KASPERSKY lab

Kaspersky Security Center 10

Best Practices for Service Providers

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.

Document revision date: 12/7/2016

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

Table of Contents

About this document

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

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

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

In this section:

In this document

Kaspersky Security Center Best Practices document contains recommendations on how to deploy, configure, and use the application, as well as describes ways of resolving typical issues in the application operation.

Planning Kaspersky Security Center deployment (see page 9)

This section provides information about how to select a DBMS for Administration Server, provide Internet access to Administration Server, and handle the standard configurations of Kaspersky Security Center. This section provides information about the role of update agents and the role of the Administration Server hierarchy. It also provides information about how to handle virtual Administration Servers, install operating system images, and manage mobile devices.

Deployment and initial setup (see page 15)

This section provides information about Administration Server deployment, Network Agent and Anti-Virus deployment, and initial setup of Kaspersky Security Center. This section also provides information about backup and recovery of Administration Server settings, as well as the details of support of out-of-office users.

Routine use (see page 84)

This section provides information about the daily routine use of the application. This section provides information on how to manage remote access to devices.

Contacting the Technical Support Service (see page 102)

AO Kaspersky Lab (see page 105)

This section provides information about Kaspersky Lab.

Trademark notices (see page 107)

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.

Sample text	Document conventions description
Example: …	Examples are on a blue background under the heading "Example".
Update means... The *Databases are out of date* event occurs.	The following elements are italicized in the text: • New terms • Names of application statuses and events
Press **ENTER**. Press **ALT**+**F4**.	Names of keyboard keys appear in bold and are all uppercase. 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 The following message then appears: `Specify the date in MM:DD:YY format.`	The following types of text content are set off with a special font: • Text in the command line • Text of messages displayed on the screen by the application • 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.

Planning Kaspersky Security Center deployment

When planning the deployment of Kaspersky Security Center components on an enterprise network, you must take into account the size and scope of the project; specifically, the following factors:

- Total number of devices
- Number of MSP clients

One Administration Server can support a maximum of 50,000 devices. If the total number of devices in an enterprise network exceeds 50,000, multiple Administration Servers must be deployed on the MSP side and combined into a hierarchy for convenient centralized management.

Up to 200 virtual servers can be created on a single Administration Server, so an individual Administration Server is required for each 200 MSP clients.

At the stage of deployment planning, the assignment of the special certificate X.509 to the Administration Server must be considered. Assignment of the X.509 certificate to the Administration Server may be useful in the following cases (partial list):

- Inspecting secure socket layer (SSL) traffic by means of an SSL termination proxy, or for using a reverse proxy
- Specifying required values in certificate fields
- Providing the required encryption strength of a certificate.

See section Specifying the Administration Server certificate (on page 19).

In this section:

How to select a DBMS for the Administration Server

When selecting the database management system (DBMS) to be used by an Administration Server, you must take into account the number of devices covered by the Administration Server. For example, the DBMS Microsoft® SQL Server® 2008 R2 Express Edition that is shipped with Kaspersky Security Center can support only a single CPU and a maximum 1 GB RAM. The size of the database is limited to 10 GB. No DBMS can be used if the Administration Server covers more than 10,000 devices. If the Administration Server supports more than 10,000 devices, you must use SQL Server versions with fewer limitations: SQL Server Workgroup Edition, SQL Server® Web Edition, SQL Server Standard Edition, or SQL Server Enterprise Edition.

The same limitation is imposed if more than 50 devices are running in the network and Application Startup Control from Kaspersky Endpoint Security for Windows is used.

If the Administration Server covers 10,000 devices (or less), or if Application Startup Control is not used, you can also use MySQL 5.0 as the DBMS.

See also:

Hardware requirements for the DBMS and the Administration Server 91

Selecting a DBMS 18

Providing Internet access to the Administration Server

To allow devices in the client network to access the Administration Server over the Internet, you have to make available the following Administration Server ports:

- 13000 TCP—Administration Server TLS port for connecting Network Agents deployed in the client network
- 8061 TCP—HTTPS port for publishing stand-alone packages using Administration Console tools
- 8060 TCP—HTTP port for publishing stand-alone packages using Administration Console tools
- 13292 TCP—TLS port required only there are mobile devices that need to be managed

If you need to provide clients basic options of network administration through Web Console, you also have to open the following Web Console ports:

- 8081 TCP—HTTPS port
- 8080 TCP—HTTP port

Standard configuration of Kaspersky Security Center

One or several Administration Servers are deployed on the MSP side. The number of Administration Servers can be defined on the basis either of the presence of available hardware (see section “Hardware requirements for the DBMS and the Administration Server“ on page 91) or the number of MSP clients supported, or the total number of devices managed.

One Administration Server can support up to 50,000 devices. You must consider the possibility of increasing the number of managed devices in the near future: it may be useful to connect a slightly smaller number of devices to a single Administration Server.

Up to 200 virtual servers can be created on a single Administration Server, so an individual Administration Server is required for each 200 MSP clients.

If multiple Servers are used, it is recommended that you combine them into a hierarchy. Using an Administration Server hierarchy allows you to avoid dubbed policies and tasks, handle the whole set of managed devices, as if they are managed by a single Administration Server: i.e., search for devices, build selections of devices, and create reports.

On each virtual server that corresponds to an MSP client, you must assign one or several update agent(s). If MSP clients and the Administration Server are linked through the Internet, it may be useful to create an update relay task for the update agents, so that they will download updates directly from Kaspersky Lab servers, not from the Administration Server.

If some devices in the MSP client network have no direct Internet access, you have to switch the update agents to the connection gateway mode. In this case, Network Agents on devices in the MSP client network will be connected, for further synchronization, to the Administration Server—but through the gateway, not directly.

As the Administration Server, most probably, will not be able to poll the in the MSP client network, it may be useful to turn this function over to an update agent.

The Administration Server will not be able to send notifications to port 15000 UDP to managed devices located beyond NAT in the MSP client network. To resolve this issue, it may be useful to enable the mode of continuous connection to the Administration Server in the properties of devices acting as update agents and running in connection gateway mode (**Do not disconnect from the Administration Server** check box). The continuous connection mode is available if the total number of update agents does not exceed 300.

About update agents

Network Agent can be used as update agent. In this mode, Network Agent can perform the following functions:

- Distribute updates (these can be retrieved either from the Administration Server or from Kaspersky Lab servers). If the updates are from Kaspersky Lab servers, a relay task must be created for the device, which acts as the update agent.
- Install software (including initial deployment of Network Agents) on other devices.
- Scan the network to detect new devices and update information about existing ones. An update agent can apply the same network scanning methods as the Administration Server.

Deployment of update agents on an enterprise network pursues the following objectives.

- Reduce the load on the Administration Server if it functions as the update source.
- Optimize Internet traffic since, in this case, each device in the MSP client network does not have to access Kaspersky Lab servers or the Administration Server for updates.
- Provide the Administration Server access to devices beyond the NAT (relative to the Administration Server) of the MSP client network, which allows the Administration Server to perform the following actions:
  - Send notifications to devices over UDP.
  - Scan the network.
  - Perform initial deployment.

An update agent is assigned for an administration group. In this case, the update agent's scope includes all devices within the administration group and all of its subgroups. However, the device acting as the update agent may not be included in the administration group to which it has been assigned.

An update agent can be assigned by a connection gateway. In this case, devices in the update agent's scope will be connected to the Administration Server through the gateway, not directly. This mode can be useful in scenarios that do not allow the establishment of a direct connection between devices with Network Agent and an Administration Server.

See also:

Building a structure of administration groups and assigning update agents 28

Administration Server hierarchy

An MSP may run multiple Administration Servers. It can be inconvenient to administer several separate Administration Servers, so a hierarchy can be applied. A master/slave configuration for two Administration Servers provides the following options:

- A slave Administration Server inherits policies and tasks from the master Administration Server, thus preventing duplication of settings.
- Selections of computers on the master Administration Server can include devices from slave Administration Servers.
- Reports on the master Administration Server can contain data (including detailed information) from slave Administration Servers.

Virtual Administration Servers

On the basis of a physical Administration Server, multiple virtual Administration Servers can be created, which will be similar to slave Administration Servers.
Compared to the discretionary access model, which is based on access control lists (ACLs), the virtual Administration Server model is more functional and provides a larger degree of isolation. In addition to a dedicated structure of administration groups for assigned devices with policies and tasks, each virtual Administration Server features its own group of unassigned devices, own sets of reports, selected devices and events, installation packages, moving rules, etc. For maximum mutual isolation of MSP clients, we recommend that you choose virtual Administration Servers as the functionality to be used. In addition, creating a virtual Administration Server for each MSP client allows you to provide clients basic options of network administration through Kaspersky Security Center Web Console.

Virtual Administration Servers are very similar to slave Administration Servers, but with the following distinctions:

- A virtual Administration Server lacks most global settings and its own TCP ports.
- A virtual Administration Server has no slave Administration Servers.
- A virtual Administration Server has no other virtual Administration Servers.
- A physical Administration Server views devices, groups, events, and objects on managed devices (items in Quarantine, applications registry, etc.) of all its virtual Administration Servers.
- A virtual Administration Server can only scan the network with update agents connected.

Managing mobile devices with Kaspersky Endpoint Security for Android

Mobile devices with installed Kaspersky Endpoint Security for Android™ (hereinafter referred to as KES devices) are managed by means of the Administration Server. Kaspersky Security Center 10 Service Pack 1 (SP1) supports the following features for managing KES devices:

- Handling mobile devices as client devices:
  - Membership in administration groups
  - Statuses, events, reports, etc.
  - Modifying local settings and assigning policies for Kaspersky Endpoint Security for Android
- Sending commands in centralized mode
- Installing mobile apps packages remotely.

KES devices are serviced by the Administration Server through TLS, TCP port 13292.

See also:

Providing Internet access to the Administration Server 11

Defining the Administration Server certificate 19

Deployment and initial setup

Kaspersky Security Center is a distributed application. Kaspersky Security Center includes the following applications:

- Administration Server—The core component, designed for managing devices of an enterprise and storing data in a DBMS.
- Administration Console—The basic tool for the administrator. Administration Console is shipped together with Administration Server, but it can also be installed individually on one or several devices run by the administrator.
- Kaspersky Security Center Web Console is a web interface for Administration Server designed for basic operations. You have to install this component together with Administration Server if you need to provide MSP clients the basic options of network administration.
- Network Agent—Designed for managing the security application installed on a device, as well as collecting information about that device. Network Agents are installed on devices of an enterprise.

Deployment of Kaspersky Security Center on an enterprise network is performed as follows:

- Installation of Administration Server
- Installation of Kaspersky Security Center Web Console on the Administration Server device
- Installation of Administration Console on the administrator's device
- Installation of Network Agent and the security application on devices of the enterprise

In this section:

Installing Administration Server

This section contains recommendations on how to install Administration Server on a computer. This section also provides scenarios for using a shared folder on the Administration Server device in order to deploy Network Agent on client devices.

In this section:

Creating accounts for services of Administration Server

By default, the installer automatically creates non-privileged accounts for services of Administration Server. This behavior is the most convenient for Administration Server installation on an ordinary device.

However, installation of Administration Server on a domain controller or a failover cluster requires a different scenario:

1. In Active Directory®, create global domain groups under the names KLAdmins and KLOperators
2. Create non-privileged domain accounts for services of Administration Server and make them members of a global domain security group named KLAdmins
3. In the Administration Server installer, specify the domain accounts that have been created.

Selecting a DBMS

When installing Administration Server, you can select the DBMS that Administration Server will use. You can either install SQL Server Express Edition included in the distribution, or select an existing DBMS. The following table lists the valid DBMS options, as well as the restrictions on their use.

Table 2. Restrictions on DBMS

DBMS	Restrictions
SQL Server Express Edition included in the distribution kit of Kaspersky Security Center	Not recommended if you intend to run a single Administration Server for more than 10,000 devices or to use Application Startup Control.
Local SQL Server edition other than Express	No limitations.

DBMS	Restrictions
Remote SQL Server edition other than Express	Only valid if both devices are in the same Windows® domain. If the domains differ, a two-way trust relationship must be established between them.
Local or remote MySQL 5.0	Administration Server can cover a maximum of 10,000 devices if Application Startup Control is not used.

Concurrent use of the Server Express Edition DBMS by Administration Server and another application is strictly forbidden.

See also:

How to select a DBMS for the Administration Server 10

Specifying the address of the Administration Server

When installing Administration Server, you must specify the external address of the Administration Server. This address will be used as the default address when creating installation packages of Network Agent. After that, you will be able to change the address of the Administration Server host by using Administration Console tools; the address will not change automatically in Network Agent installation packages that have been already created.

Defining the Administration Server certificate

If necessary, you can assign a special certificate for Administration Server by using the command line utility klsetsrvcert.

When replacing the certificate, all Network Agents that were previously connected to Administration Server through SSL will lose their connection and will return "Administration Server authentication error".

