# Kaspersky Security Center 10

## Getting started

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: 12/20/2016

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

# Table of Contents

# About this document

This Getting Started Guide is aimed at experts who are involved in installation and administration of Kaspersky Security Center, as well as experts who are in charge of technical support of organizations that use Kaspersky Security Center.

You can use this guide to quickly start using the application, become acquainted with the interface, and perform basic operations.

## In this section:

# In this document

*Getting Started with Kaspersky Security Center* contains an introduction, sections that describe typical tasks that Kaspersky Security Center performs, and a conclusion.

**Sources of information about the application (see page 10)**

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 13)**

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

**Application licensing (see page 15)**

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

**Application interface (see page 25)**

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

**Starting the application (see page 40)**

This section describes the startup of Kaspersky Security Center.

**Deploying the protection system (see page 41)**

This section describes the possible scenarios for deployment of a protection system in an organization's network.

**Performing common tasks (see page 44)**

This section describes the basic operations that you can perform using Kaspersky Security Center.

**Switching from Kaspersky Security Center 9.0 to Kaspersky Security Center 10**

This section describes the procedure for switching from Kaspersky Security Center 9.0 to Kaspersky Security Center 10, as well as the main actions for initial setup of the new version of the application.

**Conclusion (see page 92)**

This section summarizes the information in this document.

**Contacting the Technical Support Service (see page 93)**

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

**AO Kaspersky Lab (see page 96)**

This section provides information about Kaspersky Lab.

**Information about third-party code (see page 98)**

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 100)**

This section contains registered trademark notices.

# 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. |
| **Example:**<br>… | Examples are on a blue background under the heading "Example". |
| *Update* means...<br>The *Databases are out of date* event occurs. | The following elements are italicized in the text:<br>• New terms<br>• Names of application statuses and events |

| Sample text | Document conventions description |
|---|---|
| Press **ENTER**.<br>Press **ALT**+**F4**. | Names of keyboard keys appear in bold and are all uppercase.<br>Names of keys that are connected by a plus sign (+) sign indicate the use of a key combination. These keys must be pressed simultaneously. |
| Click the **Enable** button. | Names of application interface elements, such as entry fields, menu items, and buttons, appear in bold. |
| ► *To configure task schedule:* | Introductory phrases of procedures are italicized and accompanied by the arrow sign. |
| Enter `help` in the command line<br>The following message then appears:<br>`Specify the date in MM:DD:YY format.` | The following types of text content are set off with a special font:<br>• Text in the command line<br>• Text of messages displayed on the screen by the application<br>• Data that the user has to enter from the keyboard |
| <User name> | Variables are enclosed in angle brackets. Instead of a variable, the corresponding value must be inserted, with angle brackets omitted. |

# 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

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 93).

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.

# Application licensing

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

## In this section:

# 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 21).

**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 93).

# 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 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.

# 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.

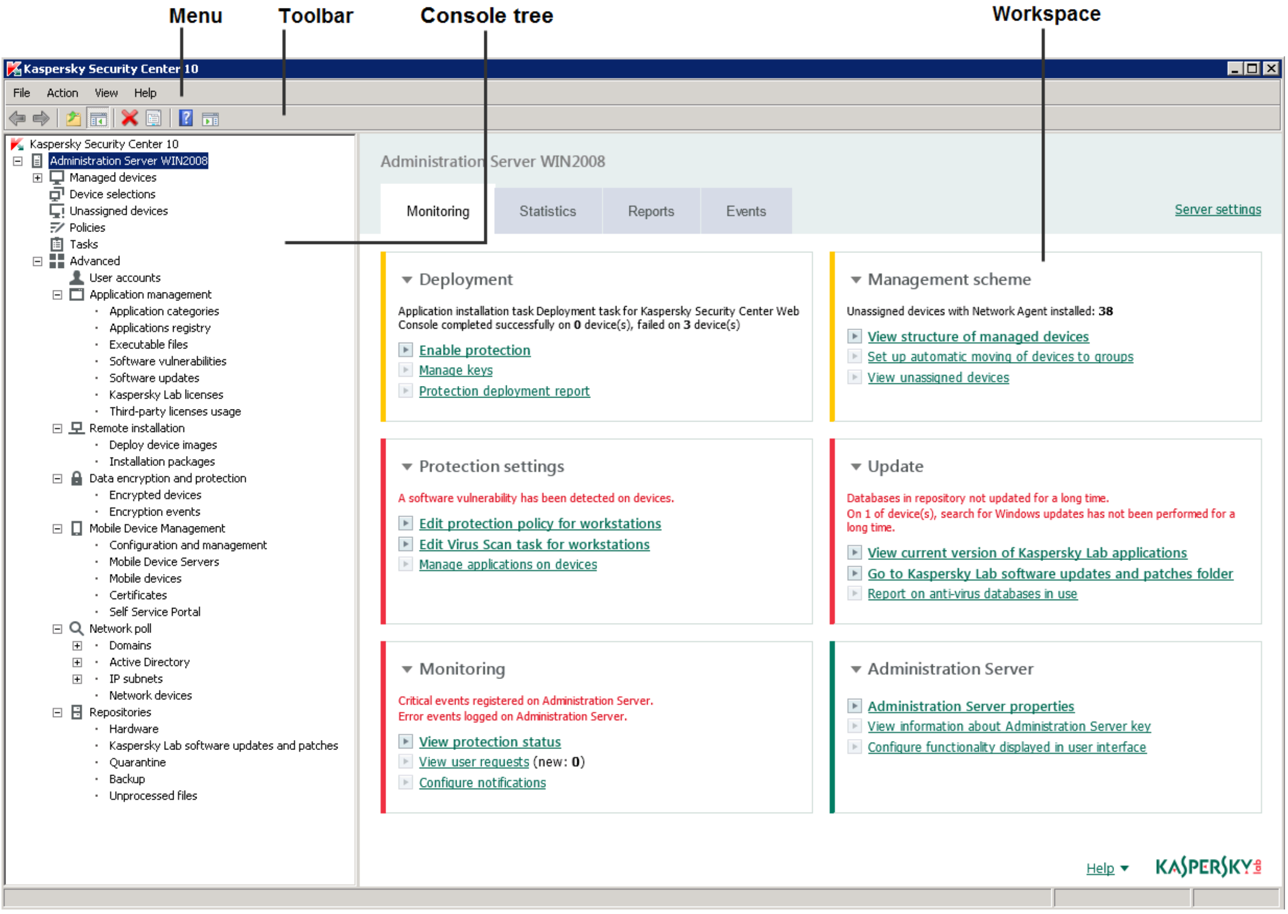
## In this section:

# Main application window

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.



Deployment

Application installation task Deployment task for Kaspersky Security Center Web Console completed successfully on **0** device(s), failed on **3** device(s)

- Enable protection
- Manage keys
- Protection deployment report

Management scheme

Unassigned devices with Network Agent installed: **38**

- View structure of managed devices
- Set up automatic moving of devices to groups
- View unassigned devices

Protection settings

A software vulnerability has been detected on devices.

- Edit protection policy for workstations
- Edit Virus Scan task for workstations
- Manage applications on devices

Update

Databases in repository not updated for a long time.
On 1 of device(s), search for Windows updates has not been performed for a long time.

- View current version of Kaspersky Lab applications
- Go to Kaspersky Lab software updates and patches folder
- Report on anti-virus databases in use

Monitoring

Critical events registered on Administration Server.
Error events logged on Administration Server.

- View protection status
- View user requests (new: **0**)
- Configure notifications

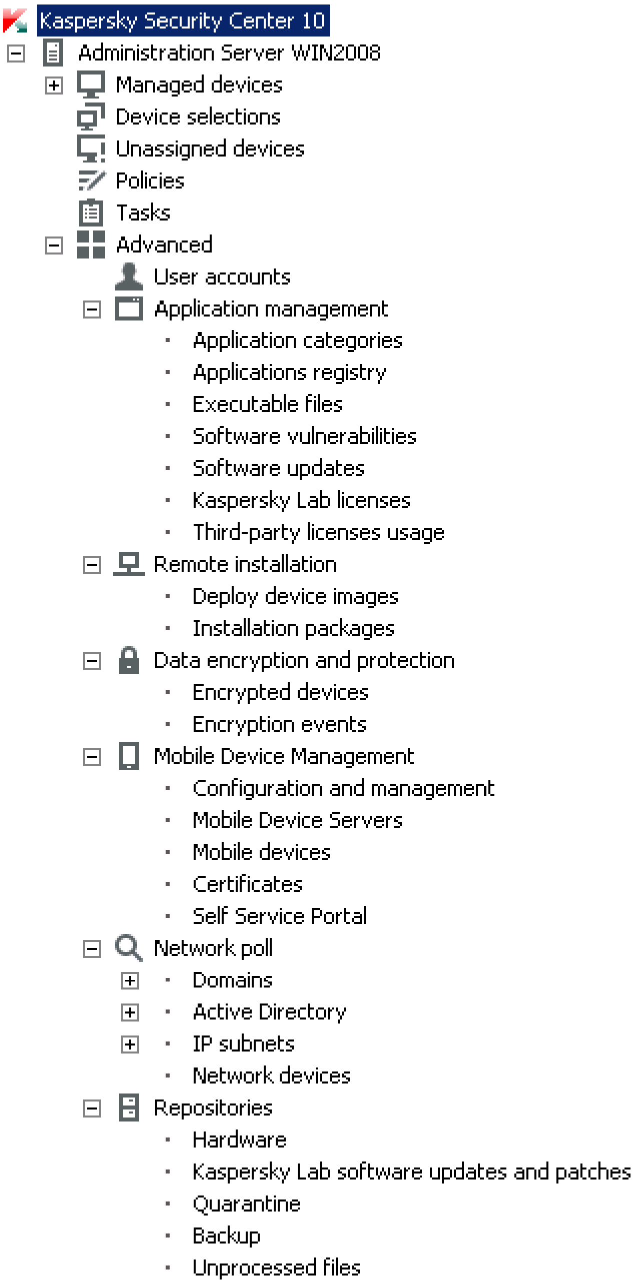
Administration Server

- Administration Server properties
- View information about Administration Server key
- Configure functionality displayed in user interface

*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.



