



# Kaspersky Security Center 10

*Best practices*

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

Dear User,

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

Warning! This document is the property of Kaspersky Lab: All rights to this document are protected by the copyright laws of the Russian Federation and by international treaties. Illegal reproduction or distribution of this document or parts hereof will result in civil, administrative, or criminal liability under applicable law.

Any type of reproduction or distribution of any materials, including translations, is allowed only with the written permission of Kaspersky Lab.

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

This document may be amended without additional notification.

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

Document revision date: 12/7/2016

© 2017 AO Kaspersky Lab. All Rights Reserved.

<http://www.kaspersky.com>

<https://help.kaspersky.com>

<http://support.kaspersky.com>

# Table of Contents

About this document .....	6
In this document .....	6
Document conventions .....	7
Planning Kaspersky Security Center deployment .....	9
How to select a DBMS for the Administration Server .....	11
Providing Internet access to the Administration Server .....	11
Internet access: Administration Server on a local network .....	12
Internet access: Administration Server in DMZ .....	12
Internet access: Network Agent in gateway mode in a DMZ .....	13
Standard configurations of Kaspersky Security Center .....	14
Standard configuration: Single office .....	15
Standard configuration: A few large-scale offices run by their own administrators .....	16
Standard configuration: Multiple small remote offices .....	17
About update agents .....	18
Administration Server hierarchy .....	19
Virtual Administration Servers .....	19
Installing images of operating systems .....	20
Mobile Device Management .....	21
Microsoft Exchange Mobile Devices Server .....	21
iOS MDM Server .....	25
Managing mobile devices with Kaspersky Endpoint Security for Android .....	27
Deployment and initial setup .....	29
Installing Administration Server .....	30
Creating accounts for services of Administration Server .....	30
Selecting a DBMS .....	31
Defining a shared folder .....	32
Specifying the address of the Administration Server .....	33
Defining the Administration Server certificate .....	34
Initial setup .....	35
Manual setup of Kaspersky Endpoint Security policy .....	36
Manual setup of the group update task for Kaspersky Endpoint Security .....	41

Manual setup of the group task for scanning a device with Kaspersky Endpoint Security .....	41
Manual setup of the schedule of the vulnerability scan task.....	41
Manual setup of the group task for updates installation and vulnerabilities fix .....	42
Building a structure of administration groups and assigning update agents.....	42
Hierarchy of policies, using policy profiles .....	44
Tasks.....	47
Device moving rules .....	48
Software categorization .....	50
Backup and restoration of Administration Server settings .....	50
A device with Administration Server is inoperable.....	52
The settings of Administration Server or the database are corrupted.....	53
Deploying Network Agent and a security application.....	53
Initial deployment .....	54
Remote installation of applications on devices with Network Agent installed .....	67
Managing restarts of target devices in the remote installation task .....	69
Suitability of databases updating in an installation package of an anti-virus application.....	70
Selecting a method for uninstalling incompatible applications when installing a Kaspersky Lab security application .....	70
Using tools for remote installation of applications in Kaspersky Security Center for running relevant executable files on managed devices .....	71
Monitoring the deployment .....	73
Configuring installers .....	74
Virtual infrastructure .....	82
Support of file system rollback for devices with Network Agent.....	85
Configuring connection profiles for out-of-office users.....	87
Deploying the Mobile Device Management feature .....	89
Installing a Microsoft Exchange Mobile Devices Server .....	89
Installing iOS MDM Server .....	92
Connecting KES devices to the Administration Server.....	97
Integration with Public Key Infrastructure .....	103
Kaspersky Security Center Web Server .....	104
Routine work.....	105
Traffic lights in Administration Console.....	105

Remote access to managed devices .....	107
Access to local tasks and statistics, "Do not disconnect from the Administration Server" check box .....	107
Checking the time of connection between a device and the Administration Server .....	108
Forced synchronization .....	108
Tunneling.....	108
Mobile Device Management .....	109
Microsoft Exchange Mobile Devices Server .....	109
iOS MDM Server .....	110
Appendices .....	113
Limitations of Kaspersky Security Center .....	114
Hardware requirements for the DBMS and the Administration Server.....	115
Assessing the disk space for an update agent .....	117
Preliminary assessment of space required in the database and on the hard drive for Administration Server .....	117
Assessing traffic between Network Agent and an Administration Server .....	119
Troubleshooting.....	120
Problems with remote installation of applications .....	121
Incorrect copying of a hard drive image .....	123
Problems with Microsoft Exchange Mobile Devices Server.....	124
Problems with iOS MDM Server.....	126
Problems with KES devices.....	130
Contacting the Technical Support Service .....	131
How to obtain technical support.....	131
Technical support by phone.....	132
Technical Support via Kaspersky CompanyAccount .....	132
AO Kaspersky Lab.....	134
Trademark notices .....	136

---

# About this document

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

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

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

## In this section:

In this document.....	<a href="#">6</a>
Document conventions.....	<a href="#">7</a>

## 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 [28](#))**

This section provides information about Administration Server deployment, Network Agent and security application 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 [105](#))**

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 [131](#))**

### **AO Kaspersky Lab (see page [134](#))**

This section provides information about Kaspersky Lab.

### **Trademark notices (see page [136](#))**

This section contains registered trademark notices.

## **Document conventions**

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

*Table 1. Document conventions*

<b>Sample text</b>	<b>Document conventions description</b>
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.
<b>Example:</b> ...	Examples are on a blue background under the heading "Example".

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



---

# 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
- Units (local offices, branches) that are detached organizationally or geographically
- Separate networks connected by narrow channels
- Necessity of access to the Kaspersky Lab Administration Server component from the Internet (see section "Providing Internet access to Administration Server" on page [11](#)).

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 in that network and combined into a hierarchy for convenient centralized management.

If an enterprise includes large-scale remote local offices (branches) with their own administrators, it is useful to deploy Administration Servers in those offices. Otherwise, those offices must be viewed as detached networks connected by narrow channels.

See section "Standard configuration: A few large-scale offices run by their own administrators" (on page [16](#)).

When using detached networks connected with narrow channels, traffic can be saved by assigning one or several Network Agents to act as update agents (at a rate of one update agent per 100 to 200 hosts). In this case, all devices in a detached network retrieve updates from such local update centers. These update agents can download updates either from the Administration Server (default option) or from Kaspersky Lab servers on the Internet.

See section "Standard configuration: Multiple small remote offices" (on page [17](#)).

The section "Standard configurations of Kaspersky Security Center" (on page [14](#)) provides detailed descriptions of the standard configurations of Kaspersky Security Center. When planning

the deployment, select the most suitable standard configuration, depending on the enterprise's structure.

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
- Integration with the public keys infrastructure (PKI) of an enterprise
- Specifying required values in certificate fields
- Providing the required encryption strength of a certificate.

See section Specifying the Administration Server certificate (on page [34](#)).

## In this section:

How to select a DBMS for the Administration Server.....	<a href="#">11</a>
Providing Internet access to the Administration Server .....	<a href="#">11</a>
Standard configurations of Kaspersky Security Center.....	<a href="#">14</a>
About update agents .....	<a href="#">18</a>
Administration Server hierarchy .....	<a href="#">19</a>
Virtual Administration Servers .....	<a href="#">19</a>
Installing images of operating systems.....	<a href="#">20</a>
Mobile Device Management.....	<a href="#">21</a>

# 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 .....	<a href="#">115</a>
Selecting a DBMS .....	<a href="#">31</a>

# Providing Internet access to the Administration Server

The following cases require Internet access to the Administration Server:

- Managing devices (laptops) of out-of-office users
- Managing devices in remote offices
- Interacting with master or slave Administration Servers located in remote offices
- Managing mobile devices

This section describes typical ways of providing access to the Administration Server over the Internet. Each of the cases focusing on providing Internet access to the Administration Server may require a dedicated certificate for the Administration Server (see section “Specifying the Administration Server certificate“ on page [34](#)).

### In this section:

Internet access: Administration Server on a local network.....	<a href="#">12</a>
Internet access: Administration Server in DMZ.....	<a href="#">12</a>
Internet access: Network Agent in gateway mode in a DMZ.....	<a href="#">13</a>

## Internet access: Administration Server on a local network

If the Administration Server is located within the internal network of an enterprise, port 13000 TCP of the Administration Server will become accessible from outside by means of port forwarding. If mobile device management is required, port 13292 TCP will become accessible.

## Internet access: Administration Server in DMZ

If the Administration Server is located in DMZ of the enterprise's network, it has no access to the enterprise's internal network. Therefore, the following limitations apply:

- The Administration Server cannot detect new devices.
- The Administration Server cannot perform initial deployment of Network Agent through push installation on devices in the internal network of the enterprise.

This only applies to the initial installation of Network Agent. Any further upgrades of Network Agent or the security application installation can, however, be performed by the Administration Server. At the same time, the initial deployment of Network Agents can be performed by other means, for example, through group policies of Microsoft® Active Directory®.

