Kaspersky Security Center 10

BEST PRACTICES

APPLICATION VERSION: 10 SERVICE PACK 1

Dear User,

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

Document revision date: 9/14/2015

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

TABLE OF CONTENTS

ABOUT THIS DOCUMENT

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

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

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

IN THIS SECTION:

IN THIS DOCUMENT

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

Planning Kaspersky Security Center deployment (see page 8)

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 and Network Access Control (NAC).

Deployment and initial setup (see page 19)

This section provides information about Administration Server deployment, Network Agent and Anti-Virus deployment, and initial setup of Kaspersky Security Center. It also provides information about backup and restoration of Administration Server settings, support of out-of-office users, and NAC configuration and usage.

Routine use (see page 63)

This section provides information about the daily routine use of the application. This section contains information about how to use remote access to computers, manage mobile devices, and apply standard NAC scenarios to monitor activities of network devices.

Contacting the Technical Support Service (see page 81)

This section provides information about how to obtain technical support and what conditions must be met to receive help from the Technical Support Service.

AO Kaspersky Lab (see page 83)

This section provides information about Kaspersky Lab.

Trademark notices

This section contains registered trademark notices.

DOCUMENT CONVENTIONS

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

Table 1. Document conventions

SAMPLE TEXT	DOCUMENT CONVENTIONS DESCRIPTION
Note that...	Warnings are highlighted with red color and boxed. Warnings contain information about actions that may lead to some unwanted outcome.
We recommend that you use...	Notes are boxed. Notes contain additional and reference information.
Example: ...	Examples are given on a yellow background under the heading "Example".
Update means... The *Databases are out of date* event occurs.	The following elements are italicized in the text: • New terms. • Names of application statuses and events.
Press **ENTER**. Press **ALT**+**F4**.	Names of keyboard keys appear in bold and are capitalized. Names of keys that are connected by a + (plus) sign indicate the use of a key combination. Those keys must be pressed simultaneously.
Click the **Enable** button.	Names of application interface elements, such as entry fields, menu items, and buttons, are set off in bold.
➧ *To configure task schedule:*	Introductory phrases of instructions are italicized and accompanied by the arrow sign.
Enter `help` in the command line The following message then appears: `Specify the date in dd:mm:yy format.`	The following types of text content are set off with a special font: • text in the command line; • text of messages displayed on the screen by the application; • data that the user have to enter from the keyboard.
<User name>	Variables are enclosed in angle brackets. Instead of a variable, the corresponding value must be inserted, with angle brackets omitted.

PLANNING KASPERSKY SECURITY CENTER DEPLOYMENT

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

- Total number of hosts
- 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 9).

One Administration Server can support a maximum 50,000 computers. If the total number of computers 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 12).

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 computers on a detached network will retrieve updates from such local update centers. These Update Agents can download updates either from the Administration Server (the default option) or from Kaspersky Lab servers on the Internet.

See section "Standard configuration: Multiple small remote offices" (on page 12).

The section "Standard configurations of Kaspersky Security Center" (on page 11) 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 (customized) certificate X.509 to the Administration Server must be considered. Assignment of the customized certificate X.509 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 the section Specifying the Administration Server certificate (on page 22).

IN THIS SECTION:

HOW TO SELECT A DBMS FOR THE ADMINISTRATION SERVER

When selecting the database management system (DBMS) to be used by an Administration Server, you must take into account the number of computers 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 SQL Server Express edition DBMS can be used if the Administration Server covers more than 10,000 hosts. If the Administration Server supports more than 10,000 computers, 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.

If the Administration Server covers 10,000 or fewer computers, MySQL 5.0 can also be used as the DBMS.

SEE ALSO:

PROVIDING INTERNET ACCESS TO THE ADMINISTRATION SERVER

The following cases require Internet access to the Administration Server:

- Managing computers (laptops) of out-of-office users
- Managing computers 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 the section “Specifying the Administration Server certificate“ on page 22).

IN THIS SECTION:

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 computers.
- The Administration Server cannot perform initial deployment of Network Agent by means of push installation on computers in the internal network of the enterprise.

This only applies to the initial installation of Network Agent. Any further upgrades of Network Agent or installation of Kaspersky Anti-Virus 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 computers via port 15000 UDP, which is not critical for the functioning of Kaspersky Security Center.
- 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 means of Update Agents located within the enterprise network:

- To perform the initial deployment on computers without Network Agent, you first install Network Agent on one of the computers and then assign it Update Agent status. As a result, initial installation of Network Agent on other computers will be performed by the Administration Server through this Update Agent.
- To detect new computers 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 computers located within the internal network of the enterprise, you must fill the entire network with Update Agents at a rate of 100 to 200 computers per one Update Agent. In the properties of the assigned Update Agents, select the **Do not disconnect 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 the port 15000 UDP on computers within the internal network of the enterprise (see section "About Update Agents" on page 12).

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 on the internal network of the enterprise, an in the network DMZ there can be a computer 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 computer that 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 computer must be assigned connection gateway status by address. You must not add any computers to this administration group.
- For Network Agents that attempt to access the Administration Server via the Internet, use **Connect to Administration Server via 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

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 70) or the total number of hosts.

An Administration Server can support up to 50,000 computers. You must consider the possibility of increasing the number of managed computers in the near future: it may be useful to connect a slightly smaller number of computers 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 dubbed policies and tasks, handle the whole set of managed computers, as if they are managed by a single Administration Server: i.e., search for computers, build selections of computers, and create reports.

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

SEE ALSO:

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 computers 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 must be combined into a hierarchy (possibly multilevel).

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

SEE ALSO:

Standard configuration: Single office 11

Administration Server hierarchy 13

Configuring connection profiles for out-of-office users 50

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 several 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 computers 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 computers have no Internet access), the Update Agents must be switched into connection gateway mode. In this case, Network Agents on computers 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 computers 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 computers acting as Update Agents (**Do not disconnect 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 9

About Update Agents 12

ABOUT UPDATE AGENTS

Network Agent can be used as an 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 computer, which acts as the Update Agent.
- Install software (including initial deployment of Network Agents) on other computers.
- Scan the network to detect new computers 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's network pursues the following objectives:

- Reduces the load on the Administration Server.
- Optimizes traffic.
- Provides the Administration Server with access to computers 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 computers 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 computers within the administration group and all of its subgroups. However, the computer 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, computers 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 computers with Network Agent and an Administration Server.

SEE ALSO:

Internet access: Network Agent in gateway mode in a DMZ 10

Standard configuration: Multiple small remote offices 12

Building a structure of administration groups and assigning Update Agents 27

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.
- Sets of selected computers on the master Administration Server can include computers 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 computers with policies and tasks, each virtual Administration Server features its own group of unassigned computers, own sets of reports, selected computers 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 computers, groups, events, and objects on managed computers (items in Quarantine, applications registry, etc.) of all its virtual Administration Servers.
- A virtual Administration Server can scan the network only with Update Agents connected.

INSTALLING IMAGES OF OPERATING SYSTEMS

Kaspersky Security Center allows the deployment of WIM images of desktop and server-based Windows® operating systems on computers 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 computer.

Two scenarios are supported for deployment of operating system images:

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

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 computers 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 on the network where the target computer is located.
- The Administration Server's shared folder must be open for reading from the network that hosts the target computer. If the shared folder is located on the Administration Server, access must be granted to the KlPxeUser 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 CPU architecture of the target computer: x86 or x86-64.

MOBILE DEVICE MANAGEMENT

IN THIS SECTION:

EXCHANGE ACTIVESYNC MOBILE DEVICE 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 AN EXCHANGE ACTIVESYNC MOBILE DEVICE SERVER

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

If no Client Access server array of Microsoft Exchange Servers has been deployed in the organization, an Exchange ActiveSync Mobile Device 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 Exchange ActiveSync Mobile Device Server.

Together with the Exchange ActiveSync Mobile Device Server, Network Agent must be installed on the computer; it helps integrate the Exchange ActiveSync Mobile Device Server with Kaspersky Security Center.

The default scan scope of the Exchange ActiveSync Mobile Device Server is the current Active Directory domain in which it was installed. Deploying an Exchange ActiveSync Mobile Device 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 Exchange ActiveSync Mobile Device Server (see section "Configuring the scan scope" on page 65). 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 an Exchange ActiveSync mobile device 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 an Exchange ActiveSync Mobile Device Server (or multiple clusters of Exchange ActiveSync Mobile Device 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 an Exchange ActiveSync Mobile Device Server 52

Configuring the scan scope 65

RIGHTS REQUIRED FOR DEPLOYMENT OF AN EXCHANGE ACTIVESYNC MOBILE DEVICE SERVER

Deployment of an Exchange ActiveSync Mobile Device Server on Microsoft Exchange Server (2010, 2013) requires domain administrator rights and the Organization Management role. Deployment of an Exchange ActiveSync Mobile Device 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 an Exchange ActiveSync Mobile Device 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 service of the Exchange ActiveSync Mobile Device Server 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>"	`Add-ADPermission -User <User or group name> -Identity "CN=Mobile Mailbox Policies,CN=<Organization name>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Domain name>" -InheritanceType All -AccessRight GenericAll`
Read	Thread "CN=<Organization name>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Domain name>"	`Add-ADPermission -User <Domain name> -Identity "CN=<Organization name>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Domain name>" -InheritanceType All -AccessRight GenericRead`
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 Mobile Device Server

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

- Device lock
- Password reset

- Device 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.).