- Kaspersky Security Center 10
  - Administration Server WIN2008
    - Managed devices
    - Device selections
    - Unassigned devices
    - Policies
    - Tasks
    - Advanced
      - User accounts
      - Application management
        - Application categories
        - Applications registry
        - Executable files
        - Software vulnerabilities
        - Software updates
        - Kaspersky Lab licenses
        - Third-party licenses usage
      - Remote installation
        - Deploy device images
        - Installation packages
      - Data encryption and protection
        - Encrypted devices
        - Encryption events
      - Mobile Device Management
        - Configuration and management
        - Mobile Device Servers
        - Mobile devices
        - Certificates
        - Self Service Portal
      - Network poll
        - Domains
        - Active Directory
        - IP subnets
        - Network devices
      - Repositories
        - Hardware
        - Kaspersky Lab software updates and patches
        - Quarantine
        - Backup
        - Unprocessed files

*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:*

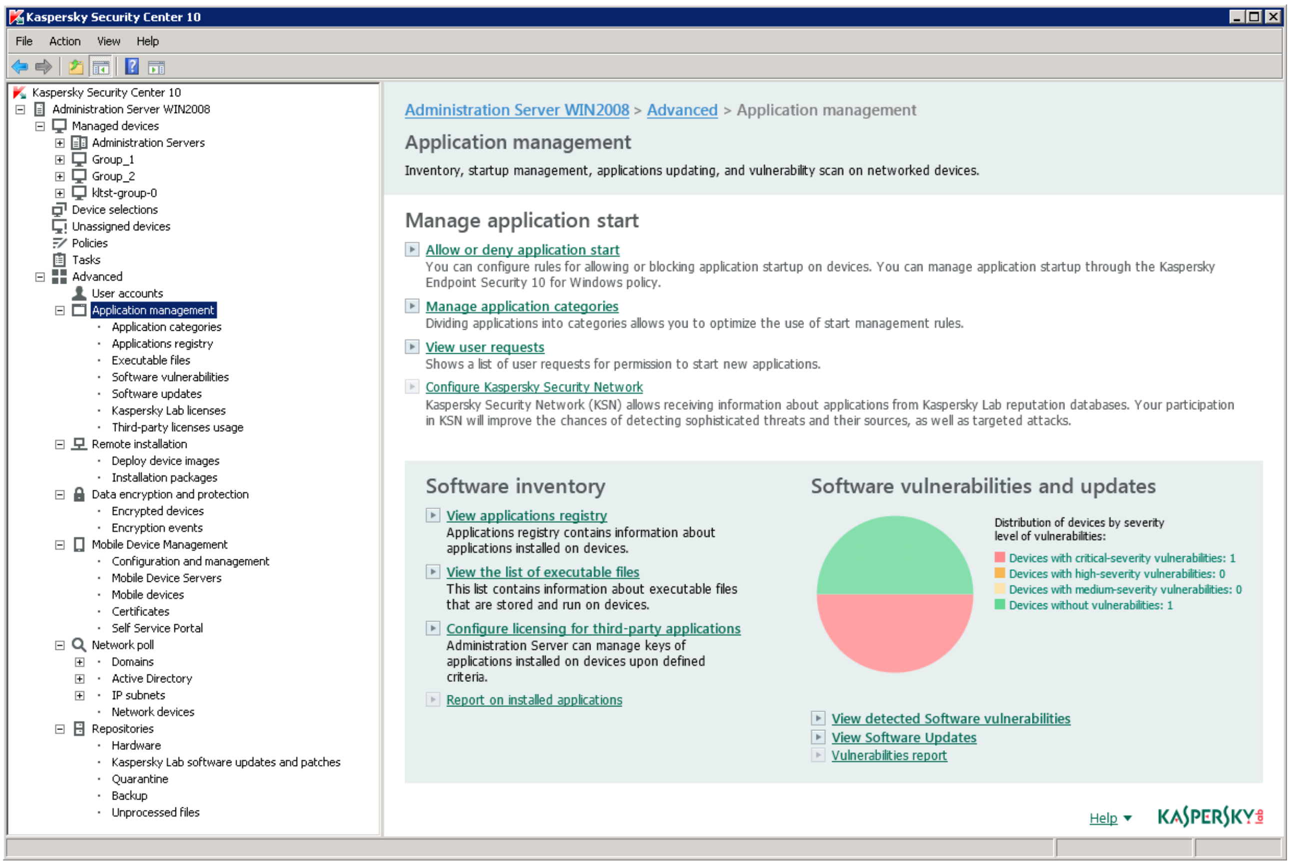
1. In the console tree, select the subfolder that you need to move to the **Advanced** folder.
2. In the context menu of the subfolder, select **View** → **Move to Advanced folder**.

# 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 33)
- 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 35).

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



Application management

Inventory, startup management, applications updating, and vulnerability scan on networked devices.

Manage application start

▸ Allow or deny application start
You can configure rules for allowing or blocking application startup on devices. You can manage application startup through the Kaspersky Endpoint Security 10 for Windows policy.

▸ Manage application categories
Dividing applications into categories allows you to optimize the use of start management rules.

▸ View user requests
Shows a list of user requests for permission to start new applications.

▸ Configure Kaspersky Security Network
Kaspersky Security Network (KSN) allows receiving information about applications from Kaspersky Lab reputation databases. Your participation in KSN will improve the chances of detecting sophisticated threats and their sources, as well as targeted attacks.

Software inventory

▸ View applications registry
Applications registry contains information about applications installed on devices.

▸ View the list of executable files
This list contains information about executable files that are stored and run on devices.

▸ Configure licensing for third-party applications
Administration Server can manage keys of applications installed on devices upon defined criteria.

▸ Report on installed applications

Software vulnerabilities and updates

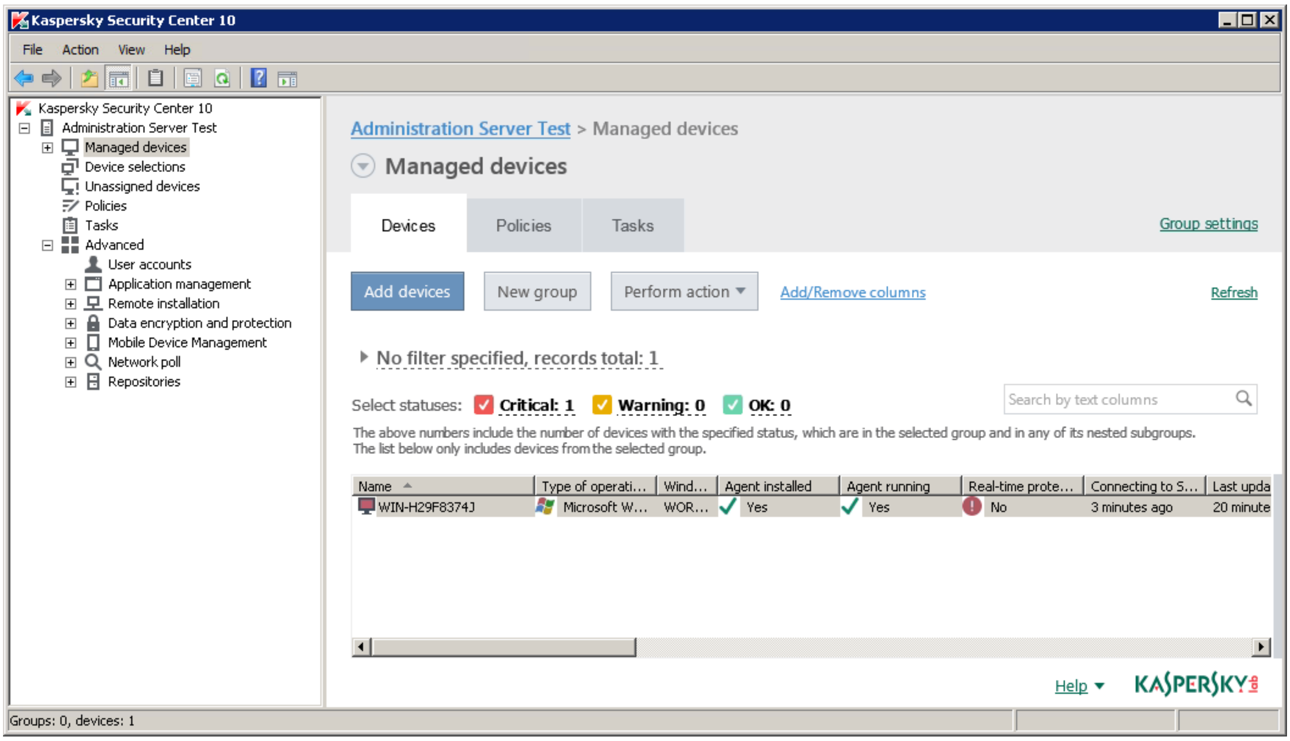
Distribution of devices by severity level of vulnerabilities:

🟥 Devices with critical-severity vulnerabilities: 1
🟧 Devices with high-severity vulnerabilities: 0
🟨 Devices with medium-severity vulnerabilities: 0
🟩 Devices without vulnerabilities: 1

▸ View detected Software vulnerabilities
▸ View Software Updates
▸ Vulnerabilities report

*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.



