KASPERSKY lab

Kaspersky Security 10 for Windows Server

Implementation Guide for Network Storage Protection

Program version: 10

Dear User,

Thank you for choosing our product. We hope that this documentation will help you in your work and answer your questions about this software product.

This document may be amended without prior notice. For the latest version, please refer to Kaspersky Lab's website at http://www.kaspersky.com/docs.

Revision date: 2/12/2016

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

Table of contents

About this Guide 6
In this document 6
Document conventions 8

Sources of information about Kaspersky Security 10
Sources for independent retrieval of information 10
Discussing Kaspersky Lab applications on the forum 12

Kaspersky Security 13

Hardware and software requirements 17
Requirements for the server on which Kaspersky Security is deployed 17
Requirements for the protected network attached storage 19
Requirements for the computer on which Kaspersky Security Console is installed 20

Integrating Kaspersky Security with network attached storages 23
Preparing for launch of the Network Attached Storage Protection task 24
Configuring security settings of local policies in the local group policy editor 25
Configuring inbound and outbound connections in Windows firewall 26

Managing Kaspersky Security Console 28
About Kaspersky Security Console 28
Starting Kaspersky Security Console from the Start menu 29
Kaspersky Security Console interface 31
Viewing status information for Network Attached Storage Protection 36
Managing Network Attached Storage Protection tasks 38
Saving a task after changing its settings 38
Starting / pausing / resuming / stopping tasks manually 39
Managing task schedules 39
Configuring the task launch schedule settings 39
Enabling and disabling scheduled tasks 41

Protecting EMC network attached storages of the Celerra / VNX group 43
About protection of EMC network attached storages of the Celerra / VNX group 43
Integrating Kaspersky Security with an EMC network attached storage of the Celerra / VNX group 44

RPC-Network Storage Protection 45
About RPC-Network Storage Protection 45
About scanning symbolic links 47
About scanning snapshots and other read-only volumes and folders 47
Configuring a connection between an RPC-network storage and Kaspersky Security 48
Selecting a user account for running the RPC-Network Storage Protection task 49
Creating the protection scope in the RPC-Network Storage Protection task 50
Adding an RPC-network storage to Kaspersky Security 50
Disabling and enabling protection of an added RPC-network storage 52
Removing an RPC-network storage from the protection scope 53
Configuring the RPC-Network Storage Protection task 53
Using the Heuristic Analyzer 56
Integration with other components of Kaspersky Security 57
Configuring general settings for RPC-Network Storage connection 59
Security levels in the RPC-Network Storage Protection task 60
About security levels in the RPC-Network Storage Protection task 60
Applying a preset security level in the RPC-Network Storage Protection task 62
Manually configuring the security level settings in the RPC-Network Storage Protection task 63
Using security level settings templates in the RPC-Network Storage Protection task 67
Creating a security settings template 67
Applying a security settings template 68
Viewing security settings in a template 69
Deleting a security settings template 69
Viewing statistics of the RPC-Network Storage Protection task 70
ICAP-Network Storage Protection 73
About ICAP-Network Storage Protection 73
Configuring a connection between an ICAP-network storage and Kaspersky Security 75
Configuring the ICAP-Network Storage Protection task 76
Configuring the settings of the connection to an ICAP-network storage 78
Using the Heuristic Analyzer 79
Using KSN for protection 80

Security levels in the ICAP-Network Storage Protection task 81
About security levels in the ICAP-Network Storage Protection task 82
Applying a preset security level in the ICAP-Network Storage Protection task 84
Manually configuring the security level settings in the ICAP-Network Storage Protection task 85
Viewing statistics of the ICAP-Network Storage Protection task 87
Managing Network Attached Storage Protection tasks from Kaspersky Security Center 89
About Network Attached Storage Protection from Kaspersky Security Center 89
Configuring Network Attached Storage Protection settings using policies 90
Configuring Network Attached Storage Protection settings for one server in Kaspersky Security Center 92
Contacting Technical Support 93
How to get technical support 93
Technical Support via Kaspersky CompanyAccount 94
Technical support by phone 95
Using trace files and AVZ scripts 95
Glossary 96
AO Kaspersky Lab 100
Information about third-party code 102
Trademark notices 103
Index 104

About this Guide

The Implementation Guide for Kaspersky Security 10 for Windows Server® (hereinafter "Kaspersky Security") is intended for specialists who install and administer Kaspersky Security, as well as for specialists who provide technical support to organizations that use Kaspersky Security.