- The Administration Server cannot send notifications to managed devices via port 15000 UDP, which is not critical for the Kaspersky Security Center functioning.
- The Administration Server cannot poll Active Directory. However, results of Active Directory polling are not required in most scenarios.

If the above limitations are viewed as critical, they can be removed by using update agents located within the enterprise network:

- To perform initial deployment on devices without Network Agent, you first install Network Agent on one of the devices and then assign it the update agent status. As a result, initial installation of Network Agent on other devices will be performed by the Administration Server through this update agent.
- To detect new devices in the internal network of the enterprise and poll Active Directory, you must enable the relevant network polling methods on one of the update agents.
- To ensure a successful sending of notifications to port 15000 UDP on managed devices located within the internal network of the enterprise, you must cover the entire network with update agents at a rate of 100 to 200 devices per one update agent. In the properties of the update agents that were assigned, select the **Do not disconnect from the Administration Server** check box. As a result, the Administration Server will establish a continuous connection to the update agents while they will be able to send notifications to port 15000 UDP on devices within the internal network of the enterprise (see section "About update agents" on page [18](#)).

## Internet access: Network Agent in gateway mode in a DMZ

The access mode described below is applied to Kaspersky Security Center 10 Service Pack 1 and later versions.

The Administration Server can be located in the internal network of the enterprise, and in that network's DMZ there can be a device with Network Agent running in gateway mode with reverse connectivity (the Administration Server establishes a connection to Network Agent). In this case, the following conditions must be met to ensure Internet access:

- Network Agent must be installed on the device, which is in the DMZ. When you install Network Agent, on the **Connection gateway** page of the Setup Wizard, select **Use as connection gateway**.
- A dedicated administration group must be created on the Administration Server; in the properties of this group, the DMZ device must be assigned the connection gateway status by address. You must not add any devices to this administration group.
- For Network Agents that attempt to access the Administration Server via the Internet, use **Connect to Server using connection gateway** to specify the newly created gateway during installation.

For the connection gateway in the DMZ, the Administration Server creates a certificate signed with the Administration Server certificate. If the administrator decides to assign a custom certificate to the Administration Server, it must be done before a connection gateway is created in the DMZ.

If some employees use laptops that can connect to the Administration Server either from the local network or over the Internet, it may be useful to create a switching rule for Network Agent in the Network Agent's policy.

## Standard configurations of Kaspersky Security Center

This section describes the following standard configurations used for deployment of Kaspersky Security Center components on an enterprise network:

- Single office
- A few large-scale offices, which are geographically detached and run by their own administrators
- Multiple small offices, which are geographically detached.

## In this section:

Standard configuration: Single office .....	<a href="#">15</a>
Standard configuration: A few large-scale offices run by their own administrators.....	<a href="#">16</a>
Standard configuration: Multiple small remote offices.....	<a href="#">17</a>

## Standard configuration: Single office

One or several Administration Servers can be deployed on the enterprise's network. The number of Administration Servers can be defined on the basis either of the specifics of available hardware (see section “Hardware requirements for the DBMS and the Administration Server“ on page [115](#)) or the total number of managed devices.

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.

Administration Servers can be deployed either on the internal network, or in the DMZ, depending on whether Internet access to the Administration Servers is required.

If multiple Servers are used, it is recommended that you combine them into a hierarchy.

Using an Administration Server hierarchy allows you to avoid duplicated 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.

If an Administration Server supports more than 5,000 hosts, it may be useful to assign the update agent status to devices in various network segments at a rate of 100 to 200 managed devices per one update agent, in order to reduce the load on the network and the Administration Server.

## See also:

Assessing the disk space for an update agent .....	<a href="#">117</a>
Assessing traffic between Network Agent and an Administration Server .....	<a href="#">119</a>
About update agents .....	<a href="#">18</a>
Administration Server hierarchy .....	<a href="#">19</a>

## Standard configuration: A few large-scale offices run by their own administrators

If a few large-scale offices are run, which are geographically detached, you must consider the option of deploying Administration Servers at each of the offices, one or several Servers per each, depending on the number of client devices and hardware available. In this case, each of the offices can be viewed as a "Standard configuration: Single office". For ease of administration, all of the Administration Servers should be combined into a hierarchy (possibly multilevel).

If some employees move between offices with their devices (laptops), a rule for Network Agent switching between Administration Servers must be created in the Network Agent policy.

## See also:

Standard configuration: Single office .....	<a href="#">15</a>
Administration Server hierarchy .....	<a href="#">19</a>
Configuring connection profiles for out-of-office users .....	<a href="#">87</a>



# Standard configuration: Multiple small remote offices

This standard configuration provides for a headquarters office and many remote small offices that can possibly be communicated to the HQ office via the Internet. Each of those remote offices may possibly be located beyond Network Address Translation (NAT), i.e., no connection can be established between two remote offices, since they are isolated.

An Administration Server must be deployed at the headquarters office, while one or multiple update agents must be assigned to all other offices. If the offices 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 at a remote office have no direct access to the Administration Server (for example, access to the Administration Server is provided over the Internet but some devices have no Internet access), update agents must be switched into connection gateway mode. In this case, Network Agents on devices at the remote office 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 remote office 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 at the remote office. 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 (**Do not disconnect from the Administration Server** check box). This mode is available if the total number of update agents does not exceed 200.

## See also:

Providing Internet access to the Administration Server .....	<a href="#">11</a>
About update agents .....	<a href="#">18</a>

# 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.

- Reduces the load on the Administration Server.
- Optimizes traffic.
- Provides the Administration Server access to devices in hard-to-reach spots of the enterprise network. The availability of an update agent on the network beyond NAT (in relation to the Administration Server) 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..... [42](#)

# Administration Server hierarchy

An organization 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. The functional scope of virtual Administration Servers can be used both by service providers (xSP) to maximize the isolation of customers, and by large-scale organizations with sophisticated workflows and numerous administrators.

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.

## Installing images of operating systems

Kaspersky Security Center allows you to deploy WIM images of desktop and server-based Windows® operating systems on devices within an enterprise network.

The following methods can be used to retrieve an operating system image that would be deployable by using Kaspersky Security Center tools:

- Import from the install.wim file included in the Windows distribution package
- Capturing an image from a reference device

Two scenarios are supported for deployment of operating system images:

- Deployment on a "clean" device, that is, without any operating system installed
- Deployment on a device running Windows

The Administration Server implicitly features a service image of Windows Preinstallation Environment (Windows PE), which is always used both for capturing operating system images, and for their deployment. All drivers required for proper functioning of all target devices must be added to WinPE. Generally, chipset drivers required for the functioning of Ethernet networking interface must be added.

The following requirements must be met in order to implement scenarios of image deployment and capture:

- Windows Automated Installation Kit (WAIK) version 2.0, or later, or Windows Assessment and Deployment Kit (WADK) must be installed on the Administration Server. If the scenario allows for installing or capturing images on Windows XP, WAIK must be installed.
- A DHCP server must be available in the network where the target device is located.
- The shared folder of the Administration Server must be open for reading from the network where the target device is located. If the shared folder is located on the Administration Server, access must be granted to the KIPxeUser account. If the shared folder is located outside the Administration Server, access must be granted to everyone.

When selecting the operating system image to be installed, the administrator must explicitly specify the CPU architecture of the target device: x86 or x86-64.

## Mobile Device Management

In this section:

Microsoft Exchange Mobile Devices Server .....	<a href="#">21</a>
iOS MDM server.....	<a href="#">25</a>
Managing mobile devices with Kaspersky Endpoint Security for Android .....	<a href="#">27</a>

## Microsoft Exchange Mobile Devices Server

An Exchange ActiveSync® Mobile Device Server allows you to manage mobile devices that are connected to an Administration Server using the Exchange ActiveSync protocol (EAS devices).

In this section:

How to deploy a Microsoft Exchange Mobile Devices Server .....	<a href="#">22</a>
Rights required for deployment of a Microsoft Exchange Mobile Devices Server .....	<a href="#">23</a>
Account for Exchange ActiveSync service .....	<a href="#">23</a>

# How to deploy a Microsoft Exchange Mobile Devices Server

If multiple Microsoft Exchange servers within a Client Access Server array have been deployed in the organization, a Microsoft Exchange Mobile Devices Server must be installed on each of the servers in that array. The **Cluster mode** option must be enabled in the Microsoft Exchange Mobile Devices Server Installation Wizard. In this case, the set of instances of the Microsoft Exchange Mobile Devices Server installed on servers in the array is called the cluster of Microsoft Exchange Mobile Devices Servers.

If no Client Access server array of Microsoft Exchange Servers has been deployed in the organization, a Microsoft Exchange Mobile Devices Server must be installed on a Microsoft Exchange Server that has Client Access. In this case, the **Standard mode** option must be enabled in the Setup Wizard of the Microsoft Exchange Mobile Devices Server.