Please note that the Administration Server certificate is often added to Network Agent packages when they are created. If this is the case, replacing the Administration Server certificate by means of the utility klsetsrvcert will not result in replacement of the Administration Server certificate in existing Network Agent packages.

It is useful to replace the certificate immediately after the installation of Administration Server and before the Quick Start Wizard completes.

For detailed information about the conditions that require certificate replacement see section "Planning the deployment taking into account an enterprise's organizational structure and network topology (see section "Planning Kaspersky Security Center deployment" on page 9).

To replace the certificate, you must create a new one (for example, by means of the enterprise PKI) in PKCS#12 format and pass it to the klsetsrvcert utility (see the table below for the values of the utility settings). The certificate specified with the utility must include the entire chain of trust.

Utility command line syntax:

klsetsrvcert [-l LOGFILE] -t TYPE [-p PASSWORD] -i FILE

Table 3. Values of the settings of klsetsrvcert utility

Setting	Value
-t TYPE	Type of the certificate to be replaced. Possible values of the setting TYPE: • C – Replace the certificate for ports 13000 and 13291; • CR – Replace the reserve certificate for ports 13000 and 13291; • M – Replace the certificate for mobile devices on port 13292.
-i FILE	Container with the certificate in PKCS#12 format (file with the extension .p12 or .pfx).

Setting	Value
-p PASSWORD	Password used for protection of the .p12 container with the certificate.
-l LOGFILE	Results output file. By default, the output is redirected into the standard output stream.

Initial setup

After Administration Server installation is complete, Administration Console launches and prompts you to perform the initial setup through the relevant wizard. When the Quick Start Wizard is running, the following policies and tasks are created in the root administration group:

- Policy of Kaspersky Endpoint Security
- Group task for updating Kaspersky Endpoint Security
- Group task for scanning a device with Kaspersky Endpoint Security
- Policy of Network Agent
- Vulnerability scan task (task of Network Agent)
- Updates installation and vulnerabilities fix task (task of Network Agent).

Policies and tasks are created with the default settings, which may turn out to be sub-optimal or even inadmissible for the organization. Therefore, you must check the properties of objects that have been created and modify them manually, if necessary.

This section provides information about the initial setup of policies, tasks, and other parameters of Administration Server.

In this section:

Manual setup of Kaspersky Endpoint Security policy

This section provides recommendations on how to configure the Kaspersky Endpoint Security policy, which is created by the Quick Start Wizard of Kaspersky Security Center.
Setup is performed in the policy properties window.

When editing a setting, please keep in mind that you must click the lock icon above the relevant setting in order to allow using its value on a workstation.

In this section:

Configuring the policy in the Anti-Virus protection section

Described below are additional setup actions, which we recommend that you perform in the policy properties window of Kaspersky Endpoint Security, in the **Anti-Virus protection** section.

Anti-Virus protection section, Firewall subsection

Check the list of networks in the policy properties. The list may not contain all networks.

► *To check the list of networks:*

1. In the policy properties window, find the **Anti-Virus protection** section and select the **Firewall** subsection.
2. In the **Available networks** section, click the **Settings** button.

   This opens the **Firewall** window. This window displays the list of networks on the **Networks** tab.

Anti-Virus protection section, File Anti-Virus subsection

Enabling the scanning of network drives can place a significant load on network drives. It is more convenient to perform indirect scanning, on file servers.

► *To disable scanning of network drives:*

1. In the policy properties window, find the **Anti-Virus protection** section and select the **File Anti-Virus** subsection.
2. In the **Security level** section, click the **Settings** button.
3. In the **File Anti-Virus** window that opens, on the **General** tab, clear the **All network drives** check box.

Configuring the policy in the Advanced Settings section

Described below are advanced setup actions, which we recommend that you perform in the policy properties window of Kaspersky Endpoint Security, in the **Advanced Settings** section.

Advanced Settings section, Reports and Storages subsection

In the **Inform Administration Server** section, please note the following settings:

- The **About vulnerabilities found** check box: This setting is primarily required for providing backward compatibility with Kaspersky Security Center 9. Detection of vulnerabilities is integrated into Kaspersky Security Center, starting from version 10. Therefore, if you use Administration Server and Network Agents of version 10 or later, make sure that this check box is cleared.

- **About started applications** check box: If this check box is selected, the Administration Server database saves information about all versions of all software modules on the networked devices. This information may require a significant amount of disk space in the Kaspersky Security Center database (dozens of gigabytes). Therefore, if the **About started applications** check box is still selected in the top-level policy, it must be cleared.

Advanced Settings section, Interface subsection

If the Anti-Virus protection in the enterprise network must be managed in centralized mode through Administration Console, you must disable the display of the Kaspersky Endpoint Security user interface on workstations (by clearing the **Display application interface** check box in the **Interaction with user** section), and enable password protection (by selecting the **Enable password protection** check box in the **Password protection** section).

Advanced Settings section, KSN Settings subsection

We recommend that you enable the use of a KSN proxy server (by selecting the **Use KSN proxy server** check box).

Configuring the policy in the Events section

In the **Events** section, you should disable the saving of any events on Administration Server, except for the following ones:

- On the **Info** tab:
  - Object disinfected
  - Object deleted
  - Application start prohibited in test mode;
  - Object moved to Quarantine
  - Object restored from Quarantine
  - Object backup copy created.
- On the **Warning** tab:
  - Self-Defense is disabled
  - Protection components are disabled
  - Incorrect reserve activation code
  - User has opted out of the encryption policy
  - Complaint of application startup blockage
  - Complaint of device access blockage
  - Complaint of web content access blockage
  - An application was detected that can be used by criminals.
- On the **Functional failure** tab:
  - Task settings error. Settings not applied
- On the **Critical event** tab:
  - Application autorun is disabled
  - Access blocked
  - Blocked

- Application start prohibited;
- Disinfection is not possible;
- End User License Agreement violated
- Could not load encryption module
- Cannot run two tasks at the same time
- Probably infected object detected
- Malicious object detected
- Active threat detected. Advanced Disinfection must be started;
- Previously opened phishing link detected
- Previously opened malicious link detected
- Network attack detected
- Not all components were updated
- Operation with the device prohibited
- Activation error
- Error enabling portable mode
- Error in interaction with Kaspersky Security Center
- Error disabling portable mode
- Application content modification error
- Error applying file encryption / decryption
- Policy cannot be applied
- Process terminated
- Network activity blocked
- Network update error.

Manual setup of the group update task for Kaspersky Endpoint Security

> Information from this subsection is only applicable to Kaspersky Security Center 10 MR1 and later versions.

If the Administration Server acts as the update source, the optimal and recommended schedule option for Kaspersky Endpoint Security 10 and later versions is **When new updates are downloaded to the repository** with the **Define task launch delay automatically** check box selected.

For a group update task in Kaspersky Endpoint Security version 8 you must explicitly specify the launch delay (1 hour or longer) and select the **Define task launch delay automatically** check box.

If a local task for downloading updates from Kaspersky Lab servers to the repository is created on each update agent, periodic scheduling will be optimal and recommended for the Kaspersky Endpoint Security group update task. In this case, the randomization interval value should be set on 1 hour.

Manual setup of the group task for scanning a device with Kaspersky Endpoint Security

The Quick Start Wizard creates a group task for scanning a device. By default, the task is assigned a **Run on Fridays at 7:00 PM** schedule with automatic randomization, and the **Run missed tasks** check box is cleared.

This means that if devices in an organization are shut down on Fridays, for example, at 6:30 PM, the device scan task will never run. You must set up the most convenient schedule for this task based on the workplace rules adopted in the organization.

Manual setup of the schedule of the vulnerability scan task

The Quick Start Wizard creates a group vulnerability scan task for Network Agent. By default, the task is assigned a **Run on Tuesdays at 7:00 PM** schedule with automatic randomization, and the **Run missed tasks** check box is selected.

If the organization's workplace rules provide for shutting down all devices at this time, the vulnerability scan task will run after the devices are turned on again, that is, on Wednesday morning. Such activity may be undesirable because a vulnerability scan may increase the load on CPUs and disk subsystems. You must set up the most convenient schedule for the vulnerability scan task based on the workplace rules adopted in the organization.

Manual setup of the group task for updates installation and vulnerabilities fix

The Quick Start Wizard creates a group task for updates installation and vulnerabilities fix for Network Agent. By default, the task is set up to run every day at 01:00 AM, with automatic randomization, and the **Run missed tasks** check box is cleared.

If the organization's workplace rules provide for shutting down devices overnight, the update installation will never run. You must set up the most convenient schedule for the vulnerability scan task based on the workplace rules adopted in the organization. It is also important to keep in mind that installation of updates may require restarting the device.

Building a structure of administration groups and assigning update agents

A structure of administration groups in Kaspersky Security Center performs the following functions:

- Sets the scope of policies.

  There is an alternate way of applying relevant collections of settings on devices, by using *policy profiles*. In this case, the scope of policies is set with tags, devices' locations in Active Directory organizational units, membership in Active Directory security groups, etc. (see section “Hierarchy of policies, using policy profiles“ on page 31).

- Sets the scope of group tasks.

There is an approach to defining the scope of group tasks that is not based on a hierarchy of administration groups: use of tasks for device selections and tasks for specific devices.

- Sets access rights to devices, virtual Administration Servers, and slave Administration Servers.
- Assigns update agents.

When building the structure of administration groups, you must take into account the topology of the enterprise network for the optimum assignment of update agents. The optimum distribution of update agents allows you to save traffic in the enterprise network.

Depending on the organizational chart and network topology adopted by the MSP client, the following standard configurations can be applied to the structure of administration groups:

- Single office
- Multiple small detached offices.

In this section:

Standard MSP client configuration: Single office

In a standard "single-office" configuration, all devices are within the enterprise network so they can "see" each other. The enterprise network may consist of a few separate parts (networks or network segments) linked by narrow channels.

The following methods of building the structure of administration groups are possible:

- Building the structure of administration groups taking into account the network topology. The structure of administration groups may not reflect the network topology with absolute precision. A match between the separate parts of the network and certain administration groups would be enough. You can use automatic assignment of update agents or assign them manually.

- Building the structure of administration groups, without taking the network topology into account. In this case, you must disable automatic assignment of update agents and then assign one or several devices to act as update agents for a root administration group in each of the separate parts of the network, for example, for the **Managed devices** group. All update agents will be at the same level and will feature the same scope spanning all devices in the enterprise network. In this case, each of Network Agents in version 10 SP1 or later will connect to the update agent that has the shortest route. The route to an update agent can be traced with the tracert utility.

When assigning update agents manually, you must assign 100 to 200 managed devices to a single update agent. Update agents must be powerful devices with a sufficient amount of free disk space (see section “Assessing the disk space for an update agent“ on page 92). Update agents must not be shut down frequently; sleep mode must be disabled on them.

Standard MSP client configuration: Multiple small isolated offices

This standard configuration provides for a number of small remote offices, which may be communicated with the head office via the Internet. Each remote office is located beyond NAT, that is, connection from one remote office to another is not possible because offices are isolated from one another.

The configuration must be reflected in the structure of administration groups: a separate administration group must be created for each remote office (groups **Office 1** and **Office 2** in the figure below).

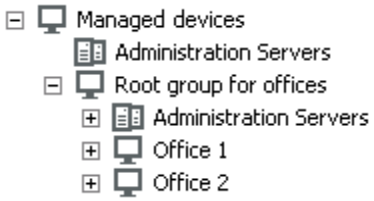

Figure 1. Remote offices are included in the administration group structure

One or multiple update agents must be assigned to each administration group corresponding to an office. Update agents must be devices at the remote office that have a sufficient amount of free disk space (see section "Assessing the disk space for an update agent" on page 92). Devices deployed in the **Office 1** group, for example, will access update agents assigned to the **Office 1** administration group.

If some users move between offices physically, with their laptops, you must select two or more devices (in addition to the existing update agents) in each remote office and assign them to act as update agents for a top-level administration group (**Root group for offices** in the figure above).

Example: A laptop is deployed in the **Office 1** administration group and then is moved physically to the office that corresponds to the **Office 2** administration group. After the laptop is moved, Network Agent attempts to access the update agents assigned to the **Office 1** group, but those update agents are unavailable. Then, Network Agent starts attempting to access the update agents that have been assigned to the **Root group for offices**. Because remote offices are isolated from one another, attempts to access update agents assigned to the **Root group for offices** administration group will only be successful when Network Agent attempts to access update agents in the **Office 2** group. That is, the laptop will remain in the administration group that corresponds to the initial office, but the laptop will use the update agent of the office where it is physically located at the moment.

Hierarchy of policies, using policy profiles

This section provides information about how to apply policies to devices in administration groups. This section also provides information about policy profiles supported in Kaspersky Security Center, starting from version 10 SP1.

In this section:

Hierarchy of policies

In Kaspersky Security Center, you use policies for defining a single collection of settings to multiple devices. For example, the policy scope of product P defined for administration group G includes managed devices with product P installed that have been deployed in group G and all of its subgroups, except for subgroups where the **Inherit from parent group** check box is cleared in the properties.

