



# Kaspersky Security Center 10

*Administrator's Guide*

*Application version: 10 Service Pack 2, Maintenance Release 1*

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: 12/13/2016

© 2017 AO Kaspersky Lab. All Rights Reserved.

<http://www.kaspersky.com>

<https://help.kaspersky.com>

<http://support.kaspersky.com>

# Table of Contents

About this document .....	14
In this document.....	14
Document conventions .....	17
Sources of information about the application.....	19
Sources for unassisted search of information.....	19
Discussing Kaspersky Lab applications on the forum .....	21
Kaspersky Security Center .....	22
What's new.....	23
Distribution kit.....	27
Hardware and software requirements.....	28
Application interface.....	43
Main application window.....	44
Console tree.....	45
Workspace .....	50
Workspace elements.....	51
Set of information blocks.....	53
Data filtering block .....	53
Context menu.....	55
Configuring the interface .....	55
Application licensing.....	58
About the End User License Agreement.....	58
About the license .....	59
About the license certificate .....	60
About key .....	60
Kaspersky Security Center licensing options.....	61
About restrictions of the main functionality .....	64
About the activation code .....	65
About the key file .....	65
About the subscription .....	66

Administration Server Quick Start Wizard .....	67
Basic concepts .....	68
Administration Server .....	68
Administration Servers hierarchy .....	69
Virtual Administration Server .....	70
Mobile device server .....	71
Web server .....	72
Network Agent Administration group .....	73
Administrator's workstation.....	74
Application management plug-in .....	75
Policies, application settings, and tasks.....	75
How local application settings relate to policies .....	78
Update agent.....	79
Managing Administration Servers.....	82
Connecting to an Administration Server and switching between Administration Servers.....	82
Access rights to Administration Server and its objects.....	85
Conditions of connection to an Administration Server via the Internet .....	86
Secure connection to Administration Server.....	87
Authenticating the Server when a device is connected .....	88
Administration Server authentication during Administration Console connection .....	88
Administration Server certificate .....	88
Disconnecting from an Administration Server.....	89
Adding an Administration Server to the console tree .....	89
Removing an Administration Server from the console tree.....	90
Changing an Administration Server service account. Utility tool klsrvswch .....	90
Viewing and modifying the settings of an Administration Server .....	91
Adjusting the general settings of Administration Server .....	92
Event processing and storage on the Administration Server.....	92
Control of virus outbreaks .....	93
Limiting traffic .....	94
Configuring Web Server.....	94
Working with internal users .....	94

Managing administration groups .....	95
Creating administration groups .....	96
Moving administration groups .....	98
Deleting administration groups.....	99
Automatic creation of a structure of administration groups.....	100
Automatic installation of applications to devices in an administration group.....	102
Managing applications remotely .....	103
Managing policies .....	103
Creating a policy.....	105
Displaying inherited policy in a subgroup .....	106
Activating a policy.....	106
Activating a policy automatically at the Virus outbreak event.....	107
Applying an out-of-office policy.....	107
Modifying a policy. Rolling back changes.....	107
Deleting a policy .....	108
Copying a policy .....	108
Exporting a policy .....	109
Importing a policy .....	109
Converting policies .....	110
Managing policy profiles .....	110
About the policy profile.....	110
Creating a policy profile.....	113
Modifying a policy profile.....	114
Removing a policy profile.....	115
Managing tasks.....	116
Creating a group task.....	117
Creating an Administration Server task.....	118
Creating a task for specific devices .....	119
Creating a local task.....	120
Displaying an inherited group task in the workspace of a nested group.....	120
Automatically turning on devices before starting a task.....	121
Automatically turning off a device after a task is completed.....	121
Limiting task run time .....	122
Exporting a task.....	122

Importing a task .....	123
Converting tasks .....	123
Starting and stopping a task manually .....	124
Pausing and resuming a task manually .....	125
Monitoring task execution .....	125
Viewing task run results stored on Administration Server .....	126
Configuring filtering of information about task run results.....	126
Modifying a task. Rolling back changes .....	127
Viewing and editing the local application settings .....	128
Managing client devices.....	129
Connecting client devices to the Administration Server .....	130
Manually connecting a client device to the Administration Server. KImover utility .....	131
Tunneling the connection between a client device and the Administration Server .....	133
Remotely connecting to the desktop of a client device .....	133
Configuring the restart of a client device.....	136
Auditing actions on a remote client device .....	137
Checking the connection between a client device and the Administration Server .....	138
Automatically checking the connection between a client device and the Administration Server.....	139
Manually checking the connection between a client device and the Administration Server. KInagchk utility .....	139
Identifying client devices on the Administration Server .....	140
Adding devices to an administration group.....	141
Changing the Administration Server for client devices.....	142
Remotely turning on, turning off, and restarting client devices .....	143
Sending a message to device users .....	144
Controlling changes in the status of virtual machines .....	144
Automatic device tagging .....	145
Remote diagnostics of client devices. Kaspersky Security Center remote diagnostics utility.....	147
Connecting the remote diagnostics utility to a client device .....	148
Enabling and disabling tracing, downloading the trace file.....	151
Downloading application settings .....	151

Downloading event logs .....	152
Starting diagnostics and downloading its results .....	152
Starting, stopping and restarting applications .....	153
Managing user accounts .....	154
Handling user accounts .....	155
Adding a user account .....	156
Configuring the check of the name of an internal user for uniqueness .....	157
Adding a user group .....	158
Adding a user to a group .....	159
Configuring rights. User roles .....	160
Adding a user role .....	160
Assigning a role to a user or a user group .....	161
Assigning the user as a device owner .....	162
Delivering messages to users .....	163
Viewing the list of user mobile devices .....	164
Installing a certificate for a user .....	164
Viewing the list of certificates handed to a user .....	165
Working with reports, statistics, and notifications .....	166
Working with reports .....	166
Creating a report template .....	167
Creating and viewing a report .....	168
Saving a report .....	168
Creating a report delivery task .....	169
Working with statistical information .....	169
Configuring event notification .....	171
Creating a certificate for an SMTP server .....	172
Event selections .....	173
Viewing an event selection .....	174
Customizing an event selection .....	174
Creating an event selection .....	175
Exporting event selection to text file .....	175
Deleting events from selection .....	175
Exporting events to an SIEM system .....	176
Device selections .....	177

Viewing a device selection .....	178
Configuring a device selection .....	178
Creating a device selection .....	179
Exporting the settings of a device selection to a file .....	179
Creating a device selection by using imported settings .....	180
Removing devices from administration groups in a selection.....	180
Policies .....	181
Tasks .....	181
Unassigned devices .....	182
Network poll .....	182
Viewing and modifying the settings for Windows network polling .....	183
Viewing and modifying Active Directory group properties .....	184
Viewing and modifying the settings for IP subnet polling.....	184
Working with Windows domains. Viewing and changing the domain settings .....	185
Working with IP subnets .....	185
Creating an IP subnet.....	186
Viewing and changing the IP subnet settings .....	186
Working with the Active Directory groups. Viewing and modifying group settings .....	187
Creating rules for moving devices to administration groups automatically.....	187
Using VDI dynamic mode on client devices.....	188
Enabling VDI dynamic mode in the properties of an installation package for Network Agent.....	189
Searching for devices making part of VDI .....	189
Moving devices making part of VDI to an administration group .....	190
Managing applications on client devices .....	191
Groups of applications .....	192
Creating application categories .....	194
Configuring application startup management on client devices .....	195
Viewing the results of statistical analysis of startup rules applied to executable files.....	196
Viewing the applications registry .....	197
Creating licensed applications groups.....	198
Managing keys for licensed applications groups.....	198
Kaspersky Security Center software inventory .....	200



Inventory of executable files .....	201
Viewing information about executable files .....	201
Software vulnerabilities .....	202
Viewing information about software vulnerabilities .....	203
Scanning applications for vulnerabilities .....	203
Fixing vulnerabilities in applications .....	204
Software updates .....	205
Viewing information about available updates .....	207
Synchronizing updates from Windows Update with Administration Server .....	208
Automatic installation of Kaspersky Endpoint Security updates on devices .....	208
Offline mode for downloading updates .....	211
Enabling and disabling the offline mode for downloading updates .....	213
Installing updates on devices manually .....	215
Configuring Windows updates in a Network Agent policy .....	217
Remote installation of operating systems and applications .....	219
Creating images of operating systems .....	221
Adding drivers for Windows Preinstallation Environment (WinPE) .....	222
Adding drivers to an installation package with an operating system image .....	223
Configuring sysprep.exe utility .....	224
Deploying operating systems on new networked devices .....	225
Deploying operating systems on client devices .....	226
Creating installation packages of applications .....	226
Issuing a certificate for installation packages of applications .....	227
Installing applications on client devices .....	228
Mobile Device Management .....	229
Managing mobile devices using an MDM policy .....	229
Handling commands for mobile devices .....	232
Commands for mobile device management .....	232
Using Google Firebase Cloud Messaging .....	235
Sending commands .....	236
Viewing the statuses of commands in the command log .....	237
Handling certificates .....	238
Installing a certificate .....	239
Configuring certificate handing rules .....	239

Integration with the public keys infrastructure .....	242
Enabling support of Kerberos Constrained Delegation.....	243
Adding a mobile device to the list of managed devices .....	244
Managing Exchange ActiveSync mobile devices .....	249
Adding a management profile .....	250
Removing a management profile.....	251
Viewing information about an EAS device .....	252
Disconnecting an EAS device from management.....	253
Managing iOS MDM devices .....	253
Issuing a certificate for an iOS MDM profile .....	254
Adding a configuration profile .....	255
Installing a configuration profile to a device .....	256
Removing a configuration profile from a device.....	257
Adding provisioning profile.....	258
Installing a provisioning profile to a device.....	259
Removing a provisioning profile from a device .....	260
Adding a managed application.....	261
Installing an app on a mobile device .....	262
Removing an app from a device .....	264
Installing Kaspersky Safe Browser on a mobile device .....	265
Viewing information about an iOS MDM device.....	266
Disconnecting an iOS MDM device from management .....	266
Managing KES devices .....	267
Creating a mobile applications package for KES devices .....	267
Enabling two-factor authentication of KES devices .....	268
Viewing information about a KES device .....	269
Disconnecting a KES device from management.....	270
Self Service Portal.....	271
About Self Service Portal.....	271
Adding a device .....	274
Connecting a user to Self Service Portal .....	275
Encryption and data protection .....	278
Viewing the list of encrypted devices .....	279
Viewing the list of encryption events .....	280

Exporting the list of encryption events to a text file .....	281
Creating and viewing encryption reports.....	281
Inventory of equipment detected on the network .....	284
Adding information about new devices .....	285
Configuring criteria used to define enterprise devices .....	286
Updating databases and software modules .....	287
Creating the download updates to the repository task .....	288
Creating a task for forcing the downloading of updates to the repositories of update agents .....	290
Configuring the download updates to the repository task .....	291
Verifying downloaded updates .....	291
Configuring test policies and auxiliary tasks .....	293
Viewing downloaded updates.....	294
Automatic distribution of updates .....	295
Distributing updates to client devices automatically.....	295
Distributing updates to slave Administration Servers automatically.....	296
Installing updates for program modules of Network Agents automatically .....	297
Assigning devices to act as update agents .....	298
Removing a device from the list of update agents .....	300
Downloading updates by update agents .....	301
Rolling back installed updates.....	302
Working with application keys.....	303
Viewing information about keys in use.....	303
Adding a key to the Administration Server repository .....	304
Deleting an Administration Server key.....	305
Deploying a key to client devices .....	305
Automatic distribution of a key .....	306
Creating and viewing a key usage report .....	307
Data repositories .....	308
Exporting a list of repository objects to a text file .....	309
Installation packages .....	309
Quarantine and Backup.....	309
Enabling remote management for files in the repositories.....	311
Viewing properties of a file placed in repository.....	311

Removing files from repositories .....	312
Restoring files from repositories .....	312
Saving a file from repositories to disk.....	313
Scanning files in Quarantine .....	313
Unprocessed files .....	314
Disinfecting unprocessed files .....	314
Saving an unprocessed file to disk .....	314
Deleting files from the Unprocessed files folder.....	315
Kaspersky Security Network (KSN).....	316
About KSN .....	316
About data provision .....	317
Setting up the access to KSN.....	318
Enabling and disabling KSN.....	320
Viewing the KSN proxy server statistics .....	321
Contacting the Technical Support Service .....	322
How to obtain technical support .....	322
Technical support by phone .....	323
Technical Support via Kaspersky CompanyAccount.....	323
Appendices.....	325
Advanced features .....	325
Kaspersky Security Center operation automation. Utility tool klakaut.....	326
Mobile users .....	326
Events in application operation.....	330
Defining the importance level of an event when a licensing restriction is exceeded.....	331
Event notifications displayed by running an executable file .....	331
Managing Kaspersky Security for Virtualization.....	332
Monitoring the anti-virus protection status using information from the system registry .....	333
Clusters and server arrays .....	334
Algorithm of installation of a patch for a Kaspersky Lab application in cluster mode .....	335
Finding devices.....	336
Connecting to devices through Windows Desktop Sharing.....	337

About the accounts in use.....	338
Custom tools.....	338
Exporting lists from dialog boxes .....	339
Network Agent disk cloning mode .....	339
Preparing a Linux device to remote installation of Network Agent.....	341
Backup copying and restoration of Administration Server data.....	343
Data backup and recovery in interactive mode .....	350
Installing an application using Active Directory group policies .....	351
Features of using the management interface .....	353
How to return to a properties window that disappeared .....	353
How to navigate the console tree .....	354
How to open the object properties window in the workspace.....	354
How to select a group of objects in the workspace.....	354
How to change the set of columns in the workspace.....	355
Reference information .....	355
Using an update agent as gateway .....	356
Using masks in string variables .....	357
Context menu commands .....	357
About connections manager .....	361
User's rights to manage Exchange ActiveSync mobile devices .....	362
About the administrator of virtual Server .....	364
List of managed devices Description of columns.....	364
Statuses of devices, tasks, and policies .....	368
File status icons in Administration Console.....	370
Using regular expressions in the search field .....	371
Glossary.....	373
AO Kaspersky Lab .....	384
Information about third-party code.....	386
Enhanced protection with Kaspersky Security Network .....	387
Trademark notices .....	388
Index.....	390

---

# About this document

Kaspersky Security Center 10 ("Kaspersky Security Center") Administrator's Guide is intended for professionals who install and administer Kaspersky Security Center, as well as for those who provide technical support to organizations that use Kaspersky Security Center.

This guide provides instructions on how to configure and use Kaspersky Security Center.

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

## In this section:

In this document .....	<a href="#">14</a>
Document conventions .....	<a href="#">17</a>

## In this document

Kaspersky Security Center Administrator's Guide contains an introduction, sections that describe the application interface, settings, and maintenance, sections that describe how to manage main tasks, and a glossary.

### Sources of information about the application (see page [19](#))

This section lists the sources of information about the application.

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

### Kaspersky Security Center (see page [22](#))

The section contains information on the purpose of Kaspersky Security Center, and its main features and components.

### **Application interface (see page [43](#))**

This section describes the main interface elements of Kaspersky Security Center, as well as how to configure the interface.

### **Application licensing (see page [58](#))**

This section provides information about general concepts related to the application licensing.

### **Quick Start Wizard (see page [67](#))**

This section provides information about the Administration Server Quick Start Wizard operation.

### **Basic concepts (see page [68](#))**

This section explains basic concepts related to Kaspersky Security Center.

### **Managing Administration Servers (see page [82](#))**

This section provides information about how to handle Administration Servers and how to configure them.

### **Managing administration groups (see page [95](#))**

This section provides information about how to handle administration groups.

### **Managing applications remotely (see page [103](#))**

This section contains information about how to perform remote management of Kaspersky Lab applications installed on devices by using policies, policy profiles, tasks, and local settings of applications.

### **Managing client devices (see page [129](#))**

This section contains information about working with client devices.

### **Working with reports, statistics, and notifications (see page [166](#))**

This section provides information about how to work with reports, statistics, and selections of events and devices in Kaspersky Security Center, as well as how to configure Administration Server notifications.

### **Unassigned devices (see page [182](#))**

This section provides information about how to manage devices on an enterprise network if they are not included in an administration group.

## **Managing applications on client computers (see page [191](#))**

This section describes how to manage groups of applications and how to update software and fix vulnerabilities that Kaspersky Security Center detects on client devices.

## **Remote installation of operating systems and applications (see page [219](#))**

This section provides information about how to create images of operating systems and deploy them on client computers over the network, as well as how to perform remote installation of applications by Kaspersky Lab and other software vendors.

## **Mobile Device Management (see page [229](#))**

This section describes how to manage mobile devices connected to Administration Server.

## **Self Service Portal (see page [271](#))**

This section contains information about Self Service Portal. The section provides Self Service Portal sign-in instructions, as well as instructions on creating Self Service Portal accounts and adding mobile devices to Self Service Portal.

## **Encryption and data protection (see page [278](#))**

This section provides information about how to manage encryption of data stored on hard drives of various devices and removable drives.

## **Inventory of equipment detected on the network (see page [284](#))**

This section provides information about inventory of hardware connected to the organization's network.

## **Updating databases and software modules (see page [287](#))**

This section describes how to download and distribute updates of databases and software modules using Kaspersky Security Center.

## **Working with application keys (see page [303](#))**

This section describes the features of Kaspersky Security Center related to handling keys of managed Kaspersky Lab applications.

## **Data repositories (see page [308](#))**

This section provides information about data stored on the Administration Server and used for tracking the condition of client devices and servicing them.



## Contacting the Technical Support Service (see page [322](#))

This section provides information about the ways and conditions for providing you technical support.

## Glossary

This section lists terms used in the guide.

## AO Kaspersky Lab (see page [384](#))

This section provides information about Kaspersky Lab.

## Information about third-party code (see page [386](#))

Information about third-party code is contained in a file named legal\_notices.txt and stored in the application installation folder.

## Trademark notices (see page [388](#))

This section contains registered trademark notices.

## 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 in red 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.

Sample text	Document conventions description
<p><b>Example:</b></p> <p>...</p>	<p>Examples are on a blue background under the heading "Example".</p>
<p><i>Update</i> means...</p> <p>The <i>Databases are out of date</i> event occurs.</p>	<p>The following elements are italicized in the text:</p> <ul style="list-style-type: none"> <li>• New terms</li> <li>• Names of application statuses and events</li> </ul>
<p>Press <b>ENTER</b>.</p> <p>Press <b>ALT+F4</b>.</p>	<p>Names of keyboard keys appear in bold and are all uppercase.</p> <p>Names of keys that are connected by a plus sign (+) sign indicate the use of a key combination. These keys must be pressed simultaneously.</p>
<p>Click the <b>Enable</b> button.</p>	<p>Names of application interface elements, such as entry fields, menu items, and buttons, appear in bold.</p>
<p>► <i>To configure task schedule:</i></p>	<p>Introductory phrases of procedures 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> <p><code>Specify the date in MM:DD:YY format.</code></p>	<p>The following types of text content are set off with a special font:</p> <ul style="list-style-type: none"> <li>• Text in the command line</li> <li>• Text of messages displayed on the screen by the application</li> <li>• Data that the user has to enter from the keyboard</li> </ul>
<p>&lt;User name&gt;</p>	<p>Variables are enclosed in angle brackets. Instead of a variable, the corresponding value must be inserted, with angle brackets omitted.</p>

---

# Sources of information about the application

This section lists the sources of information about the application.

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

## In this section:

Sources for unassisted search of information .....	<a href="#">19</a>
Discussing Kaspersky Lab applications on the forum.....	<a href="#">21</a>

## Sources for unassisted search of information

You can use the following sources to find information about Kaspersky Security Center:

- Kaspersky Security Center page on the Kaspersky Lab website.
- Kaspersky Security Center page on the Technical Support Service website.
- Online help.
- Documentation.

If you cannot find a solution for your issue, we recommend that you contact the Kaspersky Lab Technical Support Service (see section "Contacting the Technical Support Service" on page [322](#)).

An Internet connection is required to use online information sources.

## **Kaspersky Security Center page on the Kaspersky Lab website**

On the Kaspersky Security Center page (<http://www.kaspersky.com/security-center>), you can view general information about the application, its functions and features.

The Kaspersky Security Center page contains a link to eStore. There you can purchase or renew the application.

## **Page of Kaspersky Security Center in the Knowledge Base**

*Knowledge Base* is a section on the Technical Support Service website.

On the Kaspersky Security Center page (<http://support.kaspersky.com/ksc10>), you can read articles that provide useful information, recommendations, and answers to frequently asked questions on how to purchase, install, and use the application.

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

## **Online help**

The application includes full help files and context help files.

Full help provides information about how to configure and use Kaspersky Security Center.

Use the context help to find information about windows of Kaspersky Security Center, i.e., the descriptions of various settings of Kaspersky Security Center and the links to the descriptions of tasks that use those settings.

Help can be included in the application or published online on the Kaspersky Lab web resource. If Help is published online, the browser window opens when you call it. An Internet connection is required to view online Help.

## **Documentation**

Application documentation consists of the files of application guides.

The administrator's guide provides information on how to configure and use Kaspersky Security Center.

The implementation guide provides instructions on:

- Plan the application installation (taking into account the application operation principles, system requirements, standard deployment schemes, and features of compatibility with other applications).
- Prepare Kaspersky Security Center for installation, installing and activating the application.
- Configure the application after installation.

The Getting Started guide provides information needed to start using the application quickly (a description of the interface and main tasks that can be performed using Kaspersky Security Center).

## Discussing Kaspersky Lab applications on the forum

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

In this forum you can view existing topics, leave your comments, create new topics.

---

# Kaspersky Security Center

The section contains information on the purpose of Kaspersky Security Center, and its main features and components.

Kaspersky Security Center is designed for centralized execution of basic administration and maintenance tasks in an organization's network. The application provides the administrator with access to detailed information about the organization's network security level; it lets you configure all the components of protection based on Kaspersky Lab applications.

Kaspersky Security Center is an application aimed at corporate network administrators and employees responsible for protection of devices in various organizations.

Using Kaspersky Security Center, you can:

- Create a hierarchy of Administration Servers to manage the organization's network, as well as networks at remote offices or client organizations.

The *client organization* is an organization, whose anti-virus protection is ensured by service provider.

- Create a hierarchy of administration groups to manage a selection of client devices as a whole.
- Manage an anti-virus protection system built based on Kaspersky Lab applications.
- Create images of operating systems and deploy them on client devices over the network, as well as performing remote installation of applications by Kaspersky Lab and other software vendors.
- Remotely manage applications by Kaspersky Lab and other software vendors installed on client devices: install updates, find and fix vulnerabilities.
- Perform centralized deployment of keys for Kaspersky Lab applications to client devices, monitor their use, and renew licenses.
- Receive statistics and reports about the operation of applications and devices.

- Receive notifications about critical events in the operation of Kaspersky Lab applications.
- Manage mobile devices that support Kaspersky Security for Android™, Exchange ActiveSync®, or iOS Mobile Device Management (iOS MDM) protocols.
- Manage encryption of information stored on the hard drives of devices and removable drives and users' access to encrypted data.
- Perform inventory of hardware connected to the organization's network.
- Centrally manage files moved to Quarantine or Backup by security applications, as well as manage files for which processing by security applications has been postponed.

### In this section:

What's new.....	<a href="#">23</a>
Distribution kit.....	<a href="#">27</a>
Hardware and software requirements .....	<a href="#">28</a>

## What's new

Changes introduced in Kaspersky Security Center compared to the previous version:

- The maximum number of devices managed through a single Administration Server has been increased up to 100,000.
- Saving of changes made to the settings of Kaspersky Security Center policies, tasks, and Administration Server has been implemented.
- The option of rolling back the settings of an object to a selected object version has been implemented (see section "Modifying a policy. Rolling back changes" on page [107](#)).
- The possibility of filtering the revision history by user and time of modification has been implemented.

- The changeable revision storage period (set on 3 months by default) has been implemented.
- The mechanism of revision comparison has been implemented for policies and tasks.
- Export of policy revisions and task revisions to a text file has been implemented.
- Enhanced diagnostics of the automatic patch installation process. Extra warnings have been added, which are now displayed in the Kaspersky Security Center Setup Wizard when a backup copy of Administration Server data is created:
  - The importance of an available new backup copy of files and distribution packages of the previous version of Kaspersky Security Center and all patches installed is now emphasized.
  - Instructions on how to bypass update failures are now provided.
  - An additional warning displayed to the user in case he or she creates no backup copy of data has been implemented.
- Support of Kaspersky Security Center Network Agent (Windows 8/8.1, MS Surface) by tablet computers running Windows has been implemented.
- Network Agent has been optimized to reduce the Windows loading time on devices with Kaspersky Endpoint Security for Windows and Network Agent installed.
- The Network Agent operation in Windows waiting modes (sleep mode and hibernation) has been optimized.
- The possibility of checking for the latest versions of Kaspersky Lab plug-ins and installation packages has been added to the Kaspersky Security Center Setup Wizard, as well as the possibility of applying any available updates. The Kaspersky Security Center main window now also displays the availability of updates for Kaspersky Security Center plug-ins/programs/applications/components.
- Some of the terms used in Kaspersky Security Center are now replaced with more generic ones to make the application less dependent on other software products. For example, “computer” has been replaced with “device”.



- A new Software Update Installation Wizard has been implemented (see section "Installing updates on devices manually" on page [215](#)).
- The task progress details have been added. The following columns have been added to the list of columns in the **Task results** window:
  - Counters for devices on which a task is running, was completed, or returned an error.
  - Status (with the respective task status description).
- The possibility of manually assigning a name to an installation package has been added.
- A request of user confirmation has been implemented; it is prompted for if the user creates a policy for a Kaspersky Lab application in an administration group, which already has another policy for the same application.
- In the workspace of the **Unassigned devices** folder, the **Configure rules** button has been added for automatic moving unassigned devices (see section "Creating rules for moving devices to administration groups automatically" on page [187](#)).
- The **Run Protection Deployment Wizard** check box has been added to the Quick Start Wizard.
- The workspace pages on the **Statistics** tab of the Administration Server node have been visually delimited.
- Navigation has been improved in automatic tagging rules.
- Role-based access control has been improved in the Administration Server properties.
- A filter has been added for the text description in the **Events** field.
- The possibility of creating tags has been added in policy profile activation rules.
- Quick switching to policy profiles from the workspace of the **Policies** folder and from the **Policies** tab of the Administration Server node has been implemented.
- The possibility of selecting the order of columns has been added in lists.
- The installation package update indicator has been added.

- The Administration Server installation icon has been changed in the Kaspersky Security Center main installation window.
- Definitions have been improved in the Policies and Tasks Conversion Wizard.
- The descriptions of Server flags keys LP\_ConsoleMustUsePort13291 and LP\_InterUserUniqVsScope have been added.
- iOS MDM Server installation has been simplified. The iOS MDM Server Installation Wizard has been implemented.
- Self Service Portal installation has been simplified.
- The New Mobile Device Connection Wizard has been improved.
- The mobile device is no longer locked when the **Locate** and **Alarm** commands are executed (see section "**Commands for mobile device management**" on page [232](#)).
- The administrator can now set the **Critical** or **Warning** status for an Android device manually if access to the Accessibility features has not been granted to Kaspersky Endpoint Security for Android, because Web Protection is inactive in this case.
- Google Firebase Cloud Messaging setup has been simplified. Hints and tips have been added to the application interface.
- The command line backup utility has been implemented for iOS MDM Server.
- The possibility of manually specifying expiration dates of Kaspersky Security for Mobile certificates while issuing (or re-issuing) those certificates has been implemented for the Kaspersky Security Center administrator.
- The display of the Self Service Portal version number has been implemented in the Self Service Portal interface.
- If the **Mobile device support** check box was selected during Kaspersky Security Center installation, all required Mobile Device Management settings and Kaspersky Security for Mobile settings must now be defined in the Kaspersky Security Center Quick Start Wizard.
- The Manage patches and updates feature has been improved.

- The Manage vulnerabilities and patches component has been improved:
- Monitoring and searching for vulnerabilities have been improved.
- Control of actual tasks has been expanded.
- Transmission of events in Syslog (RFC 5424) format to SIEM systems has been implemented (see section "Exporting events to an SIEM system" on page [176](#)).
- The hardware types have been unified in the Kaspersky Security Center interface.
- Information about the results of the **Install required updates and fix vulnerabilities** and **Find vulnerabilities and required updates** tasks has been expanded.
- An additional check before running the **Create installation package upon reference device OS image** task has been implemented. This operation checks the administrator-defined account for the presence of write permissions in the specified shared folder for temporary storage of the image.
- Automatic creation of an incident has been implemented in case the device acting as update agent runs out of disk space (see section "Update agent" on page [79](#)).

## Distribution kit

You can purchase the application through online stores of Kaspersky Lab (for example, <http://www.kaspersky.com>, the **eStore** section) or partner companies.

If you purchase Kaspersky Security Center in an online store, you copy the application from the store's website. Information that is required for application activation is sent to you by email after payment.

For more details on the purchase methods and the distribution kit, please contact the Sales Department.

# Hardware and software requirements

## Administration Server

### Hardware requirements:

- CPU with operating frequency of 1 GHz or higher. For a 64-bit OS, the minimum CPU frequency is 1.4 GHz.
- RAM: 4 GB.
- Available disk space: 10 GB. When using Systems Management, at least 100 GB free disk space shall be available.

### Software requirements:

- Microsoft® Data Access Components (MDAC) 2.8.
- Windows DAC 6.0.
- Microsoft Windows Installer 4.5.

### Operating system:

- Microsoft Windows 10 Home 32-bit / 64-bit.
- Microsoft Windows 10 Pro 32-bit / 64-bit.
- Microsoft Windows 10 Enterprise 32-bit / 64-bit.
- Microsoft Windows 10 Education 32-bit / 64-bit.
- Microsoft Windows 10 Pro RS1 32-bit / 64-bit.
- Microsoft Windows 10 Enterprise RS1 32-bit / 64-bit.
- Microsoft Windows 10 Education RS1 32-bit / 64-bit.
- Microsoft Windows 10 Pro RS2 32-bit / 64-bit.
- Microsoft Windows 10 Enterprise RS2 32-bit / 64-bit.
- Microsoft Windows 10 Education RS2 32-bit / 64-bit.

- Microsoft Windows 8.1 Pro 32-bit / 64-bit.
- Microsoft Windows 8.1 Enterprise 32-bit / 64-bit.
- Microsoft Windows 8 Pro 32-bit / 64-bit.
- Microsoft Windows 8 Enterprise 32-bit / 64-bit.
- Microsoft Windows 7 Professional SP1 32-bit / 64-bit.
- Microsoft Windows 7 Enterprise SP1 32-bit / 64-bit.
- Microsoft Windows 7 Ultimate SP1 32-bit / 64-bit.
- Microsoft Small Business Server 2008 Standard 64-bit.
- Microsoft Small Business Server 2008 Premium 64-bit.
- Microsoft Small Business Server 2011 Essentials 64-bit.
- Microsoft Small Business Server 2011 Premium Add-on 64-bit.
- Microsoft Small Business Server 2011 Standard 64-bit.
- Microsoft Windows Server® 2008 Datacenter SP1 32-bit / 64-bit.
- Microsoft Windows Server 2008 Enterprise SP1 32-bit / 64-bit.
- Microsoft Windows Server 2008 Foundation SP2 32-bit / 64-bit.
- Microsoft Windows Server 2008 SP1 32-bit / 64-bit.
- Microsoft Windows Server 2008 Standard SP1 32-bit / 64-bit.
- Microsoft Windows Server 2008.
- Microsoft Windows Server 2008 SP1.
- Microsoft Windows Server 2008 R2 Server Core 64-bit.
- Microsoft Windows Server 2008 R2 Datacenter 64-bit.
- Microsoft Windows Server 2008 R2 Datacenter SP1 64-bit.
- Microsoft Windows Server 2008 R2 Enterprise 64-bit.
- Microsoft Windows Server 2008 R2 Enterprise SP1 64-bit.
- Microsoft Windows Server 2008 R2 Foundation 64-bit.

- Microsoft Windows Server 2008 R2 Foundation SP1 64-bit.
- Microsoft Windows Server 2008 R2 SP1 Core Mode 64-bit.
- Microsoft Windows Server 2008 R2 Standard 64-bit.
- Microsoft Windows Server 2008 R2 Standard SP1 64-bit.
- Microsoft Windows Server 2012 Server Core 64-bit.
- Microsoft Windows Server 2012 Datacenter 64-bit.
- Microsoft Windows Server 2012 Essentials 64-bit.
- Microsoft Windows Server 2012 Foundation 64-bit.
- Microsoft Windows Server 2012 Standard 64-bit.
- Microsoft Windows Server 2012 R2 Server Core 64-bit.
- Microsoft Windows Server 2012 R2 Datacenter 64-bit.
- Microsoft Windows Server 2012 R2 Essentials 64-bit.
- Microsoft Windows Server 2012 R2 Foundation 64-bit.
- Microsoft Windows Server 2012 R2 Standard 64-bit.
- Windows Storage Server 2008 R2 64-bit.
- Windows Storage Server 2012 64-bit.
- Windows Storage Server 2012 R2 64-bit.
- Windows Server 2016 Datacenter Edition 64-bit.
- Windows Server 2016 Standard Edition 64-bit.

Database server (can be installed on a different computer):

- Microsoft SQL Server® 2008 Express 32-bit.
- Microsoft SQL 2008 R2 Express 64-bit.
- Microsoft SQL 2012 Express 64-bit.
- Microsoft SQL 2014 Express 64-bit.

- Microsoft SQL Server 2008 (all editions) 32-bit / 64-bit.
- Microsoft SQL Server 2008 R2 (all editions) 64-bit.
- Microsoft SQL Server 2008 R2 Service Pack 2 64-bit.
- Microsoft SQL Server 2012 (all editions) 64-bit.
- Microsoft SQL Server 2014 (all editions) 64-bit.
- Microsoft SQL Server 2016 (all editions) 64-bit.
- Microsoft Azure SQL Database.
- MySQL 5.5 32-bit / 64-bit.
- MySQL Enterprise 5.5 32-bit / 64-bit.
- MySQL 5.6 32-bit / 64-bit.
- MySQL Enterprise 5.6 32-bit / 64-bit.
- MySQL 5.7 32-bit / 64-bit.
- MySQL Enterprise 5.7 32-bit / 64-bit.

The following virtual platforms are supported:

- VMware vSphere™ 5.5.
- VMware vSphere 6.
- VMware™ Workstation 12.x Pro.
- Microsoft Hyper-V® Server 2008.
- Microsoft Hyper-V Server 2008 R2.
- Microsoft Hyper-V Server 2008 R2 SP1.
- Microsoft Hyper-V Server 2012.
- Microsoft Hyper-V Server 2012 R2.

- Microsoft Virtual PC 2007 (6.0.156.0).
- Citrix® XenServer® 6.2.
- Citrix XenServer 6.5.
- Citrix XenServer 7.
- Parallels Desktop 11.
- Oracle® VM VirtualBox 4.0.4-70112 (Windows guest operating systems are supported).

### **Kaspersky Security Center 10 Web Console**

#### Hardware requirements:

- CPU with operating frequency of 1 GHz or higher. For a 64-bit OS, the minimum CPU frequency is 1.4 GHz.
- RAM: 512 MB.
- Available disk space: 1 GB.

#### Software requirements:

- For Microsoft Windows operating systems with Kaspersky Security Center Administration Server version Service Pack 2:
  - Microsoft Windows 10 Home 32-bit / 64-bit.
  - Microsoft Windows 10 Pro 32-bit / 64-bit.
  - Microsoft Windows 10 Enterprise 32-bit / 64-bit.
  - Microsoft Windows 10 Education 32-bit / 64-bit.
  - Microsoft Windows 10 Pro RS1 32-bit / 64-bit.
  - Microsoft Windows 10 Enterprise RS1 32-bit / 64-bit.
  - Microsoft Windows 10 Education RS1 32-bit / 64-bit.
  - Microsoft Windows 10 Pro RS2 32-bit / 64-bit.



- Microsoft Windows 10 Enterprise RS2 32-bit / 64-bit.
- Microsoft Windows 10 Education RS2 32-bit / 64-bit.
- Microsoft Windows 8.1 Pro 32-bit / 64-bit.
- Microsoft Windows 8.1 Enterprise 32-bit / 64-bit.
- Microsoft Windows 8 Pro 32-bit / 64-bit.
- Microsoft Windows 8 Enterprise 32-bit / 64-bit.
- Microsoft Windows 7 Professional SP1 32-bit / 64-bit.
- Microsoft Windows 7 Enterprise SP1 32-bit / 64-bit.
- Microsoft Windows 7 Ultimate SP1 32-bit / 64-bit.
- Microsoft Small Business Server 2008 Standard 64-bit.
- Microsoft Small Business Server 2008 Premium 64-bit.
- Microsoft Small Business Server 2011 Essentials 64-bit.
- Microsoft Small Business Server 2011 Premium Add-on 64-bit.
- Microsoft Small Business Server 2011 Standard 64-bit.
- Microsoft Windows Server® 2008 Datacenter SP1 32-bit / 64-bit.
- Microsoft Windows Server 2008 Enterprise SP1 32-bit / 64-bit.
- Microsoft Windows Server 2008 Foundation SP2 32-bit / 64-bit.
- Microsoft Windows Server 2008 SP1 32-bit / 64-bit.
- Microsoft Windows Server 2008 Standard SP1 32-bit / 64-bit.
- Microsoft Windows Server 2008.
- Microsoft Windows Server 2008 SP1.
- Microsoft Windows Server 2008 R2 Server Core 64-bit.
- Microsoft Windows Server 2008 R2 Datacenter 64-bit.

- Microsoft Windows Server 2008 R2 Datacenter SP1 64-bit.
- Microsoft Windows Server 2008 R2 Enterprise 64-bit.
- Microsoft Windows Server 2008 R2 Enterprise SP1 64-bit.
- Microsoft Windows Server 2008 R2 Foundation 64-bit.
- Microsoft Windows Server 2008 R2 Foundation SP1 64-bit.
- Microsoft Windows Server 2008 R2 SP1 Core Mode 64-bit.
- Microsoft Windows Server 2008 R2 Standard 64-bit.
- Microsoft Windows Server 2008 R2 Standard SP1 64-bit.
- Microsoft Windows Server 2012 Server Core 64-bit.
- Microsoft Windows Server 2012 Datacenter 64-bit.
- Microsoft Windows Server 2012 Essentials 64-bit.
- Microsoft Windows Server 2012 Foundation 64-bit.
- Microsoft Windows Server 2012 Standard 64-bit.
- Microsoft Windows Server 2012 R2 Server Core 64-bit.
- Microsoft Windows Server 2012 R2 Datacenter 64-bit.
- Microsoft Windows Server 2012 R2 Essentials 64-bit.
- Microsoft Windows Server 2012 R2 Foundation 64-bit.
- Microsoft Windows Server 2012 R2 Standard 64-bit.
- Windows Storage Server 2008 R2 64-bit.
- Windows Storage Server 2012 64-bit.
- Windows Storage Server 2012 R2 64-bit.
- Windows Server 2016 Datacenter Edition 64-bit.
- Windows Server 2016 Standard Edition 64-bit.

- Debian GNU/Linux® 7.x 32-bit.
- Debian GNU/Linux 7.x 64-bit.
- Ubuntu Server 14.04 LTS 32-bit.
- Ubuntu Server 14.04 LTS 64-bit.
- CentOS 6.x (up to 6.6) 64-bit.

Kaspersky Security Center 10 Web Console does not support versions of operating systems that are compatible with systemd, such as Fedora® 17.

Web server:

- Apache 2.4.25 (for Windows) 32-bit.
- Apache 2.4.25 (for Linux) 32-bit / 64-bit.

You can use the following browsers for working with Kaspersky Security Center 10 Web Console:

- Microsoft Internet Explorer® 9 and 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).

### **iOS Mobile Device Management (iOS MDM) mobile device server**

Hardware requirements:

- CPU with operating frequency of 1 GHz or higher. For a 64-bit OS, the minimum CPU frequency is 1.4 GHz.
- RAM: 2 GB.
- Available disk space: 2 GB.

Software requirements: Microsoft Windows operating system (supported version of the operating system is determined by the requirements of Administration Server).

### **Microsoft Exchange Mobile Devices Server**

All software and hardware requirements for Microsoft Exchange Mobile Devices Server are included in the requirements for the Microsoft Exchange Server.

Working with Microsoft Exchange Server 2007, Microsoft Exchange Server 2010, and Microsoft Exchange Server 2013 is supported.

### **Administration Console**

Hardware requirements:

- CPU with operating frequency of 1 GHz or higher. For a 64-bit OS, the minimum CPU frequency is 1.4 GHz.
- RAM: 512 MB.
- Available disk space: 1 GB.

Software requirements:

- Microsoft Windows operating system (supported version of the operating system is determined by the requirements of Administration Server).
- Microsoft Management Console 2.0.
- Microsoft Windows Installer 4.5.
- Microsoft Internet Explorer 7.0 or later when working with Microsoft Windows XP, Microsoft Windows Server 2003, Microsoft Windows Server 2008, Microsoft Windows Server 2008 R2, or Microsoft Windows Vista®.
- Microsoft Internet Explorer 8.0 or later when using Microsoft Windows 7.
- Microsoft Internet Explorer 10.0 or later when using Microsoft Windows 8 and 10.
- Microsoft Edge when using Microsoft Windows 10.

## Network Agent

Hardware requirements:

- CPU with operating frequency of 1 GHz or higher. For a 64-bit OS, the minimum CPU frequency is 1.4 GHz.
- RAM: 512 MB.
- Available disk space: 1 GB.

If the device with Network Agent installed also acts as update agent, this device must meet the following hardware requirements:

- CPU with operating frequency of 1 GHz or higher. For a 64-bit OS, the minimum CPU frequency is 1.4 GHz.
- RAM: 1 GB.
- Available disk space: 4 GB.

Software requirements:

- Windows Embedded POSReady 7 32-bit / 64-bit.
- Windows Embedded Standard 7 SP1 32-bit / 64-bit.
- Windows Embedded 8 Standard 32-bit / 64-bit.
- Windows Embedded 8 Industry Pro 32-bit / 64-bit.
- Windows Embedded 8 Industry Enterprise 32-bit / 64-bit.
- Windows Embedded 8.1 Industry Pro 32-bit / 64-bit.
- Windows Embedded 8.1 Industry Enterprise 32-bit / 64-bit.
- Windows Embedded 8.1 Industry Update 32-bit / 64-bit.
- Windows 10 Home 32-bit / 64-bit.
- Windows 10 Pro 32-bit / 64-bit.
- Windows 10 Enterprise 32-bit / 64-bit.

- Windows 10 Education 32-bit / 64-bit.
- Windows 10 Home RS1 32-bit / 64-bit.
- Windows 10 Pro RS1 32-bit / 64-bit.
- Windows 10 Enterprise RS1 32-bit / 64-bit.
- Windows 10 Education RS1 32-bit / 64-bit.
- Windows 10 Home RS2 32-bit / 64-bit.
- Windows 10 Pro RS2 32-bit / 64-bit.
- Windows 10 Enterprise RS2 32-bit / 64-bit.
- Windows 10 Education RS2 32-bit / 64-bit.
- Microsoft Windows 2000 Server.
- Windows 8.1 Pro 32-bit / 64-bit.
- Windows 8.1 Enterprise 32-bit / 64-bit.
- Windows 8 Pro 32-bit / 64-bit.
- Windows 8 Enterprise 32-bit / 64-bit.
- Windows 7 Professional SP1 32-bit / 64-bit.
- Windows 7 Enterprise SP1 32-bit / 64-bit.
- Windows 7 Ultimate SP1 32-bit / 64-bit.
- Windows 7 Professional 32-bit / 64-bit.
- Windows 7 Enterprise 32-bit / 64-bit.
- Windows 7 Ultimate 32-bit / 64-bit.
- Windows 7 Home Basic 32-bit / 64-bit.
- Windows 7 Premium 32-bit / 64-bit.
- Windows Vista Business SP1 32-bit / 64-bit.
- Windows Vista Enterprise SP1 32-bit / 64-bit.
- Windows Vista Ultimate SP1 32-bit / 64-bit.

- Windows Vista Business SP2 32-bit / 64-bit.
- Windows Vista Enterprise SP2 32-bit / 64-bit.
- Windows Vista Ultimate SP2 32-bit / 64-bit.
- Windows XP Professional SP3 32-bit.
- Windows XP Professional SP2 32-bit / 64-bit.
- Windows XP Home SP3 32-bit.
- Essential Business Server 2008 64-bit.
- Small Business Server 2003 Standard SP1 32-bit.
- Small Business Server 2003 Premium SP1 32-bit.
- Small Business Server 2008 Standard 64-bit.
- Small Business Server 2008 Premium 64-bit.
- Small Business Server 2011 Essentials 64-bit.
- Small Business Server 2011 Premium Add-on 64-bit.
- Small Business Server 2011 Standard 64-bit.
- Windows Home Server 2011 64-bit.
- Windows MultiPoint™ Server 2011 64-bit.
- Windows Server 2003 Enterprise SP2 32-bit / 64-bit.
- Windows Server 2003 Standard SP2 32-bit / 64-bit.
- Windows Server 2003 R2 Enterprise SP2 32-bit / 64-bit.
- Windows Server 2003 R2 Standard SP2 32-bit / 64-bit.
- Windows Server 2008 Datacenter SP1 32-bit / 64-bit.
- Windows Server 2008 Enterprise SP1 32-bit / 64-bit.
- Windows Server 2008 Foundation SP2 32-bit / 64-bit.
- Windows Server 2008 SP1 Server Core 32-bit / 64-bit.
- Windows Server 2008 Standard SP1 32-bit / 64-bit.

- Windows Server 2008 32-bit / 64-bit.
- Windows Server 2008 R2 Server Core 64-bit.
- Windows Server 2008 R2 Datacenter 64-bit.
- Windows Server 2008 R2 Datacenter SP1 64-bit.
- Windows Server 2008 R2 Enterprise 64-bit.
- Windows Server 2008 R2 Enterprise SP1 64-bit.
- Windows Server 2008 R2 Foundation 64-bit.
- Windows Server 2008 R2 Foundation SP1 64-bit.
- Windows Server 2008 R2 SP1 Core Mode 64-bit.
- Windows Server 2008 R2 Standard 64-bit.
- Windows Server 2008 R2 Standard SP1 64-bit.
- Windows Server 2012 Server Core 64-bit.
- Windows Server 2012 Datacenter 64-bit.
- Windows Server 2012 Essentials 64-bit.
- Windows Server 2012 Foundation 64-bit.
- Windows Server 2012 Standard 64-bit.
- Windows Server 2012 R2 Server Core 64-bit.
- Windows Server 2012 R2 Datacenter 64-bit.
- Windows Server 2012 R2 Essentials 64-bit.
- Windows Server 2012 R2 Foundation 64-bit.
- Windows Server 2012 R2 Standard 64-bit.
- Windows Server 2016 Datacenter Edition.
- Windows Server 2016 Standard Edition.
- Windows Nano Server 2016.
- Windows Storage Server 2008 R2 64-bit.



- Windows Storage Server 2012 64-bit.
- Windows Storage Server 2012 R2 64-bit.
- Debian GNU / Linux 8.x 32-bit.
- Debian GNU / Linux 8.x 64-bit.
- Debian GNU / Linux 7.x (up to 7.8) 32-bit.
- Debian GNU / Linux 7.x (up to 7.8) 64-bit.
- Ubuntu Server 16.04 LTS x32 32-bit.
- Ubuntu Server 16.04 LTS x64 64-bit.
- Ubuntu Server 14.04 LTS x32 32-bit.
- Ubuntu Server 14.04 LTS x64 64-bit.
- Ubuntu Desktop 16.04 LTS x32 32-bit.
- Ubuntu Desktop 16.04 LTS x64 64-bit.
- Ubuntu Desktop 14.04 LTS x32 32-bit.
- Ubuntu Desktop 14.04 LTS x64 64-bit.
- CentOS 6.x (up to 6.6) 64-bit.
- CentOS 7.0 64-bit.
- Red Hat Enterprise Linux Server 7.0 64-bit.
- SUSE Linux Enterprise Server 12 64-bit.
- SUSE Linux Enterprise Desktop 12 64-bit.
- Mac OS X 10.4 (Tiger®).
- Mac OS X 10.5 (Leopard®).
- Mac OS X 10.6 (Snow Leopard®).
- OS X 10.7 (Lion).
- OS X 10.8 (Mountain Lion).
- OS X 10.9 (Mavericks).

- OS X 10.10 (Yosemite).
- OS X 10.11 (El Capitan).
- macOS® Sierra (10.12).
- VMware vSphere™ 5.5.
- VMware vSphere 6.
- VMware Workstation 9.x.
- VMware Workstation 10.x.
- VMware Workstation 11.x.
- VMware Workstation 12.x Pro.
- Microsoft Hyper-V Server 2008.
- Microsoft Hyper-V Server 2008 R2.
- Microsoft Hyper-V Server 2008 R2 SP1.
- Microsoft Hyper-V Server 2012.
- Microsoft Hyper-V Server 2012 R2.
- Citrix XenServer 6.2.
- Citrix XenServer 6.5.
- Citrix XenServer 7.

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 in the System requirements section (<http://support.kaspersky.com/ksc10#requirements>).

---

# Application interface

This section describes the main interface elements of Kaspersky Security Center, as well as how to configure the interface.

Viewing, creation, modification and configuration of administration groups, and centralized management of Kaspersky Lab applications installed on client devices are performed from the administrator's workstation. The management interface is provided by the Administration Console component. It is a specialized stand-alone snap-in that is integrated with Microsoft Management Console (MMC); so the Kaspersky Security Center interface is standard for MMC.

Administration Console allows remote connection to Administration Server over the Internet.

For local work with client devices, the application supports remote connection to a computer through Administration Console by using the standard Microsoft Windows Remote Desktop Connection application.

To use this functionality, you must allow remote connection to the desktop on the client device.

## In this section:

Main application window.....	<a href="#">44</a>
Console tree .....	<a href="#">45</a>
Workspace .....	<a href="#">50</a>
Data filtering block .....	<a href="#">53</a>
Context menu .....	<a href="#">55</a>
Configuring the interface .....	<a href="#">55</a>

# Main application window

The main application window (see the figure below) contains a menu, a toolbar, a console tree, and a workspace. The menu bar allows you to use the windows and provides access to the Help system. The **Action** menu duplicates the context menu commands for the current console tree object.

The set of toolbar buttons provides direct access to some of the menu items. The set of buttons may change depending on the current node or folder selected in the console tree.

The appearance of the workspace of the main window depends on which node (folder) of the console tree it is associated with, and what functions it performs.

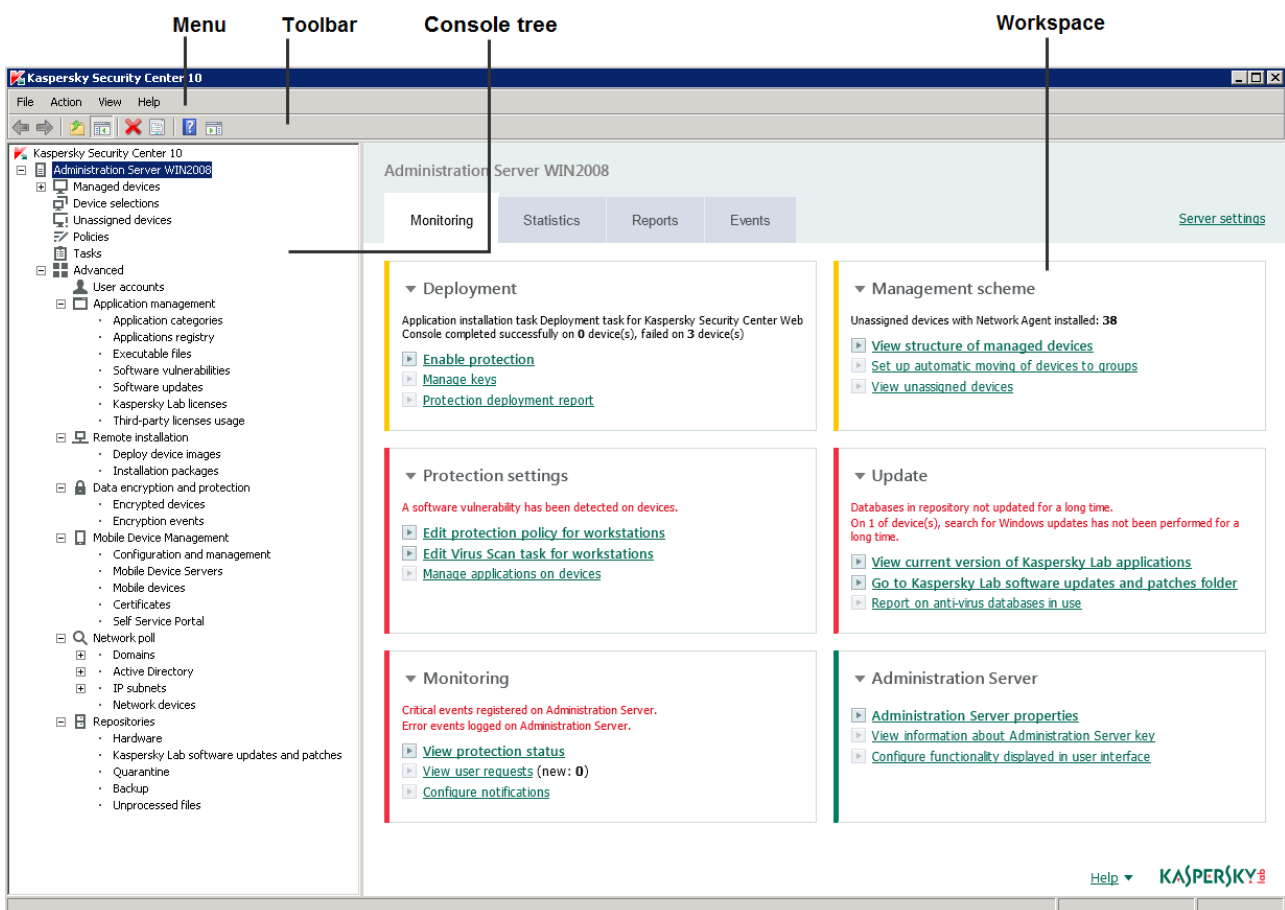


Figure 1. Kaspersky Security Center main application window

# Console tree

The console tree (see the figure below) is designed to display the hierarchy of Administration Servers in the corporate network, the structure of their administration groups, and other objects of the application, such as the **Repositories** or **Application management** folders. The name space of Kaspersky Security Center can contain several nodes including the names of servers corresponding to the installed Administration Servers included in the hierarchy.