In this Guide you can find information about configuring and using Kaspersky Security for network attached storage protection.

This Guide will also help you to learn about sources of information about the application and ways to receive technical support.

It is implied that by the moment you are reading this document you have already had a copy of the application with the RPC-Network Storage Protection and ICAP-Network Storage Protection components installed (see *Kaspersky Security 10 for Windows Server Installation Guide*) and a key with support of the Network Attached Storage Protection feature added to the application (for licensing information please refer to the *Kaspersky Security 10 for Windows Server Administrator's Guide*).

In this section

In this document 6

Document conventions 8

In this document

The Implementation Guide for Network Storage Protection contains the following sections:

Sources of information about Kaspersky Security

This section lists the sources of information about the application.

Kaspersky Security

This section describes the features, components, and distribution kit of Kaspersky Security.

Hardware and software requirements

This section lists the hardware and software requirements of Kaspersky Security.

Integrating Kaspersky Security with network attached storages

This section describes the principles of joint operation of Kaspersky Security and network attached storages.

Managing Kaspersky Security Console

This section provides information about Kaspersky Security Console and describes how to manage Kaspersky Security using Kaspersky Security Console installed on the protected server or a different computer.

Viewing the Network Attached Storage Protection status

This section contains instructions on how to view information about the current status of Network Attached Storage Protection.

Protection of EMC™ network attached storages of the Celerra™ / VNX™ group

This section provides information on the protection of EMC network attached storages of the Celerra / VNX group and on integration of Kaspersky Security with a Celerra / VNX network attached storage.

RPC-Network Storage Protection

This section provides information about the RPC-Network Storage Protection task, configuration of connection between a network attached storage and Kaspersky Security, and instructions on how to define the protection task settings and the security settings of RPC-network storages.

ICAP-Network Storage Protection

This section contains information about the ICAP-Network Storage Protection task, and how to connect a network attached storage to Kaspersky Security, as well as instructions on how to configure protection task settings and ICAP-network storage security settings.

Contacting Technical Support

This section describes the ways to receive technical support and the conditions on which it is available.

Glossary

This section contains a list of terms, which are mentioned in the document, as well as their respective definitions.

AO Kaspersky Lab

This section provides information about Kaspersky Lab AO.

Information about third-party code

This section provides information about third-party code used in the application.

Document conventions

This document uses the following conventions (see table below).

Таблица 1. Document conventions

Sample text	Description of document convention
Note that...	Warnings are highlighted in red and set off in a box. Warnings contain information about actions that my have undesirable consequences.
We recommend that you use...	Notes are set off in a box. Notes contain supplementary and reference information.
Example:	Examples are given in blocks against a blue background under the heading "Example".

Sample text	Description of document convention
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. These keys must be pressed simultaneously.
Click the **Enable** button.	Names of application interface elements, such as text boxes, menu items, and buttons, are set off in bold.
► *To configure a task schedule:*	Introductory phrases of instructions are italicized and accompanied by an arrow.
In the command line, type `help` 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 must be entered from the keyboard
<User name>	Variables are enclosed in angle brackets. Instead of a variable, the corresponding value should be inserted, omitting the angle brackets.

Sources of information about Kaspersky Security

This section lists the sources of information about the application.

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

In this section

Sources for independent retrieval of information 10

Discussing Kaspersky Lab applications on the forum 12

Sources for independent retrieval of information

You can use the following sources to find information about Kaspersky Security 10 for Windows Server:

- Kaspersky Security page on the Kaspersky Lab website
- Kaspersky Security page on the Technical Support website (Knowledge Base)
- Online help
- Manuals

If you did not find a solution to your problem, contact Kaspersky Lab Technical Support (see the section "Contacting Technical Support" on page 93).