A policy differs from any local setting by "lock" icons next to its settings. If a setting (or a group of settings) is "locked" in the policy properties, you must, first, use this setting (or group of settings) when creating effective settings and, second, must write the settings or group of settings to the downstream policy.

Creation of the effective settings on a device can be described as follows: the values of all settings that have not been "locked" are taken from the policy, then they are overwritten with the values of local settings, and then the resulting collection is overwritten with the values of "locked" settings taken from the policy.

Policies of the same product affect each other through the hierarchy of administration groups: "Locked" settings from the upstream policy overwrite the same settings from the downstream policy.

There is a special policy for out-of-office users. This policy takes effect on a device when the device switches into out-of-office mode. Policies for out-of-office users do not affect other policies through the hierarchy of administration groups.

> The policy for out-of-office users will not be supported in further versions of Kaspersky Security Center. In future versions, policy profiles will be used instead of policies for out-of-office users.

Policy profiles

Applying policies to devices only through the hierarchy of administration groups may be inconvenient in many circumstances. It may be necessary to create several instances of a single policy that differ in one or two settings for different administration groups, and synchronize the contents of those policies in the future.

To help you avoid such problems, Kaspersky Security Center, starting from version 10 SP1, supports *policy profiles*. A policy profile is a named subset of policy settings. This subset is distributed on target devices together with the policy, supplementing it under a specific condition called the *profile activation condition*. Profiles only contain settings that differ from the "basic" policy, which is active on the client device (computer or mobile device). Activation of a profile modifies the policy settings that were active on the device before the profile was activated. Those settings take values that have been specified in the profile.

The following restrictions are currently imposed on policy profiles:

- A policy can include a maximum 100 profiles.
- A policy profile cannot contain other profiles
- A policy profile cannot contain notification settings.

Contents of a profile

A policy profile contains the following constituent parts:

- Name. Profiles with identical names affect each other through the hierarchy of administration groups with common rules.
- Subset of policy settings. Unlike the policy, which contains all the settings, a profile only contains settings that are actually required ("locked" settings).
- The activation condition is a logical expression with the device properties. A profile is active (supplements the policy) only when the profile activation condition becomes true. In all other cases, the profile is inactive and ignored. The following device properties can be included in that logical expression:
    - Status of out-of-office mode.
    - Properties of network environment: name of the active rule for Network Agent connection (see section “Configuring connection profiles for out-of-office users“ on page 73)

    - Presence or absence of specified tags on the device
    - Device’s allocation in an Active Directory organizational unit (OU): explicit (the device is right in the specified OU), or implicit (the device is in an OU, which is within the specified OU at any nesting level)
    - Device's membership in an Active Directory security group (explicit or implicit)
    - Device owner's membership in an Active Directory security group (explicit or implicit)
- Profile disabling check box. Disabled profiles are always ignored and their respective activation conditions are not verified.
- Profile priority. The activation conditions of different profiles are independent, so several profiles can be activated simultaneously. If active profiles contain non-overlapping collections of settings, no problems will arise. However, if two active profiles contain different values of the same setting, an ambiguity will occur. This ambiguity is to be avoided through profile priorities: The value of the ambiguous variable will be taken from the profile that has the higher priority (the one that is rated higher in the list of profiles).

Behavior of profiles when policies affect each other through the hierarchy

Profiles with the same name are merged according to the policy merge rules.
Profiles of an upstream policy have a higher priority than profiles of a downstream policy. If editing settings is prohibited in the upstream policy (it is "locked"), the downstream policy uses the profile activation conditions from the upstream one. If editing settings is allowed in the upstream policy, the profile activation conditions from the downstream policy are used.

Since a policy profile may contain the **Device is offline** property in its activation condition, profiles completely replace the feature of policies for out-of-office users, which will no longer be supported.

A policy for out-of-office users may contain profiles, but its profiles can only be activated after the device switches into out-of-office mode.

Tasks

Depending on the task scope, the following types of tasks are provided by Kaspersky Security Center:

- Local tasks—Created directly on managed devices. Local tasks can be modified either by the administrator on the Kaspersky Security Center side by using Administration Console tools, or by the user of a remote device (for example, through the security application interface). If a local task has been simultaneously modified by the administrator and the user of a managed device, the changes made by the administrator will take effect as they have a higher priority.

- Group tasks—Affect an administration group and all of its subgroups. Group tasks also affect (optionally) devices that have been connected to slave and virtual Administration Servers deployed in that group or any of its subgroups.

- Tasks for specific devices—Affect a limited set of devices that were specified when the task was created.

- Tasks for selections of devices—Affect devices that have been included in a specified selection. Over time, the scope of the task changes as the set of devices included in the selection change. A selection of devices can be made on the basis of device attributes, including software installed on a device, as well as on the basis of tags assigned to devices. The selection is the most flexible way of defining the scope of a task.

  > Tasks for selections of devices are always run upon a schedule by the Administration Server. These tasks cannot be run on devices that lack connection with the Administration Server. Tasks will not be run on the local time of a device; instead, they will be run on the local time of the Administration Server.

- Cluster tasks (server array tasks)—Affect the nodes of a specified cluster or a server array.

Device moving rules

We recommend that you automate the allocation of devices to administration groups on the virtual server that corresponds to an MSP client, using *device moving rules*. A device moving rule

consists of three main parts: name, execution condition (logical expression with device attributes), and target administration group. A rule moves a device to the target administration group if the device attributes meet the rule execution condition.

All device moving rules have priorities. The Administration Server checks the device attributes as to whether they meet the execution condition of each rule, in ascending order of priority. If the device attributes meet the execution condition of a rule, the device is moved to the target group, so the rule processing is complete for this device. If the device attributes meet the conditions of multiple rules, the device is moved to the target group of the rule with the highest priority (that is, has the highest rank in the list of rules).

Device moving rules can be created implicitly. For example, in the properties of an installation package or a remote installation task, you can specify the administration group to which the device must be moved after Network Agent is installed on it. Also, computer moving rules can be created explicitly by the administrator of Kaspersky Security Center, in the list of moving rules. The list is located in Administration Console, in the properties of the **Unassigned devices** group.

By default, a device moving rule is intended for one-time initial allocation of devices to administration groups. The rule moves devices from the **Unassigned devices** group only once. If a device once was moved by this rule, the rule will never move it again, even if you return the device to the **Unassigned devices** group manually. This is the recommended way of applying moving rules.

You can move devices that have already been allocated to some of the administration groups. To do this, in the properties of a rule, clear the **Move only devices added to none of the administration groups** check box.

Applying moving rules to devices that have already been allocated to some of the administration groups, significantly increases the load on the Administration Server.

You can create a moving rule that would affect a single device repeatedly.

We strongly recommend that you avoid moving a single device from one group to another repeatedly (for example, in order to apply a special policy to that device, run a special group task, or update the device through a specific update agent).

Such scenarios are not supported, because they increase the load on Administration Server and network traffic to an extreme degree. These scenarios also conflict with the operating principles of Kaspersky Security Center (particularly in the area of access rights, events, and reports). Here, another solution ought to be found, e.g., through the use of policy profiles (on page 33), tasks for selections of devices (see section “Tasks“ on page 35), through the assignment of Network Agents according to the standard scenario (see section “Building a structure of administration groups and assigning update agents“ on page 28), etc.

Software categorization

The main tool for monitoring the running of applications are Kaspersky Lab categories (hereinafter also referred to as KL categories). KL categories help Kaspersky Security Center administrators to simplify the support of software categorization and minimize traffic going to managed devices.

User categories must only be created for applications that cannot be classified in any of the existing KL categories (for example, for custom-made software). User categories are created on the basis of a product installation package (MSI) or a folder with installation packages.

If a large collection of software is available, which has not been categorized through KL categories, it may be useful to create an automatically updated category. The checksums of executable files will be automatically added to this category on every modification of the folder containing distribution packages.

No automatically updated categories of software can be created on the basis of the folders My Documents, %windir%, and %ProgramFiles%. The pool of files in these folders is subject to frequent changes, which leads to an increased load on Administration Server and increased network traffic. You must create a dedicated folder with the collection of software and periodically add new items to it.

Backup and restoration of Administration Server settings

Backup of the settings of Administration Server and its database is performed through the backup task and klbackup utility. A backup copy includes all the main settings and objects pertaining to the Administration Server, such as certificates, master keys for encryption of drives on managed devices, keys for various licenses, structure of administration groups with all of its contents, tasks, policies, etc. With a backup copy you can recover the operation of an Administration Server as soon as possible, spending from a dozen minutes to a couple of hours on this.

Never neglect regular backups of Administration Server using the standard backup task.

If no backup copy is available, a failure may lead to an irrevocable loss of certificates and all Administration Server settings. This will necessitate reconfiguring Kaspersky Security Center from scratch, and performing initial deployment of Network Agent on the enterprise network again. All master keys for encryption of drives on managed devices will also be lost, risking irrevocable loss of encrypted data on devices with Kaspersky Endpoint Security.

The Quick Start Wizard creates the backup task for Administration Server settings and sets it to run daily, at 3:00 AM. Backup copies are saved by default in the folder %ALLUSERSPROFILE%\Application Data\KasperskySC.

If an instance of Microsoft SQL Server installed on another device is used as the DBMS, you must modify the backup task by specifying a UNC path, which is available for writing by both the Administration Server service and the SQL Server service, as the folder to store backup copies. This requirement, which is not obvious, derives from a special feature of backup in the Microsoft SQL Server DBMS.

If a local instance of Microsoft SQL Server is used as the DBMS, it is also useful to save backup copies on a dedicated medium in order to secure them against damage together with Administration Server.

Because a backup copy contains important data, the backup task and klbackup utility provide for password protection of backup copies. By default, the backup task is created with a blank password. You must set a password in the properties of the backup task. Neglecting this requirement causes a situation where all keys of Administration Server certificates, keys for licenses, and master keys for encryption of drives on managed devices remain unencrypted.

In addition to the regular backup, you must also create a backup copy prior to every significant change, including installation of Administration Server upgrades and patches.

To minimize the size of backup copies, select the **Compress backup copies** (**Compress backup**) check box in the SQL Server settings.

Restoration from a backup copy is performed with the utility klbackup on an operable instance of Administration Server that has just been installed and has the same version (or later) for which the backup copy was created.

The instance of Administration Server on which the restoration is to be performed, must use a DBMS of the same type (same SQL Server or MySQL) and the same (or later) version. The version of Administration Server can be the same (with an identical or later patch), or later.

This section describes standard scenarios for restoring settings and objects of Administration Server.

In this section:

A device with Administration Server is inoperable

If a device with Administration Server is inoperable due to a failure, you are recommended to perform the following actions:

- The new Administration Server must be assigned the same address: NetBIOS name, FQDN, or static IP (depending on which of them was set when Network Agents were deployed).
- Install Administration Server, using a DBMS of the same type, of the same (or later) version. You can install the same version of Server with the same (or later) patch, or a later version. After installation, do not perform the initial setup through the Wizard.
- In the **Start** menu, run the utility klbackup and perform restoration.

The settings of Administration Server or the database are corrupted

If Administration Server is inoperable due to corrupted settings or database (e.g., after a power surge), you are recommended to use the following restoration scenario:

1. Scan the file system on the damaged device.
2. Uninstall the inoperable version of Administration Server.
3. Reinstall Administration Server, using a DBMS of the same type and of the same (or later) version. You can install the same version of Server with the same (or later) patch, or a later version. After installation, do not perform the initial setup through the Wizard.
4. In the **Start** menu, run the utility klbackup and perform restoration.

It is strictly prohibited to restore Administration Server in any way other than through the klbackup utility.

Any attempts to restore Administration Server through third-party software will inevitably lead to desynchronization of data on nodes of the distributed application Kaspersky Security Center and, consequently, to improper functioning of the product.

Deploying Network Agent and a security application

To manage devices in an enterprise, you have to install Network Agent on each of them. Deployment of distributed Kaspersky Security Center on enterprise devices normally begins with installation of Network Agent on them.

In this section:

Initial deployment

If a Network Agent has already been installed on a device, remote installation of applications on that device is performed through this Network Agent. The distribution package of an application to be installed is transferred over communication channels between Network Agents and Administration Server, along with the installation settings defined by the administrator. To transfer the distribution package, you can use relay distribution nodes, that is, update agents, multicast delivery, etc. For more details on how to install applications on managed devices with Network Agent already installed, see below in this section.

You can perform initial installation of Network Agent on devices running Windows, using one of the following methods:

- Using third-party tools for remote installation, through the Microsoft Windows Group Policy mechanism: with the standard Microsoft Windows group policy management tools
- Through the Microsoft Windows Group Policy mechanism
- In forced mode, using special options in the remote installation task of Kaspersky Security Center.
- By sending device users links to stand-alone packages generated by Kaspersky Security Center. Stand-alone packages are executable modules that contain the distribution packages of selected applications with their settings defined.
- Manually, by running application installers on devices.