Together with the Microsoft Exchange Mobile Devices Server, Network Agent must be installed on the device; it helps integrate the Microsoft Exchange Mobile Devices Server with Kaspersky Security Center.

The default scan scope of the Microsoft Exchange Mobile Devices Server is the current Active Directory domain in which it was installed. Deploying a Microsoft Exchange Mobile Devices Server on a server with Microsoft Exchange Server (versions 2010, 2013) installed allows expansion of the scan scope to include the entire domain forest in the Microsoft Exchange Mobile Devices Server (see section "Configuring the scan scope" on page [110](#)). Information requested during a scan includes accounts of Microsoft Exchange server users, Exchange ActiveSync policies, and users' mobile devices connected to the Microsoft Exchange Server over Exchange ActiveSync protocol.

Multiple instances of Microsoft Exchange Mobile Devices Server cannot be installed within a single domain if they run in **Standard mode** being managed by a single Administration Server.

Within a single Active Directory domain forest, multiple instances of a Microsoft Exchange Mobile Devices Server (or multiple clusters of Microsoft Exchange Mobile Devices Servers) cannot be installed either—if they run in **Standard mode** with an expanded scan scope that includes the entire domain forest and if they are connected to a single Administration Server.

## See also:

Installing a Microsoft Exchange Mobile Devices Server .....	<a href="#">89</a>
Configuring the scan scope.....	<a href="#">110</a>

## Rights required for deployment of a Microsoft Exchange Mobile Devices Server

Deployment of a Microsoft Exchange Mobile Devices Server on Microsoft Exchange Server (2010, 2013) requires domain administrator rights and the Organization Management role.

Deployment of a Microsoft Exchange Mobile Devices Server on a Microsoft Exchange Server (2007) requires domain administrator rights and membership in the Exchange Organization Administrators security group.

## Account for Exchange ActiveSync service

When a Microsoft Exchange Mobile Devices Server is installed, an account is automatically created in Active Directory:

- On Microsoft Exchange Server (2010, 2013): KLMDM4ExchAdmin\*\*\*\*\* account with the KLMDM Role Group role
- On Microsoft Exchange Server (2007): KLMDM4ExchAdmin\*\*\*\*\* account, a member of the KLMDM Secure Group security group.

The Microsoft Exchange Mobile Devices Server service runs under this account.

If you want to cancel the automatic generation of an account, you need to create a custom one with the following rights:

- When using a Microsoft Exchange Server (2010, 2013), the account must be assigned a role that has been allowed to execute the following cmdlets:
  - Get-CASMailbox.
  - Set-CASMailbox.

- Remove-ActiveSyncDevice.
  - Clear-ActiveSyncDevice.
  - Get-ActiveSyncDeviceStatistics.
  - Get-AcceptedDomain.
  - Set-AdServerSettings.
  - Get-ActiveSyncMailboxPolicy.
  - New-ActiveSyncMailboxPolicy.
  - Set-ActiveSyncMailboxPolicy.
  - Remove-ActiveSyncMailboxPolicy.
- When using a Microsoft Exchange Server (2007), the account must be granted the access rights to Active Directory objects (see the table below).

Table 2. Access rights to Active Directory objects

Access	Object	Cmdlet
Full	Thread "CN=Mobile Mailbox Policies,CN=<Organization name>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Domain name>"	<code>Add-ADPermission -User &lt;User or group name&gt; -Identity "CN=Mobile Mailbox Policies,CN=&lt;Organization name&gt;,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=&lt;Domain name&gt;" -InheritanceType All -AccessRight GenericAll</code>
Read	Thread "CN=<Organization name>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Domain name>"	<code>Add-ADPermission -User &lt;Domain name&gt; -Identity "CN=&lt;Organization name&gt;,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=&lt;Domain name&gt;" -InheritanceType All -AccessRight GenericRead</code>



Access	Object	Cmdlet
Read/write	Properties msExchMobileMailboxPolicyLink and msExchOmaAdminWirelessEnable for objects in Active Directory	Add-ADPermission -User <User or group name> -Identity "DC=<Domain name>" -InheritanceType All -AccessRight ReadProperty,WriteProperty -Properties msExchMobileMailboxPolicyLink, msExchOmaAdminWirelessEnable
Extended right ms-Exch-Store-Active	Mailbox repositories of Exchange server, thread "CN=Databases,CN=Exchange Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=<Organization name>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Domain name>"	Get-MailboxDatabase   Add-ADPermission -User <User or group name> -ExtendedRights ms-Exch-Store-Admin

## iOS MDM Server

iOS MDM Server allows you to manage iOS devices by installing dedicated iOS MDM profiles on them. The following features are supported:

- Device lock
- Password reset
- Data wipe
- Installation or removal of apps
- Use of an iOS MDM profile with advanced settings (such as VPN settings, email settings, Wi-Fi settings, camera settings, certificates, etc.).

iOS MDM Server is a web service that receives inbound connections from mobile devices through its TLS port (by default, port 443), which is managed by Kaspersky Security Center using Network Agent. Network Agent is installed locally on a device with an iOS MDM Server deployed.

When deploying an iOS MDM Server, the administrator must perform the following actions:

- Provide Network Agent with access to the Administration Server
- Provide mobile devices with access to the TCP port of the iOS MDM Server

This section addresses two standard configurations of an iOS MDM Server.

### In this section:

Standard configuration: Kaspersky Mobile Device Management in DMZ.....	<a href="#">26</a>
Standard configuration: iOS MDM Server on the local network of an enterprise.....	<a href="#">27</a>

## Standard configuration: Kaspersky Mobile Device Management in DMZ

An iOS MDM Server is located in the DMZ of an enterprise's local network with Internet access. A special feature of this approach is the absence of any problems when the iOS MDM web service is accessed from devices over the Internet.

Because management of an iOS MDM Server requires Network Agent to be installed locally, you must ensure the interaction of Network Agent with the Administration Server. You can ensure this by using one of the following methods:

- Move the Administration Server to the DMZ.
- Use a connection gateway (see section "Internet access: Network Agent in gateway mode in DMZ" on page [13](#)):
  - a. On the device with iOS MDM Server deployed, connect Network Agent to the Administration Server through a connection gateway.
  - b. On the device with iOS MDM Server deployed, assign Network Agent to act as connection gateway.

See also:

Simplified deployment scheme.....	92
-----------------------------------	----

## Standard configuration: iOS MDM Server on the local network of an enterprise

An iOS MDM Server is located on the internal network of an enterprise. Port 443 (default port) must be enabled for external access, This, for example, can be done by publishing the iOS MDM web service on Microsoft Forefront® Threat Management Gateway (hereinafter referred to as TMG) (see section "Scheme for connecting KES devices to the Server involving Kerberos constrained delegation (KCD)" on page [98](#)).

Any standard configuration requires access to Apple web services for the iOS MDM Server (range 17.0.0.0/8) through TCP port 2195. This port is used for notifying devices of new commands by means of a dedicated service named APN (see section "Configuring the access to Apple Push Notification service" on page [95](#)).

## 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 .....	<a href="#">11</a>
Defining the Administration Server certificate .....	<a href="#">34</a>

---

# 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.
- 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
- Custom 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 .....	<a href="#">30</a>
Initial setup .....	<a href="#">35</a>
Backup and restoration of Administration Server settings.....	<a href="#">50</a>
Deploying Network Agent and the security application .....	<a href="#">53</a>
Configuring connection profiles for out-of-office users .....	<a href="#">87</a>
Deploying the Mobile Device Management feature .....	<a href="#">89</a>

# 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.....	<a href="#">30</a>
Selecting a DBMS .....	<a href="#">31</a>
Defining a shared folder .....	<a href="#">32</a>
Specifying the address of the Administration Server .....	<a href="#">33</a>
Defining the Administration Server certificate .....	<a href="#">34</a>

## 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 3. 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.
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..... [11](#)

# Defining a shared folder

When installing Administration Server, you can specify the location of the shared folder.

You can also specify the location of the shared folder after installation, in the Administration Server properties. By default, the shared folder will be created on the device with Administration Server (with the read rights for the **Everyone** subgroup). However, in some cases (high load, need for access from an isolated network, etc.), it is useful to locate the shared folder on a dedicated file resource.

The shared folder is used occasionally in Network Agent deployment.

## In this section:

Remote installation with Administration Server tools through Active Directory group policies.....	<a href="#">32</a>
Remote installation through delivery of the UNC path to a stand-alone package.....	<a href="#">33</a>
Updating from the Administration Server shared folder .....	<a href="#">33</a>
Installing images of operating systems.....	<a href="#">33</a>

## Remote installation with Administration Server tools through Active Directory group policies

If the target devices are located within a Windows domain (no workgroups), initial deployment (installation of Network Agent and the security application on devices that are not yet managed) has to be performed through Active Directory group policies. Deployment is performed by using the standard task for remote installation of Kaspersky Security Center. If the network is large-scale, it is useful to locate the shared folder on a dedicated file resource to reduce the load on the disk subsystem of the Administration Server device.