An Internet connection is required to use online information sources.

Kaspersky Security page on the Kaspersky Lab website

On the Kaspersky Security 10 for Windows Server page (http://www.kaspersky.com/business-security/windows-server-security), you can view general information about the application, its functions and features.

The Kaspersky Security 10 for Windows Server page contains a link to eStore. There you can purchase the application or renew your license.

Kaspersky Security page in Knowledge Base

Knowledge Base is a section on the Technical Support website.

The Kaspersky Security 10 for Windows Server page in the Knowledge Base (http://support.kaspersky.com/ksws10) features articles that provide useful information, recommendations, and answers to frequently asked questions about how to purchase, install, and use the application.

Knowledge Base articles can answer questions relating to not only Kaspersky Security 10 for Windows Server but also to other Kaspersky Lab applications. Knowledge Base articles can also include Technical Support news.

Kaspersky Security documentation

Kaspersky Security 10 for Windows Server Installation Guide describes how you can perform the following tasks:

- Prepare Kaspersky Security for installation, install and activate the application
- Prepare Kaspersky Security for operation
- Restore or delete Kaspersky Security

Kaspersky Security 10 for Windows Server Administrator's Guide contains information about configuring and using Kaspersky Security.

In the Implementation Guide for Network Attached Storage Protection you can find information about configuring and using Kaspersky Security for Network Attached Storage Protection.

Discussing Kaspersky Lab applications on the forum

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

On this forum you can view existing threads, leave your comments, and create new discussion threads.

Kaspersky Security

Kaspersky Security 10 for Windows Server (previously Kaspersky Anti-Virus for Windows Servers Enterprise Edition) protects servers running on Microsoft® Windows® operating systems and network attached storages against viruses and other computer security threats to which servers are exposed through file exchange. Kaspersky Security is designed for use on local area networks of medium to large organizations. Kaspersky Security users are corporate network administrators and specialists responsible for anti-virus protection of the corporate network.

You can install Kaspersky Security on the following servers:

- Terminal servers
- Print servers
- Application servers
- Domain controllers
- Servers that are protecting network attached storages
- File servers – these servers are more likely to get infected because they exchange files with user workstations

Kaspersky Security can be managed in the following ways:

- via Kaspersky Security Console installed on the same server as Kaspersky Security or on a different computer
- Using commands in the command line
- Via Administration Console of Kaspersky Security Center

The Kaspersky Security Center application can also be used for centralized administration of multiple servers running Kaspersky Security.

It is possible to review Kaspersky Security performance counters for the "System Monitor" application, as well as SNMP counters and traps.

Kaspersky Security components and functions

The application includes the following components:

- Real-Time Protection.

  Kaspersky Security scans objects when they are accessed. Kaspersky Security scans the following objects:

  - Files
  - Scripts
  - Alternate file system threads (NTFS threads)
  - Master boot record and boot sectors on the local hard drives and external devices

- Server Control.

  Kaspersky Security monitors all attempts to access network file resources, enables Applications Launch Control, and blocks access to the server for remote computers if they show malicious or encryption activity.

- RPC-Network Storage Protection and ICAP-Network Storage Protection.

  Kaspersky Security installed on a server under a Microsoft Windows operating system protects network attached storages against viruses and other security threats that infiltrate the server through exchange of files.

- On-demand scan.

  Kaspersky Security runs a single scan of the specified area for viruses and other computer security threats. Kaspersky Security scans server files and RAM and also startup objects.

The following functions are implemented in the application:

- Databases and software modules update.

  Kaspersky Security downloads updates of application databases and modules from FTP or HTTP update servers of Kaspersky Lab, Kaspersky Security Center Administration Server, or other update sources.

- Quarantine.

  Kaspersky Security quarantines probably infected objects by moving such objects from their original location to *Quarantine*. For security purposes, objects are stored in Quarantine in encrypted form.

- Backup.

  Kaspersky Security stores encrypted copies of objects classified as *Infected* or *Probably infected* in *Backup* before disinfecting or deleting them.

- Administrator and user notifications.