An iOS MDM Mobile Device 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 computer with an iOS MDM Mobile Device Server deployed.

When deploying an iOS MDM Mobile Device 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 Mobile Device Server.

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

IN THIS SECTION:

STANDARD CONFIGURATION: KASPERSKY MOBILE DEVICE MANAGEMENT IN DMZ

An iOS MDM Mobile Device 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 Mobile Device 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 10):
  a. On the computer with the deployed iOS MDM Mobile Device Server, connect Network Agent to the Administration Server by a connection gateway.
  b. On the computer with the deployed iOS MDM Mobile Device Server, assign Network Agent as the connection gateway.

SEE ALSO:

STANDARD CONFIGURATION: IOS MDM MOBILE DEVICE SERVER ON THE LOCAL NETWORK OF AN ENTERPRISE

An iOS MDM Mobile Device 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 56).

Any standard configuration requires access to Apple web services for the iOS MDM Mobile Device 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 55).

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 computers:
  - 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 9

Defining the Administration Server certificate 22

ABOUT NETWORK ACCESS CONTROL (NAC)

By default, Network Access Control (NAC) is designed for collecting and auditing information about Ethernet access granted to devices. Using NAC, you can retrieve a few basic network settings of devices, such as their MAC addresses, IP addresses, NetBIOS names, and some advanced settings defined during an active scan: operating system version, device type, list of opened network ports, etc.

Creating access distribution policies allows you to define criteria and rules that will be used for granting a device full or partial access to network resources or granting no access. A set of criteria used for describing one or several devices is called a *network object*. Criteria of a network object include basic network settings, as well as advanced settings defined during an active scan. Rules, in their turn, define the type of access to network resources that will be granted to devices (if they meet the relevant criteria).

Network Agents perform audits of device access to the network, and apply policies. A Network Agent with the NAC feature enabled is called a *NAC agent*. Proper NAC functioning requires one active NAC agent in each of the broadcasting domains on the network. For example, if a network of 50,000 devices includes 50 broadcasting domains, each of them requires one active NAC agent, for a total of 50 active NAC agents. *A NAC agent is active if it is running in Main mode*. If an active NAC agent cannot function properly (for example, when the computer is restarted), a reserve NAC agent (which normally runs in Reserve mode) can take on the functions of the active NAC agent. The reserve NAC agent (if available) must operate in the same broadcast domain as the main one.

NAC agents use an active port monitoring technology known as Nmap; thus, if most popular ports are closed on a device, the results of a scan may lack accuracy or be completely missing.

The current implementation features NAC included in Kaspersky Security Center and is built on technologies of ARP traffic manipulation and analysis. If NAC is running in Simulation mode, only ARP traffic analysis is used and no ARP traffic manipulation is applied.

In view of restrictions imposed by ARP, any NAC agent activities will not go beyond the broadcast domain. This domain is limited by a router, as a rule. Using NAC requires disconnecting the protection from ARP spoofing on routers.

IEEE 802.11 (Wi-Fi) networks are not supported currently.

SEE ALSO:

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 the computers 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 computers of the administrator.
- Network Agent—Designed for managing the Anti-Virus application installed on a computer, as well as collecting information about that computer. Network Agents are installed on the computers 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 computer
- Installation of Network Agent and an anti-virus application on computers of the enterprise.

IN THIS SECTION:

INSTALLING ADMINISTRATION SERVER

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

IN THIS SECTION:

CREATING ACCOUNTS FOR SERVICES OF ADMINISTRATION SERVER

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

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	It is recommended that you avoid covering more than 10,000 computers with a single Administration Server.
Local SQL Server edition other than Express	No limitations.
Remote SQL Server edition other than Express	Only valid if both computers 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	An Administration Server can cover a maximum 10,000 computers.

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

SEE ALSO:

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 computer 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

If the target computers are located within a Windows domain (no workgroups), initial deployment (installation of Network Agent and an Anti-Virus application on computers 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 in order to reduce the load on the disk subsystem of the Administration Server computer.

REMOTE INSTALLATION THROUGH DELIVERY OF THE UNC PATH TO A STAND-ALONE PACKAGE

If the users of networked computers in an 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 Anti-Virus application). After creating a stand-alone package, you must 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 computers, it is useful to locate the shared folder on a dedicated file resource.

INSTALLING IMAGES OF OPERATING SYSTEMS

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

SEE ALSO:

Deploying Network Agent and an anti-virus application 34

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 computer is used. If the Domain Name System (DNS) on the enterprise network has been configured and is functioning properly, you specify in the DNS the FQDN of the Administration Server computer. 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 10

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 8).

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 [-l 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: • C – Replace the certificate for ports 13000 and 13291; • CR – Replace the reserve certificate for ports 13000 and 13291; • M – Replace the certificate for mobile devices on port 13292.
-i FILE	Container with the certificate in PKCS#12 format (file with the extension .p12 or .pfx).
-p PASSWORD	Password used for protection of the .p12 container with the certificate.
-l LOGFILE	Results output file. By default, the output is redirected into the standard output stream.

INITIAL SETUP

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

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

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

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

IN THIS SECTION:

MANUAL SETUP OF KASPERSKY ENDPOINT SECURITY POLICY

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

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

IN THIS SECTION:

CONFIGURING THE POLICY IN THE ANTI-VIRUS PROTECTION SECTION

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

Anti-Virus protection section, Firewall subsection

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

To check the list of networks:

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

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

Anti-Virus protection section, File Anti-Virus subsection

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

To disable scanning of network drives:

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

CONFIGURING THE POLICY IN THE ADVANCED SETTINGS SECTION

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

Advanced Settings section, Reports and Storages subsection

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

- The **About vulnerabilities found** check box: This setting is primarily required for providing backward compatibility with Kaspersky Security Center 9. Detection of vulnerabilities is integrated into Kaspersky Security Center, starting from version 10. Therefore, if you use Administration Server and Network Agents of version 10 or later, make sure that this check box is cleared.
- The **About started applications** check box: If this check box is selected, the Administration Server database saves information about all versions of all of the application modules on the networked computers in the enterprise. 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 on the enterprise network must be managed in centralized mode through Administration Console, you must disable the display of the user interface of Kaspersky Endpoint Security 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** 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 COMPUTER WITH KASPERSKY ENDPOINT SECURITY

The Quick Start Wizard creates a group task for scanning a computer. 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 the computers within an organization are turned off on Fridays, for example, at 6:30 PM, the computer 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 turning off the computers at this time, the vulnerability scan task will run after the computers are turned on again, that is, on Wednesday morning. Such activity may be undesirable because a vulnerability scan may increase the load on the computer CPU and disk subsystem. 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 disabling computers 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 computer.

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 computers, by using *policy profiles*. In this case, the scope of policies is set with tags, computers' locations in organizational units of Active Directory, membership in Active Directory security groups, etc. (see the section “Hierarchy of policies, using policy profiles“ on page 28).

- 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 computer selections and tasks for specific computers.

- Sets access rights to computers, 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

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

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

- Building the structure of administration groups taking into account the network topology. The structure of administration groups may not reflect the network topology with absolute precision. A match between the separate parts of the network and certain administration groups would be enough. You can use automatic assignment of Update Agents or assign them manually.
- Building the structure of administration groups, without taking the network topology into account. In this case, you must disable automatic assignment of Update Agents and then assign one or several computers to act as Update Agents for a root administration group in each of the separate parts of the network, for example, for the **Managed computers** group. All Update Agents will be at the same level and will feature the same scope spanning all computers in the enterprise network. In this case, each of Network Agents in version 10 SP1 or later will connect to the Update Agent that has the shortest route. The route to an Update Agent can be traced with the tracert utility.

When assigning Update Agents manually, you must assign 100 to 200 managed computers to a single Update Agent. Update Agents must be powerful computers with a sufficient amount of free disk space (see the section “Assessing the disk space for an Update Agent“ on page 71). Update Agents must not be shut down frequently, and 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).