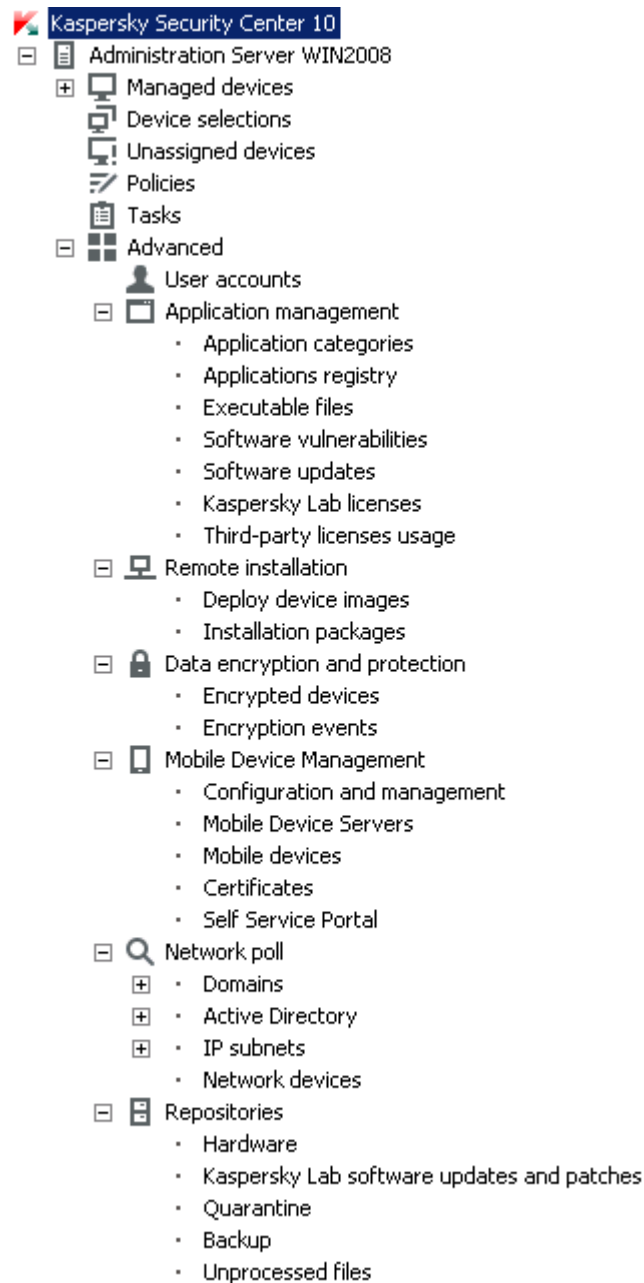


Figure 2. Console tree

## Administration Server node

The **Administration Server – <Device name>** node is a container that shows the structural organization of the selected Administration Server.

The workspace of the **Administration Server** node contains summary information about the current status of the application and devices managed through the Administration Server. Information in the workspace is distributed between various tabs:

- **Monitoring.** The **Monitoring** tab displays information about the application operation and the current status of client devices in real-time mode. Important messages for the administrator (such as messages on vulnerabilities, errors, or viruses detected) are highlighted in a specific color. You can use links on the **Monitoring** tab to perform the standard administrator tasks (for example, install and configure the security application on client devices), as well as to go to other folders of the console tree.
- **Statistics.** Contains a set of charts grouped by topics (protection status, Anti-Virus statistics, updates, etc.). These charts visualize current information about the application operation and the status of client devices.
- **Reports.** Contains templates for reports generated by the application. On this tab, you can create reports using preset templates, as well as create custom report templates.
- **Events.** Contains records on events that have been registered during the application operation. Those records are distributed between topics for ease of reading and filtering. On this tab, you can view selections of events that have been generated automatically, as well as create custom selections.

## Folders in the Administration Server node

The **Administration Server – <Device name>** node includes the following folders:

- **Managed devices.** This folder is intended for storage, display, configuration, and modification of the structure of administration groups, group policies, and group tasks.
- **Device selections.** This folder is intended for quick selection of devices that meet specified criteria (a device selection) among all managed devices. For example, you can quickly select devices on which no security application has been installed, and proceed to these devices (view the list). You can perform certain actions on these selected devices,

for example, assign them some tasks. You can use preset selections or create your own custom selections.

- **Unassigned devices.** This folder contains a list of devices that have not been included in any of the administration groups. You can perform some actions on unassigned devices: move their administration groups or install applications on them.
- **Policies.** This folder is intended for viewing and creating policies.
- **Tasks.** This folder is intended for viewing and creating tasks.
- **Advanced.** This folder contains a set of subfolders that correspond to various groups of application features.

### **Advanced folder. Moving folders in the console tree**

The **Advanced** folder includes the following subfolders:

- **User accounts.** This folder contains a list of network user accounts.
- **Application management.** This folder is intended for managing applications installed on devices in the network. The **Application management** folder contains the following subfolders:
  - **Application categories.** Intended for handling custom application categories.
  - **Applications registry.** Contains a list of applications on devices with Network Agent installed.
  - **Executable files.** Contains the list of executable files stored on client devices with Network Agent installed.
  - **Software vulnerabilities.** Contains a list of vulnerabilities in applications on devices with Network Agent installed.
  - **Software updates.** Contains a list of application updates received by Administration Server that can be distributed on devices.

- **Kaspersky Lab licenses.** Contains a list of available keys for Kaspersky Lab applications. In the workspace of this folder, you can add new keys to the key repository, deploy keys to managed devices, and view the key usage report.
- **Third-party licenses usage.** Contains a list of licensed applications groups. You can use licensed applications groups to monitor the usage of licenses for third-party software (non-Kaspersky Lab applications) and possible violations of licensing restrictions.
- **Remote installation.** This folder is intended for managing remote installation of operating systems and applications. The **Remote installation** folder contains the following subfolders:
  - **Deploy device images.** Intended for deploying images of operating systems on devices.
  - **Installation packages.** Contains a list of installation packages that can be used for remote installation of applications on devices.
- **Mobile Device Management.** This folder is intended for managing mobile devices. The **Mobile Device Management** folder contains the following subfolders:
  - **Mobile devices.** It is intended for managing mobile devices, KES, Exchange ActiveSync, and iOS MDM.
  - **Certificates.** It is intended for managing certificates of mobile devices.
- **Data encryption and protection.** This folder is intended for managing the process of data encryption on hard drives and removable drives.
- **Network poll.** This folder displays the network in which Administration Server is installed. The Administration Server retrieves information about the structure of the network and its devices through regular polls of the Windows network, IP subnets, and Active Directory® in the corporate network. Polling results are displayed in the workspaces of the corresponding folders: **Domains**, **IP subnets**, and **Active Directory**.
- **Repositories.** This folder is intended for operations with objects used to monitor the status of devices and perform maintenance. The **Repositories** folder contains the following subfolders:



- **Kaspersky Lab software updates and patches.** Contains a list of updates received by Administration Server that can be distributed to devices.
- **Hardware.** Contains a list of hardware connected to the organization's network.
- **Quarantine.** Contains a list of objects moved to Quarantine by anti-virus applications on devices.
- **Backup.** This folder contains a list of backup copies of files that were deleted or modified during disinfection on devices.
- **Unprocessed files.** Contains a list of files assigned for later scanning by anti-virus applications.

You can change the set of subfolders included in the **Advanced** folder. Frequently used subfolders can be moved from the **Advanced** folder one level up. Subfolders that are used rarely can be moved to the **Advanced** folder.

► *To move a subfolder out of the **Advanced** folder:*

1. In the console tree, select the subfolder that you want to move out of the **Advanced** folder.
2. In the context menu of the subfolder, select **View** → **Move from Advanced folder**.

You can also move a subfolder out of the **Advanced** folder in the workspace of the **Advanced** folder by clicking the **Move from Advanced folder** link in the section with the name of that subfolder.

► *To move a subfolder to the **Advanced** folder:*

1. In the console tree, select the subfolder that you need to move to the **Advanced** folder.
2. In the context menu of the subfolder, select **View** → **Move to Advanced folder**.

# Workspace

The workspace (see figure below) contains the following elements:

- Lists of objects that the administrator manages through the application (devices, administration groups, user accounts, policies, tasks, event records, other applications, etc.) (see section "Workspace elements" on page 51)
- Controls (buttons that expand lists of commands, links for command execution and proceeding to other console tree folders).
- Text and graphical information (application messages, charts in information panes, statistical and reference information) (see section "Set of information blocks" on page 53).

The contents of the workspace correspond to the node or folder selected in the console tree.

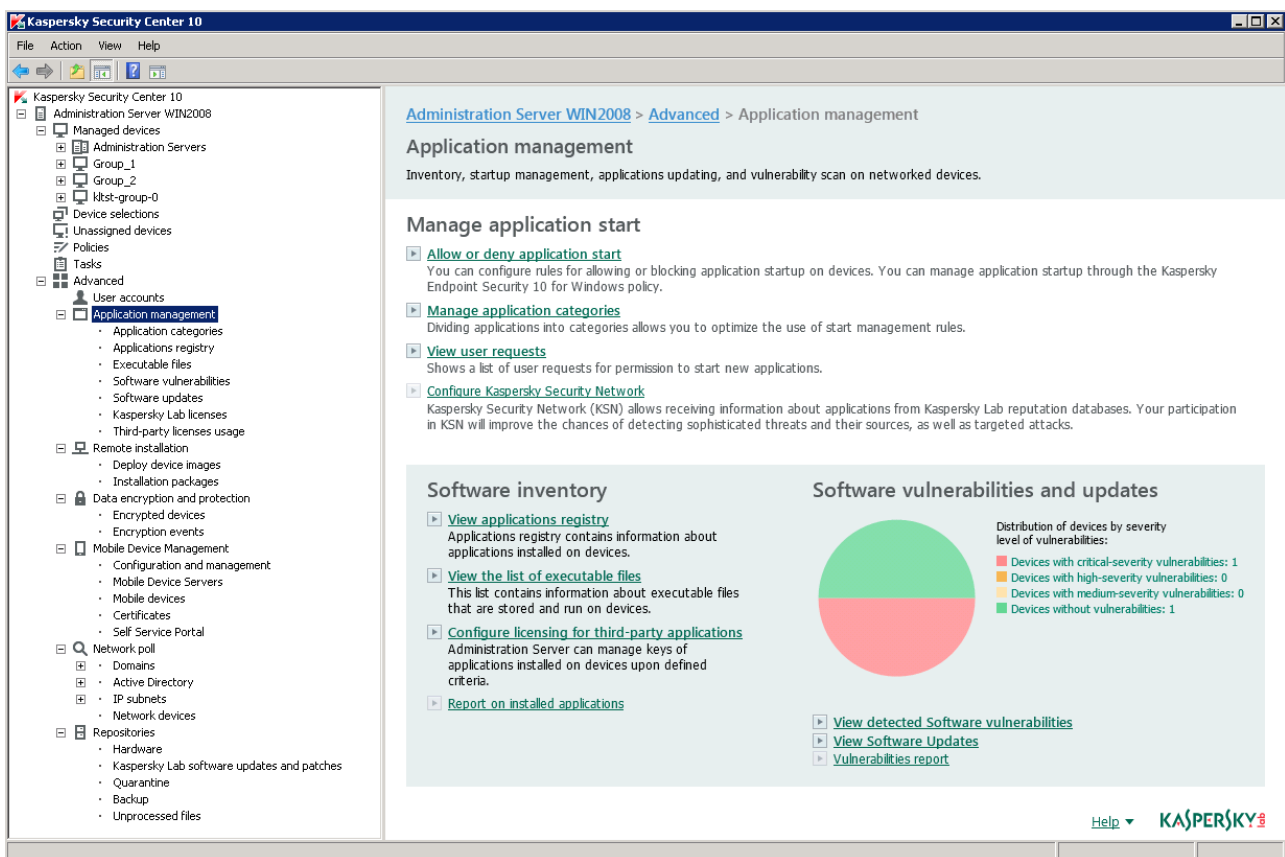


Figure 3. Workspace

The workspace of a node or folder can contain multiple tabs (see the figure below). Each tab corresponds to a specific group (type) of objects or application features.

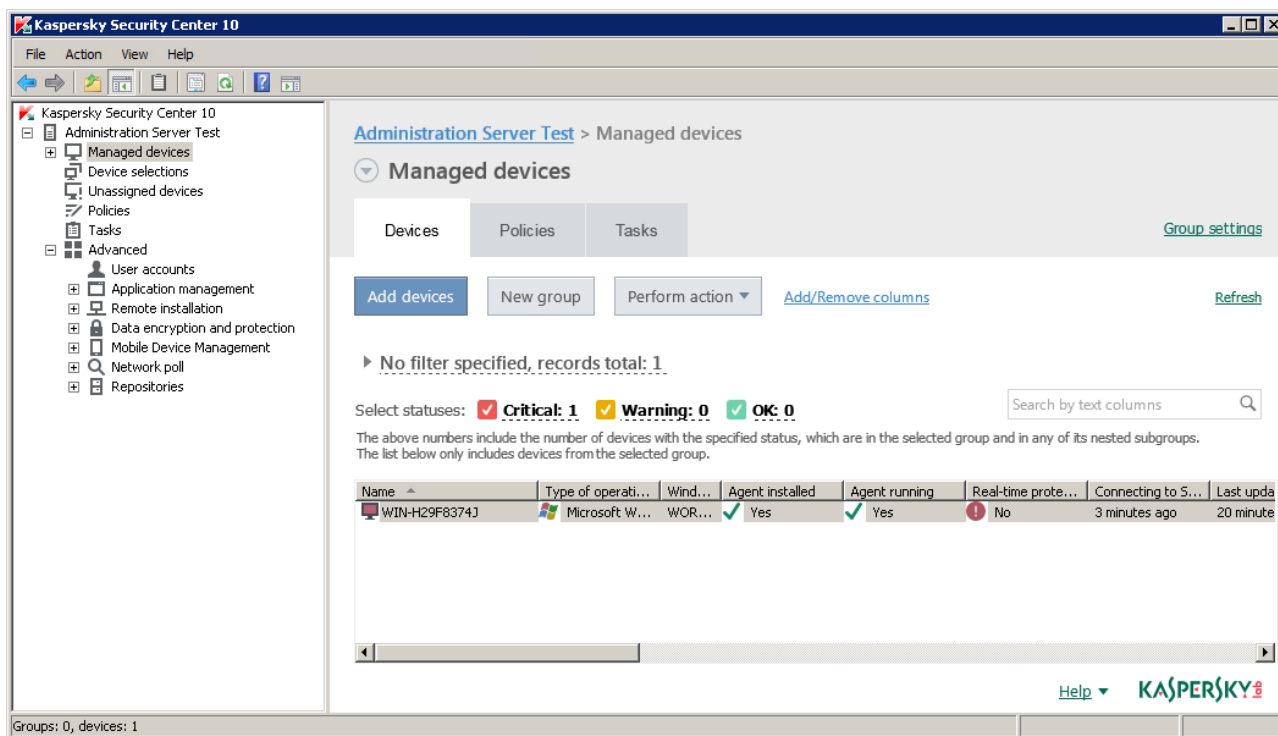


Figure 4. Workspace divided into tabs

## In this section:

Workspace elements.....	51
Set of information blocks .....	53

## Workspace elements

The workspace of a folder or a node can contain the following elements (see the figure below).

- List management block. Contains buttons that expand lists of commands and links. Designed for operations with objects selected in the list.
- List of objects. Contains management objects (such as devices, user accounts, policies, and tasks). You can sort and filter objects on the list, perform actions on them using

the management block and commands from the object context menu. You can also configure the set of columns displayed in the list.

- Block for handling a selected object. Contains summary information about a selected object. This block can also contain links for quick operations with the selected object. For example, the block for handling a selected policy contains a link to the policy settings window.
- Data filtering block. You can use the filtering block to configure the display of objects on the list. For example, you can use the data filtering block to configure the list of devices, so that only those with the Critical status are displayed.

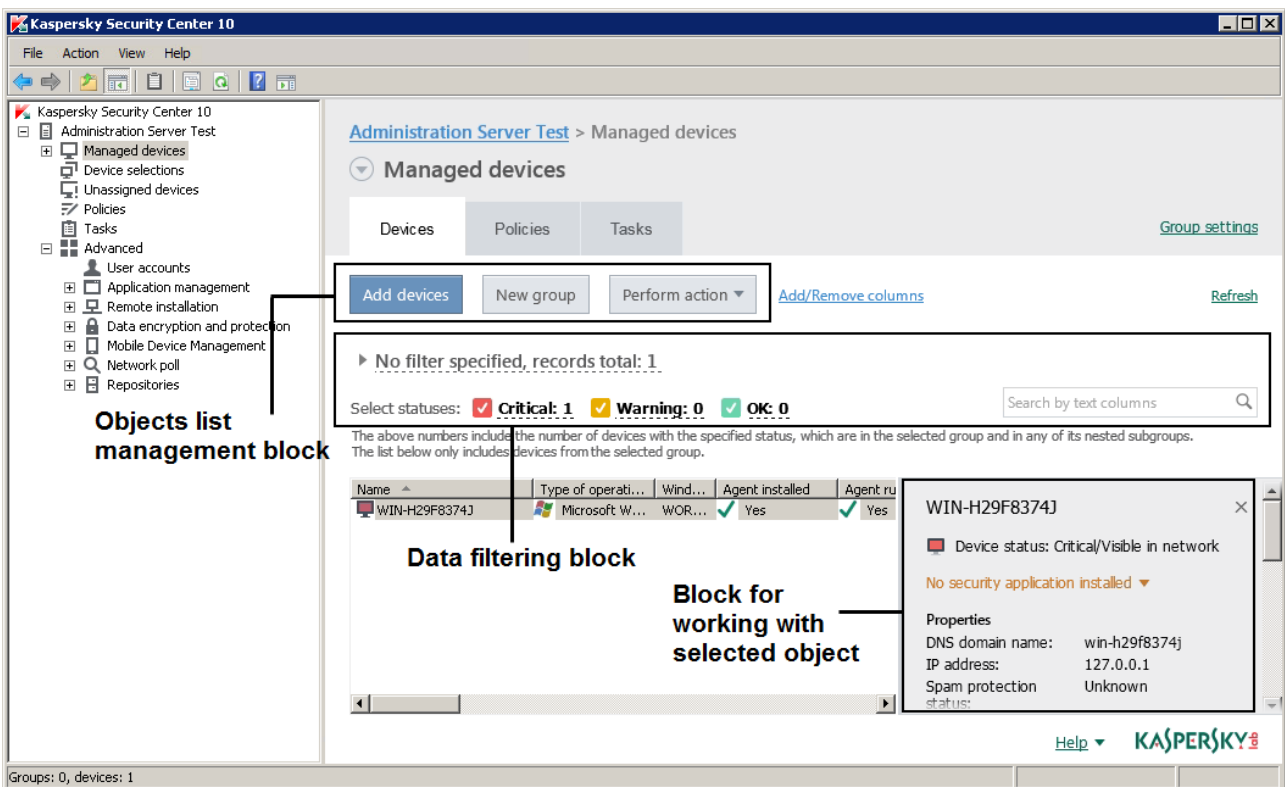


Figure 5. Information area represented by a list of management objects

# Set of information blocks

The workspace of the **Administration Server** node displays statistics on information panes on the **Statistics** tab. Information panes are distributed among a few topics (see the figure below). You can configure the display of data on information panes by changing the types of charts and the set of data presented on them, as well as by modifying and adding information panes or entire pages on the **Statistics** tab (see section "**Working with statistical information**" on page [169](#)).

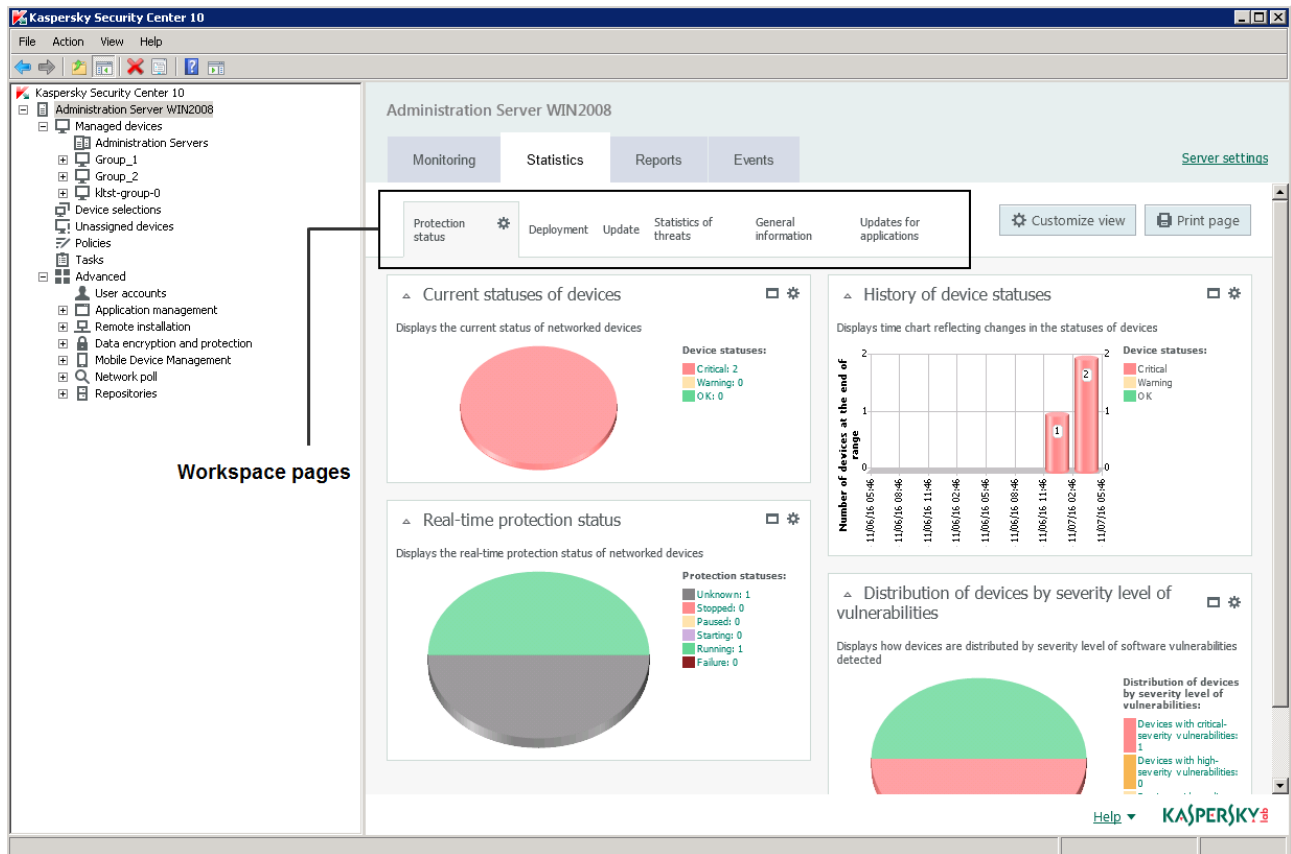
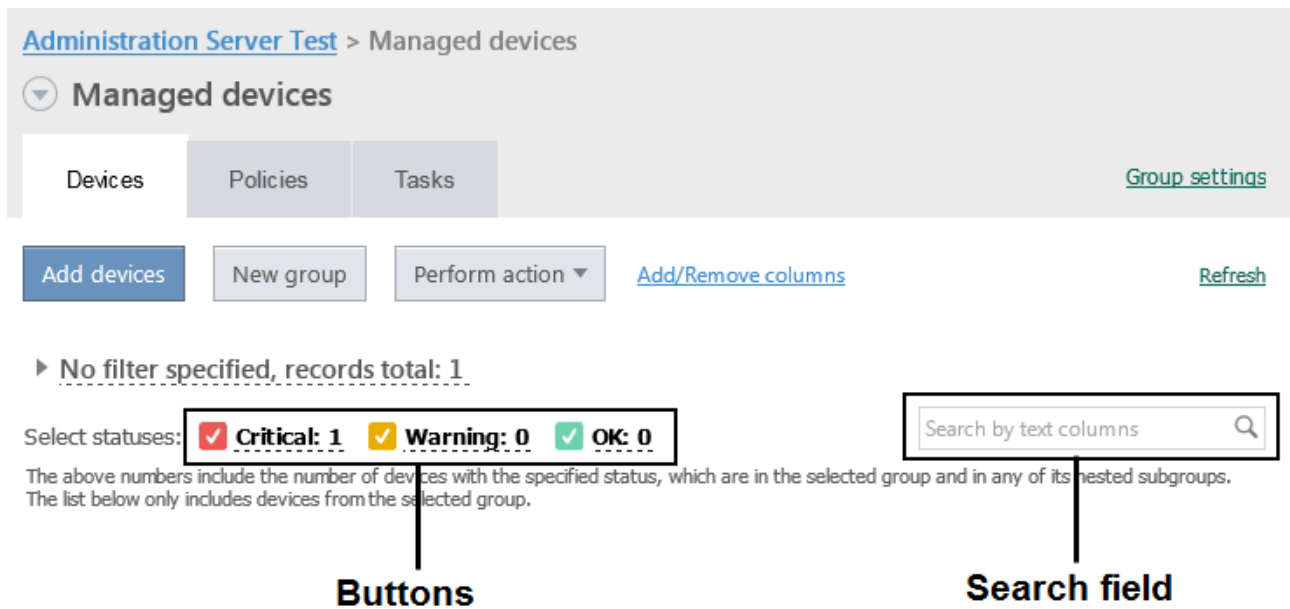


Figure 6. Workspace divided into pages

# Data filtering block

The *data filtering block* (hereinafter also referred to as *filtering block*) is used in workspaces and sections of dialog boxes that contain lists of objects (such as devices, applications, vulnerabilities, or users).

The filtering block can contain a search field, a filter, and buttons (see the figure below).



### Extended filtering block. Filtering settings

You can use the filtering block in standard or extended mode to filter data (see figure). In standard mode of the filtering block, you can filter data using the search field and the buttons in the **Select statuses** section. In extended mode of the filtering block, you can use additional filtering criteria. Additional filtering criteria are available on the **Adjust filter** link.

#### ► To configure filtering.

1. Click the **No filter specified** area.

The right part of the window displays the **Adjust filter** link.

2. Click the **Adjust filter** link to select filtering criteria.

The selected criteria will be displayed on a gray background in the **Filter** field.

3. Specify a value for each criterion (for example, "*Agent installed*").
4. In the **Select statuses** section, configure additional device filtering by statuses (*Critical*, *Warning*, or *OK*).

Devices that pass the filter will be displayed in the list. You can also find devices using keywords and regular expressions (see section "What's new" on page [23](#)) in the **Search** field.

The image displays two examples of filtering blocks in a user interface. The top block, labeled "Standard filtering block", features a header with a dropdown menu showing "No filter specified, records total: 3" and a "Filter setup" link. Below the header are two buttons: "Configure certificate generation rules" and "Integrate with public-key infrastructure", followed by a "Refresh" link. A search box labeled "Search by text columns" is positioned at the bottom right. The bottom block, labeled "Expanded filtering block", has the same header and buttons. It also includes four dropdown menus for filtering: "Type:", "Protocol:", "User:", and "Status:". A search box labeled "Search by text columns" is also present at the bottom right.

## Context menu

In the console tree of Kaspersky Security Center each object features its own context menu. Here the standard commands of the Microsoft Management Console context menu are supplemented with commands used for operations with the object. The additional context menu commands that correspond to various console tree objects are listed in the Appendices (see section "Context menu commands" on page [357](#)).

Some of the objects in the workspace (such as devices on the list of managed devices, or other listed objects) also have a context menu with additional commands.

## Configuring the interface

You can configure the interface of Kaspersky Security Center:

- Show and hide objects in the console tree, workspace, properties windows of objects (folders, sections) depending on the features being used.
- Show and hide elements of the main window (for example, console tree, standard menus such as **Actions** and **View**).

► *To configure the Kaspersky Security Center interface in accordance with the currently used feature:*

1. In the console tree, select the **Administration Server** node.
2. In the application window menu, select **View** → **Configure interface**.
3. In the **Configure interface** window that opens, configure the display of interface elements using the following check boxes:

- **Display Systems Management.**

If this check box is selected, the **Remote installation** folder displays the **Deploy device images** subfolder, while the **Repositories** folder displays the **Hardware** subfolder.

By default, this check box is cleared.

- **Display encryption and data protection.**

If this check box is selected, data encryption management is available on devices connected to the network. After you restart the application, the console tree displays the **Data encryption and protection** folder.

By default, this check box is cleared.

- **Display endpoint control settings.**

If this check box is selected, the following subsections are displayed in the **Endpoint control** section of the properties window of the Kaspersky Endpoint Security 10 for Windows policy:

- **Application Startup Control.**

- **Vulnerability Monitor.**

- **Device Control.**

- **Web Control.**

If this check box is cleared, the above-specified subsections are not displayed in the **Endpoint control** section.

By default, this check box is cleared.



- **Display Mobile Device Management.**

If this check box is selected, the **Mobile Device Management** feature is available. After you restart the application, the console tree displays the **Mobile devices** folder.

By default, this check box is cleared.

- **Display slave Administration Servers.**

If the check box is selected, the console tree displays the nodes of slave and virtual Administration Servers within administration groups.

The functionality connected with slave and virtual Administration Servers – in particular, creation of tasks for remote installation of applications to slave Administration Servers – is available at that.

By default, this check box is selected.

- **Display security settings sections.**

If this check box is selected, the **Security** section is displayed in the properties of Administration Server, administration groups and other objects. This check box allows you to give custom permissions for working with objects to users and groups of users.

By default, this check box is selected.

4. Click **OK**.

To apply some of the changes, you have to close the main application window and then open it again.

► *To configure the display of elements in the main application window:*

1. In the application window menu, select **View** → **Configure**.
2. In the **Configure view** window that opens, configure the display of main window elements using check boxes.
3. Click **OK**.

---

# Application licensing

This section provides information about general concepts related to the application licensing.

## In this section:

About the End User License Agreement.....	<a href="#">58</a>
About the license .....	<a href="#">59</a>
About the license certificate.....	<a href="#">60</a>
About key .....	<a href="#">60</a>
Kaspersky Security Center licensing options .....	<a href="#">61</a>
About restrictions of the main functionality.....	<a href="#">64</a>
About the activation code .....	<a href="#">65</a>
About the key file .....	<a href="#">65</a>
About the subscription.....	<a href="#">66</a>

## About the End User License Agreement

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

Read through the terms of the License Agreement carefully before you start using the application.

You can view the terms of the End User License Agreement using the following methods:

- While installing Kaspersky Security Center.
- By reading the document license.txt. This document is included in the application distribution kit.

You accept the terms of the End User License Agreement by confirming that you agree with the End User License Agreement when installing the application. If you do not accept the terms of the End User License Agreement, you should abort the application installation and renounce the use of the application.

## About the license

A *license* is a time-limited right to use the application, granted under the End User License Agreement.

A valid license entitles you to use the following services:

- Use of the application in accordance with the terms of the End User License Agreement.
- Technical Support.

The scope of service and the application usage term depend on the type of license under which the application has been activated.

The following license types are provided:

- *Trial* – a free license intended for trying out the application.

A trial license usually has a short license term. As soon as the trial license expires, all Kaspersky Security Center features are disabled. To continue using the application, you need to purchase the commercial license.

You can activate the application under the trial license only once.

- *Commercial* – a paid license granted upon purchase of the application.

When the commercial license term expires, the application continues running with limited functionality (for example, updates of the Kaspersky Security Center databases are not available). To continue using Kaspersky Security Center in fully functional mode, you have to renew your commercial license.

We recommend renewing the license before its expiration to ensure maximum protection against all security threats.

## About the license certificate

A *license certificate* is a document that you receive along with a key file or an activation code.

A license certificate contains the following information about the license provided:

- Order number.
- Information about the user who has been granted the license.
- Information about the application that can be activated under the license provided.
- Limit of the number of licensing units (e.g., devices on which the application can be used under the license provided).
- License term start date.
- License expiration date or license term.
- License type.

## About key

Key is a sequence of bits that you can apply to activate and then use the application in accordance with the terms of the End User License Agreement. Keys are generated by Kaspersky Lab experts.

You can add a key to the application using one of the following methods: by applying a *key file* or by entering an *activation code*. The key is displayed in the application interface as a unique alphanumeric sequence after you add it to the application.

The key may be blocked by Kaspersky Lab in case the terms of the License Agreement have been violated. If the key has been blocked, you need to add another one if you want to use the application.

A key may be active or additional.

*Active key* – a key used at the moment to work with the application. A key for the trial or commercial license can be added as the active key. The application cannot use more than one active key.

*Additional key* – a key that verifies the use of the application but is not used at the moment. The additional key automatically becomes active when the license associated with the current active key expires. An additional key can be added only if an active key has already been added.

A key for the trial license can be added as the active key only. A key for the trial license cannot be added as the additional key.

## Kaspersky Security Center licensing options

In Kaspersky Security Center, the license can apply to different groups of functionality.

### **Basic functionality of Administration Console**

The following functions are available:

- Creation of virtual Administration Servers that are used to administer a network of remote offices or client organizations.
- Creation of a hierarchy of administration groups to manage specific devices as a single entity.
- Control of the anti-virus security status of an organization.
- Remote installation of applications.
- Viewing the list of operation system images available for remote installation.
- Centralized configuration of applications installed on client devices.

- Viewing and editing existing licensed applications groups.
- Statistics and reports on the application's operation, as well as notifications about critical events.
- Encryption and data protection management.
- Viewing and manual editing of the list of hardware components detected by polling the network.
- Centralized operations with files that were moved to Quarantine or Backup and files whose processing was postponed.

Kaspersky Security Center with support of the basic functionality of Administration Console is delivered as a part of Kaspersky Lab products for protection of corporate networks. You can also download it from the Kaspersky Lab website (<http://www.kaspersky.com>).

Until the application is activated, or after the commercial license expires, Kaspersky Security Center runs in basic functionality of Administration Console mode (see section "About restrictions of the basic functionality" on page [64](#)).

### **Systems Management feature**

The following functions are available:

- Remote installation of operating systems.
- Remote installation of software updates, scanning and fixing of vulnerabilities.
- Hardware inventory.
- Licensed applications group management.
- Remote permission of connection to client devices through a component of Microsoft® Windows® named Remote Desktop Connection.
- Remote connection to client devices through Windows Desktop Sharing.
- Management of user roles.

The management unit for Systems Management is a client device in the Managed devices group.

Detailed information about devices' hardware is available during the inventory process as part of Systems Management.

For a proper functioning of Systems Management, at least 100 GB free disk space must be available.

### **Mobile Device Management feature**

The Mobile Device Management feature is used to manage Exchange ActiveSync and iOS MDM mobile devices.

The following functions are available for Exchange ActiveSync mobile devices:

- Creation and editing of mobile device management profiles, assignment of profiles to users' mailboxes.
- Configuration of mobile devices (email synchronization, apps usage, user password, data encryption, connection of removable drives).
- Installation of certificates on mobile devices.

The following functions are available for iOS MDM devices:

- Creation and editing of configuration profiles, installation of configuration profiles on mobile devices.
- Installation of applications on mobile devices via App Store® or using manifest files (.plist).
- Locking of mobile devices, resetting of the mobile device password, and deleting of all data from the mobile device.

In addition, Mobile Devices Management allows executing commands provided by relevant protocols.

The management unit for Mobile Devices Management is a mobile device. A mobile device is considered to be managed after it is connected to the Mobile Devices Server.

# About restrictions of the main functionality

Until the application is activated or after the commercial license expires, Kaspersky Security Center provides the basic functionality of Administration Console. The limitations imposed on the application operation are described below.

## Mobile Device Management

You cannot create a new profile and assign it to a mobile device (iOS MDM) or to a mailbox (Exchange ActiveSync). Edition of existing profiles and assignment of profiles to mailboxes are always available.

## Managing applications

You cannot run the update installation task and the update removal task. All tasks that had been started before the license expired will be completed, but the latest updates will not be installed. For example, if the critical update installation task had been started before the license expired, only critical updates found before the license expiration will be installed.

Launch and editing of the synchronization, vulnerability scan, and vulnerabilities database update tasks are always available. Also, no limitations are imposed on viewing, searching, and sorting of entries on the list of vulnerabilities and updates.

## Remote installation of operating systems and applications

Cannot run tasks of operating system image capturing and installation. Tasks that had been started before the license expired, will be completed.

## Hardware inventory

No information about new devices can be retrieved through the Mobile Device Server. Information about computers and connected devices is updated at that.

You receive no notifications of changes in the configurations of devices.

The equipment list is available for viewing and editing manually.

## Licensed applications group management

You cannot add a new key.

You receive no notifications of violated limitations imposed on the use of keys.



## Remote connection to client devices

Remote connection to client devices is not available.

## Anti-virus security

Anti-Virus uses databases that had been installed before the license expired.

# About the activation code

An *activation code* is a unique sequence of 20 alphanumeric characters. You enter an activation code to add a key that activates Kaspersky Security Center. You receive the activation code through the email address that you have specified, after purchasing Kaspersky Security Center or after ordering the trial version of Kaspersky Security Center.

To activate the application with an activation code, you need Internet access to establish connection with Kaspersky Lab activation servers.

If the application was activated with an activation code, the application in some cases sends regular requests to Kaspersky Lab activation servers in order to check the current status of the key. You need provide the application Internet access to make it possible to send requests.

If you lost your activation code after you had activated the application, it can be restored. You may need your activation code, e.g., to register with Kaspersky CompanyAccount. To restore the activation code, you must contact the Kaspersky Lab Technical Support Service (see section "How to obtain technical support" on page [322](#)).

# About the key file

*Key file* is a file with the .key extension provided to you by Kaspersky Lab. A key file is intended for adding a key that activates the application.

You receive your key file through the email address that you have specified, after purchasing Kaspersky Security Center or after ordering the trial version of Kaspersky Security Center.

To activate the application using a key file, you do not have to connect to Kaspersky Lab activation servers.

If the key file has been accidentally deleted, you can restore it. You may need your key file, e.g., to register with Kaspersky CompanyAccount.

To restore your key file, you should perform any of the following actions:

- Contact the Technical Support Service (<http://support.kaspersky.com/>).
- Receive a key file through Kaspersky Lab website (<https://activation.kaspersky.com/en/>) by using your available activation code.

## About the subscription

*Subscription to Kaspersky Security Center* is an order request for use of the application under the selected settings (subscription expiration date, number of protected devices). You can register your subscription to Kaspersky Security Center with your service provider (e.g., your Internet provider). A subscription can be renewed manually or in automatic mode; also, you can cancel it.

A subscription can be limited (e.g., 1-year) or unlimited (with no expiration date). To continue using Kaspersky Security Center after a limited subscription expires, you must renew it. An unlimited subscription is renewed automatically if it has been prepaid to the service provider in due dates.

When a limited subscription expires, you may be provided a grace period for renewal during which the application keeps functioning. The availability and duration of the grace period is defined by the service provider.

To use Kaspersky Security Center under subscription, you must apply the activation code received from the service provider.

You can apply a different activation code for Kaspersky Security Center only after your subscription expires or when you cancel it.

Depending on the service provider, the set of possible actions for subscription management may vary. The service provider can provide no grace period for subscription renewal so the application loses its functionality.

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

When using the application under subscription, Kaspersky Security Center automatically attempts to access the activation server in specified time intervals until the subscription expires.

You can renew your subscription on the service provider's website.

---

# Administration Server Quick Start Wizard

This section provides information about the Administration Server Quick Start Wizard operation.

Kaspersky Security Center allows adjusting a minimum set of settings required to build a centralized management system for anti-virus protection. This configuration is performed by using the Quick Start Wizard. While the Quick Start Wizard is running, the following changes are made to the application:

- The Wizard adds keys or codes that can be automatically distributed to devices within administration groups.
- Configures interaction with Kaspersky Security Network (KSN). KSN allows you to retrieve information about applications installed on managed devices if such information can be found in Kaspersky Lab reputation databases. If you have allowed the use of KSN, the wizard enables the KSN Proxy server service, which ensures connection between KSN and devices.
- It sets up email delivery of notifications informing of events in the operation of Administration Server and managed applications (successful notification delivery requires the Messenger service to be running on the Administration Server and all of the recipient devices).
- The Wizard then adjusts the update settings and vulnerability fix settings of applications installed on devices.
- A protection policy for workstations and servers is created at the top level of the hierarchy of managed devices; virus scan tasks, update tasks, and data backup tasks are also created.

The Quick Start Wizard creates protection policies only for those applications whose **Managed devices** folder does not contain any policies. The Quick Start Wizard creates no tasks if tasks with the same names have already been created for the top level in the hierarchy of managed devices.

The application prompts you to run the Quick Start Wizard after Administration Server installation, at the first connection to it. You can also start the Quick Start Wizard manually using the context menu of the **Administration Server <Device name>** node.

---

# Basic concepts

This section explains basic concepts related to Kaspersky Security Center.

## In this section:

Administration Server .....	<a href="#">68</a>
Administration Servers hierarchy .....	<a href="#">69</a>
Virtual Administration Server .....	<a href="#">70</a>
Mobile device server .....	<a href="#">71</a>
Web server .....	<a href="#">72</a>
Network Agent Administration group .....	<a href="#">73</a>
Administrator's workstation .....	<a href="#">74</a>
Application management plug-in.....	<a href="#">75</a>
Policies, application settings, and tasks .....	<a href="#">75</a>
How local application settings relate to policies .....	<a href="#">78</a>
Update agent .....	<a href="#">79</a>

## Administration Server

Kaspersky Security Center components enable remote management of Kaspersky Lab applications installed on client devices.

Devices with the Administration Server component installed will be referred to as *Administration Servers* (hereinafter also referred to as *Servers*).

Administration Server is installed on a device as a service with the following set of attributes:

- With the name "Kaspersky Security Center Administration Server".
- Set to automatically start when the operating system starts.
- With the **Local System** account or the user account selected during the installation of the Administration Server.

The Administration Server performs the following functions:

- Storage of the administration groups structure.
- Storage of information about the configuration of client devices.
- Organization of repositories for application distribution packages.
- Remote installation of applications to client devices and removal of applications.
- Updating of application databases and software modules of Kaspersky Lab applications.
- Management of policies and tasks on client devices.
- Storage of information about events that have occurred on client devices.
- Generation of reports on the operation of Kaspersky Lab applications.
- Deployment of keys to client devices, and storage of information about keys.
- Forwarding of notifications about the progress of tasks (such as detection of viruses on a client device).

## Administration Servers hierarchy

Administration Servers can be arranged in a master/slave hierarchy. Each Administration Server can have several slave Administration Servers (referred to as *slave Servers*) on different nesting levels of the hierarchy. The nesting level for slave Servers is unrestricted. The administration groups of the master Administration Server will then include the client devices of all slave Administration Servers. Thus, isolated and independent sections of computer networks

can be controlled by different Administration Servers which are in turn managed by the master Server.

*Virtual Administration Servers* (see section "Virtual Administration Server" on page [70](#)) are a particular case of slave Administration Servers.

The hierarchy of Administration Servers can be used to do the following:

- Decrease the load on Administration Server (compared to a single installed Administration Server in an entire network).
- Decrease intranet traffic and simplify work with remote offices. It is unnecessary to establish connections between the master Administration Server and all network devices, which may be located, for example, in different regions. It is sufficient to install a slave Administration Server in each network segment, distribute devices among administration groups of slave Servers, and establish connections between the slave Servers and master Server over fast communication channels.
- Distribute responsibilities among the anti-virus security administrators. All capabilities for centralized management and monitoring of anti-virus security status in corporate networks remain available.
- How service providers use Kaspersky Security Center. The service provider only needs installed Kaspersky Security Center and Kaspersky Security Center 10 Web Console. To manage a large number of client devices of various organizations, a service provider can add virtual Administration Servers to the Administration Servers hierarchy.

Each device included in the hierarchy of administration groups can be connected to one Administration Server only. You must independently monitor the connection of devices to Administration Servers. Use the feature for device search in administration groups of different Servers based on network attributes.

## Virtual Administration Server

Virtual Administration Server (also referred to as *virtual Server*) is a component of Kaspersky Security Center intended for managing anti-virus protection of the network of a client organization.

Virtual Administration Server is a particular case of a slave Administration Server and has the following restrictions as compared with physical Administration Server:

- Virtual Administration Server can be created only on master Administration Server.
- Virtual Administration Server uses the master Administration Server database. Thus, the following tasks are not supported on virtual Server: backup copying, restoration, updates verification and updates downloading. These tasks exist only on master Administration Server.
- Virtual Server does not support creation of slave Administration Servers (including virtual Servers).

Besides, virtual Administration Server has the following restrictions:

- In the virtual Administration Server properties window the number of sections is restricted.
- To remotely install Kaspersky Lab applications on client devices managed by the virtual Administration Server, you must make sure that the Network Agent is installed on one of the client devices in order to ensure communication with the virtual Administration Server. Upon first connection to the virtual Administration Server, the device is automatically assigned as update agent, thus functioning as a gateway for connection between the client devices and the virtual Administration Server.
- A virtual Server can poll the network only through update agents.
- To restart a malfunctioning virtual Server, Kaspersky Security Center restarts the master Administration Server and all virtual Administration Servers.

The administrator of a virtual Administration Server has all privileges on this particular virtual Server.

## Mobile device server

A *mobile device server* is a component of Kaspersky Security Center that provides access to mobile devices and allows managing them through Administration Console. The Mobile device server retrieves information about mobile devices and stores their profiles.

There are two types of mobile device servers:

- Microsoft Exchange Mobile Devices Server. It is installed to a device where a Microsoft Exchange server has been installed, allowing retrieval of data from the Microsoft Exchange server and passing them to Administration Server. This mobile device server is used for management of mobile devices that support Exchange ActiveSync protocol.
- iOS MDM Server. This mobile devices server is used for management of mobile devices that support the Apple Push Notification service (APNs).

Mobile devices servers of Kaspersky Security Center allow managing the following objects:

- An individual mobile device.
- Several mobile devices.
- Several mobile devices connected to a cluster of servers, simultaneously. After connecting to a cluster of servers, the mobile devices server installed on this cluster is displayed in Administration Console as a single server.

## Web server

Kaspersky Security Center *Web Server* (hereinafter also referred to as *Web Server*) is a component of Kaspersky Security Center that is installed together with Administration Server. Web Server is designed for transfer of stand-alone installation packages, iOS MDM profiles, and files from a shared folder over the network.

When you create a stand-alone installation package, it is automatically published on Web Server. A link for downloading the stand-alone package is displayed in the list of stand-alone installation packages. If necessary, you can cancel publication of the stand-alone package or publish it on Web Server again.

When you create an iOS MDM profile for a user's mobile device, it is also automatically published on Web Server. When the profile is published, it is automatically removed from Web Server after it is successfully installed to the user's mobile device (for more details on how to create and install an iOS MDM profile, please refer to the *Kaspersky Security Center Implementation Guide*).



The shared folder is designed as a storage area for information that is available to all users whose devices are managed through the Administration Server. If a user has no direct access to the shared folder, he or she can be given information from that folder by means of Web Server.

To provide users with information from a shared folder by means of Web Server, the administrator must create a subfolder named "public" in the shared folder and paste the relevant information.

The syntax of the information transfer link is as follows:

```
https://<Web Server name>:<HTTPS port>/public/<object>
```

where:

- <Web Server name> is the name of the Kaspersky Security Center Web Server.
- <HTTPS port> is an HTTPS port of Web Server that has been defined by the administrator. The HTTPS port can be set in the **Web Server** section of the properties window of Administration Server. The default port number is 8061.
- <object> is the subfolder or file to which the user will receive access.

The administrator can send the new link to the user in any convenient way, such as by email.

By using this link, the user can download the required information to a local device.

## Network Agent Administration group

Interaction between the Administration Server and devices is performed by a component of Kaspersky Security Center named *Network Agent*. Network Agent must be installed on all devices on which Kaspersky Security Center is used to manage Kaspersky Lab applications.

Network Agent is installed to a device as a service with the following set of attributes:

- With the name "Kaspersky Security Center Network Agent"
- Set to automatically start when the operating system starts.
- Using the **Local system** account.

A device, server, or workstation installed with Network Agent and managed Kaspersky Lab applications will be referred to as the *Administration Server client* (also referred to as *client device* or just *device*).

The multitude of devices in a corporate network can be subdivided into groups arranged in a hierarchical structure. Such groups are called *administration groups*. The hierarchy of administration groups is displayed in the console tree, in the Administration Server node.

An *administration group* (hereinafter also referred to as *group*) is a set of client devices combined on the basis of a certain trait for the purpose of managing the grouped devices as a single unit. All client devices within a group are configured to.

- Use the same application settings (which are defined in *group policies*).
- Use a common operation mode for all applications through creation of *group tasks* with a specified collection of settings. For example, creating and installing a common *installation package*, updating the application databases and modules, scanning the device on demand, and enabling the real-time protection.

A client device can be included only in one administration group.

You can create hierarchies for Servers and groups with any degree of nesting. A single hierarchy level can include slave and virtual Administration Servers, groups, and client devices.

## Administrator's workstation

Devices on which the *Administration Console* component is installed are referred to as *administrator's workstations*. Administrators can use those devices for centralized remote management of Kaspersky Lab applications installed on client devices.

After Administration Console is installed to the device, its icon appears in the **Start** → **Applications** → **Kaspersky Security Center** menu.

There are no restrictions on the number of administrator's workstations. From any administrator's workstation you can manage administration groups of several Administration Servers on the network at once. You can connect an administrator's workstation to an Administration Server (physical or virtual one) of any level of hierarchy.

You can include an administrator's workstation in an administration group as a client device.

Within the administration groups of any Administration Server, the same device can function as an Administration Server client, an Administration Server, or an administrator's workstation.

## Application management plug-in

Management of Kaspersky Lab applications via the Administration Console is performed using a special component named the *application management plug-in*. It is included in all Kaspersky Lab applications that can be managed by using Kaspersky Security Center.

The application management plug-in is installed on the administrator's workstation.

Using the application management plug-in, you can perform the following actions in the Administration Console:

- Creating and editing application policies and settings, as well as the settings of application tasks.
- Obtaining information about application tasks, application events, as well as application operation statistics received from client devices.

## Policies, application settings, and tasks

A named action performed by a Kaspersky Lab application is called a *task*. Tasks are organized by *types* according to their function.

Each task is associated with a set of settings that are used during performance of the task. The set of application settings that are common to all types of application tasks form the application settings. Application settings that are specific to each task type form the corresponding task settings.

A detailed description of task types for each Kaspersky Lab application can be found in the respective application guides.

Application settings defined for an individual client device through the local interface or remotely through Administration Console are referred to as *local application settings*.

The applications installed on client devices are configured centrally by defining policies.

A *policy* is a collection of application settings that are defined for an administration group.


The policy does not define all application settings.

Several 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.

An application can run in different ways for different groups of settings. Each group can have its own policy for an application.

The application settings are defined by the policy settings and the task settings.

Nested groups and slave Administration Servers inherit the tasks from groups that belong to higher hierarchy levels. A task defined for a group is performed not only on client devices included in that group, but also on client devices included in its nested groups and belonging to slave Servers on all lower levels in the hierarchy.

Each setting represented in a policy has a "lock" attribute: . The "lock" shows whether it is allowed to modify in the policies of lower hierarchy levels (for nested groups and slave Administration Servers), in task settings, and in local application settings. If a setting is "locked" in the policy, its value cannot be redefined (see section "How local application settings relate to policies" on page [78](#)).

If you clear the **Inherit settings from parent policy** check box in the **Settings inheritance** section of the **General** section in the properties window of an inherited policy, the "lock" is lifted for that policy.

You can activate a disabled policy based on occurrence of a certain event. This means that you can, for example, enforce stricter anti-virus protection settings during virus outbreaks.

You can also create an out-of-office policy.

Tasks for objects that are managed by a single Administration Server are created and configured in a centralized way. The following types of tasks can be defined:

- *Group task* is a task that defines settings for an application installed on devices within an administration group.
- *Local task* is a task for an individual device.

- *Task for specific devices* is a task for a user-defined set of devices included or not included in administration groups.
- *Administration Server task* is a task defined directly for an Administration Server.

A group task can be defined for a group even if the corresponding Kaspersky Lab application is not installed on all client devices of that group. In that case, the group task is performed only on the devices on which the application is installed.

Tasks created for a client device locally are only performed for this device. When a client device is synchronized with the Administration Server, local tasks are added to the list of tasks created for that client device.

Because application settings are defined by policies, task settings can redefine the settings that are not locked by the policy. Task settings also can redefine the settings that can be configured only for a specific instance of a task. For example, the drive name and masks of files to be scanned are configurable settings for the drive scan task.

A task can be run automatically (according to a schedule) or manually. Task results are saved locally and on the Administration Server. The administrator can receive notifications about particular performed tasks and view detailed reports.

Information about policies, application settings, and task settings for specific devices, as well as information about group tasks is saved on the Administration Server and distributed to client devices during synchronization. During synchronization, the Administration Server stores information about the local changes allowed by the policy that have been performed on client devices. Additionally, the list of applications running on the client device, their status, and the existing tasks are updated.

# How local application settings relate to policies

You can use policies to set identical values of the application settings for all devices in a group.

The values of settings specified by a policy can be redefined for individual devices in a group by using local application settings. You can set only the values of settings that the policy allows to be modified, that is, the "unlocked" settings.

The value of a setting that the application uses on a client device (see the figure below) is defined by the "lock" position for that setting in the policy:

- If setting modification is "locked", the same value (defined in the policy) is used on all client devices.
- If setting modification is "unlocked", the application uses a local value on each client device instead of the value specified in the policy. The setting can then be changed in the local application settings.



Figure 7. Policy and local application settings

This means that, when a task is run on a client device, the application applies settings that

have been defined in two different ways:

- By task settings and local application settings, if the setting is not locked against changes in the policy.
- By the group policy, if the setting is locked against changes.

Local application settings are changed after the policy is first applied in accordance with the policy settings.

## Update agent

Update agent is a device with Network Agent installed, which is used for update distribution, remote installation of applications, and retrieval of information about networked devices. An update agent can perform the following functions:

- Manage updates and installation packages received from the Administration Server by distributing them to client devices within the group (including such a method as multicasting via UDP). Updates can be retrieved either from the Administration Server or from Kaspersky Lab update servers. In the latter case, an update task must be created for the device that acts as update agent (see section "Automatic installation of Kaspersky Endpoint Security updates on devices" on page [208](#)).

Update agents accelerate update distribution and allow you to free up Administration Server resources.

- Distribute policies and group tasks through multicasting via UDP.
- Act as a gateway for connection to the Administration Server for devices in an administration group (see section "Using an update agent as gateway" on page [356](#)).

If no direct connection between managed devices within the group and the Administration Server can be established, you can use the update agent as connection gateway to the Administration Server for this group. In this case, managed devices connect to the connection gateway, which, in turn, connects to the Administration Server.

Presence of an update agent that functions as connection gateway does not block the option of direct connection between managed devices and the Administration Server.

If the connection gateway is not available, but direct connection with the Administration Server is technically possible, managed devices are connected to the Administration Server directly.

- Poll the network to detect new devices and update information about existing ones. An update agent can apply the same network polling methods as the Administration Server.
- Perform remote installation of third-party software and Kaspersky Lab applications through Microsoft Windows tools, including installation on client devices without Network Agent.

This feature allows you to remotely transfer Network Agent installation packages to client devices located in networks to which the Administration Server has no direct access.

Files are transmitted from the Administration Server to an update agent over HTTP or, if SSL connection is enabled, over HTTPS. Using HTTP or HTTPS results in a higher performance, as compared with SOAP, through cutting traffic.

