profile, and applications for which the Remove together with iOS MDM profile check box has been selected, are removed from the device.
KES device	Unlock	Device locking with a PIN code is disabled. The previously specified PIN code has been reset.
	Reset settings to factory values	All data is deleted from the mobile device and the settings are rolled back to their factory values.

Mobile device type	Commands	Command execution result
	Delete corporate data	Corporate data, entries in Contacts, the SMS history, the call log, the calendar, the Internet connection settings, and the user accounts (except for the Google account) have been deleted. Memory card data has been wiped.
	Locate	The mobile device is located and shown on Google Maps™. The mobile carrier charges a fee for sending the SMS message and for providing Internet connection.
	Mugshot	The photo has been taken with the device's front camera and saved on the Administration Server. Photos can be viewed in the command log. The mobile carrier charges a fee for sending the SMS message and for providing Internet connection.
	Alarm	The mobile device plays a sound alarm.
EAS device	Reset settings to factory values	All data is deleted from the mobile device and the settings are rolled back to their factory values.

Sending commands to a mobile device

You can send commands to manage mobile devices remotely.

► *To send a command to a mobile device:*

1. Open the main application window (see section "Application interface" on page [15](#)).
2. Select the **Manage** tab.
3. On the **Manage** tab, select the **Mobile devices** section.
4. The **Mobile devices** section displays a list of managed mobile devices
5. Select the mobile device to which you want to send a command in the list.
6. At the top of the section, click the **Properties** button.
7. In the **About this device** window that opens, select the **Manage device** section.
8. In the list of commands, select the one that you want to be executed on the device, and click the button with its name.

Depending on the command that you have selected, clicking the button with its name may open an additional window with a command confirmation prompt. For example, an additional window opens for the **Soft Wipe** command, since executing it results in a loss of data on the mobile device.

Viewing the commands log

► *To view the log of commands that have been sent to a mobile device:*

1. Open the main application window (see section "Application interface" on page [15](#)).
2. Select the **Manage** tab.
3. In the window that opens, select the **Mobile devices** section.

The **Mobile devices** section displays a list of managed mobile devices

4. In the list of mobile devices, select the one for which you want to view the command log.
5. At the top of the section, click the **Properties** button.
6. In the **About this device** window that opens, select the **Command execution log** section.

A list of commands sent to the device appears on the screen. The command log contains information about each command that has been sent to the device:

- **Date Time.** The date and time when commands were sent to the device.
- **Name Status.** Command name and status of its execution.

Removing a mobile device from the list

► *To remove a mobile device from the list:*

1. Open the main application window (see section "Application interface" on page [15](#)).
2. Select the **Manage** tab.
3. On the **Manage** tab, select the **Mobile devices** section.

A list of managed mobile devices appears on the screen.

4. Select the check box next to the mobile device that you want to remove from the list.

You can select several mobile devices.

5. Click the **Remove** button in the upper part of the section.
6. In the **Remove** window that opens, confirm removal of the device from the list by clicking the **Remove** button.

This removes the selected mobile device from the list and disconnects it from Administration Server management.

Managing tasks

Administration Server manages applications installed on client devices, by creating and running various tasks. Tasks are required for installing, launching and stopping applications, scanning files, updating databases and software modules, and taking other actions on applications.

Any number of tasks can be created for each application.

You can start and stop tasks, view run results, and delete tasks.

Task results are saved both on the Administration Server, in centralized mode, and locally, on each client device.

In this section:

Viewing a list of tasks	80
Starting and stopping a task manually	82
Viewing task run results	82
Deleting tasks	83

Viewing a list of tasks

You can view the list of tasks created for your networked devices that are managed by Administration Server. You can view the lists of tasks for each administration group separately.

► *To view a list of tasks:*

1. Open the main application window (see section "Application interface" on page [15](#)).
2. Select the **Manage** tab.
3. In the window that opens, select the **Tasks** tab.
4. In the left part of the window select an administration group for which you want to view a list of tasks:

A list of tasks for the selected administration group is displayed on the screen (see the figure below).