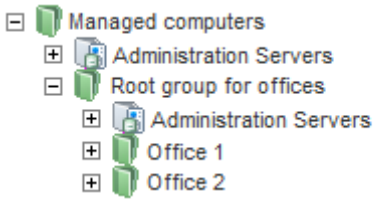

Figure 1. Creating a report delivery task

One or several Update Agents must be assigned to each administration group corresponding to an office. Update Agents must be computers at the remote office that have a sufficient amount of free disk space (see the section “Assessing the disk space for an Update Agent“ on page 71). Computers deployed in **Office 1** group, for example, will access the 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 computers (in addition to the existing Update Agents) in each remote office and assign them 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 Update Agents assigned to the **Office 1** group, but those Update Agents are unavailable. Then, Network Agent starts attempting to access 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 **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 computers in administration groups. This section also provides information about policy profiles supported in Kaspersky Security Center, starting from version 10 SP1.

IN THIS SECTION:

HIERARCHY OF POLICIES

In Kaspersky Security Center, you use policies for defining a single collection of settings to multiple computers. For example, the policy scope of product P defined for administration group G includes managed computers with product P installed that have been deployed in group G and all of its subgroups, except for those 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 computer 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 computer when the computer 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 computers through the hierarchy of administration groups only 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 computers together with the policy and supplements 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 had been 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 computer's 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 properties of the computer 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 the section “Configuring connection profiles for out-of-office users“ on page 50)
  - Presence or absence of the specified tags on the computer
  - Computer's allocation in an Active Directory organizational unit (OU): explicit (the computer is right in the specified OU) or implicit (the computer is in an OU, which is within the specified OU at any nesting level)
  - Computer's membership in an Active Directory security group (explicit or implicit).
  - Computer 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 **Computer in out-of-office mode** 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 be activated only after the computer 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 computers. Local tasks can be modified either by the administrator on the Kaspersky Security Center side by using Administration Console tools, but also by the user of a remote computer (for example, through the interface of the Anti-Virus application). If a local task has been simultaneously modified by the administrator and the user of a managed computer, 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) computers that have been connected to slave and virtual Administration Servers deployed in that group or any of its subgroups.
- Tasks for specific computers—Affect a limited set of computers that was specified when the task was created.
- Tasks for selections of computers—Affect computers that are included in a specified selection. Over time, the scope of the task changes as the set of computers included in the selection change. A selection of computers can be made on the basis of the computer attributes, including software installed on a computer, as well as on the basis of tags assigned to computers. The selection is the most flexible way of defining the scope of a task.

  Tasks for selections of computers are always run upon a schedule by Administration Server. These computer selection tasks cannot be run on computers that lack a connection with Administration Server. Tasks are not run on the local time of a target computer; instead, they are run on the local time of Administration Server.

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

COMPUTER MOVING RULES

It is advisable to set automatic allocation of computers to administration groups, This is done by applying *computer moving rules*. A computer moving rule consists of three main parts: a name, an execution condition (logical expression with the computer attributes), and a target administration group. A rule moves a computer to the target administration group if the computer attributes meet the rule execution condition.

Computer moving rules have priorities. Administration Server checks a computer attributes for meeting the execution condition of each rule, in ascending order of priority. If the computer attributes meet the execution condition of a rule, the computer moves to the target group, and rule processing is complete for the computer. If the computer attributes satisfy several rules, the computer moves to the target group of the rule with the highest priority (that is, has the highest rank in the list of rules).

Computer moving rules can be created implicitly. For example, in the properties of a remote installation package or task, you can specify the administration group to which the computer must move 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** group.

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

You can move computers that have already been allocated to administration groups. To do this, in the properties of a rule, clear the **Move only computers not added to administration groups** check box.

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

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

We strongly recommend that you avoid moving a single computer from one group to another repeatedly (for example, in order to apply a special policy to that computer, run a special group task, or update the computer through a specified 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 29), tasks for selections of computers (see the section “Tasks“ on page 30), through the assignment of Network Agents according to the standard scenario (see the section “Building a structure of administration groups and assigning Update Agents“ on page 27), etc.

SOFTWARE CATEGORIZATION

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

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 Administration Server, such as: Administration Server's certificates, master keys for encryption of drives on managed computers, 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 computers will also be lost, risking irrevocable loss of encrypted data on computers 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\Kaspersky SC.

If an instance of Microsoft SQL Server installed on another computer 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's service and the SQL Server's 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's certificates, keys for licenses, and master keys for encryption of drives on managed computers 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 COMPUTER WITH ADMINISTRATION SERVER IS INOPERABLE

If a computer 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 computer.
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 AN ANTI-VIRUS APPLICATION

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

IN THIS SECTION:

INITIAL DEPLOYMENT

If Network Agent has already been installed on a computer, remote installation of applications on that computer 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 computers on which Network Agent is already installed, see below in this section.

You can perform initial installation of Network Agent on computers 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 computer users links to standalone packages generated by Kaspersky Security Center. Standalone packages are executable modules that contain the distribution packages of selected applications with their settings defined.
- Manually, by running the installers of products on target computers.

On platforms other than Windows, initial installation of Network Agent on managed computers must be performed through available third-party tools. You can upgrade Network Agent to a new version or install other Kaspersky Lab applications on the non-Windows platforms, using Network Agent (already installed on computers) 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 the section "Standard configurations of Kaspersky Security Center" on page 11)
- Total number of hosts
- Presence of computers on the enterprise's network, which are not members of any Active Directory domain, and presence of uniform accounts with administrator rights on those computers
- Capacity of the channel between Administration Server and target computers
- Type of communication between Administration Server and remote subnets and capacity of network channels in those subnets
- Security settings applied on remote computers 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 must 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 computer), all relevant settings can be defined through the installer's user interface.

This method of defining the settings is inappropriate for non-interactive, "silent" installation of applications on groups of computers. 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 computers.

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 with Kaspersky Security Center tools, installation packages are delivered to target computers 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 just have to ensure the availability of the entire installation package, that is, 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 21).

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 37).

Immediately after Kaspersky Security Center is installed, a few installation packages are automatically generated; they are ready to be installed and include Network Agent packages and Anti-Virus packages for Microsoft Windows platform.

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 must 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 the section "Configuring installers" on page 44).

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 21

Configuring installers 44

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 computers or a selection of computers (such tasks are displayed in Administration Console, in the **Tasks for specific computers** 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 computers included in a specified group and all computers in all subgroups within that administration group. A task covers computers of slave Administration Servers included in a group or any of its subgroups if the corresponding setting has been enabled in the task.

Tasks for specific computers refresh the list of client computers at each run in accordance with the set of a selection at the moment the task starts. If a selection includes computers that have been connected to slave Administration Servers, the task will run on those computers, 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 computers connected to slave Administration Servers, you must use the retranslation task to relay installation packages used by your task to corresponding slave Administration Servers in advance.

DEPLOYMENT BY CAPTURING AND COPYING THE HARD DRIVE OF A COMPUTER

If you have to install Network Agent on computers on which an operating system and other software also must be installed (or reinstalled), you can use the mechanism of capturing and copying the computer's hard disk.

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

1. Create a "reference" computer with an installed operating system and the required software, including Network Agent and an Anti-Virus application.
2. Capture the reference image on the computer and distribute that image on new computers 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 14).

If you use any third-party tools for handling disk images, you must delete the information that Kaspersky Security Center uses to identify the managed computer, when performing deployment on a target computer from a reference image. Otherwise, Administration Server will not be able to properly distinguish computers that have been created by means of 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 computer with Network Agent installed, use one of the following methods:

- Recommended method. When installing Network Agent on a reference computer, select **Do not run service when installation completes** and capture the computer image before the first run of Network Agent service (because unique information identifying the computer is created at the first connection of Network Agent to 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 computer, stop Network Agent service and run the klmover utility with the key -dupfix. 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 utility will be run with the key -dupfix prior to (mandatory requirement) the first run of Network Agent service on target computers, 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 the section Hard drive image copying has been performed incorrectly (on page 74).

You can apply an alternate scenario for deployment of Network Agent on new computers, using 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 run upon completion of the image deployment on target computers.

This deployment scenario adds flexibility: You can use a single operating system image along with various installation options for Network Agent and / or an Anti-Virus product, including computer 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 computer (see the section "Installing images of operating systems" on page 14).

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:

- Target computers are members of an Active Directory domain.
- The deployment scheme allows you to wait for a regular restart of target computers before starting deployment of Network Agents on them (or you can apply a group policy of Windows to those computers forcedly).

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 computers 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 computers.
- The next time a target computer logs in to the domain (before users of the computer 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 computers when the operating system is loading, that is, 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 computers 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 selecting this deployment scheme, you must also assess the workload on the file resource from which files will be copied to target computers after applying the group policy of Windows.

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 computers 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 target computers 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 target computer. 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 target computers 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 21).