## Remote installation through delivery of the UNC path to a stand-alone package

If the users of networked devices in the enterprise have local administrator rights, another method of initial deployment is to create a stand-alone Network Agent package (or even a "coupled" Network Agent package together with the security application). After you create a stand-alone package, send users a link to that package, which is stored in the shared folder. Installation starts when users click the link.

## Updating from the Administration Server shared folder

In the Anti-Virus update task, you can configure updating from the shared folder of Administration Server. If the task has been assigned to a large number of devices, it is useful to locate the shared folder on a dedicated file resource.

## Installing images of operating systems

Operating system images are always installed through the Administration Server shared folder: devices read images of operating systems from this folder. If deployment of images is planned on a large number of enterprise devices, it is useful to locate the shared folder on a dedicated file resource.

See also:

| Deploying Network Agent and the security application ..... [53](#)

## Specifying the address of the Administration Server

When installing Administration Server, you can specify the address of the Administration Server host computer. This address will be used as the default address when creating installation packages of Network Agent. By default, the NetBIOS name of the Administration Server device is used.

If the Domain Name System (DNS) in the enterprise network has been configured and is functioning properly, specify in the DNS the FQDN of the Administration Server device. If Administration Server is installed in the DMZ, it may be useful to specify the external address of the Administration Server computer. 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.

### See also:

| Internet access: Administration Server in DMZ..... [12](#)

## 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).

Utility command line syntax:

```
klsetsrvcert [-I LOGFILE] -t TYPE [-p PASSWORD] -i FILE
```

Table 4. Values of the settings of klsetsrvcert utility

Setting	Value
-t TYPE	Type of the certificate to be replaced. Possible values of the setting TYPE: <ul style="list-style-type: none"><li>• C – Replace the certificate for ports 13000 and 13291;</li><li>• CR – Replace the reserve certificate for ports 13000 and 13291;</li><li>• M – Replace the certificate for mobile devices on port 13292.</li></ul>
-i FILE	Container with the certificate in PKCS#12 format (file with the extension .p12 or .pfx).
-p PASSWORD	Password used for protection of the .p12 container with the certificate.
-I 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 .....	<a href="#">36</a>
Manual setup of the group update task for Kaspersky Endpoint Security .....	<a href="#">41</a>
Manual setup of the group task for scanning a device with Kaspersky Endpoint Security.....	<a href="#">41</a>
Manual setup of the schedule of the vulnerability scan task .....	<a href="#">41</a>
Manual setup of the group task for updates installation and vulnerabilities fix .....	<a href="#">42</a>
Building a structure of administration groups and assigning update agents.....	<a href="#">42</a>
Hierarchy of policies, using policy profiles .....	<a href="#">44</a>
Tasks .....	<a href="#">47</a>
Device moving rules.....	<a href="#">48</a>
Software categorization.....	<a href="#">50</a>

## 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 .....	<a href="#">37</a>
Configuring the policy in the Advanced Settings section .....	<a href="#">38</a>
Configuring the policy in the Events section .....	<a href="#">39</a>

# 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

It is useful to enable the use of KSN Proxy (by selecting the **Use KSN Proxy Server** check box), because this will significantly improve the reliability of malware detection.

# 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.

The optimal and recommended schedule option for Kaspersky Endpoint Security versions 10 and / or 10 SP1 is **When new updates are downloaded to the repository** when the **Define task launch delay automatically** check box is 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.

# 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 [44](#)).

- 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 enterprise organizational chart and network topology, the following standard configurations can be applied to the structure of administration groups:

- Single office
- Multiple small detached offices.

### In this section:

Standard configuration: Single office .....	<a href="#">43</a>
Standard configuration: Multiple small isolated offices .....	<a href="#">43</a>

## Standard configuration: Single office

In a standard "single-office" configuration, all devices are within the enterprise network so they

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 [117](#)). Update agents must not be shut down frequently; sleep mode must be disabled on them.

## Standard 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 [117](#)). 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.....	<a href="#">45</a>
Policy profiles.....	<a href="#">46</a>

## 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 [87](#))

- 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

It is advisable to set automatic allocation of devices to administration groups through *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 was once 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 [46](#)), tasks for selections of devices (see section “Tasks” on page [47](#)), 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 [42](#)), 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 .....	<a href="#">52</a>
The settings of Administration Server or the database are corrupted .....	<a href="#">52</a>

## 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 .....	<a href="#">54</a>
Remote installation of applications on devices with Network Agent installed .....	<a href="#">67</a>
Managing device restarts in the remote installation task.....	<a href="#">69</a>
Suitability of databases updating in an installation package of an anti-virus application .....	<a href="#">70</a>
Selecting a method for uninstalling incompatible applications during installation of a security application by Kaspersky Lab.....	<a href="#">70</a>
Using tools for remote installation of applications in Kaspersky Security Center for running relevant executable files on managed devices .....	<a href="#">71</a>
Monitoring the deployment .....	<a href="#">73</a>
Configuring installers.....	<a href="#">74</a>
Virtual infrastructure .....	<a href="#">82</a>
Support of file system rollback for devices with Network Agent .....	<a href="#">85</a>

## 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:

- With third-party tools for remote installation of applications.
- By cloning an image of the administrator's hard disk with the operating system and Network Agent: using tools provided by Kaspersky Security Center for handling disk images, or using third-party tools.
- With Windows group policies: using standard Windows management tools for group policies, or in automatic mode, through the corresponding, dedicated option in the remote installation task of Kaspersky Security Center.
- 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, initial installation of Network Agent on managed devices must be performed through available third-party tools. 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 [14](#))
- Total number of devices
- Presence of devices in the enterprise network, which are not members of any Active Directory domain, and presence of uniform accounts with administrator rights on those devices

- Capacity of the channel between the Administration Server and devices
- Type of communication between Administration Server and remote subnets and capacity of network channels in those subnets
- 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 Administration Server; 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.

This method of defining the settings is inappropriate for non-interactive ("silent") installation of applications on groups of devices. In general, the administrator must specify values for settings in centralized mode; those values can subsequently be used for 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 would be specific for an individual supported application can be defined in the user interface of Administration Console when the installation package is created. When performing remote installation of applications through Kaspersky Security Center tools, installation packages are delivered to devices so that running the installer of an application makes all administrator-defined settings available for that application. 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 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 within the shared folder (see section "Defining a shared folder" on page [32](#)).

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 [61](#)).

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.

Although the key for an application can be set in the properties of an installation package, it is advisable to avoid this method of license distribution because there it is easy to obtain read access to installation packages. 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 applied in the following cases:

- When installing through Windows group policies, by using regular Microsoft tools or other third-party tools for handling Windows group policies
- When installing applications by using third-party tools intended for handling installers in Microsoft Installer format (see section "Configuring installers" on page [74](#)).

## 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.
- When performing installation from a shared folder, you must make sure that this file resource has sufficient capacity.

### See also:

Defining a shared folder .....	<a href="#">32</a>
Configuring installers.....	<a href="#">74</a>

# General information about the remote installation tasks in Kaspersky Security Center

Kaspersky Security Center provides various mechanisms for remote installation of applications, which are implemented as remote installation tasks (forced installation, installation by copying a hard drive image, installation through group policies of Microsoft Windows). 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. In addition, you can use the Remote Installation Wizard, which is based on creation of a remote installation task and results monitoring.

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 by capturing and copying the hard drive image of a device

If you need to install Network Agent on devices on which an operating system and other software also must be installed (or reinstalled), you can use the mechanism of capturing and copying the hard drive of that device.

Deployment by capturing and copying a computer's hard disk is performed as follows:

1. Create a "reference" device with an operating system and the relevant software installed, including Network Agent and a security application.
2. Capture the reference image on the device and distribute that image on new devices through the dedicated task of Kaspersky Security Center.

To capture and install disk images, you can use either third-party tools available in the enterprise, or the feature provided (under a Systems Management license) by Kaspersky Security Center (see section "Installing images of operating systems" on page [20](#)).

If you use any third-party tools to process disk images, you must delete the information that Kaspersky Security Center uses to identify the managed device, when performing deployment on a device from a reference image. Otherwise, Administration Server will not be able to properly distinguish devices that have been created by copying the same image (see <http://support.kaspersky.com/9334>).

When capturing a disk image with Kaspersky Security Center tools, this issue is solved automatically.

### Copying a disk image with third-party tools

When applying third-party tools for capturing the image of a device with Network Agent installed, use one of the following methods:

- Recommended method. When installing Network Agent on a reference device, select **Do not run service when installation completes** and capture the device image before the first run of Network Agent service (because unique information identifying the device is created at the first connection of Network Agent to the Administration Server). After that, it is recommended that you avoid running Network Agent service until the completion of the image capturing operation.
- On the reference device, stop the Network Agent service and run the `klmover` utility with the `-dupfix` key. The utility `klmover` is included in the installation package of Network Agent. Avoid any subsequent runs of Network Agent service until the image capturing operation completes.
- Make sure that `klmover` will be run with the `-dupfix` key before (mandatory requirement) the first run of the Network Agent service on target devices, at the first launch of the operating system after the image deployment. The utility `klmover` is included in the installation package of Network Agent.