Devices with Network Agent installed can be assigned to act as update agents either manually, by the administrator, or automatically, by the Administration Server (see section "Assigning devices to act as update agents" on page [298](#)). You can view the full list of update agents for specified administration groups by creating a report on the list of update agents.

The scope of an update agent is the administration group to which it has been assigned by the administrator, as well as its subgroups of all levels of embedding. If multiple update agents have been assigned in the hierarchy of administration groups, Network Agent on the managed device connects to the hierarchically closest update agent.

An NLA subnet can also be the scope of update agents. The NLA subnet is then used for manual creation of a set of devices to which the update agent will distribute updates.

If update agents are assigned automatically by the Administration Server, it assigns them by broadcast domains, not by administration groups. This occurs when all broadcast domains are known. Network Agent exchanges messages with other Network Agents in the same subnet and then sends Administration Server information about itself and other Network Agents. Administration Server can use that information to group Network Agents by broadcast domains. Broadcast domains are known to Administration Server after more than 70% Network Agents in administration groups are polled. Administration Server polls broadcast domains every two hours.



After update agents are assigned by broadcast domains, it cannot be re-assigned by administration groups.

Network Agents with the active connection profile do not participate in broadcast domain detection.

When two or more update agents are assigned to a single network area or to a single administration group, one of them becomes the active update agent, the rest of them become standby update agents. The active update agent downloads updates and installation packages directly from the Administration Server, while standby update agents retrieve updates from the active update agent only. In this case, files are once downloaded from the Administration Server after which they are distributed among update agents. If the active update agent becomes unavailable for any reason, one of the standby update agents becomes active. The Administration Server automatically assigns an update agent to act as standby.

The update agent status (*Active/Standby*) is displayed as a check box in the klnagchk report (see section "Checking the connection between a client device and the Administration Server manually. Utility tool klnagchk" on page [139](#)).

An update agent requires at least 4 GB of free disk space for operation. If the free disk space of the update agent is lower than 2 GB, Kaspersky Security Center creates an incident with the *Warning* importance level. The incident will be published in the device properties, in the **Incidents** section.

If any remote installation tasks are pending on the Administration Server, the device with the update agent will also require an amount of free disk space, which is equal to the total size of the installation packages to be installed.

If one or multiple instances of the task for update (patch) installation and vulnerability fix are pending on the Administration Server, the device with the update agent will also require an extra amount of free disk space, which is equal to twice the total size of all patches to be installed.

---

# Managing Administration Servers

This section provides information about how to handle Administration Servers and how to configure them.

## In this section:

Connecting to an Administration Server and switching between Administration Servers .....	<a href="#">82</a>
Access rights to Administration Server and its objects .....	<a href="#">85</a>
Conditions of connection to an Administration Server via the Internet .....	<a href="#">86</a>
Secure connection to Administration Server .....	<a href="#">87</a>
Disconnecting from an Administration Server .....	<a href="#">89</a>
Adding an Administration Server to the console tree .....	<a href="#">89</a>
Removing an Administration Server from the console tree .....	<a href="#">90</a>
Changing an Administration Server service account. Utility tool klsrvswch .....	<a href="#">90</a>
Viewing and modifying the settings of an Administration Server .....	<a href="#">91</a>

## Connecting to an Administration Server and switching between Administration Servers

After Kaspersky Security Center is started, it attempts to connect to an Administration Server. If several Administration Servers are available on the network, the application requests the server to which it was connected during the previous session of Kaspersky Security Center.

When the application is started for the first time after installation, it attempts to connect to the Administration Server that was specified during installation of Kaspersky Security Center.

After a connection to an Administration Server is established, the folders tree of that Server is displayed in the console tree.

If several Administration Servers have been added to the console tree, you can switch between them.

► *To switch to another Administration Server:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the context menu of the node, select **Connect to Administration Server**.
3. In the **Connection settings** window that opens, in the **Server address** field specify the name of the Administration Server to which you want to connect. You can specify an IP address or the name of a device on a Windows network as the name of the Administration Server. You can click the **Advanced** button in the bottom part of the window to configure the connection to the Administration Server (see the figure below).

To connect to the Administration Server via a port that differs from the default one, enter a value in the **Server address** field in <Administration Server name>:<Port> format.

Users who have no rights to **read** will be denied access to Administration Server.

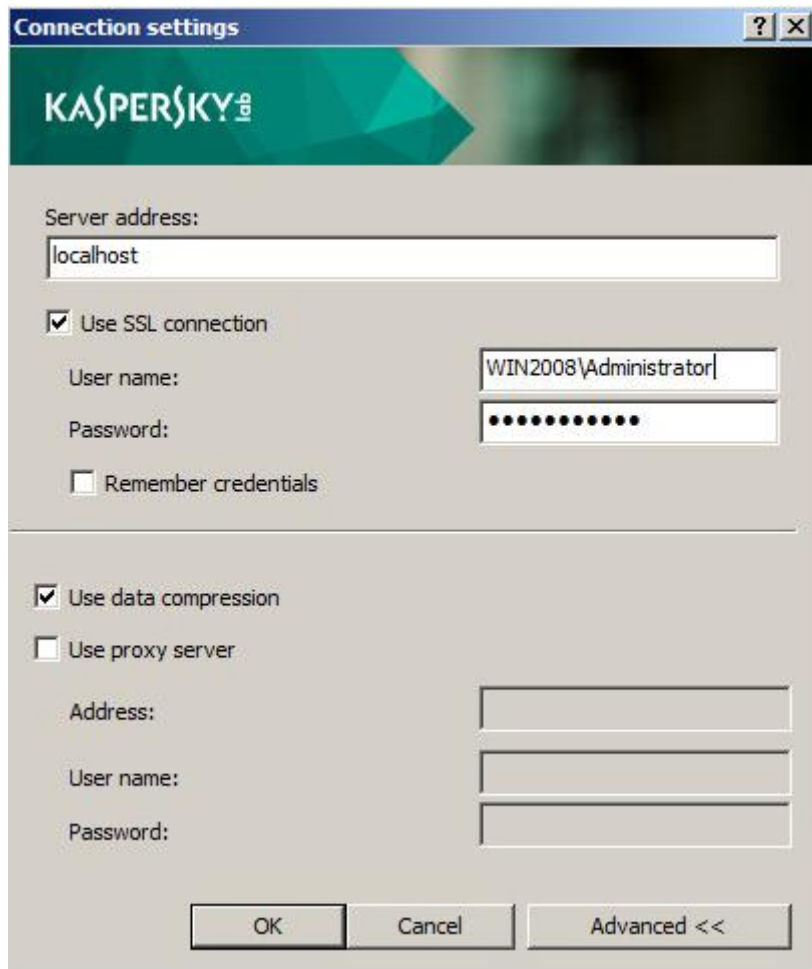


Figure 8. Connecting to Administration Server

4. Click **OK** to complete the switch between Servers.

After the Administration Server is connected, the folders tree of the corresponding node in the console tree is updated.

# Access rights to Administration Server and its objects

The **KLAdmins** and **KLOperators** groups are created automatically during Kaspersky Security Center installation. These groups are granted rights to connect to the Administration Server and to work with Administration Server objects.

Depending on which account is used for installation of Kaspersky Security Center, the **KLAdmins** and **KLOperators** groups are created as follows:

- If the application is installed under a user account included in a domain, the groups are created on the Administration Server and in the domain that includes the Administration Server.
- If the application is installed under a system account, the groups are created on the Administration Server only.

You can view the **KLAdmins** and **KLOperators** groups and modify the access privileges of the users that belong to the **KLAdmins** and **KLOperators** groups by using the standard administrative tools of the operating system.

The **KLAdmins** group is granted all access rights; the **KLOperators** group is granted only Read and Execution rights. The rights granted to the **KLAdmins** group are locked.

Users that belong to the **KLAdmins** group are called *Kaspersky Security Center administrators*, while users from the **KLOperators** group are called *Kaspersky Security Center operators*.

In addition to users included in the **KLAdmins** group, administrator rights for Kaspersky Security Center are also provided to the local administrators of devices on which Administration Server is installed.

You can exclude local administrators from the list of users who have Kaspersky Security Center administrator rights.

All operations started by the administrators of Kaspersky Security Center are performed using the rights of the Administration Server account.

An individual **KLAdmins** group can be created for each Administration Server from the network; the group will have the necessary rights for that Administration Server only.

If devices belonging to the same domain are included in the administration groups of different Administration Servers, the domain administrator is the Kaspersky Security Center administrator for all the groups. The **KLAdmins** group is the same for those administration groups; it is created during installation of the first Administration Server. All operations initiated by a Kaspersky Security Center administrator are performed using the account rights of the Administration Server for which these operations have been started.

After the application is installed, an administrator of Kaspersky Security Center can:

- Modify the rights granted to the **KLOperators** groups.
- Grant rights to access the functionality of Kaspersky Security Center to other user groups and individual users who are registered on the administrator's workstation.
- Assign access rights within each administration group.

The Kaspersky Security Center administrator can assign access rights to each administration group or to other objects of Administration Server in the **Security** section in the properties window of the selected object.

You can track user activity by using the records of events in the Administration Server operation. Event records are displayed in the **Administration Server** node on the **Events** tab. These events have the importance level **Info** and the event types begin with "**Audit**".

## Conditions of connection to an Administration Server via the Internet

If an Administration Server is remotely located outside of a corporate network, client devices can connect to it via the Internet. For devices to connect to an Administration Server over the Internet, the following conditions must be met:

- The remote Administration Server must have an external IP address and the incoming ports 13000 and 14000 must remain open.
- Network Agents must be installed on the devices.

- When installing Network Agent on devices, you must specify the external IP address of the remote Administration Server. If an installation package is used for installation, specify the external IP address manually in the properties of the installation package, in the **Settings** section.
- To use the remote Administration Server to manage applications and tasks for a device, in the properties window of the device in the **General** section, select the **Do not disconnect from the Administration Server** check box. After the check box is selected, wait until the Server is synchronized with the remote device. The number of client devices maintaining a continuous connection with an Administration Server cannot exceed 100.

To speed up the performance of tasks initiated by a remote Administration Server, you can open port 15000 on a device. In this case, to run a task, the Administration Server sends a special packet to Network Agent over port 15000 without waiting until completion of synchronization with the device.

## Secure connection to Administration Server

Data exchange between client devices and Administration Server, as well as the Administration Console connection to Administration Server, can be performed using the Secure Sockets Layer (SSL) protocol. The SSL protocol can identify the interacting parties, encrypt the data that is transferred, and protect data against modification during transfer. The SSL protocol uses public keys to authenticate the interacting parties and encrypt data.

### In this section:

Authenticating the Server when a device is connected.....	<a href="#">88</a>
Administration Server authentication during Administration Console connection .....	<a href="#">88</a>
Administration Server certificate .....	<a href="#">88</a>

# Authenticating the Server when a device is connected

When a client device connects to Administration Server for the first time, Network Agent on the device downloads a copy of the Administration Server certificate and stores it locally.

If you install Network Agent to a device locally, you can select the Administration Server certificate manually.

The downloaded copy of the certificate is used to verify Administration Server rights and permissions during subsequent connections.

During future sessions, Network Agent requests the Administration Server certificate at each connection of the device to Administration Server and compares it with the local copy. If the copies do not match, the device is not allowed access to Administration Server.

## Administration Server authentication during Administration Console connection

At the first connection to Administration Server, Administration Console requests the Administration Server certificate and saves it locally on the administrator's workstation. After that, each time when Administration Console tries to connect to this Administration Server, the Administration Server is identified based on the certificate copy.

If the Administration Server certificate does not match the copy stored on the administrator's workstation, the Administration Console offers to confirm connection to the Administration Server with the specified name and download a new certificate. After the connection is established, Administration Console saves a copy of the new Administration Server certificate, which will be used to identify the Administration Server in the future.

## Administration Server certificate

Administration Server authentication during connection by Administration Console and data exchange with devices is performed based on the *Administration Server certificate*. The certificate is also used for authentication when a connection is being established between master and slave Administration Servers.



The Administration Server certificate is created automatically during installation of the Administration Server component and is stored in the ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert folder.

The Administration Server certificate is created only once, during Administration Server installation. If the Administration Server certificate is lost, you need to reinstall the Administration Server component and perform data recovery in order to restore the certificate (see section "Backup copying and restoration of Administration Server data" on page [343](#)).

## Disconnecting from an Administration Server

► *To disconnect from an Administration Server:*

1. In the console tree select the node corresponding to the Administration Server that should be disconnected.
2. From the context menu of the node select **Disconnect from Administration Server**.

## Adding an Administration Server to the console tree

► *To add an Administration Server to the console tree:*

1. In the main window of Kaspersky Security Center select the **Kaspersky Security Center** node from the console tree.
2. From the context menu of the node select **Create** → **Administration Server**.

As a result, a node named **Administration Server - <Device name> (Not connected)** will be created in the console tree from which you will be able to connect to any of the Administration Servers installed on the network.

# Removing an Administration Server from the console tree

► *To remove an Administration Server from the console tree:*

1. In the console tree select the node corresponding to the Administration Server that you want to remove.
2. From the context menu of the node select **Remove**.

# Changing an Administration Server service account. Utility tool klsrvswch

If you need to change the Administration Server service account set when installing Kaspersky Security Center, you can use a utility named klsrvswch and designed for changing the Administration Server account.

When installing Kaspersky Security Center, the utility is automatically copied in the application installation folder.

Number of launches of the utility is virtually unlimited.

► *To change an Administration Server service account:*

1. Launch the klsrvswch utility from the installation folder of Kaspersky Security Center.

This action also launches the wizard for modification of Administration Server service account. Follow the instructions of the Wizard.

2. In the **Administration Server service account** window select any of the two options for setting an account:

- **Local System Account.** The Administration Server service will start under the *Local System Account* and using its credentials.

Correct operation of Kaspersky Security Center requires that the account used to start the Administration Server service had the rights of administrator of the resource where the Administration Server database is hosted.

- **User account.** The Administration Server service is started under the account of a user within the domain. In this case the Administration Server is to initiate all operations by using the rights of that account.

To select the user whose account will be used to start the Administration Server service:

1. Click the **Find now** button and select a user in the **Select: User** window that opens.  
Close the **Select: User** window and click **Next**.
2. In the **Account password** window set a password for the selected user account, if necessary.

After the wizard completes its operations, the Administration Server account is changed.

When using an SQL server in a mode that presupposes authenticating user accounts with Microsoft Windows tools, access to the database should be granted. The user account must have the status of owner of the Kaspersky Anti-Virus database. The dbo schema is used by default.

## Viewing and modifying the settings of an Administration Server

You can adjust the settings of an Administration Server in the properties window of this Server.

► *To open the Properties: Administration Server window,*

Select **Properties** from the context menu of the Administration Server node in the console tree.

### In this section:

Adjusting the general settings of Administration Server.....	<a href="#">92</a>
Event processing and storage on the Administration Server.....	<a href="#">92</a>
Control of virus outbreaks.....	<a href="#">93</a>
Limiting traffic .....	<a href="#">94</a>
Configuring Web Server .....	<a href="#">94</a>
Working with internal users.....	<a href="#">94</a>

# Adjusting the general settings of Administration Server

You can adjust the general settings of Administration Server in the **General**, **Settings**, **Events Storage**, and **Security** of the properties window of Administration Server.

The **Security** section may not be displayed in the Administration Server properties window if the display has been disabled in the Administration Console interface.

► *To enable the display of the **Security** section in Administration Console:*

1. In the **View** menu of the main application window, select **Configure interface**.
2. In the **Configure interface** window that opens, select the **Display security settings sections** check box and click **OK**.
3. In the window with the application message, click **OK**.

The **Security** section will be displayed in the Administration Server properties window.

# Event processing and storage on the Administration Server

Information about events in the operation of the application and managed devices is saved in the Administration Server database. Each event is attributed to a certain type and level of severity (Critical event, Functional failure, Warning, or Info). Depending on the conditions under which an event occurred, the application can assign different levels of severity to events of the same type.

You can view types and levels of severity assigned to events in the **Event notification** section of the Administration Server properties window. In the **Event notification** section, you can also configure processing of every event by the Administration Server:

- Registration of events on the Administration Server and in event logs of the operating system on a device and on the Administration Server.
- Method used for notifying the administrator of an event (for example, an SMS or an email message).

In the **Events storage** section of the Administration Server properties window, you can configure event storage in the Administration Server database by limiting the number of event records or the record storage time. The default capacity of the Administration Server database is 400,000 events. The maximum recommended capacity of the database is 15,000,000 events. If the number of events in the database reaches the maximum value specified by the administrator, the application deletes the oldest events and rewrites them with new ones.

## Control of virus outbreaks

Kaspersky Security Center allows you to quickly respond to emerging threats of virus outbreaks. Risks of virus outbreaks are assessed by monitoring virus activity on devices.

You can configure assessment rules for threats of virus outbreaks and actions to take in case one emerges; to do this, use the **Virus outbreak** section of the properties window of Administration Server.

You can specify the notification procedure for the *Virus outbreak* event in the **Event notification** section of the Administration Server properties window (see section "Processing and storing events on the Administration Server" on page [92](#)), in the *Virus outbreak* event properties window.

The *Virus outbreak* event is generated upon detection of *Malicious object detected* events in the operation of security applications. So, you should save information about all *Malicious object detected* events on Administration Server in order to recognize virus outbreaks.

You can specify the settings for saving information about any *Malicious object detected* event in the policies of the security applications.

When counting *Malicious object detected* events, only information from the devices of the master Administration Server is taken into account. The information from slave Administration Servers is not taken into account. For each slave Server the *Virus outbreak* event is configured individually.

## Limiting traffic

To reduce traffic volumes within a network, the application provides the option to limit the speed of data transfer to an Administration Server from specified IP ranges and IP subnets.

You can create and configure traffic limiting rules in the **Traffic** section of the Administration Server properties window.

## Configuring Web Server

Web Server is designed for publishing stand-alone installation packages, iOS MDM profiles, and files from a shared folder.

You can define the settings for Web Server connection to the Administration Server and set the Web Server certificate in the **Web Server** section of the Administration Server properties window.

## Working with internal users

The accounts of *internal users* are used to work with virtual Administration Servers.

Under the account of an internal user, the administrator of a virtual Administration Server can start Kaspersky Security Center 10 Web Console to check the anti-virus security status of the network. Kaspersky Security Center grants the rights of real users to internal users of the application.

The accounts of internal users are created and used only within Kaspersky Security Center. No data on internal users is transferred to the operating system. Kaspersky Security Center authenticates internal users.

You can configure accounts of internal users in the **User accounts** folder of the console tree (see section "Handling user accounts" on page [155](#)).

---

# Managing administration groups

This section provides information about how to handle administration groups.

You can perform the following actions on administration groups:

- add any number of nested groups of any level of hierarchy to administration groups;
- add devices to administration groups;
- change the hierarchy of administration groups by moving individual devices and entire groups to other groups;
- remove nested groups and devices from administration groups;
- add slave and virtual Administration Servers to administration groups;
- move devices from the administration groups of an Administration Server to those of another Server;
- define which Kaspersky Lab applications will be automatically installed on devices included in a group.

## In this section:

Creating administration groups .....	<a href="#">96</a>
Moving administration groups .....	<a href="#">98</a>
Deleting administration groups .....	<a href="#">99</a>
Automatic creation of a structure of administration groups .....	<a href="#">100</a>
Automatic installation of applications to devices in an administration group .....	<a href="#">102</a>

# Creating administration groups

The hierarchy of administration groups is created in the main application window of Kaspersky Security Center in the **Managed devices** folder. Administration groups are displayed as folders in the console tree (see the figure below).

Immediately after installation of Kaspersky Security Center, the **Managed devices** folder contains only an empty **Administration Servers** folder.

The user interface settings determine whether the **Administration Servers** folder appears in the console tree. To display this folder, open **View** → **Configure interface** and, in the **Configure interface** window that opens, select the **Display slave Administration Servers** check box.

When creating a hierarchy of administration groups, you can add devices and virtual machines to the **Managed devices** folder, and add nested groups. You can add slave Administration Servers to the **Administration Servers** folder.



Identically to the **Managed devices** folder, each created group initially only contains an empty **Administration Servers** folder intended to handle slave Administration Servers of this group. Information about policies, tasks of this group, and computers included is displayed on the corresponding tabs in the workspace of this group.

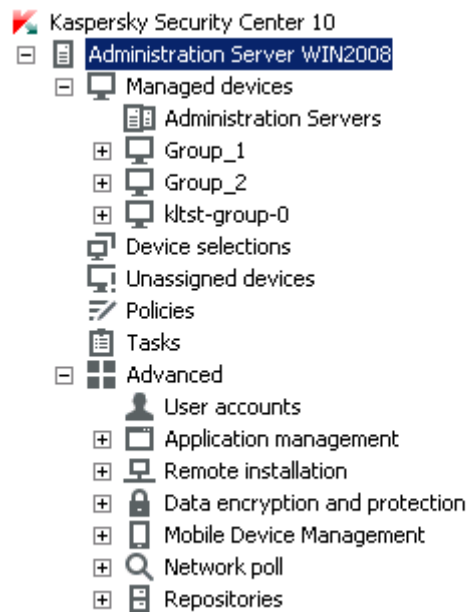


Figure 9. Viewing administration groups hierarchy

► *To create an administration group:*

1. In the console tree, open the **Managed devices** folder.
2. If you want to create a subgroup in an existing administration group, in the **Managed devices** folder select a nested folder corresponding to the group, which should comprise the new administration group.

If you create a new top-level administration group, you can skip this step.

3. Start the administration group creation process in one of the following ways:
  - By using the **Create** → **Group** command from the context menu.
  - By clicking the **New group** button located in the workspace of the main application window, on the **Groups** tab.
4. In the **Group name** window that opens, enter a name for the group and click the **OK** button.

As a result, a new administration group folder with the specified name appears in the console tree.

The application allows creating a hierarchy of administration groups based on the structure of Active Directory or the domain network's structure. Also, you can create a structure of groups from a text file.

► *To create a structure of administration groups:*

1. In the console tree, select the **Managed devices** folder.
2. In the context menu of the **Managed devices** folder, select **All Tasks** → **Create groups structure**.

As a result, the New Administration Group Structure Wizard launches. Follow the instructions of the Wizard.

## Moving administration groups

You can move nested administration groups within the groups hierarchy.

An administration group is moved together with all nested groups, slave Administration Servers, devices, group policies and tasks. The system will apply to the group all the settings that correspond to its new position in the hierarchy of administration groups.

The name of the group should be unique within one level of the hierarchy. If a group with the same name already exists in the folder into which you move the administration group, you should change the name of the latter. If you have not changed the name of the group being moved, an index in (**<serial number>**) format is automatically added to its name when it is moved, for example: **(1)**, **(2)**.

You cannot rename the **Managed devices** group because it is a built-in element of Administration Console.

► *To move a group to another folder of the console tree:*

1. Select a group to move from the console tree.
2. Do one of the following:
  - Move the group using the context menu:
    1. Select **Cut** from the context menu of the group.
    2. Select **Paste** from the context menu of the administration group to which you need to move the selected group.
  - Move the group using the main application menu:
    - a. In the main menu, select **Action** → **Cut**.
    - b. Select the administration group to which you need to move the selected group, from the console tree.
    - c. In the main menu, select **Action** → **Paste**.
  - Move the group to another one in the console tree using the mouse.

## Deleting administration groups

You can delete an administration group if it contains no slave Administration Servers, nested groups, or client devices, and if no group tasks or policies have been created for it.

Before deleting an administration group, you must delete all slave Administration Servers, nested groups, and client devices from that group.

► *To delete a group:*

1. Select an administration group in the console tree.
2. Do one of the following:
  - Select **Remove** from the context menu of the group.
  - In the main application menu, select **Action** → **Remove**.
  - Press the **DEL** key.

# Automatic creation of a structure of administration groups

Kaspersky Security Center allows you to create a structure of administration groups using the Groups hierarchy creation wizard.

The Wizard creates a structure of administration groups based on the following data:

- structures of Windows domains and workgroups;
- structures of Active Directory groups;
- contents of a text file created by the administrator manually.

When generating the text file, the following requirements should be met:

- The name of each new group must begin with a new line; and the delimiter must begin with a line break. Blank lines are ignored.

## Example:

Office 1

Office 2

Office 3

Three groups of the first hierarchy level will be created in the target group.

- The name of the nested group must be entered with a slash mark (/).

## Example:

Office 1/Division 1/Department 1/Group 1

Four subgroups nested into each other will be created in the target group.

- To create several nested groups of the same hierarchy level, you must specify the "full path to the group".

### Example:

Office 1/Division 1/Department 1

Office 1/Division 2/Department 1

Office 1/Division 3/Department 1

Office 1/Division 4/Department 1

One group of the first hierarchy level Office 1 will be created in the destination group; this group will include four nested groups of the same hierarchy level: "Division 1", "Division 2", "Division 3", and "Division 4". Each of these groups will include the "Department 1" group.

If you use a Wizard to create the administration groups structure, the network integrity is preserved: new groups do not replace the existing ones. A client device cannot be included in an administration group a second time because the device is removed from the **Unassigned devices** group when it is moved to the administration group.

If, when creating the administration group structure, a device was not included in the **Unassigned devices** group for some reason (it was shut down or disconnected from the network), it will not be automatically moved to the administration group. You can add devices to administration groups manually after the Wizard finishes.

► *To launch the automatic creation of a structure of administration groups:*

1. Select the **Managed devices** folder in the console tree.
2. In the context menu of the **Managed devices** folder, select **All Tasks** → **Create groups structure**.

As a result, the New Administration Group Structure Wizard launches. Follow the instructions of the Wizard.

# Automatic installation of applications to devices in an administration group

You can specify which installation packages must be used for automatic remote installation of Kaspersky Lab applications to client devices that have recently been added to a group.

► *To configure automatic installation of applications to new devices in an administration group:*

1. In the console tree, select the required administration group.
2. Open the properties window of this administration group.
3. In the **Automatic installation** section, select the installation packages to be installed to new computers by selecting the check boxes next to the names of the installation packages of the required applications. Click **OK**.

As a result, group tasks will be created that will be run on the client devices immediately after they are added to the administration group.

If some installation packages of one application were selected for automatic installation, the installation task will be created for the most recent application version only.

---

# Managing applications remotely

This section contains information about how to perform remote management of Kaspersky Lab applications installed on devices by using policies, policy profiles, tasks, and local settings of applications.

## In this section:

Managing policies .....	<a href="#">103</a>
Managing policy profiles .....	<a href="#">110</a>
Managing tasks.....	<a href="#">116</a>
Viewing and editing the local application settings .....	<a href="#">128</a>

## Managing policies

The applications installed on client devices are centrally configured by defining policies.

Policies created for applications in an administration group are displayed in the workspace, on the **Policies** tab. The name of each policy is preceded by an icon that indicates its status (see section "Statuses of devices, tasks, and policies" on page [368](#)).

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

A policy is applied as follows: if a device is running resident tasks (real-time protection tasks), they keep running with the new values of the settings. Any periodic tasks (on-demand scan, update of application databases) started keep running with the values unchanged. Next time they are run with the new values of the settings.

If Administration Servers are structured hierarchically, slave Administration Servers receive policies from the master Administration Server and distribute them to client devices. When inheritance is enabled, policy settings can be modified on the master Administration Server. After that,

any changes made to the policy settings are propagated to inherited policies on slave Administration Servers.

If the connection is terminated between the master and slave Administration Servers, the policy on the slave Server continues, using the applied settings. Policy settings modified on the master Administration Server are distributed to a slave Administration Server after the connection is re-established.

If inheritance is disabled, policy settings can be modified on a slave Administration Server independently from the master Administration Server.

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.

The results of policy distribution to the slave Administration Server are displayed in the policy properties window of the console on the master Administration Server.

The results of policy distribution to client devices are displayed in the policy properties window of the Administration Server to which they are connected.

## In this section:

Creating a policy .....	<a href="#">105</a>
Displaying inherited policy in a subgroup.....	<a href="#">106</a>
Activating a policy .....	<a href="#">106</a>
Activating a policy automatically at the Virus outbreak event .....	<a href="#">107</a>
Applying an out-of-office policy .....	<a href="#">107</a>
Modifying a policy. Rolling back changes .....	<a href="#">107</a>
Deleting a policy .....	<a href="#">108</a>
Copying a policy .....	<a href="#">108</a>
Exporting a policy.....	<a href="#">109</a>
Importing a policy.....	<a href="#">109</a>
Converting policies.....	<a href="#">110</a>



# Creating a policy

In Administration Console, you can create policies directly in the folder of the administration group for which a policy is to be created, or in the workspace of the **Policies** folder.

► *To create a policy in the folder of an administration group:*

1. In the console tree, select an administration group for which you want to create a policy.
2. In the workspace of the group, open the **Policies** tab.
3. Run the New Policy Wizard by clicking the **Create a policy** button.

This starts the New Policy Wizard. Follow the instructions of the Wizard.

► *To create a policy in the workspace of the **Policies** folder:*


1. In the console tree, select the **Policies** folder.
2. Run the New Policy Wizard by clicking the **Create a policy** button.

This starts the New Policy Wizard. Follow the instructions of the Wizard.

You can create several policies for one application from the group, but only one policy can be active at a time. When you create a 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 blocked from editing (lock  is set) take effect on client devices regardless of which settings had been previously specified for the application.

# Displaying inherited policy in a subgroup

► *To enable the display of inherited policies for a nested administration group:*

1. In the console tree select the administration group for which inherited policies should be displayed.
2. In the workspace for the selected group select the **Policies** tab.
3. From the context menu of the list of policies select **View** → **Inherited Policies**.

As a result, inherited policies are displayed on the list of policies with this icon:

-  – if they were inherited from a group created on the master Administration Server.
-  – if they were inherited from a top-level group

When the settings inheritance mode is enabled, inherited policies are only available for modification in the group in which they have been created. Modification of inherited policies is not available in the group, which inherits them.

## Activating a policy

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

1. In the workspace of the group, on the **Policies** tab select the policy that you need to make active.
2. To activate the policy, perform one of the following actions:
  - From the context menu of the policy select **Active policy**.
  - In the policy properties window open the **General** section and select **Active policy** from the **Policy status** settings group.

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.

## Activating a policy automatically at the Virus outbreak event

- ▶ *To make a policy perform the automatic activation at the Virus outbreak event:*
  1. In the Administration Server properties window open the **Virus outbreak** section.
  2. Open the **Policy activation** window by clicking the **Configure policies to activate on "Virus outbreak" event** link and add the policy to the selected list of policies activated upon detection of a virus outbreak.

If a policy has been activated on the *Virus outbreak* event, the manual mode is the only way that you can use to return to the previous policy.

## Applying an out-of-office policy

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

- ▶ *To apply a selected out-of-office policy:*

In the properties window of the policy, open the **General** section and select **Out-of-office policy** from the **Policy status** settings group.

The policy will be applied to the devices if they are disconnected from the corporate network.

## Modifying a policy. Rolling back changes

- ▶ *To edit a policy:*
  1. In the console tree, select the **Policies** folder.
  2. In the workspace of the **Policies** folder, select a policy and proceed to the policy properties window using the context menu.
  3. Make the relevant changes.
  4. Click **Apply**.

The changes made to the policy will be saved in the policy properties, in the **Revision history** section.

You can roll back changes made to the policy, if necessary.

► *To roll back changes made to the policy:*

1. In the console tree, select the **Policies** folder.
2. Select the policy in which changes need to be rolled back, and proceed to the policy properties window using the context menu.
3. In the policy properties window, select the **Revision history** section.
4. In the list of policy revisions, select the number of the revision to which you need to roll back changes.
5. Click the **Advanced** button and select the **Roll back** value in the drop-down list.

## Deleting a policy

► *To delete a policy:*

1. In the workspace of an administration group, on the **Policies** tab, select the policy that you need to delete.
2. Delete the policy using one of the following methods:
  - By selecting **Remove** from the context menu of the policy.
  - By clicking the **Delete policy** link located in the workspace, in the section intended for handling the selected policy.

## Copying a policy

► *To copy a policy:*

1. In the workspace of the required group, on the **Policies** tab select a policy.
2. From the context menu of the policy select **Copy**.
3. In the console tree, select a group to which you want to add the policy.

You can add a policy to the group, from which it was copied.

4. From the context menu of the list of policies for the selected group, on the **Policies** tab select **Paste**.

As a result, the policy is copied with all its settings and applied to the devices within the group into which it was copied. If you paste the policy to the same group from which it has been copied, the (**<sequence number>**) index is automatically added to the name of the policy: for example, **(1)**, **(2)**.

An active policy becomes inactive while it is copied. If necessary, you can make it active.

## Exporting a policy

► *To export a policy:*

1. Export a policy in one of the following ways:
  - In the context menu of the policy, select **All Tasks** → **Export**.
  - By clicking the **Export policy to file** link located in the workspace, in the section intended for handling the selected policy.
2. In the **Save as** window that opens, specify the name of the policy file and the path to save it. Click the **Save** button.

## Importing a policy

► *To import a policy:*

1. In the workspace of the required group, on the **Policies** tab select one of the following methods of importing policies:
  - By selecting **All Tasks** → **Import** from the context menu of the list of policies.
  - Click the **Import policy from file** link in the management block for policy list.
2. In the window that opens, specify the path to the file from which you want to import a policy. Click the **Open** button.

The policy is then displayed in the list of policies.

If a policy with the name coinciding with that of the imported policy is already included on the list of policies, the name of the imported policy will be expanded with the with a suffix (**<next number>**), for example: **(1)**, **(2)**.

# Converting policies

Kaspersky Security Center can convert policies from earlier versions of Kaspersky Lab applications into those from up-to-date versions of the same applications.

Conversion is available for policies of the following applications:

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4.
- Kaspersky Endpoint Security 8 for Windows.
- Kaspersky Endpoint Security 10 for Windows.

► *To convert policies:*

1. From the console tree select Administration Server for which you want to convert policies.
2. In the Administration Server context menu, select **All Tasks** → **Policies and Tasks Batch Conversion Wizard**.

The Policies and Tasks Batch Conversion Wizard. Follow the instructions of the Wizard.

After the wizard finishes its operation, new policies are created, which use the settings of policies from earlier versions of Kaspersky Lab applications.

# Managing policy profiles

This section contains information about policy profiles that are used for effective management of groups of client devices. The advantages of policy profiles are described, as well as ways of applying them. This section also provides instructions on how to create, configure and delete policy profiles.

## About the policy profile

A 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 were 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 the 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 because export and import of profiles are supported, as well as creation (by copying) of new profiles based on existing ones.
- Several policy profiles can be active on a single client device simultaneously.
- Hierarchy of policies is supported.

### **Profile activation rules. Priorities of profiles**

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

- Network Agent on a client device connects to the Administration Server that has a specified set of connection settings, such as Administration Server address, port number, and so forth.
- The client device is offline.
- The client device has been assigned specified tags.
- The client device is located in a specific unit of Microsoft Active Directory® and 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.

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

### **Policies in the hierarchy of administration groups**

Although 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 appear as follows: *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, that is, 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 to 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.



# Creating a policy profile

Creating a policy profile is only available for policies of Kaspersky Endpoint Security 10 Service Pack 1 for Windows.

► *To create a policy profile for an administration group:*

1. In the console tree, select the administration group for which you want to create a policy profile.
2. In the workspace of the group, open the **Policies** tab.
3. Select a policy and switch to the policy properties window using the context menu.
4. Open the **Policy profile** section in the policy properties window and click the **Add** button.
5. In the **Properties: New profile** window, configure the policy profile:
  - In the **General** section, specify the name of the profile.  
The profile name cannot include more than 100 characters.
  - Enable or disable the profile using the **Enable profile** check box.  
If this check box is cleared, the profile is not used for managing the device.
6. In the **Activation rules** section, create activation rules for the profile.
  - Click the **Add** button.
  - Define the policy profile activation rules in the **Property: New rule**.
  - Click **OK**.
7. Edit the policy settings in the corresponding sections.
8. After the profile is configured and activation rules are created, save the changes by clicking the **OK** button.

As a result, the profile will be saved. The profile will be activated on the device when the activation rules are triggered.

Profiles that have been created for a policy are displayed in the policy properties, in the **Policy profiles** section. You can modify a policy profile and change the profile priority (see section "Editing a policy profile" on page [114](#)), as well as remove the profile (see section "Removing a policy profile" on page [115](#)).

Several policy profiles can be activated simultaneously when the activation rules trigger.

## Modifying a policy profile

### Editing the settings of a policy profile

Editing a policy profile is only available for policies of Kaspersky Endpoint Security 10 Service Pack 1 for Windows.

► *To modify a policy profile:*

1. In the console tree, select the administration group for which the policy profile should be modified.
2. In the workspace of the group, open the **Policies** tab.
3. Select a policy and switch to the policy properties window using the context menu.
4. Open the **Policy profile** section in the policy properties.

This section contains a list of profiles that have been created for the policy. Profiles are displayed on the list in accordance with their priorities.

5. Select a policy profile and click the **Properties** button.
6. Configure the profile in the properties window:
  - If necessary, in the **General** section, change the profile name and enable or disable the profile using the **Enable profile** check box.
  - In the **Activation rules** section, edit the profile activation rules.
  - Edit the policy settings in the corresponding sections.
7. Click **OK**.

The modified settings will take effect either after the device is synchronized with the Administration Server (if the policy profile is active), or after an activation rule is triggered (if the policy profile is inactive).

### Changing the priority of a policy profile

The priorities of policy profiles define the activation order of profiles on a client device. Priorities are used if identical activation rules are set for different policy profiles.

For example, two policy profiles have been created: *Profile 1* and *Profile 2*, which differ by the respective values of a single setting (*Value 1* and *Value 2*). The priority of *Profile 1* is higher than that of *Profile 2*. Moreover, there are also profiles with priorities that are lower than that of *Profile 2*. The activation rules for those profiles are identical.

When an activation rule triggers, *Profile 1* will be activated. The setting on the device will take *Value 1*. If you remove *Profile 1*, then *Profile 2* will have the highest priority, so the setting will take *Value 2*.

On the list of policy profiles, profiles are displayed in accordance with their respective priorities. The profile with the highest priority is ranked first. You can change the priority of a profile using

the  and  buttons.

## Removing a policy profile

► *To remove a policy profile:*

1. In the console tree, select the administration group for which you want to remove a policy profile.
2. In the workspace of the administration group, select the **Policies** tab.
3. Select a policy and switch to the policy properties window using the context menu.
4. Open the **Policy profile** section in the properties of the policy of Kaspersky Endpoint Security.
5. Select the policy profile that you want to remove and click the **Remove** button.

As a result, the policy profile will be removed. The active status will pass either to another policy profile whose activation rules are triggered on the device, or to the policy.

## Managing tasks

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

Tasks are subdivided into the following types:

- *Group tasks.* Tasks that are performed on the devices of the selected administration group.
- *Administration Server tasks.* Tasks that are performed on the Administration Server.
- *Tasks for specific devices.* Tasks that are performed on selected devices, regardless of whether they are included in any administration groups.
- *Local tasks.* Tasks that are performed on a specific device.

An application task can only be created if the management plug-in for that application is installed on the administrator's workstation.

You can compile a list of devices for which a task will be created by using one of the following methods:

- Select networked devices discovered by Administration Server.
- Manually specify a list of devices. You can use an IP address (or IP range), NetBIOS name, or DNS name as the device address.
- Import a list of devices from a TXT file containing the addresses of devices to be added (each address must be placed in an individual line).

If you import a list of devices from a file or create one manually, and devices are identified by their names, the list can only contain devices for which information has already been added to the Administration Server database when connecting those devices or during a network poll.

For each application, you can create any number of group tasks, tasks for specific devices, or local tasks.

The exchange of information about tasks between an application installed on a device and the Kaspersky Security Center database is carried out when Network Agent is connected to Administration Server.

You can make changes to the settings of tasks, view their progress, copy, export, import, and delete them.

Tasks are started on a device only if the application for which the task was created is running. When the application is not running, all running tasks are canceled.

Results of completed tasks are saved in the event logs of Microsoft Windows and Kaspersky Security Center, both centrally on the Administration Server and locally on each device.

## Creating a group task

In Administration Console, you can create tasks directly in the folder of the administration group for which a group task is to be created, or in the workspace of the **Tasks** folder.

► *To create a group task in the folder of an administration group:*

1. In the console tree, select the administration group for which you want to create a task.
2. In the group workspace, open the **Tasks** tab.
3. Run the task creation by clicking the **Create a task** button.

This starts the New Task Wizard. Follow the instructions of the Wizard.

► *To create a task in the workspace of the **Tasks** folder:*

1. In the console tree, select the **Tasks** folder.
2. Run the task creation by clicking the **Create a task** button.

This starts the New Task Wizard. Follow the instructions of the Wizard.

# Creating an Administration Server task

The Administration Server performs the following tasks:

- Automatic distribution of reports.
- Downloading of updates to the repository.
- Backup of Administration Server data.
- Maintenance of the database.
- Windows Update synchronization.
- Creation of an installation package based on the OS image of a reference device.

On a virtual Administration Server, only the automatic report delivery task and the installation package creation task based on the reference device OS image are available. The repository of the virtual Administration Server displays updates downloaded to the master Administration Server. Backup of virtual Server's data is performed along with backup of master Administration Server's data.

► *To create an Administration Server task:*

1. In the console tree, select the **Tasks** folder.
2. Start creating the task in one of the following ways:
  - In the console tree, in the context menu of the **Tasks** folder, select **Create** → **Task**.
  - Click the **Create a task** button in the workspace of the **Tasks** folder.

This starts the New Task Wizard. Follow the instructions of the Wizard.

The **Download updates to the repository**, **Perform Windows Update synchronization**, **Database maintenance**, and **Backup of Administration Server data** tasks can be created only once. If the **Download updates to the repository**, **Database maintenance**, **Back up Administration Server data**, and **Windows Update synchronization** tasks have been already created for the Administration Server, they will not be displayed in the task type selection window of the New Task Wizard.

# Creating a task for specific devices

In Kaspersky Security Center, you can create tasks for specific devices. Devices joined in a set can be included in various administration groups or remain outside of any administration groups. Kaspersky Security Center can perform the following main tasks for specific devices:

- Install application remotely (for more information, please refer to the *Kaspersky Security Center Implementation Guide*).
- Send message for user (see section "Sending a message to the users of devices" on page [143](#)).
- Change the Administration Server (see section "Changing the Administration Server for client devices" on page [142](#)).
- Manage the device (see section "Remotely turning on, turning off, and restarting client devices" on page [143](#)).
- Verify updates (see section "Verifying downloaded updates" on page [291](#)).
- Distribute installation package (for more information, see *Kaspersky Security Center Implementation Guide*).
- Install application remotely on the slave Administration Servers (for more information, see *Kaspersky Security Center Implementation Guide*).
- Uninstall application remotely (for more information, see *Kaspersky Security Center Implementation Guide*).

► *To create a task for specific devices:*

1. In the console tree, select the **Tasks** folder.
2. Start creating the task in one of the following ways:
  - In the console tree, in the context menu of the **Tasks** folder, select **Create** → **Task**.
  - Click the **Create a task** button in the workspace of the **Tasks** folder.

This starts the New Task Wizard. Follow the instructions of the Wizard.

# Creating a local task

► *To create a local task for a device:*

1. Select the **Devices** tab in the workspace of the group that includes the device.
2. From the list of devices on the **Devices** tab, select the device for which a local task must be created.
3. Start creating the task for the selected device by using one of the following methods:
  - Click the **Perform action** button and select **Create a task** in the drop-down list.
  - Click the **Create a task** link in the workspace of the device.
  - From the device properties as follows:
    - a. In the context menu of the device, select **Properties**.
    - b. In the device properties window that opens, select the **Tasks** section and click **Add**.

This starts the New Task Wizard. Follow the instructions of the Wizard.



Detailed instructions on how to create and configure local tasks are provided in the Guides for the respective Kaspersky Lab applications.

# Displaying an inherited group task in the workspace of a nested group

► *To enable the display of inherited tasks of a nested group in the workspace:*

1. Select the **Tasks** tab in the workspace of a nested group.
2. In the workspace of the **Tasks** tab, click the **Show inherited tasks** button.

As a result, inherited tasks are displayed on the list of tasks with one of the following icons:

-  – if they were inherited from a group created on the master Administration Server.
-  – if they were inherited from a top-level group



If the inheritance mode is enabled, inherited tasks can only be edited in the group in which they have been created. Inherited tasks cannot be edited in the group, which inherits the tasks.

## Automatically turning on devices before starting a task

Kaspersky Security Center lets you configure the task settings in such a way that the operating system is loaded on turned off devices before the task is started.

► *To configure the automatic startup of devices before starting a task:*

1. In the task properties window, select the **Schedule** section.
2. Click the **Advanced** link to open the window intended for configuring actions on devices.
3. In the **Advanced** window that opens, select the **Activate device before the task is started through Wake On LAN (min)** check box and specify the time interval in minutes.

After this, all devices that were shut down will automatically turn on the specified number of minutes before the task start, and the operating system will load on them.

Automatic loading of the operating system is only available on devices that support the Wake-on-LAN feature.

## Automatically turning off a device after a task is completed

Kaspersky Security Center lets you configure the settings of a task in such a way that the devices to which it is applied are automatically turned off after the task is completed.

► *To automatically turn off the devices after the task is complete:*

1. In the task properties window, select the **Schedule** section.
2. Click the **Advanced** link to open the window intended for configuring actions on devices.
3. In the **Advanced** window that opens, select the **Shut down device when task is complete** check box.

## Limiting task run time

► *To limit the time during which a task is run on devices:*

1. In the task properties window, select the **Schedule** section.
2. Open the window intended for configuration of actions on client devices, by clicking **Advanced**.
3. In the **Advanced** window that opens, select the **Stop if the task is taking longer than (min)** check box and specify the time interval in minutes.

As a result, if the task is not yet complete on the device when the specified time interval expires, Kaspersky Security Center stops the task automatically.

## Exporting a task

You can export group tasks and tasks for specific devices into a file. Administration Server tasks and local tasks are not available for export.

► *To export a task:*

1. In the context menu of the task, select **All Tasks** → **Export**.
2. In the **Save as** window that opens, specify the name of the file and the path to save it.
3. Click the **Save** button.

The rights of local users are not exported.

# Importing a task

You can import group tasks and tasks for specific devices. Administration Server tasks and local tasks are not available for import.

► *To import a task:*

1. Select the task list to which the task should be imported:
  - If you want to import the task to the list of group tasks, in the workspace of the relevant administration group, select the **Tasks** tab.
  - If you want to import a task into the list of tasks for specific devices, select the **Tasks for specific devices** folder in the console tree.
2. Select one of the following options to import the task:
  - In the context menu of the task list, select **All Tasks** → **Import**.
  - Click the **Import task from file** link in the task list management block.
3. In the window that opens, specify the path to the file from which you want to import task.
4. Click the **Open** button.

As a result, the task is displayed in the list of tasks.

If a task with the same name as that of the imported task is already included in the selected list, an index in (<serial number>) format will be added to the name of the imported one, for example: (1), (2).

# Converting tasks

You can use Kaspersky Security Center to convert tasks from earlier versions of Kaspersky Lab applications into those from up-to-date versions of the applications.

Conversion is available for tasks of the following applications:

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4.
- Kaspersky Endpoint Security 8 for Windows.
- Kaspersky Endpoint Security 10 for Windows.

► *To convert tasks:*

1. In the console tree, select an Administration Server for which you want to convert tasks.
2. In the Administration Server context menu, select **All Tasks** → **Policies and Tasks Batch Conversion Wizard**.

The Policies and Tasks Batch Conversion Wizard. Follow the instructions of the Wizard.

After the wizard completes its operation, new tasks are created, which use the settings of tasks from earlier versions of the applications.

## Starting and stopping a task manually

You can start and stop tasks using two methods: from the context menu of the task or in the properties window of the client device to which the task has been assigned.

Users included in the **KLAdmins group** (see section "Rights of access to Administration Server and its objects" on page [85](#)) can run group tasks from the device's context menu.

► *To start or stop a task from the context menu or the properties window of the task:*

1. In the list of tasks, select a task.
2. Start or stop the task in one of the following ways:
  - In the context menu of the task, select **Start** or **Stop**.
  - In the task properties window, in the **General** section, click **Start** or **Stop**.


► *To start or stop a task from the context menu or the properties window of the client device:*

1. In the list of devices, select the device.

2. Start or stop the task in one of the following ways:

- In the context menu of the device, select **All Tasks** → **Run a Task**. Select the relevant task from the list of tasks.

The list of devices to which the task is assigned will be replaced with the device that you have selected. The task starts.

- In the device properties window, open the **Tasks** section and click the  or



## Pausing and resuming a task manually

► *To pause or resume a running task:*

1. In the list of tasks, select a task.

2. Pause or resume the task using one of the following methods:

- In the context menu of the task, select **Pause** or **Resume**.
- In task properties window, select the **General** section and click **Pause** or **Resume**.

## Monitoring task execution

► *To monitor task execution,*

In the task properties window, select the **General** section.

In the middle part of the **General** section, the current task status is displayed.

# Viewing task run results stored on Administration Server

Kaspersky Security Center lets you view the results for group tasks, tasks for specific devices, and Administration Server tasks. No run results can be viewed for local tasks.

► *To view the task results:*

1. In the task properties window, select the **General** section.
2. Click the **Results** link to open the **Task results** window.

# Configuring filtering of information about task run results

Kaspersky Security Center lets you filter information about results for group tasks, tasks for specific devices, and Administration Server tasks. No filtering is available for local tasks.

► *To set up the filtering of information about task run results:*

1. In the task properties window, select the **General** section.
2. Click the **Results** link to open the **Task results** window.

The table in the upper part of the window contains a list of all devices for which the task is assigned. The table in the lower part of the window displays the results of the task performed on the selected device.

3. Right-click the relevant table to open the context menu and select **Filter**.
4. In the **Set filter** window that opens, define the filter settings in the **Events**, **Devices**, and **Time** sections. Click **OK**.

As a result, the **Task results** window displays information that meets the settings specified in the filter.

# Modifying a task. Rolling back changes

## ► *To modify a task:*

1. In the console tree, select the **Tasks** folder.
2. In the workspace of the **Tasks** folder, select a task and proceed to the task properties window using the context menu.
3. Make the relevant changes.

In the **Exclusions from task scope** section, you can set up the list of subgroups to which the task is not applied.

4. Click **Apply**.

The changes made to the task will be saved in the task properties, in the **Revision history** section.

You can roll back changes made to a task, if necessary.

## ► *To roll back changes made to a task:*

1. In the console tree, select the **Tasks** folder.
2. Select the task in which changes need to be rolled back, and proceed to the task properties window using the context menu.
3. In the task properties window, select the **Revision history** section.
4. In the list of task revisions, select the number of the revision to which you need to roll back changes.
5. Click the **Advanced** button and select the **Roll back** value in the drop-down list.

# Viewing and editing the local application settings

The Kaspersky Security Center administration system allows remote management of local application settings on devices via the Administration Console.

*Local application settings* are the settings of an application that are specific for a device. You can use Kaspersky Security Center to set local application settings for devices included in administration groups.

Detailed descriptions of settings of Kaspersky Lab applications are provided in respective Guides.

► *To view or change application's local settings:*

1. In the workspace of the group to which the relevant device belongs, select the **Devices** tab.
2. In the device properties window, in the **Applications** section, select the necessary application.
3. Open the application properties window by double-clicking the application name or by clicking the **Properties** button.

As a result, the local settings window of the selected application opens so that you can view and edit those settings.

You can change the values of the settings that have not been prohibited for modification by a group policy (i.e., those not marked with the "lock" in a policy).



---

# Managing client devices

This section contains information about working with client devices.

## In this section:

Connecting client devices to the Administration Server .....	<a href="#">130</a>
Manually connecting a client device to the Administration Server. Klmover utility .....	<a href="#">131</a>
Tunneling the connection between a client device and the Administration Server .....	<a href="#">133</a>
Remotely connecting to the desktop of a client device .....	<a href="#">133</a>
Configuring the restart of a client device.....	<a href="#">136</a>
Auditing actions on a remote client device.....	<a href="#">137</a>
Checking the connection between a client device and the Administration Server .....	<a href="#">138</a>
Identifying client devices on the Administration Server.....	<a href="#">140</a>
Adding devices to an administration group .....	<a href="#">141</a>
Changing the Administration Server for client devices.....	<a href="#">142</a>
Remotely turning on, turning off, and restarting client devices .....	<a href="#">143</a>
Sending a message to device users.....	<a href="#">143</a>
Controlling changes in the status of virtual machines.....	<a href="#">144</a>
Automatic device tagging .....	<a href="#">145</a>
Remote diagnostics of client devices. Kaspersky Security Center remote diagnostics utility ...	<a href="#">147</a>

# Connecting client devices to the Administration Server

The connection of the client device to Administration Server is established by the Network Agent installed on the client device.

When a client device connects to Administration Server, the following operations are performed:

- Automatic data synchronization:
  - Synchronization of the list of applications installed on the client device.
  - Synchronization of the policies, application settings, tasks, and task settings.
- Retrieval of up-to-date information about the condition of applications, execution of tasks and applications' operation statistics by the Server.
- Delivery of the event information to Administration Server for processing.

Automatic data synchronization is performed regularly in accordance with the Network Agent settings (for example, every 15 minutes). You can specify the connection interval manually.

Information about an event is delivered to Administration Server as soon as it occurs.

Kaspersky Security Center lets you configure connection between a client device and Administration Server so that the connection remains active after all operations are completed. Uninterrupted connection is necessary in cases when real-time monitoring of application status is required and Administration Server is unable to establish a connection to the client for some reason (for example, connection is protected by a firewall, opening of ports on the client device is not allowed, or the client device IP address is unknown). You can establish an uninterrupted connection between a client device and Administration Server in the device properties window in the **General** section.

We recommend that you establish an uninterrupted connection with the most important devices. The total number of connections simultaneously maintained by the Administration Server is limited to a few hundreds.

When synchronizing manually, the system uses an auxiliary connection method, with which connection is initiated by Administration Server. Before establishing the connection on a client device, you must open the UDP port. Administration Server sends a connection request to the UDP port of the client device. In response, the Administration Server's certificate is verified. If the Server certificate matches the certificate copy stored on the client device, the connection is established.

The manual launch of synchronization is also used for obtaining up-to-date information about the condition of applications, execution of tasks, and applications' operation statistics.

## Manually connecting a client device to the Administration Server. Klmover utility

If you need to manually connect a client device to the Administration Server, you can use the klmover utility on the client device.

When installing Network Agent on a client device, the utility is automatically copied to the Network Agent installation folder.

- ▶ *To manually connect a client device to the Administration Server by using the klmover utility:*

On the device, start the klmover utility from the command line.

When started from the command line, the klmover utility can perform the following actions (depending on the keys in use):

- connects Network Agent to Administration Server with the specified settings;
- records the operation results into the event log file or displays them on the screen.

Utility command line syntax:

```
klmover [-logfile <file name>] [-address <server address>] [-pn  
<port number>] [-ps <SSL port number>] [-nossl] [-cert <path  
to certificate file>] [-silent] [-dupfix]
```

The command-line parameters are as follows:

- `-logfile <file name>`– record the utility run results into a log file.