No filter specified, records total: 1

Select statuses: ☑ Critical: 1 ☑ Warning: 0 ☑ OK: 0

The above numbers include the number of devices with the specified status, which are in the selected group and in any of its nested subgroups.
The list below only includes devices from the selected group.

| Name | Type of operati... | Wind... | Agent installed | Agent running | Real-time prote... | Connecting to S... | Last upda |
|---|---|---|---|---|---|---|---|
| WIN-H29F8374J | Microsoft W... | WOR... | ✓ Yes | ✓ Yes | ! No | 3 minutes ago | 20 minute |

Groups: 0, devices: 1

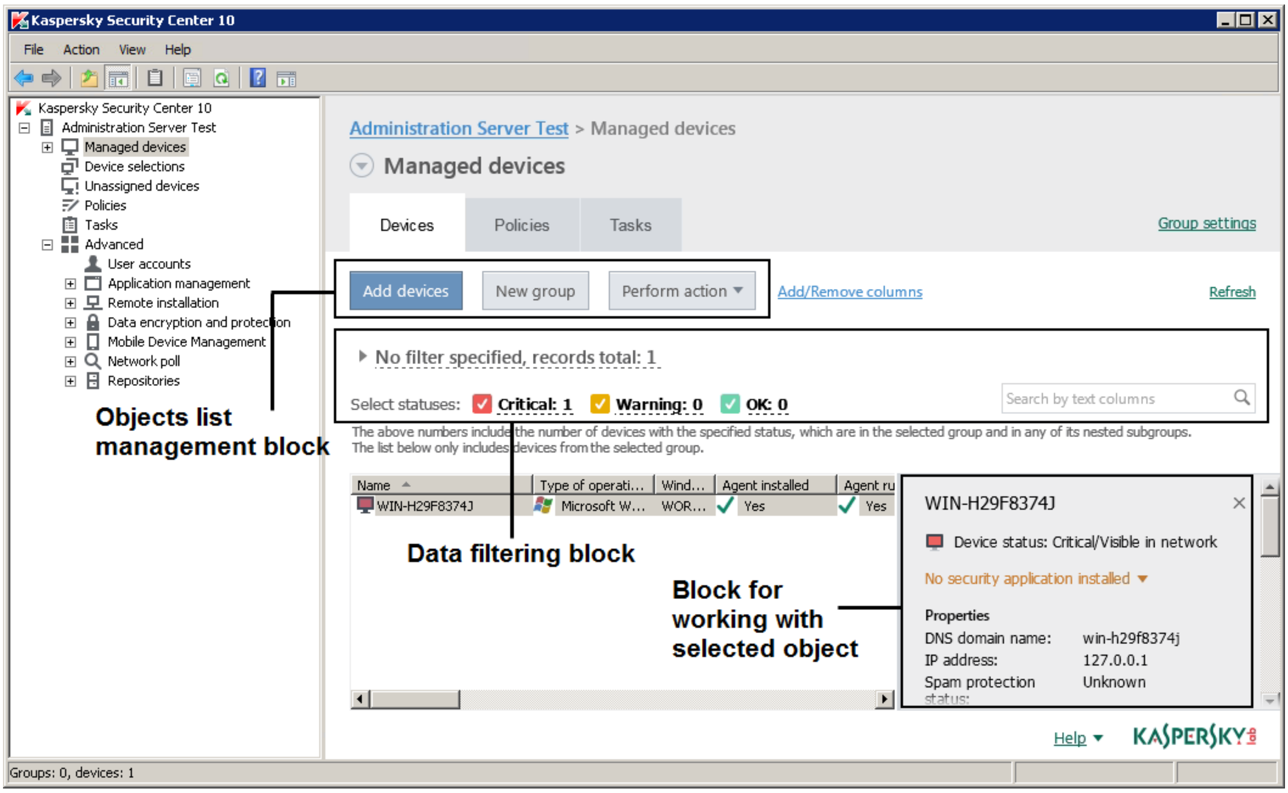
*Figure 4. Workspace divided into tabs*

## In this section:

# 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.



No filter specified, records total: 1

Select statuses: Critical: 1 Warning: 0 OK: 0

The above numbers include the number of devices with the specified status, which are in the selected group and in any of its nested subgroups. The list below only includes devices from the selected group.

WIN-H29F8374J Microsoft W… WOR… Yes Yes

WIN-H29F8374J

Device status: Critical/Visible in network

No security application installed

Properties

DNS domain name: win-h29f8374j

IP address: 127.0.0.1

Spam protection status: Unknown

Groups: 0, devices: 1

Objects list management block

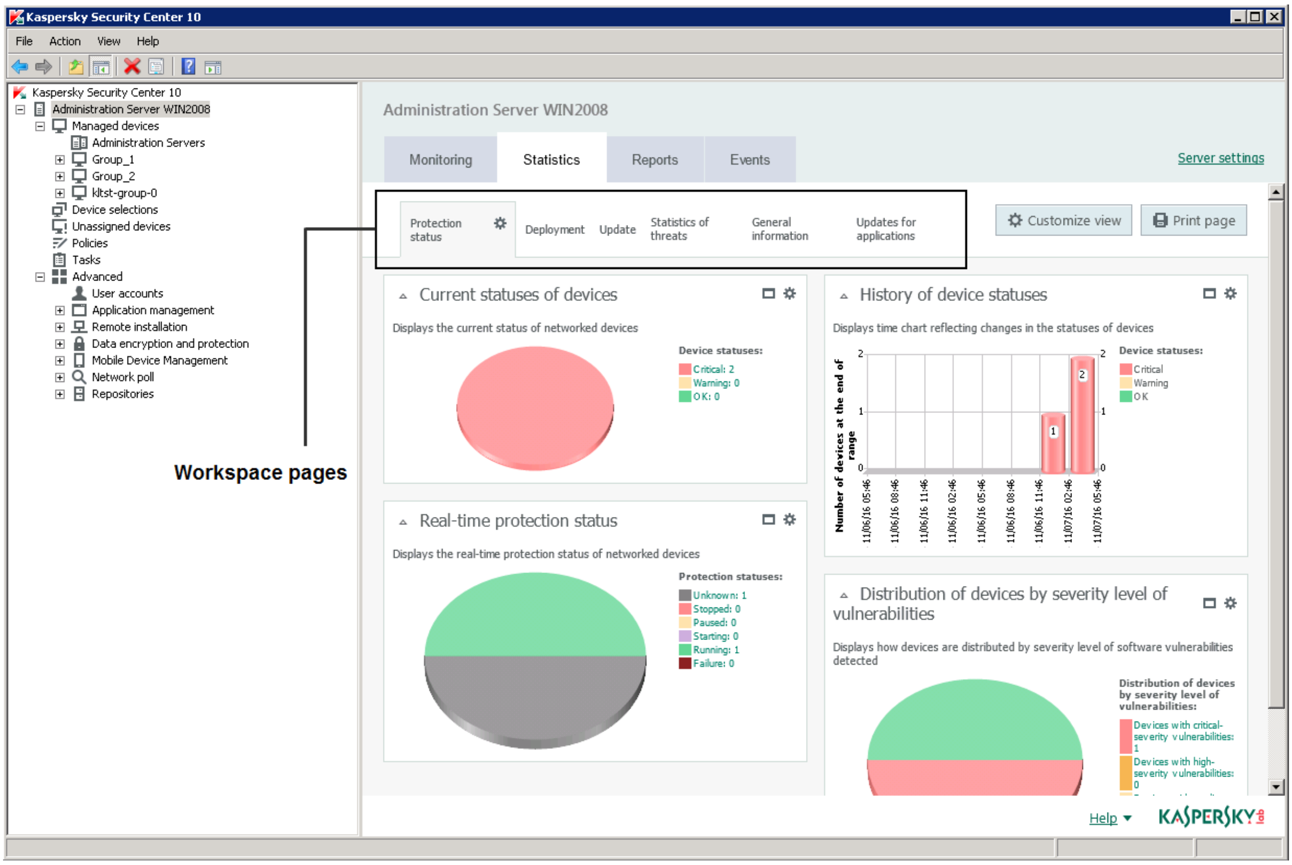
Data filtering block

Block for working with selected object

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 data display on those information panes: change the types of charts and the set of data presented on them, modify and add information panes or entire pages on the **Statistics** tab.