In addition to its ease of use, automatic creation of Windows group policies through Kaspersky Security Center has this advantage: when planning the installation of Network Agent, you can easily specify the administration group of Kaspersky Security Center into which computers 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 target computers 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 computers of 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 44).

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 computers log in to the domain, or if any target computers that are not members of the Active Directory domain are available, you can use the forced installation of selected installation packages through the remote installation task of Kaspersky Security Center.

In this case, you can specify target computers either explicitly (with a list), or by selecting the administration group of Kaspersky Security Center to which they belong, or by creating a selection of computers 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 computers 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 of the target computers and remote registration of supporting services on them. The following conditions must be met in this case:

- Target computers must be available for connection either from the Administration Server's side, or from the Update Agent's side.
- Name resolution for target computers must function properly on the network.
- The administrative shares (admin$) must remain enabled on target computers.
- The system service Server must be running on target computers (by default, it is running).
- The following ports must be opened on target computers to allow remote access through Windows tools: TCP 139, TCP 445, UDP 137, UDP 138.
- Simple File Sharing mode must be disabled on target computers.
- On target computers, 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 computers must be members of the domain, or uniform accounts with administrator rights must be created on target computers in advance.

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

When creating a group task, keep in mind that each group task affects all computers 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, in the properties of the administration group, open the list of installation packages and select the ones that must be installed on computers in this group. As a result, the selected installation packages will be automatically installed on all computers 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 computers.

Forced installation can also be applied if target computers are not directly accessible for Administration Server: e.g., computers are on isolated networks, or computers are on the local network while 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 computers on subnets communicated with Administration Server via a narrow channel while a broader channel is available between computers on that subnet. However, note that this installation method places a significant load on computers acting as Update Agents. Therefore, it is recommended that you select powerful computers 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 71).

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 computers that have no access to the shared folder of Kaspersky Security Center. The administrator can copy the stand-alone package to an external device, deliver it to a relevant computer, and then run it.

You can create a stand-alone package from a Network Agent package, a package of another (for example, Anti-Virus) 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 computers (those that have not been allocated to any administration group) will be automatically moved when installation of Network Agent 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 COMPUTERS 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 computer, you can upgrade the version of Network Agent on this computer, as well as install, upgrade, or remove any supported applications with 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 36).

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

In order to optimize the load on the Administration Server and minimize traffic between the Administration Server and target computers, 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 12) and Building a structure of administration groups and assigning Update Agents (on page 27)). In this case, installation packages and the installer's settings are distributed from Administration Server to target computers 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 computers 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 folder %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\FTServer. 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 folder %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\$FTClTmp.

Files cannot be deleted from the $FTClTmp 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 computers.

MANAGING RESTARTS OF TARGET COMPUTERS IN THE REMOTE INSTALLATION TASK

Computers 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 the computer**. In this case, no automatic restart will be performed. To complete the installation, you must restart the computer (for example, manually or through the computer management task). Information about the compulsory restart will be saved in the task results and in the computer status. This option is suitable for tasks of installation on servers and other computers where continuous operation is critical.
- **Restart the computer**. In this case, the computer is always restarted automatically if a restart is required for completion of the installation. This option is useful when running installation tasks on computers that provide for regular pauses in their operation (turning off or restart).
- **Prompt user for action**. In this case, the restart reminder is displayed on the screen of the client computer and asks 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 deployment of anti-virus protection, you must keep in mind the possibility of updating anti-virus databases (including modules of automatic patches) shipped along with the distribution package of the anti-virus 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). The pre-deployment database update will reduce the number of restarts required for completion of Anti-Virus protection deployment on target computers.

SELECTING A METHOD FOR UNINSTALLING INCOMPATIBLE APPLICATIONS WHEN INSTALLING A KASPERSKY LAB ANTI-VIRUS APPLICATION

Installation of an Anti-Virus application of Kaspersky Lab through Kaspersky Security Center may require removing 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 installation of an Anti-Virus application, all incompatible applications are removed automatically if in the properties window of the installation package of this Anti-Virus application (**Incompatible applications** section) the **Uninstall incompatible applications automatically** check box is selected.

Removing incompatible applications through a dedicated task

To remove incompatible applications, use the **Uninstall application remotely** task. This task must be run on target computers immediately before the Anti-Virus application installation task is run. 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 installer of an Anti-Virus application cannot remove an incompatible application properly.

USING TOOLS FOR REMOTE INSTALLATION OF APPLICATIONS IN KASPERSKY SECURITY CENTER FOR RUNNING RELEVANT EXECUTABLE FILES ON MANAGED COMPUTERS

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 the target computers.

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:

```
[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:

```
[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:

```
[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:

```
[SetupProcessResult_SuccessCodes]
0= Installation completed successfully
3010=A reboot 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 computer 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:

```
[SetupProcessResult_NeedReboot]
3010=
```

MONITORING THE DEPLOYMENT

To monitor the deployment of Kaspersky Security Center, as well as check the availability of an Anti-Virus application and Network Agent on managed computers, you can watch a traffic light icon named **Deployment** located in the workspace of the Administration Server node in the Administration Console main window (see section "Traffic lights in Administration Console" on page 63).

The traffic light reflects the current status of the deployment. Next to the traffic light is displayed the number of computers with Network Agent and Anti-Virus applications installed. When any active installation tasks are running, you can monitor their progress here. When any installation errors are returned, the number of errors is displayed; you can also click a link to view more details on an error.

You can also use the deployment chart in the workspace of the **Managed computers folder on the** Groups tab. The chart reflects the deployment process, showing the number of computers without Network Agent, with Network Agent, or with Network Agent and an anti-virus 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 results window opens and shows two lists: the upper one lists the statuses of the task on target computers, while the lower one lists the task events on the computer that is currently selected in the upper list.

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

CONFIGURING INSTALLERS

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

IN THIS SECTION:

GENERAL INFORMATION

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

INSTALLATION IN SILENT MODE (WITH A RESPONSE FILE)

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

An overview of an example run follows:

```
setup.exe /s
```

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

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

INSTALLATION IN SILENT MODE (WITHOUT A RESPONSE FILE)

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

Example:

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

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

Example:

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

You can specify several response files in a single command.

INSTALLATION IN SILENT MODE (WITHOUT A RESPONSE FILE)

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)	• 1 • Null
INSTALLATIONMODETYPE	Type of Administration Server installation	• Standard • Custom
INSTALLDIR	Product installation folder	
ADDLOCAL	List of components to install (separated by commas)	CSAdminKitServer, Nagent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, CiscoNACServer, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86
NETRANGETYPE	Network Size	• NRT_1_100—From 1 to 100 computers • NRT_100_1000—From 100 to 1,000 computers • NRT_GREATER_1000—1,000 or more computers
SRV_ACCOUNT_TYPE	Way of specifying the user for operation of Administration Server service	• SrvAccountDefault – User account will be created automatically • SrvAccountUser—User account is defined manually
SERVERACCOUNTNAME	User name for service	
SERVERACCOUNTPWD	User password for service	
DBTYPE		• MySQL • MSSQL
MYSQLSERVERNAME	Full name of MySQL server	
MYSQLSERVERPORT	Number of port for connection to MySQL server	
MYSQLDBNAME	Name of MySQL server database	
MYSQLACCOUNTNAME	User name for connection to MySQL server database	
MYSQLACCOUNTPWD	User password for connection to MySQL server database	
MSSQLCONNECTIONTYPE	Type of use of MSSQL database	• InstallMSSEE – Install from a package • ChooseExisting—Use the installed server
MSSQLSERVERNAME	Full name of SQL Server instance	
MSSQLDBNAME	Name of SQL server database	
MSSQLAUTHTYPE	Method of authentication for connection to SQL Server	• Windows • SQLServer
MSSQLACCOUNTNAME	User name for connection to SQL Server in SQLServer mode	

MSI PROPERTY	DESCRIPTION	AVAILABLE VALUES
MSSQLACCOUNTPWD	User password for connection to SQL Server in SQLServer mode	

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

EXISTSHAREFOLDERNAME	Full path to an existing shared folder	
SERVERPORT	Number of port for connection to Administration Server	
SERVERSSLPORT	Number of port for establishing SSL connection to Administration Server	
SERVERADDRESS	Administration Server address	
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	• 1 • Null
INSTALLDIR	Installation folder	
INSTALL_NSAC	Whether to install NAC	• 1 • Null
SERVERADDRESS	Administration Server address (required)	
SERVERPORT	Number of port for connection to Administration Server	
SERVERSSLPORT	Number of port for SSL connection	
USESSL	Whether to use SSL connection	• 1 • Null
OPENUDPPORT	Whether to open a UDP port	• 1 • Null
UDPPORT	UDP port number	