If the hard drive image has been copied incorrectly, see section [Hard drive image copying](#) has been performed incorrectly (on page [123](#)).

You can apply an alternate scenario for Network Agent deployment on new devices through operating system images:

- The captured image contains no Network Agent installed
- A stand-alone package of Network Agent located in the shared folder of Kaspersky Security Center has been added to the list of executable files that are run upon completion of the image deployment on target devices.

This deployment scenario adds flexibility: You can use a single operating system image along with various installation options for Network Agent and / or the security application, including device moving rules related to the stand-alone package. This slightly complicates the deployment process: You have to provide access to the network folder with stand-alone packages from a target device (see section "Installing images of operating systems" on page [20](#)).

## 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.
- 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.

When this deployment scheme is selected, you must also assess the load on the file resource from which files will be copied to devices after applying the Windows group policy.

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

The simplest way to install applications through group policies of Microsoft Windows is to select the **Assign the package installation in the Active Directory group policies** check box in the properties of the remote installation task of Kaspersky Security Center. In this case, Administration Server automatically performs the following actions when you run the task:

- Creates required objects in the group policy of Microsoft Windows.
- Creates dedicated security groups, includes the target devices in those groups, and assigns installation of selected applications for them. The set of security groups will be updated at every task run, in accordance with the pool of devices at the moment of the run.

To make this feature operable, in the task properties, specify an account that has write permissions in Active Directory group policies.

If you intend to install both Network Agent and another application through the same task, selecting the **Assign the package installation in the Active Directory group policies** check box causes the application to create an installation object in the Active Directory policy for Network Agent only. The second application selected in the task will be installed through the tools of Network Agent as soon as the latter is installed on the device. If you want to install an application other than Network Agent through Windows group policies, you must create an installation task for this installation package only (without the Network Agent package).

If required objects are created in the group policy by using Kaspersky Security Center tools, the shared folder of Kaspersky Security Center will be used as the source of the installation package. When planning the deployment, you must correlate the reading speed for this folder with the number of devices and the size of the distribution package to be installed. It may be useful to locate the shared folder of Kaspersky Security Center in a high-performance dedicated file repository (see section "Defining a shared folder" on page [32](#)).

In addition to its ease of use, automatic creation of Windows group policies through Kaspersky Security Center has this advantage: when planning Network Agent installation, you can easily specify the Kaspersky Security Center administration group into which devices will be automatically moved after installation completes. You can specify this group in the New Task Wizard or in the settings window of the remote installation task.

When handling Windows group policies through Kaspersky Security Center, you can specify devices for a group policy object by creating a security group. Kaspersky Security Center synchronizes the contents of the security group with the current set of devices in the task. When using other tools for handling group policies, you can associate objects of group policies with selected OUs of Active Directory directly.

### **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, he or she can provide links to packages stored in the shared folder of Kaspersky Security Center, or upload those packages to a dedicated file server and then provide links to them.

The following installation scenarios are possible:

- The administrator creates an installation package and sets up its properties in Administration Console. The group policy object provides a link to the msi file of this package stored in the shared folder of Kaspersky Security Center.
- 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 [74](#)).

## Forced deployment through the remote installation task of Kaspersky Security Center

If you need to start deploying Network Agents or other applications immediately, without waiting for the next time target devices log in to the domain, or if any target devices that are not members of the Active Directory domain are available, you can force installation of selected installation packages through the remote installation task of 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.



This type of installation consists in copying files to the administrative resource (admin\$) on each device and performing remote registration of supporting services on them. The following conditions must be met in this case:

- Devices must be available for connection either from the Administration Server side, or 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.

Forced installation can also be applied if devices cannot be directly accessed by the Administration Server: for example, devices are in isolated networks, or they are in a local network while the Administration Server item is in DMZ. To make forced installation possible, you must provide update agents to each of the isolated networks.

Using update agents as local installation centers may also be useful when performing installation on devices in subnets communicated with Administration Server via a low-capacity channel while a broader channel is available between devices in the same subnet. However, 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 [117](#)).

## 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. The stand-alone installation package is stored in the shared folder of Kaspersky Security Center.

You can use Kaspersky Security Center to send selected users an email message containing a link to this file in the shared folder, prompting them to run the file (either in interactive mode, or with the key "-s" 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 shared folder of Kaspersky Security Center. The administrator can also copy the stand-alone package to an external drive, 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 stored in the shared folder of Kaspersky Security Center, 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 [59](#)).

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 [18](#)) and Building a structure of administration groups and assigning update agents (on page [42](#))). 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\adminikit\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\adminikit\1103\FTCITmp 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.

## 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 [105](#)). 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 through the corresponding event selection in the Administration Server node on the **Events** tab.

# 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.....	<a href="#">74</a>
Installation in silent mode (with a response file) .....	<a href="#">74</a>
Installation in silent mode (without a response file).....	<a href="#">75</a>
Partial installation configuration through setup.exe.....	<a href="#">76</a>
Administration Server installation settings .....	<a href="#">76</a>
Network Agent installation settings.....	<a href="#">80</a>

## 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 5. Properties of MSI

MSI property	Description	Available values
EULA	Acceptance of the licensing terms (required)	<ul style="list-style-type: none"><li>• 1</li><li>• Null</li></ul>
INSTALLATIONMODETYPE	Type of Administration Server installation	<ul style="list-style-type: none"><li>• Standard</li><li>• Custom</li></ul>
INSTALLDIR	Product installation folder	

MSI property	Description	Available values
ADDLOCAL	List of components to install (separated by commas)	<p>CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86.</p> <p>Minimum list of components sufficient for proper Administration Server installation:</p> <pre>ADDLOCAL=CSAdminKitServer,CSAdminKitConsole,KSNProxy,Microsoft_VC90_CRT_x86,Microsoft_VC100_CRT_x86</pre>
NETRANGE TYPE	Network Size	<ul style="list-style-type: none"> <li>• NRT_1_100—From 1 to 100 devices</li> <li>• NRT_100_1000—From 101 to 1000 devices</li> <li>• NRT_GREATER_1000—1001+ devices</li> </ul>
SRV_ACCOUNT_TYPE	Way of specifying the user for the operation of the Administration Server service	<ul style="list-style-type: none"> <li>• SrvAccountDefault – User account will be created automatically</li> <li>• SrvAccountUser—User account is defined manually</li> </ul>
SERVERACCOUNTNAME	User name for the service	
SERVERACCOUNTPWD	User password for the service	
DBTYPE		<ul style="list-style-type: none"> <li>• MySQL</li> <li>• MSSQL</li> </ul>
MYSQLSERVERNAME	Full name of MySQL server	

MSI property	Description	Available values
MYSQLSER VERPORT	Number of port for connection to MySQL server	
MYSQLDBN AME	Name of MySQL server database	
MYSQLACC OUNTNAME	User name for connection to MySQL server database	
MYSQLACC OUNTPWD	User password for connection to MySQL server database	
MSSQLCON NECTIONTY PE	Type of use of MSSQL database	<ul style="list-style-type: none"> <li>• InstallMSSEE – Install from a package</li> <li>• ChooseExisting—Use the installed server</li> </ul>
MSSQLSER VERNAME	Full name of SQL Server instance	
MSSQLDBN AME	Name of SQL server database	
MSSQLAUT HTYPE	Method of authentication for connection to SQL Server	<ul style="list-style-type: none"> <li>• Windows</li> <li>• SQLServer</li> </ul>
MSSQLACC OUNTNAME	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	<ul style="list-style-type: none"> <li>• Create—Create a new shared folder. In this case, the following properties must be defined: <ul style="list-style-type: none"> <li>• SHARELOCALPATH – path to a local folder</li> <li>• SHAREFOLDERNAME—Network name of a folder</li> </ul> </li> <li>• Null—Property EXISTSHAREFOLDERNAME must be defined</li> </ul>
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
SERVERCERT2048BITS	Size of the key for the Administration Server certificate (bits)	<ul style="list-style-type: none"> <li>• 1—The size of the key for the Administration Server certificate is 2,048 bits.</li> <li>• 0—The size of the key for the Administration Server certificate is 1,024 bits.</li> <li>• If no value is specified, the size of the key for the Administration Server certificate is 1,024 bits.</li> </ul>
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 6. Properties of MSI