Displays the current status of networked devices

Displays time chart reflecting changes in the statuses of devices

Displays the real-time protection status of networked devices

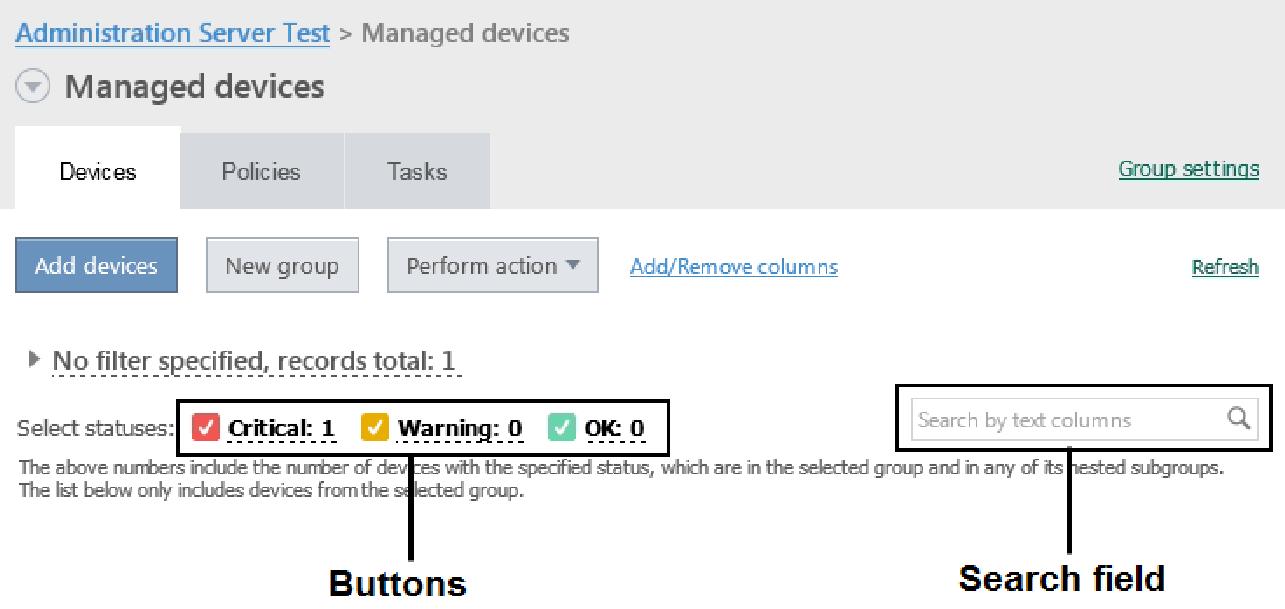
Displays how devices are distributed by severity level of software vulnerabilities detected

*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).



The above numbers include the number of devices with the specified status, which are in the selected group and in any of its nested subgroups. The list below only includes devices from the selected group.

**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.

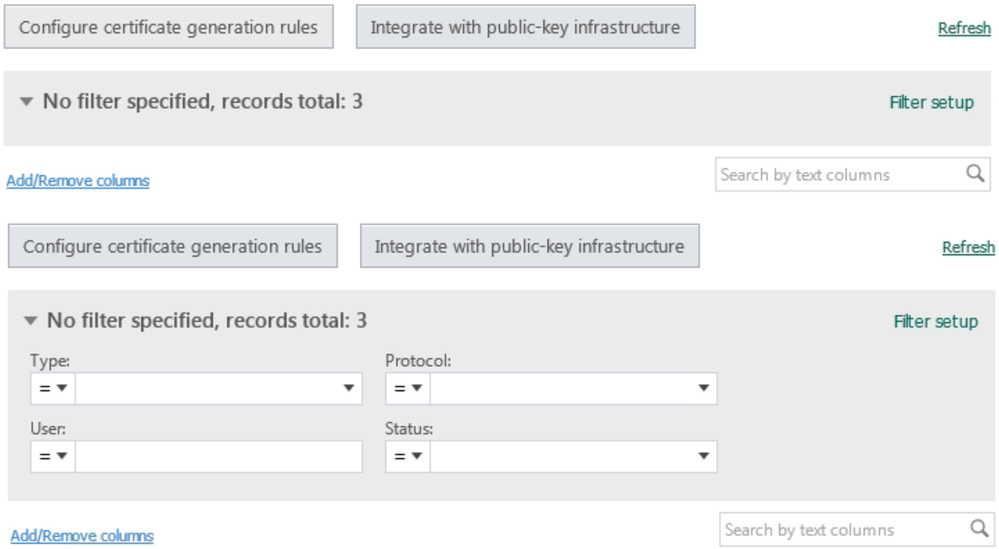
2. Click the **Adjust filter** link to select filtering criteria.

   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 search for devices using keywords and regular expressions in the **Search** field.


Configure certificate generation rules
Integrate with public-key infrastructure
Refresh
No filter specified, records total: 3
Filter setup
Add/Remove columns
Search by text columns
Configure certificate generation rules
Integrate with public-key infrastructure
Refresh
No filter specified, records total: 3
Filter setup
Type:
=
Protocol:
=
User:
=
Status:
=
Add/Remove columns
Search by text columns

**Standard filtering block**

**Expanded filtering block**

# 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 list of additional context menu commands corresponding to various console tree objects is provided in Appendices.

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**.

# Starting the application

This section describes the startup of Kaspersky Security Center.

Kaspersky Security Center starts automatically when you start the Administration Server.

► *To run Administration Console of the application,*

select **Kaspersky Security Center** in the **Kaspersky Security Center** group of the **Start** → **Applications** menu.

This **Kaspersky Security Center** program group is created on administrator workstations during Administration Console installation.

# Deploying the protection system

This section describes two possible scenarios for deploying a protection system on an organization's network:

- Deploying a protection system within an organization.
- Deploying a protection system on a client organization's network (when using the SPE version).

> If you need to deploy a protection system within an organization that includes remote offices that are not in the organization's network, you can use the anti-virus protection deployment scenario for service providers.

For detailed descriptions of operations included in the above-listed protection deployment scenarios, please refer to the section "Performing common tasks" (see page 44).

## In this section:

# Deploying a protection system within an organization

► *To deploy a protection system on a corporate network, perform the following actions:*

1. Install and configure Administration Server and Administration Console (see section "Installing Kaspersky Security Center components" on page 45).
2. Create administration groups and add client devices to them (see section "Creating administration groups" on page 46).

3. Install Network Agent and any required Kaspersky Lab applications on the selected client devices remotely.

4. If necessary, update the databases of Kaspersky Lab applications on the client devices (for more details, see the *Kaspersky Security Center Administrator's Guide*).

5. If necessary, perform advanced configuration of installed applications using policies (see section "Configuring a policy for an application" on page 82) and local settings of applications (see section "Viewing and editing the local settings of an application" on page 82).

6. Configure notifications of events on client devices to be sent to the administrator (see section "Configuring event notification" on page 83).

7. Check the functioning of notifications of events in the operation of the protection system (see section "Verifying downloaded updates" on page 79).

8. View reports (see section "Creating and viewing a report" on page 85) and configure automatic delivery of required reports by email (see section "Creating a report delivery task" on page 86).

9. Configure automatic installation of applications on new devices on the network (see section "Configuring automatic installation of applications" on page 77).

After that, the protection system is deployed in the corporate network.

# Deploying a protection system on a client organization's network

► *To deploy anti-virus protection across a client organization's network:*

1. Install Administration Server and Administration Console to the administrator's workstation (see section "Installing Kaspersky Security Center components" on page 45).

2. Install Kaspersky Security Center 10 Web Console on the administrator workstation.

3. Configure Administration Server for work with Kaspersky Security Center 10 Web Console (for more details, see the *Kaspersky Security Center Implementation Guide*).
4. Create and configure a virtual Administration Server to manage the client organization's network (see section "Creating a virtual Administration Server" on page 55).
5. Define and configure an update agent in the client organization's network.
6. Configure the Network Agent installation package that you intend to use for Network Agent installation on devices in the client organization.
7. Install Network Agent and any required Kaspersky Lab applications on the selected client devices remotely.
8. If necessary, perform advanced configuration of installed applications using policies (see section "Configuring a policy for an application" on page 82) and local settings of applications (see section "Viewing and editing the local settings of an application" on page 82).

After you complete the above steps, the protection system will be deployed on the client organization's network.

# Performing typical tasks

This section describes the basic operations that you can perform using Kaspersky Security Center.

## In this section:

# Installing Kaspersky Security Center components

► *To install Administration Server and Administration Console:*

1. Select the device on which Administration Server and Administration Console will be installed. We recommend that you install these components on a device that is included in the domain.

   You can install Kaspersky Security Center 10 Administration Server and Kaspersky Security Center 10 Administration Console on the same computer where Administration Server and Administration Console from version 9.0 are already running.

   We also recommend that the installation be performed by using the domain administrator's rights. This allows the automatic creation of the **KLAdmins** and **KLOperators** user groups, and provides the necessary rights to the account under which Administration Server will be running.

2. Run the setup.exe executable file and follow the instructions of the Setup Wizard.

3. Select the typical installation. Most of the settings are determined automatically.

> Custom installation is described in detail in the *Kaspersky Security Center Implementation Guide*.

The following applications required for the application operation will be installed shortly after unless they were installed earlier:

- Microsoft Windows Installer 3.1.
- Microsoft Data Access® Components (MDAC) 2.8.
- Microsoft .NET Framework 2.0.
- Microsoft SQL Server® 2008 R2 Express Edition.

These additional applications do not require any maintenance or administration.

During the next step of the Wizard, the application files will be copied to the computer, and the database will be created in which Administration Server centralizes information about the network anti-virus protection.

After the Wizard completes, you can start Administration Console and perform initial configuration by using the Quick Start Wizard.