  You can configure the application to notify the administrator and users who access the protected server about events in Kaspersky Security operation and the status of Anti-Virus protection on the server.

- Importing and exporting settings.

  You can export Kaspersky Security settings to an XML configuration file and import settings into Kaspersky Security from the configuration file. All application settings or only settings for individual components can be saved to a configuration file.

- Applying templates.

  You can manually configure the security settings of a node in the server file resources tree and save the values of the configured settings to a template. This template can then be used to configure the security settings of other nodes in Kaspersky Security protection and scan tasks.

- Writing events to the event log.

  Kaspersky Security logs information about the settings of application components, the current status of tasks, events that occurred during their run, events associated with Kaspersky Security management, and information required for failure diagnostics in the Kaspersky Security operation.

- Hierarchical storage.

  Kaspersky Security can operate in hierarchical storage management mode (HSM systems). HSM systems allow data relocation between fast local drives and slow long-term data storage devices.

- Trusted zone.

  You can create a list of exclusions for protection scope or scan scope which Kaspersky Security applies to On-Demand Scan, Real-Time File Protection, Script Monitoring, and RPC-Network Storage Protection.

- Managing permissions.

  You can configure the rights of managing Kaspersky Security and the rights of managing Windows services, that are registered by the application, for users and groups of users.

Hardware and software requirements

This section lists the hardware and software requirements of Kaspersky Security.

In this section

Requirements for the server on which Kaspersky Security is deployed 17

Requirements for the protected network attached storage 19

Requirements for the computer on which Kaspersky Security Console is installed 20

Requirements for the server on which Kaspersky Security is deployed

Before installing Kaspersky Security, you must uninstall other anti-virus applications from the server.

You can install Kaspersky Security without uninstalling Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition.

Hardware requirements for the server

General requirements:

- x86-64-compatible single-core or multicore systems
- disk space requirements:
  - for installing all application components: 70 MB
  - for downloading and storing anti-virus databases of the application: 2 GB (recommended)
  - for storing objects in Quarantine and in Backup: 400 MB (recommended)

- for storing logs: 1 GB (recommended)

Minimum configuration:

- processor: 1.4 GHz single-core
- RAM: 1GB
- drive subsystem: 4 GB of free space

Recommended configuration:

- processor: 2.4 GHz quad-core
- RAM: 2 GB
- drive subsystem: 4 GB of free space

Software requirements for the server

You can install Kaspersky Security on a server under a 32-bit or 64-bit Microsoft Windows operating system.

For installation and operation of Kaspersky Security, Microsoft Windows Installer 3.1 must be installed on the server.

You can install Kaspersky Security on a server under one of the following 32-bit Microsoft Windows operating systems:

- Windows Server 2008 Standard / Enterprise / Datacenter SP1 or later
- Windows Server 2008 Core Standard / Enterprise / Datacenter SP1 or later

You can install Kaspersky Security on a server under one of the following 64-bit Microsoft Windows operating systems:

- Windows Server 2008 Standard / Enterprise / Datacenter SP1 or later
- Windows Server 2008 Core Standard / Enterprise / Datacenter SP1 or later
- Windows Server 2008 R2 Standard / Enterprise / Datacenter SP1 or later
- Windows Server 2008 R2 Core Standard / Enterprise / Datacenter SP1 or later

- Windows Hyper-V® Server 2008 R2 SP1 or later
- Windows Server 2012 Essentials / Standard / Foundation / Datacenter
- Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter
- Windows Hyper-V Server 2012
- Windows Hyper-V Server 2012 R2

You can install Kaspersky Security on the following terminal servers:

- Microsoft Remote Desktop Services based on Windows 2008 Server
- Microsoft Remote Desktop Services based on Windows 2012 Server
- Microsoft Remote Desktop Services based on Windows 2012 Server R2
- Citrix® XenApp® 6.0, 6.5, 7.0, 7.5, 7.6
- Citrix XenDesktop® 7.0, 7.1, 7.5, 7.6

Requirements for the protected network attached storage

Kaspersky Security can be used to protect the following network attached storages:

- NetApp with one of the following operating systems:
  - Data ONTAP 7.x and Data ONTAP 8.x in 7-mode
  - Data ONTAP 8.2.1 or higher in cluster-mode
- EMC Celerra / VNX with the following software:
  - EMC DART 6.0.36 or higher
  - Celerra (CAVA) Anti-Virus Agent 4.5.2.3 or higher
- EMC Isilon™ with the operating system OneFS™ 7.0 or later

- Hitachi NAS on one of the following platforms:
  - HNAS 4100
  - HNAS 4080
  - HNAS 4060
  - HNAS 4040
  - HNAS 3090
  - HNAS 3080
- IBM® NAS series IBM System Storage® N series
- Oracle® NAS Systems series Oracle ZFS Storage Appliance
- Dell™ NAS on the platform Dell Compellent™ FS8600

Requirements for the computer on which Kaspersky Security Console is installed

Hardware requirements for the computer

Recommended RAM amount: at least 128 MB.

Free disk space: 30 MB.

Software requirements for the computer

You can install Kaspersky Security Console on a computer running a 32-bit or 64-bit Microsoft Windows operating system.

The computer should have Microsoft Windows Installer 3.1 in order to support installation and operation of Kaspersky Security Console.

You can install Kaspersky Security Console on a computer running one of the following 32-bit Microsoft Windows operating systems:

- Windows Server 2008 Standard / Enterprise / Datacenter SP1 or later
- Microsoft Windows XP Professional with Service Pack 2 or later
- Microsoft Windows Vista® Editions
- Microsoft Windows 7 Editions
- Microsoft Windows 8
- Microsoft Windows 8 Enterprise / Professional
- Microsoft Windows 8.1
- Microsoft Windows 8.1 Enterprise / Professional
- Microsoft Windows 10 Enterprise / Professional

You can install Kaspersky Security Console on a computer running one of the following 64-bit Microsoft Windows operating systems:

- Windows Server 2008 Standard / Enterprise / Datacenter SP1 or later
- Windows Server 2008 R2 Standard / Enterprise / Datacenter SP1 or later
- Windows Hyper-V Server 2008 R2 SP1 or later
- Windows Server 2012 Essentials / Standard / Foundation / Datacenter
- Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter
- Windows Hyper-V Server 2012
- Windows Hyper-V Server 2012 R2
- Microsoft Windows XP Professional Edition SP2 or later
- Microsoft Windows Vista Editions
- Microsoft Windows 7 Editions
- Microsoft Windows 8

- Microsoft Windows 8 Enterprise / Professional
- Microsoft Windows 8.1
- Microsoft Windows 8.1 Enterprise / Professional
- Microsoft Windows 10 Enterprise / Professional

Integrating Kaspersky Security with network attached storages

This section provides information about the principles of joint operation of Kaspersky Security and network attached storages.

Protecting an EMC network attached storage of the Celerra / VNX group

Kaspersky Security interacts with an EMC network attached storage of the Celerra / VNX group using CAVA (Celerra Antivirus Agent) running on the computer with Kaspersky Security installed. When running, Kaspersky Security checks the computer for installed CAVA, which must meet the requirements of Kaspersky Security (see section "Requirements for the protected network storage" on page 19).

When an attempt is made to read or write a file stored in a network attached storage, this storage initiates a network request and hands the file to CAVA. CAVA writes the received file to a local disk of the computer, saving it in a dedicated folder. The Real-Time File Protection component intercepts the file operation and scans the file in accordance with the settings defined in the Real-Time File Protection task, for example, disinfecting or deleting the file. CAVA analyzes Kaspersky Security actions and uses this information to create the check result and hand it to the network attached storage.

RPC-Network Storage Protection

Interaction between Kaspersky Security and an RPC-network storage (such as NetApp or Hitachi NAS in RPC mode) requires the RPC (Remote Procedure Call) protocol.