On platforms other than Microsoft Windows, you have to perform initial installation of Network Agent on managed devices either through the existing third-party tools, or manually, by sending users an archive with a pre-configured distribution package. You can upgrade Network Agent to a new version or install other Kaspersky Lab applications on non-Windows platforms, using Network Agents (already installed on devices) to perform remote installation tasks. In this case, installation is identical to that on computers with Windows installed.

When selecting a method and a strategy for deployment of products in a managed network, you must consider a number of factors (partial list):

- Configuration of the enterprise network (see section "Standard configurations of Kaspersky Security Center" on page 12)
- Total number of devices
- Presence of Windows domains in the managed network, possibility to modify Active Directory group policies in those domains
- Awareness of the user account(s) with local administrator rights on devices on which initial deployment of Kaspersky Lab applications has been planned (i.e., availability of a domain user account with local administrator rights, or presence of unified local user accounts with administrator rights on those devices)
- Connection type and bandwidth of network channels between the Administration Server and MSP client networks, as well as the bandwidth of channels inside those networks
- Security settings applied on remote devices at the start of deployment (such as use of UAC and Simple File Sharing mode)

Configuring installers

Before starting deployment of Kaspersky Lab applications on a network, you must specify the installation settings, that is, those defined during the application installation. When installing Network Agent, you should specify, at a minimum, an address for connection to the Administration Server and the proxy settings; some advanced settings may also be required.
Depending on the installation method that you have selected, you can define settings in different ways. In the simplest case (manual interactive installation on a selected device), all relevant settings can be defined through the user interface of the installer, so, in some cases, initial deployment can even be performed by sending users a link to the Network Agent distribution package together with the settings (Administration Server address, etc.) that the user must enter in the installer interface (see section "Options for manual installation of applications" on page 52).

This method is not recommended for use since it is inconvenient for users, entailing a high risk of errors when defining settings manually; it is also non-usable with non-interactive silent installation of applications on device groups. In general, the administrator must specify values

for settings in centralized mode; those values can subsequently be used for creation of stand-alone packages. Stand-alone packages are self-extracting archives that contain distribution packages with settings defined by the administrator. Stand-alone packages can be located on resources that allow both downloading by end users (for example, on Kaspersky Security Center Web Server) and non-interactive installation on selected networked devices.

Installation packages

The first and main method of defining the installation settings of applications is all-purpose and thus suitable for all installation methods, both with Kaspersky Security Center tools, and with most third-party tools. This method consists of creating installation packages of applications in Kaspersky Security Center.

Installation packages are generated using the following methods:

- Automatically, from specified distribution packages, on the basis of included *descriptors* (files with .kud extension that contain rules for installation and results analysis, and other information)
- From the executable files of installers or from installers in Microsoft Windows Installer (*.msi) format are for standard or supported applications.

Generated installation packages are organized hierarchically as folders with nested subfolders and files. In addition to the original distribution package, an installation package contains editable settings (including the installer's settings and rules for processing such cases as necessity of restarting the operating system in order to complete installation), as well as minor auxiliary modules.

Values of installation settings that are specific for a selected application to be supported can be specified in the Administration Console user interface when creating an installation package (more settings can be found in the properties of an installation package that has already been created). When performing remote installation of applications through Kaspersky Security Center tools, installation packages are delivered to target devices so that running the installer of an application makes all administrator-defined settings available for it. When using third-party tools for installation of Kaspersky Lab applications, you only have to ensure the availability of the entire installation package on the target device, that is, the availability of the distribution package and its settings. Installation packages are created and stored by Kaspersky Security Center in a dedicated subfolder of the shared data folder.

Do not specify any details of privileged user accounts in the settings of installation packages.

For details on how to use this method of defining the settings for Kaspersky Lab applications before deploying them with third-party tools, see section "Deployment using group policies of Microsoft Windows" (see section "Deployment using group policies of Microsoft Windows" on page 47).

Immediately after Kaspersky Security Center installation, a few installation packages are automatically generated; they are ready for installation and include Network Agent packages and security application packages for Microsoft Windows.

In some cases, using installation packages for deployment of applications in an MSP client network implies the need to create installation packages on virtual Servers that correspond to MSP clients. Creating installation packages on virtual Servers allows you to use different installation settings for different MSP clients. In the first instance, this is useful when handling Network Agent installation packages since Network Agents deployed in the networks of different MSP clients use different addresses to connect to the Administration Server. Actually, the connection address determines the Server to which Network Agent connects.

In addition to the possibility to create new installation packages immediately on a virtual Administration Server, the main operation mode for installation packages on virtual Administration Servers is the “relaying” of installation packages from the master Administration Server to virtual ones. You can relay selected (or all) installation packages to selected virtual Administration Servers (including all Servers within a selected administration group) using the corresponding Administration Server task. Also, you can select the list of installation packages of the master Administration Server when creating a new virtual Administration Server. The packages that you have selected will be immediately relayed to a newly created virtual Administration Server.

When relaying an installation package, its contents are not copied entirely. The file repository on a virtual Administration Server, which corresponds to the installation package being relayed, only stores files of settings that are specific for that virtual Server. The main part of the installation package (including the distribution package of the application being installed) remains unchanged; it is stored only in the master Administration Server repository. This allows you to increase the system performance dramatically and reduce the required disk volume. When handling installation packages relayed to virtual Administration Servers (i.e., when running remote installation tasks or creating stand-alone installation packages), the data from the original

installation package of the master Administration Server is “merged” with the settings files, which correspond to the relayed package on the virtual Administration Server.

> Although the license key for an application can be set in the installation package properties, it is advisable to avoid this license distribution method because it is easy to accidentally obtain read access to files in the folder. You should use automatically distributed keys or product installation tasks for keys.

MSI properties and transform files

Another way of configuring installation on Windows platform is to define MSI properties and transform files. This method can be used when performing installation through third-party tools intended for installers in Microsoft Installer format (see section «Configuring installers» on page 59), as well as when performing installation through Windows group policies using standard Microsoft tools or other third-party tools designed for handling Windows group policies.

Deployment with third-party tools for remote installation of applications

When any tools for remote installation of applications (such as Microsoft System Center) are available in an enterprise, it is convenient to perform initial deployment by using those tools.

The following actions must be performed:

- Select the method for configuring installation that best suits the deployment tool to be used.
- Define the mechanism for synchronization between the modification of the settings of installation packages (through the Administration Console interface) and the operation of selected third-party tools used for deployment of applications from installation package data.

See also:

Configuring installers..... 59

General information about the remote installation tasks in Kaspersky Security Center

Kaspersky Security Center provides a broad range of methods for remote installation of applications, which are implemented as remote installation tasks. You can create a remote installation task both for a specified administration group and for specific devices or a selection of devices (such tasks are displayed in Administration Console, in the **Tasks** folder).
When creating a task, you can select installation packages (those of Network Agent and / or another application) to be installed within this task, as well as specify certain settings that define the method of remote installation.

> Tasks for administration groups affect both devices included in a specified group and all devices in all subgroups within that administration group. A task covers devices of slave Administration Servers included in a group or any of its subgroups if the corresponding setting is enabled in the task.

Tasks for specific devices refresh the list of client devices at each run in accordance with the selection contents at the moment the task starts. If a selection includes devices that have been connected to slave Administration Servers, the task will run on those devices, too. For details on those settings and installation methods see below in this section.

> To ensure a successful operation of a remote installation task on devices connected to slave Administration Servers, you must use the relaying task to relay installation packages used by your task to corresponding slave Administration Servers in advance.

Deployment using group policies of Microsoft Windows

It is recommended that you perform the initial deployment of Network Agents through Microsoft Windows group policies if the following conditions are met:

- This device is member of an Active Directory domain.
- Access to the domain controller is granted with the administrator rights, which allow you to create and modify Active Directory group policies.

- Configured installation packages can be moved to the network hosting target managed devices (to a shared folder that is available for reading by all target devices).
- The deployment scheme allows you to wait for the next routine restart of target devices before starting deployment of Network Agents on them (or you can force a Windows group policy to be applied to those devices).

This deployment scheme consists of the following:

- The application distribution package in Microsoft Installer format (MSI package) is located in a shared folder (a folder where the LocalSystem accounts of target devices have read permissions).
- In the Active Directory group policy, an installation object is created for the distribution package.
- The installation scope is set by specifying the organizational unit (OU) and/or the security group, which includes the target devices.
- The next time a target device logs in to the domain (before device users log in to the system), all installed applications are checked for the presence of the required application. If the application is not found, the distribution package is downloaded from the resource specified in the policy and is then installed.

An advantage of this deployment scheme is that assigned applications are installed on target devices while the operating system is loading, that is, even before the user logs in to the system. Even if a user with sufficient rights removes the application, it will be reinstalled at the next launch of the operating system. This deployment scheme's shortcoming is that changes made by the administrator to the group policy will not take effect until the devices are restarted (if no additional tools are involved).

You can use group policies to install both Network Agent and other applications if their respective installers are in Windows Installer format.

Besides, when you select this deployment method, you have to assess the load on the file resource from which files will be copied to target devices after you apply the Windows group policy. You also have to choose the method of delivering the configured installation package to that resource, as well as the method of synchronizing the relevant changes in its settings.

Handling Microsoft Windows policies through the remote installation task of Kaspersky Security Center

This deployment method is only available if access to the controller of the domain, which contains the target devices, is possible from the Administration Server device, while the shared folder of the Administration Server (the one storing installation packages) is accessible for reading from target devices. Owing to the above reasons, this deployment method is not viewed as applicable to MSP.

Unassisted installation of applications through policies of Microsoft Windows

The administrator can create objects required for installation in a Windows group policy on his or her own behalf. In this case, you have to upload the packages to a stand-alone file server and provide a link to them.

The following installation scenarios are possible:

- The administrator creates an installation package and sets up its properties in Administration Console. Then the administrator copies the entire EXEC subfolder of this package from the shared folder of Kaspersky Security Center to a folder on a dedicated file resource of the enterprise. The group policy object provides a link to the msi file of this package stored in a subfolder on the dedicated file resource of the enterprise.

- The administrator downloads the application distribution package (including that of Network Agent) from the Internet and uploads it to the dedicated file resource of the enterprise. The group policy object provides a link to the msi file of this package stored in a subfolder on the dedicated file resource of the enterprise. The installation settings are defined by configuring the MSI properties or by configuring MST transform files (see section "Configuring installers" on page 59).

Forced deployment through the remote installation task of Kaspersky Security Center

If you have a user account(s) with local administrator rights on target devices, and if at least one device with Network Agent installed acts as the update agent in each subnet of target devices (see section "About update agents" on page 13), you can force installation of the selected installation packages through the remote installation task provided by Kaspersky Security Center.

In this case, you can specify target devices either explicitly (with a list), or by selecting the Kaspersky Security Center administration group to which they belong, or by creating a selection of devices based upon a specific criterion. The installation start time is defined by the task schedule. If the **Run missed tasks** setting is enabled in the task properties, the task can be run either immediately after target devices are turned on, or when they are moved to the target administration group.

Forced installation consists of delivery of installation packages to update agents, subsequent copying of files to the admin$ resource on each of the target devices, and remote registration of supporting services on those devices. Delivery of installation packages to update agents is performed through a Kaspersky Security Center feature that ensures network interaction. The following conditions must be met in this case:

- Target devices must be accessible from the update agent side.
- Name resolution for target devices must function properly in the network.
- The administrative shares (admin$) must remain enabled on target devices.
- The Server system service must be running on target devices (by default, it is running).
- The following ports must be opened on target devices to allow remote access through Windows tools: TCP 139, TCP 445, UDP 137, UDP 138.
- Simple File Sharing mode must be disabled on target devices.
- On target devices, the access sharing and security model must be set as *Classic – local users authenticate as themselves*, it can be in no way *Guest only – local users authenticate as Guest*.
- Target devices must be members of the domain, or uniform accounts with administrator rights must be created on target devices in advance.

Devices in workgroups can be adjusted in accordance with the above requirements by using the riprep.exe utility, which is described on Kaspersky Lab Technical Support website (http://support.kaspersky.com/7434).

During installation on new devices that have not yet been allocated to any of the Kaspersky Security Center administration groups, you can open the remote installation task properties and specify the administration group to which devices will be moved after Network Agent installation.

When creating a group task, keep in mind that each group task affects all devices in all nested groups within a selected group. Therefore, you must avoid duplicating installation tasks in subgroups.

Automatic installation is a simplified way to create tasks for forced installation of applications. To do this, open the administration group properties, open the list of installation packages and select the ones that must be installed on devices in this group. As a result, the selected installation packages will be automatically installed on all devices in this group and all of its subgroups. The time interval over which the packages will be installed depends on the network throughput and the total number of networked devices.

To allow forced installation, you should make sure that update agents are present in each of the isolated subnets hosting target devices.

Note that this installation method places a significant load on devices acting as update agents. Therefore, it is recommended that you select powerful devices with high-performance storage units as update agents. Moreover, the free disk space in the partition with the folder *%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit* must exceed, by many times, the total size of the distribution packages of installed applications (see section "Assessing the disk space for an update agent" on page 92).