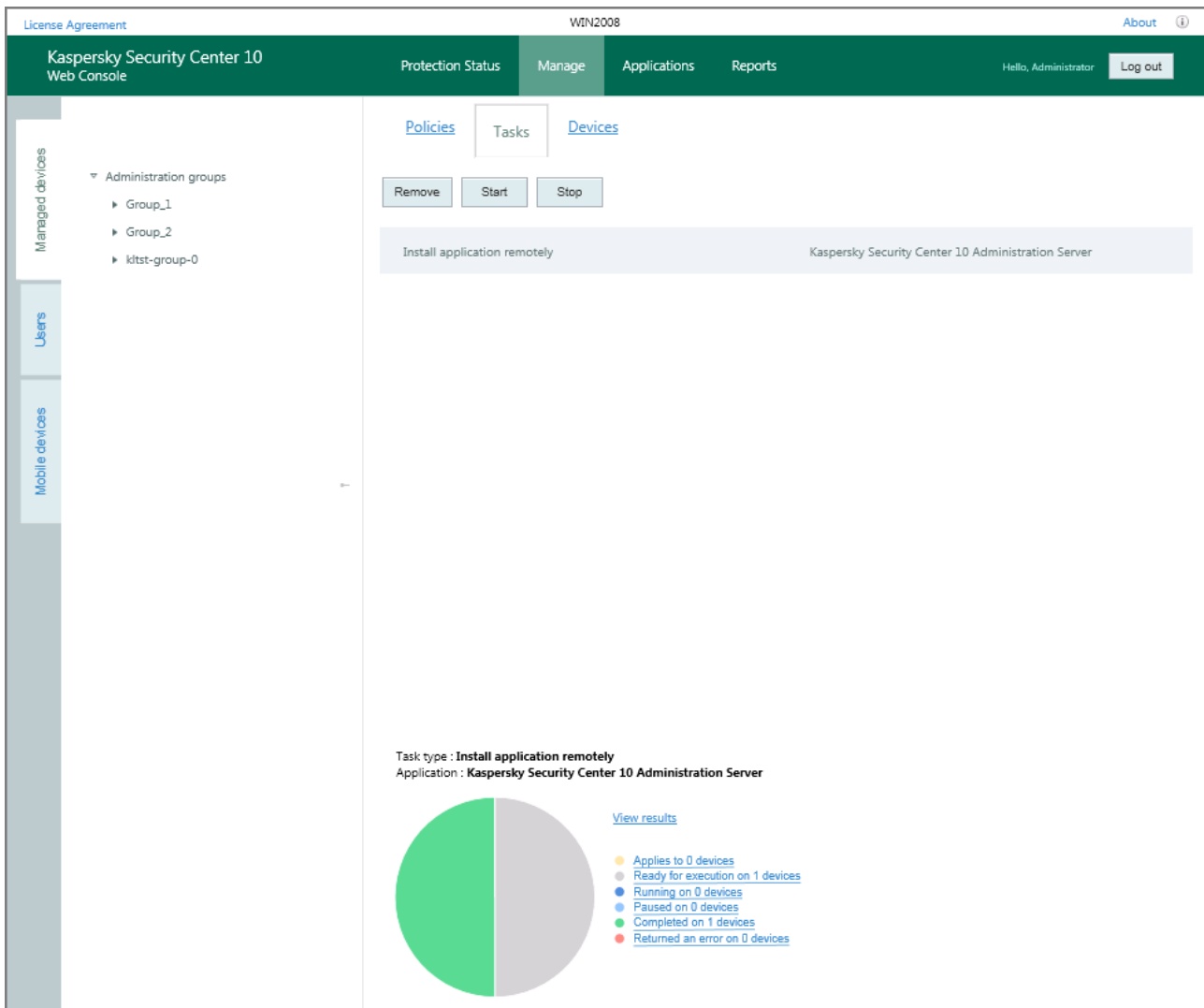




Figure 16. Viewing a list of tasks

The list of tasks contains the following information:

- Task name.
- The name of the application for which the task has been created.

The bottom part of the window displays the run statistics for the task selected from the list of tasks.

To view information about a specific task, use the following interface elements to find it on the list:

- Buttons  – take you to the next/previous, first/last page of the list of tasks.
- Icon  in the column header – sorts entries in the list of tasks by column value in ascending or descending alphabetical order.

Starting and stopping a task manually

► *To start or stop a task manually:*

1. In the main application window (see section "Application interface" on page [15](#)), on the **Manage** tab, select the **Tasks** tab.
2. From the list select a task that you want to start or stop.
3. Click the **Start** or **Stop** button.

As a result, the task will be started or stopped.

You can only run a task on a client device if the application for which that task was created is running. When the application is not running, all running tasks are canceled.