# 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.

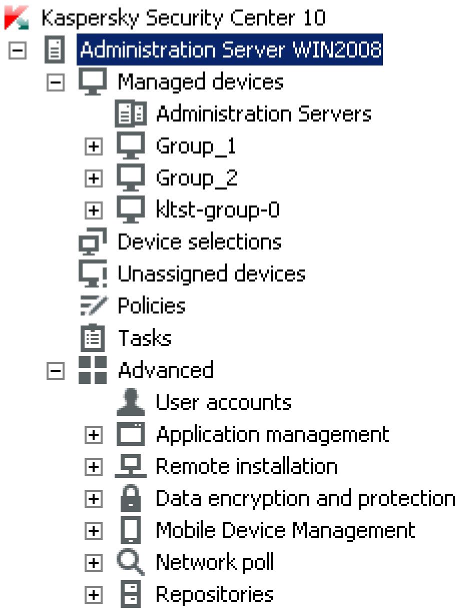


*Figure 7. Viewing administration groups hierarchy*

► *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.

# Installing Kaspersky Security Center 10 Web Console

Administration Console must be installed on the device on which you want to install Kaspersky Security Center 10 Web Console.

> On devices running Windows 7, Windows Server 2008, or Windows Vista, the KB2533623 (https://support.microsoft.com/en-us/kb/2533623) update must also be installed.

Kaspersky Security Center 10 Web Console installation requires local administrator rights.

► *To install Kaspersky Security Center 10 Web Console on a local device,*

run the install.exe file from the CD with the Kaspersky Security Center 10 Web Console distribution package.

The corresponding wizard will guide you through the installation. The Setup Wizard prompts you to define the application settings. Follow the instructions of the Wizard.

> Kaspersky Security Center 10 Web Console installation from a distribution package downloaded from the Internet is no different than installation from the installation CD.

## The wizard's steps

# Step 1. Reviewing the License Agreement

At this step of the Setup Wizard, you should read the License Agreement, which is to be concluded between you and Kaspersky Lab.

Please, read the End User License Agreement carefully. If you accept all of the provisions, select the **I accept the terms of the License Agreement** check box. Installation continues.

If you do not accept the End User License Agreement, cancel installation by clicking the **Cancel** button.

> Remote installation of Kaspersky Security Center 10 Web Console through an installation package or local installation in non-interactive mode means automatic acceptance of the terms of the End User License Agreement related to the application that you intend to install.
> You can view the End User License Agreement for a specific application in the distribution kit of the application or on the Kaspersky Lab Technical Support website.

# Step 2. Connecting to Kaspersky Security Center

Select a method of Kaspersky Security Center 10 Web Console connection to Kaspersky Security Center. The following connection options are available:

- **Use Apache server installed on local device**. If this option is selected, Kaspersky Security Center 10 Web Console connects to Kaspersky Security Center through an Apache server installed on a local device (you can select Apache server installation at the next step of the Wizard).
- **Use Apache server installed on remote device**. You can select this option if an Apache server is already installed on a remote device. In this case, only the server part of Kaspersky Security Center 10 Web Console is installed locally. To connect Kaspersky Security Center 10 Web Console to Kaspersky Security Center, install the client part of Kaspersky Security Center 10 Web Console on a remote device. If you select this option, the Setup Wizard proceeds to Step 8 (see section "Step 8. Starting Kaspersky Security Center 10 Web Console installation" on page 53).

► *To install the client part of Kaspersky Security Center 10 Web Console on a remote device running Linux,*

run one of the following files depending on the type of your system:

- For 32-bit systems:
  - kscwebconsole-10.<build_number>.i386.rpm;
  - kscwebconsole_10.<build_number>_i386.deb.
- For 64-bit systems:
  - kscwebconsole-10.<build_number>.x86_64.rpm;
  - kscwebconsole_10.<build_number>_x86_64.deb.

# Step 3. Selecting the destination folder

Specify the destination folder for Kaspersky Security Center 10 Web Console installation. By default, this will be <Drive>:\Program Files\Kaspersky Lab\Kaspersky Security Center Web Console. If this folder does not exist, it will be created automatically. You can change the destination folder by using the **Browse** button.

# Step 4. Selecting the Apache server installation mode

If no Apache server is installed on the device, at this step, the Setup Wizard prompts you to install Apache HTTP Server 2.4.25.

By default, Apache HTTP Server 2.4.25 is selected as the installation option. If you do not want to install the Apache server through the Kaspersky Security Center 10 Web Console Setup Wizard, clear the **Install Apache HTTP Server 2.4.25** check box.

> Apache Server installation may prompt you to restart the device.

# Step 5. Installing Apache Server

At this step of the Wizard, Apache HTTP Server 2.4.25 is installed and configured.

Before installation, specify the certificate that will be used for encryption of the connection between the Apache server and the user browser. Select one of the following options:

- **Generate new certificate**. Create a certificate for working via HTTPS.
- **Choose existing**. Use an existing certificate for working via HTTPS. Specify a certificate using one of the available methods:
  - **Select certificate file**. You can select an existing certificate by clicking the **Browse** button.
  - **Select a private key**. You can specify a certificate using the file of its closed key by clicking the **Browse** button.

# Step 6. Selecting the ports

Define the following settings:

- Number of the SSL port for encrypted connection of the device to the Administration Server. The default port number is 13291.
- Number of the port for the device connection to the Apache server. The default port number is 9000.
- Address of the device with Administration Server installed. The default address is localhost.

  If the device on which Kaspersky Security Center 10 Web Console and Self Service Portal are to be installed is in DMZ, select the **Connection gateway** check box and specify the connection gateway address in the **Server address** field.
- Number of the port for the device connection to Kaspersky Security Center 10 Web Console. The default port number is 8080.
- Number of the port for the device connection to Self Service Portal. The default port number is 8081.

After you install Kaspersky Security Center 10 Web Console and Self Service Portal, you can change the default port numbers.

# Step 7. Selecting an account

Specify the user's domain account under which installation packages will be downloaded to users' mobile devices by means of QR codes. The account must be specified in <*Domain name*>\<*Account name*> format.

Click the **Test** button to test the Administration Server connection.

# Step 8. Starting Kaspersky Security Center 10 Web Console installation

Click the **Start** button to start Kaspersky Security Center 10 Web Console installation.

The installation process is displayed on the Wizard page.

# Step 9. Completing Kaspersky Security Center 10 Web Console installation

If Apache Server, version 2.4.25 or later, is already installed on the computer, or if automatic installation of Apache Server returned an error, at this step of the Kaspersky Security Center 10 Web Console Setup Wizard, you are prompted to open the file with instructions on how to configure an Apache server. To open the instructions file, select the **Open readme.txt** check box.

To complete the Setup Wizard, click the **Finish** button.

# Upgrading Kaspersky Security Center 10 Web Console

You can install Kaspersky Security Center 10 Web Console on a device on which an earlier version of Kaspersky Security Center 10 Web Console has been installed. When upgrading to version 10, all data and settings from the previous version of Kaspersky Security Center Web Console are saved.

► *To upgrade Kaspersky Security Center Web Console from version 9.0 to version 10,*

run setup.exe for version 10.

The **Kaspersky Security Center 10 Web Console Setup Wizard** window opens. Follow the instructions of the Wizard.

> We recommend that you avoid aborting the Setup Wizard operation.
> Aborting the upgrading process at the stage of Kaspersky Security Center 10 Web Console installation may lead to the inoperability of Kaspersky Security Center Web Console 9.0.

# Creating a virtual Administration Server

► *To add a virtual Administration Server to the selected administration group:*

1. In the console tree, in the administration group folder, select the **Administration Servers** node.
2. Start the process of virtual Administration Server creation in one of the following ways:
   - In the context menu of the **Administration Servers** node, select **Create** → **Virtual Administration Server**.
   - Click the **Add virtual Administration Server** link in the workspace.

The New Virtual Administration Server Wizard starts. Follow the instructions of the Wizard.

# Assigning computers 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 a device, keep in mind the operation features of update agents and requirements set for the device that acts as update agent.

   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.

# Mobile Device Management

Kaspersky Security Center allows managing mobile devices that support Exchange ActiveSync (EAS device) and iOS Mobile Device Management (iOS MDM device), and Kaspersky Endpoint Security for Android (KES device) protocols.

Kaspersky Security Center supports the following features:

- Creation of an MDM policy that allows centralized configuration of EAS devices and iOS MDM devices.

- Management of EAS devices and iOS MDM devices through remote commands.

- Management of mobile applications packages.
- Option for users to manage their devices remotely (send commands, install apps), using corporate Self Service Portal.

> The list of functions available for a specific mobile device depends on the Exchange ActiveSync support features on that device.

Kaspersky Security Center allows managing mobile devices through *Mobile Devices Servers*. A mobile device server is a component of Kaspersky Security Center that provides access to mobile devices and lets you manage them through the Administration Console.

There are two types of mobile device servers:

- Microsoft Exchange Mobile Devices Server. Used for managing EAS devices. To be installed on the client computer on which the Microsoft Exchange server has been installed. The Microsoft Exchange Mobile Devices Server lets you retrieve data from the Microsoft Exchange server and then transmit it to the Administration Server.
- iOS MDM Server. Used for managing iOS MDM devices. To be installed on a client computer. iOS MDM Server allows you to connect iOS MDM devices to the Administration Server and manage them through Apple® Push Notifications (APNs).