Running stand-alone packages created by Kaspersky Security Center

The above-described methods of initial deployment of Network Agent and other applications cannot always be implemented because it is not possible to meet all of the applicable conditions. In such cases, you can create a common executable file called a *stand-alone installation package* through Kaspersky Security Center, using installation packages with the relevant installation settings that have been prepared by the administrator. A stand-alone installation package can be published either on an internal Web Server (included in Kaspersky Security Center) if this is deemed reasonable (outside access to that Web Server has been configured for target device users), or on an exclusively deployed Web Server included in Kaspersky Security Center 10 Web Console. You can also copy stand-alone packages to another Web Server.

You can use Kaspersky Security Center to send selected users an email message containing a link to the stand-alone package file on the currently used Web Server, prompting them to run the file

(either in interactive mode, or with the "-s" key for silent installation). You can attach the stand-alone installation package to an email message and then send it to the users of devices that have no access to the Web Server. The administrator can also copy the stand-alone package to an external device, deliver it to a relevant device, and then run it later.

You can create a stand-alone package from a Network Agent package, a package of another application (for example, the security application), or both. If the stand-alone package has been created from Network Agent and another application, installation starts with Network Agent.

When creating a stand-alone package with Network Agent, you can specify the administration group to which new devices (those that have not been allocated to any of the administration groups) will be automatically moved when Network Agent installation completes on them.

Stand-alone packages can run in interactive mode (by default), displaying the result for installation of applications they contain, or they can run in silent mode (when run with the key "-s"). Silent mode can be used for installation from scripts, for example, from scripts configured to run after an operating system image is deployed. The result of installation in silent mode is determined by the return code of the process.

Options for manual installation of applications

Administrators or experienced users can install applications manually in interactive mode. They can use either original distribution packages or installation packages generated from them and stored in the shared folder of Kaspersky Security Center. By default, installers run in interactive mode and prompt users for all required values. However, when running the process setup.exe from the root of an installation package with the key "-s", the installer will be running in silent mode and with the settings that have been defined when configuring the installation package.

> When running setup.exe from the root of an installation package, the package will first be copied to a temporary local folder, and then the application installer will be run from the local folder.

Remote installation of applications on devices with Network Agent installed

If an operable Network Agent connected to the master Administration Server (or to any of its slave Servers) is installed on a device, you can upgrade Network Agent on this device, as well as install, upgrade, or remove any supported applications through Network Agent.

You can enable this option by selecting the **Using Network Agent** check box in the properties of the remote installation task (see section "General information about the tasks for remote installation of applications in Kaspersky Security Center" on page 47).

If this check box is selected, installation packages with installation settings defined by the administrator will be transferred to target devices over communication channels between Network Agent and the Administration Server.

To optimize the load on the Administration Server and minimize traffic between the Administration Server and target devices, it is useful to assign update agents in every remote network or in every broadcasting domain (see sections "About update agents (see section "About update agents" on page 13) and Building a structure of administration groups and assigning update agents (on page 28)). In this case, installation packages and the installer settings are distributed from the Administration Server to target devices through update agents.

Moreover, you can use update agents for broadcasting (multicast) delivery of installation packages, which allows reducing network traffic significantly when deploying applications.

When transferring installation packages to target devices over communication channels between Network Agents and the Administration Server, all installation packages that have been prepared for transfer will also be cached in the %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\FTServer folder. When using multiple large installation packages of various types and involving a large number of update agents, the size of this folder may increase dramatically.

Files cannot be deleted from the FTServer folder manually. When original installation packages are deleted, the corresponding data will be automatically deleted from the FTServer folder.

All data received on the update agents side are saved to the %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\$FTClTmp folder.

Files cannot be deleted from the $FTCITmp folder manually. As tasks using data from this folder complete, the contents of this folder will be deleted automatically.

Because installation packages are distributed over communication channels between Administration Server and Network Agents from an intermediate repository in a format optimized for network transfers, no changes are allowed in installation packages stored in the original folder of each installation package. Those changes will not be automatically registered by Administration Server. If you need to modify the files of installation packages manually (although you are recommended to avoid this scenario), you must edit any of the settings of an installation package in Administration Console. Editing the settings of an installation package in Administration Console causes Administration Server to update the package image in the cache that has been prepared for transfer to target devices.

Managing restarts of target devices in the remote installation task

Devices often need a restart to complete the remote installation of applications (particularly on Windows).

If you use the remote installation task of Kaspersky Security Center, in the New Task Wizard or in the properties window of the task that has been created (**OS restart** section), you can select the action to perform when a restart is required:

- **Do not restart device**. In this case, no automatic restart will be performed. To complete the installation, you must restart the device (for example, manually or through the device management task). Information about the required restart will be saved in the task results and in the device status. This option is suitable for installation tasks on servers and other devices where continuous operation is critical.
- **Restart the device** In this case, the computer is always restarted automatically if a restart is required for completion of the installation. This option is useful for installation tasks on devices that provide for regular pauses in their operation (shutdown or restart).
- **Prompt user for action**. In this case, the restart reminder is displayed on the screen of the client device, prompting the user to restart it manually. Some advanced settings can be defined for this option: text of the message for the user, message display frequency, and time interval after which the restart will be forced (without the user's confirmation).

The **Prompt user for action** is the most suitable for workstations where users need a possibility of selecting the most convenient time for a restart.

Suitability of databases updating in an installation package of an anti-virus application

Before starting the protection deployment, you must keep in mind the possibility of updating anti-virus databases (including modules of automatic patches) shipped together with the distribution package of the security application. It is useful to update the databases in the installation package of the application before starting the deployment (for example, by using the corresponding command in the context menu of a selected installation package). This will reduce the number of restarts required for completion of protection deployment on target devices. If your remote installation involves installation packages that have been relayed to virtual Servers from the master Administration Server, you only need to update databases in the original package on the master Server. In this case, you do not have to update databases in relayed packages on virtual Servers.

Selecting a method for uninstalling incompatible applications when installing a Kaspersky Lab security application

Installation of Kaspersky Lab security applications through Kaspersky Security Center may require removal of third-party software incompatible with the application being installed. There are two main ways of removing the third-party applications.

Automatic removal of incompatible applications using the installer

This is supported by various types of installation. Before the security application installation, all incompatible applications are removed automatically if the properties window of the installation package of this security application (**Incompatible applications** section) has the **Uninstall incompatible applications automatically** check box selected.

Removing incompatible applications through a dedicated task

To remove incompatible applications, use the **Uninstall application remotely** task. This task should be run on devices before the security application installation task. For example, in the installation task, you can select the schedule type **On completing another task** where the other task is **Uninstall application remotely**.

This method of uninstallation is useful when the security application installer cannot properly remove an incompatible application.

Using tools for remote installation of applications in Kaspersky Security Center for running relevant executable files on managed devices

Using the New Package Wizard, you can select any executable file and define the settings of the command line for it. For this you can add to the installation package either the selected file itself or the entire folder in which this file is stored. Then you must create the remote installation task and select the installation package that has been created.

While the task is running, the specified executable file with the defined settings of the command prompt will be run on target devices.

If you use installers in Microsoft Windows Installer (msi) format, Kaspersky Security Center analyzes the installation results by means of standard tools.

If a Systems Management license is available, Kaspersky Security Center (when creating an installation package for any supported application in the corporate environment) also uses rules for installation and analysis of installation results that are in its updatable database.

Otherwise, the default task for executable files waits for the completion of the running process, and of all its child processes. After completion of all of the running processes, the task will be completed successfully regardless of the return code of the initial process. To change such behavior of this task, before creating the task, you have to manually modify the .kud file that was generated by Kaspersky Security Center in the folder of the newly created installation package.

For the task not to wait for the completion of the running process, set the value of the Wait setting to 0 in the [SetupProcessResult] section:

Example:

[SetupProcessResult]

Wait=0

For the task to wait only for the completion of the running process on Windows, not for the completion of all child processes, set the value of the WaitJob setting to 0 in the [SetupProcessResult], section, for example:

Example:

[SetupProcessResult]

WaitJob=0

For the task to complete successfully or return an error depending on the return code of the running process, list successful return codes in the [SetupProcessResult_SuccessCodes], section, for example:

Example:

[SetupProcessResult_SuccessCodes]

0=

3010=

In this case, any code other than those listed will result in an error returned.

To display a string with a comment on the successful completion of the task or an error in the task results, enter brief descriptions of errors corresponding to return codes of the process in the [SetupProcessResult_SuccessCodes] and [SetupProcessResult_ErrorCodes] sections, for example:

Example:

[SetupProcessResult_SuccessCodes]

0= Installation completed successfully

3010=A restart is required to complete the installation

[SetupProcessResult_ErrorCodes]

1602=Installation canceled by the user

1603=Fatal error during installation

To use Kaspersky Security Center tools for managing the device restart (if a restart is required to complete an operation), list the return codes of the process that indicate that a restart must be performed, in the [SetupProcessResult_NeedReboot] section:

Example:

[SetupProcessResult_NeedReboot]

3010=

Monitoring the deployment

To monitor the Kaspersky Security Center deployment and make sure that a security application and Network Agent are installed on managed devices, you have to check the traffic light in the **Deployment** section. This traffic light is located in the workspace of the Administration Server node in the main window of Administration Console (see section "Traffic lights in Administration Console" on page 84). The traffic light reflects the current deployment status. The number of devices with Network Agent and security applications installed is displayed next to the traffic light. When any installation tasks are running, you can monitor their progress here. If any installation errors occur, the number of errors is displayed here. You can view the details of any error by clicking the link.

You can also use the deployment chart in the workspace of the **Managed devices** folder on the **Groups** tab. The chart reflects the deployment process, showing the number of devices without Network Agent, with Network Agent, or with Network Agent and a security application.

For more details on the progress of the deployment (or the operation of a specific installation task) open the results window of the relevant remote installation task: Right-click the task and select **Results** in the context menu. The window displays two lists: the upper one contains the task statuses on devices, while the lower one contains task events on the device that is currently selected in the upper list.

Information about deployment errors are added to the Kaspersky Event Log on Administration Server. Information about errors is also available in the corresponding selection of events in the **Reports and notifications** folder, the **Events** subfolder.

Configuring installers

This section provides information about the files of Kaspersky Security Center installers and the installation settings, as well as recommendations on how to install Administration Server and Network Agent in silent mode.

In this section:

General information

Installers of the components of Kaspersky Security Center 10 (Administration Server, Network Agent, and Administration Console) are built on Windows Installer technology. An msi package is the core of an installer. This format of packaging allows using all of the advantages provided by Windows Installer: scalability, availability of a patching system, transformation system, centralized installation through third-party solutions, and transparent registration with the operating system.

Installation in silent mode (with a response file)

The installers of Administration Server and Network Agent have the feature of working with the response file (ss_install.xml), where the settings for installation in silent mode without user participation are integrated. The ss_install.xml file is located in the same folder as the msi package; it is used automatically during installation in silent mode. The silent installation mode is enabled with the command line key "/s".

An overview of an example run follows:

```
setup.exe /s
```

The ss_install.xml file is an instance of the internal format of settings of the Kaspersky Security Center installer. Distribution packages contain the ss_install.xml file with the default settings.

> Please do not modify ss_install.xml manually. This file can be modified through the tools of Kaspersky Security Center when editing the settings of installation packages in Administration Console.

Installation in silent mode (without a response file)

You can install Network Agent with a single msi package, specifying the values of MSI properties in the standard way. This scenario allows Network Agent to be installed by using group policies. To avoid conflicts between settings defined through MSI properties and settings defined in the response file, you can disable the response file by setting the property DONT_USE_ANSWER_FILE=1. An example of a run of the Network Agent installer with an msi package is as follows.

Example:

msiexec /i "Kaspersky Network Agent.msi" /qn DONT_USE_ANSWER_FILE=1 SERVERADDRESS=kscserver.mycompany.com

You can also define the installation settings for an msi package by preparing the response file in advance (one with the .mst extension). This command appears as follows:

Example:

msiexec /I "Kaspersky Network Agent.msi" /qn TRANSFORMS=test.mst;test2.mst

You can specify several response files in a single command.

Partial installation configuration through setup.exe

When running installation of products through setup.exe, you can add the values of any properties of MSI to the msi package.

This command appears as follows:

Example:

/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"

Administration Server installation settings

The table below describes the MSI properties that you can configure when installing Administration Server. All of the settings are optional, except for EULA.