Viewing task run results

► *To view the run results of a task:*

1. In the main application window (see section "Application interface" on page [15](#)), on the **Manage** tab, select the **Tasks** tab.
2. From the list of tasks select one for which you want to view the run results.
3. Click the **View results** button.

The run results for the selected task are displayed in the window that opens.

Deleting tasks

► *To delete a task, perform the following steps:*

1. In the main application window (see section "Application interface" on page [15](#)), on the **Manage** tab, select the **Tasks** tab.
2. From the list of tasks select one that you want to delete.
3. Click the **Remove** button.
4. In the window that opens, confirm the task deletion by clicking the **Yes** button.

As a result, the task will be deleted from the list.

Working with reports

This section provides instructions on how to perform the following operations on reports provided by Administration Server to which the application is connected: view, print, send by email, and save report data to a file.

In this section:

About reports	84
Actions on reports	85
Viewing reports	86
Exporting reports	87
Configuring report delivery.....	87

About reports

Kaspersky Security Center 10 Web Console allows you to gain access to reports of Administration Server to which the application is connected.

Reports provide various information about the status of the protection system on devices managed by the Administration Server.

The list of available reports is created by your service provider's administrator. The list of reports may vary depending on the access rights assigned to your account.

Actions on reports

You can perform the following operations on Administration Server reports:

- **View reports**

You can view reports published for you by the service provider's administrator. The reports are read-only. You cannot modify them.

- **Export reports**

After viewing a report, you can export it and save it, for example, for later analysis and processing. You can export a report to one of three formats: HTML, XML, or PDF.

- **Configure automatic report delivery by email**

Administration Server permits automatic delivery of reports by email. You may need to configure Kaspersky Security Center 10 Web Console to deliver reports by email to you and other staff members involved in the anti-virus protection of your network (for example, system administrators or other IT experts).

You can manage the automatic delivery of reports by modifying the delivery settings: set of delivered reports and list of recipients' email addresses. All recipients in the list receive the same set of reports.

Administration Server sends reports once a day, at midnight.

See also:

Viewing reports	86
Exporting reports	87
Configuring report delivery.....	87

Viewing reports

► To view a report:

1. Open the main application window (see section "Application interface" on page 15).
2. Select the **Reports** tab.
3. In the left part of the window, from the list of reports, select a report that you want to view (see the figure below).