MSI PROPERTY	DESCRIPTION	AVAILABLE VALUES
USEPROXY	Whether to use a proxy server	• 1 • Null
PROXYADDRESS	Proxy address	
PROXYPORT	Number of port for connection to Administration Server	
PROXYLOGIN	Account for connection to proxy server	
PROXYPASSWORD	Password of account for connection to proxy server	
GATEWAYMODE	Connection gateway use mode	• 0—Do not use connection gateway • 1—Use this Network Agent as connection gateway • 2—Connect to Administration Server through connection gateway
GATEWAYADDRESS	Connection gateway address	
CERTSELECTION	Method of receiving a certificate	• GetOnFirstConnection—Receive a certificate from Administration Server • GetExistent—Select an existing certificate. If this option is selected, the CERTFILE property must be defined
CERTFILE	Path to the certificate file	
VMVDI	Enable dynamic mode for Virtual Desktop Infrastructure (VDI)	• 1 • Null
LAUNCHPROGRAM	Whether to run Network Agent service after installation	• 1 • Null

VIRTUAL INFRASTRUCTURE

Kaspersky Security Center supports the use of virtual machines. The application supports installation of Network Agent and an Anti-Virus application on each virtual machine, as well as protection of virtual machines at the level of hypervisor. In the first case, you can use either a regular anti-virus 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 the version 10 MR1, Kaspersky Security Center supports rollbacks of virtual machines to their previous state (see the section "Support of file system rollback for computers with Network Agent" on page 50).

IN THIS SECTION:

TIPS ON REDUCING THE LOAD ON VIRTUAL MACHINES

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

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

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

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

- Retrieving information about software installed
- Retrieving information about hardware
- Retrieving information about vulnerabilities detected
- Retrieving information about updates required

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

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

If you want events from dynamic virtual machines to be stored on 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 removal of computers** 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 the deployment, by copying a disk image (see section "Deployment by capturing and copying the hard disk of a computer" on page 37).

However, in the two following cases, Network Agent detects the copying automatically, so you do not have to perform all of the complex actions listed in the section "Deployment by capturing and copying the hard disk of a computer":

- The **Enable dynamic mode for VDI** check box was selected when Network Agent was installed—After each reboot of the operating system, this virtual machine will be recognized as a new computer, regardless of whether it has been copied or not.
- One of the following hypervisors is in use: VMware™, HyperV®, or Xen®: Network Agent detects the copying of the virtual machine by the changed ID's 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 COMPUTERS WITH NETWORK AGENT

Kaspersky Security Center is a distributed application. Rolling back the file system to a previous state on a computer with installed Network Agent will lead to a desynchronization of data and incorrect 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 computers with installed Network Agent affects the folder %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ are only critical scenarios for Kaspersky Security Center. Therefore, you must always exclude this folder from the recovery procedure, if possible.

Because the working principles of some enterprises provide for rollbacks of the file system of computers, support for the file system rollback on computers with Network Agent installed has been added to Kaspersky Security Center, starting with version 10 MR1 (Administration Server and Network Agents must be version 10 MR1 or later). When detected, those computers are automatically reconnected to 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, presented in the following example, to the registry and restart the Administration Server service.

Operating system on a computer that has 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 computer that has Administration Server installed (64-bit):

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Products\1093\1.0.0.0\ServerFlags]
“KLSRV_HST_VM_REVERT_DETECTION”=dword:00000001
```

By default, support of file system rollback detection is enabled in Kaspersky Security Center 10 SP1.

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

A rollback of the system state is absolutely not allowed on a computer 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 31).

CONFIGURING CONNECTION PROFILES FOR OUT-OF-OFFICE USERS

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

Using different addresses of a single Administration Server

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

Computers with installed Network Agent can connect to 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). At the same time, 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 10), 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 several offices with different Administration Servers and some of the computers with installed Network Agent move between them, you need Network Agent to connect to the Administration Server of the local network in the office where the computer is 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 should 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 9

Internet access: Network Agent in gateway mode in a DMZ 10

DEPLOYING THE MOBILE DEVICE MANAGEMENT FEATURE

IN THIS SECTION:

INSTALLING AN EXCHANGE ACTIVESYNC MOBILE DEVICE 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 Exchange ActiveSync Mobile Device 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** dropdown list, select **Required**.

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

LOCAL INSTALLATION OF AN EXCHANGE ACTIVESYNC MOBILE DEVICE SERVER

For a local installation of an Exchange ActiveSync Mobile Device Server, the administrator must perform the following operations:

1. Copy the contents of the folder \Server\Packages\MDM4Exchange\ from the distribution package of Kaspersky Security Center to a client computer.
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 installation of the Exchange ActiveSync Mobile Device Server
  - Operation mode of the Exchange ActiveSync Mobile Device Server: standard mode or cluster mode (see section "How to deploy an Exchange ActiveSync Mobile Device Server" on page 15)
  - Possibility of specifying the account under which the service of Exchange ActiveSync Mobile Device Server will run (see section "Account for Exchange ActiveSync service" on page 15)
  - Enabling / disabling automatic configuration of the IIS web server.

The Installation Wizard of the Exchange ActiveSync Mobile Device Server must be run under an account that has all of the required rights (see section "Rights required for deployment of an Exchange ActiveSync Mobile Device Server" on page 15).

REMOTE INSTALLATION OF AN EXCHANGE ACTIVESYNC MOBILE DEVICE SERVER

To configure the remote installation of an Exchange ActiveSync Mobile Device 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 **Exchange ActiveSync Mobile Device 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 Exchange ActiveSync Mobile Device Server.

To install an Exchange ActiveSync Mobile Device 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 **Exchange ActiveSync Mobile Device Server** package.
3. Open the context menu of the package and select **Install application**.
4. In the Remote Installation Wizard that opens, select a computer (or multiple computers 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 computer.

   This account must have all of the required rights (see the section "Rights required for deployment of an Exchange ActiveSync Mobile Device Server" on page 15).

INSTALLING AN IOS MDM MOBILE DEVICE SERVER

The number of copies of an iOS MDM Mobile Device 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 Mobile Device 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 Mobile Device Server:

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

Both deployment schemes are described below.

SIMPLIFIED DEPLOYMENT SCHEME

When deploying an iOS MDM Mobile Device 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 17).

DEPLOYMENT SCHEME INVOLVING KERBEROS CONSTRAINED DELEGATION (KCD)

The deployment scheme with Kerberos constrained delegation (KCD) requires the Administration Server and the iOS MDM Mobile Device 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 the integration with the Public Key Infrastructure.
    3. In the **Generation of general type certificates** section, specify the source of certificates.

See the sections:

- Standard configuration: Kaspersky Mobile Device Management on the local network of an enterprise (see section "Standard configuration: iOS MDM Mobile Device Server on the local network of an enterprise" on page 17).
- Integration with PKI (Public Key Infrastructure) (see section "Integration with Public Key Infrastructure" on page 59).

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

- iOS MDM web service is running on port 443
- Name of the computer with TMG is tmg.mydom.local.
- Name of computer 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/kes4mob.mydom.local

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

setspn -a http/iosmdm.mydom.local iosmdm

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

To delegate traffic, trust the computer with TMG (tmg.mydom.local) to the service that is defined by the SPN (http/iosmdm.mydom.local).

To trust the computer 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 computer with TMG installed (tmg.mydom.local).
2. In the computer 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 devices' timely responses to the administrator's commands, you need to specify an Apple Push Notification Service certificate (hereinafter referred to as APNs certificate) in the settings of the iOS MDM Mobile Device Server.

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 side of the iOS MDM web service through a proxy server, you must perform the following actions on the computer 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\KLIOSMDM\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\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\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
- Deployment scheme involving 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 9).

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 dropdown 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 the integration with the Public Key Infrastructure.
  3. In the **Generation of general type certificates** section, specify the source of certificates.

See the sections:

- Integration with PKI (Public Key Infrastructure) (see section "Integration with Public Key Infrastructure" on page 59)
- Providing Internet access to the Administration Server (on page 9).

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
- Name of the computer with TMG is tmg.mydom.local
- Name of the computer with Administration Server is ksc.mydom.local
- Name of the external publishing of the point of access to the mobile protocol is kes4mob.mydom.global.

Domain account for Administration Server

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

A domain account must be specified by the following reasons:

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

Service Principal Name for http/kes4mob.mydom.local

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

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

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

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

To trust the computer 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 computer with TMG installed (tmg.mydom.local).
2. In the computer 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 dropdown 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 CLOUD MESSAGING

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

To enable the use of GCM:

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 Cloud Messaging service** section.
4. In the **Sender ID** and **API Key** fields, specify the GCM: SENDER_ID and API Key settings.

GCM 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 GCM.

Configuring GCM: retrieving SENDER_ID, API Key

To configure GCM, 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 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 computer 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 computer with Administration Server from which integration with PKI is initiated.
- It has the right to **Log On As Service**.
- The computer with Administration Server must be logged on at least once under this account to create a permanent user profile.

KASPERSKY SECURITY CENTER OPERATOR

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.

CONFIGURING AND USING NAC

This section provides recommendations on initial setup and use of NAC. Below are the requirements to computers intended to be used as NAC agents, as well as priorities of restrictions to be imposed on network devices specified in the NAC rules.

Examples for setup of NAC for some standard configurations are also provided.

IN THIS SECTION:

SEE ALSO:

ASSIGNING NAC AGENTS

When assigning an NAC agent, you must select a computer that meets the following criteria:

- It has free resources and the load on both the CPU and network services is low.
- It is the most powerful among other computers.
- It is rarely restarted and / or shut down.

Assigning a computer meeting these requirements to act as an NAC agent will result in faster data collection and scanning; it will also increase the performance of NAC policies applied. If a NAC agent is intended to operate in a broadcast domain that already includes network devices (of which the activity must be restricted), time may elapse before the network is analyzed and the NAC policy takes effect. As a rule, the policy takes effect 10 to 15 minutes after it is applied (in a broadcast domain that includes 300 devices).

The number of devices that can be served by a single NAC agent depends on the infrastructure and the scale of the network's broadcast domain, as well as on the number of network objects and rules. NAC functions reliably with a proportion of 1,000 devices per one NAC agent.

To test the efficiency of a NAC policy, the NAC agent provides the Simulation mode. Simulation mode consists of broadcasting the NAC policy in the driver, but the actual network activity of devices covered by access restrictions is not limited at all. While in Simulation mode, Network Agent only receives information from the NAC driver about the need of applying a rule to the device. This information is available from the $klnac.log file (see section "Determining the applicability of an NAC rule" on page 68). In other respects, this mode is identical to the normal mode (Standard).

When running, a NAC agent creates additional virtual adapters (one for each physical adapter in the system), and their media access control (MAC) addresses are randomly generated on Administration Server. This list of MAC addresses is generated once, at the first run of Administration Server, and it cannot be modified later. At the initialization stage, the adapter of the NAC agent makes a few attempts of configuring DHCP, using one of the available MAC addresses from the list. If the network infrastructure does not provide for a DHCP server, or if the DHCP server configuration uses the static MAC–IPv4 reservation, the NAC agent requires manual configuration of the interface.

Manual configuration of a NAC agent (not recommended)

You can perform manual configuration through the Windows registry on a NAC agent by importing the following file.

For a 32-bit version of Windows:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\NagentFlags]
"EnfUseDHCP"=dword:00000000
"EnfIpv4"="10.16.72.2"
"EnfSubnetMask"="255.255.252.0"
"EnfIpv4Gateway"="10.16.72.1"
```