Table 4. Properties of MSI

MSI property	Description	Available values
EULA	Acceptance of the licensing terms (required)	• 1 • Null
INSTALLATIONMODETYPE	Type of Administration Server installation	• Standard • Custom
INSTALLDIR	Product installation folder	

MSI property	Description	Available values
ADDLOCAL	List of components to install (separated by commas)	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. Minimum list of components sufficient for proper Administration Server installation: `ADDLOCAL=CSAdminKitServer,CSAdminKitConsole,KSNProxy,Microsoft_VC90_CRT_x86,Microsoft_VC100_CRT_x86`
NETRANGETYPE	Network Size	• NRT_1_100—From 1 to 100 devices • NRT_100_1000—From 101 to 1000 devices • NRT_GREATER_1000—1001+ devices
SRV_ACCOUNT_TYPE	Way of specifying the user for the operation of the Administration Server service	• SrvAccountDefault – User account will be created automatically • SrvAccountUser—User account is defined manually
SERVERACCOUNTNAME	User name for the service	
SERVERACCOUNTPWD	User password for the service	
DBTYPE		• MySQL • MSSQL
MYSQLSERVERNAME	Full name of MySQL server	

MSI property	Description	Available values
MYSQLSERVERPORT	Number of port for connection to MySQL server	
MYSQLDBNAME	Name of MySQL server database	
MYSQLACCOUNTNAME	User name for connection to MySQL server database	
MYSQLACCOUNTPWD	User password for connection to MySQL server database	
MSSQLCONNECTIONTYPE	Type of use of MSSQL database	• InstallMSSEE – Install from a package • ChooseExisting—Use the installed server
MSSQLSERVERNAME	Full name of SQL Server instance	
MSSQLDBNAME	Name of SQL server database	
MSSQLAUTHTYPE	Method of authentication for connection to SQL Server	• Windows • SQLServer
MSSQLACCOUNTNAME	User name for connection to SQL Server in SQLServer mode	

MSI property	Description	Available values
MSSQLACCOUNTPWD	User password for connection to SQL Server in SQLServer mode	

CREATE_SHARE_TYPE	Method of specifying the shared folder	• Create—Create a new shared folder. In this case, the following properties must be defined:
		  • SHARELOCALPATH – path to a local folder
		  • SHAREFOLDERNAME—Network name of a folder
		• Null—Property EXISTSHAREFOLDERNAME must be defined

EXISTSHAREFOLDERNAME	Full path to an existing shared folder	
SERVERPORT	Port number to connect to Administration Server.	
SERVERSSLPORT	Number of port for establishing SSL connection to Administration Server	
SERVERADDRESS	Administration Server address	

MSI property	Description	Available values
SERVERCERT 2048BITS	Size of the key for the Administration Server certificate (bits)	• 1—The size of the key for the Administration Server certificate is 2,048 bits. • 0—The size of the key for the Administration Server certificate is 1,024 bits. • If no value is specified, the size of the key for the Administration Server certificate is 1,024 bits.
MOBILESERVERADDRESS	Address of the Administration Server for connection of mobile devices; ignored if the MobileSupport component has not been selected	

Network Agent installation settings

The table below describes the MSI properties that you can configure when installing Network Agent. All of the settings are optional, except for SERVERADDRESS.

Table 5. Properties of MSI

MSI property	Description	Available values
DONT_USE_ANSWER_FILE	Read installation settings from response file	• 1 • Null
INSTALLDIR	Installation folder	
SERVERADDRESS	Administration Server address (required)	

MSI property	Description	Available values
SERVERPORT	Number of port for connection to Administration Server	
SERVERSSLPORT	Number of port for SSL connection	
USESSL	Whether to use SSL connection	• 1 • Null
OPENUDPPORT	Whether to open a UDP port	• 1 • Null
UDPPORT	UDP port number	
USEPROXY	Whether to use a proxy server	• 1 • Null
PROXYADDRESS	Proxy address	
PROXYPORT	Number of port for connection to Administration Server	
PROXYLOGIN	Account for connection to proxy server	
PROXYPASSWORD	Password of account for connection to proxy server Do not specify any details of privileged user accounts in the settings of installation packages.	

MSI property	Description	Available values
GATEWAYMODE	Connection gateway use mode	• 0—Do not use connection gateway. • 1—Use this Network Agent as connection gateway • 2—Connect to Administration Server through connection gateway
GATEWAYADDRESS	Connection gateway address	
CERTSELECTION	Method of receiving a certificate	• GetOnFirstConnection—Receive a certificate from Administration Server • GetExistent—Select an existing certificate. If this option is selected, the CERTFILE property must be defined
CERTFILE	Path to the certificate file	
VMVDI	Enable dynamic mode for Virtual Desktop Infrastructure (VDI)	• 1 • Null
LAUNCHPROGRAM	Whether to run Network Agent service after installation	• 1 • Null

Virtual infrastructure

Kaspersky Security Center supports the use of virtual machines. The application supports installation of Network Agent and the security application on each virtual machine, as well as protection of virtual machines at the hypervisor level. In the first case, you can use either a standard security application or Kaspersky Security for Virtualization / Light Agent to protect your virtual machines (see http://support.kaspersky.com/ksv3). In the second case, protection of virtual

machines is provided by Kaspersky Security for Virtualization / Agentless (see http://support.kaspersky.com/ksv).

Starting from version 10 MR1, Kaspersky Security Center supports rollback of virtual machines to their previous state (see section "Support of file system rollback for devices with Network Agent" on page 71).

In this section:

Tips on reducing the load on virtual machines

When installing Network Agent on a virtual machine, you are advised to consider disabling some Kaspersky Security Center features that seem to be of little use for virtual machines.

When installing Network Agent on a virtual machine or on a template intended for generation of virtual machines, it is useful to perform the following actions:

- If you are running a remote installation, in the properties window of the Network Agent installation package (section **Advanced**), select the **Optimize settings for VDI (Virtual Desktop Infrastructure)** check box.
- If you are running an interactive installation through a Wizard, in the Wizard window, select the **Optimize Network Agent settings for virtual infrastructure** check box.

Selecting those check boxes will alter the settings of Network Agent so that the following features remain disabled by default (before applying a policy):

- Retrieving information about software installed
- Retrieving information about hardware

- Retrieving information about vulnerabilities detected
- Retrieving information about updates required

Usually, those features are not necessary on virtual machines because they use uniform software and virtual hardware.

Disabling the features is reversible. If any of the disabled features is required, you can enable it through the policy of Network Agent, or through the local settings of Network Agent. The local settings of Network Agent are available through the context menu of the relevant device in Administration Console.

Support of dynamic virtual machines

Kaspersky Security Center supports dynamic virtual machines. If a virtual infrastructure has been deployed on the enterprise network, dynamic (temporary) virtual machines can be used in certain cases. The dynamic VMs are created under unique names based on a template that has been prepared by the administrator. The user works on a VM for a while, then, after being turned off, this virtual machine will be removed from the virtual infrastructure. If Kaspersky Security Center has been deployed on the enterprise's network, a virtual machine with installed Network Agent will be added to the database of Administration Server. After you turn off a virtual machine, the corresponding entry must also be removed from the database of Administration Server.

To make functional the feature of automatic removal of entries on virtual machines, when installing Network Agent on a template for dynamic virtual machines, select the **Enable dynamic mode for VDI** check box:

- For remote installation—In the properties window of the installation package of Network Agent (**Advanced** section)
- For interactive installation—In the Network Agent Installation Wizard window.

> Avoid selecting the **Enable dynamic mode for VDI** check box when installing Network Agent on physical devices.

If you want events from dynamic virtual machines to be stored on the Administration Server for a while after you remove those virtual machines, then, in the Administration Server properties

window, in the **Events storage** section, select the **Store events after devices are deleted** check box and specify the maximum storage time for events (in days).

Support of virtual machines copying

Copying a virtual machine with installed Network Agent or creating one from a template with installed Network Agent is identical to the deployment of Network Agents by capturing and copying a hard drive image. So, in general case, when copying virtual machines, you need to perform the same actions as when deploying Network Agent by copying a disk image.

However, the two cases described below showcase Network Agent, which detects the copying automatically. Owing to the above reasons, you do not have to perform the sophisticated operations described under «Deployment by capturing and copying the hard drive of a device»:

- The **Enable dynamic mode for VDI** check box was selected when Network Agent was installed: after each restart of the operating system, this virtual machine will be recognized as a new device, regardless of whether it has been copied.
- One of the following hypervisors is in use: VMware™, HyperV®, or Xen®: Network Agent detects the copying of the virtual machine by the changed IDs of the virtual hardware.

Analysis of changes in virtual hardware is not absolutely reliable. Before applying this method widely, you must test it on a small pool of virtual machines for the version of the hypervisor currently used on your enterprise.

Support of file system rollback for devices with Network Agent

Kaspersky Security Center is a distributed application. Rolling back the file system to a previous state on a device with Network Agent installed will lead to data desynchronization and improper functioning of Kaspersky Security Center.

The file system (or a part of it) can be rolled back in the following cases:

- When copying an image of the hard drive
- When restoring a state of the virtual machine by means of the virtual infrastructure
- When restoring data from a backup copy or a recovery point.

Scenarios under which third-party software on devices with Network Agent installed affects the %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ folder are only critical scenarios for Kaspersky Security Center. Therefore, you must always exclude this folder from the recovery procedure, if possible.

Because the workplace rules of some enterprises provide for rollbacks of the file system on devices, support for the file system rollback on devices with Network Agent installed has been added to Kaspersky Security Center, starting with version 10 MR1 (Administration Server and Network Agents must be of version 10 MR1 or later). When detected, those devices are automatically reconnected to the Administration Server with full data cleansing and full synchronization.

> By default, support of file system rollback detection is disabled in Kaspersky Security Center 10 MR1.
>
> To enable this feature, you must import the reg file, which is presented in the following example, to the Registry and restart the Administration Server service.

Operating system on a device with Administration Server installed (32-bit):

```
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags]

"KLSRV_HST_VM_REVERT_DETECTION"=dword:00000001
```

Operating system on a device with Administration Server installed (64-bit):

```
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Products\1093\1.0.0.0\ServerFlags]

"KLSRV_HST_VM_REVERT_DETECTION"=dword:00000001
```

By default, support of file system rollback detection is enabled in Kaspersky Security Center 10 Service Pack 2.

As much as possible, avoid rolling back the %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ folder on devices with Network Agent installed, because full resynchronization of data requires a large amount of resources.

A rollback of the system state is absolutely not allowed on a device with Administration Server installed. Nor is a rollback of the database used by Administration Server.

You can restore a state of Administration Server from a backup copy only with the standard klbackup utility (see section "Backup and restoration of Administration Server settings" on page 38).

Configuring connection profiles for out-of-office users

Out-of-office users of laptops (hereinafter also referred to as "devices") may need to change the method of connecting to an Administration Server or switch between Administration Servers depending on the current location of the device in the enterprise network.

Using different addresses of a single Administration Server

The following procedure is only applied to Kaspersky Security Center 10 SP1 and later.

Devices with Network Agent installed can connect to the Administration Server either from the internal enterprise network or from the Internet. This situation may require Network Agent to use different addresses for connection to Administration Server: the external Administration Server address for the Internet connection and the internal Administration Server address for the internal network connection.

To do this, you must add a profile (for connection to Administration Server from the Internet) to the Network Agent policy. Add the profile in the policy properties (**Network** section, **Connection** subsection). In the profile creation window, you must clear the **Use to receive updates only** check box and select the **Synchronize connection settings with Server settings specified in this profile** check box. If you use a connection gateway to access the Administration Server (for example, in a Kaspersky Security Center configuration as that described in "Internet access: Network Agent in gateway mode in DMZ"), you must specify the connection gateway address in the corresponding field of the connection profile.

Switching between Administration Servers depending on the current network

> The following procedure is only applied to Kaspersky Security Center 10 MR1 and later.

If the organization has multiple offices with different Administration Servers and some of the devices with Network Agent installed move between them, you need Network Agent to connect to the Administration Server of the local network in the office where the device is currently located.

In this case, you must create a profile for connection to Administration Server in the properties of the policy of Network Agent for each of the offices, except for the home office where the original home Administration Server is located. You must specify the addresses of Administration Servers in connection profiles and select or clear the **Use to receive updates only** check box:

- Select the check box if you need Network Agent to be synchronized with the home Administration Server, while using the local Server for downloading updates only
- Clear the check box if it is necessary for Network Agent to be managed completely by the local Administration Server.

After that, you must set up the conditions of switching to the newly created profiles: at least one condition for each of the offices, except for the home office. Every condition's purpose consists in detection of items that are specific for an office's network environment. If a condition is true, the corresponding profile gets activated. If none of the conditions is true, Network Agent switches to the home Administration Server.

See also:

Deploying the Mobile Device Management feature

In this section:

Connecting KES devices to the Administration Server

Depending on the method used for connection of devices to the Administration Server, two deployment schemes are possible for Kaspersky Mobile Device Management for KES devices:

- Scheme of deployment with direct connection of devices to the Administration Server
- Scheme of deployment involving Forefront® Threat Management Gateway (TMG)

Direct connection of devices to the Administration Server

KES devices can connect directly to port 13292 of the Administration Server.

Depending on the method used for authentication, two options are possible for connection of KES devices to the Administration Server:

- Connecting devices with a user certificate.
- Connecting devices without a user certificate.

Connecting a device with a user certificate

When connecting a device with a user certificate, that device is associated with the user account to which the corresponding certificate has been assigned through Administration Server tools.

In this case, two-way SSL authentication (mutual authentication) will be used, Both the Administration Server and the device will be authenticated with certificates.