MSI property	Description	Available values
DONT_USE_ANSWER_FILE	Read installation settings from response file	<ul style="list-style-type: none"> <li>• 1</li> <li>• Null</li> </ul>
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	<ul style="list-style-type: none"> <li>• 1</li> <li>• Null</li> </ul>
OPENUDPPORT	Whether to open a UDP port	<ul style="list-style-type: none"> <li>• 1</li> <li>• Null</li> </ul>
UDPPORT	UDP port number	
USEPROXY	Whether to use a proxy server	<ul style="list-style-type: none"> <li>• 1</li> <li>• Null</li> </ul>
PROXYADDRESS	Proxy address	
PROXYPORT	Number of port for connection to Administration Server	
PROXYLOGIN	Account for connection to proxy server	
PROXYPASSWORD	<p>Password of account for connection to proxy server</p> <p>Do not specify any details of privileged user accounts in the settings of installation packages.</p>	

MSI property	Description	Available values
GATEWAYMODE	Connection gateway use mode	<ul style="list-style-type: none"> <li>• 0—Do not use connection gateway.</li> <li>• 1—Use this Network Agent as connection gateway</li> <li>• 2—Connect to Administration Server through connection gateway</li> </ul>
GATEWAYADDRESS	Connection gateway address	
CERTSELECTION	Method of receiving a certificate	<ul style="list-style-type: none"> <li>• GetOnFirstConnection—Receive a certificate from Administration Server</li> <li>• GetExistent—Select an existing certificate. If this option is selected, the CERTFILE property must be defined</li> </ul>
CERTFILE	Path to the certificate file	
VMVDI	Enable dynamic mode for Virtual Desktop Infrastructure (VDI)	<ul style="list-style-type: none"> <li>• 1</li> <li>• Null</li> </ul>
LAUNCHPROGRAM	Whether to run Network Agent service after installation	<ul style="list-style-type: none"> <li>• 1</li> <li>• Null</li> </ul>

## 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 [85](#)).

### In this section:

Tips on reducing the load on virtual machines.....	<a href="#">83</a>
Support of dynamic virtual machines.....	<a href="#">84</a>
Support of virtual machines copying.....	<a href="#">85</a>

## 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. Therefore, when copying virtual machines, you usually take the same steps as during deployment performed through disk image copying (see section "Deployment by capturing and copying the hard disk of a device" on page [59](#)).

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\admindkit\ 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\SOFTWAREWow6432Node\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\admindkit\ 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 [50](#)).

## 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 Administration Server (for example, in a Kaspersky Security Center configuration as that described in "Internet access: Network Agent in gateway mode in DMZ" (on page [13](#)), you must specify the address of the connection gateway 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:

Providing Internet access to the Administration Server .....	<a href="#">11</a>
Internet access: Network Agent in gateway mode in a DMZ.....	<a href="#">13</a>



# Deploying the Mobile Device Management feature

In this section:

Installing a Microsoft Exchange Mobile Devices Server .....	<a href="#">89</a>
Installing iOS MDM Server .....	<a href="#">92</a>
Connecting KES devices to the Administration Server .....	<a href="#">97</a>
Integration with Public Key Infrastructure .....	<a href="#">103</a>
Kaspersky Security Center operator .....	<a href="#">104</a>

## Installing a Microsoft Exchange Mobile Devices Server

### Configuring the Internet Information Services web server

When using Microsoft Exchange Server (versions 2010 and 2013), you have to activate the Windows authentication mechanism for a Windows PowerShell™ virtual directory in the settings of the Internet Information Services (IIS) web server. This authentication mechanism is activated automatically if the **Automatic configuration of IIS** check box is selected in the Microsoft Exchange Mobile Devices Server Installation Wizard (default option).

Otherwise, you will have to activate the authentication mechanism on your own.

► *To activate the Windows authentication mechanism for a PowerShell virtual directory manually:*

1. In Internet Information Services (IIS) Manager console, open the properties of the PowerShell virtual directory.
2. Go to the **Authentication** section.
3. Select **Windows authentication**, and then click the **Enable** button.
4. Open **Advanced Settings**.
5. Select the **Enable Kernel-mode authentication** check box.
6. In the **Extended Protection** drop-down list, select **Required**.

When Microsoft Exchange Server 2007 is used, the IIS web server requires no configuration.

## Local installation of a Microsoft Exchange Mobile Devices Server

For a local installation of a Microsoft Exchange Mobile Devices Server, the administrator must perform the following operations:

1. Copy the contents of the \Server\Packages\MDM4Exchange\ folder from the Kaspersky Security Center distribution package to a client device.
2. Run the setup.exe executable file.

Local installation includes two types of installation:

- Standard installation is a simplified installation that does not require the administrator to define any settings; it is recommended in most cases.
- Extended installation is an installation that requires from the administrator to define the following settings:
  - Path for Microsoft Exchange Mobile Devices Server installation
  - Microsoft Exchange Mobile Devices Server operation mode: standard mode or cluster mode (see section "How to deploy a Microsoft Exchange Mobile Devices Server" on page [22](#))

- Possibility of specifying the account under which the Microsoft Exchange Mobile Devices Server service will run (see section "Account for Exchange ActiveSync service" on page [23](#))
- Enabling / disabling automatic configuration of the IIS web server.

The Microsoft Exchange Mobile Devices Server Installation Wizard must be run under an account that has all of the required rights (see section "Rights required for deployment of a Microsoft Exchange Mobile Devices Server" on page [23](#)).

## Remote installation of a Microsoft Exchange Mobile Devices Server

► *To configure the remote installation of a Microsoft Exchange Mobile Devices Server, the administrator must perform the following actions:*

1. In the tree of Kaspersky Security Center Administration Console, select the **Remote installation** folder, then the **Installation packages** subfolder.
2. In the **Installation packages** subfolder, open the properties of the **Microsoft Exchange Mobile Devices Server** package.
3. Go to the **Settings** section.

This section contains the same settings as those used for the local installation of the product.

After the remote installation is configured, you can start installing the Microsoft Exchange Mobile Devices Server.

► *To install a Microsoft Exchange Mobile Devices Server:*

1. In the tree of Kaspersky Security Center Administration Console, select the **Remote installation** folder, then the **Installation packages** subfolder.
2. In the **Installation packages** subfolder, select the **Microsoft Exchange Mobile Devices Server** package.
3. Open the context menu of the package and select **Install application**.

4. In the Remote Installation Wizard that opens, select a device (or multiple devices for installation in cluster mode).
5. In the **Run application installer under specified account** field, specify the account under which the installation process will be run on the remote device.

This account must have all of the required rights (see section "Rights required for deployment of a Microsoft Exchange Mobile Devices Server" on page [23](#)).

## Installing iOS MDM Server

The number of copies of iOS MDM Server to be installed can be selected either based on available hardware or on the total number of mobile devices covered.

However, keep in mind that the recommended maximum number of mobile devices for a single installation of Kaspersky Mobile Device Management is 50,000 at most. In order to reduce the load, the entire pool of devices can be distributed among several servers that have iOS MDM Server installed.

Authentication of iOS MDM devices is performed through user certificates (any profile installed on a device contains the certificate of the device owner). Thus, two deployment schemes are possible for an iOS MDM Server:

- Simplified scheme
- Deployment scheme involving Kerberos constrained delegation (KCD)

Both deployment schemes are described below.

### Simplified deployment scheme

When deploying an iOS MDM Server under the simplified scheme, mobile devices connect to the iOS MDM web service directly. In this case, user certificates issued by Administration Server can only be applied for devices authentication. Integration with Public Key Infrastructure (PKI) is impossible for user certificates (see section "Standard configuration: Kaspersky Mobile Device Management in DMZ" on page [26](#)).

# Deployment scheme involving Kerberos constrained delegation (KCD)

The deployment scheme with Kerberos constrained delegation (KCD) requires the Administration Server and the iOS MDM Server to be located on the internal enterprise network.

This deployment scheme provides for the following:

- Integration with Microsoft Forefront TMG.
- Use of KCD for authentication of mobile devices
- Integration with the PKI for applying user certificates

When using this deployment scheme, you must do the following:

- In Administration Console, in the settings of the iOS MDM web service, select the **Ensure compatibility with Kerberos Constrained Delegation** check box.
- As the certificate for the iOS MDM web service, specify the customized certificate that was defined when the iOS MDM web service was published on TMG.
- User certificates for iOS devices must be issued by the Certificate Authority (CA) of the domain. If the domain contains multiple root CAs, user certificates must be issued by the CA that was specified when the iOS MDM web service was published on TMG.

You can ensure that the user certificate is in compliance with the this CA-issuance requirement by using one of the following methods:

- Specify the user certificate in the New iOS MDM Profile 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:

- Standard configuration: Kaspersky Mobile Device Management on the local network of an enterprise (see section "Standard configuration: iOS MDM Server on the local network of an enterprise" on page [27](#)).
- Integration with PKI (Public Key Infrastructure) (see section "Integration with Public Key Infrastructure" on page [103](#))

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

- iOS MDM web service is running on port 443
- The name of the device with TMG is tmg.mydom.local.
- Name of device with the iOS MDM web service is iosmdm.mydom.local.
- Name of external publishing of the iOS MDM web service is iosmdm.mydom.global.