For a 64-bit version of Windows:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\NagentFlags]
"EnfUseDHCP"=dword:00000000
"EnfIpv4"="10.16.72.2"
"EnfSubnetMask"="255.255.252.0"
"EnfIpv4Gateway"="10.16.72.1"
```

Manual setup is only available on NAC agents with a single active physical interface. If multiple active physical interfaces are in use, the newly set configuration will be applied to the virtual adapter of the first interface selected at random.

RESTRICTIONS IN NAC RULES

Restrictions in NAC rules have the following priorities (in descending order):

- NAC agents (highest-level priority, for internal use).

  Computers with NAC agents are always accessible for network interaction with devices, regardless of restrictions imposed on activities of those devices.
- White list. NAC agents impose no restrictions on devices on this list.
- Blocked manually from Administration Console.
- Logged in to Authorization Portal. NAC agents impose no restrictions on devices on this list.
- Blocked. Access to those network devices will be blocked.
- Blocked, except for the list of special addresses (restriction type "Allow access to service addresses").

  Devices on this list will only be granted access to the list of special addresses of the rule. Access to other addresses will be blocked.
- Devices with the restriction "Redirect to Authorization Portal" imposed (lowest-level priority).

  Immediately after authorization, a device will be added to the list "Logged in to Authorization Portal" so it will not be restricted by the NAC agent anymore. Before logging in to Authorization Portal, devices under this restriction always have access to the list of DNS servers on the network.

When specifying network objects, pay close attention to whether the device matches the network object type. For example, if a network object belongs to the type "Computers", the criteria of that object will only be met by devices with the type "Computers" detected after an active scan.

ENABLING NAC

To enable NAC:

1. In Administration Console, create a policy of Network Agent and, in the policy properties (section **Settings**, **NAC operation mode**), enable NAC in **Standard** mode.
2. Assign NAC agents in broadcast domains that include the devices for which you intend to restrict network activity.
3. In the properties of Network Agent, on the relevant NAC agents, select the **Standard** mode for the NAC agent.

STANDARD CONFIGURATIONS OF NAC

Below are examples of setup of NAC in some of the standard network configurations.

Configuration "Corporate devices only"

Multiple network devices connect to a broadcast domain on an Ethernet network, such as computers, laptops, or network printers. The administrator is aware of their origins and so assigns those devices the "Corporate" attribute in Administration Console, in the **Repositories/Hardware** node. The administrator wants to completely restrict access to network resources on all devices that have not been marked "Corporate" (computers, file servers, printers, etc.)

To do this, the administrator must perform the following actions:

1. Enable NAC (see section "Enabling NAC" on page 61).
2. In the policy's properties, create a network object named "Non-corporate devices" (any name can be entered for the object) of the type "Devices of any type". Add the criterion "Devices not marked as corporate" to the list of criteria.
3. Create an access restriction rule intended to "Block network access". Add the object "Non-corporate devices" to the list of network objects of the rule.

Configuration "Access to network printer only"

Multiple network devices connect to a broadcast domain on an Ethernet network, such as computers, laptops, or network printers. The administrator is unaware of their origins but must grant access, to the network printer with the IP address 192.168.1.135, to all devices that have been marked "Computer" within this segment.

To do this, the administrator must perform the following actions:

1. Enable NAC (see section "Enabling NAC" on page 61).
2. In the policy properties, create an object of the type "Network addresses" named "Printer 192.168.1.135", which describes the IP address 192.168.1.135.
3. Create a network object named "All computers in this segment" belonging to the type "Computers". Add the criterion "By network attributes" to the list of criteria, which describes the range of IP addresses in this segment (for example, 192.168.1.2 – 192.168.1.254).
4. Create an access restriction rule intended to "Allow access to network addresses". Add the object "All computers in this segment" to the list of network objects of the rule, and then add the object "Printer 192.168.1.135" to the list of allowed network addresses.

Configuration "Access through Authorization Portal"

Multiple network devices connect to a broadcast domain on an Ethernet network. The administrator is unaware of their origins, but he or she has to allow access to the network resources to computers on which users have logged in via Authorization Portal.

To do this, the administrator must perform the following actions:

1. Enable NAC (see section "Enabling NAC" on page 61).
2. In the policy properties, create an account for Authorization Portal named "Guest".
3. Create a network object named "All computers in this segment" belonging to the type "Computers". Add the criterion "By network attributes" to the list of criteria, which describes the range of IP addresses in this segment (for example, 192.168.1.2 – 192.168.1.254).
4. Create an access restriction rule intended to "Redirect to authorization portal". Add the object "All computers in this segment" to the list of network objects of the rule.

The Kaspersky Captive Portal service starts automatically on the NAC agent. Network traffic of devices (defined as "Computers") will be redirected to Authorization Portal, which will open the authorization page in the user's browser. If the user enters the Guest account credentials, the computer will be marked as authorized and the user will have full access to the network resources.

JavaScript must be enabled in the browsers of Authorization Portal users.

ROUTINE WORK

IN THIS SECTION:

TRAFFIC LIGHTS IN ADMINISTRATION CONSOLE

The main indicator for the condition of Kaspersky Security Center and managed computers is a set of traffic lights in the workspace of the **Administration Server** node in Administration Console (**Getting started**). Six traffic lights are displayed. Each of the traffic lights covers a different scope of features of Kaspersky Security Center.

Table 7. Scopes of traffic lights in Administration Console

NAME OF TRAFFIC LIGHT	SCOPE OF TRAFFIC LIGHT
Deployment	Installation of Network Agent and an Anti-Virus application on computers on the enterprise network.
Managing computers	Structure of administration groups. Network scanning. Computer moving rules
Protection of computers and virus scanning	Anti-virus application's functionality: state of protection, virus scanning
Update	Updates and patches
Monitoring	Protection status
Administration Server	Features and properties of Administration Server

Each of the traffic lights has three possible color-coded statuses:

Table 8. Color codes of traffic lights

STATUS	COLOR CODE	CODE 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

All of the six traffic lights must remain green.

REMOTE ACCESS TO MANAGED COMPUTERS

IN THIS SECTION:

ACCESS TO LOCAL TASKS AND STATISTICS, "DO NOT DISCONNECT FROM THE ADMINISTRATION SERVER" CHECK BOX

By default, Kaspersky Security Center does not feature continuous connectivity between managed computers and the Administration Server. Network Agents on managed computers periodically establish connections and synchronize with the Administration Server. The interval between those synchronization sessions (by default, it is 15 minutes) is defined in a policy of Network Agent. If an early synchronization is required (for example, to force the application of a policy), the Administration Server sends Network Agent a signed network packet to port UDP 15000. If a connection between Administration Server and a managed computer using UDP is not possible for any reason, synchronization will run at the next regular connection of Network Agent to the Administration Server during 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 (Anti-Virus application or Network Agent), creating a tunnel, etc. To resolve this issue, in the properties of the managed computer (section **General**), select the **Do not disconnect from the Administration Server** check box. The maximum total number of computers with the **Do not disconnect from the Administration Server** check box selected is 300.

CHECKING THE TIME OF CONNECTION BETWEEN A COMPUTER AND THE ADMINISTRATION SERVER

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

FORCED SYNCHRONIZATION

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

In the context menu of managed computers in Administration Console of a computer, the **All tasks** menu item contains the **Force synchronization command**. When Kaspersky Security Center 10 SP1 executes this command, the **Forced synchronization assigned** check box is selected in the computer's properties, then the Administration Server attempts to connect to the computer. 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 computer. Tunneling is designed for connecting a client application on a computer with Administration Console installed to a TCP port on a managed computer—if a direct connection is not possible between the Administration Console computer and the target computer.

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:

EXCHANGE ACTIVESYNC MOBILE DEVICE SERVER

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

HANDLING EXCHANGE ACTIVESYNC POLICIES

After you install Exchange ActiveSync Mobile Device 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.

In addition, in the properties window of the Exchange ActiveSync Mobile Device Server, 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 the Exchange ActiveSync HTTP protocol for one or multiple accounts.

CONFIGURING THE SCAN SCOPE

In the properties of the installed Exchange ActiveSync Mobile Device Server, in the **Settings** section, you can configure the scan scope. By default, the scan scope is the current domain in which the Exchange ActiveSync Mobile Device 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 Mobile Device Server