Connecting a device without a user certificate

When connecting a device without a user certificate, that device is associated with none of the user's accounts on the Administration Server. However, when the device receives any certificate, the device will be associated with the user to which the corresponding certificate has been assigned through Administration Server tools.

When connecting that device to the Administration Server, one-way SSL authentication will be applied, which means that only the Administration Server is authenticated with the certificate. After the device receives the user certificate, the authentication type will change to two-way SSL authentication (mutual authentication) (see section "Providing Internet access to the Administration Server" on page 11).

Scheme for connecting KES devices to the Server involving Kerberos constrained delegation (KCD)

The scheme for connecting KES devices to the Administration Server involving Kerberos constrained delegation (KCD) provides for the following:

- Integration with Microsoft Forefront TMG.
- Use of Kerberos Constrained Delegation (hereinafter referred to as KCD) for authentication of mobile devices
- Integration with Public Key Infrastructure (hereinafter referred to as PKI) for applying user certificates.

When using this connection scheme, please note the following:

- The type of connection of KES devices to TMG must be "two-way SSL authentication", that is, a device must connect to TMG through its proprietary user certificate. To do this, you need to integrate the user certificate into the installation package of Kaspersky Endpoint Security for Android, which has been installed on the device. This KES package must be created by the Administration Server specifically for this device (user).

- You must specify the special (customized) certificate instead of the default server certificate for the mobile protocol:

  1. In the properties window of the Administration Server, in the **Settings** section, select the **Open port for mobile devices** check box and then select **Add certificate...** in the drop-down list.

  2. In the window that opens, specify the same certificate that was set on TMG when the point of access to the mobile protocol was published on the Administration Server.

- User certificates for KES devices must be issued by the Certificate Authority (CA) of the domain. Keep in mind that if the domain includes multiple root CAs, user certificates must be issued by the CA, which has been set in the publication on TMG.

  You can make sure the user certificate is in compliance with the above-described requirement, using one of the following methods:

  - Specify the special user certificate in the New Installation Package Wizard and in the Certificate Installation Wizard.

  - Integrate the Administration Server with the domain's PKI and define the corresponding setting in the rules for issuance of certificates:

    1. In Administration Console, in the workspace of the **Mobile Device Management / Certificates** folder, click the **Integrate with public-key infrastructure** link to go to the **Certificates issuance rules** window.

    2. In the **Integration with PKI** section, configure integration with the Public Key Infrastructure.

    3. In the **Generation of general type certificates** section, specify the source of certificates.

See sections:

- Integration with PKI (Public Key Infrastructure) (see section "Integration with Public Key Infrastructure" on page 81).
- Providing Internet access to the Administration Server (on page 11).

Below is an example of setup of Kerberos Constrained Delegation (KCD) with the following assumptions:

- Point of access to the mobile protocol on the Administration Server side is set up on port 13292.
- The name of the device with TMG is tmg.mydom.local.
- The name of the device with Administration Server is ksc.mydom.local.
- Name of the external publishing of the point of access to the mobile protocol is kes4mob.mydom.global.

Domain account for Administration Server

You must create a domain account (for example, KSCMobileSrvcUsr) under which the Administration Server service will run. You can specify an account for the Administration Server service when installing the Administration Server or through the klsrvswch utility. The klsrvswch utility is located in the installation folder of Administration Server.

A domain account must be specified by the following reasons:

- The feature for management of KES devices is an integral part of Administration Server.
- To ensure a proper functioning of Kerberos Constrained Delegation (KCD), the receive side (i.e., the Administration Server) must run under a domain account.

Service Principal Name for http/kes4mob.mydom.local

In the domain, under the KSCMobileSrvcUsr account, add an SPN for publishing the mobile protocol service on port 13292 of the device with Administration Server.
For the kes4mob.mydom.local device with Administration Server, this will appear as follows:

setspn -a http/kes4mob.mydom.local:13292 mydom\KSCMobileSrvcUsr

Configuring the domain properties of the device with TMG (tmg.mydom.local)

To delegate traffic, trust the device with TMG (tmg.mydom.local) to the service defined by the SPN (http/kes4mob.mydom.local:13292).

To trust the device with TMG to the service defined by the SPN (http/kes4mob.mydom.local:13292), the administrator must perform the following actions:

1. In the MMC snap-in named "Active Directory Users and Computers", select the device with TMG installed (tmg.mydom.local).
2. In the device properties, on the **Delegation** tab, set the **Trust this computer for delegation to specified service only** toggle to **Use any authentication protocol**.
3. In the **Services to which this account can present delegated credentials** list, add the SPN http/kes4mob.mydom.local:13292.

Special (customized) certificate for the publishing (kes4mob.mydom.global)

To publish the mobile protocol of Administration Server, you must issue a special (customized) certificate for the FQDN kes4mob.mydom.global and specify it instead of the default server certificate in the settings of the mobile protocol of Administration Server in Administration Console. To do this, in the properties window of the Administration Server, in the **Settings** section, select the **Open port for mobile devices** check box and then select **Add certificate...** in the drop-down list.

Please note that the server certificate container (file with the extension .p12 or .pfx) must also contain a chain of root certificates (public keys).

Configuring publication on TMG

On TMG, for traffic that goes from the mobile device side to port 13292 of kes4mob.mydom.global, you have to configure KCD on the SPN (http/kes4mob.mydom.local:13292), using the server certificate issued for the FQND kes4mob.mydom.global. Please note that publishing and the published access point (port 13292 of the Administration Server) must share the same server certificate.

Using Google Firebase Cloud Messaging

To ensure timely responses of KES devices on Android to the administrator's commands, you need to enable the use of Google™ Firebase Cloud Messaging (hereinafter referred to as GFCM) in the Administration Server properties.

► *To enable the use of GFCM:*

1. In Administration Console, select the **Mobile Device Management** node, and the **Mobile devices** folder.
2. In the context menu of the **Mobile devices** folder, select **Properties**.
3. In the folder properties, select the **Settings of Google Firebase Cloud Messaging service** section.
4. In the **Sender ID** and **API Key** fields, specify the GFCM: SENDER_ID and API Key settings.

GFCM service runs in the following address ranges:

- From the KES device's side, access is required to ports 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS), and 5230 (HTTPS) of the following addresses:
  - google.com
  - android.googleapis.com
  - android.apis.google.com
  - All of the IP addresses listed in Google's ASN of 15169.
- From the Administration Server side, access is required to port 443 (HTTPS) of the following addresses:
  - android.googleapis.com
  - All of the IP addresses listed in Google's ASN of 15169.

If the proxy server settings (**Advanced / Internet connection settings**) have been defined in the Administration Server properties in Administration Console, they will be used for interaction with GFCM.

Configuring GFCM: retrieving SENDER_ID, API Key

To configure GFCM, the administrator must perform the following actions:

1. Register with the Google portal https://accounts.google.com.
2. Go to the developers portal https://console.developers.google.com/project.
3. Create a new project by clicking the **Create Project** button, specify the project's name, and specify the ID.
4. Wait for the project to be created.

   On the first page of the project, in the upper part of the page, the **Project Number** field shows the relevant SENDER_ID.

5. Go to the **APIs & auth / APIs** section, and enable **Google Firebase Cloud Messaging for Android**.
6. Go to the **APIs & auth / Credentials** section, and click the **Create New Key** button.
7. Click the **Server key** button.
8. Impose restrictions (if any), click the **Create** button.
9. Retrieve the API Key from the properties of the newly created key (**API key** field).

Integration with Public Key Infrastructure

Integration with Public Key Infrastructure (hereinafter referred to as PKI) is primarily intended for simplifying the issuance of domain user certificates by Administration Server.

The administrator can assign a domain certificate for a user in Administration Console.
This can be done using one of the following methods:

- Assign the user a special (customized) certificate from a file in the New Device Connection Wizard or in the Certificate Installation Wizard.
- Perform integration with PKI and assign PKI to act as the source of certificates for a specific type of certificates or for all types of certificates.

The settings of integration with PKI are available in the workspace of the **Mobile Device Management / Certificates** folder by clicking the **Integrate with public-key infrastructure** link.

General principle of integration with PKI for issuance of domain user certificates

In Administration Console, click the **Integrate with public-key infrastructure** link in the workspace of the **Mobile Device Management / Certificates** folder to specify a domain account that will be used by Administration Server to issue domain user certificates through the domain's CA (hereinafter referred to as the account under which integration with PKI is performed).

Please note the following:

- The settings of integration with PKI provide you the possibility to specify the default template for all types of certificates. Note that the rules for issuance of certificates (available in the workspace of the **Mobile Device Management / Certificates** folder by clicking the **Certificate generation rules** link) allow you to specify an individual template for every type of certificates.

- A special Enrollment Agent (EA) certificate must be installed on the device with Administration Server, in the certificates repository of the account under which integration with PKI is performed. The Enrollment Agent (EA) certificate is issued by the administrator of the domain's CA (Certificate Authority).

The account under which integration with PKI is performed must meet the following criteria:

- It is a domain user.

- It is a local administrator of the device with Administration Server from which integration with PKI is initiated.

- It has the right to **Log On As Service**.

- The device with Administration Server installed must be run at least once under this account to create a permanent user profile.

Kaspersky Security Center Web Server

Kaspersky Security Center Web Server (hereinafter referred to as Web Server) is a component of Kaspersky Security Center. Web Server is designed for publishing stand-alone installation packages, stand-alone installation packages for mobile devices, and files from the shared folder.

Installation packages that have been created are published on Web Server automatically and then removed after the first download. The administrator can send the new link to the user in any convenient way, such as by email.

By clicking the link, the user can download the required information to a mobile device.

Web Server settings

If a fine-tuning of Web Server is required, its properties provide you the possibility to change ports for HTTP (8060) and HTTPS (8061). In addition to changing ports, you can replace the server certificate for HTTPS and change the FQDN of Web Server for HTTP.

Routine work

In this section:

Traffic lights in Administration Console

Administration Console allows you to quickly assess the current status of Kaspersky Security Center and managed devices by checking traffic lights. The traffic lights are shown in the workspace of the **Administration Server** node, on the **Getting started** tab. The tab provides six information panes with traffic lights. Each pane with a traffic light corresponds to a specific functional scope of Kaspersky Security Center (see the table below).

Table 6. Scopes covered by traffic lights in Administration Console

Pane name	Traffic light scope
Deployment	Installing Network Agent and security applications on devices in an enterprise network
Managing devices	Structure of administration groups. Network scanning. Device moving rules
Protection of devices and virus scanning	Security application functionality: protection status, virus scanning
Update	Updates and patches
Monitoring	Protection status
Administration Server	Administration Server features and properties

Each traffic light can turn any of these five colors (see the table below). The color of a traffic light depends on the current status of Kaspersky Security Center and on events that were logged.

Table 7. Color codes of traffic lights

Status	Traffic light color	Traffic light color meaning
Informational	Green	No administrator's intervention required
Warning	Yellow	Administrator's intervention required
Critical	Red	Heavy problems have been encountered. Administrator's intervention required to solve them
Informational	Light blue	Events have been logged that are unrelated to potential or actual threats to the security of managed devices.
Informational	Gray	The details of events are not available or have not yet been retrieved.

All of the traffic lights on those panes should be kept green.

Remote access to managed devices

In this section:

Access to local tasks and statistics, "Do not disconnect from the Administration Server" check box

By default, Kaspersky Security Center does not feature continuous connectivity between managed devices and the Administration Server. Network Agents on managed devices periodically establish connections and synchronize with the Administration Server. The interval between those synchronization sessions (by default, it is 15 minutes) is defined in a policy of Network Agent. If an early synchronization is required (for example, to force the application of a policy), the Administration Server sends Network Agent a signed network packet to port UDP 15000. If a connection between the Administration Server and a managed device via UDP is not possible for any reason, synchronization will run at the next regular connection of Network Agent to the Administration Server within the synchronization interval.

Some operations cannot be performed without an early connection between Network Agent and the Administration Server, such as running and stopping local tasks, receiving statistics for a managed product (security application or Network Agent), creating a tunnel, etc. To resolve this issue, in the properties of the managed device (**General** section), select the **Do not disconnect from the Administration Server** check box. If the managed device accesses the Administration Server via an update agent, which is running in gateway mode, not directly, this check box must be selected in the properties of the device, which acts as the update agent and

functions as the gateway. The maximum total number of devices with the **Do not disconnect from the Administration Server** check box selected is 300.

Checking the time of connection between a device and the Administration Server

Upon shutting down a device, Network Agent notifies the Administration Server of this event. In Administration Console, that device is displayed as shut down. However, Network Agent cannot notify Administration Server of all such events. The Administration Server, therefore, periodically analyzes the **Last connection time** attribute (the value of this attribute is displayed in Administration Console, in the device properties, in the **General** section) for each device and compares it against the synchronization interval from the current settings of Network Agent. If a device has not responded over more than three successive synchronization intervals, that device is marked as shut down.

Forced synchronization

Although Kaspersky Security Center automatically synchronizes the status, settings, tasks, and policies for managed devices, in some cases the administrator needs to know exactly whether synchronization has already been performed for a specified device at the present moment.