### **Service Principal Name for http/iosmdm.mydom.local**

In the domain, you have to register the service principal name (SPN) for the device with the iOS MDM web service (iosmdm.mydom.local):

```
setspn -a http/iosmdm.mydom.local iosmdm
```

### **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 that is defined by the SPN (http/iosmdm.mydom.local).

► *To trust the device with TMG to the service defined by the SPN*

*(http/iosmdm.mydom.local), 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. Add the SPN (http/iosmdm.mydom.local) to the **Services to which this account can present delegated credentials** list.

### **Special (customized) certificate for the published web service (iosmdm.mydom.global)**

You have to issue a special (customized) certificate for the iOS MDM web service on the FQDN iosmdm.mydom.global and specify that it replaces the default certificate in the settings of iOS MDM web service in Administration Console.

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

### **Publishing the iOS MDM web service on TMG**

On TMG, for traffic that goes from a mobile device to port 443 of iosmdm.mydom.global, you have to configure KCD on the SPN (<http://iosmdm.mydom.local>), using the certificate issued for the FQDN (iosmdm.mydom.global). Please note that publishing, and the published web service must share the same server certificate.

## **Configuring access to Apple Push Notification service**

To ensure a proper functioning of iOS MDM web service and timely responses of mobile devices to the administrator's commands, you need to specify an Apple Push Notification Service certificate (hereinafter referred to as APNs certificate) in the iOS MDM Server settings.

For information on how to retrieve an APNs certificate, see this article in the Knowledge Base on Technical Support website: <http://support.kaspersky.com/11077>.

Interacting with Apple Push Notification (hereinafter referred to as APNs), the iOS MDM web service connects to the external address gateway.push.apple.com through port 2195 (outbound). Therefore, the iOS MDM web service requires access to port TCP 2195 for the range of addresses 17.0.0.0/8. From the iOS device side is access to port TCP 5223 for the range of addresses 17.0.0.0/8.

If you intend to access APNs from the iOS MDM web service side through a proxy server, you must perform the following actions on the device with the iOS MDM web service installed:

1. Add the following strings to the registry:

- For a 32-bit operating system:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KL  
IOSMDM\1.0.0.0\Conset]
```

```
"ApnProxyHost"="<Proxy Host Name>"
```

```
"ApnProxyPort"="<Proxy Port>"
```

```
"ApnProxyLogin"="<Proxy Login>"
```

```
"ApnProxyPwd"="<Proxy Password>"
```

- For a 64-bit operating system:

```
[HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\KasperskyLab\Components\3  
4\Connectors\KLIOSMDM\1.0.0.0\Conset]
```

```
"ApnProxyHost"="<Proxy Host Name>"
```

```
"ApnProxyPort"="<Proxy Port>"
```

```
"ApnProxyLogin"="<Proxy Login>"
```

```
"ApnProxyPwd"="<Proxy Password>"
```

2. Restart the iOS MDM web service.



# 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 [103](#))
- 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, KSCMobileSvcUsr) 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 `klsvswch` utility. The `klsvswch` 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 KSCMobileSvcUsr 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\KSCMobileSvcUsr
```

## 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, iOS MDM profiles, and files from the shared folder.

The iOS MDM profiles and 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, the properties of Administration Console Web Server provide 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.....	<a href="#">105</a>
Remote access to managed devices.....	<a href="#">107</a>
Mobile Device Management.....	<a href="#">109</a>

## 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 7. Scopes covered by traffic lights in Administration Console

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

Pane name	Traffic light scope
<b>Monitoring</b>	Protection status
<b>Administration Server</b>	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 8. 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.....	<a href="#">107</a>
Checking the time of connection between a device and the Administration Server.....	<a href="#">108</a>
Forced synchronization .....	<a href="#">108</a>
Tunneling .....	<a href="#">108</a>

## 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 no connection through UDP is possible between the Administration Server and a managed device for any reason, synchronization will run at the next routine connection between Network Agent and 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. 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.

# Mobile Device Management

In this section:

Microsoft Exchange Mobile Devices Server .....	<a href="#">109</a>
iOS MDM server.....	<a href="#">110</a>

## Microsoft Exchange Mobile Devices Server

After successful installation, the Microsoft Exchange Mobile Devices Server is displayed in Kaspersky Security Center Administration Console, in the **Mobile Device Management** folder.

## Handling Exchange ActiveSync policies

After you install Microsoft Exchange Mobile Devices Server, in the **Mailboxes** section of the Server properties window, you can view information about accounts of the Microsoft Exchange server that have been retrieved by polling the current domain or domain forest.

Also, in the Microsoft Exchange Mobile Devices Server properties window, you can use the following buttons:

- **Change profiles** allows you to open the **Policy profiles** window, which contains a list of policies retrieved from the Microsoft Exchange server. In this window, you can create, edit, or delete Exchange ActiveSync policies. The **Policy profiles** window is almost identical to the policy editing window in Exchange Management Console.
- **Assign profiles to mobile devices** allows you to assign a selected Exchange ActiveSync policy to one or several accounts.
- **Enable/disable ActiveSync** allows you to enable or disable Exchange ActiveSync HTTP for one or multiple accounts.

## Configuring the scan scope

In the properties of the newly installed Microsoft Exchange Mobile Devices Server, in the **Settings** section, you can configure the scan scope. By default, the scan scope is the current domain in which the Microsoft Exchange Mobile Devices Server is installed. Selecting the **Entire domain forest** value expands the scan scope to include the entire domain forest.

## Working with EAS devices

Devices retrieved by scanning the Microsoft Exchange server will be added to the common list of devices, which is located in the **Mobile Device Management** node, in the **Mobile devices** folder.

If you want the **Mobile devices** folder to display Exchange ActiveSync devices only (hereinafter referred to as EAS devices), filter the device list by clicking the **Exchange ActiveSync (EAS)** link that is located above this list.

You can manage EAS devices by means of commands. For example, the **Delete data** command allows you to remove all data from a device and reset the device settings to the factory settings. This command is useful if the device is lost or stolen, when you need to prevent corporate or personal data from falling into the hands of a third party.

If all data has been deleted from the device, it will be deleted again the next time the device connects to the Microsoft Exchange Server. The command will be reiterated until the device is removed from the list of devices. This behavior is caused by the operation principles of the Microsoft Exchange server.

To remove an EAS device from the list, in the context menu of the device, select **Remove**. If the Exchange ActiveSync account is not deleted from the EAS device, the latter will reappear on the list of devices after the next synchronization of the device with the Microsoft Exchange server.

## iOS MDM Server

This section focuses on the main features for devices managed by an iOS MDM Server (hereinafter referred to as iOS MDM devices).

## In this section:

Adding a new device by publishing a link to a profile.....	<a href="#">111</a>
Adding a new mobile device through profile installation by the administrator.....	<a href="#">111</a>
Sending commands to a device .....	<a href="#">112</a>
Checking the execution status of commands sent.....	<a href="#">112</a>

## Adding a new device by publishing a link to a profile

In Administration Console, the administrator creates a new iOS MDM profile, using the New Mobile Device Connection Wizard. The Wizard performs the following actions:

- The iOS MDM profile is automatically published on the web server.
- The user is sent a link to the iOS MDM profile by SMS or by email. Upon receiving the link, the user installs the iOS MDM profile on the mobile device.
- The mobile device connects to the iOS MDM Server.

## See also:

Kaspersky Security Center operator.....	<a href="#">104</a>
---	---------------------

## Adding a new device through profile installation by the administrator

To connect a mobile device to an iOS MDM Server by installing an iOS MDM profile on that mobile device, the administrator must perform the following actions:

1. In Administration Console, open the New Device Connection Wizard.
2. Create a new iOS MDM profile by selecting the **Show certificate after input completes** check box in the Wizard window.

3. Save the iOS MDM profile.
4. Install the iOS MDM profile on the user's mobile device through the Apple Configurator utility.

The mobile device connects to the iOS MDM Server.

## See also:

Kaspersky Security Center operator.....	<a href="#">104</a>
---	---------------------

## Sending commands to a device

- ▶ *To send a command to an iOS MDM device, the administrator must perform the following actions:*
  1. In Administration Console, open the **Mobile Device Management** node.
  2. Select the **Mobile devices** folder.
  3. In the **Mobile devices** folder, select the mobile device to which the commands need to be sent.
  4. In the context menu of the mobile device, select **Commands for iOS devices** or **Manage device**. In the list that appears, select the command to be sent to the mobile device.

## Checking the execution status of commands sent

- ▶ *To check the execution status of a command that has been sent to a mobile device, the administrator must perform the following actions:*
  1. In Administration Console, open the **Mobile Device Management** node.
  2. Select the **Mobile devices** folder.
  3. In the **Mobile devices** folder, select the mobile device on which the execution status needs to be checked for the selected commands.
  4. In the context menu of the mobile device, select **Show command log**.