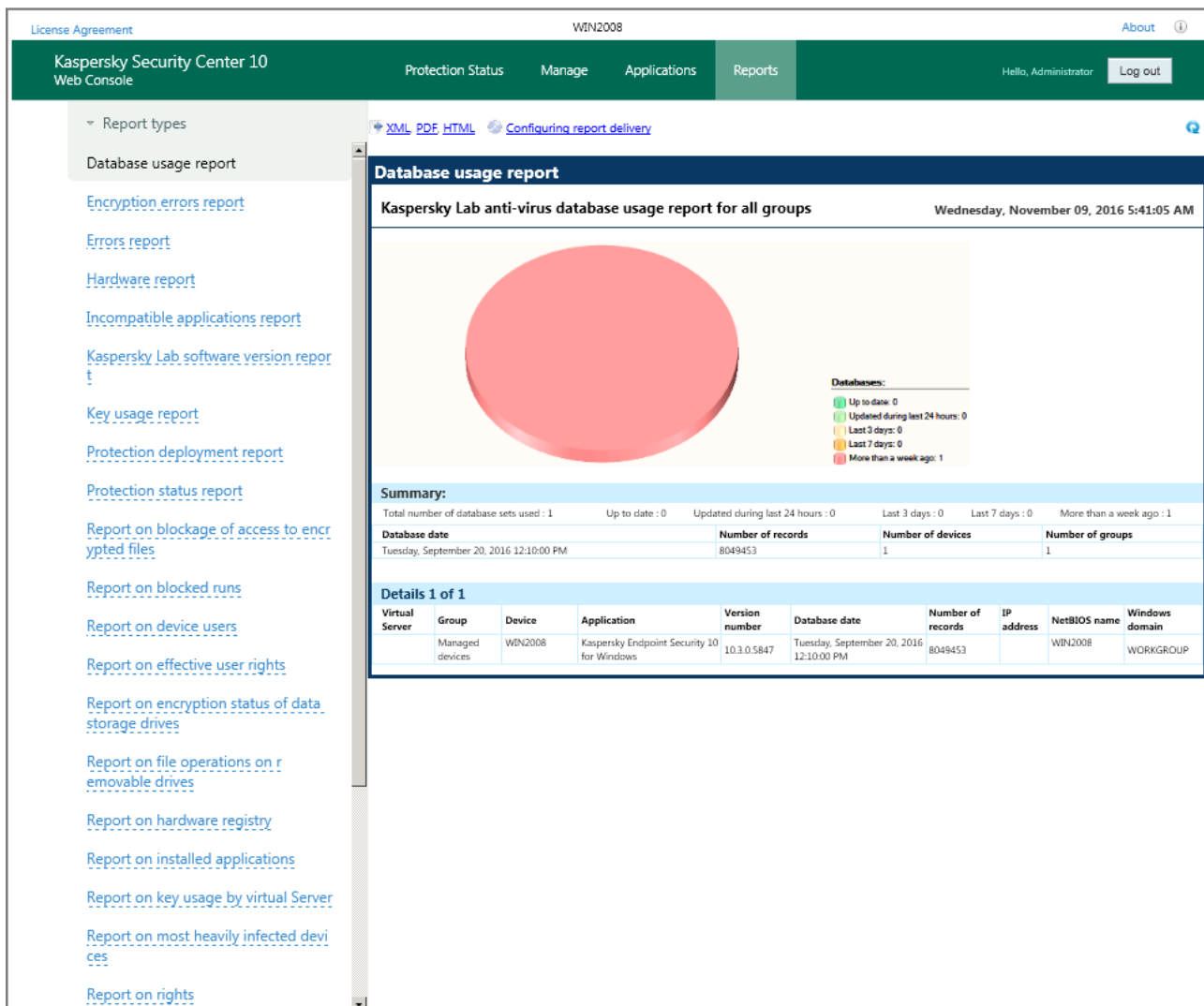



Figure 17. Viewing reports

In the right part of the window, the report contents are displayed. In the upper-right part of the window, the date and time of the report creation are displayed.

You can update the report contents to view updated data.

► *To update report contents:*

Click  in the top right corner of the window.

Exporting reports

► *To export a report:*

1. Open the main application window (see section "Application interface" on page [15](#)).
2. Select the **Reports** tab.
3. In the left part of the window, click a report that you want to export.

In the right part of the window, the report contents are displayed.

4. In the upper part of the window, click the link for the export format you want:
 - To export a report in XML format, click **XML**.
 - To export a report in PDF format, click **PDF**.
 - To export a report in HTML format, click the **HTML**.

The report in the selected format opens in the web browser window or in the window of a viewing application associated with the selected format (such as Acrobat® Reader, for .pdf).

5. Save the report to file by using browser tools or the viewing application.

Configuring report delivery

► *To configure report delivery by email:*

1. Open the main application window (see section "Application interface" on page [15](#)).
2. Select the **Reports** tab.
3. Click the link in the upper part of the main window to open the **Configuring report delivery** window.
4. In the list of reports, select the check boxes next to reports that you want to include in the delivery. If you want to include all reports in the delivery, select the check box next to **Report type**.
5. Create a delivery list containing recipient email addresses:
 - To add an email address to the delivery list:
 - a. Enter the email address in the **Recipient's address** text box.
 - b. Press **Enter**.

The new email address is displayed in the delivery list.
 - To remove an email address from the delivery list, select an address that you want to remove and click the **Remove** button.
 - To modify an email address in the delivery list:
 - a. In the delivery list select the email address that you intend to modify.

The selected email address is displayed in the **Recipient's address** field.
 - b. Change the email address in the **Recipient's address** field, and press **Enter**.

The new email address is displayed in the delivery list.
6. Click the **Save** button.

The notification delivery settings are applied immediately.

Changing your account password

You can change the password of your account after you sign in to Kaspersky Security Center 10 Web Console. You might have to change your password, for example, if you want to set an account password that is easier to remember.

► *To change the password of your account:*

1. Open the main application window (see section "Application interface" on page [15](#)).
2. In the upper-right corner of the screen, click **Change password** to open the **Change password** window.
3. In the **New password** and **Confirm password** text boxes enter the new password.
4. Click the **Change password** button.

The password of your account is changed.

Exiting Kaspersky Security Center 10 Web Console

You can log off Kaspersky Security Center 10 Web Console from any tab of the application interface.