By default information is saved in the standard output stream (stdout). If the key is not in use, results and error messages are displayed on the screen.

- `-address <server address>`– address of Administration Server for connection.

You can specify an IP address, the NetBIOS name, or DNS name of a device as its address.

- `-pn <port number>`– number of the port via which non-encrypted connection to Administration Server will be established.

The default port number is 14000.

- `-ps <SSL port number>`– number of the SSL port via which encrypted connection to Administration Server is established using the SSL protocol.

The default port number is 13000.

- `-noSSL`– use non-encrypted connection to Administration Server.

If the key is not in use, Network Agent is connected to Administration Server over the encrypted SSL protocol.

- `-cert <path to certificate file>`– use the specified certificate file for authentication of access to Administration Server.

If the key is not in use, Network Agent receives a certificate at the first connection to Administration Server.

- `-silent` – run the utility in silent mode.

Using the key may be useful if, for example, the utility is started from the logon script at the user's registration.

- `-dupfix` – the key is used if Network Agent has been installed using a method that differs from the usual one (with the distribution package) – for example, by recovering it from an ISO disk image.

# Tunneling the connection between a client device and the Administration Server

Connection tunneling between a remote client device and Administration Server is required if the port used for connection to Administration Server is not available on the device. The port on the device may be unavailable in the following cases:

- The remote device is connected to a local network that uses a NAT mechanism.
- The remote device is part of the local network of Administration Server, but its port is closed by a firewall.

► *To tunnel the connection between a client device and Administration Server:*

1. In the console tree, select the folder of the group that contains the client device.
2. On the **Devices** tab, select the device.
3. In the context menu of the device, select **All Tasks** → **Connection Tunneling**.
4. In the **Connection Tunneling** window that opens, create a tunnel.

## Remotely connecting to the desktop of a client device

The administrator can obtain remote access to the desktop of a client device through a Network Agent installed on the device. Remote connection to a device through the Network Agent is also possible if the TCP and UDP ports of the client device are closed.

Upon establishing the connection with the device, the administrator gains full access to information stored on this device and can manage applications installed on it.

Remote connection with a device can be established using two methods:

- Using a standard Microsoft Windows component named Remote Desktop Connection. Connection to a remote desktop is established through the standard Windows utility `mstsc.exe` in accordance with the utility's settings.

Connection to the current remote desktop session of the user is established without the user's knowledge. Once the administrator connects to the session, the device user is disconnected from the session without an advance notification.

- Using the Windows Desktop Sharing technology. When connecting to an existing session of the remote desktop, the session user on the device receives a connection request from the administrator. No information about remote activity on the device and its results will be saved in reports created by Kaspersky Security Center.

The administrator can connect to an existing session on a client device without disconnecting the user who is operating in this session. In this case, the administrator and the session user on the device will share access to the desktop.

The administrator can configure an audit of user activity on a remote client device. During the audit, the application saves information about files on the client device that have been opened and/or modified by the administrator (see section "Audit of actions on a remote client device" on page [137](#)).

To connect to the desktop of a client device through Windows Desktop Sharing, you must meet the following conditions:

- Microsoft Windows Vista or a later Windows operating system is installed on the device.
- Microsoft Windows Vista or a later Windows operating system is installed on the administrator's workstation. The type of operating system of the device hosting Administration Server imposes no restrictions on connection through Windows Desktop Sharing.
- Kaspersky Security Center uses a license for Systems Management.

► *To connect to the desktop of a client device through the Remote Desktop Connection component:*

1. In the Administration Console tree, select the device to which you need to obtain access.
2. In the context menu of the device, select **All Tasks** → **Connect to device** → **Create new RDP session**.

As a result, the standard Windows utility mstsc.exe starts, which helps establishing connection to the remote desktop.

3. Follow the instructions shown in the utility's dialog boxes.

Upon establishing the connection to the device, the desktop is available in the remote connection window of Microsoft Windows.

► *To connect to the desktop of a client device through Windows Desktop Sharing:*

1. In the Administration Console tree, select the device to which you need to obtain access.
2. In the context menu of the device, select **All Tasks** → **Connect to device** → **Desktop Sharing**.
3. In the **Select remote desktop session** window that opens, select the session on the device to which you need to connect.

If connection to the device is established successfully, the desktop of the device will be available in the **Kaspersky Remote desktop session viewer** window.

4. To start interaction with the device, in the main menu of the **Kaspersky Remote desktop session viewer** window, select **Actions** → **Interactive mode**.

## See also:

Kaspersky Security Center licensing options .....	<a href="#">61</a>
---	--------------------

# Configuring the restart of a client device

While using, installing, or removing Kaspersky Security Center, a restart of the device may be required. The application lets you configure the device restart settings.

► *To configure the restart of a client device:*

1. In the console tree, select the administration group for which you need to configure the restart.
2. In the workspace of the group, open the **Policies** tab.
3. Select a policy of Kaspersky Security Center Network Agent in the list of policies, then select **Properties** in the context menu of the policy.
4. In the properties window of the policy, select the **Restart management** section.
5. Select the action that must be performed if a restart of the device is required:
  - Select **Do not restart the operating system** to block the automatic restart.
  - Select **Restart the operating system automatically if needed** to allow automatic restart.
  - Select **Prompt user for action** to enable prompting the user to allow the restart.

You can specify the frequency of restart requests, enable forced restart and forced closure of applications in blocked sessions on the device by selecting the corresponding check boxes.

6. Click the **OK** button to save the changes and close the policy properties window.

As a result, restart of the device will be configured.



# Auditing actions on a remote client device

The application enables auditing of the administrator's actions on a remote client device. During the audit, the application saves information about files on the device that have been opened and/or modified by the administrator. Audit of the administrator's actions is available when the following conditions are met:

- An active Systems Management license is available.
- The administrator has the right to start shared access to the desktop of the remote device.

► *To enable auditing of actions on a remote client device:*

1. In the console tree, select the administration group for which the audit of the administrator's actions should be configured.
2. In the workspace of the group, open the **Policies** tab.
3. Select a policy of Kaspersky Security Center Network Agent, then select **Properties** in the context menu of the policy.
4. In the policy properties window, select the **Desktop sharing** section.
5. Select the **Enable audit** check box.
6. In the **Masks of files of which reading should be monitored** and **Masks of files of which modifications should be monitored** lists, add file masks on which actions should be monitored during the audit.

By default, the application monitors actions on files with txt, rtf, doc, xls, docx, xlsx, odt, pdf extensions.

7. Click the **OK** button to save the changes and close the policy properties window.

This results in configuration of the audit of the administrator's actions on the user's remote device with shared desktop access.

Records of the administrator's actions on the remote device are logged:

- In the event log on the remote device.
- In a file with the syslog extension located in the Network Agent folder on a remote device (for example, C:\ProgramData\KasperskyLab\adminkit\1103\logs).
- In the events database of Kaspersky Security Center.

## Checking the connection between a client device and the Administration Server

Kaspersky Security Center lets you check connections between a client device and Administration Server, automatically or manually.

Automatic check of connection is performed on Administration Server. Manual check of the connection is performed on the device.

### In this section:

Automatically checking the connection between a client device and the Administration Server .....	<a href="#">139</a>
Manually checking the connection between a client device and the Administration Server. Klnagchk utility.....	<a href="#">139</a>

# Automatically checking the connection between a client device and the Administration Server

► *To start an automatic check of the connection between a client device and Administration Server:*

1. In the console tree, select the administration group that includes the device.
2. In the workspace of the administration group, on the **Devices** tab, select the device.
3. In the context menu of the device, select **Check device accessibility**.

This opens a window containing information about the accessibility of the device.

# Manually checking the connection between a client device and the Administration Server. Klnagchk utility

You can check the connection and obtain detailed information about the settings of the connection between a client device and Administration Server using the klnagchk utility.

When installing Network Agent on a device, the klnagchk utility is automatically copied to the Network Agent installation folder.

When started from the command line, the klnagchk utility can perform the following actions (depending on the keys in use):

- Displays on the screen or logs the values of the settings used for connecting the Network Agent installed on the device to Administration Server.
- Records into an event log file Network Agent statistics (since its last startup) and utility operation results, or displays the information on the screen.
- Makes an attempt to establish connection between Network Agent and Administration Server.

If the connection attempt fails, the utility sends an ICMP packet to check the status of the device on which Administration Server is installed.

- ▶ *To check the connection between a client device and Administration Server using the klnagchk utility:*

On the device, start the klnagchk utility from the command line.

Utility command line syntax:

```
klnagchk [-logfile <file name>] [-sp] [-savecert <path  
to certificate file>] [-restart]
```

The command-line parameters are as follows:

- `-logfile <file name>` – record the values of the settings of connection between Network Agent and Administration Server and the utility operation results into a log file.  
  
By default information is saved in the standard output stream (stdout). If the key is not in use, settings, results, and error messages are displayed on the screen.
- `-sp` – show the password for the user's authentication on the proxy server.  
  
The setting is in use if the connection to Administration Server is established via a proxy server.
- `-savecert <filename>` – save the certificate used to access the Administration Server in the specified file.
- `-restart` – restart the Network Agent after the utility has completed.

## Identifying client devices on the Administration Server

Client devices are identified based on their names. A device name is unique among all the names of devices connected to Administration Server.

The name of a device is relayed to Administration Server either when the Windows network is polled and a new device is discovered in it, or during the first connection of the Network Agent installed on a device to Administration Server. By default, the name matches the device name in the Windows network (NetBIOS name). If a device with this name is already registered on the Administration Server, an index with the next sequence number will be added to the new device name, for example: **<Name>-1**, **<Name>-2**. The device is added to the administration group under this name.

# Adding devices to an administration group

► *To include one or several devices in a selected administration group:*

1. In the console tree, open the **Managed devices** folder.
2. In the **Managed devices** folder, select the nested folder that corresponds to the group to which the client devices will be included.

If you want to include the devices in the **Managed devices** group, you can skip this step.

3. In the workspace of the selected administration group, on the **Devices** tab, start the process of including the devices in the group by using one of the following methods:
  - Add the devices to the group by clicking the **Add devices** button in the section intended for managing the list of devices.
  - In the context menu of the list of devices, select **Create** → **Device**.

This will start the Add Devices Wizard. Following its instructions, select a method for adding the devices to the group and create a list of devices to include in the group.

If you create the list of devices manually, you can use an IP address (or an IP range), a NetBIOS name, or a DNS name as the address of a device. You can manually add to the list only devices for which information has already been added to the Administration Server database when connecting the device, or after a network poll.

To import a list of devices from a file, specify a.txt file with a list of addresses of devices to be added. Each address must be specified in a separate line.

After the wizard finishes its operation, the selected devices are included in the administration group and displayed in the list of devices under names generated by Administration Server.

You can add a device to the selected administration group by dragging it from the **Unassigned devices** folder to the folder of that administration group.

# Changing the Administration Server for client devices

You can change the Administration Server that manages client devices to a different Server using the **Change Administration Server** task.

► *To change the Administration Server managing client devices to a different Server:*

1. Connect to the Administration Server that manages the devices.
2. Create the Administration Server change task using one of the following methods:
  - If you need to change the Administration Server for devices included in the selected administration group, create a group task (see section "Creating a group task" on page [117](#)).
  - If you need to change the Administration Server for devices included in different administration groups or in none of the existing groups, create a task for specific devices (see section "Creating a task for specific devices" on page [119](#)).

This starts the New Task Wizard. Follow the instructions of the Wizard. In the **Task type** window of the New Task Wizard select the **Kaspersky Security Center** node, open the **Advanced** folder, and select the **Change Administration Server** task.

3. Run the created task.

After the task is completed, the client devices for which it had been created are put under the management of the Administration Server specified in the task settings.

If the Administration Server supports encryption and data protection and you are creating a **Change Administration Server** task, a warning is displayed stating that, in case any encrypted data is stored on devices, after the devices are put under the management of the new Server, users will be able to access only the encrypted data with which they previously worked. In other cases, no access to encrypted data is provided. For the detailed descriptions of scenarios in which no access to encrypted data is provided please refer to the Kaspersky Endpoint Security 10 for Windows Administrator's Guide.

# Remotely turning on, turning off, and restarting client devices

Kaspersky Security Center lets you remotely manage client devices: turn on, turn off, and restart them.

► *To remotely manage client devices:*

1. Connect to the Administration Server that manages the devices.
2. Create a device management task by using one of the following methods:
  - If you need to turn on, turn off, or restart devices included in a selected administration group, create a group task (see section "Creating a group task" on page [117](#)).
  - If you need to turn on, turn off, or restart devices included in different administration groups or belonging to none of them, create a task for specific devices (see section "Creating a task for specific devices" on page [119](#)).

This starts the New Task Wizard. Follow the instructions of the Wizard. In the **Task type** window of the New Task Wizard, select the **Kaspersky Security Center** node, open the **Advanced** folder, and select the **Manage devices** task.

3. Run the created task.

After the task is complete, the command (turn on, turn off, or restart) will be executed on the selected devices.

# Sending a message to device users

► *To send a message to users of devices:*

1. Connect to the Administration Server that manages the devices.
2. Create a message forwarding task for device users in one of the following ways:
  - If you need to send a message to users of devices included in the selected administration group, create a group task (see section "Creating a group task" on page [117](#)).
  - If you need to send a message to users of devices that belong to different administration groups or do not belong to any of the them at all, create a task for specific devices (see section "Creating a task for specific devices" on page [119](#)).

This starts the New Task Wizard. Follow the instructions of the Wizard. In the **Task type** window, select the **Kaspersky Security Center** node, open the **Advanced** folder and select the **Send message to user** task.

3. Run the created task.

After the task completes, the created message will be sent to the users of the selected devices.

# Controlling changes in the status of virtual machines

Administration Server stores information about the status of managed devices, such as the hardware registry and the list of installed applications, and the settings of managed applications, tasks and policies. If a virtual machine functions as a managed device, the user can restore its status at any time using a previously created snapshot of the virtual machine. As a result, information about the status of the virtual machine on Administration Server may become outdated.

For example, the administrator had created a protection policy on Administration Server at 12:00 P.M., which started to run on virtual machine VM\_1 at 12:01 P.M. At 12:30 P.M., the user of virtual machine VM\_1 changed its status by restoring it from a snapshot made at 11:00 A.M.



As a result, the protection policy stops running on the virtual machine. However, outdated information on Administration Server states that the protection policy on virtual machine VM\_1 keeps running.

Kaspersky Security Center helps controlling all changes in the status of virtual machines.

After each synchronization with a device, Administration Server generates a unique ID, which is stored both on the device side and on the Administration Server side. Before starting the next synchronization, Administration Server compares the values of those IDs on both sides. If the values of the IDs mismatch, Administration Server recognizes the virtual machine as restored from a snapshot. Administration Server resets all the settings of policies and tasks that are active for the virtual machine and sends the up-to-date policies and the list of group tasks to it.

## Automatic device tagging

The application can automatically tag devices. Automatic device tagging is performed using rules. You can create and edit tagging rules in the Administration Server properties window and/or in the properties window of a device.

► *To create and configure automatic device tagging rules:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the context menu of the Administration Server, select **Properties**.
3. In the Administration Server properties window, select the **Tagging rules** section.
4. In the **Tagging rules** section, click the **Add** button.

This opens the **Properties: New rule** window.

5. In the **General** section of the **Properties: New rule** window, configure the general properties of the rule:

- Specify the rule name.

The rule name cannot contain more than 255 characters and cannot include any special characters (\*<>\_?:"|).

- In the **Tag to assign** drop-down list, select a previously added tag or enter a new one.
- Enable or disable the rule using the **Enable rule** check box.

6. In the **Conditions** section, click the **Add** button to add a new condition, or click the **Properties** button to edit an existing condition.

This opens the properties window of the new condition or the selected one.

7. In the window that opens, configure the tagging condition:
  - In the **General** section, specify the condition name.
  - In the **Network** section, configure the triggering of the rule based on the device network properties (device name in the Windows network, belonging to a domain or an IP subnet, etc.).
  - In the **Active Directory** section, configure the triggering of the rule based on whether the device belongs to an Active Directory OU or group.
  - In the **Applications** section, configure the triggering of the rule based on the presence of Network Agent on the device, and on the operating system type, version, and architecture.
  - In the **Virtual machines** section, configure the triggering of the rule based on whether the device belongs to various types of virtual machines.
  - In the **Applications registry** section, configure the triggering of the rule based on the presence of applications of different vendors on the device.
8. After the condition is configured, click the **OK** button in the **Property: New condition** window.

9. Add or configure other conditions of the tagging rule.

The tagging rule conditions that you have added will be displayed in the **Conditions** section of the rule properties window.

10. Click **OK** in the rule properties window.

The tag activation rule is saved. The rule will be applied on devices that meet the rule conditions. When the rule is applied, the tag will be assigned to the devices. A device is automatically assigned multiple tags if the corresponding tagging rules are triggered simultaneously. You can view the list of all added tags in the properties window of any device in the **Tags** section. In the **Tags** section, you can also proceed to the automatic tagging rules by clicking the corresponding link.

# Remote diagnostics of client devices. Kaspersky Security Center remote diagnostics utility

The utility for remote diagnostics of Kaspersky Security Center (hereinafter referred to as the remote diagnostics utility) is designed for remote execution of the following operations on client devices:

- Enabling and disabling tracing, changing the tracing level, downloading the trace file.
- Downloading application settings.
- Downloading event logs.
- Starting diagnostics and downloading diagnostics results.
- Starting and stopping applications.

The remote diagnostics utility is automatically installed on the device together with the Administration Console.

## In this section:

Connecting the remote diagnostics utility to a client device .....	<a href="#">148</a>
Enabling and disabling tracing, downloading the trace file.....	<a href="#">151</a>
Downloading application settings .....	<a href="#">151</a>
Downloading event logs .....	<a href="#">152</a>
Starting diagnostics and downloading its results .....	<a href="#">152</a>
Starting, stopping and restarting applications .....	<a href="#">153</a>

# Connecting the remote diagnostics utility to a client device

► To connect the remote diagnostics utility to a client device:

1. Select any administration group from the console tree.
2. In the workspace, on the **Devices** tab, in the context menu of any device, select **Custom tools** → **Remote diagnostics**.

As a result, the main window of the remote diagnostics utility opens.

3. In the first field of the main window of the remote diagnostics utility, specify which tools you intend to use to connect to the device:

- **Access using Microsoft Windows network.**
- **Access using Administration Server.**

4. If you have selected **Access using Microsoft Windows network** in the first field of the main utility window, perform the following actions:

- In the **Device** field, specify the address of the device to which you need to connect

You can use an IP address, NetBIOS name, or DNS name as the device address.

The default value is the address of the device from whose context menu the utility was started.

- Specify an account for connecting to the device:
  - **Connect as current user** (selected by default). Connecting under the current user account.
  - **Use provided user name and password to connect.**  
Connecting under a provided user account. Specify the **User name** and the **Password** of the required account.

Connection to a device is possible only under the account of the local administrator of the device.

5. If you have selected **Access using Administration Server** in the first field of the main utility window, perform the following actions:

- In the **Administration Server** field, specify the address of the Administration Server from which you intend to connect to the device.

You can use an IP address, NetBIOS or DNS name as the server address.

The default value is the address of Server from which the utility has been run.

- If required, select the **Use SSL**, **Compress traffic**, and **Device belongs to slave Administration Server** check boxes.

If the **Device belongs to slave Administration Server** check box is selected, you can fill in the **Slave Server** field with the name of the slave Administration Server that manages the device by clicking the **Browse** button.

6. To connect to the device, click the **Sign in** button.

This opens the window intended for remote diagnostics of the device (see the figure below). The left part of the window contains links to operations of device diagnostics. The right part of the window contains the object tree of the device with which the utility can operate. The bottom part of the window displays the progress of the utility's operations.

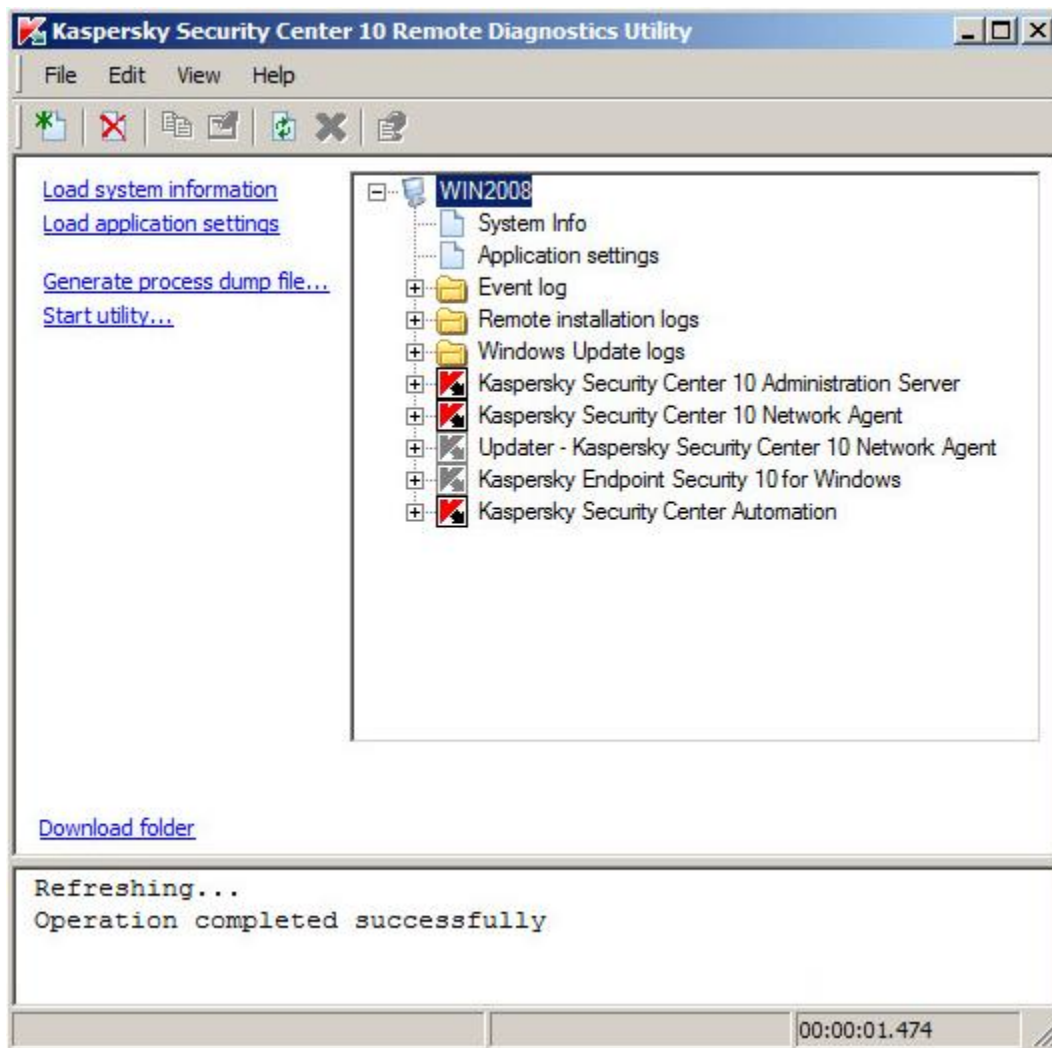


Figure 10. Remote diagnostics utility. Window of remote diagnostics of client computer

The remote diagnostics utility saves files downloaded from devices on the desktop of the device from which it was started.

# Enabling and disabling tracing, downloading the trace file

► *To enable tracing on a remote device, download the trace file, or disable tracing:*

1. Run the remote diagnostics utility and connect to the necessary device.
2. In the objects tree of the device, select the application for which you need to build a trace and enable tracing by clicking the **Enable tracing** link in the left part of the remote diagnostics utility window.

Tracing can be enabled and disabled for applications with self-defense only if the device is connected using tools of Administration Server.

In some cases, the protection application and its task must be restarted in order to enable tracing.

3. In the node of the application for which tracing is enabled, in the **Trace files** folder select the required file and download it by clicking the **Download file** link. For large-sized files only the most recent trace parts can be downloaded.

You can delete the highlighted trace file. The file can be deleted after tracing is disabled.

4. Disable tracing for the selected application by clicking the **Disable tracing** link.

## Downloading application settings

► *To download application settings from a remote device:*

1. Run the remote diagnostics utility and connect to the necessary device.
2. From the objects tree of the remote diagnostics window, select the top node with the name of the device and select the necessary action in the left part of the window:
  - **Load system information.**
  - **Load application settings.**

- **Generate process dump file.**

In the window that opens after you click this link, specify the executable file of the selected application for which you need to generate a dump file.

- **Start utility.**

In the window that opens after you click this link, specify the executable file of the selected utility and its startup settings.

As a result, the selected utility is downloaded and started on the device.

## Downloading event logs

► *To download an event log from a remote device:*

1. Run the remote diagnostics utility and connect to the necessary device.
2. In the **Event log** folder of the device object tree, select the relevant log and download it by clicking the **Download Kaspersky Event Log** link in the left part of the remote diagnostics utility window.

## Starting diagnostics and downloading its results

► *To start diagnostics for an application on a remote device and download its results:*

1. Run the remote diagnostics utility and connect to the necessary device.
2. From the object tree of the device, select the necessary application and start diagnostics by clicking the **Run diagnostics** link.

As a result, a diagnostics report appears in the node of the selected application in the objects tree.

3. Select the newly generated diagnostics report in the objects tree and download it by clicking the **Download file** link.



# Starting, stopping and restarting applications

You can start, stop, and restart applications only if you have connected the device using Administration Server tools.

► *To start, stop, or restart an application:*

1. Run the remote diagnostics utility and connect to the necessary device.
2. From the object tree of the device, select the required application and select an action in the left part of the window:
  - **Stop application.**
  - **Restart application.**
  - **Start application.**

Depending on the action that you have selected, the application will be started, stopped, or restarted.

---

# Managing user accounts

This section provides information about users' accounts and roles supported by the application. This section contains instructions on how to create accounts and roles for users of Kaspersky Security Center. This section also contains instructions on how to handle list of the user's certificates and mobile devices and how to deliver messages to users.

## In this section:

Handling user accounts.....	<a href="#">155</a>
Adding a user account.....	<a href="#">156</a>
Configuring the check of the name of an internal user for uniqueness .....	<a href="#">157</a>
Adding a user group.....	<a href="#">158</a>
Adding a user to a group .....	<a href="#">159</a>
Configuring rights. User roles .....	<a href="#">160</a>
Assigning the user as a device owner .....	<a href="#">162</a>
Delivering messages to users.....	<a href="#">163</a>
Viewing the list of a user's mobile devices.....	<a href="#">164</a>
Installing a certificate for a user .....	<a href="#">164</a>
Viewing the list of certificates handed to a user .....	<a href="#">165</a>

# Handling user accounts

Kaspersky Security Center allows managing user accounts and groups of accounts.

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.
- Accounts of internal users (see section "Handling internal users" on page [94](#)). These accounts are applied when virtual Administration Servers are used. Accounts of internal users are created (see section "Adding a user account" on page [156](#)) and used only within Kaspersky Security Center.

All user accounts can be viewed in the **User accounts** folder of the console tree. The **User accounts** folder is a subfolder of the **Advanced** folder by default.

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

- Configure users' rights of access to the application's features by means of roles (see section "Configuring rights. User roles" on page [160](#)).
- Send messages to users by email and SMS (see section "Delivering messages to users" on page [163](#)).
- View the list of the user's mobile devices (see section "Viewing the list of the user's mobile devices" on page [164](#)).
- Issue and install certificates on the user's mobile devices (see section "Installing a certificate for a user" on page [164](#)).
- View the list of certificates handed to the user (see section "Viewing the list of certificates handed to the user" on page [165](#)).

# Adding a user account

► To add a new Kaspersky Security Center user account:

1. In the console tree, open the **User accounts** folder.

The **User accounts** folder is a subfolder of the **Advanced** folder by default.

2. In the workspace, click the **Add user** button to open the **Properties** window.
3. In the **Properties** window, specify the account settings and set a password for the user connection to Kaspersky Security Center.

The password must contain uppercase or lowercase alphanumeric characters, or special symbols (@#\$%^&\*-\_!+=[]{}|\\:\',.?/'~()\"). The password must contain from 8 to 16 characters.

The number of attempts for entering the password is limited. By default, the maximum number of password entry attempts is 10. The number of allowed password entry attempts can be changed in the registry with the SrvSpIPpcLogonAttempts key.

If the user entered an invalid password the specified number of times, the user account will be blocked for one hour. The administrator can unlock the user account only by changing the password.

If the **Disable account** check box is selected, an internal user (such as a user with administrator or operator privileges) is unable to connect to the application. You can select this check box, for example, in case of the dismissal of an employee. By default, this check box is cleared.

4. Click **OK**.

The newly created user account will be displayed in the workspace of the **User accounts** folder.

# Configuring the check of the name of an internal user for uniqueness

You can configure the check of the name of an internal user of Kaspersky Security Center for uniqueness when this name is added to the application. The check of the name of an internal user for uniqueness can only be performed on a virtual Administration Server or on the master Administration Server for which the user account is to be created, or on all virtual Administration Servers and on the master Administration Server. By default, the name of an internal user is checked for uniqueness on all virtual Administration Servers and on the master Administration Server.

► *To enable the check of the name of an internal user for uniqueness on a virtual Administration Server or on the master Administration Server:*

1. Open the system registry of the device on which Administration Server is installed (for example, locally, using the regedit command in the **Start** → **Run** menu).
2. Go to the following hive:
  - For a 64-bit system:  
`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\ .core\ .independent\KLLIM`
  - For a 32-bit system:  
`HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\ .core\ .independent\KLLIM`
3. For the LP\_InterUserUniqVsScope (DWORD) key, set the 00000001 value.  
  
0 is the default value specified for this key.
4. Restart the Administration Server service.

As a result, the name will only be checked for uniqueness on the virtual Administration Server on which the internal user was created, or on the master Administration Server if the internal user was created on the master Administration Server.

► *To enable the check of the name of an internal user on all virtual Administration Servers and on the master Administration Server:*

1. Open the system registry of the device on which Administration Server is installed (for example, locally, using the regedit command in the **Start** → **Run** menu).

2. Go to the following hive:

- For a 64-bit system:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34  
\.core\independent\KLLIM
```

- For a 32-bit system:

```
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\independent\KLLIM
```

3. For the LP\_InterUserUniqVsScope (DWORD) key, set the 00000000 value.

0 is the default value specified for this key.

4. Restart the Administration Server service.

As a result, the check of the name for uniqueness will be performed on all virtual Administration Servers and on the master Administration Server.

## Adding a user group

You can add groups of users, perform flexible configuration of groups and user group access to various application features. User groups can be assigned names that correspond to their respective purposes. For example, the name can correspond to where users are located in the office or to the name of the company's organizational unit to which the users belong.

One user can belong to several user groups. A user account managed by a virtual Administration Server can belong only to user groups of this virtual Server and have access rights only within this virtual Server.

► *To add a user group:*

1. In the console tree select the **User accounts** folder.

The **User accounts** folder is a subfolder of the **Advanced** folder by default.

2. Click the **Add security group** button.

In the **Properties: New group** window, configure the settings of the user group you are adding:

3. In the **General** section, specify the name of the group.

The group name cannot be more than 100 characters long. The group name must be unique.

4. In the **Users** section, add user accounts to the group.

5. Click **OK**.

The user group that you have added appears in the **User accounts** folder of the console tree.

## Adding a user to a group

► *To add a user to a group:*

1. In the console tree select the **User accounts** folder.

The **User accounts** folder is a subfolder of the **Advanced** folder by default.

2. In the list of user accounts and groups, select the group to which you want to add the user.

3. From the context menu of the group, select **Properties**.

4. In the group properties window, select the **Group users** section and click the **Add** button.

A window with a list of users opens.

5. In the list, select a user or users that you want to include in the group.

6. Click **OK**.

As a result, the user or users are added to the group.

# Configuring rights. User roles

You can flexibly configure access to various features of the application by administrators, users, and user groups. You can provide users rights of access to the application's features, using one of the two methods:

- Configuring the rights for each user or group of users individually.
- Create standard user roles with a predefined set of rights and assign those roles to users depending on their scope of duties.

*User role* is an exclusively created and predefined set of rights of access to the application's features. A role can be provided to a user or a group of users. Applying roles simplifies and reduces routine procedures of configuring users' rights of access to the application. Access rights within a role are configured in accordance with the 'standard' tasks and the users' scope of duties. For example, a user role can only have rights to read and send information commands to mobile devices of other users through Self Service Portal.

User roles can be assigned names that correspond to their respective purposes. You can create an unlimited number of roles in the application.

## Adding a user role

► *To add a user role:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the context menu of the Administration Server, select **Properties**.
3. In the Administration Server properties window, select the **User roles** section and click the **Add** button.



4. In the **Properties: New role** window, configure the role:

- In the **General** section, specify the name of the role.

The name of a role cannot include more than 100 characters.

- In the **Rights** section, configure the set of rights, by selecting the **Allow** and **Deny** check boxes next to the application's features.

5. Click **OK**.

As a result, the role will be saved.

User roles that have been created for Administration Server are displayed in the Server properties window, in the **User roles** section. You can edit and delete user roles, as well as assign roles to user groups (see section "Assigning a role to a user or a user group" on page [161](#)) or to individual users.

The **User roles** section is available if the **Display security settings sections** check box is selected in the interface settings window. (see section "Configuring the interface" on page [55](#)).

## Assigning a role to a user or a user group

► *To assign a role to a user or a group of users:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the context menu of the Administration Server, select **Properties**.
3. In the Administration Server properties window, select the **Security** section.
4. In the **Names of groups or users** field, select a user or a group of users that should be assigned a role.

If the user or the group is not contained in the field, you can add it by clicking the **Add** button.

When you add a user by clicking the **Add** button, you can select the type of user authentication (Microsoft Windows or Kaspersky Security Center). Kaspersky Security Center authentication is used for selecting the accounts of internal users that are used for handling virtual Administration Servers.

5. Open the **Roles** tab and click the **Add** button.

The **User roles** window opens. This window displays user roles that have been created.

6. In the **User roles** window, select a role for the user group.
7. Click **OK**.

As a result, the role with a set of rights for handling Administration Server will be assigned to the user of the user group. Roles that have been assigned are displayed on the **Roles** tab in the **Security** section of the Administration Server properties window.

The **Security** section is available if the **Display security settings sections** check box is selected in the interface settings window (see section "Configuring the interface" on page [55](#)).

## Assigning the user as a device owner

You can assign the user as a device owner to allocate a device to that user. If you need to perform some actions on the device (for example, upgrade hardware), the administrator can notify the device owner to authorize those actions.

► *To assign a user as the owner of a device:*

1. In the console tree, select the **Managed devices** folder.
2. In the workspace of the folder, on the **Devices** tab, select the device for which you need to assign an owner.
3. In the context menu of the device, select **Properties**.
4. In the device properties window, select **System Info** → **Sessions**.
5. Click the **Assign** button next to the **Device owner** field.

6. In the **User selection** window, select the user to assign as the device owner and click **OK**.
7. Click **OK**.

As a result, the device owner is assigned. By default, the **Device owner** field contains the value from Active Directory; it is updated at each Active directory poll (see section "Viewing and modifying Active Directory group properties" on page [184](#)). You can view the list of device owners in the **Report on device owners**. You can create a report using the New Report Template Wizard (see section "Creating a report template" on page [167](#)).

## Delivering messages to users

### ► *To send a message to a user by email:*

1. In the console tree, in the **User accounts** folder, select a user.

The **User accounts** folder is a subfolder of the **Advanced** folder by default.

2. In the user's context menu, select **Notify by email**.
3. Fill in the relevant fields in the **Send message to user** window and click the **OK** button.

As a result, the message will be sent to the email that has been specified in the user's properties.

### ► *To send an SMS message to a user:*

1. In the console tree, in the **User accounts** folder, select a user.
2. In the user's context menu, select **Send SMS**.
3. Fill in the relevant fields in the **SMS text** window and click the **OK** button.

As a result, the message will be sent to the mobile device with the number that has been specified in the user's properties.

# Viewing the list of user mobile devices

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

1. In the console tree, in the **User accounts** folder, select a user.

The **User accounts** folder is a subfolder of the **Advanced** folder by default.

2. In the context menu of the user account, select **Properties**.
3. In the properties window of the user account, select the **Mobile devices** section.

In the **Mobile devices** section, you can view the list of the user's mobile devices and information about each of them. You can click the **Export to file** button to save the list of mobile devices to a file.

## Installing a certificate for a user

You can install three types of certificates for a user:

- Shared certificate, which is required to identify the user's mobile device.
- Mail certificate, which is required to set up the corporate mail on the user's mobile device.
- VPN certificate, which is required to set up the virtual private network on the user's mobile device.

► *To hand a certificate to a user and then install it:*

1. In the console tree, open the **User accounts** folder and select a user account.

The **User accounts** folder is a subfolder of the **Advanced** folder by default.

2. In the context menu of the user account, select **Install certificate**.

The Certificate Installation Wizard starts. Follow the instructions of the Wizard.

After the Certificate Installation Wizard has finished, the certificate will be created and installed for the user. You can view the list of installed certificates of a user and export it to a file (see section "Viewing the list of certificates handed to a user" on page [165](#)).

# Viewing the list of certificates handed to a user

► *To view a list of all certificates handed to a user:*

1. In the console tree, in the **User accounts** folder, select a user.

The **User accounts** folder is a subfolder of the **Advanced** folder by default.

2. In the context menu of the user account, select **Properties**.

3. In the properties window of the user account, select the **Certificates** section.

In the **Certificates** section, you can view the list of the user's certificates and information about each of them. You can click the **Export to file** button to save the list of certificates to a file.

---

# Working with reports, statistics, and notifications

This section provides information about how to work with reports, statistics, and selections of events and devices in Kaspersky Security Center, as well as how to configure Administration Server notifications.

## In this section:

Working with reports .....	<a href="#">166</a>
Working with statistical information .....	<a href="#">169</a>
Configuring event notification.....	<a href="#">171</a>
Creating a certificate for an SMTP server.....	<a href="#">172</a>
Event selections.....	<a href="#">173</a>
Exporting events to an SIEM system.....	<a href="#">176</a>
Device selections.....	<a href="#">177</a>
Policies.....	<a href="#">181</a>
Tasks .....	<a href="#">181</a>

## Working with reports

Reports in Kaspersky Security Center contain information about the status of managed devices. Reports are generated based on information stored on Administration Server. You can create reports for the following types of objects:

- For device selections created according to specific settings.
- For administration groups.

- For specific devices from different administration groups.
- For all devices on the network (in the deployment report).

The application has a selection of standard report templates. It is also possible to create custom report templates. Reports are displayed in the main application window, in the **Administration Server** folder of the console tree.

### In this section:

Creating a report template .....	<a href="#">167</a>
Creating and viewing a report .....	<a href="#">168</a>
Saving a report .....	<a href="#">168</a>
Creating a report delivery task .....	<a href="#">169</a>

## Creating a report template

► *To create a report template:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Reports** tab.
3. Click the **Create a report template** button.

As a result, the New Report Template Wizard starts. Follow the instructions of the Wizard.

After the Wizard finishes its operation, the newly created report template is added to the selected **Administration Server** folder of the console tree. You can use this template for generating and viewing reports.

# Creating and viewing a report

► *To create and view a report:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Reports** tab.
3. Select the report template that you need in the list of templates.

As a result, the workspace will display a report created on the selected template.

The report displays the following data:

- The name and type of report, its brief description and the reporting period, as well as information about the group of devices for which the report is generated.
- Chart showing most representative report data.
- Consolidated table with calculated report indicators.
- Table with detailed report data.

# Saving a report

► *To save a created report:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Reports** tab.
3. Select the report template that you need in the list of templates.
4. From the context menu of the selected report template select **Save**.

The Report Saving Wizard starts. Follow the instructions of the Wizard.

After the Wizard finishes its operation, the folder opens into which you have saved the report file.



# Creating a report delivery task

Reports can be emailed. Delivery of reports in Kaspersky Security Center is carried out using the report delivery task.

► *To create a delivery task for a report:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Reports** tab.
3. Select the report template that you need in the list of reports.
4. In the report template's context menu, select the **Deliver reports** item.

This will start the Report Delivery Task Creation Wizard. Follow the instructions of the Wizard.

► *To create a task of sending several reports:*

1. In the console tree, in the node with the name of the relevant Administration Server, select the **Tasks** folder.
2. In the workspace of the **Tasks** folder, click the **Create a Task** button.

This starts the New Task Wizard. Follow the instructions of the Wizard. In the **Task type** wizard window select **Deliver reports**.

The newly created report delivery task is displayed in the **Tasks** folder of the console tree.

A report delivery task is created automatically if the email settings were defined during Kaspersky Security Center installation (see section "Administration Server Quick Start Wizard" on page [67](#)).

# Working with statistical information

Statistics on the status of the protection system and managed devices are displayed in the workspace of the **Administration Server** node on the **Statistics** tab. The **Statistics** tab contains a few second-level tabs (pages). Each page displays information panes with statistics.

The statistical information is displayed in information panes as a table or chart (pie or bar). The data in the information panes is updated while the application is running and reflects the current state of the protection application.

You can modify the set of pages on the **Statistics** tab, the number of information panes on each page, and the data display mode in information panes.

► *To add a new page with information panes on the **Statistics** tab:*

1. Click the **Customize view** button in the top right corner of the **Statistics** tab.

The **Properties: Statistics** window opens. This window contains a list of pages that are currently shown on the **Statistics** tab. In this window, you can change the display order for the pages on the tab, add and remove pages, and proceed to configuration of page properties by clicking the **Properties** button.

2. Click the **Add** button.


This opens the properties window of a new page.

3. Configure the new page:

- In the **General** section, specify the page name.
- In the **Information panes** section, click the **Add** button to add information panes that must be displayed on the page.

Click the **Properties** button in the **Information panes** section to configure the properties of information panes that have been added: name, type and appearance of the chart on the pane, and data used to build the chart.

4. Click **OK**.

The page with information panes that you have added appears on the **Statistics** tab. Click  to instantly proceed to the page configuration or to the selected information pane on the page.

# Configuring event notification

Kaspersky Security Center allows you to select a method of notifying the administrator of events on client devices and to configure notification.

- Email. When an event occurs, the application sends a notification to email addresses specified. You can edit the text of the notification.
- SMS. When an event occurs, the application sends a notification to the phone numbers specified. You can configure SMS notifications to be sent via the mail gateway or by means of the Kaspersky SMS Broadcasting utility.
- Executable file. When an event occurs on a device, the executable file is started on the administrator's workstation. Using this executable file, the administrator can receive the parameters of an event that occurred (see section "Event notifications displayed by running an executable file" on page [331](#)).

► *To configure notification of events occurring on client devices:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Events** tab.
3. Click the **Configure notifications and event export** link and select the **Configure notifications** value in the drop-down list.

This opens the **Properties: Events** window.

4. In the **Notification** section, select a notification method (by email, by SMS, or by running an executable file) and define the notification settings.
5. In the **Notification message** field, enter the text that the application will send when an event occurs.

You can use the drop-down list on the right from the text field to add substitution settings with event details (for example, event description, time of occurrence, etc.).

If the notification text contains a % character, you have to specify it twice in a row to allow message sending. For example, "CPU load is 100%%".

6. Click the **Send test message** button to check if notification has been configured correctly.

The application sends a test notification to the specified user.

7. Click **OK** to save the changes.

As a result, the re-adjusted notification settings are applied to all events occurring on client devices.

You can also quickly configure event notifications in the event properties window by clicking the **Configure events in Kaspersky Endpoint Security** and **Configure Administration Server events** links.

### See also:

| [Event processing and storage on the Administration Server](#) ..... [92](#)

## Creating a certificate for an SMTP server

► *To create a certificate for an SMTP server:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Events** tab.
3. Click the **Configure notifications and event export** link and select the **Configure notifications** value in the drop-down list.

The event properties window opens.

4. On the **Email** tab, click the **Settings** link to open the **Settings** window.
5. In the **Settings** window click the **Specify certificate** link to open the **Certificate for signing** window.
6. In the **Certificate for signing** window, click the **Specify** button.

This opens the **Certificate** window.

7. In the **Certificate type** drop-down list, specify the public or private type of certificate:
  - If the private type of certificate (**PKCS #12 container**) is selected, specify the certificate file and the password.
  - If the public type of certificate (**X.509 certificate**) is selected:
    - a. Specify the private key file (one with the \*.prk or \*.pem extension).
    - b. Specify the private key password.
    - c. Specify the public key file (one with the \*.cer extension).
8. Click **OK**.

As a result, the certificate for the SMTP server is issued.

## Event selections

Information on the events in Kaspersky Security Center operation and managed applications is saved both in the Microsoft Windows system log and in the Kaspersky Security Center event log. You can view information from the Kaspersky Security Center event log in the workspace of the **Administration Server** node, on the **Events** tab.

Information on the **Events** tab is represented as a list of event selections. Each selection includes events of a specific type only. For example, the "Device status is Critical" selection contains only records about changes of device statuses to "Critical". After application installation, the **Events** tab contains some standard event selections. You can create additional (custom) event selections or export event information to a file.

### In this section:

Viewing an event selection .....	<a href="#">174</a>
Customizing an event selection .....	<a href="#">174</a>
Creating an event selection .....	<a href="#">175</a>

Exporting event selection to text file.....	<a href="#">175</a>
Deleting events from selection.....	<a href="#">175</a>

## Viewing an event selection

► *To view the event selection:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Events** tab.
3. In the **Selection events** drop-down list, select the relevant event selection.

If you want events from this selection to be constantly displayed in the workspace, click the ☆ button next to the selection.

As a result, the workspace will display a list of events, stored on the Administration Server, of the selected type.

You can sort information in the list of events, either in ascending or descending order in any column.

## Customizing an event selection

► *To customize an event selection:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Events** tab.
3. Open the relevant event selection on the **Events** tab.
4. Click the **Selection properties** button.

In the event selection properties window that opens you can configure the event selection.

# Creating an event selection

► *To create an event selection:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Events** tab.
3. Click the **Create a selection** button.
4. In the **New event selection** window that opens, enter the name of the new selection and click **OK**.

As a result, a selection with the name that you specified is created in the **Event selections** drop-down list.

By default, a created event selection contains all events stored on the Administration Server. To make a selection display only the events you are particularly interested in, you should customize the selection.

# Exporting event selection to text file

► *To export an event selection to text file:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Events** tab.
3. Click the **Import/Export** button.
4. In the drop-down list, select **Export events to file**.

This starts the Events Export Wizard. Follow the instructions of the Wizard.

# Deleting events from selection

► *To delete events from a selection:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Events** tab.

3. Select the events that you want to delete by using a mouse, the **Shift** or **Ctrl** key.
4. Delete the selected events by one of the following ways:
  - In the context menu of any of the selected events, select **Remove**.  
  
If you select the **Delete All** item from the context menu, all displayed events will be deleted from the selection, regardless of your choice of events for deletion.
  - Click the **Delete event** link if one event is selected, or **Delete events** link if several events are selected in the working block for these events.

As a result, the selected events are deleted.

## Exporting events to an SIEM system

The application allows you to export events that have been registered in the operation of Administration Server and other Kaspersky Lab applications installed on client devices, to an SIEM system (where SIEM stands for Security Information and Event Management).

► *To configure events export to an SIEM system:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Events** tab.
3. Click the **Configure notifications and event export** link and select the **Configure export to SIEM system** value in the drop-down list.

The events properties window opens, displaying the **Exporting events** section.

4. Select the **Automatically export events to SIEM system database** check box.
5. In the **SIEM system** drop-down list, select the system to which you need to export events.

Events can be exported to SIEM systems, such as QRadar (LEEF format), ArcSight (CEF format), Splunk (CEF format), and Syslog format (RFC 5424). The ArcSight (CEF format) system is selected by default.



6. Specify the address of an SIEM system server and a port for connection to that server in the corresponding fields.

Clicking the **Export archive** button causes the application to export newly created events to the database of the SIEM system starting from the specified date. By default, the application exports events starting from the current date.

7. Click **OK**.

As a result, after you select the **Automatically export events to SIEM system database** check box and configure connection with the server, the application will automatically export all events to the SIEM system when they are registered in the operation of Administration Server and other Kaspersky Lab applications.

For more details of event export, see Online Help on Kaspersky Lab web resource <https://stage.help.kaspersky.com/KSC/EventExport/en-US/140015.htm>.

## Device selections

Information about the status of devices is displayed in the **Device selections** folder of the the console tree.

Information in the **Device selections** folder is displayed as a list of device selections. Each selection contains devices that meet specific conditions. For example, the **Devices with the Critical status** selection contains only devices with the *Critical* status. After application installation, the **Device selections** folder contains some standard selections. You can create additional (custom) device selections, export selection settings to file, or create selections with settings imported from another file.


## In this section:

Viewing a device selection.....	<a href="#">178</a>
Configuring a device selection .....	<a href="#">178</a>
Creating a device selection.....	<a href="#">179</a>
Exporting the settings of a device selection to a file .....	<a href="#">179</a>
Creating a device selection by using imported settings .....	<a href="#">180</a>
Removing devices from administration groups in a selection.....	<a href="#">180</a>

## Viewing a device selection

### ► *To view a device selection:*

1. In the console tree, select the **Device selections** folder.
2. In the workspace of the folder, in the **Devices in this selection** drop-down list, select the relevant device selection.

If you need devices from this selection to be constantly displayed in the workspace, click the  button next to the selection.

The workspace will display a list of devices that meet the selection criteria.

You can sort the information in the list of devices either in ascending or descending order in any column.

## Configuring a device selection

### ► *To configure a device selection:*

1. In the console tree, select the **Device selections** folder.
2. Select the relevant device selection.

3. Click the **Selection properties** button.
4. In the properties window that opens, configure the general selection properties and the criteria for including devices in this selection.
5. Click **OK**.

## Creating a device selection

► *To create a device selection:*

1. In the console tree, select the **Device selections** folder.
2. In the workspace of the folder, click **Advanced** and select the **Create a selection** in the drop-down list.
3. In the **New device selection** window that opens, enter the name of the new selection and click **OK**.

As a result, a new folder with the name you entered will appear in the console tree in the **Device selections** folder. By default, the new device selection contains all devices included in administration groups of the Server on which the selection was created. To make a selection display only the devices you are particularly interested in, configure the selection by clicking the **Selection properties** button.

## Exporting the settings of a device selection to a file

► *To export the settings of a device selection to a text file:*

1. In the console tree, select the **Device selections** folder.
2. In the workspace of the folder, click the **Advanced** button and select **Export settings** in the drop-down list.
3. In the **Save as** window that opens, specify a name for the selection settings export file, select a folder to save it to, and click the **Save** button.

The settings of the device selection will be saved to the specified file.

# Creating a device selection by using imported settings

► *To create a device selection by using imported settings:*

1. In the console tree, select the **Device selections** folder.
2. In the workspace of the folder, click the **Advanced** button and select **Import** in the drop-down list.
3. In the window that opens, specify the path to the file from which you want to import the selection settings. Click the **Open** button.

As a result, in the **Device selections** folder, a **New selection** is created. Its settings are imported from the file that you specified.

If a selection named **New selection** already exists in the **Device selections** folder, an index in (**<sequence number>**) format is added to the name of the selection being created, for example: **(1)**, **(2)**.

## Removing devices from administration groups in a selection

When handling a device selection, you can remove devices from administration groups right in this selection, without switching to the administration groups from which these devices need to be removed.

► *To remove devices from administration groups:*

1. In the console tree, select the **Device selections** folder.
2. Select the devices that you want to remove by using the **Shift** or **Ctrl** keys.
3. Remove the selected devices from administration groups in one of the following ways:
  - In the context menu of any of the selected devices, select **Remove**.
  - Click the **Perform action** button and select **Remove from group** in the drop-down list.

As a result, the selected devices will be removed from their respective administration groups.

# Policies

Information about policies is stored in the **Policies** folder.

The **Policies** folder displays a list of policies that have been created in administration groups. After the application installation, the folder contains a list of policies that have been created automatically. You can update the list of policies and create policies, as well as view the properties of any policy selected in the list.

This chart displays the progress of the applying of the policy on the client devices to which it has been assigned. When the entire chart goes green, this means that the policy is applied on all client devices.

# Tasks

Information about tasks is stored in the **Tasks** folder.

The **Tasks** folder displays a list of tasks that have been assigned to client devices in administration groups and to the Administration Server. After the application installation, the folder contains a list of tasks that have been created automatically. You can update the list of tasks and create tasks, as well as view the properties of tasks, run and stop tasks.

---

# Unassigned devices

This section provides information about how to manage devices on an enterprise network if they are not included in an administration group.

## In this section:

Network poll.....	<a href="#">182</a>
Working with Windows domains. Viewing and changing the domain settings.....	<a href="#">185</a>
Working with IP subnets.....	<a href="#">185</a>
Working with the Active Directory groups. Viewing and modifying group settings .....	<a href="#">186</a>
Creating rules for moving devices to administration groups automatically .....	<a href="#">187</a>
Using VDI dynamic mode on client devices .....	<a href="#">188</a>

## Network poll

Information about the structure of the network and devices on this network is received by the Administration Server through regular polling of the Windows network, IP subnets, and Active Directory within the corporate computer network. The contents of the **Unassigned devices** folder will be updated on the basis of the results of this polling.

The Administration Server can use the following types of network scanning:

- **Windows network polling.** You can run either a quick or a full scan of the Windows network. During a quick poll, the Administration Server only retrieves information from the list of the NetBIOS names of devices in all network domains and workgroups. During a full poll, the following information is requested from each client device: operating system, IP address, DNS name, NetBIOS name.
- **IP subnets polling.** The Administration Server polls the specified IP subnets using ICMP packets, and compiles a complete set of data on devices within those IP subnets.
- **Active Directory groups polling.** Information about the Active Directory unit structure and DNS names of the devices from Active Directory groups is recorded to the Administration Server database.

Kaspersky Security Center uses this information and the details of the corporate network's structure to update the contents of the **Unassigned devices** and **Managed devices** folders. If devices in the corporate network have been configured to be moved to administration groups automatically, the discovered devices are included in administration groups.

### In this section:

Viewing and modifying the settings for Windows network polling .....	<a href="#">183</a>
Viewing and modifying Active Directory group properties .....	<a href="#">184</a>
Viewing and modifying the settings for IP subnet polling .....	<a href="#">184</a>

## Viewing and modifying the settings for Windows network polling

► *To modify the settings for the Windows network polling:*

1. In the console tree, in the **Network poll** folder, select the **Domains** subfolder.

You can proceed to the **Network poll** folder from the **Unassigned devices** folder by clicking **Poll now**.

2. In the workspace of the **Domains** folder, click the **Configure polling** button.

This will open the **Properties: Domains** window in which you can view and edit the settings of Windows network polling.

On the virtual Administration Server you can view and edit the polling settings of the Windows network in the properties window of the update agent, in the **Network poll** section.

## Viewing and modifying Active Directory group properties

► *To modify the settings for polling Active Directory groups:*

1. In the console tree, in the **Network poll** folder, select the **Active Directory** subfolder.

You can proceed to the **Network poll** folder from the **Unassigned devices** folder by clicking **Poll now**.

2. Click **Configure polling** to open the **Properties: Active Directory** window.

In the **Properties: Active Directory** window, you can view and edit the settings of Active Directory group polling.

On the virtual Administration Server you can view and edit the settings of polling Active Directory groups in the properties window of the update agent, in the **Network poll** section.

## Viewing and modifying the settings for IP subnet polling

► *To modify the settings for IP subnets polling:*

1. In the console tree, in the **Network poll** folder, select the **IP subnets** subfolder.

You can proceed to the **Network poll** folder from the **Unassigned devices** folder by clicking **Poll now**.

2. Click **Configure polling** to open the **Properties: IP subnets** window.



In the **Properties: IP subnets** window, you can view and edit the settings of IP subnet polling.

On the virtual Administration Server you can view and edit the settings of polling IP subnets in the properties window of the update agent, in the **Network poll** section. Client devices discovered during the poll of IP subnets are displayed in the **Domains** folder of the virtual Administration Server.

## Working with Windows domains. Viewing and changing the domain settings

► *To modify the domain settings:*

1. In the console tree, in the **Network poll** folder, select the **Domains** subfolder.
2. Select a domain and open its properties window in one of the following ways:
  - From the context menu of the domain, select **Properties**.
  - By clicking the **Show group properties** link.

This will open the **Properties: <Domain name>** properties window in which you can configure the properties of the selected domain.

## Working with IP subnets

You can customize existing IP subnets and create the new ones.

**In this section:**

Creating an IP subnet .....	<a href="#">186</a>
Viewing and changing the IP subnet settings.....	<a href="#">186</a>

# Creating an IP subnet

► *To create an IP subnet:*

1. In the console tree, in the **Network poll** folder, select the **IP subnets** subfolder.
2. In the context menu of the folder, select **Create** → **IP subnet**.
3. In the **New IP subnet** window that opens customize the new IP subnet.

As a result, new IP subnet appears in the **IP subnets** folder.

# Viewing and changing the IP subnet settings

► *To modify the IP subnet settings:*

1. In the console tree, in the **Network poll** folder, select the **IP subnets** subfolder.
2. Select an IP subnet and open its properties window in one of the following ways:
  - From the context menu of the IP subnet, select **Properties**.
  - By clicking the **Show group properties** link.

This will open the **Properties: <IP subnet name>** properties window in which you can configure the properties of the selected IP subnet.

# Working with the Active Directory groups. Viewing and modifying group settings

► *To modify the settings for the Active Director group:*

1. In the console tree, in the **Network poll** folder, select the **Active Directory** subfolder.
2. Select an Active Directory group and open its properties window in one of the following ways:
  - From the context menu of the group, select **Properties**.
  - By clicking the **Show group properties** link.

This will open the **Properties: <Active Directory group name>** window in which you can customize the selected Active Directory group.

## Creating rules for moving devices to administration groups automatically

You can configure devices to be moved automatically to administration groups after they are discovered during a poll in an enterprise network.

► *To configure rules for moving devices to administration groups automatically:*

1. In the console tree, select the **Unassigned devices** folder.
2. In the workspace of this folder, click **Configure rules**.

This will open the **Properties: Unassigned devices** window. In the **Move devices** section, configure the rules to move devices to administration groups automatically.

# Using VDI dynamic mode on client devices

A virtual infrastructure can be deployed on a corporate network using temporary virtual machines. Kaspersky Security Center detects temporary virtual machines and adds information about them to the Administration Server database. After a user finishes using a temporary virtual machine, this machine is removed from the virtual infrastructure. However, a record about the removed virtual machine may be saved in the database of the Administration Server. Also, non-existent virtual machines may be displayed in Administration Console.

To prevent information about non-existent virtual machines from being saved, Kaspersky Security Center supports dynamic mode for Virtual Desktop Infrastructure (VDI). The administrator can enable the support of dynamic mode for VDI (see section "Enabling VDI dynamic mode in the properties of a Network Agent installation package" on page [189](#)) in the properties of a Network Agent installation package that will be installed on a temporary virtual machine.

When a temporary virtual machine is disabled, Network Agent notifies the Administration Server that the machine has been disabled. If the virtual machine has been disabled successfully, it is removed from the list of devices connected to the Administration Server. If the virtual machine is disabled with errors and Network Agent does not send a notification about the disabled virtual machine to the Administration Server, a backup scenario is used. Under this scenario, the virtual machine is removed from the list of devices connected to the Administration Server after three unsuccessful attempts to synchronize with the Administration Server.

## In this section:

Enabling VDI dynamic mode in the properties of an installation package for Network Agent...	<a href="#">189</a>
Searching for devices making part of VDI.....	<a href="#">189</a>
Moving devices making part of VDI to an administration group.....	<a href="#">190</a>

# Enabling VDI dynamic mode in the properties of an installation package for Network Agent

► *To enable VDI dynamic mode:*

1. In the **Remote installation** folder of the console tree, select the **Installation packages** subfolder.
2. In the context menu of the Network Agent installation package, select **Properties**.  
  
The **Properties: Kaspersky Security Center Network Agent** window opens.
3. In the **Properties: Kaspersky Security Center Network Agent** window, select the **Advanced** section.
4. In the **Advanced** section, select the **Enable dynamic mode for VDI** check box.

The device on which Network Agent is to be installed will be a part of Virtual Desktop Infrastructure.

## Searching for devices making part of VDI

► *To find devices that make part of VDI:*

1. Select **Search** from the context menu of the **Unassigned devices** folder.
2. In the **Search** window, on the **Virtual machines** tab, in the **Part of Virtual Desktop Infrastructure** drop-down list, select **Yes**.
3. Click the **Find now** button.

The application search for devices that make part of Virtual Desktop Infrastructure.

# Moving devices making part of VDI to an administration group

► *To move devices that make part of VDI to an administration group:*

1. In the workspace of the **Unassigned devices** folder, click **Configure rules**.

This opens the properties window of the **Unassigned devices** folder.

2. In the properties window of the **Unassigned devices** folder, in the **Move devices** section, click the **Add** button.

The **New rule** window opens.

3. In the **New rule** window, select the **Virtual machines** section.
4. In the **Part of Virtual Desktop Infrastructure** drop-down list, select **Yes**.

A rule will be created for device relocation to an administration group.

---

# Managing applications on client devices

Kaspersky Security Center allows you to manage applications by Kaspersky Lab and other vendors installed on client devices.

The administrator can perform the following actions:

- Create application categories based on specified criteria.
- Manage application categories using specially created rules.
- Manage applications run on devices.
- Perform inventories and maintain a registry of software installed on devices.
- Fix vulnerabilities in software installed on devices.
- Install updates from Windows Update and other software vendors on devices.
- Monitor the use of keys for licensed applications groups.

## In this section:

Groups of applications.....	<a href="#">191</a>
Software vulnerabilities .....	<a href="#">202</a>
Software updates.....	<a href="#">205</a>

# Groups of applications

This section describes how to handle groups of applications installed on devices.

## Creating application categories

Kaspersky Security Center allows you to create categories of applications installed on devices.

You can create application categories using the following methods:

- The administrator specifies a folder in which executable files have been included in the selected category.
- The administrator specifies a device from which executable files are to be included in the selected category.
- The administrator sets criteria that should be used to include applications in the selected category.

When an application category is created, the administrator can set rules for the application category. Rules define the behavior of applications included in the specified category. For example, you can block or allow startup of applications included in the category.

## Managing applications run on devices

Kaspersky Security Center allows you to manage runs of applications on devices in White List mode (for details refer to the Administrator's Guide for Kaspersky Endpoint Security 10 for Windows). While in White List mode, on selected devices you can only start applications included in the specified categories. The administrator can view results of static analysis applied to rules of applications run on devices for each user.

## Inventory of software installed on devices

Kaspersky Security Center allows you to perform inventory of software on devices. Network Agent retrieves information about all applications installed on devices. Information retrieved during inventory is displayed in the workspace of the **Applications registry** folder. The administrator can view detailed information about any application, including its version and manufacturer.

The number of executable files received from a single device cannot be more than 150,000. Having reached this limit, Kaspersky Security Center cannot receive any new files.



## Licensed applications group management

Kaspersky Security Center allows the creation of licensed applications groups. A licensed applications group includes applications that meet criteria set by the administrator.

The administrator can specify the following criteria for licensed applications groups:

- Application name.
- Application version.
- Manufacturer.
- Application tag.

Applications that meet one or several criteria are automatically included in a group. To create a licensed applications group, you should set at least one criterion for including applications in this group.

Each licensed applications group has its own key. The key of a licensed applications group defines the maximum allowed number of installations for applications included in this group. If the number of installations has exceeded the limit set by the key, an informational event is logged on Administration Server. The administrator can specify an expiration date for the key. When this date arrives, an informational event is logged on Administration Server.

## Viewing information about executable files

Kaspersky Security Center retrieves all information about executable files that have been run on devices since the operating system had been installed on them. Information about executable files is displayed in the main application window, in the workspace of the **Executable files** folder.

### In this section:

Creating application categories .....	<a href="#">194</a>
Configuring application startup management on client devices .....	<a href="#">195</a>
Viewing the results of statistical analysis of startup rules applied to executable files.....	<a href="#">196</a>
Viewing the applications registry .....	<a href="#">197</a>
Creating licensed applications groups .....	<a href="#">198</a>
Managing keys for licensed applications groups .....	<a href="#">198</a>

Kaspersky Security Center software inventory .....	<a href="#">200</a>
Inventory of executable files .....	<a href="#">201</a>
Viewing information about executable files .....	<a href="#">201</a>

## Creating application categories

► *To create an application category:*

1. In the **Application management** folder of the console tree, select the **Application categories** subfolder.
2. Click the **Create a category** link to start the Create User Category Wizard.
3. In the Wizard window select a type of user category:
  - **Category with content added manually.** In this case, you can manually specify criteria according to which executable files will be assigned to the category being created.
  - **Category with content added automatically.** In this case, you can specify a folder from which executable files will be automatically assigned to the category being created.

When creating a category, which adds files automatically, the application performs inventory on the following file formats: exe, com, dll, sys, bat, ps1, cmd, js, vbs, reg, msi, msc, cpl, html, htm, drv, ocx, and scr.

- **Category which includes executable files from selected devices.** In this case, you can specify a device. Executable files detected on this device will be automatically assigned to that category.
4. Follow the instructions of the Wizard.

When you have finished with the Wizard, a custom application category is created. You can view newly created categories using the list of categories in the workspace of the **Application categories** folder.

## Configuring application startup management on client devices

► *To configure the applications run management on client devices:*

1. In the **Application management** folder of the console tree, select the **Application categories** subfolder.
2. In the workspace of the **Application categories** folder, create an application category (see section "Creating application categories" on page [194](#)) that you want to manage.
3. In the **Managed devices** folder, on the **Policies** tab, click the **Create Kaspersky Endpoint Security policy** link to run the New Policy Wizard for Kaspersky Endpoint Security 10 for Windows and follow the instructions of the Wizard.

If such a policy already exists, you can skip this step. You can configure management of the startup of applications in a specified category through the settings of the policy. The newly created policy is displayed in the **Managed devices** folder on the **Policies** tab.

4. Select **Properties** from the context menu of the policy for Kaspersky Endpoint Security 10 for Windows.

The properties window of the policy for Kaspersky Endpoint Security 10 for Windows opens.

5. In the properties window of the policy for Kaspersky Endpoint Security 10 for Windows, in the **Application Startup Control** section click the **Add** button.

The **Application Startup Control** window opens.

6. In the **Application Startup Control rule** window, in the **Category** drop-down list, select an application category that the startup rule will cover. Configure the startup rule for the selected application category.

For more details on the application startup control rules, refer to the Kaspersky Endpoint Security 10 for Windows Administrator's Guide.

7. Click **OK**.

Applications will be run on devices included in the specified category according to the rule that you have created. The created rule is displayed in the properties window of the policy for Kaspersky Endpoint Security 10 for Windows, in the **Application Startup Control** section.

## Viewing the results of statistical analysis of startup rules applied to executable files

► *To view information about which executable files are prohibited for users to run:*

1. In the **Managed devices** folder of the console tree, select the **Policies** tab.
2. In the **Protection policies** context menu select **Properties**.

The properties window of the protection policy opens.

3. In the protection policy properties window select the **Application Startup Control** section and click the **Statistical analysis** button.

The **Analysis of the access rights list** window opens.

4. The left part of the **Analysis of the access rights list** window displays a list of users based on Active Directory data.
5. Select a user from the list.

The right part of the window displays categories of applications assigned to this user.

6. To view executable files which are prohibited for the user to run, in the **Analysis of the access rights list** window click the **View files** button.

A window opens, displaying a list of executable files, which are prohibited for the user to run.

7. To view the list of executable files included in a category, select the application category and click the **View files in category** button.

This opens a window displaying a list of executable files included in the application category.

# Viewing the applications registry

Retrieval of information about installed applications is only available for computers running Microsoft Windows.

- ▶ *To view the registry of applications installed on client devices,*

In the **Application management** folder of the console tree, select the **Applications registry** subfolder.

The workspace of the **Applications registry** folder contains a list of applications that have been detected by Network Agent installed on the devices.

You can view the details of any application by opening its context menu and selecting **Properties**. The application properties window displays the application details and information about its executable files, as well as a list of devices on which the application is installed.

To view applications that meet specific criteria, you can use filtering fields in the workspace of the **Applications registry** folder.

Information about Kaspersky Lab applications and third-party software installed on devices that are connected to slave and virtual Administration Servers is also stored in the applications registry of the master Administration Server. Open the applications registry report to view this information, upon adding data from slave and virtual Administration Servers.

- ▶ *To add information from slave Administration Servers to the applications registry report:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Reports** tab.
3. In the workspace of the **Reports** tab, select **Kaspersky Lab software version report**.
4. Select **Properties** from the context menu of the report.

The **Properties: Kaspersky Lab software version report** window opens.

5. In the **Administration Servers hierarchy** section select the **Include data from slave and virtual Administration Servers** check box.

6. Click **OK**.

As a result, information from slave and virtual Administration Servers will be included in the **Kaspersky Lab software version report**.

## Creating licensed applications groups

► *To create a licensed applications group:*

1. In the **Application management** folder of the console tree, select the **Third-party licenses usage** subfolder.
2. Click the **Add a group of licensed applications** link to run the **Licensed Application Group Addition Wizard**.
3. Follow the instructions of the Wizard.

After the Wizard completes, a licensed applications group is created and displayed in the **Third-party licenses usage** folder.

## Managing keys for licensed applications groups

► *To create a key for a licensed applications group:*

1. In the **Application management** folder of the console tree, select the **Third-party licenses usage** subfolder.
2. In the workspace of the **Third-party licenses usage** folder click the **Manage keys of licensed applications** link to open the **Key Management in licensed applications** window.
3. In the **Key Management in licensed applications** window click the **Add** button.

The **Key** window opens.

4. In the **Key** window, specify the settings of the key and restrictions that the key imposes on the licensed applications group.

- **Name.** The name of the key.
- **Comment.** Notes on the selected key.
- **Restriction.** The number of devices on which the application using this key can be installed.
- **Expiration date.** The expiration date of the key.

Created keys are displayed in the **Key Management in licensed applications** window.

► *To apply a key to a licensed applications group:*

1. In the **Application management** folder of the console tree, select the **Third-party licenses usage** subfolder.
2. In the **Third-party licenses usage** folder, select a licensed applications group to which you want to apply a key.
3. Select **Properties** from the context menu of the licensed applications group.

This opens the properties window of the licensed applications group.

4. In the properties window of the licensed applications group, in the **Keys** section, select **Control if license limit is exceeded**.
5. Click the **Add** button.

The **Selecting a key** window opens.

6. In the **Selecting a key** window, select a key that you want to apply to a licensed applications group.
7. Click **OK**.

Restrictions imposed on a licensed applications group and specified in the key will also apply to the selected licensed applications group.

# Kaspersky Security Center software inventory

Kaspersky Security Center performs inventory of all software installed on managed client devices.

Network Agent compiles a list of applications installed on a device, and then transmits this list to Administration Server. Network Agent automatically receives information about installed applications from the Windows registry.

To save the device resources, Network Agent starts receiving information about installed applications 10 minutes after the Network Agent service starts, by default.

► *To change the software inventory start time, which elapses after the Network Agent service runs on a device:*

1. Open the system registry of the device on which Network Agent is installed (for example, locally, using the regedit command in the **Start** → **Run** menu).
2. Go to the following hive:

- For a 64-bit system:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34  
\1103\1.0.0.0\NagentFlags
```