For detailed information about how to manage mobile devices refer to the *Kaspersky Security Center Administrator's Guide*.

Hereinafter, a brief description of actions is provided, which must be performed in order to connect EAS devices and iOS MDM devices to Administration Server.

# Management through iOS MDM and Microsoft Exchange ActiveSync

Kaspersky Security Center allows managing mobile devices that are connected to Administration Server via Exchange ActiveSync protocol. Exchange ActiveSync (EAS) mobile devices are those connected to a Microsoft Exchange Mobile Devices Server and managed by Administration Server.

The following operating systems support Exchange ActiveSync protocol:

- Windows Mobile.
- Windows CE.
- Windows Phone® 7.
- Windows Phone 8.
- Android.
- Bada.
- BlackBerry® 10.
- iOS®.
- Symbian.

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

Deployment of a mobile device management system using Exchange ActiveSync protocol includes the following steps:

1. The administrator installs Exchange ActiveSync Mobile Devices Server on a selected client device (see section "Installing Exchange ActiveSync Mobile Devices Server" on page 60).
2. The administrator creates a management profile(s) in Administration Console for managing EAS devices and adds that profile(s) to the mailboxes of Exchange ActiveSync users.

   > *Management profile of Exchange ActiveSync mobile devices* is an ActiveSync policy used on a Microsoft Exchange server for managing Exchange ActiveSync mobile devices. Only one EAS device management profile can be assigned to a Microsoft Exchange mailbox.

For the instruction on how to create an EAS device management profile, please refer to the *Kaspersky Security Center Administrator's Guide*.

Users of mobile EAS devices connect to their Exchange mailboxes. A management profile imposes restrictions on mobile devices (see section "Connecting mobile devices to Microsoft Exchange Mobile Devices Server" on page 62).

For information about how add an EAS device management profile and how to manage Exchange ActiveSync mobile devices, please refer to the *Kaspersky Security Center Administrator's Guide*.

# Installing a Mobile device server for Exchange ActiveSync

A Microsoft Exchange Mobile Devices Server should be installed on a client device with a Microsoft Exchange server installed. It is recommended to install the Microsoft Exchange Mobile Devices Server to a Microsoft Exchange server with the Client Access role assigned. If several Microsoft Exchange servers with the Client Access role in the same domain are combined into a Client Access Array, it is recommended to install the Microsoft Exchange Mobile Devices Server on each Microsoft Exchange server in that array in cluster mode.

► *To install a Microsoft Exchange Mobile Devices Server on a local device:*

1. Run the setup.exe executable file.

   A window opens prompting you to select Kaspersky Lab applications to install.

2. In the applications selection window, click the **Install Microsoft Exchange Mobile Devices Server** link to run the Microsoft Exchange Mobile Devices Server Setup Wizard.

3. Choose the type of Microsoft Exchange Mobile Devices Server installation in the **Installation settings** window:

   - To install Microsoft Exchange Mobile Devices Server with the default settings, select **Standard installation** and click the **Next** button.

   - To define the settings for installation of the Microsoft Exchange Mobile Devices Server manually, select **Advanced installation** and click **Next**. Then do the following:

     a. Select destination folder in **Destination Folder** window. The default folder is <Disk>:\Program Files\Kaspersky Lab\Mobile Device Management for Exchange. If such folder does not exist, it is created automatically during the installation. You can change the destination folder by using the **Browse** button.

b. Choose the Microsoft Exchange Mobile Devices Server installation mode (normal or cluster) in the **Installation mode** window: normal or cluster mode.

c. In **Select Account** window, choose an account that will be used to manage mobile devices:

   - **Create account and role group automatically**.
     Account will be created automatically.

   - **Specify an account**. Account should be selected manually. Click the **Select** button to select the user account and specify the password. The selected user should belong to a group with rights to manage mobile devices via ActiveSync.

d. In **IIS settings** window, enable or disable automatic configuration of Internet Information Services (IIS) web server properties.

> If you have locked the automatic configuration of Internet Information Services (IIS) properties, enable the "Windows authentication" mechanism manually in IIS settings for PowerShell Virtual Directory. If "Windows authentication" mechanism is disabled, Microsoft Exchange Mobile Devices Server will not operate correctly. Please refer to IIS documentation for more information about configuring IIS.

e. Click **Next**.

4. Verify Microsoft Exchange Mobile Devices Server installation properties in the window that opens, then click **Install**.

When the Wizard is complete, the Microsoft Exchange Mobile Devices Server is installed on the local device. The Microsoft Exchange Mobile Devices Server will be displayed in the **Mobile Device Management** folder of the console tree.

# Connecting mobile devices to a Microsoft Exchange Mobile Devices Server

Before connecting any mobile devices, you should configure Microsoft Exchange Server in order to allow devices to be connected via ActiveSync protocol.

To connect a mobile device to a Microsoft Exchange Mobile Devices Server, the user connects to his or her Microsoft Exchange mailbox from the mobile device through ActiveSync. When connecting, the user must specify the connection settings in the ActiveSync client, such as email address and email password.

The user's mobile device connected to the Microsoft Exchange server is displayed in the **Mobile devices** subfolder contained in the **Mobile Device Management** folder of the console tree.

After the Exchange ActiveSync mobile device is connected to a Microsoft Exchange Mobile Devices Server, the administrator can manage the Exchange ActiveSync mobile device that has been connected. For instructions on how to manage Exchange ActiveSync mobile devices, please refer to the *Kaspersky Security Center Administrator's Guide*.

# Deploying a system for management via iOS MDM protocol

Kaspersky Security Center allows managing mobile devices running under iOS. iOS MDM mobile devices refer to iOS mobile devices that are connected to an iOS MDM Server and managed by an Administration Server.

Connection of mobile devices to an iOS MDM Server is performed in the following sequence:

1. The administrator installs iOS MDM Server on the selected client device. Installation of iOS MDM Server is performed using the standard tools of the operating system.

2. The administrator receives an Apple® Push Notification Service certificate, also known as APNs certificate (see section "Receiving an APNs certificate" on page 69).

   The APNs certificate allows Administration Server to connect to the APNs server to send push notifications to iOS MDM mobile devices.

3. The administrator installs the APNs certificate on the iOS MDM Server (see section "Installing an APNs certificate on an iOS MDM Server" on page 71).

4. The administrator creates an iOS MDM profile for the user of the iOS mobile device.

   The iOS MDM profile contains a collection of settings for connecting iOS mobile devices to Administration Server.

5. The administrator issues a shared certificate to the user (see section "Issuing and installing a shared certificate on a mobile device" on page 72).

   The shared certificate is required to confirm that the mobile device is owned by the user.

6. The user clicks the link sent by the administrator and downloads an installation package to the mobile device.

   The installation package contains a certificate and an iOS MDM profile.

   After the iOS MDM profile is downloaded and the iOS MDM 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.

7. The administrator adds a configuration profile on the iOS MDM Server and installs the configuration profile on the mobile device after it is connected.

   The configuration profile contains a collection of settings and restrictions for the iOS MDM mobile device, for example, settings for installation of applications, settings for the use of various features of the device, email and scheduling settings. A configuration profile lets you configure iOS MDM mobile devices in accordance with the organization's security policies.

8. If necessary, the administrator adds provisioning profiles on the iOS MDM Server and then installs these provisioning profiles on mobile devices.

   *Provisioning profile* is a profile that is used for managing applications distributed in ways other than via App Store®. A provisioning profile contains information about the license; it is linked to a specific application.

For instructions on how to manage iOS MDM mobile devices, please refer to the *Kaspersky Security Center Administrator's Guide*.

## In this section:

# Installing iOS MDM Server

► *To install iOS MDM Server on a local device:*

1. Run the setup.exe executable file.

   A window opens prompting you to select Kaspersky Lab applications to install.

   In the applications selection window, click the **Install iOS MDM Server** link to run the iOS MDM Server Setup Wizard.

2. Select a destination folder.

   The default destination folder is <Disk>:\Program Files\Kaspersky Lab\Mobile Device Management for iOS. If such folder does not exist, it is created automatically during the installation. You can change the destination folder by using the **Browse** button.

3. In the **Settings for connection to iOS MDM Server** window of the Wizard, in the **External port to connect to iOS MDM service** field, specify an external port for connecting mobile devices to the iOS MDM service.

External port 5223 is used by mobile devices for communication with the APNs server. Make sure that port 5223 is opened in the firewall for connection with the address range 17.0.0.0/8.

Port 443 is used for connection to iOS MDM Server by default. If port 443 is already in use by another service or application, it can be replaced with, for example, port 9443.

The iOS MDM Server uses external port 2195 to send notifications to the APNs server.

APNs servers run in load balancing mode. Mobile devices do not always connect to the same IP addresses to receive notifications. The 17.0.0.0/8 address range is reserved for Apple, which is why it is recommended to specify this entire range as an allowed range in Firewall settings.

4. If you want to configure interaction ports for application components manually, select the **Set up local ports manually** check box and then specify values for the following settings:

   - **Port to connect to Network Agent**. In this field, specify a port for connecting the iOS MDM service to Network Agent. The default port number is 9799.

   - **Port for connection to iOS MDM service**. In this field, specify a local port for connecting Network Agent to the iOS MDM service. The default port number is 9899.

   It is recommended to use default values.

5. In the **External address of Mobile Device Server** window of the Wizard, in the **Web address for remote connection to Mobile Device Server** field, specify the address of the client device on which iOS MDM Server is to be installed.