To exit the application, you should first log off Kaspersky Security Center 10 Web Console.

If you exit the browser without logging off (for example, by closing the window or the browser tab), the session remains active for the next 24 hours.

- ▶ *To log off Kaspersky Security Center 10 Web Console,*
from the main application window (see section "Application interface" on page [15](#)), click the **Log out** link in the top right corner of the window.

You have just logged off Kaspersky Security Center 10 Web Console. In the browser, an entry window for user name and password opens (see section "Connecting to Administration Server" on page [18](#)).

Glossary

A

Administration group

A set of devices grouped together in accordance with the performed functions and the Kaspersky Lab applications installed on those devices. Devices are grouped for convenience of management as one single entity. A group can include other groups. A group can contain group policies for each application installed in it and appropriate group tasks.

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.

Anti-virus protection service provider

An organization that provides a client organization with anti-virus protection services based on Kaspersky Lab solutions.

Application Shop

Component of Kaspersky Security Center. Application Shop is used for installing applications on Android devices owned by users. Application Shop allows you to publish the apk files of applications and links to applications in Google Play.

C

Client administrator

A staff member of a client organization who is responsible for the anti-virus protection status.

E

EAS device

A mobile device connected to Administration Server over Exchange ActiveSync protocol. Devices with the iOS, Android, and Windows Phone® operating systems can be connected and managed via the Exchange ActiveSync protocol.

H

HTTPS

Secure protocol for data transfer, using encryption, between a web browser and a web server. HTTPS is used to gain access to restricted information, such as corporate or financial data.

I

Installation package

A set of files created for remote installation of a Kaspersky Lab application by using the Kaspersky Security Center 10 Web Console remote administration system. An installation package is created

based on special files with the .kpd and .kud extensions that are included in the application distribution package; it contains a set of settings required for application setup and its configuration for normal functioning immediately after installation. Parameter values correspond to application defaults.

iOS MDM device

A mobile device that is connected to the iOS MDM Server over the iOS MDM protocol. Devices running on iOS operating system can be connected and managed over iOS MDM protocol.

J

JavaScript

A programming language that expands the performance of web pages. Web pages created using JavaScript can perform functions (for example, change the view of interface elements or open additional windows) without refreshing the web page with new data from a web server. To view pages created by using JavaScript, enable the JavaScript support in the configuration of your browser.

K

KES device

A mobile device that is connected to Administration Server and managed through Kaspersky Endpoint Security for Android.

L

Local installation

Installation of a security application on a device in a corporate network that presumes manual installation startup from the distribution package of the security application or manual startup of a published installation package that was pre-downloaded to the device.

M

Managed devices

Corporate networked devices that are included in an administration group.

Manual installation

Installation of a security application on a device in the corporate network from the distribution package. Manual installation requires an immediate participation of an administrator or another IT specialist. Usually manual installation is done if remote installation has completed with an error.

N

Network anti-virus protection

A set of technical and organizational measures that lower the risk of allowing viruses and spam to penetrate an enterprise network, and that prevent network attacks, phishing, and other threats. Network security increases when you use security applications and services and when you apply and adhere to the corporate data security policy.

Network protection status

Current protection status, which defines the safety of corporate networked devices. The network protection status includes such factors as installed security applications, usage of keys, and number and types of threats detected.

R

Remote installation

Installation of Kaspersky Lab applications through features provided by Kaspersky Security Center 10 Web Console.

S

Service provider's administrator

A staff member at an anti-virus protection service provider. This administrator performs installation and maintenance jobs for anti-virus protection systems based on Kaspersky Lab anti-virus products and also provides technical support to customers.

SSL

A data encryption protocol on the Internet and local networks. SSL is used in web applications to create a secure connection between a client and a server.

W

Web portal

A means of access over a browser to the features of Kaspersky Security Center 10 Web Console. A web portal consists of web pages that contain text and graphical information and management add-ins for Kaspersky Security Center 10 Web Console. Web pages open in the browser after you log on to the web portal. To log on to a web portal, you must have the web portal address, account name and password.

AO Kaspersky Lab

Kaspersky Lab is an internationally renowned vendor of systems for computer protection against various types of threats, including viruses, malware, spam, network and hacker 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). In Russia, according to IDC, Kaspersky Lab is the first choice among all vendors of computer protection systems for home users (IDC Endpoint Tracker 2014).