---

# 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 .....	<a href="#">113</a>
Hardware requirements for the DBMS and the Administration Server .....	<a href="#">115</a>
Assessing the disk space for an update agent .....	<a href="#">117</a>
Preliminary assessment of space required in the database and on the hard drive for Administration Server .....	<a href="#">117</a>
Assessing traffic between Network Agent and an Administration Server .....	<a href="#">119</a>
Troubleshooting .....	<a href="#">120</a>

# Limitations of Kaspersky Security Center

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

Table 9. 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 <b>Do not disconnect from the Administration Server</b> 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 10. 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 11. 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 12. 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 13. 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:

$$(200 * C + 2.3 * E + 2.5 * A), \text{ KB}$$

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:

$$(220 * C + 0.15 * E + 0.17 * A), \text{ KB}$$

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 14. 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 15. 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 .....	<a href="#">121</a>
Incorrect copying of a hard drive image.....	<a href="#">123</a>
Problems with Microsoft Exchange Mobile Devices Server .....	<a href="#">124</a>
Problems with iOS MDM Server.....	<a href="#">126</a>
Problems with KES devices .....	<a href="#">130</a>

# 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 16. 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.
Poor hardware requirements	The system hardware does not meet the application requirements (RAM, free space on the hard drive, etc.)

Issue	Common causes and solutions
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 with Network Agent installed has been copied without following the rules of deployment (see section "Deployment by capturing and copying the hard drive of a device" on page [59](#)), some devices may be displayed together in Administration Console as 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 Microsoft Exchange Mobile Devices Server

This section provides information about errors and problems that may be encountered when using a Microsoft Exchange Mobile Devices Server.

### Error during installation of a Microsoft Exchange Mobile Devices Server

If an error occurred during a local or remote installation, you can find out the cause of the error by viewing the error.log file located on the device where the product installation has been run,

at C:\Windows\Temp\klmdm4exch-2014-11-28-15-56-37\ (numbers stand for the date and time of the product installation). As a rule, information from the file error.log is enough for solving the problem.

The table below lists examples of the most common errors logged in the error.log file.

Table 17. Common errors

Error	Description	Cause
Error occurred on installation step: 'Test connection to PowerShell'	Error: Processing data from remote server failed with the following error message: The user "oreh-security.ru/Users/TestInstall" isn't assigned to any management roles.	The account under which the product installation has been run, does not have the Organization Management role.
Error occurred on installation step: 'Test connection to PowerShell'	Connecting to remote server failed with the following error message: The WinRM client cannot process the request. The authentication mechanism requested by the client is not supported by the server or unencrypted traffic is disabled in the service configuration. Verify the unencrypted traffic setting in the service configuration or specify one of the authentication mechanisms supported by the server. To use Kerberos, specify the computer name as the remote destination. Also verify that the client computer and the destination computer are joined to a domain. To use Basic, specify the computer name as the remote destination, specify Basic authentication and provide user name and password. Possible authentication mechanisms reported by server: Digest For more information, see the about_Remote_Troubleshooting Help topic.	Windows authentication mechanism is not enabled in the settings of IIS web server for PowerShell virtual directory.

### List of devices and mail accounts is empty

To find out the cause, which makes it impossible to retrieve the list of devices and mail accounts, you can view the events saved in Administration Console, in the **Reports and notifications/Events/Functional failures** folder. If the events contain no information, check

the connection between the Administration Server and Network Agent on the device with Microsoft Exchange Mobile Devices Server deployed.

## Problems with iOS MDM Server

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

### In this section:

Portal support.kaspersky.com .....	<a href="#">126</a>
Checking APN service for accessibility.....	<a href="#">126</a>
Recommended procedure for solving problems with iOS MDM web service .....	<a href="#">127</a>

## Portal support.kaspersky.com

Information about some of the problems that occur when using iOS MDM Server, is given in the Knowledge Base on Technical Support website <http://support.kaspersky.com/ks10mob>.

## Checking APN service for accessibility

To check APN service for accessibility, you can use the following commands from the utility Telnet:

- From the iOS MDM web service side:

```
$ telnet gateway.push.apple.com 2195
```

- From the iOS MDM device side (the check must be performed from the network on which the device is located):

```
$ telnet 1-courier.push.apple.com 5223
```

# Recommended procedure for solving problems with iOS MDM web service

If you encounter some problems when using iOS MDM web service, perform the following actions:

1. Check the certificates for accuracy.
2. Check the events of Administration Console for errors and incomplete commands from iOS MDM Server.
3. Check the mobile device through the iPhone Configuration Utility console.
4. Check the trace files of the iOS MDM web service: Internal services, such as the RPC service and web service (100 streams), must be running successfully.

## Checking the certificate of iOS MDM web service for accuracy using an OpenSSL-based cross-platform utility

### Example of a command:

```
$ openssl s_client -connect mymdm.mycompany.com:443
```

### Execution result

```
CONNECTED(00000003)
```

```
...
```

```
---
```

```
Certificate chain
```

```
0 s:/C=RU/ST=Msk/L=Msk/O=My Company/OU=AdminKit/CN=mymdm.mycompany.com
```

```
i:/CN=Kaspersky iOS MDM Server CA
```

```
...
```

```
.
```

## Checking trace files of the iOS MDM web service

To find out how to receive trace files of the iOS MDM web service, please refer to the relevant article in the Knowledge Base on Technical Support website <http://support.kaspersky.com/9792>.

### Example of successful tracing:

```
I1117 20:58:39.050226 7984] [MAIN]: Starting service...
I1117 20:58:39.050226 7984] [RPC]: Starting rpc service...
...
I1117 20:58:39.081428 7984] [RPC]: Rpc service started
I1117 20:58:39.081428 3724] [WEB]: Starting web service...
I1117 20:58:39.455832 3724] [WEB]: Starting thread [T000]
I1117 20:58:39.455832 3724] [WEB]: Starting thread [T001]
...
I1117 20:58:39.455832 3724] [WEB]: Starting thread [T099]
```

### Example of tracing with an occupied socket:

```
[WEB]: Starting web service...
```

```
Error 28 fault: SOAP-ENV:Server [no subcode] "Only one usage of each socket address
(protocol/network address/port) is normally permitted."
```

```
Detail: [no detail]
```

```
[WEB]: Web service terminated
```



## Checking trace files using the console of iPhone Configuration Utility

### Example of successful tracing:

Services covering MDM – profiled, mdmd

mdmd[174] <Notice>: (Note ) MDM: mdmd starting...

mdmd[174] <Notice>: (Note ) MDM: Looking for managed app states to clean up

profiled[175] <Notice>: (Note ) profiled: Service starting...

mdmd[174] <Notice>: (Note ) MDM: Network reachability has changed.

mdmd[174] <Notice>: (Note ) MDM: Network reachability has changed.

mdmd[174] <Notice>: (Note ) MDM: Polling MDM server <https://10.255.136.71> for commands

mdmd[174] <Notice>: (Note ) MDM: Transaction completed. Status: 200

mdmd[174] <Notice>: (Note ) MDM: Attempting to perform MDM request: DeviceLock

mdmd[174] <Notice>: (Note ) MDM: Handling request type: DeviceLock

mdmd[174] <Notice>: (Note ) MDM: Command Status: Acknowledged

profiled[175] <Notice>: (Note ) profiled: Recomputing passcode requirement message

profiled[175] <Notice>: (Note ) profiled: Locking device

mdmd[174] <Notice>: (Note ) MDM: Transaction completed. Status: 200

mdmd[174] <Notice>: (Note ) MDM: Server has no commands for this device.

mdmd[174] <Notice>: (Note ) MDM: mdmd stopping...

# 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 .....	<a href="#">130</a>
Checking the settings of Google Firebase Cloud Messaging service.....	<a href="#">130</a>
Checking Google Firebase Cloud Messaging for accessibility.....	<a href="#">130</a>

## 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:\[YOUR PROJECT NUMBER\]:access](https://code.google.com/apis/console/#project:[YOUR PROJECT NUMBER]:access).

## 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 [101](#)), 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 .....	<a href="#">131</a>
Technical support by phone .....	<a href="#">132</a>
Technical Support via Kaspersky CompanyAccount .....	<a href="#">132</a>

## 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](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

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

Apple, iPhone are trademarks of Apple Inc. registered in the USA and elsewhere.

Xen is a trademark of Citrix Systems, Inc. and / or its subsidiaries registered in the United States Patent and Trademark Office and elsewhere.

Android, Google are trademarks of Google, Inc.

JavaScript is a registered trademark of Oracle Corporation and / or its affiliated companies.

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

UNIX is a trademark registered in the U.S. and elsewhere and is used under license from X/Open Company Limited.

VMware and ESXi are trademarks of VMware, Inc., or trademarks owned by VMware, Inc. and registered in the U.S. and elsewhere.