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

IN THIS SECTION:

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 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 device.
- The device connects to the iOS MDM Mobile Device Server.

SEE ALSO:

Adding a new device by installing a profile by the administrator

To connect a device to an iOS MDM Mobile Device Server by installing an iOS MDM profile to that 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 to the user device by means of the Apple Configurator utility.

The device will connect to the iOS MDM Mobile Device Server.

SEE ALSO:

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 device to which the commands will be sent.
  4. In the context menu of the device, select **Commands for iOS devices** or **Manage device**. In the list that appears, select the command to be sent to the device.

CHECKING THE EXECUTION STATUS OF COMMANDS SENT

- *To check the execution status of a command that has been sent to a 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 device on which the execution status needs to be checked for selected commands.
  4. In the context menu of the device, select **Show command log**.

NAC: EVENTS AND STANDARD SCENARIOS

This section provides descriptions of NAC events that are published by NAC agents, as well as recommendations on how to use NAC within standard scenarios for this feature.

NAC EVENTS

There are two types of events published by NAC agents:

- Device detected. This event is published at the first detection of a device by an NAC agent. The text of the event contains the MAC address and IP address of the device (as of the time of the detection).
- Device authorized. This event is published at each successful logging in of the device to Authorization Portal. The text of the event contains the MAC address and IP address of the device (as of the time of the detection).

STANDARD SCENARIOS FOR NAC

This section describes the standard scenarios for the use of NAC in order to monitor activities of network devices.

IN THIS SECTION:

AUDIT OF ACTIVITIES OF NETWORK DEVICES

Audit of activities of network devices can be performed in online mode in Administration Console, in the **Unassigned devices/Network devices** folder. The workspace of this folder displays a list of devices that have ever been detected on the network. You can use the context menu to block or unblock a device manually.

Audit of activities of network devices can also be performed in offline mode in Administration Console, in the **Reports and notifications/Events** folder.

RESTRICTING THE NETWORK ACTIVITY OF A DEVICE

There are two ways of restricting the network activity of a device:

- In Administration Console, find the device in the workspace of the **Unassigned devices** folder, and then select **Block** in the context menu of the device
- In the policy of Network Agent, create a network object of the type **Devices of any type** and add the available set of criteria to the list of criteria. If the MAC address of the device is known, this will be the **By network attributes** criterion with the value of the attribute, which corresponds to the MAC address of the device.

LIFTING RESTRICTIONS IMPOSED ON THE NETWORK ACTIVITY OF A DEVICE

There are also two ways of unblocking a device:

- If the device was blocked by the administrator manually, you can unblock it by clearing the check box in the **Block** item of the context menu in the **Unassigned devices** folder in Administration Console.
- If the network activity of the device was restricted by some NAC rules, those restrictions can be lifted either by adding the relevant network object to the white list of devices in the settings of Network Agent (section **Network Access Control (NAC)**), or by modifying the network object so that the device does not meet its criteria anymore.

DETERMINING THE APPLICABILITY OF AN NAC RULE

Upon completion of setup, the policy with NAC rules (hereinafter also referred to as the NAC policy) is delivered to NAC agents. Applying the policy to a device starts immediately after any outbound network activity from that device is detected.

To determine whether a NAC rule applies (and which of the rules applies) to a device on the network, you must know the broadcast domain within which the device operates, and must have remote access to the NAC agent that applies the NAC policy in that domain.

For example, in broadcast domain *X*, device *Y* operates with MAC address *Z*. In the Network Agent policy, this device is described (by means of a network object), and rule *R* has been created to restrict the device's access to the network. In broadcast domain *X*, NAC agent *E* operates. Audit of activities of the NAC agent can be performed by means of the $klnac.log file. The procedure for audit of NAC agent E is given below.

Audit of activities of a NAC agent

To perform the audit of activities of NAC agent E, the administrator must perform the following actions:

1. Obtain remote access to the file system of NAC agent E.
2. In the %WINDIR%\Temp folder, find the $klnac.log file, and then open it with any text editor that supports UNIX®, such as Wordpad.
3. In the text file, find the strings associated with Rule activity, where the string RuleName is followed by the name of the rule to be applied (*R*). Then, after a minus sign (-), are the following network attributes, whose activity is restricted: MAC SRC and IPv4 SRC. If the MAC address *Z* is found, rule *R* has been applied and is running.

   Also, in the $klnac.log file, you can learn when the device was detected for the first time and which network resource it attempted to access at that time (in the strings associated with Device discovery).

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

IN THIS SECTION:

LIMITATIONS OF KASPERSKY SECURITY CENTER

The following table displays the limitations of the current version of Kaspersky Security Center 10 SP1.

Table 9. Limitations of Kaspersky Security Center 10 SP1

TYPE OF LIMITATION	VALUE
Maximum number of managed computers	50,000
Maximum number of computers with the **Do not disconnect from the Administration Server** check box selected	300
Maximum number of administration groups	10,000
Maximum number of events to store	15,000,000
Maximum number of policies	2,000
Maximum number of tasks	2,000
Maximum total number of Active Directory objects (OUs and accounts of users, computers, 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 computers that a single Update Agent can serve	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 computers.

Administration Server and SQL Server are deployed on the same computer

Table 10. Hardware requirements for the computer

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 computers

Table 11. Hardware requirements to the computer 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 computer 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 on the enterprise's network, each of them covering from 100 to 200 computers.
- 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 COMPUTERS
15	10,000
30	20,000

SYNCHRONIZATION INTERVAL (MINUTES)	NUMBER OF MANAGED COMPUTERS
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 available on Administration Server, the computer with the Update Agent will also require an amount of free disk space 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 repair are available on Administration Server, the computer with the Update Agent will also require an amount of free disk space equal to twice the total size of all patches to be installed.

PRELIMINARY ASSESSMENT OF SPACE REQUIRED IN THE DATABASE AND ON THE HARD DRIVE FOR ADMINISTRATION SERVER

Assessing the space required in the database of Administration Server

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

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

where:

C is	Number of computers
E is	Number of events to store
A is	Total number of Active Directory objects: • Computer 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 computer with Administration Server installed

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

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

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

Updates

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

Installation packages

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

Remote installation tasks

If some remote installation tasks are available on Administration Server, the computer with Administration Server will require an additional amount of free disk space (in the folder %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit), 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 table below shows the average daily rates of traffic between Administration Server of Kaspersky Security Center 10 MR1, build 10.1.249, and a managed computer (with Network Agent of 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 SERVER TO THE MANAGED COMPUTER (DOWNLOAD)	FROM THE MANAGED COMPUTER TO 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 table below shows the average daily rates of traffic between Administration Server of Kaspersky Security Center 10 SP1 and a managed computer (with Network Agent of Kaspersky Security Center 10 SP1 and Kaspersky Endpoint Security 10 SP1).

Table 15. Average daily traffic rates: Kaspersky Security Center 10 SP1

	FROM SERVER TO THE MANAGED COMPUTER (DOWNLOAD)	FROM THE MANAGED COMPUTER TO ADMINISTRATION SERVER (UPLOAD)
Average daily traffic rate with the default settings of the update task	17 MB	3.5 MB
Average daily traffic rate with the update task disabled	0.8 MB	1 MB

TROUBLESHOOTING

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

IN THIS SECTION:

PROBLEMS WITH REMOTE INSTALLATION OF APPLICATIONS

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

Table 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.
Incompatible application	An application, which is incompatible with the application being installed, is already installed on the computer. 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 computer, you need to restart the OS and retry the installation process.

ISSUE	COMMON CAUSES AND SOLUTIONS
Wrong version of installer	Installation of this installation package is not supported by the version of the installer, which is actual on this computer.