Kaspersky Security maintains a continuous connection with the network attached storage and regularly initiates RPC requests. When an attempt is made to read or create / write to a file stored in a network attached storage, the latter provides Kaspersky Security direct access to the file using the CIFS protocol. The RPC-Network Storage Protection component scans the file in accordance with the settings defined in the RPC-Network Storage Protection task. When a threat is detected, Kaspersky Security performs the actions defined in the task settings (including file disinfection or deletion) on the file, and then it sends the scan result to the network attached storage.

ICAP-Network Storage Protection

With an ICAP-network storage (such as EMC Isilon, IBM NAS, or Hitachi NAS in ICAP mode), Kaspersky Security functions as a service operating via the Internet Content Adaptation Protocol (ICAP).

When an attempt is made to read or create / write to a file stored in a network attached storage, the latter generates an ICAP request to Kaspersky Security and sends the file inside this request. The ICAP-Network Storage Protection component scans the file in accordance with the settings defined in the ICAP-Network Storage Protection task. When a threat is detected, Kaspersky Security performs the actions defined in the task settings on the file, and then it returns the scan result to the network attached storage. If the Disinfect action is specified in the settings, and the file is successfully disinfected, Kaspersky Security returns the disinfected file to the network attached storage as the response to the request.

In this section

Preparing for launch of the Network Attached Storage Protection task 24

Preparing for launch of the Network Attached Storage Protection task

This section provides instructions on how to prepare a Microsoft Windows with Kaspersky Security installed for integration with network data storage systems and subsequent launch of the Network Attached Storage Protection task.

In this section

Configuring security settings of local policies in the local group policy editor 25

Configuring inbound and outbound connections in Windows firewall 26

Configuring security settings of local policies in the local group policy editor

The names of settings may vary under different Windows operating systems.

► *To define the security settings of local policies in the local group policy editor:*

1. Open the **Local group policy editor** using one of the following methods:
   - If you define the settings locally, click the **Start** button, enter the `gpedit.msc` command at the search bar, and press **ENTER**.
   - If you define the settings from another computer:
     a. Click the **Start** button, enter the `mmc` command at the search bar, and press **ENTER**.

     The **Management Console** window opens.

     b. In the window that opens, select **File** → **Add or remove a snap-in**.

     The **Add or remove snap-ins** window opens.

     c. In the list of available snap-ins, select the **Group policy object editor** snap-in and click the **Add** button.

     The Group Policy Wizard starts.

     d. In the Wizard window, click the **Browse** button.

     The **Search group policy object** window opens.

     e. In the window that opens, on the **Computers** tab, select **Another computer** and specify a server with Kaspersky Security installed, using one of the following methods:
        - In the entry field, specify the domain name of a server with Kaspersky Security installed
        - Click the **Browse** button and, in the computer selection window that opens, select a server with Kaspersky Security installed, using search by domain or by workgroup.
2. Click **OK**.

   a. Any changes will be saved.

3. Select **Computer configuration** → **Windows configuration** → **Security settings** → **Local policies** → **Security settings**.

4. Specify the following values for network access settings:

   - **Network access: Let For everyone permissions apply to anonymous users** – **Enabled**
   - **Network access: Do not allow anonymous enumeration of SAM accounts** – **Disabled**
   - **Network access: Restrict anonymous access to named pipes and shares** – **Disabled**

5. Restart the server with Kaspersky Security installed.

The applied changes take effect.

Configuring inbound and outbound connections in Windows firewall

> The names of settings may vary under different Windows operating systems.

► *To configure inbound and outbound connections in Windows firewall:*

1. Open the settings window of Windows firewall in one of the following ways:

   - If you configure Windows firewall locally, click the **Start** button, enter the `wf.msc` command at the search bar, and press **ENTER**.
   - If you configure Windows firewall from another computer:

     a. Click the **Start** button, enter the `mmc` command at the search bar, and press **ENTER**.

     The **Management Console** window opens.

     b. In the window that opens, select **File** → **Add or remove a snap-in**.

     The **Add or remove snap-ins** window opens.

c. In the list of available snap-ins, select the **Windows firewall** snap-in and click the **Add** button.

The **Select computer** window opens.

d. In the window that opens, select **Another computer** and specify a server with Kaspersky Security installed, using one of the following methods:

- In the entry field, specify the domain name of a server with Kaspersky Security installed
- Click the **Browse** button and, in the integrated security subject selection window that opens, select a server with Kaspersky Security installed, using search by domain or by workgroup.