- For a 32-bit system:

```
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\N  
agentFlags
```

3. For the KLINV\_INV\_COLLECTOR\_START\_DELAY\_SEC key, set the required value in seconds.

The default value is 600 seconds.

4. Restart the Network Agent service.

As a result, the software inventory start time, which elapses after the Network Agent service runs, will be changed.



# Inventory of executable files

You can use an inventory task to perform inventory of executable files on client devices.

Kaspersky Endpoint Security 10 for Windows provides the feature of inventory of executable files.

The number of executable files received from a single device cannot be more than 150,000. Having reached this limit, Kaspersky Security Center cannot receive any new files.

► *To create an inventory task for executable files on client devices:*

1. In the console tree, select the **Tasks** folder.
2. In the workspace of the **Tasks** folder, click the **Create a Task** button.

This starts the New Task Wizard

3. In the **Select the task type** window of the Wizard, select **Kaspersky Endpoint Security** as the task type, then select **Inventory** as the task subtype, and click **Next**.
4. Follow the further instructions of the Wizard.

After the Wizard is done, an inventory task for Kaspersky Endpoint Security is created.

The newly created task is displayed in the list of tasks in the workspace of the **Tasks** folder.

A list of executable files that have been detected on devices during inventory is displayed in the workspace of the **Executable files** folder.

During inventory, the application detects executable files in the following formats: mz, com, pe, ne, sys, cmd, bat, ps1, js, vbs, reg, msi, cpl, dll, jar, and HTML files.

## Viewing information about executable files

► *To view a list of all executable files detected on client devices,*

In the **Application management** folder of the console tree, select the **Executable files** subfolder.

The workspace of the **Executable files** folder displays a list of executable files that have been run on devices since the installation of the operating system or have been detected while running the inventory task of Kaspersky Endpoint Security 10 for Windows.

To view details of executable files that match specific criteria, you can use filtering.

- ▶ *To view the properties of an executable file,*

From the context menu of the file, select **Properties**.

A window opens displaying information about the executable file and a list of devices on which this executable file can be found.

## Software vulnerabilities

The **Software vulnerabilities** folder included in the **Application management** folder contains a list of vulnerabilities in applications that have been detected on client devices by Network Agent installed on them.

The feature that enables analysis of information about software vulnerabilities is only available for computers running on Microsoft Windows operating systems.

By opening the properties window of a selected application in the **Software vulnerabilities** folder, you can obtain general information about a vulnerability, about the application where it has been detected, view the list of devices on which the vulnerability has been found, and information about how to fix this vulnerability.

You can find the details of application vulnerabilities on Kaspersky Lab website (<https://threats.kaspersky.com>).

# Viewing information about software vulnerabilities

- ▶ *To view a list of vulnerabilities detected on client devices,*

In the **Application management** folder of the console tree, select the **Software vulnerabilities** subfolder.

The workspace of the folder displays a list of vulnerabilities in applications detected on devices by Network Agent installed on them.

- ▶ *To obtain information about a selected vulnerability,*  
select **Properties** from the context menu of the vulnerability.

The properties window of the vulnerability opens, displaying the following information:

- Application in which the vulnerability has been detected.
- List of devices on which the vulnerability has been detected.
- Information on whether the vulnerability has been fixed.

- ▶ *To view the report on all detected vulnerabilities,*

In the **Software vulnerabilities** folder, click the **View vulnerabilities report** link.

A report on vulnerabilities in applications installed on devices will be generated. You can view this report in the node with the name of the relevant Administration Server, by opening the Reports tab.

The feature that lets you receive information about software vulnerabilities is only available for computers running on Microsoft Windows operating systems.

## Scanning applications for vulnerabilities

If you have configured the application through the Quick Start Wizard, the vulnerability scan task is created automatically. You can view the task in the **Managed devices** folder, on the **Tasks** tab.

► *To create a task for vulnerability scan in applications installed on client devices:*

1. In the **Application management** folder of the console tree, select the **Software vulnerabilities** subfolder.
2. Click the **Configure vulnerability scan** link in the workspace to run the Vulnerabilities and Required Updates Search Task Creation Wizard.

The Task Creation Wizard window opens.

3. Follow the instructions of the Wizard.

After the Wizard completes its operation, the **Find vulnerabilities and required updates** task is created and displayed on the list of tasks in the **Managed devices** folder, on the **Tasks** tab.

When the **Find vulnerabilities and required updates** task is complete, the Administration Server displays a list of vulnerabilities found in applications installed on the device; it also displays all relevant software updates that can be deployed to networked devices, such as new versions of applications.

Network Agent receives information about any available Windows updates and other Microsoft product updates from Windows Update or the Administration Server, in case if the Administration Server acts as WSUS. Information is transmitted when applications are started (if this is provided for by the policy) and at each routine run of the **Perform Windows Update synchronization** task on client devices.

You can find the details of third-party software that can be updated through Kaspersky Security Center, by visiting the Technical Support website, on the Kaspersky Security Center page, in the Server Management section (<http://support.kaspersky.com/us/9327>).

## Fixing vulnerabilities in applications

If you have selected **Find and install required updates** in the **Update management settings** window of the Quick Start Wizard, the **Install required updates and fix vulnerabilities** task is created automatically. The task is displayed in the **Managed devices** folder on the **Tasks** tab.

► *To create the vulnerabilities fix task using available updates for applications:*

1. In the console tree, select the **Managed devices** folder on the **Tasks** tab.
2. Click the **Create a task** link to run the New Task Wizard.
3. In the **Select the task type** window of the Wizard, specify **Install required updates and fix vulnerabilities** as the task type.
4. Follow the instructions of the Wizard.

After the Wizard completes its operation, the **Install required updates and fix vulnerabilities** task is created and displayed in the **Tasks** folder.

► *To fix a selected vulnerability using updates available for the application:*

1. In the **Application management** folder of the console tree, select the **Software vulnerabilities** subfolder.
2. In the **Software updates** folder, click the **Run Vulnerability Fix Wizard** button.

The Vulnerability Fix Wizard opens.

The Vulnerability Fix Wizard features are only available under the Systems Management license.

3. Follow the instructions of the Wizard.

When the Wizard completes its operation, the **Install required updates and fix vulnerabilities** task is created and displayed in the **Tasks** folder, or a rule for fixing the vulnerability is added to the existing **Install required updates and fix vulnerabilities** task.

## Software updates

Kaspersky Security Center lets you manage updates of software installed on client devices and fix vulnerabilities in Microsoft applications and other vendors' products through installation of required updates.

Kaspersky Security Center searches for updates through the update search task and downloads them to the updates repository. After completing the search of updates, the application provides the administrator with information about available updates and vulnerabilities in applications that can be fixed using those updates.

Information about available updates for Microsoft Windows is provided by Windows Update service. Administration Server can be used as Windows Update server (WSUS). To use Administration Server as Windows Update server, you should configure synchronization of updates with Windows Update. After you have configured data synchronization with Windows Update, Administration Server provides updates to Windows Update services on devices in centralized mode and with the set frequency.

You can also manage software updates through a Network Agent policy. To do this, you should create a Network Agent policy and configure software updating in the corresponding windows of the New Policy Wizard.

The administrator can view a list of available updates in the **Software updates** subfolder included in the **Application management** folder. This folder contains a list of updates for Microsoft applications and other vendors' products retrieved by Administration Server that can be distributed to devices. After viewing information about available updates, the administrator can install them to devices.

Kaspersky Security Center updates some applications by removing the previous version of the application and installing the new one.

Before installing the updates to all of the devices, you can perform a test installation to make sure installed updates will cause no failures to the operation of applications on the devices.

You can find the details of third-party software that can be updated through Kaspersky Security Center, by visiting the Technical Support website, on the Kaspersky Security Center page, in the Server Management section (<http://support.kaspersky.com/us/9327>).

## In this section:

Viewing information about available updates .....	<a href="#">207</a>
Synchronizing updates from Windows Update with Administration Server .....	<a href="#">208</a>

Automatic installation of Kaspersky Endpoint Security updates on devices .....	<a href="#">208</a>
Offline mode for downloading updates .....	<a href="#">211</a>
Enabling and disabling the offline mode for downloading updates .....	<a href="#">213</a>
Installing updates on devices manually .....	<a href="#">215</a>
Configuring Windows updates in a Network Agent policy .....	<a href="#">217</a>

## Viewing information about available updates

- ▶ *To view a list of available updates for applications installed on client devices,*

In the **Application management** folder of the console tree, select the **Software updates** subfolder.

In the workspace of the folder, you can view a list of available updates for applications installed on devices.

- ▶ *To view the properties of an update,*

in the workspace of the **Software updates** folder select **Properties** from the context menu of the update.

The following information is available for viewing in the properties window of the update:

- List of client devices for which the update is intended (*target devices*)
- List of system components (prerequisites) that need to be installed before the update (if any)
- Software vulnerabilities that the update should fix

# Synchronizing updates from Windows Update with Administration Server

If you have selected **Use Administration Server as WSUS server** in the **Update management settings** window of the Quick Start Wizard, the Windows Update synchronization task is created automatically. You can run the task in the **Tasks** folder. The functionality of a Microsoft software update is only available after the **Perform Windows Update synchronization** task is successfully completed.

► *To create a task for synchronizing Windows Updates with Administration Server:*

1. In the **Application management** folder of the console tree, select the **Software updates** subfolder.
2. Click the **Additional actions** button and select **Configure Windows Update synchronization** from the drop-down list.

This runs the Windows Update Center Data Retrieval Task Creation Wizard.

3. Follow the instructions of the Wizard.

The Wizard creates the **Perform Windows Update synchronization** task displayed in the **Tasks** folder.

You can also create the Windows Update synchronization task in the **Tasks** folder by clicking **Create a task**.

The **Perform Windows Update synchronization** task only downloads metadata from Microsoft servers. If the network employs no WSUS server, i.e., each client device downloads Microsoft updates from external servers independently.

## Automatic installation of Kaspersky Endpoint Security updates on devices

You can configure automatic updates of databases and application modules of Kaspersky Endpoint Security on client devices.



► *To configure download and automatic installation of Kaspersky Endpoint Security updates on devices:*

1. In the console tree, select the **Tasks** folder.
2. Create an **Update** task in one of the following ways:
  - In the console tree, in the context menu of the **Tasks** folder, select **Create** → **Task**.
  - In the workspace of the **Tasks** folder, click the **Create a Task** button.

This starts the New Task Wizard.

3. In the **Select the task type** window of the Wizard, select **Kaspersky Endpoint Security** as the task type, then select **Update** as the task subtype, and click **Next**.
4. Follow the further instructions of the Wizard.

After the Wizard is done, an update task for Kaspersky Endpoint Security is created.

The newly created task is displayed in the list of tasks in the workspace of the **Tasks** folder.

5. In the workspace of the **Tasks** folder, select an update task that you have created.
6. From the context menu of the task, select **Properties**.
7. In the task properties window, select the **Settings** section.

In the **Settings** section, you can define the update task settings in local or offline mode:

- **Local mode update settings:** a connection is established between the Administration Server and the device.
  - **Offline mode update settings:** no connection is established between Kaspersky Security Center and the device (for example, when the device has no Internet connection).
8. Click the **Setting up** button to select the update source.
  9. Select the **Download application module updates** check box to download and install application module updates together with application databases.

If the check box is selected, Kaspersky Endpoint Security notifies the user about available application module updates and includes application module updates in the update package while running the update task. Configure the use of update modules:

- **Install critical and approved updates.** If any updates are available for application modules, Kaspersky Endpoint Security automatically installs them with the *Critical* status; the remaining updates will be installed after they are approved by the administrator.

To approve software updates:

- a. In the console tree, open the **Software updates** folder.
- b. In the update properties window, in the **General** section, in the **Update approval** field, set the **Approved** value.

The default value is **Undefined**.

If you are configuring the properties an update for Kaspersky Lab applications that cannot be uninstalled and set the value of the **Update approval** field on **Declined**, Kaspersky Security Center will not uninstall this update from devices on which it had been previously installed.

If an update for Kaspersky Lab applications cannot be uninstalled, this property is displayed in the update properties window, on the **General** tab, in the **Installation requirements**.

- **Install approved updates only.** If any application module updates are available, Kaspersky Endpoint Security installs them after their installation is approved; they will be installed locally through the application interface or on the Kaspersky Security Center side.

If application module updates require reviewing and accepting the terms of the End User License Agreement, the application installs updates after the terms of the End User License Agreement have been accepted by the user.

10. Select the **Copy updates to folder** check box in order for the application to save downloaded updates to the folder specified by clicking the **Browse** button.

11. Click **OK**.

When running the **Update** task, the application sends requests to Kaspersky Lab update servers.

Some updates require installation of the latest versions of plug-ins of managed applications.

## Offline mode for downloading updates

Network Agents on managed devices may sometimes not connect to the Administration Server to receive updates. For example, Network Agent may have been installed on a laptop that sometimes has no Internet connection and no local network access. Moreover, the administrator may limit the time for connecting devices to the network. In such cases, Network Agents cannot receive updates from the Administration Server upon the existing schedule. If you have configured the updating of managed applications (such as Kaspersky Endpoint Security) using Network Agent, each update will require a connection to the Administration Server. When no connection is established between Network Agent and the Administration Server, updating is impossible. You can configure the connection between Network Agent and the Administration Server so that Network Agent connects to the Administration Server at specified time intervals. At worst, if the specified connection intervals are overlaid with periods when no connection is available, the databases will never be updated. Besides that, issues may occur when multiple managed applications simultaneously attempt to access the Administration Server to receive updates. In this case, the Administration Server may stop responding to requests (similarly to a DDoS attack).

To reduce the load on the Administration Server and improve update distribution, Kaspersky Security Center features an offline mode for downloading updates for databases and modules of managed applications.

### How the offline mode for downloading updates works

Every time the Administration Server receives updates, it notifies Network Agents of which updates will be required for managed applications. When Network Agents receive information on which updates will soon be required by managed applications, they download the relevant files from the Administration Server beforehand. At the first connection with a Network Agent, the Administration Server initiates an update download by that Agent. To distribute the load on the Administration Server, Network Agents start connecting to the Administration Server and

download updates in a random order during the time interval specified by the Administration Server. This time interval depends on the number of Network Agents that download updates and on the size of those updates. After Network Agent on a device downloads all the updates, they become available for applications on that device.

To reduce the load on the Administration Server, you can use Network Agents as update agents.

When a managed application on a device attempts to access Network Agent for updates, this Network Agent checks if it has all required updates. If the updates were received from the Administration Server 25 hours since they had been requested for by the managed application, or later, Network Agent does not connect to the Administration Server and supplies the managed application with the updates from the local cache. Connection with the Administration Server may not be established at that, but it is not required for updating. Otherwise, update installation is performed in standard mode, according to the schedule of the update download task.

By default, the offline mode for downloading updates is enabled. You can enable or disable the offline mode in the registry of the computer on which Administration Server is installed (see section "Enabling and disabling the offline mode for downloading updates" on page [213](#)).

### **Advantages and disadvantages of the offline mode for downloading updates**

The offline mode for downloading updates has the following advantages:

- Kaspersky Security Center can choose the time for downloading updates, thus avoiding errors in updates of managed applications. Applications always have reliable access to the latest updates that can be downloaded from the Administration Server.
- Administration Server can manage the load when distributing updates.

The offline mode for downloading updates has the following disadvantages:

- Network traffic may increase between the Administration Server and Network Agent because the offline mode implies that updates are distributed to Network Agents each time the Administration Server receives new updates. In standard mode, updates are distributed upon the update task schedule.
- Added load on the Administration Server is possible because the Administration Server defines which updates are needed by each managed device.

## Tips on using the offline update model

- A certain time interval is always observed between the moment the Administration Server received new updates for applications and the moment Network Agent finishes downloading the updates from the Administration Server. If the update task starts running during this time interval, managed devices will receive outdated database updates from Network Agent.

We recommend that you set the update task schedule so that the update starts after the Administration Server receives updates. In this case, the update task is run by Kaspersky Security Center, so applications receive updates as soon as possible.

- If the update download task is run too frequently, Network Agent may lack time to download all the required updates before the next task run.

We recommend that you increase the interval between runs of the download updates to the repository task.

## Enabling and disabling the offline mode for downloading updates

► *To enable or disable the offline mode for downloading updates for an administration group:*

1. In the Console tree, select the administration group for which you need to enable the offline mode for downloading updates.
2. In the group workspace, open the **Policies** tab.
3. On the **Policies** tab, select the Network Agent policy.
4. In the context menu of the policy, select **Properties**.

Open the properties window of the Network Agent policy.

5. In the policy properties window, select the **Manage patches and updates** section.
6. Select or clear the **Download updates and anti-virus databases from Administration Server in advance** check box to enable or disable the offline mode for downloading updates, respectively.

By default, the offline mode for downloading updates is enabled.

As a result, the offline mode for downloading updates will be enabled or disabled.

► *To enable or disable the offline mode for downloading updates for all administration groups simultaneously:*

1. Open the system registry of the device on which Administration Server is installed (for example, locally, using the regedit command in the **Start** → **Run** menu).
2. Go to the following hive:

- For a 64-bit system:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags

- For a 32-bit system:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Components\34\1093\1.0.0.0\ServerFlags

3. Set one of the following values for the SrvDisableOfflineUpdates (DWORD) key: 0 – to enable the offline mode for downloading updates; 1 – to disable the offline mode for downloading updates.

By default, the 0 value is specified for this key (the offline mode for downloading updates is enabled).

4. Restart the Administration Server service.

As a result, the offline mode for downloading updates will be disabled for all administration groups.

# Installing updates on devices manually

If you have selected **Find and install required updates** in the **Update management settings** window of the Quick Start Wizard, the **Install required updates and fix vulnerabilities** task is created automatically. You can run or stop the task in the **Managed devices** folder on the **Tasks** tab.

If you have selected **Search for critical updates** in the Quick Start Wizard, you can install software updates to client devices through the **Install required updates and fix vulnerabilities** task.

► *To create an update installation task, do the following:*

1. In the **Application management** folder of the console tree, select the **Software updates** subfolder.
2. In the **Software updates** folder open the context menu of an update and select **Install update** → **New task**, or click the **Install update (create task)** link in the section intended for handling selected updates.

This opens the Updates Installation and Vulnerabilities Fix Task Creation Wizard.

3. Follow the instructions of the Wizard.

After the Wizard completes its operation, the **Install required updates and fix vulnerabilities** task is created and displayed in the **Tasks** folder.

You can enable automatic installation of system components (prerequisites) prior to installation of an update in Install Applications and Fix Vulnerabilities task properties. When this option is enabled, all required system components are installed before the update. A list of the required components can be found in properties of the update.

In the properties of Install Applications and Fix Vulnerabilities task, you can allow installation of updates that upgrade application to a new version.

If the task settings provide rules for installation of third-party updates, the Administration Server downloads all relevant updates from their vendors' websites. Updates are saved to the Administration Server repository and then distributed and installed on devices where they are applicable.

If the task settings provide rules for installation of Microsoft updates and the Administration Server acts as WSUS, the Administration Server downloads all relevant updates to the repository and then distributes them to managed devices. If the network employs no WSUS server, each client device downloads Microsoft updates from external servers independently.

► *To create an installation task for a selected update:*

1. In the **Application management** folder of the console tree, select the **Software updates** subfolder.
2. In the **Software updates** folder, click the **Run Update Installation Wizard** button.

The Update Installation Wizard opens.

The Update Installation Wizard features are only available under the Systems Management license.

3. Follow the instructions of the Wizard.

When the Wizard completes its operation, the **Install required updates and fix vulnerabilities** task is created and displayed in the **Tasks** folder, or a new rule for fixing the vulnerability is added to the existing **Install required updates and fix vulnerabilities** task.

Upgrading to a new version of the application may cause a malfunction of dependent applications on devices.

In the settings of the updates installation task you can configure a test installation of updates.

► *To configure a test installation of updates:*

1. In the console tree, select the **Install required updates and fix vulnerabilities** task in the **Managed devices** folder on the **Tasks** tab.
2. From the context menu of the task, select **Properties**.

The properties window of the **Install required updates and fix vulnerabilities** task opens.



3. In the properties window of the task, in the **Test installation** section select one of the available options for test installation:
  - **Do not scan.** Select this option if you do not want to perform a test installation of updates.
  - **Run scan on selected devices.** Select this option if you want to test updates installation on selected devices. Click the **Add** button and select devices on which you need to perform test installation of updates.
  - **Run scan on devices in the specified group.** Select this option if you want to test updates installation on a group of devices. In the **Specify a test group** field, specify a group of devices on which you want to perform a test installation.
  - **Run scan on specified percentage of devices.** Select this option if you want to test updates installation on some portion of devices. In the **Percentage of test devices out of all target devices** field, specify the percentage of devices on which you want to perform a test installation of updates.
4. Upon selecting any of the options but the first one, in the **Time to take the decision if the installation is to be continued** field, specify the number of hours that should elapse from the test installation of updates until the start of installation of the updates to all the devices.

## Configuring Windows updates in a Network Agent policy

► *To configure Windows Updates in a Network Agent policy:*

1. In the **Managed devices** folder, on the **Policies** tab, select a Network Agent policy.
2. In the context menu of the policy, select **Properties**.

Open the properties window of the Network Agent policy.

3. In the policy properties window, select the **Software updates and vulnerabilities** section.

4. Select the **Use Administration Server as WSUS server** check box to download Windows updates to the Administration Server and then distribute them on client devices through Network Agents.

If this check box is cleared, Windows updates are not downloaded to the Administration Server. In this case, client devices receive Windows updates on their own.

5. Select the Windows Update search mode:
  - **Active.** The Administration Server initiates a request from Windows Update Agent on a client device to the update source: Windows Update Servers, or WSUS. After that, Network Agent passes information received from Windows Update Agent to Administration Server.
  - **Passive.** In this mode, Network Agent periodically passes the Administration Server information about updates retrieved at the last synchronization of Windows Update Agent with the update source. If no synchronization of Windows Update Agent with an update source is performed, information about updates on the Administration Server becomes out-of-date.
  - **Disabled.** The Administration Server retrieves no information about updates.
6. Click **Apply**.

---

# Remote installation of operating systems and applications

Kaspersky Security Center allows you to create images of operating systems and deploy them on client devices in the network, as well as perform remote installation of applications by Kaspersky Lab and other vendors.

## Capturing images of operating systems

Kaspersky Security Center can capture images of operating systems from devices and transfer those images to Administration Server. Such images of operating systems are stored on Administration Server in a dedicated folder. The operating system image of a reference device can be captured and created by using the Add new package task (see section "Creating an installation package of an application" on page [226](#)).

To create images of operating systems, Windows Automated Installation Kit (WAIK) tool package should be installed on Administration Server.

The functionality of operating system image capturing has the following features:

- An operating system image cannot be captured on a device on which Administration Server is installed.
- While capturing an operating system image, utility sysprep.exe resets the settings of the reference device. If you need to restore the settings of the reference device, select the **Create backup copy of the device state** check box in the Operating System Image Creation Wizard.
- The image capturing process provides for a restart of the reference device.

## Deploying images of operating systems on new devices

The administrator can use images to deploy on new networked devices on which no operating system has been installed yet. A technology named Preboot eXecution Environment (PXE) is used

in this case. The administrator selects a networked device that will act as PXE server. This device must meet the following requirements:

- Network Agent must be installed on the device.
- No DHCP server must be active on the device, since a PXE server uses the same ports as a DHCP server.
- The network segment comprising the device must not contain any other PXE servers.

The following conditions must be met to deploy an operating system: a network card must be mounted on the device, the device must be connected to the network, and the Network boot option must be selected in BIOS when booting the device.

Deployment of an operating system is performed as follows:

1. The PXE server establishes a connection with the new client device while the latter is booting up.
2. The client device becomes included in Windows Preinstallation Environment (WinPE).

Adding the device to WinPE may require configuration of the set of drivers for WinPE.

3. The client device is registered on Administration Server.
4. The administrator assigns the client device an installation package with an operating system image.

The administrator can add required drivers to the installation package with the operating system image and specify a configuration file with the operating system settings (answer file) that should apply during installation.

5. The operating system is deployed on the client device.

The administrator can manually specify the MAC addresses of client devices that have not yet connected, and assign them the installation package with the operating system image.

When the selected client devices connect to the PXE server, the operating system is automatically installed on those devices.

## Deploying images of operating systems on devices where another operating system has already been installed

Deployment of images of operating systems on client devices where another operating system has already been installed is performed through the remote installation task for specific devices.

### Installing applications by Kaspersky Lab and other vendors

The administrator can create installation packages of any applications, including those specified by the user, and install the applications on client devices through the remote installation task.

#### In this section:

Creating images of operating systems .....	<a href="#">221</a>
Adding drivers for Windows Preinstallation Environment (WinPE) .....	<a href="#">222</a>
Adding drivers to an installation package with an operating system image.....	<a href="#">223</a>
Configuring sysprep.exe utility .....	<a href="#">224</a>
Deploying operating systems on new networked devices.....	<a href="#">225</a>
Deploying operating systems on client devices.....	<a href="#">226</a>
Creating installation packages of applications .....	<a href="#">226</a>
Issuing a certificate for installation packages of applications .....	<a href="#">227</a>
Installing applications on client devices .....	<a href="#">228</a>

## Creating images of operating systems

Images of operating systems are created through the reference device operating system image making task.

- ▶ *To create the reference computer operating system image making task:*
  1. In the **Remote installation** folder of the console tree, select the **Installation packages** subfolder.
  2. Click **Create installation package** to run the New Package Wizard.
  3. In the **Select installation package type** window of the Wizard, click **Create package with operating system image**.
  4. Follow the instructions of the Wizard.

When the Wizard completes its operation, an Administration Server task is created named **Copy the OS image from the device**. You can view the task in the **Tasks** folder.

When the **Copy the OS image from the device** task is complete, an installation package is created that you can use to deploy the operating system on client devices through a PXE server or the remote installation task. You can view the installation package in the **Installation packages** folder.

## Adding drivers for Windows Preinstallation Environment (WinPE)

- ▶ *To add drivers for WinPE:*
  1. In the **Remote installation** folder of the console tree, select the **Deploy device images** subfolder.
  2. In the workspace of the **Deploy device images** folder, click the **Additional actions** button and select **Configure Windows Update synchronization** in the drop-down list.

This opens the **Windows Preinstallation Environment drivers** window.
  3. In the **Windows Preinstallation Environment drivers** window click the **Add** button.

The **Add driver** window opens.

4. In the **Add driver** window specify the name of a driver and the path to the driver installation package. You can specify the path to an installation package by clicking the **Select** button in the **Add driver** window.

5. Click **OK**.

The driver will be added to the Administration Server repository. When added to the repository, the driver is displayed in the **Select driver** window.

6. Click **OK** in the **Select driver** window.

The driver will be added to Windows Preinstallation Environment (WinPE).

## Adding drivers to an installation package with an operating system image

► *To add drivers to an installation package with an operating system image:*

1. In the **Remote installation** folder of the console tree, select the **Installation packages** subfolder.
2. From the context menu of an installation package with an operating system image select **Properties**.

The installation package properties window opens.

3. In the installation package properties window select the **Additional drivers** section.
4. Click the **Add** button in the **Additional drivers** section.

The **Select driver** window opens.

5. In the **Select driver** window select drivers that you want to add to the installation package with the operating system image.

You can add new drivers to the Administration Server repository by clicking the **Add** button in the **Select driver** window.

6. Click **OK**.

Added drivers are displayed in the **Additional drivers** section of the properties window of the installation package with the operating system image.

## Configuring sysprep.exe utility

Utility sysprep.exe is intended to prepare the device to creation of an operating system image.

► *To configure sysprep.exe utility:*

1. In the **Remote installation** folder of the console tree, select the **Installation packages** subfolder.
2. From the context menu of an installation package with an operating system image select **Properties**.

The installation package properties window opens.

3. In the installation package properties window select the **sysprep.exe settings** section.
4. In the **sysprep.exe settings** section, specify a configuration file that will be used when deploying the operating system on the client device:
  - **Use default configuration file.** Select this option to use the answer file generated by default when capturing the operating system image.
  - **Specify custom values of main settings.** Select this option to specify values for settings via the user interface.
  - **Specify configuration file.** Select this option to use a custom answer file.
5. To apply the changes made, click the **Apply** button.



# Deploying operating systems on new networked devices

► *To deploy an operating system on new devices that have not yet had any operating system installed:*

1. In the **Remote installation** folder of the console tree, select the **Deploy device images** subfolder.
2. Click the **Additional actions** button and select **Manage the list of PXE servers in the network** in the drop-down list.

This opens the **Properties: Deploy device images** window showing the **PXE servers** section.

3. In the **PXE servers** section, click the **Add** button and, in the **PXE servers** window that opens, select the device that will be used as PXE server.

The device that you added is displayed in the PXE servers section.

4. In the **PXE servers** section select a PXE server and click the **Properties** button.
5. In the properties window of the selected PXE server, on the **PXE server connection settings** tab configure connection between Administration Server and the PXE server.
6. Boot the client device on which you want to deploy the operating system.
7. In the client device's BIOS, select the Network boot installation option.

The client device connects to the PXE server and is then displayed in the workspace of the **Deploy device images** folder.

8. In the **Actions** section, click the **Assign installation package** link to select the installation package that will be used for the operating system installation on the selected device.

After you added the device and assigned the installation package to it, the operating system deployment starts automatically on this device.

9. To cancel the operating system deployment on the client device, click the **Cancel OS image installation** link in the **Actions** section.

► *To add devices by MAC address:*

- In the **Deploy device images** folder, click **Add device MAC address** to open the **New device** window, and specify the MAC address of the device that you want to add.
- In the **Deploy device images** folder, click **Import MAC addresses of devices from file** to select the file containing a list of MAC addresses of all devices on which you want to deploy an operating system.

## Deploying operating systems on client devices

► *To deploy an operating system on client devices with another operating system installed:*

1. In the console tree, open the **Remote installation** folder and click **Deploy installation package on managed devices (workstations)** to run the Protection Deployment Wizard.
2. In the **Select installation package** window of the Wizard specify an installation packages with an operating system image.
3. Follow the instructions of the Wizard.

When the Wizard completes its operation, a remote installation task is created for the operating system installation on client devices. You can start or stop the task in the **Tasks** folder.

## Creating installation packages of applications

► *To create an installation package of an application:*

1. In the **Remote installation** folder of the console tree, select the **Installation packages** subfolder.
2. Click **Create installation package** to run the New Package Wizard.

3. In the **Select installation package type** window of the Wizard click one of the following buttons:
  - **Create installation package for a Kaspersky Lab application.** Select this option if you want to create an installation package for a Kaspersky Lab application.
  - **Create installation package for specified executable file.** Select this option if you want to create an installation package for an application requested by the user.
  - **Create installation package based on OS image of reference device.** Select this option if you need to create an installation package with an image of the operating system of a reference device.

When the Wizard completes its operation, an Administration Server task is created named **Copy the OS image from the device**. When this task is completed, an installation package is created that you can use to deploy the operating system image through a PXE server or the remote installation task.

4. Follow the instructions of the Wizard.

When the Wizard completes its operation, an installation package is created that you can use to install the application on client devices. You can view the installation package in the **Installation packages** folder.

For detailed information on installation packages, see *Kaspersky Security Center Implementation Guide*.

## Issuing a certificate for installation packages of applications

► *To issue a certificate for the installation package of an application:*

1. In the **Remote installation** folder of the console tree, select the **Installation packages** subfolder.

The **Remote installation** folder is a subfolder of the **Advanced** folder by default.

2. In the context menu of the **Installation packages** folder, select **Properties**.

This opens the properties window of the **Installation packages** folder.

3. In the properties window of the **Installation packages** folder, select the **Sign stand-alone packages** section.

4. In the **Sign stand-alone packages** section, click the **Specify** button.

This opens the **Certificate** window.

5. In the **Certificate type** field, specify the public or private certificate type:
  - If the **PKCS #12 container** value is selected, specify the certificate file and the password.
  - If the **X.509 certificate** value is selected:
    - a. Specify the private key file (one with the \*.prk or \*.pem extension).
    - b. Specify the private key password.
    - c. Specify the public key file (one with the \*.cer extension).

6. Click **OK**.

As a result, a certificate for the installation package of the application is issued.

## Installing applications on client devices

### ► *To install an application on client devices:*

1. In the console tree, open the **Remote installation** folder and click **Deploy installation package on managed devices (workstations)** to run the Protection Deployment Wizard.
2. In the **Select installation package** window of the Wizard specify the installation package of an application that you want to install.
3. Follow the instructions of the Wizard.

The Wizard's activities create a remote installation task to install the application to client computers. You can start or stop the task in the **Tasks** folder.

You can install Network Agent on client devices running Windows, Linux, and MacOS through the Protection Deployment Wizard.

Before remote installation of Network Agent on a Linux device, you must prepare that device (see section "Preparing a Linux device to remote installation of Network Agent" on page [341](#)).

---

# Mobile Device Management

This section describes how to manage mobile devices connected to Administration Server. For details on how to connect mobile devices, please refer to the *Kaspersky Security Center Implementation Guide*.

## In this section:

Managing mobile devices using an MDM policy.....	<a href="#">229</a>
Handling commands for mobile devices .....	<a href="#">232</a>
Handling certificates.....	<a href="#">238</a>
Adding a mobile device to the list of managed devices .....	<a href="#">244</a>
Managing Exchange ActiveSync mobile devices .....	<a href="#">249</a>
Managing iOS MDM devices .....	<a href="#">253</a>
Managing KES devices .....	<a href="#">267</a>

## Managing mobile devices using an MDM policy

To manage iOS MDM and EAS devices, you can use the Kaspersky Mobile Device Management 10 Service Pack 1 management plug-in, which is included in the distribution kit of Kaspersky Security Center. 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 modifying the configuration settings of iOS MDM and EAS devices without using iPhone Configuration Utility and the management profile of Exchange Active Sync, 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 data storage on the device in encrypted form.
  - Configuring synchronization of 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 use of mobile applications on the device.
- For managing iOS MDM devices:
  - Configuring device password security settings.
  - Configuring restrictions on usage 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 the region where the device is located.
  - Configuring device connection to the Internet through the proxy server (Global HTTP proxy).
  - Configuring the account with which the user can access corporate apps and services (Single Sign On (SSO) technology).
  - Monitoring Internet usage (visits to websites) on mobile devices.
  - Configuring wireless networks (Wi-Fi), access points (APNs), and virtual private networks (VPNs) 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 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 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 such 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.

# Handling commands for mobile devices

This section contains information about commands for mobile devices management supported by the application. The section provides instructions on how to send commands to mobile devices, as well as how to view the execution statuses of commands in the commands log.

## Commands for mobile device management

The application supports commands for mobile devices 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.

Commands are used on three types of mobile devices:

- iOS MDM device.
- KES device.
- EAS device.

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

For all types of devices, if the **Reset settings to factory values** command is successfully executed, all data is deleted from the mobile 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, will be deleted from the mobile device.



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

Table 2. Supported commands for mobile device management

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

Mobile device type	Commands	Command execution result
	Remove provisioning profile	The provisioning profile is deleted from the mobile device.
	Install app	The app is installed on the mobile device.
	Remove app	The app is removed from the mobile device.
	Enter redemption code	Redemption code entered for a paid app.
	Configure roaming	Data roaming and voice roaming enabled or disabled.
	Install Kaspersky Safe Browser	Kaspersky Safe Browser is installed on the mobile device.
KES device	Lock	The mobile device is locked.
	Unlock	Mobile device locking with a PIN is disabled. The previously specified PIN has been reset.
	Reset settings to factory values	All data is deleted from the mobile device and the settings are rolled back to their default values.
	Delete corporate data	All installed configuration profiles, provisioning profiles, the iOS MDM profile, and applications for which the <b>Remove together with iOS MDM profile</b> check box has been selected are removed from the device.
	Synchronize device	The mobile device data is synchronized with the Administration Server.

Mobile device type	Commands	Command execution result
	Locate	The mobile device is located and shown on Google Maps™. The mobile carrier charges a fee for sending SMS messages and for providing Internet connectivity.
	Mugshot	The mobile device is locked. The photo has been taken by the front camera of the device and saved on Administration Server. Photos can be viewed in the command log. The mobile carrier charges a fee for sending SMS messages and for providing Internet connectivity.
	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 default values.

## Using Google Firebase Cloud Messaging

To ensure timely delivery of commands to KES devices managed by Android operating systems, Kaspersky Security Center uses the mechanism of push notifications. Push notifications are exchanged between KES devices and Administration Server through Google Firebase Cloud Messaging. In Kaspersky Security Center Administration Console, you can define the settings of Google Firebase Cloud Messaging to connect KES devices to the service.

To retrieve the settings of Google Firebase Cloud Messaging, the administrator must have a Google account. For more details on how to retrieve the Google Firebase Cloud Messaging settings, please refer to the corresponding article in the Knowledge Base on the Technical Support website <http://support.kaspersky.com/11770>.

► *To configure Google Firebase Cloud Messaging:*

1. In the **Mobile Device Management** folder of the console tree, select the **Mobile devices** subfolder.

2. In the context menu of the **Mobile devices** folder, select **Properties**.

This opens the properties window of the **Mobile devices** folder.

3. Select the **Google Firebase Cloud Messaging settings** section.

4. In the **Sender ID** field, specify the number of a Google API project that you have received when creating one in the Google Developer Console.

5. In the **API key** field, enter a common API key that you have created in the Google Developer Console.

At the next synchronization with Administration Server, KES devices managed by Android operating systems will be connected to Google Firebase Cloud Messaging.

You can edit the settings of Google Firebase Cloud Messaging by clicking the **Reset settings** button.

## Sending commands

► *To send a command to the user's mobile device:*

1. In the **Mobile Device Management** folder of the console tree, select the **Mobile devices** subfolder.

The folder workspace displays a list of managed mobile devices.

2. Select the user's mobile device to which you need to send a command.

3. In the context menu of the mobile device, select **Show command log**.
4. In the **Mobile device management commands** window, proceed to the section with the name of the command that you need to send to the mobile device, then click the **Send command** button.

Depending on the command that you have selected, clicking the **Send command** button may open the window of advanced settings of the application. For example, when you send the command for deleting a provisioning profile from a mobile device, the application prompts you to select the provisioning profile that must be deleted from the mobile device. Define the advanced settings of the command in that window and confirm your selection. After that, the command will be sent to the mobile device.

You can click the **Resend** button to send the command to the user's mobile device once again.

You can click the **Remove from queue** button to cancel execution of a command that had been sent if the latter has not yet been executed.

The **Command log** section displays commands that have been sent to the mobile device, with the respective execution statuses. Click **Refresh** to refresh the list of commands.