Installation already running	Installation of another application has already been started on this computer.
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 computer 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.)
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's installer again after restarting the computer.
Restart required to continue installation	To proceed with the installer, you need to restart the computer.

INCORRECT COPYING OF A HARD DRIVE IMAGE

If a hard disk with installed Network Agent has been copied without following the rules of deployment (see section "Deployment by capturing and copying the hard disk of a computer" on page 37), some computers 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 computers that have been copied from the image incorrectly, using third-party tools, and then install it again. Network Agent cannot be removed with the tools of Kaspersky Security Center, because Administration Server cannot distinguish between faulty computers (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 installation folder of Network Agent, with the "-dupfix" key (klmover -dupfix) once on faulty computers (those copied from the image incorrectly). The utility cannot be run with the tools of Kaspersky Security Center, because Administration Server cannot distinguish between faulty computers (they all share the same icon in Administration Console).

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

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

  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 computer results in an automatic "fix" of those Network Agents (with the assumption that all of the copied computers have unique NetBIOS names).

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

  - If a 32-bit operating system is installed on the computer 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 computer 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 EXCHANGE ACTIVESYNC MOBILE DEVICE SERVER

This section provides information about errors and problems that may be encountered when using an Exchange ActiveSync Mobile Device Server.

Error during installation of an Exchange ActiveSync Mobile Device Server

If an error occurred during a local or remote installation, you can find out the cause of the error by viewing the file error.log located on the computer 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 Network Agent on the computer on which the Exchange ActiveSync Mobile Device Server is deployed, and Administration Server.

PROBLEMS WITH IOS MDM MOBILE DEVICE SERVER

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

IN THIS SECTION:

PORTAL SUPPORT.KASPERSKY.COM

Information about some of the problems that occur when using an iOS MDM Mobile Device 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 Mobile Device Server.
3. Check the device by using the console of iPhone Configuration Utility.
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

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 CLOUD MESSAGING SERVICE

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

CHECKING GOOGLE CLOUD MESSAGING FOR ACCESSIBILITY

To check Google Cloud Messaging service for accessibility from the Kaspersky Security Center side (see section "Using Google Cloud Messaging" on page 58), you can use the following Telnet command:

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

ISSUES WITH NETWORK ACCESS CONTROL (NAC)

This section provides information about errors and problems that may be encountered when using Network Access Control (NAC).

Cannot run the NAC agent on Network Agent

Possible cause:

- Components of NAC have not been installed or have been installed with errors. The description of this error must be added to Kaspersky Event Log.

Possible solution:

- Eliminate the error's cause (if possible) and restart the Kaspersky Network Agent service.

NAC has been configured in the policy and the NAC agent is enabled, but the NAC rule cannot be applied (the device activity is not limited by the NAC agent)

Possible cause:

- Incorrect settings of NAC rules in the policy

Possible solutions:

- Check whether the device meets the criteria given in the network object.
- Check whether the NAC agent is running in Standard mode and whether Kaspersky Event Log on the host shows no error messages.
- Check whether the computer with the NAC agent operates in the same broadcast domain as the device.

NAC has been configured in the policy, the NAC agent is running, the rule is applied, but the device's access to network resources is unlimited notwithstanding (in a virtual environment)

Possible cause:

- Incorrect settings of the network infrastructure.

Possible solutions:

- For VMvare ESXi™:
  - The options Promiscuous Mode, MAC Address Changes, and Forged Transmits must be configured in Accept mode.
- For Microsoft Hyper-V:
  - On the server with the Hyper-V role, for each <vm_name> virtual machine, you must run: Set-VMNetworkAdapter –VMName <vm_name> –MacAddressSpoofing On.

High load on the CPU in kernel mode

Possible cause:

- An extremely high broadcasting activity in the network domain (thousands of devices), or the NAC agent is overloaded with other low-level operations (disk I/O, file network services, etc.)

Possible solutions:

- Move the NAC agent on another computer that experiences a lower workload
- Move or disable services with high requirements to the CPU in kernel mode.

The "Redirect to Authorization Portal" rule is not working

Possible cause:

- Incorrect settings of NAC in the policy
- Incorrect settings of the network infrastructure.

Possible solutions:

- Check whether the rule can operate and is applied to the device (see section "Determining the applicability of a NAC rule" on page 68).
- Check whether the Kaspersky Captive Portal service is running on the NAC agent and Kaspersky Event Log shows no errors related to that service.
- Check whether port TCP 80 (used by the Kaspersky Captive Portal service by default) is not occupied by other web servers. If the port is occupied, free it up (by moving the web server on another host in the network) and restart the Kaspersky Captive Portal service. After freeing up the port and restarting the service, check whether the browser on the computer with the NAC agent opens the authorization page when you click the link shown as http://<enforcer_host> .

The scan is complete, but the type of device or the OS version cannot be determined

Possible cause:

- Kaspersky Network Scanner service is not running
- The network ports are closed on this device.

Possible solutions:

- Check whether the KNS service can be run and Kaspersky Event Log shows no error description. If an error appears, try to eliminate it (if possible) and restart the service.
- Make sure that the firewall that may interfere with active scanning of network ports is disabled on this device.

CONTACTING TECHNICAL SUPPORT SERVICE

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

IN THIS SECTION:

ABOUT TECHNICAL SUPPORT

If you cannot find a solution to your problem in the application documentation or in one of the sources of information about the application, we recommend that you contact Kaspersky Lab Technical Support. Technical Support specialists 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 Technical Support, please read the support rules (http://support.kaspersky.com/support/rules).

You can contact Technical Support in one of the following ways:

- By calling Kaspersky Lab Technical Support.
- By sending a request to Kaspersky Lab Technical Support using the Kaspersky CompanyAccount portal.

TECHNICAL SUPPORT BY PHONE

In most regions, you can phone specialists at Kaspersky Lab Technical Support. You can receive information about how to obtain technical support in your region and the contacts of Technical Support on the website of Kaspersky Lab Technical Support (http://support.kaspersky.com/b2c).

Before contacting Technical Support, please read the support rules (http://support.kaspersky.com/support/rules). These rules provide information about the hours open for calls at Kaspersky Lab Technical Support, as well as the data that a support specialist will need to help you.

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 specialists through online requests. The Kaspersky CompanyAccount portal allows you to monitor the progress of electronic request processing by Kaspersky Lab specialists and store a 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 website (http://support.kaspersky.com/faq/companyaccount_help).

AO KASPERSKY LAB

Kaspersky Lab software is internationally renowned for its systems for 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 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 3000 qualified specialists.

PRODUCTS. Kaspersky Lab's products provide protection for all systems—from home computers to large corporate networks.

The personal product range includes applications that provide 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 for protection against DDoS attacks, protection of environments managed with industrial control systems, and fraud prevention. Used in conjunction with centralized management tools, these solutions ensure effective automated protection against computer threats for companies and organizations of any scale. Kaspersky Lab's products are certified by the 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's 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 include them in 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 used by many other software vendors, including Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, General Dynamics, Facebook, Juniper Networks, Lenovo, H3C, 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 researches conducted by the renowned Austrian anti-virus lab AV-Comparatives made Kaspersky Lab one of the two leaders in the number of Advanced+ certificates awarded, which brought the company the Top Rated certificate. But Kaspersky Lab's main achievement 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 official site:	http://www.kaspersky.com
Virus encyclopedia:	http://www.securelist.com
Anti-Virus Lab:	http://newvirus.kaspersky.com (for scanning suspicious 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; use 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.