In the context menu of managed devices in Administration Console, the **All Tasks** menu item contains the **Force synchronization** command. When Kaspersky Security Center 10 Service Pack 2 executes this command, the **Forced synchronization assigned** check box is selected in the device properties, then the Administration Server attempts to connect to the device. If this attempt is successful, forced synchronization will be performed and the check box will be cleared. Otherwise, synchronization will be forced and the check box will be cleared only after the next scheduled connection between Network Agent and the Administration Server. The cleared check box notifies the administrator of a successful synchronization.

Tunneling

Kaspersky Security Center allows tunneling TCP connections from Administration Console via the Administration Server and then via Network Agent to a specified port on a managed device. Tunneling is designed for connecting a client application on a device with Administration Console installed to a TCP port on a managed device—if no direct connection is possible between Administration Console and the target device.

For example, tunneling is used for connections to a remote desktop, both for connecting to an existing session, and for creating a new remote session.

Tunneling can also be enabled by using external tools. For example, the administrator can run the putty utility, the VNC client, and other tools in this way.

Appendices

This section provides reference information and additional facts for using Kaspersky Security Center:

- Information about the limitations imposed by the current version of the application (maximum numbers of managed devices, policies, tasks, etc.)
- Hardware requirements for installation of Administration Server and a DBMS
- Reference information about the disk space required for the operation of the application components
- Reference information about the average daily traffic between Network Agent and Administration Server
- Information about how to solve regular problems that arise when using Kaspersky Security Center, including how to solve problems with management of users' mobile devices.

In this section:

Limitations of Kaspersky Security Center

The following table displays the limitations of the current version of Kaspersky Security Center 10 Service Pack 2.

Table 8. Limitations of Kaspersky Security Center 10 Service Pack 2

Type of limitation	Value
Maximum number of managed devices	50,000
Maximum number of devices with the **Do not disconnect from the Administration Server** check box selected	300
Maximum number of administration groups	10,000
Maximum number of events to store	15,000,000
Maximum number of policies	2,000
Maximum number of tasks	2,000
Maximum total number of Active Directory objects (OUs and accounts of users, devices, and security groups)	1,000,000
Maximum number of profiles in a policy	100
Maximum number of slave Administration Servers on a single master Administration Server	500
Maximum number of virtual Administration Servers	200
Maximum number of devices that a single update agent can cover	500

Hardware requirements for the DBMS and the Administration Server

The following tables give the minimum hardware requirements to a DBMS and Administration Server covering 50,000 devices.

Administration Server and SQL Server are deployed on the same device

Table 9. Hardware requirements for the device

CPU	8 cores, 2,500 to 3,000 MHz
RAM	16 GB
Hard disk	500 GB, SATA RAID
Network adapter	1 Gbit
Operating system	Windows x86–64

Administration Server and SQL Server are deployed on different devices

Table 10. Hardware requirements for the device with Administration Server

CPU	4 cores, 2,500 to 3,000 MHz
RAM	8 GB
Hard disk	300 GB, RAID recommended
Network adapter	1 Gbit
Operating system	Windows x86–64

Table 11. Hardware requirements for the device with SQL Server

CPU	4 cores, 2,500 to 3,000 MHz
RAM	16 GB
Hard disk	200 GB, SATA RAID
Network adapter	1 Gbit
Operating system	Windows x86–64

The following assumptions are made:

- Update agents are assigned in the enterprise network, each of them covering from 100 to 200 devices.
- The backup task saves backup copies to a file resource located on a dedicated server.
- The synchronization interval for Network Agents is set as specified in the table below.

Table 12. Synchronization interval for Network Agents

Synchronization interval (minutes)	Number of managed devices
15	10,000
30	20,000
45	30,000
60	40,000
75	50,000

Assessing the disk space for an update agent

An update agent requires at least 4 GB of free disk space.

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

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

Preliminary assessment of space required in the database and on the hard drive for Administration Server

Assessing the space required in the database of Administration Server

The approximate amount of space that must be reserved in the database can be assessed using the following formula:

(200 * C + 2.3 * E + 2.5 * A), KB

where:

C is	the number of devices,
E is	Number of events to store
A is	Total number of Active Directory objects: Device accounts User accounts Accounts of security groups Active Directory organizational units. If the scanning of Active Directory is disabled, A is considered to equal zero.

If Administration Server distributes Windows updates (thus acting as the Windows Server Update Services (WSUS) server), the database will require an additional 2.5 GB.

Note that some unallocated space always appears in the database when the application is running. Thus, the actual size of the database file (by default, the KAV.MDF file if you use SQL Server as the DBMS) often turns out to be approximately twice as large as the amount of space occupied in the database.

The size of the transaction log (by default, the file KAV_log.LDF if you use SQL Server as the DBMS) may reach 2 GB.

Assessing the disk space on the device with Administration Server

The approximate disk space in the %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit folder on the device with Administration Server can be estimated using the following formula:

(220 * C + 0.15 * E + 0.17 * A), KB

For the values of the variables C, E, and A please refer to the table above.

Updates

The shared folder requires at least 4 GB to store updates.

Installation packages

If some installation packages are stored on Administration Server, the shared folder will require an additional amount of free disk space, equal to the total size of all of those installation packages.

Remote installation tasks

If some remote installation tasks are available on the Administration Server, the device with Administration Server will require an additional amount of free disk space (in the %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit folder), equal to the total size of all installation packages to be installed.

Patches

If Administration Server is involved in installation of patches, an additional amount of disk space will be required:

- In the patches folder—An amount of disk space, equal to the total size of all patches that have been downloaded. The default folder for storing patches is %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\wusfiles. The folder can be changed by means of the utility klsrvswch. If Administration Server is used as the WSUS server, you are advised to allocate at least 100 GB to this folder.

- In the folder %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit—An amount of disk space, equal to the total size of the patches referenced by existing instances of the task for update (patch) installation and vulnerability repair.

Assessing traffic between Network Agent and an Administration Server

The following table displays the average daily rates of traffic between an Administration Server on Kaspersky Security Center 10 MR1, build 10.1.249, and a managed device (with a Network

Agent from Kaspersky Security Center 10 MR1, build 10.1.249, and Kaspersky Endpoint Security 10 MR1, build 10.2.1.23).

Table 13. Average daily traffic rates: Kaspersky Security Center 10 MR1

	From the Administration Server to the managed device (download)	From the managed device to the Administration Server (upload)
Average daily traffic rate with the default settings of the update task	27 MB	2.7 MB
Average daily traffic rate with the update task disabled	0.8 MB	1 MB

The following table displays the average daily rates of traffic between an Administration Server from Kaspersky Security Center 10 Service Pack 2 and a managed device (with a Network Agent from Kaspersky Security Center 10 Service Pack 2 and Kaspersky Endpoint Security 10 Service Pack 1).

Table 14. Average daily traffic: Kaspersky Security Center 10 Service Pack 2

	From the Administration Server to the managed device (download)	From the managed device to the Administration Server (upload)
Average daily traffic rate with the default settings of the update task	17 MB	3.5 MB
Average daily traffic rate with the update task disabled	0.8 MB	1 MB

Troubleshooting

This section provides information about the most frequent errors and problems encountered when deploying and using Kaspersky Security Center, as well as recommendations on how to solve those issues.

In this section:

Problems with remote installation of applications

The table below lists problems that may be encountered when installing applications remotely, as well as common causes of those issues.

Table 15. Problems with remote installation of applications

Issue	Common causes and solutions
Installation rights are inadequate	The account under which installation is running has insufficient rights to execute the operations required to install the application.
Low disk space	Not enough free disk space for installation completion. Free up more disk space and retry the operation.
Unplanned OS restart	An unplanned restart of the OS has occurred during installation, the exact result of installation may be unavailable. Check the installer's settings for correctness or contact Technical Support.
Required file not found	A required file has not been found in the installation package. Check your installation package for integrity.
Incompatible platform	The installation package is not intended for this platform. Use a dedicated installation package.

Issue	Common causes and solutions
Incompatible application	An application, which is incompatible with the application being installed, is already installed on the device. Before starting the installation, remove all applications that are listed as incompatible.
Poor system requirements	The installation package requires some additional software in the system. Check whether the system configuration meets the system requirements of the application being installed.
Incomplete installation	The previous installation or removal of the application has not completed normally. To complete the previous installation or removal of the application on this device, you need to restart the OS and retry the installation process.
Wrong version of installer	Installation of this installation package is not supported by the current version of the installer on this device.
Installation already running	Installation of another application has already been started on this device.
Could not open installation package.	Could not open installation package Possible causes: The package is missing, the package is corrupted, not enough rights to access the package.
Incompatible localization	The installation package is not intended for installation on this localization of the OS.
Installation blocked by policy	Installation of applications on this device is prohibited by a policy.
Error writing file	A writing error has occurred during the application installation. Check the account under which installation has been run for required rights, and evaluate the free disk space.
Invalid uninstall password	The password for application removal has been incorrect.

Issue	Common causes and solutions
Poor hardware requirements	The system hardware does not meet the application requirements (RAM, free space on the hard drive, etc.)
Invalid installation folder	The application cannot be installed in the specified folder as it is prohibited by the installer's policy.
New installation attempt required after restart	You need to run the application installer again after restarting the device.
Restart required to continue installation	To proceed with the installer, you need to restart the device.

Incorrect copying of a hard drive image

If a hard drive image with Network Agent installed has been copied without following the rules of deployment, some devices may be displayed together in Administration Console under a single icon with a name that changes constantly.

You can resolve this issue using one of the following methods:

- Removing Network Agent.

  This method is the most reliable. You must remove Network Agent on devices that have been incorrectly copied from the image, using third-party tools, and then install it again. Network Agent cannot be removed through Kaspersky Security Center tools, because Administration Server cannot distinguish between faulty devices (they all share the same icon in Administration Console).

- Running the klmover utility with the "-dupfix" key.

  Use third-party tools to run the klmover utility, located in the Network Agent installation folder, with the "-dupfix" key (klmover -dupfix) once on faulty devices (those incorrectly copied from the image). You cannot run the utility with Kaspersky Security Center tools, because Administration Server cannot distinguish between faulty devices (they all share the same icon in Administration Console).

  Then delete the icon on which the faulty devices had been displayed before you run the utility.

- Toughening up the rule for detection of incorrectly copied devices.

  > This method is only applicable if Administration Server and Network Agents version 10 SP1 or later are installed.

  The rule for detection of incorrectly copied Network Agents must be toughened so that changing the NetBIOS name of a device results in an automatic "fix" of those Network Agents (with the assumption that all of the copied devices have unique NetBIOS names).

  On the device with Administration Server, you must import the reg file shown below to the Registry and then restart the Administration Server service.

  - If a 32-bit operating system is installed on the device with Administration Server:

```
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags]

"KLSRV_CheckClones"=dword:00000003
```

  - If a 64-bit operating system is installed on the device with Administration Server:

```
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Products\1093\1.0.0.0\ServerFlags]

"KLSRV_CheckClones"=dword:00000003
```

Problems with KES devices

This section provides information about errors and problems that may be encountered when using KES devices, as well as ways of solving those issues.

In this section:

Portal support.kaspersky.com

Information about problems that may arise when using KES devices is given in the Knowledge Base on Technical Support website http://support.kaspersky.com/ks10mob.

Checking the settings of Google Firebase Cloud Messaging service

A check of the Google Firebase Cloud Messaging settings can be performed on Google portal https://code.google.com/apis/console/#project:[YOUR.

Checking Google Firebase Cloud Messaging for accessibility

To check Google Firebase Cloud Messaging service for accessibility from the Kaspersky Security Center side (see section "Using Google Firebase Cloud Messaging" on page 80), you can use the following Telnet command:

```
telnet android.googleapis.com 443
```

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 cannot find a solution to your issue in the application documentation or in one of the sources of information about the application, we recommend that you contact Technical Support. 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 34 offices in 31 countries. The company employs more than 3,000 qualified experts.

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

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

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

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

Technologies. Many technologies that are now part and parcel of modern anti-virus tools were originally developed by Kaspersky Lab. It is no coincidence that the program kernel of Kaspersky Anti-Virus is integrated in products made by many other software vendors, including: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, and ZyXEL. Many of the company's innovative technologies are patented.

Achievements. Over the years, Kaspersky Lab has won hundreds of awards for its services in combating computer threats. For example, in 2014, tests and research conducted by the renowned Austrian anti-virus lab AV-Comparatives rated Kaspersky Lab as one of the two leaders in the number of Advanced+ certificates awarded, which earned the company the Top Rated certificate. However, the main achievement of Kaspersky Lab is the loyalty of its users worldwide. The company's products and technologies protect more than 400 million users, and its corporate clients number more than 270,000.

Kaspersky Lab website	http://www.kaspersky.com
Virus encyclopedia:	https://securelist.com
Anti-Virus Lab:	https://newvirus.kaspersky.com/ (for scanning unknown files and websites)
Kaspersky Lab web forum:	http://forum.kaspersky.com

Trademark notices