   This address will be used for connecting managed mobile devices to the iOS MDM service. The client device must be available for connection of iOS MDM devices.

You can specify the address of a client device in any of the following formats:

- Device FQDN (such as mdm.example.com)
- Device NetBIOS name
- Device IP address

> Please avoid adding the URI scheme and the port number in the address string: these values will be added automatically.

When the Wizard completes, iOS MDM Server is installed on the local device. The iOS MDM Server is displayed in the **Mobile Device Management** folder of the console tree.

# Installing iOS MDM Server in non-interactive mode

Kaspersky Security Center allows you to install iOS MDM Server on a local device in non-interactive mode, i.e. without interactive input of installation settings.

► *To install iOS MDM Server on a local device in non-interactive mode,*

run the command

```
.\exec\setup.exe /s /v"DONT_USE_ANSWER_FILE=1
<setup_parameters>"
```

where `setup_parameters` is a list of settings and their respective values separated with spaces (`PRO1=PROP1VAL PROP2=PROP2VAL`). Run the setup.exe file from the CD containing the distribution package of Kaspersky Security Center in the Server folder.

The names and possible values for settings that can be used when installing iOS MDM Server in non-interactive mode are listed in the table below. Settings can be specified in any convenient order.

*Table 2.*

*Table 3. Settings of iOS MDM Server installation in non-interactive mode*

| Setting name | Setting description | Available values |
|---|---|---|
| EULA | Acceptance of the terms of the License Agreement.<br>This setting is mandatory. | - 1 – I accept the terms of the License Agreement<br>- Other value, or no value – I do not accept the terms of the License Agreement (installation is not performed) |
| DONT_USE_ANSWER_FILE | Whether or not to use an XML file with iOS MDM Server installation settings.<br>The XML file is included in the installation package or stored on the Administration Server. You do not have to specify an additional path to the file.<br>This setting is mandatory. | - 1 – Do not use the XML file with settings<br>- Other value, or no value defined – use the XML file with settings |
| INSTALLDIR | iOS MDM Server installation folder.<br>This setting is optional. | String value, for example, `INSTALLDIR=\"C:\install\"` |
| CONNECTORPORT | Local port for connecting the iOS MDM service to Network Agent.<br>The default port number is 9799.<br>This setting is optional. | Numerical value |
| LOCALSERVERPORT | Local port for connecting Network Agent to the iOS MDM service.<br>The default port number is 9899.<br>This setting is optional. | Numerical value |

| Setting name | Setting description | Available values |
|---|---|---|
| EXTERNALSERVERPORT | Port for connecting a device to the iOS MDM Server.<br>The default port number is 443.<br>This setting is optional. | Numerical value |
| EXTERNAL_SERVER_URL | External address of the client device on which iOS MDM Server is to be installed. This address will be used for connecting managed mobile devices to the iOS MDM service. The client device must be available for connection through iOS MDM.<br>The address must not include the URL scheme and number of the port since these values will be added automatically.<br>This setting is optional. | • Device FQDN (such as mdm.example.com)<br>• Device NetBIOS name<br>• Device IP address |
| WORKFOLDER | Workfolder of the iOS MDM Server.<br>If no workfolder is specified, data will be written to the default folder.<br>This setting is optional. | String value, for example, `WORKFOLDER=\"C:\work\"` |
| MTNCY | Use of iOS MDM Server by multiple virtual Servers.<br>This setting is optional. | • 1 – The iOS MDM Server will be used by multiple virtual Administration Servers<br>• Other value, or no value defined – The iOS MDM Server will not be used by multiple virtual Administration Servers. |

**Example:**

```
\exec\setup.exe /s /v"EULA=1 DONT_USE_ANSWER_FILE=1 EXTERNALSERVERPORT=9443
EXTERNAL_SERVER_URL=\"www.test-mdm.com\""
```

The iOS MDM Server installation settings are presented in detail in the Installing iOS MDM Server section (on page 64).

# Use of iOS MDM Server by multiple virtual Servers

► *To enable the use of iOS MDM Server by multiple virtual Administration Servers:*

1. Open the system registry of the client device with iOS MDM Server installed (for example, locally, using the regedit command in the **Start** → **Run** menu).
2. Go to the following hive:

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0
3. For the ConnectorFlags (DWORD) key, set the 02102482 value.
4. Go to the following hive:

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0
5. For the ConnInstalled (DWORD) key, set the 00000001 value.
6. Restart the iOS MDM Server service.

Key values must be entered in the specified sequence.

# Receiving an APNs certificate

When the Certificate Signing Request (CSR) is created at the first step of the APNs Certificate Wizard, its private key is stored in your device's RAM. Therefore, all wizard steps must be completed within a single session of the application.

► *To receive an APNs certificate:*

1. In the **Mobile devices** folder of the console tree, select an iOS MDM Server.

   The **Mobile devices** folder is a subfolder of the **Advanced** folder by default.

2. In the context menu of the iOS MDM Server, select **Properties**.

   This opens the properties window of the iOS MDM Server.

3. In the properties window of the iOS MDM Server, select the **Certificates** section.

4. In the **Certificates** section, in the **Apple Push Notification certificate** group of settings, click the **Request new** button.

   The Receive APNs Certificate Wizard starts and the **Request new** window opens.

5. Create a Certificate Signing Request (hereinafter referred to as CSR request). To do this, perform the following actions:

   a. Click the **Create CSR** button.

   b. In the **Create CSR** window that opens, specify a name for your request, the names of your company and department, your city, region, and country.

   c. Click the **Save** button and specify a name for the file to which your CSR request will be saved.

   The private key of the certificate is saved in the device's memory.

6. Use your CompanyAccount to send the file with the CSR request you have created to Kaspersky Lab to be signed.

   > Signing of your CSR request will only be available after you upload to CompanyAccount portal a key that allows using Mobile Device Management feature.

   After your online request is processed, you will receive a CSR request file signed by Kaspersky Lab.

7. Send the signed CSR request file to Apple Inc. https://identity.apple.com/pushcert using a random Apple ID.

   > We recommend that you avoid using a personal Apple ID. Create a dedicated Apple ID to use it as corporate one. After you have created an Apple ID, link it with the organization's mailbox, not a mailbox of an employee.

   After your CSR request is processed in Apple Inc., you will receive the public key of the APNs certificate. Save the file to the disk.

8. Export the APNs certificate together with the private key created when generating the CSR request, in PFX file format. To do this, perform the following actions:

   a. In the **Request new APNs certificate** window, click the **Complete CSR** button.

   b. In the **Open** window, choose a file with the public key of the certificate, received from Apple Inc. as the result of CSR request processing, and press **Open** button.

   Certificate export process will be started.

   c. In the next window, enter private key password and click **OK**.

   This password will be used for the APNs certificate installation on the iOS MDM Server.

   d. In the **Save APNs Certificate** window, specify file name for APNs certificate, choose folder and click **Save**.

Private and public keys of the certificate are combined, and APNs certificate is saved in PFX format. After that, you can install the APNs certificate on the iOS MDM Server (see section "Installing an APNs certificate on an iOS MDM Server" on page 71).

For more detailed instructions on how to create a CSR and send it to Apple Inc., please refer to the Knowledge Base on the Kaspersky Lab Technical Support Service website (http://support.kaspersky.com/11077).

# Installing an APNs certificate on an iOS MDM Server

After you have received the APNs certificate, you must install it on the iOS MDM Server.

► *To install the APNs certificate on the iOS MDM Server:*

1. In the **Mobile devices** folder of the console tree, select an iOS MDM Server.

   The **Mobile devices** folder is a subfolder of the **Advanced** folder by default.

2. In the context menu of the iOS MDM Server, select **Properties**.

   This opens the properties window of the iOS MDM Server.

3. In the properties window of the iOS MDM Server, select the **Certificates** section.

In the **Certificates** section, in the **Apple Push Notification certificate** group of settings click the **Install** button.

1. Select the PFX file that contains the APNs certificate.
2. Enter the password of the private key specified when exporting the APNs certificate (see section "Receiving an APNs certificate" on page 69).

As a result, the APNs certificate will be installed on the iOS MDM Server. The certificate details will be displayed in the properties window of the iOS MDM Server, in the **Certificates** section.

# Issuing and installing a shared certificate on a mobile device

► *To issue a shared certificate to a user:*

1. In the console tree, in the **User accounts** folder, select a user account.
2. In the context menu of the user account, select **Install certificate**.

The Certificate Installation Wizard starts. Follow the instructions of the Wizard.

When the Wizard finishes its operation, a certificate will be created and added to the list of the user's certificates.

The handed certificate will be downloaded by the user, along with the installation package that contains the iOS MDM profile.

After the mobile device is connected to the iOS MDM Server, the iOS MDM profile settings will be applied on the user's device. The administrator will be able to manage the device after connection.

The user's mobile device connected to the iOS MDM Server is displayed in the **Mobile Devices** subfolder within the **Mobile Device Management** folder of the console tree.

For instructions on how to hand certificates and manage iOS MDM mobile devices, please refer to the *Kaspersky Security Center Administrator's Guide*.

# Adding an iOS MDM device to the list of managed devices

► *To add the iOS MDM device of a user to the list of managed devices using a link to App Store:*

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 device**.

   The Add new device wizard starts running. 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 device.

   - Specify a shared certificate file.