5. Click the **OK** button to close the **Mobile device management commands** window.

## Viewing the statuses of commands in the command log

The application saves to the command log information about all commands that have been sent to mobile devices. The command log contains information about the time and date each command was sent to the mobile device, their respective statuses, and detailed descriptions of command execution results. For example, in case a command fails to be executed, the log displays the cause of the error. Records are stored in the command log for 30 days at most.

Commands sent to mobile devices can have the following statuses:

- *Running* – the command has been sent to the mobile device.
- *Completed* – the command execution has been successfully completed.

- *Completed with error* – the command execution has failed.
- *Deleting* – the command is being removed from the queue of commands sent to the mobile device.
- *Deleted* – the command has been successfully removed from the queue of commands sent to the mobile device.
- *Error deleting* – the command could not be removed from the queue of commands sent to the mobile device.

The application maintains a command log for each mobile device.

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

1. In the **Mobile Device Management** folder of the console tree, select the **Mobile devices** subfolder.

The folder workspace displays a list of managed mobile devices.

2. In the list of mobile devices, select the one for which you want to view the command log.
3. In the context menu of the mobile device, select **Show command log**.

The **Commands for mobile devices management** window opens. The sections of the **Commands for mobile devices management** window correspond to the commands that can be sent to the mobile device.

4. Select sections with the commands that you need and view information about how the commands are sent and executed by opening the **Command log** section.

In the **Command log** section, you can view the list of commands that have been sent to the mobile device and details on those commands. The **Show commands** filter lets you display only commands with the selected status in the list.

## Handling certificates

This section contains information about how to handle certificates of mobile devices. The section contains instructions on how to install certificates on users' mobile devices and how to configure

certificate handing rules. The section also contains instructions on how to integrate the application with the public keys infrastructure and how to configure the support of Kerberos.

## Installing a certificate

You can install three types of certificates to a user's mobile device:

- Shared certificates for identifying the mobile device.
- Mail certificates for configuring the corporate mail on the mobile device.
- VPN certificate for setting up access to a virtual private network on the mobile device.

► *To install a certificate on a user's mobile device:*

1. In the console tree, open the **Mobile Device Management** folder and select the **Certificates** subfolder.
2. In the workspace of the **Certificates** folder, click the **Add certificate** link to run the Certificate Installation Wizard.

Follow the instructions of the Wizard.

After the Wizard completes its activities, a certificate will be created and added to the list of the user's certificates; in addition, a notification will be sent to the user providing him or her with a link for downloading and installing the certificate on the mobile device. You can view the list of all certificates and export it to a file (see section "Viewing the list of certificates handed to a user" on page [165](#)). You can delete and re-hand certificates, as well as view their properties.

## Configuring certificate handing rules

► *To configure certificate handing rules:*

1. In the console tree, open the **Mobile Device Management** folder and select the **Certificates** subfolder.

By default, the **Mobile Device Management** folder is a subfolder of the **Advanced** folder.

2. In the workspace of the **Certificates** folder, click the **Configure certificate issuance rules** button to open the **Certificate generation rules** window.



3. Proceed to the section with the name of a certificate type:

**Generation of general type certificates** – to configure handing of general-type certificates.

**Generation of mail certificates** – to configure handing of mail certificates.

**Generation of VPN certificates** – to configure handing of VPN certificates.

4. In the **Generation settings** section, configure the handing of the certificate:

- Specify the certificate term in days.
- Select a source of certificates (**Administration Server** or **Certificates are specified manually**).

Administration Server is selected as the default source of certificates.

- Specify a certificate template (**Default template**, **Other template**).

Configuration of templates is available if the **Integration with PKI** section features the integration with the public keys infrastructure configured (on page [242](#)).

5. In the **Automatic update settings** section, configure automatic updates of the certificate:

- In the **Update when certificate expires in (days)** field, specify how many days should remain until the validity term expiration to update the certificate.
- To enable automatic updates of certificates, select the **Renew certificate automatically if possible** check box.

A general-type certificate can be renewed manually only.

6. In the **Encryption settings** section, enable and configure encryption of generated certificates.

Encryption is only available for general-type certificates.

- a. Select the **Enable encryption of certificates** check box.
- b. Use the slider to define the maximum number of symbols in the password for encryption.

7. Click **OK**.

# Integration with the public keys infrastructure

Integration of the application with the Public Key Infrastructure (PKI) is required to simplify generation of domain certificates for users. Following integration, certificates are issued automatically.

You need to configure the account for integration with PKI. The account must meet the following requirements:

- Be a domain user and administrator on the device with Administration Server installed.
- Be granted the SeServiceLogonRight privilege on the device with Administration Server installed.

To create a permanent user profile, log on at least once under the configured user account on the device with Administration Server installed. In this user's repository of certificates on the Administration Server device, install the Enrollment Agent certificate provided by domain administrators.

► *To configure integration with the public keys infrastructure:*

1. In the console tree, open the **Mobile Device Management** folder and select the **Certificates** subfolder.

By default, the **Mobile Device Management** folder is a subfolder of the **Advanced** folder.

2. In the workspace, click the **Integrate with public-key infrastructure** button to open the **Integration with PKI** section of the **Certificate generation rules** window.

This opens the **Integration with PKI** section of the **Certificate generation rules** window.

3. Select the **Integrate issuance of certificates with PKI** check box.
4. In the **Account** field, specify the name of the user account to be used for integration with the public key infrastructure.
5. In the **Password** field, enter the domain password for the account.

6. In the **Specify certificate template name in PKI system** list, select the certificate template based on which certificates will be generated for domain users.

A dedicated service is run in Kaspersky Security Center under the specified user account. This service is responsible for issuing domain certificates of users. The service is run when the list of certificate templates is loaded by clicking the **Update list** button or when a certificate is generated.

7. Click **OK** to save the settings.

Following integration, certificates are issued automatically.

## Enabling support of Kerberos Constrained Delegation

The application supports usage of Kerberos Constrained Delegation.

► *To enable support of Kerberos Constrained Delegation:*

1. In the console tree, open the **Mobile Device Management** folder.
2. In the **Mobile Device Management** folder of the console tree, select the **Mobile Device Servers** subfolder.
3. In the workspace of the **Mobile Device Servers** folder, select an iOS MDM Server.
4. In the context menu of the iOS MDM Server, select **Properties**.
5. In the properties window of the iOS MDM Server, select the **Settings** section.
6. In the **Settings** section, select the **Ensure compatibility with Kerberos Constrained Delegation** check box.
7. Click **OK**.

# Adding a mobile device to the list of managed devices

To add a mobile device of a user to the list of managed devices, a shared certificate must be delivered and installed on the device. Shared certificates are used for identifying mobile devices by Administration Server. After a shared certificate is delivered and installed on a mobile device, the latter appears on the list of managed devices. Mobile devices of users are added to the list of managed devices by means of a Wizard.

## Running the New Mobile Device Connection Wizard

► *To run the New Mobile Device Connection Wizard:*

1. In the console tree select the **User accounts** folder.

By default, the **User accounts** folder is a subfolder of the **Advanced** folder.

2. Select the user account whose mobile device you want add to the list of managed devices.
3. In the context menu of the user account, select **Add mobile device**.

The New Mobile Device Connection Wizard starts running.

4. In the **Operating system** window, select the operating system type of the mobile device (*Android* or *iOS*).

Further actions in the New Mobile Device Connection Wizard depend on the operating system type that you have selected (see instructions below).

## Adding a mobile device if a shared certificate is delivered using an App Store link

► *To install Kaspersky Safe Browser from App Store on an iOS device and then connect the device to the Administration Server:*

1. In the **Operating system** window of the Wizard, select **iOS** for the type of operating system of the mobile device.
2. In the **iOS MDM device protection method** window of the Wizard, select **Install Kaspersky Safe Browser by using AppStore link**.

3. In the **Certificate source** window of the Wizard, you have to specify the method of creation of the shared certificate that Administration Server will use to identify the mobile device. You can specify a shared certificate using any of the two methods:
  - Create a shared certificate automatically, by means of Administration Server tools, then deliver the certificate to the mobile device.
  - Specify a shared certificate file.
4. In the **User notification method** window of the Wizard, define the settings for notification of the mobile device user of certificate creation with an SMS message or by email.
5. In the **Result** window of the Wizard, click **Finish** to close the Certificate Installation Wizard.

After the Wizard finishes its activities, a link and a QR code will be sent to the user's mobile device thus allowing him or her to download Kaspersky Safe Browser via App Store. The user clicks the link or scans the QR code. After that, the operating system of the mobile device prompts the user to accept Kaspersky Safe Browser installation. The user installs Kaspersky Safe Browser on the mobile device. When Kaspersky Safe Browser is installed, the user rescans the QR code to retrieve the Administration Server connection settings. When the QR code is rescanned in Safe Browser, the user retrieves the Administration Server connection settings and a shared certificate. The mobile device connects to the Administration Server and downloads a shared certificate. After the certificate is installed on the mobile device, the latter is displayed in the **Mobile devices** folder, which is a subfolder of the **Mobile Device Management** folder of the console tree.

If Kaspersky Safe Browser has been previously installed on the mobile device, the user must independently enter the settings for connecting to the Administration Server. After that, the shared certificate must be installed on the mobile device (see section "Installing a certificate" on page [239](#)). In this case, Kaspersky Safe Browser will not be downloaded and installed.

## Adding a mobile device if a shared certificate is delivered within an iOS MDM profile

► *To connect an iOS device to the Administration Server via iOS MDM:*

1. In the **Operating system** window of the Wizard, select **iOS** for the type of operating system of the mobile device.
2. In the **iOS MDM device protection method** window of the Wizard, select **Use iOS MDM profile of iOS MDM Server**.

In the field that appears below, select the iOS MDM Server.

3. In the **Certificate source** window of the Wizard, you have to specify the method of creation of the shared certificate that Administration Server will use to identify the mobile device. You can specify a shared certificate using any of the two methods:
  - Create a shared certificate automatically, by means of Administration Server tools, then deliver the certificate to the mobile device.
  - Specify a shared certificate file.
4. In the **User notification method** window of the Wizard, define the settings for notification of the mobile device user of certificate creation with an SMS message or by email.
5. In the **Result** window of the Wizard, click **Finish** to close the Certificate Installation Wizard.

As a result, the iOS MDM profile is automatically published on the Kaspersky Security Center Web Server. The mobile device user receives a notification with a link for downloading the iOS MDM profile from the Web Server. The user clicks the link. After that, the mobile device's operating system prompts the user to accept the iOS MDM profile installation. If the user accepts, the iOS MDM profile will be downloaded to the mobile device. After the iOS MDM profile is downloaded and the mobile device is synchronized with the Administration Server, the device is displayed in the **Mobile devices** folder, which is a subfolder of the **Mobile Device Management** folder of the console tree.

To allow the user to proceed to the Kaspersky Security Center Web Server using the link, connection with the Administration Server over port 8061 must be available on the mobile device.

## Adding a mobile device if a shared certificate is delivered using a Google Play link

► *To install Kaspersky Endpoint Security for Android from Google Play on a KES device and then connect the device to the Administration Server:*

1. In the **Operating system** window of the Wizard, select **Android** for the mobile device operating system type.
2. In the **Kaspersky Endpoint Security for Android installation method** window of the Wizard, select **By using a Google Play link**.
3. In the **Certificate source** window of the Wizard, you have to specify the method of creation of the shared certificate that Administration Server will use to identify the mobile device. You can specify a shared certificate using any of the two methods:
  - Create a shared certificate automatically, by means of Administration Server tools, then deliver the certificate to the mobile device.
  - Specify a shared certificate file.
4. In the **User notification method** window of the Wizard, define the settings for notification of the mobile device user of certificate creation with an SMS message or by email.
5. In the **Result** window of the Wizard, click **Finish** to close the Certificate Installation Wizard.

After the Wizard finishes its activities, a link and a QR code will be sent to the user's mobile device thus allowing him or her to download Kaspersky Endpoint Security for Android. The user clicks the link or scans the QR code. After that, the mobile device's operating system prompts the user to accept Kaspersky Endpoint Security for Android installation. After Kaspersky Endpoint Security for Android is downloaded and installed, the mobile device connects to the Administration Server and downloads a shared certificate. After the certificate is installed on the mobile device, the latter is displayed in the **Mobile devices** folder, which is a subfolder of the **Mobile Device Management** folder of the console tree.

## Adding a mobile device if a shared certificate is delivered within a mobile app

- ▶ *To install Kaspersky Endpoint Security for Mobile on an Android device and then connect that device to the Administration Server:*

Kaspersky Endpoint Security for Mobile published on the Administration Server is used for installation.

1. In the **Operating system** window of the Wizard, select **Android** for the mobile device operating system type.
2. In the **Kaspersky Endpoint Security for Android installation method** window of the Wizard, select **By using a link from own Web Server**.

In the field that appears below, select an installation package or create a new one by clicking **New**.

3. In the **Certificate source** window of the Wizard, you have to specify the method of creation of the shared certificate that Administration Server will use to identify the mobile device. You can specify a shared certificate using any of the two methods:
  - Create a shared certificate automatically, by means of Administration Server tools, then deliver the certificate to the mobile device.
  - Specify a shared certificate file.
4. In the **User notification method** window of the Wizard, define the settings for notification of the mobile device user of certificate creation with an SMS message or by email.
5. In the **Result** window of the Wizard, click **Finish** to close the Certificate Installation Wizard.

As a result, the mobile applications package of Kaspersky Endpoint Security for Android is automatically published on the Kaspersky Security Center Web Server. The mobile applications package contains the app, the settings for connecting the mobile device to the Administration Server, and a certificate. The mobile device user will receive a notification containing a link for downloading the package from the Web Server. The user clicks the link. After that, the operating system of the device prompts the user to accept the installation of the mobile applications package. If the user agrees, the package will be downloaded



on the mobile device. After the package is downloaded and the mobile device is synchronized with the Administration Server, the device is displayed in the **Mobile devices** folder, which is a subfolder of the **Mobile Device Management** folder of the console tree.

## Managing Exchange ActiveSync mobile devices

This section describes advanced features for management of EAS devices through Kaspersky Security Center.

In addition to management of EAS devices by means of commands, the administrator can use the following options:

- Create management profiles for EAS devices, assign them to users' mailboxes (see page [250](#)). *EAS device management profile* is a policy of Exchange ActiveSync that is used on a Microsoft Exchange server to manage EAS devices. In an EAS device management profile, you can configure the following groups of settings:
  - User password management settings.
  - Mail synchronization settings.
  - Restrictions on the use of the mobile device features.
  - Restrictions on the use of mobile applications on the mobile device.

Depending on the mobile device model, settings of a management profile can be applied partially. The status of an Exchange ActiveSync policy that has been applied can be viewed in the mobile device's properties.

- View information about the settings of EAS device management (see page [252](#)). For example, the administrator can refer to the properties of a mobile device to know the time of the last synchronization with a Microsoft Exchange server, the EAS device's ID, the Exchange ActiveSync policy name and its current status on the mobile device.
- Disconnect EAS devices from management if they are out of use (see page [253](#)).
- Define the settings of Active Directory polling by the Microsoft Exchange Mobile Devices Server, which allows updating the information about users' mailboxes and mobile devices.

For information about how to connect Exchange ActiveSync mobile devices to the Microsoft Exchange Mobile Devices Server, please refer to the *Kaspersky Security Center Implementation Guide*.

## Adding a management profile

To manage EAS devices, you can create EAS device management profiles and assign them to selected Microsoft Exchange mailboxes.

Only one EAS device management profile can be assigned to a Microsoft Exchange mailbox.

► *To add an EAS device management profile for a Microsoft Exchange mailbox:*

1. In the console tree, open the **Mobile Device Management** folder.
2. In the **Mobile Device Management** folder of the console tree, select the **Mobile Device Servers** subfolder.
3. In the workspace of the **Mobile Device Servers** folder, select a Microsoft Exchange Mobile Devices Server.
4. In the context menu of the Microsoft Exchange Mobile Devices Server, select **Properties**.

The Mobile Device Server properties window opens.

5. In the properties window of the **Microsoft Exchange Mobile Devices Server**, select the **Mailboxes** section.
6. Select a mailbox and click the **Assign profile** button.

The **Policy profiles** window opens.

7. In the **Policy profiles** window, click the **Add** button.

The **New profile** window opens.

8. Configure the profile on the tabs of the **New profile** window.

- If you want to specify the profile name and the refreshing interval, select the **General** tab.
- If you want to configure the password of the mobile device user, select the **Password** tab.
- If you want to configure synchronization with the Microsoft Exchange server, select the **Synchronization settings** tab.
- If you want to configure restrictions on the mobile device features, select the **Device** tab.
- If you want to configure restrictions on the use of mobile applications on the mobile device, select the **Applications on device** tab.

9. Click **OK**.

The new profile will be displayed on the list of profiles in the **Policy profiles** window.

If you want this profile to be automatically assigned to new mailboxes, as well as to those of which the profiles have been deleted, select it on the list of profiles and click the **Set as default profile** button.

The default profile cannot be deleted. To delete the current default profile, you should assign the "default profile" attribute to a different profile.

10. Click **OK** in the **Policy profiles** window.

The management profile settings will be applied on the EAS device at the next synchronization of the device with the Microsoft Exchange Mobile Devices Server.

## Removing a management profile

► *To remove an EAS device management profile for a Microsoft Exchange mailbox:*

1. In the console tree, open the **Mobile Device Management** folder.
2. In the **Mobile Device Management** folder of the console tree, select the **Mobile Device Servers** subfolder.

3. In the workspace of the **Mobile Device Servers** folder, select a Microsoft Exchange Mobile Devices Server.

4. In the context menu of the Microsoft Exchange Mobile Devices Server, select **Properties**.

The Mobile Device Server properties window opens.

5. In the properties window of the Microsoft Exchange Mobile Devices Server, select the **Mailboxes** section.

6. Select a mailbox and click the **Change profiles** button.

The **Policy profiles** window opens.

7. In the **Policy profiles** window, select the profile that you want to remove and click the deletion button marked with a red cross.

The selected profile will be removed from the list of management profiles. The current default profile will be applied to EAS devices managed by the profile that has been removed.

If you want to remove the current default profile, re-assign the 'default profile' property to another profile, then remove the first one.

## Viewing information about an EAS device

► *To view information about an EAS device:*

1. In the **Mobile Device Management** folder of the console tree, select the **Mobile devices** subfolder.

The folder workspace displays a list of managed mobile devices.

2. In the workspace, filter EAS devices by clicking the *Exchange ActiveSync (EAS)* link.

3. From the context menu of the mobile device select **Properties**.

As a result, the properties window of the EAS device opens.

The properties window of the mobile device displays information about the connected EAS device.

# Disconnecting an EAS device from management

► To disconnect an EAS device from management by the Microsoft Exchange Mobile Devices Server:

1. In the **Mobile Device Management** folder of the console tree, select the **Mobile devices** subfolder.

The folder workspace displays a list of managed mobile devices.

2. In the workspace, filter EAS devices by clicking the *Exchange ActiveSync (EAS)* link.
3. Select the mobile device that you need to disconnect from management by the Microsoft Exchange Mobile Devices Server.
4. In the context menu of the mobile device, select **Remove**.

As a result, the EAS device is marked for removal with a red cross icon. The mobile device is removed from the list of managed devices after it is removed from the Exchange ActiveSync Server database. To do so, the administrator must remove the user account on the Microsoft Exchange server.

## Managing iOS MDM devices

This section describes advanced features for management of iOS MDM devices through Kaspersky Security Center. The application supports the following options for management of iOS MDM devices:

- Define the settings of managed iOS MDM devices in centralized mode and restrict features of devices through configuration profiles. You can add or modify configuration profiles and install them on mobile devices.
- Install apps on mobile devices bypassing App Store by means of provisioning profiles. For example, you can use provisioning profiles for installation of in-house corporate apps on users' mobile devices. A provisioning profile contains information about an app and a mobile device.
- Install apps on an iOS MDM device via App Store. Before installing an app to an iOS MDM device, you must add that app to an iOS MDM Server.

Every 24 hours, a PUSH notification is sent to all connected iOS MDM devices in order to synchronize data with the iOS MDM Server.

For information about how to install an iOS MDM Server, please refer to the *Kaspersky Security Center Implementation Guide*.

You can refer to the device properties window to view information about the configuration profile and provisioning profile, as well as applications installed on the iOS MDM device (see section "Viewing information about an iOS MDM device" on page [266](#)).

## Issuing a certificate for an iOS MDM profile

You can issue a certificate for an iOS MDM profile to allow a mobile device to verify it.

► *To create an iOS MDM profile certificate:*

1. In the **Mobile Device Management** folder of the console tree, select the **Mobile devices** subfolder.

The **Mobile Device Management** folder is a subfolder of the **Advanced** folder by default.

2. In the context menu of the **Mobile devices** folder, select **Properties**.
3. In the properties window of the folder, select the **Connection settings for iOS devices** section.

4. Click the **Specify** button next to the **Select certificate** field.

This opens the **Certificate** window.

5. In the **Certificate type** field, specify the public or private certificate type:
  - If the **PKCS #12 container** value is selected, specify the certificate file and the password.
  - If the **X.509 certificate** value is selected:
    - a. Specify the private key file (one with the \*.prk or \*.pem extension).
    - b. Specify the private key password.
    - c. Specify the public key file (one with the \*.cer extension).
6. Click **OK**.

As a result, the iOS MDM profile certificate is issued.

# Adding a configuration profile

To create a configuration profile, you should install iPhone Configuration Utility on the device with Administration Console installed. You should download iPhone Configuration Utility from Apple Inc. website and install it by using standard tools of your operating system.

► *To create a configuration profile and add it to an iOS MDM Server:*

1. In the console tree, select the **Mobile Device Management** folder.

The **Mobile Device Management** folder is a subfolder of the **Advanced** folder by default.

2. In the workspace of the **Mobile Device Management** folder, select the **Mobile Device Servers** subfolder.

3. In the workspace of the **Mobile Device Servers** folder, select an iOS MDM Server.

4. In the context menu of the iOS MDM Server, select **Properties**.

The Mobile Device Server properties window opens.

5. In the properties window of the iOS MDM Server, select the **Configuration profiles** section.

6. In the **Configuration profiles** section, click the **Create** button.

The **Add new configuration profile** window opens.

7. In the **Add new configuration profile** window, specify a name and ID for the profile.

The configuration profile ID should be unique; the value should be specified in Reverse-DNS format, for example, *com.companyname.identifier*.

8. Click **OK**.

An application named iPhone Configuration Utility then starts.

9. Reconfigure the profile in iPhone Configuration Utility.

For a description of the profile settings and instructions on how to configure the profile, please refer to the documentation enclosed with iPhone Configuration Utility.

After you have configured the profile with iPhone Configuration Utility, the new configuration profile is displayed in the **Configuration profiles** section in the properties window of the iOS MDM Server.

You can click the **Modify** button to modify the configuration profile.

You can click the **Import** button to load the configuration profile to a program.

You can click the **Export** button to save the configuration profile to a file.

The profile that you have created should be installed on iOS MDM devices (see section "Installing a configuration profile on a device" on page [256](#)).

## Installing a configuration profile to a device

► *To install a configuration profile to a mobile device:*

1. In the **Mobile Device Management** folder of the console tree, select the **Mobile devices** subfolder.

The folder workspace displays a list of managed mobile devices.

2. In the workspace, filter iOS MDM devices by protocol type (*iOS MDM*).
3. Select the user's mobile device on which you need to install a configuration profile.

You can select multiple mobile devices to install the profile simultaneously.

4. In the context menu of the mobile device, select **Show command log**.
5. In the **Mobile device management commands** window, proceed to the **Install profile** section and click the **Send command** button.

You can also send the command to the mobile device by selecting **All commands** in the context menu of that mobile device, and then selecting **Install profile**.

As a result, the **Select profiles** window opens showing a list of profiles. Select from the list the profile that you need to install on the mobile device. You can select multiple profiles to install them on the mobile device simultaneously. To select the range of profiles, use the **SHIFT** key. To combine profiles into a group, use the **CTRL** key.



6. Click the **OK** button to send the command to the mobile device.

When the command is executed, the selected configuration profile will be installed on the user's mobile device. If the command is successfully executed, the current status of the command in the commands log will be shown as *Done*.

You can click the **Resend** button to send the command to the user's mobile device once again.

You can click the **Remove from queue** button to cancel execution of a command that had been sent if the latter has not yet been executed.

The **Command log** section displays commands that have been sent to the mobile device, with the respective execution statuses. Click **Refresh** to refresh the list of commands.

7. Click the **OK** button to close the **Mobile device management commands** window.

The profile that you have installed can be viewed and removed, if necessary (see section "Removing a configuration profile from a device" on page [257](#)).

## Removing a configuration profile from a device

► *To remove a configuration profile from a mobile device:*

1. In the **Mobile Device Management** folder of the console tree, select the **Mobile devices** subfolder.

The folder workspace displays a list of managed mobile devices.

2. In the workspace, filter iOS MDM devices by clicking the **iOS MDM** link.
3. Select the user's mobile device from which you need to remove the configuration profile.

You can select multiple mobile devices to remove the profile simultaneously.

4. In the context menu of the mobile device, select **Show command log**.
5. In the **Commands for mobile devices management** window, go to the **Remove profile** section and click the **Send command** button.

You can also send the command to the mobile device by selecting **All commands** from the context menu of the device, then selecting **Remove profile**.

As a result, the **Remove profiles** window opens showing the list of profiles.

6. Select from the list the profile that you need to remove from the mobile device. You can select multiple profiles to remove them from the mobile device simultaneously. To select the range of profiles, use the **SHIFT** key. To combine profiles into a group, use the **CTRL** key.

7. Click the **OK** button to send the command to the mobile device.

When the command is executed, the selected configuration profile will be removed from the user's mobile device. If the command is executed successfully, the current status of the command will be shown as *Completed*.

You can click the **Resend** button to send the command to the user's mobile device once again.

You can click the **Remove from queue** button to cancel execution of a command that had been sent if the latter has not yet been executed.

The **Command log** section displays commands that have been sent to the mobile device, with the respective execution statuses. Click **Refresh** to refresh the list of commands.

8. Click the **OK** button to close the **Commands for mobile devices management** window.

## Adding provisioning profile

► *To add a provisioning profile to an iOS MDM Server:*

1. In the console tree, open the **Mobile Device Management** folder.
2. In the **Mobile Device Management** folder of the console tree, select the **Mobile Device Servers** subfolder.
3. In the workspace of the **Mobile Device Servers** folder, select an iOS MDM Server.
4. In the context menu of the iOS MDM Server, select **Properties**.

The Mobile Device Server properties window opens.

5. In the properties window of the **iOS MDM Server**, go to the **Provisioning profiles** section.
6. In the **Provisioning profiles** section, click the **Import** button and specify the path to a provisioning profile file.

The profile will be added to the iOS MDM Server settings.

You can click the **Export** button to save the provisioning profile to a file.

The provisioning profile that you have imported can be installed on iOS MDM devices (see section "Installing a provisioning profile on a device" on page [259](#)).

## Installing a provisioning profile to a device

► *To install a provisioning profile on a mobile device:*

1. In the **Mobile Device Management** folder of the console tree, select the **Mobile devices** subfolder.

The folder workspace displays a list of managed mobile devices.

2. In the workspace, filter iOS MDM devices by protocol type (*iOS MDM*).
3. Select the user's mobile device on which you need to install the provisioning profile.

You can select multiple mobile devices to install the provisioning profile simultaneously.

4. In the context menu of the mobile device, select **Show command log**.
5. In the **Mobile device management commands** window, proceed to the **Install provisioning profile** section and click the **Send command** button.

You can also send the command to the mobile device by selecting **All commands** from the context menu of that mobile device, and then selecting **Install provisioning profile**.

As a result, the **Select provisioning profiles** window opens showing a list of provisioning profiles. Select from the list the provisioning profile that you need to install on the mobile device. You can select multiple provisioning profiles to install them on the mobile device simultaneously. To select the range of provisioning profiles, use the **SHIFT** key. To combine provisioning profiles into a group, use the **CTRL** key.

6. Click the **OK** button to send the command to the mobile device.

When the command is executed, the selected provisioning profile will be installed on the user's mobile device. If the command is successfully executed, the current status of the command in the commands log will be shown as *Completed*.

You can click the **Resend** button to send the command to the user's mobile device once again.

You can click the **Remove from queue** button to cancel execution of a command that had been sent if the latter has not yet been executed.

The **Command log** section displays commands that have been sent to the mobile device, with the respective execution statuses. Click **Refresh** to refresh the list of commands.

7. Click the **OK** button to close the **Mobile device management commands** window.

The profile that you have installed can be viewed and removed, if necessary (see section "Removing a provisioning profile from a device" on page [260](#)).

## Removing a provisioning profile from a device

► *To remove a provisioning profile from a mobile device:*

1. In the **Mobile Device Management** folder of the console tree, select the **Mobile devices** subfolder.

The folder workspace displays a list of managed mobile devices.

2. In the workspace, filter iOS MDM devices by protocol type (*iOS MDM*).
3. Select the user's mobile device from which you need to remove the provisioning profile.

You can select multiple mobile devices to remove the provisioning profile simultaneously.

4. In the context menu of the mobile device, select **Show command log**.
5. In the **Commands for Mobile Device Management** window, go to the **Remove provisioning profile** section and click the **Send command** button.

You can also send the command to the mobile device by selecting **All commands** from the context menu and then selecting **Remove provisioning profile**.

As a result, the **Remove provisioning profiles** window opens showing the list of profiles.

6. Select from the list the provisioning profile that you need to remove from the mobile device. You can select multiple provisioning profiles to remove them from the mobile device simultaneously. To select the range of provisioning profiles, use the **SHIFT** key. To combine provisioning profiles into a group, use the **CTRL** key.
7. Click the **OK** button to send the command to the mobile device.

When the command is executed, the selected provisioning profile will be removed from the user's mobile device. Applications that are related to the deleted provisioning profile will not be operable. If the command is executed successfully, the current status of the command will be shown as *Completed*.

You can click the **Resend** button to send the command to the user's mobile device once again.

You can click the **Remove from queue** button to cancel execution of a command that had been sent if the latter has not yet been executed.

The **Command log** section displays commands that have been sent to the mobile device, with the respective execution statuses. Click **Refresh** to refresh the list of commands.

8. Click the **OK** button to close the **Commands for mobile devices management** window.

## Adding a managed application

Before installing an app to an iOS MDM device, you must add that app to an iOS MDM Server. An application is considered as managed if it has been installed on a device via Kaspersky Security Center. A managed application can be handled remotely by means of Kaspersky Security Center.

► *To add a managed application to an iOS MDM Server:*

1. In the console tree, open the **Mobile Device Management** folder.
2. In the **Mobile Device Management** folder of the console tree, select the **Mobile Device Servers** subfolder.
3. In the workspace of the **Mobile Device Servers** folder, select an iOS MDM Server.

4. In the context menu of the iOS MDM Server, select **Properties**.

This opens the properties window of the iOS MDM Server.

5. In the properties window of the iOS MDM Server, select the **Managed applications** section.

6. Click the **Add** button in the **Managed applications** section.

The **Add an application** window opens.

7. In the **Add an application** window, in the **App name** field, specify the name of the application to be added.

8. In the **Apple ID or App Store link** field, specify the Apple ID of the application to be added, or specify a link to a manifest file that can be used to download the application.

9. If you want a managed application to be removed from the user's mobile device along with the iOS MDM profile when removing the latter, select the **Remove together with iOS MDM profile** check box.

10. If you want to block the application data backup through iTunes, select the **Block data backup** check box.

11. Click **OK**.

The added application is displayed in the **Managed applications** section of the properties window of the iOS MDM Server.

## Installing an app on a mobile device

- *To install an app on an iOS MDM mobile device:*

1. In the **Mobile Device Management** folder of the console tree, select the **Mobile devices** subfolder.

The **Mobile Device Management** folder is a subfolder of the **Advanced** folder by default. The folder workspace displays a list of managed mobile devices.

2. Select the iOS MDM device on which you want to install an app.

You can select multiple mobile devices to install the application simultaneously.

3. In the context menu of the mobile device, select **Show command log**.

4. In the **Mobile device management commands** window, go to the **Install app** section and click the **Send command** button.

You can also send the command to the mobile device by selecting **All commands** in the context menu of that mobile device, and then selecting **Install app**.

As a result, the **Select apps** window opens showing a list of profiles. Select from the list the application that you need to install on the mobile device. You can select multiple applications to install them on the mobile device simultaneously. To select a range of apps, use the **SHIFT** key. To combine apps into a group, use the **CTRL** key.

5. Click the **OK** button to send the command to the mobile device.

When the command is executed, the selected application will be installed on the user's mobile device. If the command is successfully executed, its current status in the command log will be shown as *Completed*.

You can click the **Resend** button to send the command to the user's mobile device once again. You can click the **Remove from queue** button to cancel execution of a command that had been sent if the latter has not yet been executed.

The **Command log** section displays commands that have been sent to the mobile device, with the respective execution statuses. Click **Refresh** to refresh the list of commands.

6. Click the **OK** button to close the **Commands for mobile devices management** window.

Information about the installed application is displayed in the properties of the iOS MDM mobile device (see section "Viewing information about an iOS MDM device" on page [266](#)).

You can remove the app from the mobile device through the command log or through the context menu of the mobile device (see section "Removing an app from a device" on page [264](#)).

# Removing an app from a device

► To remove an app from a mobile device:

1. In the **Mobile Device Management** folder of the console tree, select the **Mobile devices** subfolder.

The folder workspace displays a list of managed mobile devices.

2. In the workspace, filter iOS MDM devices by protocol type (*iOS MDM*).
3. Select the user's mobile device from which you need to remove the app.

You can select multiple mobile devices to remove the app simultaneously.

4. In the context menu of the mobile device, select **Show command log**.
5. In the **Mobile device management commands** window, go to the **Remove app** section and click the **Send command** button.

You can also send the command to the mobile device by selecting **All commands** in the context menu of the mobile device, then selecting **Remove app**.

As a result, the **Remove apps** window opens showing a list of applications.

6. Select from the list the app that you need to remove from the mobile device. You can select multiple apps to remove them simultaneously. To select a range of apps, use the **SHIFT** key. To combine apps into a group, use the **CTRL** key.
7. Click the **OK** button to send the command to the mobile device.

When the command is executed, the selected app will be removed from the user's mobile device. If the command is executed successfully, the current status of the command will be shown as *Completed*.

You can click the **Resend** button to send the command to the user's mobile device once again.

You can click the **Remove from queue** button to cancel execution of a command that had been sent if the latter has not yet been executed.

The **Command log** section displays commands that have been sent to the mobile device, with the respective execution statuses. Click **Refresh** to refresh the list of commands.

8. Click the **OK** button to close the **Commands for mobile devices management** window.



# Installing Kaspersky Safe Browser on a mobile device

► *To install Kaspersky Safe Browser on an iOS MDM mobile device:*

1. In the **Mobile Device Management** folder of the console tree, select the **Mobile devices** subfolder.

The **Mobile Device Management** folder is a subfolder of the **Advanced** folder by default. The workspace of the **Mobile Device Management** folder displays a list of managed mobile devices.

2. Select the iOS MDM device on which you need to install Kaspersky Safe Browser.

You can select multiple mobile devices to install Kaspersky Safe Browser simultaneously.

3. In the context menu of the mobile device, select **Show command log**.

4. In the **Mobile device management commands** window, proceed to the **Install Kaspersky Safe Browser** section and click the **Send command** button.

You can also send the command to the device by selecting **All commands** in the context menu of that mobile device, and then selecting **Install Kaspersky Safe Browser**.

When the command is executed, Kaspersky Safe Browser will be installed on the user's mobile device. If the command is successfully executed, its current status in the command log will be shown as *Completed*.

You can click the **Resend** button to send the command to the user's mobile device once again. You can click the **Remove from queue** button to cancel execution of a command that had been sent if the latter has not yet been executed.

The **Command log** section displays commands that have been sent to the mobile device, with the respective execution statuses. Click **Refresh** to refresh the list of commands.

5. Click the **OK** button to close the **Mobile device management commands** window.

Information about the Kaspersky Safe Browser installed is displayed in the properties of the iOS MDM mobile device (see section "Viewing information about an iOS MDM device" on page [266](#)). You can remove the app from the mobile device through the command log or through the context menu of the mobile device (see section "Removing an app from a device" on page [264](#)).

# Viewing information about an iOS MDM device

► *To view information about an iOS MDM device:*

1. In the **Mobile Device Management** folder of the console tree, select the **Mobile devices** subfolder.

The folder workspace displays a list of managed mobile devices.

2. In the workspace, filter iOS MDM devices by clicking the **iOS MDM** link.
3. Select the mobile device about which you need to view information.
4. From the context menu of the mobile device select **Properties**.

As a result, the properties window of the iOS MDM device opens.

The properties window of the mobile device displays information about the connected iOS MDM device.

# Disconnecting an iOS MDM device from management

► *To disconnect an iOS MDM device from the iOS MDM Server:*

1. In the **Mobile Device Management** folder of the console tree, select the **Mobile devices** subfolder.

The folder workspace displays a list of managed mobile devices.

2. In the workspace, filter iOS MDM devices by clicking the **iOS MDM** link.
3. Select the mobile device that you need to disconnect.
4. In the context menu of the mobile device, select **Remove**.

As a result, the iOS MDM device will be marked on the list for removal. The mobile device will be automatically removed from the list of managed devices after it is removed from the iOS MDM Server database. The mobile device will be removed from the iOS MDM Server database within one minute.

After the iOS MDM device is disconnected from management, all installed configuration profiles, the iOS MDM profile, and applications for which the **Remove together with iOS MDM profile** check box had been selected will be removed from the mobile device (see section "**Adding a managed application**" on page [261](#)).

## Managing KES devices

Kaspersky Security Center supports the following mobile KES device management features:

- Centrally manage KES devices by using commands (see section "Commands for mobile device management" on page [232](#)).
- View information about the settings for management of KES devices (see section "Viewing information about a KES device" on page [269](#)).
- Install applications by using mobile applications packages (see section "Creating a mobile applications package for KES devices" on page [267](#)).
- Disconnect KES devices from management (see section "Disconnecting a KES device from management" on page [270](#)).

For detailed information about how to handle KES devices and connect them to Administration Server please refer to the *Kaspersky Security Center 10 Implementation Guide*.

## Creating a mobile applications package for KES devices

A Kaspersky Endpoint Security 10 for Mobile license is required to create a mobile applications package for KES devices.

► *To create a mobile applications package:*

1. In the **Remote installation** folder of the console tree, select the **Installation packages** subfolder.

The **Remote installation** folder is a subfolder of the **Advanced** folder by default.

2. Click the **Additional actions** button and select **Manage packages of mobile applications** from the drop-down list.

3. In the **Mobile applications packages management** window, click the **New**.
4. The Mobile Applications Package Creation Wizard starts. Follow the instructions of the Wizard.
5. If you want to place an application into a container, in the **Settings** window of the Wizard, select the **Create container with selected application** check box.

The newly created mobile applications package is displayed in the **Mobile applications packages management** window.

Containers are used to control activities of applications running on the user's mobile device. Security policy rules can be applied to applications placed into a container. You can configure rules for applications in the properties window of the policy of Kaspersky Endpoint Security 10 for Mobile, in the **Containers** section. For more details on containers and how to manage them, please refer to the documentation enclosed with Kaspersky Endpoint Security 10 for Mobile.

You can place a third-party app in a container. You cannot place the Kaspersky Endpoint Security 10 for Mobile installation package into a container.

## Enabling two-factor authentication of KES devices

► *To enable two-factor authentication of a KES device:*

1. Open the system registry of the client device with Administration Server installed (for example, locally, using the regedit command in the **Start** → **Run** menu).
2. Go to the following hive:

- For a 64-bit system:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34  
\.core\independent\KLLIM
```

- For a 32-bit system:

```
HKLM\Software\KasperskyLab\Components\34\.core\independent\KLLIM
```

3. Create a key with the LP\_MobileMustUseTwoWayAuthOnPort13292 name.
4. Specify REG\_DWORD as the key type.
5. Set the key value on 1.
6. Restart the Administration Server service.

As a result, mandatory two-factor authentication of the KES device using a shared certificate will be enabled after you run the Administration Server service.

The first connection of the KES device to the Administration Server does not require a certificate.

By default, two-factor authentication of KES devices is disabled.

## Viewing information about a KES device

► *To view information about a KES device:*

1. In the **Mobile Device Management** folder of the console tree, select the **Mobile devices** subfolder.

The folder workspace displays a list of managed mobile devices.

2. In the workspace, filter KES devices by protocol type (*KES*).
3. Select the mobile device about which the information you need to view.
4. From the context menu of the mobile device select **Properties**.

This opens the properties window of the KES device.

The properties window of the mobile device displays information about the connected KES device.

# Disconnecting a KES device from management

To disconnect a KES device from management, the user has to remove Network Agent from the mobile device. Once the user has removed Network Agent, the mobile device details are removed from the Administration Server database, so the administrator can remove the mobile device from the list of managed devices.

► *To remove a KES device from the list of managed devices:*

1. In the **Mobile Device Management** folder of the console tree, select the **Mobile devices** subfolder.

The folder workspace displays a list of managed mobile devices.

2. In the workspace, filter KES devices by protocol type (*KES*).
3. Select the mobile device that you need to disconnect from management.
4. In the context menu of the mobile device, select **Remove**.

As a result, the mobile device is removed from the list of managed devices.

If Kaspersky Endpoint Security for Android has not been removed from the mobile device, that mobile device reappears on the list of managed devices after synchronization with the Administration Server.

---

# Self Service Portal

This section contains information about Self Service Portal. The section provides Self Service Portal sign-in instructions, as well as instructions on creating Self Service Portal accounts and adding mobile devices to Self Service Portal.

## In this section:

About Self Service Portal.....	<a href="#">271</a>
Adding a device .....	<a href="#">274</a>
Connecting a user to Self Service Portal .....	<a href="#">275</a>

## About Self Service Portal

Self Service Portal is a web portal that lets the administrator delegate some of the mobile device management functions to users. Any mobile device user who has signed in to Self Service Portal can add his or her mobile device to Self Service Portal. When you add a mobile device, an iOS MDM profile is installed on an iOS MDM device while Kaspersky Endpoint Security for Android is installed on a KES device, and [corporate policies are applied](#) to the device (see section "[Adding a device](#)" on page [274](#)). When done, the mobile device becomes managed.

Self Service Portal supports automatic user authorization using Kerberos Constrained Delegation and domain authorization.

Self Service Portal supports mobile devices with the iOS and Android operating systems.

The user can perform the following actions on Self Service Portal:

- Download apps from the corporate Application Shop. Apps must be preliminarily added to the corporate Application Shop in Kaspersky Security Center 10 Web Console. For more details on how to add apps to the Application Shop, please refer to the *Kaspersky Security Center Web Console 10 User Guide*. To upload apps to Self Service Portal, the user must select the **Applications** tab in the Self Service Portal window.
- Send commands to the managed mobile device on his or her own, for example, in case the mobile device is lost or stolen. To send commands to the user, you must select the **Devices** tab in the Self Service Portal window. A proprietary set of commands is supported for each mobile device type (see table below).
- Unlock the mobile device on his or her own by clicking **Show unlock code** if it had been locked.

Table 3. Supported commands for mobile device management

Mobile device type	Commands	Command execution result
iOS MDM device	Lock	The mobile device is locked.
	Reset settings to factory values	All data has been deleted from the mobile device, settings have been rolled back to the default values, and the mobile device is no longer managed.
	Delete corporate data	Corporate data, iOS MDM profile, and Network Agent have been deleted; the mobile device is no longer managed.



Mobile device type	Commands	Command execution result
KES device	Lock	The mobile device is locked.
	Reset settings to factory values	All data has been deleted from the mobile device, settings have been rolled back to the default values, and the mobile device is no longer managed.
	Delete corporate data	Corporate data, iOS MDM profile, and Network Agent have been deleted; the mobile device is no longer managed.
	Locate	The mobile device is located and shown on Google Maps. The mobile carrier charges a fee for sending SMS messages and for providing Internet connectivity.
	Alarm	The mobile device plays a sound alarm.
	Mugshot	The mobile device is locked. 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 on Self Service Portal. The mobile carrier charges a fee for sending SMS messages and for providing Internet connectivity.

Self Service Portal uses the global list of Kaspersky Security Center users. The list is expanded automatically when importing users from Active Directory (see section "Viewing and modifying Active Directory group properties" on page [184](#)) or manually (see section "Adding a user account" on page [156](#)).

If domain authorization on Self Service Portal is prohibited by the administrator, users can use alias accounts for authorization. Creating aliases for authentication on Self Service Portal is available in the properties of user accounts (see section "Connecting a user to Self Service Portal" on page [275](#)).

The administrator can grant users the following Self Service Portal usage permissions:

- Read.
- Modify.
- Connect new devices.
- Send only information commands to mobile devices (which do not affect the device status).

**Mugshot** and **Locate** are information commands.

- Send commands to mobile devices.

## Adding a device

Before adding a mobile device to Self Service Portal, the user has to accept the Self Service Portal End User License Agreement and sign in to the portal.

The algorithm of adding the user's mobile device to Self Service Portal comprises the following steps:

1. The user opens the main page of the portal.
2. Self Service Portal creates an installation package and then displays a one-time link for downloading the installation package and a QR code in which the link is encoded. The screen shows the time interval during which a link for downloading the installation package will be available. A message with a link for downloading the installation package is sent to the user's email address.

The installation package is required to install Network Agent on the mobile device and apply corporate policies.

A new installation package can be created only after the previously created package has been removed from Administration Server.

3. By clicking the **Create package to install on new device** link, the user is taken to the installation package download page on the mobile device to be added to Self Service Portal.
4. Self Service Portal detects the operating system of the user's mobile device.

If the mobile device's operating system could be detected automatically, the installation package download page opens. If the device operating system could not be determined automatically, a window opens letting the user choose an operating system manually.

5. The user downloads the installation package and installs Network Agent on the mobile device.
6. After Network Agent has been installed, the device connects to Administration Server.

As a result, the mobile device will be added to the list of managed devices and the corporate policies will be applied to it. A link to information about connecting to the Administration Server is sent to the user's email address.

## Connecting a user to Self Service Portal

If the use of domain authorization of users on Self Service Portal is forbidden, you can create alias accounts for users in the Administration Console. Users can sign in to Self Service Portal using alias accounts.

► *To connect a user (under an alias) to Self Service Portal:*

1. In the **Mobile Device Management** folder, select the **Self Service Portal** subfolder.
2. In the workspace of the **Self Service Portal** folder, click **Send invitation to connect to Self Service Portal**.

This runs the Self Service Portal Connection Wizard. Follow the Wizard's steps.

3. In the **Configure rights** window of the Wizard, click **Settings** to configure Self Service Portal access rights for users and user groups.

If the **Do not show this message again** check box is selected, the **Configure rights** window will not appear at the next run of the Wizard.

4. In the **Select Self Service Portal address** window, you can specify the Self Service Portal address to which the user will connect.

You can skip the Self Service Portal address selection. In this case, you will have to enter a Self Service Portal address in the invitation text manually.

5. In the **Select users to connect to Self Service Portal** window, specify the users whom you need to connect to Self Service Portal.

6. In the **Configure aliases of user accounts** window of the Wizard, configure the use of user aliases and domain accounts for connection to **Self Service Portal**:

- Select the **Use aliases of user accounts to log in to Self Service Portal** check box to configure the delivery of invitations to selected users, prompting them to connect to Self Service Portal.

If this check box is cleared, the invitation to connect to Self Service Portal will only be sent to domain users who were selected at the previous step of the Wizard.

- Select **Create aliases if users have none** to allow Kaspersky Security Center to automatically create aliases for all user accounts that have none yet. Invitations for connection to Self Service Portal will be sent to users for whom aliases were created. Kaspersky Security Center creates no new aliases for users who already have some.
- Select **Send invitation to domain account for users without aliases** to block the application from automatically creating aliases for domain users that have none yet. If a user has no alias, the invitation for connection to Self Service Portal will be sent to the domain account.

- Select the **Create new passwords for aliases** check box to allow Kaspersky Security Center to create new passwords for all aliases (both for new and for previously created ones). The details of the new password and the old one will be sent to users in the text of the invitation for connection to Self Service Portal.

If this check box is cleared, a password will only be generated for newly created aliases.

- Specify the number of characters in the password for connection to Self Service Portal for user aliases. The default password length is 16 characters.
7. In the **Delivery of invitations to Self Service Portal** window, select the method of delivering Self Service Portal invitation messages both for new and for existing users.
  8. Click **Edit message** to view and, if necessary, edit the invitation text.

After the Wizard is finished, the selected users will receive the invitation providing all information required to connect to Self Service Portal. You can create an unlimited number of Self Service Portal aliases for a single user. After you create an alias, it will be shown in the properties window of the user account, in the **User aliases for Self Service Portal** section. After a user alias for Self Service Portal is created, it cannot be changed. You can delete a selected alias by clicking the red cross button next to the list of aliases for Self Service Portal.

---

# Encryption and data protection

Data encryption reduces the risk of unintentional leakage in case your notebook, removable drive, or hard drive is stolen/lost, or upon access of unauthorized users and applications.

Kaspersky Endpoint Security 10 for Windows provides encryption functionality.

Kaspersky Endpoint Security 10 for Windows allows you to encrypt files stored on local drives of a device and removable drives, as well as removable and hard drives entirely.

Encryption rules are configured through Kaspersky Security Center by defining policies.

Encryption and decryption upon existing rules are performed when applying a policy.

Availability of the encryption management feature is determined by the user interface settings (see section "Configuring the interface" on page [55](#)).

The administrator can perform the following actions:

- Configure and perform file encryption/decryption on local drives of the device.
- Configure and perform file encryption on removable drives.
- Create rules of access to encrypted files by applications.
- Create and deliver to the user a key file for access to encrypted files if file encryption is restricted on the user's device.
- Configure and perform hard drive encryption.
- Manage user access to encrypted hard drives and removable drives (manage authentication agent accounts, create and deliver to users information on request for account name and password restoration, as well as access keys for encrypted devices).
- View encryption statuses and files encryption reports.

These operations are performed using tools integrated into Kaspersky Endpoint Security 10 for Windows. For detailed instructions on how to perform operations and a description of encryption features please refer to the *Kaspersky Endpoint Security 10 for Windows Administrator's Guide*.

## In this section:

Viewing the list of encrypted devices.....	<a href="#">279</a>
Viewing the list of encryption events .....	<a href="#">280</a>
Exporting the list of encryption events to a text file.....	<a href="#">281</a>
Creating and viewing encryption reports.....	<a href="#">281</a>

# Viewing the list of encrypted devices

► *To view the list of devices storing encrypted information:*

1. Select the **Data encryption and protection** folder in the console tree of Administration Server.
2. Open the list of encrypted devices using one of the following methods:
  - By clicking the **Go to list of encrypted devices** link in the **Manage encrypted devices** section.
  - In the console tree select the **Encrypted devices** folder.

As a result, the workspace displays information about devices on the network storing encrypted files, and about devices encrypted at the drive level. After the information on a device is decrypted, the device is automatically removed from the list.

You can sort the information in the list of devices either in ascending or descending order in any column.

The presence or absence of the **Data encryption and protection** folder in the console tree is determined by the user interface settings (see section "Configuring the interface" on page [55](#)).

# Viewing the list of encryption events

When running data encryption/decryption tasks on devices, Kaspersky Endpoint Security 10 for Windows sends to Kaspersky Security Center information about events of the following types:

- Cannot encrypt/decrypt a file, or create an encrypted archive due to a lack of free disk space.
- Cannot encrypt/decrypt a file, or create an encrypted archive due to license issues.
- Cannot encrypt/decrypt a file, or create an encrypted archive due to missing access rights.
- The application has been prohibited to access an encrypted file.
- Unknown errors.

► *To view a list of events that have occurred when encrypting data on devices:*

1. Select the **Data encryption and protection** folder in the console tree of Administration Server.
2. Go to the list of events occurring during encryption, using one of the following methods:
  - By clicking the **Go to error list** link in the **Data encryption errors** control section.
  - In the console tree select the **Encryption events** folder.

As a result, the workspace displays information about problems that have occurred during data encryption on devices.

You can take the following actions on the list of encryption events:

- Sort data records in ascending or descending order in any of the columns.
- Perform quick search for records (by text match with a substring in any of the list fields).
- Export the list of events to a text file.

The presence or absence of the **Data encryption and protection** folder in the console tree is determined by the user interface settings (see section "Configuring the interface" on page [55](#)).



# Exporting the list of encryption events to a text file

► *To export the list of encryption events to a text file:*

1. Create a list of encryption events (see section "Viewing the list of encryption events" on page [280](#)).
2. From the context menu of the events list select **Export list**.

The **Export list** window opens.

3. In the **Export list** window specify the name of the text file with the events list, select a folder to save it, and click the **Save** button.

The list of encryption events will be saved to the file that you have specified.

# Creating and viewing encryption reports

The administrator can generate the following reports:

- Report on encryption status of data storage drives containing information about the device encryption status for all groups of devices
- Report on rights of access to encrypted devices, which contains information about the status of user accounts that have been granted access to encrypted devices
- Report about errors in encryption of files and folders containing information about errors that have occurred when running data encryption/decryption tasks on devices
- Report on encryption status of managed devices containing information about whether the encryption status of devices meets the encryption policy.
- Report on blockage of access to encrypted files containing information about blocking application access to encrypted files

► *To view the report on devices encryption:*

1. In the console tree, select the **Data encryption and protection** folder.
2. Do one of the following:
  - Click the **Device encryption report** link to start the New Report Template Wizard.
  - Select the **Encrypted devices** subfolder, then click the **Device encryption report** button to run the New Report Template Wizard.
3. Follow the steps of the New Report Template Wizard.

In the **Administration Server** node, on the **Reports** tab, a new report appears. The report generation process starts. The report appears in the workspace of the **Reports** tab.

► *To view the report on rights of access to encrypted devices:*

1. In the console tree, select the **Data encryption and protection** folder.
2. Do one of the following:
  - Click the **Report on rights of access to encrypted devices** link in the **Manage encrypted devices** section to start the New Report Template Wizard.
  - Select the **Encrypted devices** subfolder, then click the **Report on rights of access to encrypted devices** link to start the New Report Template Wizard.
3. Follow the steps of the New Report Template Wizard.

In the **Administration Server** node, on the **Reports** tab, a new report appears. The report generation process starts. The report appears in the workspace of the **Reports** tab.

► *To view the report about errors in encryption of files and folders:*

1. In the console tree, select the **Data encryption and protection** folder.
2. Do one of the following:
  - Click the **Report about errors in encryption of files and folders** link in the **Data encryption errors** control section to start the New Report Template Wizard.
  - Select the **Encryption events** subfolder, then click the **Report about errors in encryption of files and folders** link to start the New Report Template Wizard.
3. Follow the steps of the New Report Template Wizard.

The new report appears on the **Reports** tab in the Administration Server node. The report generation process starts. The report appears in the workspace of the **Reports** tab.

► *To view the report on the status of device encryption:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Reports** tab.
3. Click the **Create a report template** button to start the New Report Template Wizard.
4. Follow the instructions of the New Report Template Wizard. In the **Selecting the report template type** window, in the **Others** section, select **Report on encryption status of managed devices**.

After you have finished with the New Report Template Wizard, a new report template appears in the Administration Server node, on the **Reports** tab.

5. In the node of the relevant Administration Server on the **Reports** tab, select the report template that was created during the previous steps of the instructions.

The report generation process starts. The report appears in the workspace of the **Reports** tab.

For information about whether the encryption statuses of devices and removable drives match the encryption policy, view the information panes on the **Statistics** tab of the Administration Server node (see section "Working with statistical information" on page [169](#)).

► *To view the file access blocking report:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Reports** tab.
3. Click the **Create a report template** button to start the New Report Template Wizard.
4. Follow the instructions of the New Report Template Wizard. In the **Selecting the report template type** window, in the **Others** section select **Report on access blockage to files**.

After you have finished with the New Report Template Wizard, a new report template appears in the **Administration Server** node on the **Reports** tab.

5. In the node of the **Administration Server** on the **Reports** tab, select the report template that was created during the previous steps of the instructions.

The report generation process starts. The report appears in the workspace of the **Reports** tab.

---

# Inventory of equipment detected on the network

Kaspersky Security Center retrieves information about the equipment detected during the network poll. Inventory covers all equipment connected to the organization's network. Information about the equipment is updated after each new network poll. The list of detected equipment may contain the following types of devices:

- Devices.
- Mobile devices.
- Network devices.
- Virtual devices.
- OEM components.
- Computer peripherals.
- Connected devices.
- VoIP phones.
- Network repositories.

Equipment detected during a network poll is displayed in the **Repositories** subfolder of the **Hardware** folder of the console tree.

The administrator can add new devices to the equipment list manually or edit information about equipment that already exists on the network. In the properties of a device you can view and edit detailed information about that device.

The administrator can assign the "Enterprise equipment" attribute to detected devices. This attribute can be assigned manually in the properties of a device, or the administrator can specify criteria for the attribute to be assigned automatically. In this case, the "Enterprise

equipment" attribute is assigned by device type. You can allow or prohibit network connection of equipment by the "Enterprise equipment" attribute.

Kaspersky Security Center allows writing off equipment. To do this, select the **Device is written off** check box in the properties of a device. Such device is not displayed on the equipment list.

## In this section:

Adding information about new devices .....	<a href="#">285</a>
Configuring criteria used to define enterprise devices .....	<a href="#">286</a>

# Adding information about new devices

► *To add information about new devices on the network:*

1. In the **Repositories** folder of the console tree, select the **Hardware** subfolder.
2. In the workspace of the **Hardware** folder, click the **Add device** button to open the **New device** window.

The **New device** window opens.

3. In the **New device** window, in the **Type** drop-down list select a device type that you want to add.
4. Click **OK**.

The device properties window opens on the **General** section.

5. In the **General** section fill in the entry fields with data on the device. The **General** section lists the following settings:
  - **Corporate device.** Select the check box if you want to assign the "Corporate" attribute to the device. Using this attribute, you can search for devices in the **Hardware** folder.
  - **Device is written off.** Select the check box if you do not want the device to be displayed on the list of devices in the **Hardware** folder.

6. Click **Apply**.

The new device will be displayed in the workspace of the **Hardware** folder.

# Configuring criteria used to define enterprise devices

► *To configure criteria of detection for enterprise devices:*

1. In the **Repositories** folder of the console tree, select the **Hardware** subfolder.
2. In the workspace of the **Hardware** folder, click the **Configure criteria for corporate devices** link to open the hardware properties window.
3. In the hardware properties window, in the **Corporate devices** section, select a method for assigning the "Corporate" attribute to the device:
  - **Set the "Corporate" attribute manually.** The "Corporate hardware" attribute is assigned to the device manually in the device properties window in the **General** section.
  - **Set the "Corporate" attribute automatically.** In the **By device type** block of settings, specify device types to which the application will automatically assign the "Corporate" attribute.
4. Click **Apply**.

---

# Updating databases and software modules

This section describes how to download and distribute updates of databases and software modules using Kaspersky Security Center.

To maintain the protection system's reliability, you should timely update the databases and Kaspersky Lab application modules, managed through Kaspersky Security Center.

To update databases and Kaspersky Lab application modules that are managed through Kaspersky Security Center, the **Download updates to the repository** task of the Administration Server is used. When the task is complete, updates for databases and application modules are downloaded to the Administration Server from the update source.

The **Download updates to the repository** task is not available on virtual Administration Servers. The repository of the virtual Administration Server displays updates downloaded to the master Administration Server.

You can configure the updates to be verified for operability and errors before they are distributed to client devices.

When running the **Download updates to the repository** task, the following information is sent to Kaspersky Lab update servers in automatic mode in order to ensure the downloading of relevant versions of databases and application modules:

- Application ID and version.
- Application setup ID.
- Active key ID.
- **Download updates to the repository** task run ID.

All information being sent contains no personal details or other confidential data. Kaspersky Lab protects information as provided by the requirements of the current legislation.

## In this section:

Creating the download updates to the repository task.....	<a href="#">288</a>
Creating the download updates to the update agents' repository task.....	<a href="#">290</a>
Configuring the download updates to the repository task .....	<a href="#">291</a>
Verifying downloaded updates .....	<a href="#">291</a>
Configuring test policies and auxiliary tasks .....	<a href="#">293</a>
Viewing downloaded updates .....	<a href="#">294</a>
Automatic distribution of updates .....	<a href="#">295</a>
Rolling back installed updates .....	<a href="#">302</a>

# Creating the download updates to the repository task

The download updates to the repository task of the Administration Server is created automatically by the Kaspersky Security Center Quick Start Wizard. You can create only one download updates to the repository task. That is why you can create a download updates to the repository task only if this task was removed from the Administration Server tasks list.

► *To create a download updates to the repository task:*

1. In the console tree, select the **Tasks** folder.
2. Start creating the task in one of the following ways:
  - In the console tree, in the context menu of the **Tasks** folder, select **Create** → **Task**.
  - Click the **Create a task** button in the workspace.



This starts the New Task Wizard. Follow the instructions of the Wizard. In the **Task type** wizard window, select **Download updates to the repository**.

After the Wizard completes, the **Download updates to the repository** task will be created in the list of Administration Server tasks.

When an Administration Server performs the **Download updates to the repository** task, updates to databases and software modules of applications are downloaded from the updates source and stored in the shared folder. If you create this task for an administration group, it will only be applied to Network Agents included in the specified administration group.

Updates are distributed to client devices and slave Administration Servers from the shared folder.

The following resources can be used as a source of updates for the Administration Server:

- Kaspersky Lab update servers – Kaspersky Lab servers to which the updated anti-virus database and the application modules are uploaded.
- Master Administration Server.
- FTP/HTTP server or a network updates folder – an FTP server, an HTTP server, a local or a network folder added by the user and containing the latest updates. When selecting a local folder, you should specify a folder on the device with Administration Server installed.

To update Administration Server from an FTP/HTTP server or from a network folder, you should copy to those resources the correct structure of folders containing updates that matches the structure created when using Kaspersky Lab update servers.

Source selection depends on task settings. By default, updating is performed over the Internet from Kaspersky Lab update servers.

# Creating a task for forcing the downloading of updates to the repositories of update agents

► *To create the download updates to the update agents' repository task for a selected administration group:*

1. In the console tree, select the **Tasks** folder.
2. In the workspace of this folder, click the **Create a task** button.
3. In the **Task type** window of the New Task Wizard, select the **Kaspersky Security Center 10 Administration Server** node, expand the **Advanced** folder, and select the **Force downloading of updates to repositories of update agents** task.
4. Follow the Wizard's steps.

When the wizard completes its operation, the newly created **Force downloading of updates to repositories of update agents** task appears on the list of Network Agent tasks in the target administration group and in the **Tasks** folder.

When the **Force downloading of updates to repositories of update agents** task is performed, updates for databases and software modules are downloaded from the update source and stored in the shared folder. The task results are only used by update agents in the target administration group if the **Download updates to the repository** task of the Administration Server has not been explicitly specified for them.

If the **Force downloading of updates to repositories of update agents** task is created for a group of devices, the administrator cannot access the shared folder with updates.

If a local **Force downloading of updates to repositories of update agents** task is created for the device, the administrator can access the shared folder with updates.

# Configuring the download updates to the repository task

► *To configure the download updates to the repository task:*

1. In the workspace of the **Tasks** console tree folder, select **Download updates to the repository** in the task list.
2. Open the task properties window in one of the following ways:
  - From the context menu of the task, select **Properties**.
  - By clicking the **Change task settings** link in the workspace of the selected task.

This will open the **Download updates to the repository** task properties window. In this window you can configure how the updates are downloaded to the Administration Server repository.

## Verifying downloaded updates

► *To make Kaspersky Security Center verify downloaded updates before distributing them to client devices:*

1. In the workspace of **Tasks** folder, select the **Download updates to the repository** task in the list of tasks.
2. Open the task properties window in one of the following ways:
  - From the context menu of the task, select **Properties**.
  - By clicking the **Change task settings** link in the workspace of the selected task.
3. In the task properties window that opens, in the **Updates verification** section, select the **Verify updates before distributing** check box and then select the update verification task in one of the following ways:
  - Click **Select** to choose an existing update verification task.
  - Click the **Create** button to create an update verification task.

This starts the Update Verification Task Wizard. Follow the instructions of the Wizard.

When creating the update verification task, select the administration group that contains devices on which the task will be run. Devices included in this group are called *test devices*.

It is recommended to use devices with the most reliable protection and the most popular application configuration across the network. This approach increases the quality of scans, and minimizes the risk of false positives and the probability of virus detection during scans. If viruses are detected on test devices, the update verification task is considered unsuccessful.

4. Click **OK** to close the properties window of the download updates to the repository task.

As a result, the update verification task is performed as part of the download updates to the repository task. The Administration Server will download updates from the source, save them in the temporary repository, and run the update verification task. If the task completes successfully, the updates will be copied from the temporary repository to the Administration Server shared folder (<Kaspersky Security Center installation folder>\Share\Updates) and distributed to all client devices for which the Administration Server is the source of updates.

If the results of the update verification task show that updates located in the temporary repository are incorrect or if the update verification task completes with an error, such updates will not be copied to the shared folder, and the Administration Server will retain the previous set of updates. The tasks that have the **When new updates are downloaded to the repository** schedule type are not started then, either. These operations will be performed at the next start of the download updates to the repository task if scanning of the new updates completes successfully.

A set of updates is considered to be invalid if any of the following conditions is met on at least one test device:

- Update task error has occurred.
- The real-time protection status of the security application changed after the updates had been applied.
- An infected object has been detected while running the on-demand scan task.
- A runtime error of a Kaspersky Lab application has occurred.

If none of the listed conditions is true for any test device, the set of updates is considered to be valid, and the update verification task completes successfully.

## Configuring test policies and auxiliary tasks

When creating an update verification task, the Administration Server generates test policies, auxiliary group update tasks and on-demand scan tasks.

Auxiliary group update and on-demand scan tasks take some time. These tasks are performed when the update verification task is executed. The update verification task is performed during execution of the download updates to the repository task. The duration of the download updates to the repository task includes auxiliary group update and on-demand scan tasks.

You can change the settings of test policies and auxiliary tasks.

► *To change settings of a test policy or an auxiliary task:*

1. In the console tree, select a group for which the update verification task is created.
2. In the group workspace, select one of the following tabs:
  - **Policies**, if you want to edit the test policy settings.
  - **Tasks**, if you want to change auxiliary task settings.
3. In the tab workspace select a policy or a task, whose settings you want to change.
4. Open the policy (task) properties window in one of the following ways:
  - From the context menu of the policy (task), select **Properties**.
  - By clicking the **Change policy settings (Change task settings)** link in the workspace of the selected policy (task).

To verify updates correctly, the following restrictions should be imposed on the modification of test policies and auxiliary tasks:

- In the auxiliary task settings:
  - Save all tasks with the **Critical event** and **Functional failure** importance levels on Administration Server. Using the events of these types, the Administration Server analyzes the operation of applications.
  - Use Administration Server as the source of updates.
  - Specify task schedule type: **Manually**.
- In the settings of test policies:
  - Disable the iChecker, iSwift, and iStream scanning acceleration technologies.
  - Select an action to perform on infected objects: **Do not prompt/Skip/Write information to report**.
- In the settings of test policies and auxiliary tasks:

If the device needs a restart after installation of updates for software modules, it must be performed immediately. If the device is not restarted, it is impossible to test this type of updates. For some applications installation of updates that require a restart may be prohibited or configured to prompt the user for confirmation first. These restrictions should be disabled in the settings of test policies and auxiliary tasks.

## Viewing downloaded updates

► *To view the list of downloaded updates,*

In the console tree, in the **Repositories** folder, select the **Kaspersky Lab software updates and patches** subfolder.

The workspace of the **Kaspersky Lab software updates and patches** folder shows the list of updates that have been saved on the Administration Server.

# Automatic distribution of updates

Kaspersky Security Center allows you to automatically distribute and install updates on client devices and slave Administration Servers.

## In this section:

Distributing updates to client devices automatically .....	<a href="#">295</a>
Distributing updates to slave Administration Servers automatically .....	<a href="#">296</a>
Installing updates for program modules of Network Agents automatically .....	<a href="#">297</a>
Assigning devices to act as update agents .....	<a href="#">298</a>
Removing a device from the list of update agents.....	<a href="#">300</a>
Downloading updates by update agents.....	<a href="#">301</a>

## Distributing updates to client devices automatically

► *To distribute updates of the selected application to client devices automatically immediately after they are downloaded to the Administration Server repository:*

1. Connect to the Administration Server, which manages the client devices.
2. Create an update deployment task for the selected client devices using one of the following methods:
  - If you need to distribute updates to client devices that belong to a selected administration group, create a task for the selected group (see section "Creating a group task" on page [117](#)).
  - If you need to distribute updates to client devices that belong to different administration groups or do not belong to any of them, create a task for specific devices (see section "Creating a task for specific devices" on page [119](#)).

This starts the New Task Wizard. Follow its instructions and perform the following actions:

- a. In the **Task type** wizard window, in the node of the required application select the updates deployment task.

The name of the updates deployment task displayed in the **Task type** window depends on the application for which you create this task. For detailed information about names of update tasks for the selected Kaspersky Lab application, see the corresponding Guides.

- b. In the **Schedule** wizard window, in the **Scheduled start** field, select **When new updates are downloaded to the repository**.

As a result, the newly created update distribution task will start for the selected devices every time any updates are downloaded to the Administration Server repository.

If an update distribution task for the required application has already been created for the selected devices, to automatically distribute updates to client devices, in the task properties window, in the **Schedule** section, select **When new updates are downloaded to the repository** as the start option in the **Scheduled start** field.

## Distributing updates to slave Administration Servers automatically

- ▶ *To distribute the updates of the selected application to slave Administration Servers immediately after the updates are downloaded to the master Administration Server repository:*

1. In the console tree, in the master Administration Server node, select the **Tasks** folder.
2. In the list of tasks in the workspace, select the download updates to the repository task of the Administration Server.



3. Open the **Settings** section of the selected task in one of the following ways:
  - From the context menu of the task, select **Properties**.
  - By clicking the **Edit settings** link in the workspace of the selected task.
4. In the **Settings** section of the task properties window, select the **Other settings** subsection, click the **Configure** link. This opens the **Other settings** window.
5. In the **Other settings** window that opens, select the **Force update of slave Servers** check box.

In the settings of the updates download task of the Administration Server, on the **Settings** tab of the task properties window, select the **Force update of slave Servers** check box.

As a result, after the master Administration Server retrieves updates, the updates download tasks automatically start on slave Administration Servers regardless of their schedule.

## Installing updates for program modules of Network Agents automatically

► *To install updates for program modules of Network Agents automatically after they are uploaded to the Administration Server repository:*

1. In the console tree, in the master Administration Server node, select the **Tasks** folder.
2. In the list of tasks in the workspace, select the download updates to the repository task of the Administration Server.
3. Open the properties window of the selected task using one of the following methods:
  - From the context menu of the task, select **Properties**.
  - By clicking the **Edit settings** link in the workspace of the selected task.
4. In the task properties window, select the **Settings** section.
5. Click the **Configure** link in the **Other settings** section to open the **Other settings** window.

6. In the **Other settings** window that opens, select the **Update Network Agent modules** check box.

If this check box is selected, updates for program modules of Network Agent will be automatically installed after they are uploaded to the Administration Server repository. If this check box is cleared, Network Agent updates will not be installed automatically. Retrieved updates can be installed manually. By default, this check box is selected.

Network Agent program modules can only be installed automatically for Network Agent 10 Service Pack 1 or later.

7. Click **OK**.

As a result, updates for Network Agent program modules will be installed automatically.

## Assigning devices to act as update agents

Kaspersky Security Center allows you to assign devices to act as update agents.

Assignment can be performed automatically (using Administration Server) or manually.

If the administration group structure reflects the network topology, or if selected network segments correspond to a specific administration group, you can use automatic assignment of update agents.

If the administration group structure does not reflect the network topology, we recommend that you disable automatic assignment of update agents and assign one or several devices to act as update agents in each of the selected network segments instead.

When assigning update agents manually, we recommend that you assign 100–200 managed devices to a single update agent.

► *To manually assign a device to act as update agent:*

1. In the console tree, select the **Administration Server** node.
2. In the context menu of the Administration Server, select **Properties**.

3. In the Administration Server properties window, select the **Update agents** section and click the **Add** button.

This opens the **Add update agent** window.

4. In the **Add update agent** window, perform the following actions:
  - a. Select a device that will act as update agent (select one in an administration group, or specify the IP address of a device). When selecting the device, keep in mind the operation features of update agents and requirements set for a device that acts as update agent (see section "Update agent" on page [79](#)).
  - b. Indicate the specific devices to which the update agent will distribute updates. You can specify an administration group or a Network Location Awareness (NLA) subnet.

5. Click **OK**.

The update agent that you have added will be displayed in the list of update agents, in the **Update agents** section.

6. Select the newly added update agent in the list and click the **Properties** button to open its properties window.

7. Configure the update agent in the properties window:

- In the **General** section, specify the SSL port number, the address and number of the IP delivery port for IP multicasting, as well as the set of data distributed by the update agent (any update agent can distribute updates and/or installation packages).
- In the **Scope** section, specify the scope to which the update agent will distribute updates (administration groups and/or an NLA subnet).
- In the **Network poll** section, configure the polling of Windows domains, Active Directory, and IP subnets by the update agent.
- In the **Advanced** section, specify the folder that the update agent must use to store distributed data.

As a result, the selected devices act as update agents.

► *To assign update agents automatically through the Administration Server:*

1. In the console tree, select the **Administration Server** node.
2. In the context menu of the Administration Server, select **Properties**.
3. In the Administration Server properties window, in the **Update agents** section, select the **Define update agents automatically** check box.

If automatic assignment of devices to act as update agents is enabled, you cannot configure update agents manually nor edit the list of update agents.

4. Click **OK**.

As a result, Administration Server assigns and configures update agents automatically.

## Removing a device from the list of update agents

► *To remove a device from the list of update agents:*

1. In the console tree, select the **Administration Server** node.
2. In the context menu of the Administration Server, select **Properties**.
3. In the Administration Server properties window, in the **Update agents** section, select the device that acts as update agent, and click the **Remove** button.

As a result, the device will be removed from the list of update agents and will stop acting as update agent.

You cannot remove a device from the list of update agents if it was appointed by the Administration Server automatically (see section "Assigning devices to act as update agents" on page [298](#)).

# Downloading updates by update agents

Kaspersky Security Center allows update agents to receive updates from the Administration Server, Kaspersky Lab servers, or from a local or network folder.

► *To configure update download for an update agent:*

1. In the console tree, select the **Administration Server** node.
2. In the context menu of the Administration Server, select **Properties**.
3. In the Administration Server properties window, in the **Update agents** section, select the update agent through which updates will be delivered to client devices in the group.
4. Click the **Properties** button to open the properties window of the selected update agent.
5. In the update agent properties window, select the **Updates source** section.
6. Select an update source for the update agent:
  - To allow the update agent to receive updates from the Administration Server, select **Retrieve from Administration Server**.
  - To allow the update agent to receive updates using the task, select **Use update download task**:
    - Click **Select** to choose an existing updates download task of the update agent.
    - Click the **New task** button to create the updates download task for the update agent.

The update download task by an update agent is a local task. You have to create a new update download task for each device that acts as update agent.

As a result, the update agent will receive updates from the specified source.

# Rolling back installed updates

► *To roll back the updates that have been installed:*

1. In the **Application management** folder of the console tree, select the **Software updates** subfolder.
2. In the workspace of the **Software updates** folder, select the update that you want to roll back.
3. In the context menu of the update, select **Delete update files**.
4. Run the update task (see section "Automatic installation of Kaspersky Endpoint Security updates on devices" on page [208](#)).

When this task is complete, the update installed on the client device is rolled back and its status is changed to **Not installed**.

---

# Working with application keys

This section describes the features of Kaspersky Security Center related to handling keys of managed Kaspersky Lab applications.

Kaspersky Security Center allows you to perform centralized distribution of keys for Kaspersky Lab applications on client devices, monitor their use, and renew licenses.

When adding a key using Kaspersky Security Center, the settings of the key are saved on Administration Server. Based on this information, the application generates a key usage report and notifies the administrator of expiry of licenses and violation of license restrictions implied by the settings of keys. You can configure notifications of the use of keys within the Administration Server settings.

## In this section:

Viewing information about keys in use .....	<a href="#">303</a>
Adding a key to the Administration Server repository .....	<a href="#">304</a>
Deleting an Administration Server key.....	<a href="#">305</a>
Deploying a key to client devices .....	<a href="#">305</a>
Automatic distribution of a key .....	<a href="#">306</a>
Creating and viewing a key usage report.....	<a href="#">307</a>




## Viewing information about keys in use

► *To view information about keys in use,*

In the console tree, in the **Application management** folder, select the **Kaspersky Lab licenses** subfolder.

The workspace of the folder displays a list of keys used on client devices.

Next to each of the keys an icon is displayed, corresponding to the type of use:

-  – Information about the key is received from a client device connected to the Administration Server. The file of this key is stored outside of the Administration Server.
-  – The key file is stored in the Administration Server repository. Automatic distribution is disabled for this key.
-  – The key file is stored in the Administration Server repository. Automatic distribution is enabled for this key.

You can view information about keys used with the application on a client device, by opening the **Applications** section of the properties window of that client device (see section "Viewing and editing the local application settings" on page [128](#)).

To define the up-to-date settings of virtual Administration Server keys, the Administration Server sends a request to Kaspersky Lab activation servers at least once per day.

## Adding a key to the Administration Server repository

► *To add a key to the Administration Server repository:*

1. In the console tree, in the **Application management** folder, select the **Kaspersky Lab licenses** subfolder.
2. Start the key adding task using one of the following methods:
  - From the context menu of the list of keys select **Add key**.
  - By clicking the **Add key** link in the workspace of the list of keys.

This will start the Add Key Wizard. Follow the instructions of the Wizard.



# Deleting an Administration Server key

► *To delete an Administration Server key:*

1. In the context menu of the Administration Server, select **Properties**.
2. In the Administration Server properties window that opens, select the **Keys** section.
3. Delete the active or additional key by clicking the **Remove** button.

This deletes the key.

If an additional key has been added, after the active key is deleted the additional key automatically becomes the active key.

After the active key is deleted, such features as **Systems Management** (see section "**Kaspersky Security Center licensing options**" on page [61](#)) and **Mobile Device Management** (see section "**Kaspersky Security Center licensing options**" on page [61](#)) become unavailable for Administration Server. You can add (see section "Adding a key to the Administration Server repository" on page [304](#)) a key that has been deleted, or add a different key.

## Deploying a key to client devices

Kaspersky Security Center allows distributing a key to client devices through the key distribution task.

► *To distribute a key to client devices:*

1. In the console tree, in the **Application management** folder, select the **Kaspersky Lab licenses** subfolder.
2. In the workspace of the list of keys, click the **Deploy key to managed devices** button.

This starts the Key Distribution Task Creation Wizard. Follow the instructions of the Wizard.

Tasks created through the Key Distribution Task Creation Wizard are tasks for specific devices stored in the **Tasks** folder of the console tree.

You can also create a group or local key distribution task through the Task Creation Wizard for an administration group and for a client device.

# Automatic distribution of a key

Kaspersky Security Center allows automatic distribution of keys to managed devices if they are located in the keys repository on the Administration Server.

► *To distribute a key to managed devices automatically:*

1. In the console tree, in the **Application management** folder, select the **Kaspersky Lab licenses** subfolder.
2. In the workspace of the folder, select the key that you want to distribute to devices automatically.
3. Open the properties window of the selected key using one of the following methods:
  - From the context menu of the key select **Properties**.
  - By clicking the **View key properties** link in the workspace of the selected key.
4. In the key properties window that opens, select the **Automatically deployed key** check box. Close the key properties window.

As a result, the key will be automatically distributed as the active or additional key to all compatible devices.

Key distribution is performed by means of the Network Agent. No additional key distribution tasks are created for the application.

Automatic distribution of a key as the active or additional key takes into account the licensing limit of the number of devices imposed in the key's properties. If the licensing limit is reached, distribution of this key on devices ceases automatically.

# Creating and viewing a key usage report

► *To create a report on usage of keys on client devices:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Reports** tab.
3. Select the report template named **Key usage report**, or create a new report template of the same type.

As a result, the workspace of the key usage report displays information about active and additional keys used on the client devices. The report also contains information about devices on which the keys are used, and about restrictions specified in the settings of those keys.

---

# Data repositories

This section provides information about data stored on the Administration Server and used for tracking the condition of client devices and servicing them.

The **Repositories** folder of the console tree displays the data used for tracking the statuses of client devices.

The **Repositories** folder contains the following objects:

- Updates downloaded by the Administration Server that are distributed to client devices (see section "Viewing downloaded updates" on page [294](#)).
- List of equipment detected on the network.
- Keys detected on client devices (see section "Working with application keys" on page [303](#)).
- Files placed to Quarantine folders on devices by security applications.
- Files placed to Backup on client devices.
- Files postponed for a later scan by security applications.

## In this section:

Exporting a list of repository objects to a text file .....	<a href="#">309</a>
Installation packages.....	<a href="#">309</a>
Quarantine and Backup.....	<a href="#">309</a>
Unprocessed files .....	<a href="#">314</a>

# Exporting a list of repository objects to a text file

You can export the list of objects from the repository to a text file.

► *To export the list of objects from the repository to a text file:*

1. In the console tree, select **Repositories** folder, the necessary subfolder.
2. In the repository subfolder, select **Export list**.

This will open the **Export list** window, in which you can specify the name of text file and path to the folder where it was placed.

## Installation packages

Kaspersky Security Center places the installation packages of applications by Kaspersky Lab and third-party vendors into data repositories.

An *installation package* is a set of files required to install an application. An installation package contains the setup settings and initial configuration of the application being installed.

If you want to install an application on a client device, you must create an installation package for that application (see section "Creating installation packages of applications" on page [226](#)), or use an existing one. The list of created installation packages is stored in the **Remote installation** folder of the console tree, the **Installation packages** subfolder.

For detailed information on installation packages, see *Kaspersky Security Center Implementation Guide*.

## Quarantine and Backup

Kaspersky Lab anti-virus applications installed on client devices may place files to Quarantine or Backup during computer scan.

*Quarantine* is a special repository for storing files that are probably infected with viruses and files that cannot be disinfected at the time when they are detected.

*Backup* is designed for storing backup copies of files that have been deleted or modified during the disinfection process.

Kaspersky Security Center creates a summarized list of files placed to Quarantine or Backup by Kaspersky Lab applications on client devices. Network Agents on client devices transmit information about the files in Quarantine and Backup to the Administration Server. You can use Administration Console to view the properties of files stored in repositories on devices, run virus scans of those repositories, and delete files from them.

Operations with Quarantine and Backup are supported for versions 6.0 or later of Kaspersky Anti-Virus for Windows Workstations and Kaspersky Anti-Virus for Windows Servers, as well as for Kaspersky Endpoint Security 10 for Windows.

Kaspersky Security Center does not copy files from repositories to Administration Server. All files are stored in repositories on devices. You can restore a file only on the device with the anti-virus application, which placed that file to the repository.

### In this section:

Enabling remote management for files in the repositories .....	<a href="#">310</a>
Viewing properties of a file placed in repository .....	<a href="#">311</a>
Removing files from repositories .....	<a href="#">312</a>
Restoring files from repositories.....	<a href="#">312</a>
Saving a file from repositories to disk .....	<a href="#">313</a>
Scanning files in Quarantine .....	<a href="#">313</a>

# Enabling remote management for files in the repositories

By default, you cannot manage files placed in repositories on client devices.

► *To enable remote management of files stored in repositories on client devices:*

1. In the console tree, select an administration group, for which you want to enable remote management for files in the repository.
2. In the group workspace, open the **Policies** tab.
3. On the **Policies** tab, select the policy of the security application that has placed the files to the repositories on the devices.
4. In the policy settings window in the **Inform Administration Server** group of settings, select the check boxes corresponding to the repositories for which you want to enable the remote management.

The location of the **Inform Administration Server** settings group in the policy properties window and the names of check boxes depend on the currently used security application.

## Viewing properties of a file placed in repository

► *To view properties of a file in Quarantine or Backup:*

1. In the console tree, select the **Repositories** folder, the **Quarantine** or **Backup** subfolder.
2. In the workspace of the **Quarantine (Backup)** folder, select a file whose properties you want to view.
3. Open the file properties window in one of the following ways:
  - From the context menu of the file, select **Properties**.
  - Click the **Show object properties** link in the workspace of the selected file.

# Removing files from repositories

► *To delete a file from Quarantine or Backup:*

1. In the console tree, select the **Repositories** folder, the **Quarantine** or **Backup** subfolder.
2. In the workspace of the **Quarantine (Backup)** folder select the files that you want to delete by using the **Shift** and **Ctrl** keys.
3. Delete the files in one of the following ways:
  - From the context menu of the files select **Remove**.
  - Click the **Delete objects (Delete object** if you want to delete one file) link in the workspace of the selected files.

As a result, the security applications that placed files to repositories on client devices will delete the same files from those repositories.

# Restoring files from repositories

► *To restore a file from Quarantine or Backup:*

1. In the console tree, select the **Repositories** folder, the **Quarantine** or **Backup** subfolder.
2. In the workspace of the **Quarantine (Backup)** folder select the files that you want to restore by using the **Shift** and **Ctrl** keys.
3. Start files restoration in one of the following ways:
  - From the context menu of the files, select **Restore**.
  - By clicking the **Restore** link in the workspace of the selected files.

As a result, the security applications that placed files to repositories on client devices will restore the same files to their original folders.



# Saving a file from repositories to disk

Kaspersky Security Center allows you to save to disk copies of files that were placed by a security application to Quarantine or Backup on a client device. Files are copied to the device with Kaspersky Security Center installed, to the specified folder.

► *To save a copy of file from Quarantine or Backup to hard drive:*

1. In the console tree, select the **Repositories** folder, the **Quarantine** or **Backup** subfolder.
2. In the workspace of the **Quarantine (Backup)** folder, select a file that you want to copy to the hard drive.
3. Start copying the files in one of the following ways:
  - In the context menu of the file, select the **Save to Disk** item.
  - Click the **Save to Disk** link in the workspace of the selected file.

As a result, the security application that placed the file to Quarantine on the client device will save a copy of that file to the specified folder.

# Scanning files in Quarantine

► *To scan quarantined files:*

1. In the console tree, select the **Repositories** folder, the **Quarantine** subfolder.
2. In the workspace of the **Quarantine** folder select the files that you want to scan by using the **Shift** and **Ctrl** keys.
3. Start the file scanning process in one of the following ways:
  - Select **Scan Quarantined Files** from the context menu of the file.
  - By clicking the **Test** link in the workspace of the selected files.

As a result, the application runs the on-demand scan task for security applications that have placed the selected files to Quarantine on the devices where those files are stored.

# Unprocessed files

Information about unprocessed files detected on client devices is stored in the **Repositories** folder, in the **Unprocessed files** subfolder.

Postponed processing and disinfection are performed by the security application upon request or after a specified event occurs. You can configure the postponed processing.

## Disinfecting unprocessed files

► *To start disinfection of unprocessed files:*

1. In the console tree, select the **Repositories** folder, the **Unprocessed files** subfolder.
2. In the workspace of the **Unprocessed files** folder, select a file that you want to disinfect.
3. Start disinfecting the file in one of the following ways:
  - From the context menu of the file, select **Disinfect**.
  - By clicking the **Disinfect** link in the workspace of the selected file.

The attempt to disinfect this file is then performed.

If the file is disinfected, the security application installed on the client device restores it to its original folder. The record about the file is removed from list in the **Unprocessed files** folder. If the file cannot be disinfected, the security application installed on the device deletes it from that device. The record about the file is removed from list in the **Unprocessed files** folder.

## Saving an unprocessed file to disk

Kaspersky Security Center allows you to save to disk copies of unprocessed files found on client devices. Files are copied to the device with Kaspersky Security Center installed, to the specified folder.

► *To save a copy of an unprocessed file to disk:*

1. In the console tree, select the **Repositories** folder, the **Unprocessed files** subfolder.
2. In the workspace of the **Unprocessed files** folder, select files that you want to copy on the hard drive.
3. Start copying the files in one of the following ways:
  - In the context menu of the file, select the **Save to Disk** item.
  - Click the **Save to Disk** link in the workspace of the selected file.

As a result, the security application installed on the client device on which the unprocessed file has been found will save a copy of that file to the specified folder.

## Deleting files from the Unprocessed files folder

► *To delete a file from the **Unprocessed files** folder:*

1. In the console tree, select the **Repositories** folder, the **Unprocessed files** subfolder.
2. In the workspace of the **Unprocessed files** folder select the files that you want to delete by using the **Shift** and **Ctrl** keys.
3. Delete the files in one of the following ways:
  - From the context menu of the files select **Remove**.
  - Click the **Delete objects** (**Delete object** if you want to delete one file) link in the workspace of the selected files.

As a result, the security applications that placed the files to repositories on client devices, will delete the same files from those repositories. The records about files are removed from list in the **Unprocessed files** folder.

---

# Kaspersky Security Network (KSN)

This section describes how to use an online service infrastructure named Kaspersky Security Network (KSN). The section provides the details on KSN, as well as instructions on how to enable KSN, configure access to KSN, and view the statistics of the use of KSN proxy server.

## About KSN

Kaspersky Security Network (KSN) is an online service infrastructure that provides access to the online Knowledge Base of Kaspersky Lab, which contains information about the reputation of files, web resources, and software. The use of data from Kaspersky Security Network ensures faster responses by Kaspersky Lab applications to threats, improves the effectiveness of some protection components, and reduces the risk of false positives. KSN allows you to use Kaspersky Lab reputation databases to retrieve information about applications installed on client devices.

By participating in KSN, you agree to send to Kaspersky Lab in automatic mode information about the operation of Kaspersky Lab applications installed on client devices that are managed through Kaspersky Security Center, in accordance with the KSN Statement. Information is transferred in accordance with the current KSN access settings (see section "Setting up access to KSN" on page [318](#)).

The application prompts you to join KSN when installing the application and when running the Quick Start Wizard (see section "Administration Server Quick Start Wizard" on page [67](#)). You can start or stop using KSN at any moment when using the application (see section "Enabling and disabling KSN" on page [320](#)).

Client devices managed by the Administration Server interact with KSN through KSN Proxy. KSN Proxy provides the following features:

- Client devices can send requests to KSN and transfer information to KSN even if they do not have direct access to the Internet.
- The KSN proxy server caches processed data, thus reducing the load on the outbound channel and the time period spent for waiting for information requested by a client device.

You can configure KSN Proxy server in the **KSN proxy server** section of the Administration Server properties window (see section "Setting up access to KSN" on page [318](#)).

# About data provision

By participating in Kaspersky Security Network, you agree to send to Kaspersky Lab in automatic mode information about the operation of Kaspersky Lab applications installed on client devices that are managed through Kaspersky Security Center. Kaspersky Lab experts use information retrieved from client devices to solve problems in Kaspersky Lab applications or to modify some of their features.

If you participate in Kaspersky Security Network, you agree to send to Kaspersky Lab in automatic mode the following information retrieved by Kaspersky Security Center on your device:

- Name, version, and language of the software product for which the update is to be installed.
- Version of the update database that is used by the software during installation.
- Result of the update installation.
- Device ID and Network Agent version.
- Software settings used when installing updates, such as the IDs of operations executed and the codes of results for those operations.

If you cancel your participation in Kaspersky Security Network program, the above-listed details will not be sent to Kaspersky Lab.

Retrieved information is protected by Kaspersky Lab pursuant to the requirements of the current legislation and the existing rules of Kaspersky Lab. Kaspersky Lab uses retrieved information in non-personalized form only and as general statistics. The general statistical data is generated automatically based on originally retrieved information and contains no personal details or other confidential data. The originally retrieved information is stored in encrypted form and erased as it is accumulated (two times per year). The storage term of general statistical data is unlimited.

Provision of data is accepted on a voluntary basis. The feature of data provision can be enabled or disabled at any moment in the application settings window.

# Setting up the access to KSN

► *To set up Administration Server's access to KSN:*

1. In the console tree, select the Administration Server for which you need to configure the access to KSN.
2. In the context menu of the Administration Server, select **Properties**.
3. In the Administration Server properties window, in the **KSN proxy server** section, select the **KSN proxy server settings** section.
4. Select the **Use Administration Server as proxy server** check box to enable the KSN Proxy service.

Data is sent from client devices to KSN in accordance with the Kaspersky Endpoint Security policy, which is active on those client devices. If this check box is cleared, no data will be sent to KSN from the Administration Server and client devices through Kaspersky Security Center. However, client devices can send data to KSN directly (bypassing Kaspersky Security Center), in accordance with their respective settings. The Kaspersky Endpoint Security for Windows policy, which is active on client devices, determines which data will be directly (bypassing Kaspersky Security Center) sent by those devices to KSN.

5. Select the **I agree to participate in Kaspersky Security Network** check box.

If this check box is selected, client devices send patch installation results to Kaspersky Lab. When selecting this check box, you should read and accept the terms of the KSN Statement.

If you are using Private KSN (the infrastructure of KSN is located not on Kaspersky Lab servers but, for instance, within the Internet provider's network), select the **Configure Private KSN** check box and click the **Select file with KSN settings** button to download the settings of Private KSN (files with the extensions pkcs7, pem). After the settings are downloaded, the interface displays the provider's name and contacts, as well as the creation date of the file with the settings of Private KSN.

The following Kaspersky Lab applications support Private KSN:

- Kaspersky Security Center 10 Service Pack 1 or later
- Kaspersky Endpoint Security 10 Service Pack 1 or later

- Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2
- Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent

If you use application versions earlier than Kaspersky Security for Virtualization 3.0 Agentless Protection Service Pack 2 or earlier than Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent when running Private KSN, we recommend that you use slave Administration Servers for which the use of Private KSN has not been enabled.

6. Configure the Administration Server connection to the KSN Proxy service:

- In the **TCP port** entry field, specify the number of the TCP port that will be used for connecting to KSN Proxy server. The default port to connect to KSN Proxy server is 13111.
- If you need the Administration Server to connect to KSN Proxy server through a UDP port, select the **Use UDP port** check box and specify a port number in the **UDP port** field. By default, this check box is cleared, and UDP port 15111 is used for connecting to KSN Proxy server.

7. Select the **Connect slave Administration Servers to KSN via master Administration Server** check box.

If this check box is selected, slave Administration Servers use the master Administration Server as the KSN proxy server. If this check box is cleared, slave Administration Servers connect to KSN on their own. In this case, managed devices use slave Administration Servers as KSN proxy servers.

Slave Administration Servers use the master Administration Server as a proxy server if the **KSN proxy server** section in the properties of slave Administration Servers has the **Use Administration Server as proxy server** check box selected.

8. Click **OK**.

As a result, the KSN access settings will be saved.

# Enabling and disabling KSN

## ► To enable KSN:

1. In the console tree, select the Administration Server for which you need to enable KSN.
2. In the context menu of the Administration Server, select **Properties**.
3. In the Administration Server properties window, in the **KSN proxy server** section, select the **KSN proxy server settings** subsection.
4. Select the **Use Administration Server as proxy server**.

As a result, the KSN proxy server is enabled.

5. Select the **I agree to participate in Kaspersky Security Network** check box.

As a result, KSN will be enabled.

If this check box is selected, client devices send patch installation results to Kaspersky Lab. When selecting this check box, you should read and accept the terms of the KSN Statement.

6. Click **OK**.

## ► To disable KSN:

1. In the console tree, select the Administration Server for which you need to enable KSN.
2. In the context menu of the Administration Server, select **Properties**.
3. In the Administration Server properties window, in the **KSN proxy server** section, select the **KSN proxy server settings** subsection.
4. Clear the **Use Administration Server as proxy server** check box to disable the KSN Proxy service, or clear the **I agree to participate in Kaspersky Security Network** check box.

If this check box is cleared, client devices will send no patch installation results to Kaspersky Lab.

If you are using Private KSN, clear the **Configure Private KSN** check box.

As a result, KSN will be disabled.

5. Click **OK**.



# Viewing the KSN proxy server statistics

*KSN proxy server* is a service that ensures interaction between the Kaspersky Security Network infrastructure and client devices managed through the Administration Server.

Using a KSN Proxy server provides you the following features:

- Client devices can send requests to KSN and transfer information to KSN even if they do not have direct access to the Internet.
- The KSN proxy server caches processed data, thus reducing the load on the outbound channel and the time period spent for waiting for information requested by a client device.

In the Administration Server properties window, you can configure the KSN Proxy server and view the statistics on the KSN Proxy server usage.

► *To view the statistics of KSN proxy server:*

1. In the console tree, select the Administration Server for which you need to view the KSN statistics.
2. In the context menu of the Administration Server, select **Properties**.
3. In the Administration Server properties window, in the **KSN proxy server** section, select the **KSN proxy server statistics** subsection.

This section displays the statistics of the operation of KSN proxy server. If necessary, perform these additional actions:

- Click **Refresh** to update the statistics on the KSN Proxy server usage.
  - Click the **Export to file** button to export the statistics to a CSV file.
  - Click the **Check KSN connection** button to check if the Administration Server is currently connected to KSN.
4. Click the **OK** button to close the Administration Server properties window.

---

# Contacting the Technical Support Service

This section provides information about the ways and conditions for providing you technical support.

## In this section:

How to obtain technical support .....	<a href="#">322</a>
Technical support by phone.....	<a href="#">323</a>
Technical Support via Kaspersky CompanyAccount .....	<a href="#">323</a>

## How to obtain technical support

If you do not find a solution to your problem in the documentation or in other sources of information about the application (see section "Sources of information about the application" on page [19](#)), we recommend that you contact the Kaspersky Lab Technical Support Service. Technical Support Service experts will answer your questions about installing and using the application.

Technical support is only available to users who purchased the commercial license. Users who have received a trial license are not entitled to technical support.

Before contacting the Technical Support Service, we recommend that you read through the technical support rules (<http://support.kaspersky.com/support/rules>).

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

- By calling the Technical Support Service by phone (<http://support.kaspersky.com/support/contacts>).
- By sending a request to the Kaspersky Lab Technical Support Service using the Kaspersky CompanyAccount portal (<https://companyaccount.kaspersky.com>).

## Technical support by phone

In most regions of the world, you can call experts at the Kaspersky Lab Technical Support Service. You can receive information about how to obtain technical support in your region and the contact information of the Technical Support Service on the website of the Kaspersky Lab Technical Support Service (<http://support.kaspersky.com/b2c>).

Before contacting the Technical Support Service, please read the technical support rules (<http://support.kaspersky.com/support/rules>).

## Technical Support via Kaspersky CompanyAccount

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

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

The Kaspersky CompanyAccount portal is available in the following languages:

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

To learn more about Kaspersky CompanyAccount, please visit the Technical Support Service website ([http://support.kaspersky.com/faq/companyaccount\\_help](http://support.kaspersky.com/faq/companyaccount_help)).

---

# Appendices

This section provides information that complements the document text.

## In this section:

Advanced features .....	<a href="#">325</a>
Features of using the management interface .....	<a href="#">353</a>
Reference information .....	<a href="#">355</a>

## Advanced features

This section describes a range of additional options of Kaspersky Security Center designed for expanding the functionality of centralized management of applications on devices.

## In this section:

Kaspersky Security Center operation automation. Utility tool klakaut .....	<a href="#">326</a>
Mobile users .....	<a href="#">326</a>
Events in application operation .....	<a href="#">330</a>
Defining the importance level of an event when a licensing restriction is exceeded .....	<a href="#">331</a>
Event notifications displayed by running an executable file .....	<a href="#">331</a>
Managing Kaspersky Security for Virtualization .....	<a href="#">332</a>
Monitoring the anti-virus protection status using information from the system registry .....	<a href="#">333</a>
Clusters and server arrays.....	<a href="#">334</a>

Algorithm of installation of a patch for a Kaspersky Lab application in cluster mode .....	<a href="#">335</a>
Finding devices.....	<a href="#">336</a>
Connecting to devices through Windows Desktop Sharing.....	<a href="#">337</a>
About the accounts in use .....	<a href="#">338</a>
Custom tools.....	<a href="#">338</a>
Exporting lists from dialog boxes .....	<a href="#">339</a>
Network Agent disk cloning mode.....	<a href="#">339</a>
Preparing a Linux device to remote installation of Network Agent.....	<a href="#">341</a>
Backup copying and restoration of Administration Server data .....	<a href="#">343</a>
Data backup and recovery in interactive mode .....	<a href="#">350</a>
Installing an application through Active Directory group policies .....	<a href="#">351</a>

## Kaspersky Security Center operation automation. Utility tool klakaut

You can automate the operation of Kaspersky Security Center using the klakaut utility. The klakaut utility and a help system for it are located in the installation folder of Kaspersky Security Center.

### Mobile users

Kaspersky Security Center provides the option of switching the Network Agent of a client device to other Administration Servers if the following settings of the network have been changed:

- Subnet—The subnet address and mask have changed.
- DNS domain—The DNS suffix of the subnet has changed.

- Default gateway address—The address of the main network gateway has changed.
- DHCP server address—The IP address of the network DHCP server has changed.
- DNS server address—The IP address of the network DNS server has changed.
- WINS server address—The IP address of the network WINS server has changed.
- Windows domain accessibility—The status of the Windows domain to which the client device is connected has changed.

The functionality is supported for the following operating systems: Microsoft Windows XP / Windows Vista; Microsoft Windows Server 2003 / 2008.

The initial settings of the Network Agent connection to the Server are defined when installing the Network Agent. Afterwards, if rules of switching the Network Agent to other Administration Servers have been created, the Network Agent responds to changes in the network settings as follows:

- If the network settings comply with one of the rules created, Network Agent connects to Administration Server specified in this rule. Applications installed on client devices switch to out-of-office policies provided that such behavior is enabled by a rule.
- If none of the rules apply, Network Agent roll back to the default settings of connection to the Administration Server specified during the installation. Applications installed on client devices switch back to active policies.
- If the Administration Server is not accessible, Network Agent uses out-of-office policies.

By default, Network Agent switches to out-of-office policy if the Administration Server remains inaccessible for more than 45 minutes.

The settings of Network Agent connection to Administration Server are saved in a connection profile. In the connection profile, you can create rules for switching client devices to out-of-office policies, as well as configure the profile so that it could be used for downloading updates only.

## In this section:

Creating an Administration Server connection profile for mobile users.....	<a href="#">328</a>
Creating a Network Agent switching rule.....	<a href="#">329</a>

# Creating an Administration Server connection profile for mobile users

► *To create a profile for connecting Network Agent to Administration Server for mobile users:*

1. In the console tree, select the administration group containing the client devices for which you need to create a profile for connecting Network Agent to the Administration Server.
2. Do one of the following:
  - If you need to create a connection profile for all devices in the group, select a Network Agent policy in the group workspace, on the **Policies** tab. Open the properties window of the selected policy.
  - If you need to create a connection profile for a device in a group, select that device in the group workspace, on the **Devices** tab, and perform the following actions:
    - a. Open the properties window of the selected device.
    - b. In the **Applications** section of the device properties window, select Network Agent.
    - c. Open the Network Agent properties window.
3. In the properties window that opens, in the **Network** section select the **Connection** subsection.



4. In the **Administration Server connection profiles** section click the **Add** button.

By default, the list of connection profiles contains the <Not connected> profile only. The profile cannot be edited or removed. It does not specify any Server for connection, so Network Agent, after switching to it, will not attempt to connect to any Server while applications installed on client devices will run under out-of-office policies. The <Not connected> profile can be used if devices are disconnected from the network.

5. In the **New profile** window that opens, configure the connection profile and select the **Enable out-of-office policies** check box.

As a result, a profile for connecting Network Agent to Administration Server is created for mobile users. When Network Agent connects to Administration Server using this profile, applications installed on the client device will use out-of-office policies.

## Creating a Network Agent switching rule


- *To create a rule of switching the Network Agent from one Administration Server to another in case of changes in the network settings:*

1. In the console tree, select the administration group containing the devices for which you need to create a Network Agent switching rule.
2. Do one of the following:
  - If you need to create a switching rule for all devices in the group, go to the group workspace and select a Network Agent policy on the **Policies** tab. Open the properties window of the selected policy.
  - If you need to create a switching rule for a device selected from a group, go to the group workspace, select the device on the **Devices** tab, and perform the following actions:
    - a. Open the properties window of the selected device.
    - b. In the **Applications** section of the device properties window, select Network Agent.
    - c. Open the Network Agent properties window.

3. In the properties window that opens, in the **Network** section select the **Connection** subsection.
4. In the **Switch profiles** section click the **Add** button.
5. In the **New rule** window that opens, configure a switching rule and select the **Rule activated** check box to enable the use of the rule.

As a result, a new switching rule is created; anytime its conditions are met, the Network Agent uses the connection profile specified in the rule to connect to the Administration Server.

The switching rules are checked for a match to the network layout in the order of their appearance in the list. If a network matches several rules, the first one will be used.

You can change the order of rules on the list using the  and  buttons.

## Events in application operation

Kaspersky Security Center allows you to get information about events in the operation of Administration Server and other Kaspersky Lab applications installed on client devices.

Four importance levels exist for Kaspersky Lab applications:

- **Critical event.**
- **Functional failure**
- **Warning**
- **Info.**

You can configure the events processing rules for each importance level individually.

### See also:

| Adjusting the general settings of Administration Server ..... [92](#)

# Defining the importance level of an event when a licensing restriction is exceeded

Kaspersky Security Center allows you to get information about events when some licensing restrictions are exceeded by Kaspersky Lab applications installed on client devices.

The importance level of such events when a licensing restriction is exceeded is defined according to the following rules:

- If the number of currently used units covered by a single license falls in 90–100% of the total number of units covered by the same license, the event is published with the **Info** importance level.
- If the number of currently used units covered by a single license falls in 100–110% of the total number of units covered by the same license, the event is published with the **Warning** importance level.
- If the number of currently used units covered by a single license exceeds 110% of the total number of units covered by the same license, the event is published with the **Critical event** importance level.

See also:

| [Adjusting the general settings of Administration Server..... 92](#)

## Event notifications displayed by running an executable file

Kaspersky Security Center can notify the administrator about events on client devices by running an executable file. The executable file must contain another executable file with placeholders of the event to be relayed to the administrator.

Table 4. Placeholders for describing an event

Placeholder	Placeholder description
%SEVERITY%	Event importance level
%COMPUTER%	Name of the device where the event occurred
%DOMAIN%	Domain
%EVENT%	Event
%DESCR%	Event description
%RISE_TIME%	Time created
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Task name
%KL_PRODUCT%	Kaspersky Security Center Network Agent
%KL_VERSION%	Network Agent version number
%HOST_IP%	IP address
%HOST_CONN_IP%	Connection IP address

### Example

Event notifications are sent by an executable file (such as *script1.bat*) inside which another executable file (such as *script2.bat*) with the %COMPUTER% placeholder is launched. When an event occurs, the *script1.bat* file is run on the administrator's device, which, in turn, runs the *script2.bat* file with the %COMPUTER% placeholder. As a result, the administrator receives the name of the device where the event occurred.

## Managing Kaspersky Security for Virtualization

Kaspersky Security Center supports the option of connection of virtual machines to Administration Server. Virtual machines are managed via Kaspersky Security for Virtualization 3.0. For more details, please refer to the Kaspersky Security for Virtualization 3.0 Administrator's Guide.

# Monitoring the anti-virus protection status using information from the system registry

► To monitor the anti-virus protection status on a client device using information logged by Network Agent to the system registry:

1. Open the system registry of the client device (for example, locally, using the regedit command from the **Start** → **Run** menu).
2. Go to the following hive:

```
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103
\1.0.0.0\Statistics\AVState
```

As a result, the system registry displays information about the anti-virus protection status of the client device.


The anti-virus protection status corresponds to the values of the keys described in the table below.

Table 5. Registry keys and their possible values

Key (data type)	Value	Description
Protection_AdmServer (REG_SZ)	<Administration Server name>	Name of the Administration Server, which manages the device.
Protection_AvInstalled (REG_DWORD)	non-zero	A security application is installed on the device.
Protection_AvRunning (REG_DWORD)	non-zero	The real-time protection is enabled on the device.
Protection_HasRtp (REG_DWORD)	non-zero	A real-time protection component is installed.
	Real-time protection status:	
	0	Unknown
	2	Inactive.

Key (data type)	Value	Description
	3	Paused.
	4	Starting.
	5	Active.
	6	Active, high level (maximum protection).
	7	Active, default (recommended) settings are applied.
	8	Active, custom settings are applied.
	9	Operation failure.
Protection_LastFscan (REG_SZ)	DD-MM-YYYY HH-MM-SS	Date and time (in UTC format) of the last full scan.
Protection_BasesDate (REG_SZ)	DD-MM-YYYY HH-MM-SS	Date and time (in UTC format) of the application databases release.
Protection_LastConnected (REG_SZ)	DD-MM-YYYY HH-MM-SS	Date and time (in UTC format) of the last connection to the Administration Server.

## Clusters and server arrays

Kaspersky Security Center supports the cluster technology. If Network Agent sends to Administration Server information confirming that an application installed on a client device makes part of a server array, this client device becomes a cluster node. The cluster will be added as an individual object in the **Managed devices** folder of the console tree with the  icon.

A few typical features of a cluster can be distinguished:

- A cluster and any of its nodes are always in the same administration group.
- If the administrator attempts to move a cluster node, the node moves back to its original location.
- If the administrator attempts to move a cluster to a different group, all of its nodes also move with it.

## Algorithm of installation of a patch for a Kaspersky Lab application in cluster mode

Kaspersky Security Center only supports manual installation of patches for Kaspersky Lab applications in cluster mode.

To install a patch for a Kaspersky Lab application:

1. Download the patch to each node of the cluster.
2. Run patch installation on the active node.

Wait for the patch to be successfully installed.

3. Run the patch on all subnodes of the cluster consecutively.

If you are running the patch from the command line, use the `-CLUSTER_SECONDARY_NODE` key

After that, the patch is installed on all nodes of the cluster.

4. Run the Kaspersky Lab cluster services manually.

Every node of the cluster is displayed in Administration Console as a device with Network Agent installed.

For information about installed patches, see the **Software updates** folder or the report on the versions of updates for software modules of Kaspersky Lab applications.

## See also:

| Adjusting the general settings of Administration Server..... [92](#)

# Finding devices

Kaspersky Security Center allows you to find devices on the basis of specified criteria.

Search results can be saved to a text file.

The search feature allows you to find the following devices:

- Client devices in administration groups of an Administration Server and its slave Servers.
- Unassigned devices managed by an Administration Server and its slave Servers.

### ► *To find client devices included in an administration group:*

1. In the console tree select an administration group folder.
2. Select **Search** from the context menu of the administration group folder.
3. On the tabs of the **Search** window, specify the criteria for the search of devices, and click the **Find now** button.

As a result, devices that meet the specified search criteria, are displayed in a table in the lower part of the **Search** window.

### ► *To find unassigned devices:*

1. In the console tree, select the **Unassigned devices** folder.
2. In the context menu of the **Unassigned devices** folder, select **Search**.
3. On the tabs of the **Search** window, specify the criteria for the search of devices, and click the **Find now** button.

As a result, devices that meet the specified search criteria, are displayed in a table in the lower part of the **Search** window.



► *To find devices regardless of whether they are included in an administration group:*

1. In the console tree select the **Administration Server– <Server Name>** node.
2. Select **Search** from the context menu of the node.
3. On the tabs of the **Search** window, specify the criteria for the search of devices, and click the **Find now** button.

As a result, devices that meet the specified search criteria, are displayed in a table in the lower part of the **Search** window.

In the **Search** window you can also search for administration groups and slave Administration Servers using a drop-down list in the top right corner of the window. Search for administration groups and slave Administration Servers is not available if you have opened the **Search** window from the **Unassigned devices** folder.

To find devices, you can use regular expressions in text boxes of the **Search** window (see section "Using regular expressions in the search field" on page [371](#)).

Full text search in the **Search** window is available:

- On the **Network** tab, in the **Comment** field
- On the **Hardware** tab, in the **Device**, **Vendor**, and **Description** fields.

## Connecting to devices through Windows Desktop Sharing

► *To connect to a device through Windows Desktop Sharing:*

1. In the console tree, on the **Devices** tab, select the **Managed devices** folder.

The workspace of this folder displays a list of devices.

2. In the context menu of the device to which you need to connect, select **Connect to device** → **Windows Desktop Sharing**.

The **Select remote desktop session** window opens.

3. In the **Select remote desktop session** window, select a desktop session for connection to the device.
4. Click **OK**.

The device is connected.

## About the accounts in use

You can specify an account under which the task should be run.

For example, to perform an on-demand scan task, you need access rights to the object being scanned, and to perform an update task, you need authorized proxy server user rights.

The opportunity to specify an account for the task run allows avoiding problems with on-demand scan tasks and update tasks in case the user running a task does not have the required access rights.

During the execution of remote installation/uninstallation tasks, the specified account is used to download to client computers the files required to install/uninstall an application in case Network Agent is not installed or unavailable. If Network Agent is installed and available, the account is used if according to tasks settings, files delivery is performed by using Microsoft Windows utilities from the shared folder only. In this case, the account must have the following rights on the device:

- The right to start applications remotely.
- The right to use the Admin\$ resource.
- The right to *Log On As Service*.

If the files are delivered to devices through Network Agent, the account is not used. All file copying and installation operations are then performed by the **Network Agent (Local System Account)**.

## Custom tools

Kaspersky Security Center allows you to create a list of *custom tools* (hereinafter also referred to as simply *tools*), i.e., applications activated for a client device in Administration Console, through the **Custom tools** group of the context menu. Each tool in the list will be associated

with a separate menu command, which the Administration Console uses to start the application corresponding to that tool.

The application starts on the administrator's workstation. The application can accept the attributes of a remote client device as command-line arguments (NetBIOS name, DNS name, or IP address). Connection to the remote device can be established through tunneling.

By default, the list of custom tools contains the following service programs for each client device:

- **Remote diagnostics** is a utility for remote diagnostics of Kaspersky Security Center.
- **Remote Desktop** is a standard Microsoft Windows Remote Desktop Connection component.
- **Device management** is a standard Microsoft Windows component.

► *To add or remove custom tools, or to edit their settings,*

in the context menu of the client device, select **Custom tools** → **Configure custom tools**.

As a result, the **Custom tools** window opens. In this window you can add or remove custom tools, and edit their settings using the **Add**, **Modify**, and **Remove** buttons.

## Exporting lists from dialog boxes

In dialog boxes of the application you can export lists of objects to text files.

Export of a list of objects is possible for dialog box sections that contain the **Export to file** button.

## Network Agent disk cloning mode

Cloning the hard drive of a reference device is a popular method of software installation on new devices. If Network Agent is running in normal mode on the hard drive of the reference device, the following problem arises:

After the reference disk image with Network Agent is deployed on new devices, they are displayed in Administration Console under a single icon. This problem arises because the cloning procedure causes new devices to keep identical internal data, which allows the Administration Server to associate a device with an icon in Administration Console.

The special *Network Agent disk cloning mode* allows you to avoid problems with an incorrect display of new devices in Administration Console. Use this mode when deploying software (with Network Agent) on new devices by cloning the disk.

In disk cloning mode, Network Agent keeps running, but it does not connect to the Administration Server. When exiting the cloning mode, Network Agent deletes the internal data, which causes Administration Server to associate multiple devices with a single icon in Administration Console. Upon completing the cloning of the reference device image, new devices are displayed in Administration Console properly (under individual icons).

### **Network Agent disk cloning mode usage scenario**

1. The administrator installs Network Agent on the reference device.
2. The administrator checks the connection between Network Agent and the Administration Server using the `klnagchk` utility (see section "Checking the connection between a client device and the Administration Server manually. Utility tool `klnagchk`" on page [139](#)).
3. The administrator enables the Network Agent disk cloning mode.
4. The administrator installs software and patches on the device, and restarts it as many times as needed.
5. The administrator clones the hard disk of the reference device on any number of devices.
6. Each cloned copy must meet the following conditions:
  - a. The device name must be changed.
  - b. The device must be restarted.
  - c. The disk cloning mode must be disabled.

## Enabling and disabling the disk cloning mode using the klmover utility

► *To enable / disable the Network Agent disk cloning mode:*

1. Run the klmover utility on the device with Network Agent installed that you need to clone.

The klmover utility is located in the Network Agent installation folder.

2. To enable the disk cloning mode, enter the following command in the Windows command prompt: `klmover -cloningmode 1`.

Network Agent switches into the disk cloning mode.

3. To request the current status of the disk cloning mode, enter the following command in the command prompt: `klmover -cloningmode`.

As a result, the utility window shows whether the disk cloning mode is enabled or disabled.

4. To disable the disk cloning mode, enter the following command in the utility command line: `klmover -cloningmode 0`.

## Preparing a Linux device to remote installation of Network Agent

► *To prepare a device running Linux to remote installation of Network Agent:*

1. Test the device configuration:

- a. Check if you can connect to the device through an SSH client (such as PuTTY).

If you cannot connect to the device, open the file `/etc/ssh/sshd_config` and make sure that the following settings have the respective values listed below:

```
PasswordAuthentication no
```

```
ChallengeResponseAuthentication yes
```

Save the file (if necessary) and restart the SSH service using the `sudo service ssh restart` command.

- b. Disable the Sudo password for the user account under which the device is to be connected.

Use the visudo command in Sudo to open the sudoers configuration file. In this file, specify the following: username ALL = (ALL) NOPASSWD: ALL. In this case, username is the user account, which is to be used for the device connection via SSH.

- c. Save sudoers and then close it.
- d. Connect to the device again through SSH and make sure that the Sudo service does not prompt you to enter a password; you can do this using the sudo whoami command.

2. Download and create an installation package:

- a. Before installation on the device, make sure that it already has all the dependencies (programs and libraries) installed for this package.

You can view the dependencies for each package on your own, using utilities that are specific for the Linux distribution on which that package is to be installed. For more details about utilities, see your operating system documentation.

- b. Download the Network Agent installation package.
- c. To create a remote installation package, use the following files:
  - klnagent.kpd
  - ainstall.sh
  - DEB or RPM package of Network Agent
- d. Before you create the installation package, open the ainstall.sh file and edit String 81: Mkdir -p "\$ LogDir"

3. Create a remote installation task with the following settings:

- In the **Settings** window of the New Task Wizard, select the **Using operating system resources by means of Administration Server** check box. Clear all other check boxes.
- In the **Select Account** window, to run the task, specify the settings of the user account, which is used for the device connection through SSH.

4. Run the remote installation task.

Installation may return an error if you are installing Network Agent with SSH on devices running Fedora versions earlier than 20. In this case, for successful installation of Network Agent, comment out the Defaults requiretty option in the /etc/sudoers file. For a detailed description of the condition of the Defaults requiretty option, which may cause problems during connection via SSH, please refer to the Bugzilla bugtracker website ([https://bugzilla.redhat.com/show\\_bug.cgi?id=1020147](https://bugzilla.redhat.com/show_bug.cgi?id=1020147)).

## Backup copying and restoration of Administration Server data

Data backup allows you to move Administration Server from one device to another without data loss. Through backup, you can restore data when moving the Administration Server database to another device, or when upgrading to a newer version of Kaspersky Security Center.

You can create a backup copy of Administration Server data using one of the following methods:

- Create and run a data backup task using the Administration Console.
- Run kbackup on the device with Administration Server installed. This utility is included in the Kaspersky Security Center distribution kit; after the installation of the Administration Server the utility is located in the root of the destination folder specified at the application installation.

The following data are saved in the backup copy of the Administration Server:

- Information database of the Administration Server (policies, tasks, application settings, events saved on the Administration Server).
- Configuration details of the structure of administration groups and client devices.
- Repository of distribution packages of applications for remote installation.
- Administration Server certificate.

Recovery of Administration Server data is only possible using the kbackup utility.

## In this section:

Creating a data backup task .....	<a href="#">344</a>
Data backup and recovery utility (klbackup) .....	<a href="#">345</a>
Data backup and recovery in interactive mode .....	<a href="#">345</a>
Data backup and recovery in non-interactive mode .....	<a href="#">346</a>
Moving an Administration Server to another device .....	<a href="#">348</a>

## Creating a data backup task

Backup tasks are Administration Server tasks; they are created by the Quick Start Wizard.

If a backup task created by the Quick Start Wizard has been deleted, you can create one manually.

► *To create an Administration Server data backup task:*

1. In the console tree, select the **Tasks** folder.
2. Start creating the task in one of the following ways:
  - In the console tree, in the context menu of the **Tasks** folder, select **Create** → **Task**.
  - Click the **Create a task** button in the workspace.

This starts the New Task Wizard. Follow the instructions of the Wizard. In the **Task type** window of the Wizard select the task type named **Backup of Administration Server data**.

The **Backup of Administration Server data** task can only be created in a single copy. If the Administration Server data backup task has already been created for the Administration Server, it is not displayed in the task type selection window of the Backup Task Creation Wizard.



# Data backup and recovery utility (klbackup)

You can copy Administration Server data for backup and future recovery using the klbackup utility making part of the Kaspersky Security Center distribution kit.

The klbackup utility can run in either of the two following modes:

- Interactive (see section "Data backup and recovery in interactive mode" on page [345](#))
- Non-interactive (see section "Data backup and recovery in non-interactive mode" on page [346](#)).

## Data backup and recovery in interactive mode

► *To create a backup copy of Administration Server data in interactive mode:*

1. Run the klbackup utility located in the installation folder of Kaspersky Security Center.

The Backup and Restore Wizard starts.

2. In the first window of the Wizard select **Perform backup of Administration Server data**.

If you select the **Restore or backup Administration Server certificate only** check box, a backup copy of the Administration Server certificate will only be saved.

Click **Next**.

3. In the next window of the Wizard specify a password and a destination folder for backup. Click the **Next** button to start backup.

► *To recover Administration Server data in interactive mode:*

1. Uninstall Administration Server and then reinstall it again.
2. Run the klbackup utility located in the installation folder of Kaspersky Security Center.

As a result, the Backup and Restore Wizard starts.

The klbackup utility must be started under the same account under which you installed Administration Server.

3. In the first window of the Wizard select **Restore Administration Server data**.

If you select the **Restore or backup Administration Server certificate only** check box, the Administration Server will only be recovered.

Click **Next**.

4. In the **Restore settings** window of the Wizard:

- Specify the folder, which contains a backup copy of Administration Server data.
- Specify the password that was entered during data backup.

5. Click the **Next** button to restore data.

When restoring data, you must specify the same password that was entered during backup. If you specify an invalid password, data will not be restored. If the path to a shared folder changed after backup, check the operation of tasks that use restored data (restore tasks, remote installation tasks). If necessary, edit the settings of these tasks.

While data is being restored from a backup file, the shared folder of Administration Server must not be accessed by anybody. The account under which the klbackup utility is started must have full access to the shared folder.

## Data backup and recovery in non-interactive mode

- *To create a backup copy or recover Administration Server data in non-interactive mode,*

run klbackup with the required set of keys from the command line of the device with Administration Server installed.

Utility command line syntax:

```
klbackup [-logfile LOGFILE] -path BACKUP_PATH  
[-use_ts][[-restore] -savecert PASSWORD
```

If no password is specified in the command line of the klbackup utility, the utility requests entering the password interactively.

The command-line parameters are as follows:

- `-logfile LOGFILE` – save a report on Administration Server data backup and recovery.
- `-path BACKUP_PATH` – save information in the BACKUP\_PATH folder or use data from the BACKUP\_PATH folder for recovery (mandatory setting).

The database server account and the klbackup utility should be granted permissions for changing data in the folder BACKUP\_PATH.

- `-use_ts` – when saving data, copy information to the folder BACKUP\_PATH, to the subfolder with a name containing the current system date and operation time in format `klbackup YYYY-MM-DD # HH-MM-SS`. If no key is specified, information is saved in the root of the folder BACKUP\_PATH.

When attempting to save information in a folder that already stores a backup copy, an error message appears. No information will be updated.

Availability of the `-use_ts` key allows maintaining an Administration Server data archive. For example, if the `-path` key indicates the folder `C:\KLBackups`, the folder `klbackup 2006-06-19 # 11-30-18` then stores information about the status of the Administration Server as of June, 19, 2006 at 11:30:18 AM.

- `-restore` – recover Administration Server data. Data recovery is performed based on information contained in the folder BACKUP\_PATH. If no key is available, data are backed up in the folder BACKUP\_PATH.
- `-savecert PASSWORD` – save or recover the Administration Server certificate; to encrypt and decrypt the certificate, use the password specified by the setting PASSWORD.

When restoring data, you must specify the same password that was entered during backup. If you specify an invalid password, data will not be restored. If the path to a shared folder changed after backup, check the operation of tasks that use restored data (restore tasks, remote installation tasks). If necessary, edit the settings of these tasks.

While data is being restored from a backup file, the shared folder of Administration Server must not be accessed by anybody. The account under which the klbackup utility is started must have full access to the shared folder.

## Moving an Administration Server to another device

► *To move an Administration Server to another device without shifting the Administration Server database:*

1. Create a backup copy of Administration Server data.
2. Install the Administration Server to the selected device.

To simplify the process of moving administration groups, it is recommended that you make sure that the address of the new Administration Server is the same as the address of the previous Administration Server. The address (the device name in the Windows network, or an IP address) is specified in the settings for connecting the Network Agent to the Administration Server.

3. On the new Administration Server recover Administration Server data from the backup copy.

4. If the address (the device name in the Windows network, or the IP address) of the new Administration Server does not coincide with that of the previous Administration Server, to connect client devices to the new Administration Server, create an Administration Server shift task for the **Managed devices** group on the previous Administration Server.

If the addresses coincide, you do not have to create a Server shift task, since the connection will be performed to the address specified in the settings.

5. Delete the previous Administration Server.

► *To move an Administration Server to another device and change the Administration Server database:*

1. Create a backup copy of Administration Server data.
2. Install a new SQL server.

To transfer information correctly, the database on the new SQL server should have the same collation schemes as the previous SQL server.

3. Install a new Administration Server. The name of the previous SQL server database and that of the new one should be the same.

To simplify the process of moving administration groups, it is recommended that you make sure that the address of the new Administration Server is the same as the address of the previous Administration Server. The address (the device name in the Windows network, or an IP address) is specified in the settings for connecting the Network Agent to the Administration Server.

4. On the new Administration Server recover the data from the previous Administration Server from the backup copy.
5. If the address (the device name in the Windows network, or the IP address) of the new Administration Server does not coincide with that of the previous Administration Server, to connect client devices to the new Administration Server, create an Administration Server shift task for the **Managed devices** group on the previous Administration Server.

6. If the addresses coincide, you do not have to create a Server shift task, since the connection will be performed to the address specified in the settings.
7. Delete the previous Administration Server.

## Data backup and recovery in interactive mode

The Administration Server database maintenance allows you to reduce the database volume, improve the performance and operation reliability of the application. We recommend that you maintain the Administration Server database at least every week.

The Administration Server database maintenance is performed through the dedicated task. The application performs the following actions when maintaining the database:

- Checks the database for errors.
- Re-organizes database indexes.
- Updates the database statistics.
- Shrinks the database (if necessary).

The Administration Server database maintenance task does not support MySQL. If you use MySQL as the DBMS, the administrator will have to maintain the database on his or her own.

► *To create an Administration Server database maintenance task:*

1. In the console tree, select the node of the Administration Server for which you want to create a database maintenance task.
2. Select the **Tasks** folder.
3. In the workspace of the **Tasks** folder, click the **Create a Task** button.

This starts the New Task Wizard.

4. In the **Select task type** window of the Wizard, select **Databases maintenance** as the task type and click **Next**.
5. If you need to shrink the Administration Server database during maintenance, in the **Settings** window of the Wizard, select the **Shrink database** check box.
6. Follow the further instructions of the Wizard.

The newly created task is displayed in the list of tasks in the workspace of the **Tasks** folder.

Only one database maintenance task can be running for a single Administration Server.

If a database maintenance task has already been created for an Administration Server, no new database maintenance task can be created.

## Installing an application using Active Directory group policies

Kaspersky Security Center allows you to install Kaspersky Lab applications by using Active Directory group policies.

You can install applications using Active Directory group policies only by using installation packages that include Network Agent.

► *To install an application using Active Directory group policies:*

1. Run the creation of a group remote installation task or a remote installation task for specific devices.
2. In the New Task Wizard's **Settings** window select the **Assign the package installation in the Active Directory group policies** check box.
3. Run the created remote installation task manually or wait for its scheduled start.

This starts the following remote installation sequence:

1. When the task is running, the following objects are created in each domain that includes any client devices from the specified set:
  - A group policy under the name **Kaspersky\_AK{GUID}**
  - the **Kaspersky\_AK{GUID}** security group that corresponds to the group policy. This security group includes client devices covered by the task. The content of the security group defines the scope of the group policy.
2. In this case, applications are installed on client devices directly from **Share**, i.e., the shared network folder of the application. In the Kaspersky Security Center installation folder, an auxiliary nested folder will be created that contains the .msi file for the application to be installed.
3. When new devices are added to the task scope, they are added to the security group after the next task start. If the **Run missed tasks** check box is selected in the task schedule, devices are added to the security group immediately.
4. When devices are deleted from the task scope, they are deleted from the security group after the next task start.
5. When a task is deleted from Active Directory, the policy, the link to the policy, and the corresponding security group are deleted.

If you want to apply another installation scheme using Active Directory, you can configure the required settings manually. This may be required in the following cases, for example:

- when the anti-virus protection administrator does not have rights to make changes to the Active Directory of certain domains;
- when the original installation package needs to be stored on a separate network resource;
- when it is necessary to link a group policy to specific Active Directory units.



The following options for using an alternative installation scheme through Active Directory are available:

- If installation is to be performed directly from the Kaspersky Security Center shared folder, in the Active Directory group policy properties you must specify the .msi file located in the exec subfolder of the installation package folder for the required application.
- If the installation package has to be located on another network resource, you must copy the whole exec folder content to it, because in addition to the file with .msi extension the folder contains configuration files generated when the package was created. To install the key with the application, copy the key file to this folder as well.

## Features of using the management interface

In this section:

How to return to a properties window that disappeared .....	<a href="#">353</a>
How to navigate the console tree .....	<a href="#">354</a>
How to open the object properties window in the workspace .....	<a href="#">354</a>
How to select a group of objects in the workspace.....	<a href="#">354</a>
How to change the set of columns in the workspace.....	<a href="#">355</a>




## How to return to a properties window that disappeared

Sometimes an opened object properties window disappears from the screen. This happens because the properties window is covered by the main application window (this situation is characteristic of the Microsoft Management Console).

- ▶ *To go to the properties window that disappeared,*  
press **ALT+TAB**.

## How to navigate the console tree

To navigate the console tree, you can use the following toolbar buttons:

-  – One step back.
-  – One step forward.
-  – One level up.

You can also use a navigation chain located in the upper-right corner of the workspace. The navigation chain contains the full path to the folder of the console tree in which you are currently located. All elements of the chain, except for the last one, are links to the objects in the console tree.

## How to open the object properties window in the workspace

You can change the properties of the most Administration Console objects in the object properties window.

- ▶ *To open the properties window of an object located in the workspace:*
  - From the context menu of the object, select **Properties**.
  - Select an object and press **ALT+ENTER**.

## How to select a group of objects in the workspace

You can select a group of objects in the workspace. You can select a group of objects, for example, to create a set of devices for which you may create tasks later.

► *To select an objects range:*

1. Select the first object in the range and press **SHIFT**.
2. Hold down the **SHIFT** key and select the last object in the range.

The range will be selected.

► *To group separate objects:*

1. Select the first object in the group and press **CTRL**.
2. Hold down the **CTRL** key and select other objects that you want to include in the group.

The objects will be grouped.

## How to change the set of columns in the workspace

Administration Console allows you to change a set of columns displayed in the workspace.

► *To change a set of columns displayed in the workspace:*

1. In the console tree, click the object for which you wish to change the set of columns.
2. In the Administration Console menu, select **View** → **Add/Remove columns**.
3. In the window that opens, create a set of columns to be displayed.

## Reference information

Tables of this section provide summary information about the context menu of Administration Console objects, as well as about the statuses of console tree objects and workspace objects.

### In this section:

Using an update agent as gateway .....	<a href="#">356</a>
Using masks in string variables.....	<a href="#">357</a>

Context menu commands.....	<a href="#">357</a>
About connections manager .....	<a href="#">361</a>
User's rights to manage Exchange ActiveSync mobile devices .....	<a href="#">362</a>
About the administrator of virtual Server.....	<a href="#">364</a>
List of managed devices Description of columns .....	<a href="#">364</a>
Statuses of devices, tasks, and policies .....	<a href="#">368</a>
File status icons in Administration Console.....	<a href="#">370</a>
Using regular expressions in the search field.....	<a href="#">371</a>

## Using an update agent as gateway

If the Administration Server is outside the demilitarized zone (DMZ), Network Agents from this zone cannot connect to the Server.

When connecting the Administration Server with Network Agents, you can use an update agent as the gateway. The update agent opens a port to Administration Server for the connection to be created. When the Administration Server is started, it connects to that update agent and maintains this connection during the entire session.

Upon receiving a signal from the Administration Server, the update agent sends a UDP signal to the Network Agents in order to allow connection to the Administration Server. When the Network Agents receive that signal, they connect to the update agent, which exchanges information between them and the Administration Server.

# Using masks in string variables

Using masks for string variables is allowed. When creating masks, you can use the following regular expressions:

- Wildcard character (\*)– any string of 0 or more characters.
- Question mark (?) – any single character.
- [<range>]– Any single character from the specified range or array.

For example: [0–9] – any numeral; [abcdef] – any of the characters a, b, c, d, e, f.

## Context menu commands

This section lists Administration Console objects and corresponding context menu items (see table below).

Table 6. Items of the context menu of Administration Console objects

Object	Menu item	Menu item purpose
General items of context menu	Search	Opens the devices search window.
	Refresh	Refreshes the display of the selected object.
	Export list	Exports the current list to a file.
	Properties	Opens the properties window of the selected object.
	View → Add/Remove columns	Adds or removes columns to/from the table of objects in the workspace.
	View → Large icons	Shows objects in the workspace as large icons.
	View → Small icons	Shows objects in the workspace as small icons.

<b>Object</b>	<b>Menu item</b>	<b>Menu item purpose</b>
	<b>View → List</b>	Shows objects in the workspace as a list.
	<b>View → Table</b>	Shows objects in the workspace as a table.
	<b>View → Configure</b>	Configures the display of Administration Console elements.
<b>Kaspersky Security Center</b>	<b>Create → Administration Server</b>	Adds an Administration Server to the console tree.
<b>&lt;Administration Server name&gt;</b>	<b>Connect to Administration Server</b>	Connect to Administration Server.
	<b>Disconnect from Administration Server</b>	Disconnect from Administration Server.
<b>Managed devices</b>	<b>Install application</b>	Runs the Application Remote Installation Wizard.
	<b>View → Configure interface</b>	Configures the display of interface elements.
	<b>Remove</b>	Removes the Administration Server from the console tree.
	<b>Install application</b>	Runs the Remote Installation Wizard for the administration group.
	<b>Reset Virus Counter</b>	Resets the virus counters for devices included in the administration group.
	<b>Virus Activity</b>	Creates a virus activity report for devices included in the administration group.

<b>Object</b>	<b>Menu item</b>	<b>Menu item purpose</b>
	<b>Create → Group</b>	Creates an administration group.
	<b>All Tasks → Create groups structure</b>	Creates a structure of administration groups based on the structure of domains or Active Directory.
	<b>All tasks → Show Message</b>	Runs the New Message for User Wizard intended for the users of devices included in the administration group.
<b>Managed devices → Administration Servers</b>	<b>Create → Slave Administration Server</b>	Runs the Add Slave Administration Server Wizard.
	<b>Create → Virtual Administration Server</b>	Runs the New Virtual Administration Server Wizard.
<b>Device selections</b>	<b>Create → New selection</b>	Creates a device selection.
	<b>All tasks → Import</b>	Imports a selection from a file.
<b>Application management → Application categories</b>	<b>Create → Category</b>	Creates an application category.
<b>Application management → Applications registry</b>	<b>Filter</b>	Sets up a filter for the list of applications.
	<b>Monitored Applications</b>	Configures the publishing of events on installation of applications.
	<b>Remove applications that are not installed</b>	Clears the list of all details of applications that are no longer installed on networked devices.

<b>Object</b>	<b>Menu item</b>	<b>Menu item purpose</b>
<b>Application management → Software updates</b>	<b>Accept License Agreements for updates</b>	Accepts the License Agreements of software updates.
<b>Application management → Kaspersky Lab software licenses</b>	<b>Add Key</b>	Adds a key to the Administration Server repository.
	<b>Activate application</b>	Runs the Application Activation Task Creation Wizard.
	<b>Keys Report</b>	Creates and shows a report on keys on client devices.
<b>Application management → Third-party licenses usage</b>	<b>Create → Licensed applications group</b>	Create a licensed applications group.
<b>Mobile Device Management → Mobile devices</b>	<b>Create → Mobile device</b>	Connect a new mobile device of the user.
<b>Mobile Device Management → Certificates</b>	<b>Create → Certificate</b>	Create a certificate.
	<b>Create → Mobile device</b>	Connect a new mobile device of the user.
<b>Remote installation → Installation packages</b>	<b>Show current application versions</b>	Shows the list of up-to-date versions of Kaspersky Lab applications available on web servers.
	<b>Create → Installation package</b>	Create an installation package.
	<b>All Tasks → Update databases</b>	Updates application databases in installation packages.



Object	Menu item	Menu item purpose
	<b>All Tasks → Show the general list of stand-alone packages</b>	Shows the list of stand-alone packages created for installation packages.
<b>Network poll → Domains</b>	<b>All Tasks → Device Activity</b>	Sets up the Administration Server's response to inactivity of networked devices.
<b>Network poll → IP subnets</b>	<b>Create → IP subnet</b>	Create an IP subnet.
<b>Repositories → Kaspersky Lab software updates and patches</b>	<b>Download updates</b>	Runs the download updates to the repository task of the Administration Server.
	<b>Updates download settings</b>	Configures the download updates to the repository task of the Administration Server.
	<b>Anti-Virus Database Versions Report</b>	Creates and shows a report on versions of databases.
	<b>All Tasks → Clear updates repository</b>	Clears the repository of updates on the Administration Server.
<b>Repositories → Hardware</b>	<b>Create → Device</b>	Creates a new device.

## About connections manager

In the Network Agent properties window, in the **Network** section, in the **Connection Manager** subsection, you can specify time intervals during which Network Agent will transmit data to the Administration Server.

**Connect when necessary** If this option is selected, the connection is established when Network Agent has to send data to the Administration Server.

**Connect at specified time periods** If this option is selected, Network Agent connects to the Administration Server at a specified time. You can add several connection time periods.

## User's rights to manage Exchange ActiveSync mobile devices

To manage mobile devices running under the Exchange ActiveSync protocol with Microsoft Exchange Server 2010 or Microsoft Exchange Server 2013, make sure that the user is included in a role group for which the following commandlets are allowed to execute:

- Get-CASMailbox.
- Set-CASMailbox.
- Remove-ActiveSyncDevice.
- Clear-ActiveSyncDevice.
- Get-ActiveSyncDeviceStatistics.
- Get-AcceptedDomain.
- Set-AdServerSettings.
- Get-ActiveSyncMailboxPolicy.
- New-ActiveSyncMailboxPolicy.
- Set-ActiveSyncMailboxPolicy.
- Remove-ActiveSyncMailboxPolicy.

To manage mobile devices running under the Exchange ActiveSync protocol with Microsoft Exchange Server 2007, make sure that the user has been granted the administrator rights. If the rights have not been granted, execute the commandlets to assign the administrator rights to the user (see the table below).

Table 7. Administrator rights required for managing Exchange ActiveSync mobile devices on Microsoft Exchange Server 2007

Access	Object	Cmdlet
Full	Branch "CN=Mobile Mailbox Policies,CN=Your Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=yourdomain"	Add-ADPermission -User <User or group name> -Identity "CN=Mobile Mailbox Policies,CN=<Organization name>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Domain name>" -InheritanceType All -AccessRight GenericAll
Read	Branch "CN= Your Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=yourdomain"	Add-ADPermission -User <User or group name> -Identity "CN=<Organization name>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Domain name>" -InheritanceType All -AccessRight GenericRead
Read/write	Properties msExchMobileMailboxPolicy Link and msExchOmaAdminWireless Enable for objects in Active Directory	Add-ADPermission -User <User or group name> -Identity "DC=<Domain name>" -InheritanceType All -AccessRight ReadProperty,WriteProperty -Properties msExchMobileMailboxPolicyLink, msExchOmaAdminWirelessEnable
Full	Mailbox repositories for ms-Exch-Store-Admin	Get-MailboxDatabase   Add-ADPermission -User <user or group name> -ExtendedRights ms-Exch-Store-Admin

For detailed information about how to use commandlets in the Exchange Management Shell console, please refer to the website of Microsoft Exchange Server Technical Support [http://technet.microsoft.com/en-us/library/bb123778\(v=exchg.150\).aspx](http://technet.microsoft.com/en-us/library/bb123778(v=exchg.150).aspx).

## About the administrator of virtual Server

The administrator of an enterprise network managed through a virtual Administration Server starts Kaspersky Security Center 10 Web Console to view the anti-virus protection details under the user account specified in this window.

If necessary, several administrator accounts can be created on a virtual Server.

The administrator of a virtual Administration Server is an internal user of Kaspersky Security Center. No data on internal users is transferred to the operating system. Kaspersky Security Center authenticates internal users.

## List of managed devices Description of columns

The following table displays the names and respective descriptions of columns of the list of managed devices.

Table 8. Descriptions of columns of the list of managed devices

Column name	Value
Name	NetBIOS name of the client device. The descriptions of device name icons are given in the Appendix (see section "Statuses of devices, tasks, and policies" on page <a href="#">368</a> ).
Operating system type	Type of the operating system installed on the client device.
Windows domain	Name of the Windows domain in which the client device is located.
Agent installed	Result of Network Agent installation on the client device.
Agent running	The result of Network Agent's operation.
Real-time protection	Security application is installed (Yes, No).

Column name	Value
Connecting to Server	Time period that has elapsed since the client device had been connected to the Administration Server.
Last update	The time period that has elapsed since the last update of Kaspersky Security Center Administration Server.
Status	Current status of the client device ( <i>OK</i> , <i>Critical</i> , or <i>Warning</i> ).
Status description	<p>Reasons for the change of the client device status to <i>Critical</i> or <i>Warning</i>.</p> <p>The device status changes to <i>Warning</i> or <i>Critical</i> by the following reasons:</p> <ul style="list-style-type: none"> <li>• No security application is installed.</li> <li>• Too many viruses have been detected.</li> <li>• The real-time protection level differs from the one set by the administrator.</li> <li>• A virus scan has not been performed for a long time.</li> <li>• The databases are obsolete.</li> <li>• The client computer has not been connected for a long time.</li> <li>• There are unprocessed objects.</li> <li>• Restart required.</li> <li>• Incompatible applications are installed.</li> <li>• Software vulnerabilities have been detected.</li> <li>• Windows Updates has not been searched for a long time.</li> <li>• A certain state of data encryption.</li> <li>• The settings of the mobile device do not comply with the policy.</li> <li>• There are unprocessed incidents.</li> <li>• The license expires soon.</li> </ul>

Column name	Value
	<p>The device status only changes to <i>Critical</i> by the following reasons:</p> <ul style="list-style-type: none"> <li>• The license has expired.</li> <li>• Connection with the client device has been lost.</li> <li>• Protection is disabled.</li> <li>• The security application is not running.</li> </ul> <p>Managed Kaspersky Lab applications on client devices can add status descriptions to the list. Kaspersky Security Center can receive the description of a client device status from managed Kaspersky Lab applications installed on that device. If the status that has been assigned to the device by managed application is other than that assigned by Kaspersky Security Center, Administration Console shows the status, which is the most critical to the device security. For example, if a managed application has assigned the <i>Critical</i> status to the device while Kaspersky Security Center has assigned it the <i>Warning</i> status, Administration Console shows the <i>Critical</i> status for that device with the corresponding description provided by the managed application.</p>
Info update	Time period that has elapsed since the client device had been last successfully synchronized with the Administration Server.
DNS domain name	DNS domain name of the client device.
DNS domain	The main DNS suffix.
IP address	IP address of the client device. It is recommended to use the IPv4 address.
Last visible time	Time period during which the client device has remained visible on the network.





Column name	Value
On-demand scan	Date and time of the last scan of the client device performed by the security application upon the user's request.
Viruses found	The number of viruses found.
Real-time protection status	Real-time protection status ( <i>Starting, Running, Running (maximum protection), Running (maximum speed), Running (recommended), Running (user-defined settings), Stopped, Paused, Failure</i> ).
Connection IP address	The IP address that is used for connection to Kaspersky Security Center Administration Server.
Network Agent version	Version of the Network Agent.
Protection version	Version of the security application installed on the client device.
Databases version	The version of the anti-virus databases.
Turn-on time	Date and time when the client device was last turned on.
Restart	A restart of the client device is required.
Update agent	Name of the device that acts as the update agent for this client device.
Description	Description of the client device received after a network scan.
Encryption status	Data encryption status of the client device.
WUA status	Status of Windows Update Agent on the client device. "Yes" corresponds to client devices that retrieve updates through Windows Update from the Administration Server. "No" corresponds to client devices that retrieve updates through Windows Update from other sources.

Column name	Value
Operating system bit size	Bit size of the operating system installed on the client device.
Spam protection status	Spam protection status ( <i>Running, Starting, Stopped, Paused, Failure, Unknown</i> )
Data Leakage Prevention status	Status of Data Leakage Prevention ( <i>Running, Starting, Stopped, Paused, Failure, Unknown</i> )
Protection status for SharePoint Servers	Status of Content Filtering ( <i>Running, Starting, Stopped, Paused, Failure, Unknown</i> )
Anti-virus protection status of mail servers	Anti-virus protection status of mail servers ( <i>Running, Starting, Stopped, Paused, Failure, Unknown</i> )

## Statuses of devices, tasks, and policies








The table below contains a list of icons displayed in the console tree and in the Administration Console workspace, next to the names of devices, tasks, and policies. Those icons define the statuses of objects.

Table 9. Statuses of devices, tasks, and policies

Icon	Status
	Device with an operating system for workstations detected in the system but not yet included in any of the administration groups.
	Device with an operating system for workstations included in an administration group, with the <i>OK</i> status.
	Device with an operating system for workstations included in an administration group, with the <i>Warning</i> status.
	Device with an operating system for workstations included in an administration group, with the <i>Critical</i> status.






Icon	Status
	Device with an operating system for workstations included in an administration group, which has lost connection with the Administration Server.
	Device with an operating system for servers detected in the system but not yet included in any of the administration groups.
	Device with an operating system for servers included in an administration group, with the <i>OK</i> status.
	Device with an operating system for servers included in an administration group, with the <i>Warning</i> status.
	Device with an operating system for servers included in an administration group, with the <i>Critical</i> status.
	Device with an operating system for servers included in an administration group, which has lost connection with the Administration Server.
	Mobile device detected in the network and included in none of the administration groups.
	Mobile device included in an administration group, with the <i>OK</i> status.
	Mobile device included in an administration group, with the <i>Warning</i> status.
	Mobile device included in an administration group, with the <i>Critical</i> status.
	Mobile device included in an administration group, having lost its connection with the Administration Server.
	Active policy.
	Inactive policy.







Icon	Status
	Active policy inherited from a group that was created on the master Administration Server.
	Active policy inherited from a top-level group.
	Task (group task, Administration Server task, or task for specific devices) with the <i>Scheduled</i> or <i>Completed</i> status.
	Task (group task, Administration Server task, or task for specific devices) with the <i>Running</i> status.
	Task (group task, Administration Server task, or task for specific devices) with the <i>Completed with error</i> status.
	Task inherited from a group that was created on the master Administration Server.
	Task inherited from a top-level group.

## File status icons in Administration Console

For ease of file management in Kaspersky Security Center Administration Console, icons are displayed next to the names of files. Icons indicate statuses assigned to files by managed Kaspersky Lab applications on client devices. Icons are shown in the workspaces of the **Quarantine**, **Backup**, and **Unprocessed files** folders.

Table 10. Correspondence between icons and file statuses

Icon	Status
	File with the <i>Infected</i> status.
	File with the <i>Warning</i> or <i>Probably infected</i> status.
	File with the <i>Placed to folder by user</i> status.

Icon	Status
	File with the <i>False positive</i> status.
	File with the <i>Disinfected</i> status.
	File with the <i>Deleted</i> status.
	File in the <b>Quarantine</b> folder with the <i>Not infected, Password-protected</i> or <i>Requires to be sent to Kaspersky Lab</i> status. If there is no status description next to an icon, this means that the managed Kaspersky Lab application on the client device has reported an unknown status to Kaspersky Security Center.
	File in the <b>Backup</b> folder with the <i>Not infected, Password-protected</i> or <i>Requires to be sent to Kaspersky Lab</i> status. If there is no status description next to an icon, this means that the managed Kaspersky Lab application on the client device has reported an unknown status to Kaspersky Security Center.
	File in the <b>Unprocessed files</b> folder with the <i>Not infected, Password-protected, or Requires to be sent to Kaspersky Lab</i> status. If there is no status description next to an icon, this means that the managed Kaspersky Lab application on the client device has reported an unknown status to Kaspersky Security Center.

## Using regular expressions in the search field

You can use the following regular expressions in the search field to search for specific words and characters:

- \*. Replaces any sequence of characters. To search for such words as Server, Servers, or Server room, enter the `Server*` expression in the search field.
- ?. Replaces any single character. To search for such words as Word or Ward, enter the `W?rd` expression in the search field.

Text in the search field cannot begin with the ? symbol.

- [`<range>`]. Replaces any single character from a specified range or set. To search for any numeral, enter the [`0-9`] expression in the search field. To search for one of the characters – a, b, c, d, e, or f – enter the [`abcdef`] expression in the search field.

Use the following regular expressions in the search field to run a full-text search:

- Space. You will see all computers whose descriptions contain any of the listed words. To search for a phrase that contains such word as Slave or Virtual (or both these words), enter the `Slave Virtual` expression in the search field.
- Plus sign (+), AND or &&. When a plus sign precedes a word, all search results will contain this word. To find a phrase that contains both Slave and Virtual, you can enter `+Slave+Virtual`, `Slave AND Virtual`, `Slave && Virtual` as the query in the search field.
- OR or ||. When placed between two words, it indicates that one word or the other can be found in the text. To search for a phrase that contains such word as Slave or Virtual, you can enter any of the following expressions in the search field: `Slave OR Virtual`, `Slave || Virtual`.
- Minus sign (-). When a minus sign precedes a word, no search results will contain this word. To search for a phrase that must contain such word as Slave and must not contain such word as Virtual, you must enter the `+Slave-Virtual` expression in the search field.
- "`<some text>`". Text enclosed in quotation marks must be present in the text. To search for a phrase that contains such word combination as Slave Server, you must enter the `Slave Server` expression in the search field.

Full-text search is available in the following filtering blocks:

- In the event list filtering block, by the **Event** and **Description** columns.
- In the user account filtering block, by the **Name** column.
- In the applications registry filtering block, by the **Name** column if the **Group applications by name** check box is cleared.

---

# Glossary

## A

### **Active key**

Key that is used at the moment to work with the application.

### **Additional key**

A key that certifies the right to use the application but is not currently being used.

### **Administration Console**

A Kaspersky Security Center component that provides a user interface for the administrative services of Administration Server and Network Agent.

### **Administration group**

A set of devices grouped by function and by installed Kaspersky Lab applications. Devices are grouped as a single entity for the convenience of management. A group can include groups. A group can contain group policies and group tasks for each installed application.

### **Administration Server client (Client device)**

A device, server, or workstation on which Network Agent is installed and managed Kaspersky Lab applications are running.

### **Administrator rights**

The level of the user's rights and privileges required for administration of Exchange objects within an Exchange organization.

## **Anti-virus databases**

Databases that contain information about computer security threats that are known to Kaspersky Lab at the time of release of the anti-virus databases. Records that are contained in anti-virus databases allow detecting malicious code in scanned objects. The anti-virus databases are created by Kaspersky Lab experts and updated every hour.

## **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.

## **Authentication Agent**

An interface for passing the authentication process to access encrypted hard drives and load the operating system after the system hard drive has been encrypted.

## **Available update**

A package of updates for the modules of a Kaspersky Lab application including a set of urgent patches released during a certain time interval, and modifications to the application architecture.

## **B**

### **Broadcast domain**

A logical area of a computer network in which all nodes can exchange data using a broadcasting channel at the level of OSI (Open Systems Interconnection Basic Reference Model).

## C

### **Configuration profile**

Policy that contains a collection of settings and restrictions for an iOS MDM mobile device.

## D

### **Demilitarized zone (DMZ)**

Demilitarized zone is a segment of a local network that contains servers, which respond to requests from the global Web. In order to ensure the security of an organization's local network, access to the LAN from the demilitarized zone is protected with a firewall.

### **Device owner**

Device owner is a user whom the administrator can contact when the need arises to perform certain operations on a device.

## E

### **EAS device**

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

## G

### Group task

A task defined for an administration group and performed on all client devices included in that administration group.

## H

### Home Administration Server

Home Administration Server is the Administration Server that was specified during Network Agent installation. The home Administration Server can be used in settings of Network Agent connection profiles.

## I

### Installation package

A set of files created for remote installation of a Kaspersky Lab application by using the Kaspersky Security Center remote administration system. The installation package contains a range of settings needed to install the application and get it running immediately after installation. Settings correspond to application defaults. The installation package is created using files with the .kpd and .kud extensions included in the application distribution kit.

### Internal users

The accounts of internal users are used to work with virtual Administration Servers. Under the account of an internal user, the administrator of a virtual Administration Server can start



Kaspersky Security Center 10 Web Console to check the anti-virus security status of the network. Kaspersky Security Center grants the rights of real users to internal users of the application.

The accounts of internal users are created and used only within Kaspersky Security Center. No data on internal users is transferred to the operating system. Kaspersky Security Center authenticates internal users.

## **iOS MDM device**

A mobile device that is connected to the iOS MDM Server by using the iOS MDM protocol. Devices running the iOS operating system can be connected and managed by means of the iOS MDM protocol.

## **iOS MDM profile**

Collection of settings for connecting iOS mobile devices to Administration Server. The user installs an iOS MDM profile to a mobile device, after which this mobile device connects to Administration Server.

## **iOS MDM Server**

A component of Kaspersky Security Center that is installed on a client device, allowing connection of iOS mobile devices to the Administration Server and management of iOS mobile devices through Apple Push Notifications (APNs).

# **K**

## **Kaspersky Security Center administrator**

The person managing the application operations through the Kaspersky Security Center system of remote centralized administration.

## **Kaspersky Security Center Web Server**

A component of Kaspersky Security Center installed together with Administration Server. Web Server is designed for transfer of stand-alone installation packages, iOS MDM profiles, and files from a shared folder over the network.

## **Kaspersky Security Network (KSN)**

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

## **KES device**

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

## **L**

### **Licensed applications group**

A group of applications created on the basis of criteria set by the administrator (for example, by vendor), for which statistics of installations on client devices are maintained.

### **Local task**

A task defined and running on a single client device.

## M

### **MDM policy**

A collection of application settings used for managing mobile devices through Kaspersky Security Center. Different application settings are used to manage different types of mobile devices. A policy includes the settings for complete configuration of all application features.

### **Microsoft Exchange Mobile Devices Server**

A component of Kaspersky Security Center that allows you to connect Exchange ActiveSync mobile devices to the Administration Server. Installed on a client device.

### **Mobile device server**

A component of Kaspersky Security Center that provides access to mobile devices and allows managing them through Administration Console.

## N

### **Network Agent**

A Kaspersky Security Center component that enables interaction between the Administration Server and Kaspersky Lab applications that are installed on a specific network node (workstation or server). This component is common for all of the company's products for Windows.

Separate versions of Network Agent exist for Kaspersky Lab products developed for Novell®, Unix™ and Mac.

## Network Location Awareness subnet

Network Location Awareness (NLA) subnet is a subnet that spans a set of devices specified manually. Within the Kaspersky Security Center functionality, an NLA subnet can be used for manual creation of a set of devices to which an update agent will distribute updates.

## P

### Patch importance level

Attribute of the patch. There are five importance levels for Microsoft patches and third-party patches:

- Critical.
- High.
- Medium.
- Low.
- Unknown.

The importance level of a third-party patch or Microsoft patch is determined by the least favorable severity level among the vulnerabilities that the patches should fix.

### Policy

A policy determines the settings of an application and manages the access to configuration of an application installed on computers within an administration group. An individual policy must be created for each application. You can create an unlimited number of various policies for applications installed on computers in each administration group, but only one policy can be applied to each application at a time within an administration group.

## Profile

Collection of settings of Exchange ActiveSync mobile devices that define their behavior when connected to a Microsoft Exchange server.

## Provisioning profile

Collection of settings for applications' operation on iOS mobile devices. A provisioning profile contains information about the license; it is linked to a specific application.

## R

## Restoration

Relocation of the original object from Quarantine or Backup to its original folder where the object had been stored before it was quarantined, disinfected or deleted, or to a user-defined folder.

## Restoration of Administration Server data

Restoration of Administration Server data from the information saved in Backup by using the backup utility. The utility can restore:

- Information database of the Administration Server (policies, tasks, application settings, events saved on the Administration Server).
- Configuration details of the administration group structure and client devices.
- Repository of the installation files for remote installation of applications (content of the folders: Packages, Uninstall Updates).
- Administration Server certificate.

## Role group

A group of users of Exchange ActiveSync mobile devices who are granted identical administrator rights (see section "Administrator rights" on page 405).

## S

### Shared certificate

A certificate intended for identifying the user's mobile device.

## T

### Task

Functions performed by Kaspersky Lab application are implemented as tasks, such as Real-time file protection, Full device scan, and Database update.

### Task for specific devices

A task assigned to a set of client devices from arbitrary administration groups and performed on those devices.

## U

### Update agent

Device with Network Agent installed, which is used for update distribution, remote installation of applications, collection of information about devices in an administration group and/or broadcasting domain. Update agents are designed to reduce the load on the Administration Server during update distribution and to optimize network traffic. Update agents can be assigned automatically, by the Administration Server, or manually, by the administrator.

## V

### Virtual Administration Server

A component of Kaspersky Security Center, designed for management of the protection system of a client organization's network.

Virtual Administration Server is a particular case of a slave Administration Server and has the following restrictions as compared with physical Administration Server:

- Virtual Administration Server can be created only on master Administration Server.
- Virtual Administration Server uses the master Administration Server database. Thus, the following tasks are not supported on virtual Server: backup copying, restoration, updates verification and updates downloading. These tasks exist only on master Administration Server.
- Virtual Server does not support creation of slave Administration Servers (including virtual Servers).

### Virus outbreak

Series of deliberate attempts to infect a device with a virus.

### Vulnerability

A flaw in an operating system or an application that may be exploited by malware makers to penetrate into the operating system or the application and corrupt its integrity. A large number of vulnerabilities in an operating system makes it unreliable, because viruses that have penetrated into the operating system may cause operation failures in the operating system itself and in installed applications.

## W

### Windows Server Update Services (WSUS)

An application used for distribution of updates for Microsoft applications on users' computers in an organization's network.

---

# 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 38 offices in 33 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 a file named `legal_notices.txt` and stored in the application installation folder.

---

# Enhanced protection with Kaspersky Security Network

Kaspersky Lab offers an extra layer of protection to users through the Kaspersky Security Network. This protection method is designed to combat advanced persistent threats and zero-day attacks. Integrated cloud technologies and the expertise of Kaspersky Lab virus analysts make Kaspersky Endpoint Security the unsurpassed choice for protection against the most sophisticated network threats.

Details on enhanced protection in Kaspersky Endpoint Security are available on the Kaspersky Lab website.

---

# Trademark notices

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

Active Directory, ActiveSync, Excel, Internet Explorer, Hyper-V, Microsoft, MultiPoint, SQL Server, Tahoma, Windows, Windows Server, Windows Phone, and Windows Vista are trademarks of Microsoft Corporation registered in the United States and elsewhere.

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

AirPlay, AirDrop, AirPrint, App Store, Apple, FaceTime, FileVault, iBook, iBooks, iPad, iPhone, iTunes, Leopard, Mac, Mac OS, OS X, Safari, Snow Leopard, and Tiger are trademarks of Apple Inc. registered in the United States and elsewhere.

AMD and AMD64 are trademarks of Advanced Micro Devices, Inc.

Apache and the Apache feather logo are trademarks owned by the Apache Software Foundation.

BlackBerry is owned by Research In Motion Limited and is registered in the United States and may be pending or registered elsewhere.

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

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

Citrix and XenServer are trademarks of Citrix Systems, Inc. and / or its subsidiaries registered in the United States Patent Office and elsewhere.

Debian is a registered trademark of Software in the Public Interest, Inc.

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

Firefox is a registered trademark of the Mozilla Foundation.

FreeBSD is a registered trademark of FreeBSD foundation.

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

QRadar is a trademark of International Business Machines Corporation, registered in many jurisdictions worldwide.

CentOS, Fedora and Red Hat Enterprise Linux are trademarks of Red Hat Inc. registered in the United States and elsewhere.

Linux is a trademark owned by Linus Torvalds and registered in the U.S. and elsewhere.

Novell is a trademark owned by Novell, Inc. and registered in the United States and elsewhere.

Symbian is a trademark owned by the Symbian Foundation Ltd.

SPL, Splunk are trademarks of Splunk, Inc. registered in the United States and elsewhere.

SUSE is a trademark of SUSE LLC registered in the United States and elsewhere.

UNIX is a trademark registered in the U.S. and elsewhere and is used under license from X/Open Company Limited.

VMware, VMware vSphere are trademarks of VMware, Inc., or trademarks owned by VMware, Inc. and registered in the U.S. and elsewhere.

---

# Index

## A

Active Directory .....	350
Addition	
Administration Server .....	89
client computer .....	141
Administration groups .....	68
Administration Server .....	68
Administration Server certificate .....	88
Anti-virus protection .....	332
Application licensing .....	58, 60
Application management .....	103
Arrays .....	333

## B

Backup	
task .....	343
utility .....	344
Batch policies and tasks conversion wizard .....	110, 123

## C

Certificate	
-------------	--

installing a certificate for a user .....	164, 239
mail.....	164, 239
shared .....	164, 239
VPN.....	164, 239
Client computers.....	73
connecting to the Server .....	131
message to the user .....	144
Clusters.....	333
Console tree.....	45
Context menu .....	55, 356

## D

Deleting	
Administration Server .....	90
policy .....	108

## E

Encryption .....	277
Event selections	
creating.....	175
settings .....	174
viewing the log .....	174
Exchange ActiveSync mobile device.....	248

exec .....350

## G

### Group tasks

filtering .....126

inheriting .....120

### Groups

structure.....100

## I

Image.....221

### Importing

policy .....109

task.....123

### Installation

Active Directory .....350

iOS MDM mobile device.....252

### IP subnet

creating.....186

editing.....184, 186

## K

Key .....302

distribution .....305



installation.....	303
removing.....	304
report.....	306

## L

License .....	59
End User License Agreement .....	58
key file .....	65
Licensed applications group .....	198
Limiting traffic .....	94

## M

Management	
client computer.....	143
initial configuration.....	67
keys.....	302
policies .....	103
Microsoft Exchange Mobile Devices Server .....	248
Mobile users	
profile.....	327
switching rules.....	328

## N

Network poll .....	182
--------------------	-----

Active Directory groups.....	184
Windows network .....	183
Notifications.....	171

## P

### Policies

activation .....	106
copying .....	108
exporting.....	109
importing.....	109
mobile users.....	325
removing.....	108
Policy .....	75
creating.....	105
Policy profile.....	110
Policy profile	
creating .....	113
removing .....	115

### Poll

IP subnets.....	184
-----------------	-----

## R

### Report template

creating.....	167
---------------	-----

Reports	
delivery .....	169
generating.....	168
keys.....	306
viewing .....	168

Repositories	
applications registry .....	197
installation packages .....	308
keys.....	302

## S

Statistics.....	169
-----------------	-----

## T

Task.....	75
key adding .....	303

### Tasks

backup copying .....	343
changing Administration Server.....	142
delivery of reports.....	169
exporting.....	122
group tasks .....	117
importing.....	123

local .....	120
managing client computers .....	143
running .....	125
viewing the results.....	126

## U

### Update

distribution .....	294, 295, 297
downloading.....	287
scanning .....	290
viewing .....	293

Update agents .....	297
---------------------	-----

Updating the application.....	205
-------------------------------	-----

### User role

adding.....	242
-------------	-----

User roles.....	160
-----------------	-----

#### User role

adding .....	160
assigning .....	161

## V

Virtual Administration Server .....	70
-------------------------------------	----

Vulnerability.....	202
--------------------	-----