Kaspersky Lab was founded in Russia in 1997. Today, Kaspersky Lab is an international group of companies running 34 offices in 31 countries. The company employs more than 3,000 qualified experts.

Products. Kaspersky Lab products provide protection for all systems, ranging from home computers to large corporate networks.

The personal product range includes applications that provide information security for desktop, laptop, and tablet computers, as well as for smartphones and other mobile devices.

The company offers solutions and technologies for protection and control of workstations and mobile devices, virtual machines, file servers and web servers, mail gateways, and firewalls. The company's portfolio also includes dedicated products aimed at protection against DDoS attacks, protection of environments managed with industrial control systems, and fraud prevention. Used in conjunction with the centralized management tools of Kaspersky Lab, these solutions ensure effective automated protection against computer threats for organizations of any scale. Kaspersky Lab products are certified by 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 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 add the corresponding signatures to 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 the program kernel of Kaspersky Anti-Virus is integrated in products made by many other software vendors, 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, and 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. For example, in 2014, tests and research conducted by the renowned Austrian anti-virus lab AV-Comparatives rated Kaspersky Lab as one of the two leaders in the number of Advanced+ certificates awarded, which earned the company the Top Rated certificate. However, the main achievement of Kaspersky Lab is the loyalty of its users worldwide. The company's products and technologies protect more than 400 million users, and its corporate clients number more than 270,000.

Kaspersky Lab website <http://www.kaspersky.com>

Virus encyclopedia: <https://securelist.com>

Anti-Virus Lab: <https://newvirus.kaspersky.com/> (for scanning unknown files and websites)

Kaspersky Lab web forum: <http://forum.kaspersky.com>

Information about third-party code

Information about third-party code is contained in the file legal_notices.txt. In Kaspersky Security Center 10 Web Console, you can view information from legal_notices.txt in the **About the program** window by clicking the **Information about third-party code** link.

Trademark notices

The registered trademarks and service marks are the property of their owners.

Acrobat is either registered trademark or trademark of Adobe Systems Incorporated in the United States and/or elsewhere.

The Bluetooth word, mark and logos are owned by Bluetooth SIG, Inc.

Android, Chrome, Google, Google Play, Google Maps, and YouTube are trademarks of Google, Inc.

Active Directory, ActiveSync, Internet Explorer, Microsoft, Windows, and Windows Phone are trademarks of Microsoft Corporation registered in the United States and elsewhere.

AirPlay, AirPrint, Apple, iPhone, iTunes, Mac, Mac OS, OS X, and Safari are trademarks of Apple Inc. registered in the United States and elsewhere.

Cisco and IOS are registered trademarks or trademarks of Cisco Systems, Inc. and / or its affiliates in the United States and elsewhere.

Firefox is a registered trademark of the Mozilla Foundation.

JavaScript, Oracle and Java are registered trademarks of Oracle and/or its affiliates.

Index

A

Account.....	17
name	17
password	17, 89
settings	17
Administration groups	20, 27
Administration Server.....	11, 20
connection	18
Anti-virus protection	
service provider	11
Anti-virus protection service provider	11
Anti-virus security	11
Automatic delivery of reports	85, 88

C

Client	11
Client administrator	6, 11
Computer properties	30
Computer status	20
Computers.....	20

IP address.....	30
list.....	28
managed.....	20, 27, 28, 30
name	20, 30
properties.....	30
unassigned	20, 28, 30
Connection	18
H	
HTTPS	11
I	
Informational area.....	15
Installation	
remote	36
wizard	36
Installation package	34
J	
JavaScript	17
K	
Kaspersky Security Center Web Console.....	11

M

Main window	15
-------------------	----

N

Network protection status	20
---------------------------------	----

P

Policy profile	54
----------------------	----

Protection status	20
-------------------------	----

R

Real-time protection status	20
-----------------------------------	----

Critical	20
----------------	----

OK	20
----------	----

Warning	20
---------------	----

Reports	84, 85
---------------	--------

automatic delivery	85, 88
--------------------------	--------

saving to file	85, 87
----------------------	--------

viewing	85, 86
---------------	--------

S

Security message	20
------------------------	----

list	20
------------	----

Service provider's administrator	11, 34
--	--------

Session	90
closing	90
Software requirements	14
SSL.....	11

W

Web browser	11, 14, 17
Web interface	11
Web portal.....	11
address.....	17