4. In the **Device type** window of the Wizard, select **Link to App Store**.

5. In the **User notification method** window of the Wizard, configure notification of the mobile device user of certificate creation (with an SMS message or by email).

6. In the **Certificate info** window of the Wizard, click the **Finish** button to close the Certificate Installation Wizard.

After the Wizard finishes its activities, a link and a QR code will be sent to the user device thus allowing him or her to download Kaspersky Safe Browser from App Store. The user clicks the link or scans the QR code. After that, the operating system of the 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. Using the scanning feature of Kaspersky Safe Browser, the user scans the QR code and retrieves the settings for device connection to the Administration Server. The user saves those settings on the device. After that, the mobile device automatically 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. In this case, Kaspersky Safe Browser will not be downloaded and installed again.

If an iOS MDM profile has previously been installed on an iOS MDM device, this device will be displayed twice on the list of devices in the **Mobile devices** folder (dubbed) after Kaspersky Safe Browser and the shared certificate are installed on the device. The device is dubbed on the list due to two shared (identification) certificates available on it.

# Installing applications using Remote Installation Wizard

To install Kaspersky Lab applications, you can use the Remote Installation Wizard. The Remote Installation Wizard allows remote installation of applications either through pre-created installation packages or directly from a distribution package.

For the proper operation of the remote installation task on a client device with no Network Agent installed, the following ports must be open: TCP 139 and 445; UDP 137 and 138. By default, these ports are open for all devices included in the domain. They are opened automatically by the remote installation preparation utility.

► *To install the application using the Remote Installation Wizard:*

1. Establish a connection with the Administration Server that controls the relevant administration group.
2. Select an administration group in the console tree.
3. In the workspace of the group, click the **Perform action** button and select **Install application** in the drop-down list.

   This will start the Remote Installation Wizard. Follow the instructions of the Wizard.
4. At the final step of the Wizard, click **Next** to create and run a remote installation task on the selected devices.

When the Remote Installation Wizard completes, Kaspersky Security Center performs the following actions:

- Creates an installation package for application installation (if it was not created earlier). The installation package is located in the **Remote installation** folder, in the **Installation packages** subfolder, under a name that corresponds to the application's name and version. You can use this installation package for the application installation in the future.
- It creates and runs a remote installation task for specific devices or for an administration group. The newly created remote installation task is stored in the **Tasks** folder or added to the tasks of the administration group for which it

has been created. You can later launch this task manually. The task name corresponds to the name of the application installation package: **Installation <Name of installation package>**.

# Viewing a protection deployment report

You can use the protection deployment report to monitor the progress of network protection deployment.

► *To view a protection deployment 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** folder, select the report template named **Protection deployment report**.

The workspace displays a report containing information about protection deployment on all networked devices.

You can generate a new protection deployment report and specify the type of data that it should include:

- For an administration group.
- For specific devices.
- For a device selection.
- For all devices.

For detailed information about how to create a new report refer to the *Administrator's Guide of Kaspersky Security Center*.

> Kaspersky Security Center assumes that a device has protection deployed if it has a security application installed and real-time protection enabled.

# Configuring automatic installation of applications

► *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.

# 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.

# 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.

# 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 want to distribute updates to client devices that belong to a selected administration group, create a task for the selected group.
   - If you want to distribute updates to client devices that belong to different administration groups or belong to none of the administration groups, create a task for specific devices.

   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.

# Configuring a policy for an application

► *To configure a policy for an application:*

1. In the console tree, select an administration group for which you want to configure a policy.
2. In the workspace of the selected group, on the **Policies** tab, select the policy of the relevant application.
3. Open the policy properties window and configure the policy.

After the changes are saved, the policy with modified settings is applied to the devices of the administration group.

# 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).

# 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. The administrator can receive the parameters of the event that has occurred by means of the executable file.

► *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.

# Testing notifications

To check whether event notifications are sent, the application uses the notification of the EICAR test “virus” detection on client devices.

► *To verify sending of event notifications:*

1. Stop the real-time file system protection task on a client device and copy the EICAR test “virus” to that client device. Now re-enable real-time protection of the file system.

2. Run a scan task for client devices in an administration group or for specific devices, including one with the EICAR “virus”.

   If the scan task is configured correctly, the test "virus" will be detected. If notifications are configured correctly, you are notified that a virus has been detected.

   In the workspace of the **Administration Server** node, on the **Events** tab, the **Recent events** selection displays a record of detection of a "virus".

> The EICAR test "virus" contains no code that can do harm to your device. However, most manufacturers' security applications identify this file as virus. You can download the test "virus" from the official EICAR website (http://www.eicar.org/86-0-Intended-use.html).

# 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.

> The report delivery task is created automatically if email settings have been defined during the Kaspersky Security Center installation.

# Viewing the report on detected viruses

► *To view the general report on detected viruses:*

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 **Statistics** tab.
3. On the **Statistics** tab, select the **Statistics of threats** page.

The information panes of this page by default display the following data the previous 24 hours:

- History of virus activity.
- Most frequently occurring viruses.
- Computers with the largest number of viruses detected.
- Users on whose computers the largest number of viruses has been detected.

In the workspace of the **Administration Server** node, on the **Reports** tab, you can also view detailed reports on viruses that have been detected in the network:

- **Viruses report**.
- **Report on most heavily infected devices**.
- **Report on users of infected devices**.

When you select the relevant report, a dedicated window displays detailed information about viruses that have been detected since the Administration Server installation.

You can edit the settings of any report: for example, the time interval for which the report is generated and the set of fields displayed in the report (for more details, please refer to the *Kaspersky Security Center Administrator's Guide*).

# 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.

# Monitoring the network status

You can track the status of devices managed by the Administration Server named **<Server name>** in the workspace of the **<Server name>** node. Information about the application operation is divided into functional sections:

- Deployment of protection on the network (**Deployment** section).
- Creation of a structure of administration groups that contain managed devices (**Manage devices** section).
- Protection performance on client devices (**Device protection and virus scan** section).
- Updates of databases and software modules (**Update** section).
- Monitoring and notifications (**Monitoring** section).

You can quickly assess the current status of your network and detect possible problems by color indicators in sections. A green indicator means that all required tasks have already been performed in this section and no problems are found. A yellow or red indicator means that some important or critical events have been detected. A blue indicator means that the application has registered some events that are unrelated to potential or actual threats to the security of managed devices (for example, download of updates to the Administration Server repository has started). A gray indicator means that event details are not available or have not yet been received.

In addition to the color indication, each section provides a brief description of the protection system status or a problem arisen. Sections also provide links that you can use to proceed to main tasks.

# 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.

# Upgrading Kaspersky Security Center

You can install Administration Server 10 on a device with an earlier version of Administration Server installed. When you upgrade Administration Server to version 10, all data and settings from the previous version of the application are saved.

> Before upgrading Kaspersky Security Center, you have to decrypt all encrypted drives of devices on which application components (Administration Servers, Network Agents) are installed. When Kaspersky Security Center is upgraded, decrypted disks can be re-encrypted.

► *To upgrade Administration Server of the 9.0 version to the 10 version:*

1. Run the executable file setup.exe for the version 10.

   A window opens prompting you to select Kaspersky Lab applications to install.

   In the application selection window, click the **Install Kaspersky Security Center Administration Server** link to run the Administration Server Setup Wizard. Follow the instructions of the Wizard.

2. Read the License Agreement concluded between you and Kaspersky Lab. If you agree with all of its terms, select the **I accept the terms of the License Agreement** check box.

   Installation of the application then continues. The Setup Wizard prompts you to create a backup copy of the data of Kaspersky Security Center 9.0 Administration Server.

   Kaspersky Security Center supports data recovery from a backup copy of Administration Server created by an older version of the application.

3. If you need to create a backup copy, in the **Administration Server Backup** window that opens, select the **Create backup copy of Administration Server** check box.

A backup copy of Administration Server data is created by the klbackup utility. This utility is included in the application distribution, and is located in the root of the Kaspersky Security Center installation folder.

> For details on the operation of the data backup and recovery utility, refer to the Kaspersky Security Center Full Help, "Applications" section.

4. Install Administration Server version 10, following the Setup Wizard's instructions.

> We recommend that you avoid aborting the Setup Wizard operation.
> Canceling the product setup at the step of Administration Server installation may cause Kaspersky Security Center 9.0 to fail.

5. For devices on which the earlier version of Network Agent are installed, create and run the remote installation task for the new version of Network Agent.

   After completing the remote installation task, the Network Agent version will be upgraded.

If problems occur during Administration Server installation, you can restore the previous version of Administration Server using the backup copy of the Administration Server data created before the upgrade.

If at least one Administration Server of the new version has been installed in the network, other Administration Servers in the network can be upgraded using the remote installation task that uses the Administration Server installation package.

# Conclusion

This section summarizes the information in this document.

The document describes a simple scenario of deploying protection on an enterprise network, as well as the actions required to quickly deploy protection and start using Kaspersky Security Center. For more details on the features of Kaspersky Security Center and protection deployment scenarios please refer to the *Kaspersky Security Center Implementation Guide* and the *Kaspersky Security Center Administrator's Guide*.

# 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

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 10), 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).

# 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.

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

Apple and App Store are trademarks of Apple Inc. registered in the United States and elsewhere.

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.

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

Android is a trademark of Google, Inc.

Linux is a trademark owned by Linus Torvalds and registered in the U.S. and elsewhere.

Symbian is a trademark owned by the Symbian Foundation Ltd.