2. Click **OK**.

a. Any changes will be saved.

3. Create rules for inbound and outbound connections with the following settings:

- Allow inbound connections from all remote ports to local ports TCP 137 – 139, TCP 445.
- Allow outbound connections from all local ports to remote ports TCP 137 – 139, TCP 445.

By default, Windows firewall allows all inbound connections for which no denying rules have been set. If the default settings are applied, no rule should be created for outbound connections.

The Windows firewall settings can also be defined by a group or domain policy.

Managing Kaspersky Security Console

This section provides information about Kaspersky Security Console and describes how to manage Kaspersky Security using Kaspersky Security Console installed on the protected server or a different computer.

In this section

About Kaspersky Security Console 28

Starting Kaspersky Security Console from the Start menu 29

Kaspersky Security Console interface 31

Viewing status information for Network Attached Storage Protection 36

Managing Network Attached Storage Protection tasks 38

About Kaspersky Security Console

Kaspersky Security Console is an isolated snap-in added to the Microsoft Management Console.

Kaspersky Security can be managed via the Kaspersky Security Console installed on the protected server or on another computer on the corporate network.

Detailed information about installation and configuration of Kaspersky Security Console is provided in the *Kaspersky Security 10 for Windows Server Installation Guide*.

If Kaspersky Security Console and Kaspersky Security are installed on different computers assigned to different domains, limitations may be imposed on delivery of information from Kaspersky Security to Kaspersky Security Console. For example, after a Kaspersky Security task starts, its status may remain unchanged in the Console.

During installation of Kaspersky Security Console the installation wizard creates the kavfs.msc file in the Installation folder and adds Kaspersky Security snap-in to the list of isolated Microsoft Windows snap-ins.

You can start Kaspersky Security Console from the **Start** menu. The Kaspersky Security snap-in msc-file can be run or the Kaspersky Security snap-in can be added to the existing Microsoft Management Console as a new element in the tree (see section "Kaspersky Security Console window interface" on page 31).

Under a 64-bit version of Microsoft Windows, the Kaspersky Security snap-in can be added only in the 32-bit version of Microsoft Management Console. To do so, open Microsoft Management Console from the command line by executing the command: mmc.exe /32.

Multiple Kaspersky Security snap-ins can be added to one Microsoft Management Console opened in author mode to use it to manage the protection of multiple servers on which Kaspersky Security is installed.

Starting Kaspersky Security Console from the Start menu

The names of settings may vary under different Windows operating systems.

Make sure that Kaspersky Security Console is installed on the computer.

► *To start Kaspersky Security Console from the Start menu take the following steps:*

in the **Start** menu, select **Programs** → **Kaspersky Security 10 for Windows Server** → **Administration Tools** → **Kaspersky Security Console**.

To add other snap-ins to Kaspersky Security Console, start the Console in author mode.

► *To start Kaspersky Security Console in author mode take the following steps:*

1. In the **Start** menu, select **Programs** → **Kaspersky Security 10 for Windows Server** → **Administration Tools**.

2. In the context menu of **Kaspersky Security Console**, select the **Author** command.

Kaspersky Security Console is started in author mode.

If Kaspersky Security Console has been started on the protected server, the Console window opens (see section "Kaspersky Security Console window interface" on page 31).

If you have started Kaspersky Security Console not on a protected server but on a different computer, connect to the protected server.

► *To connect to a protected server:*

1. In the console tree, open the context menu of the **Kaspersky Security** node.

2. Select the **Connect to another computer** command.

   The **Select computer** window opens.

3. Select **Another computer** in the window that opens.

4. Specify the network name of the protected server in the entry field on the right.

5. Click **OK**.

Kaspersky Security Console is connected to the protected server.

If the user account that you are using to log in to Microsoft Windows does not have sufficient permissions to access Kaspersky Security Management on the server, select the **Connect as user** check box and specify a different user account that has such permissions.

Kaspersky Security Console interface

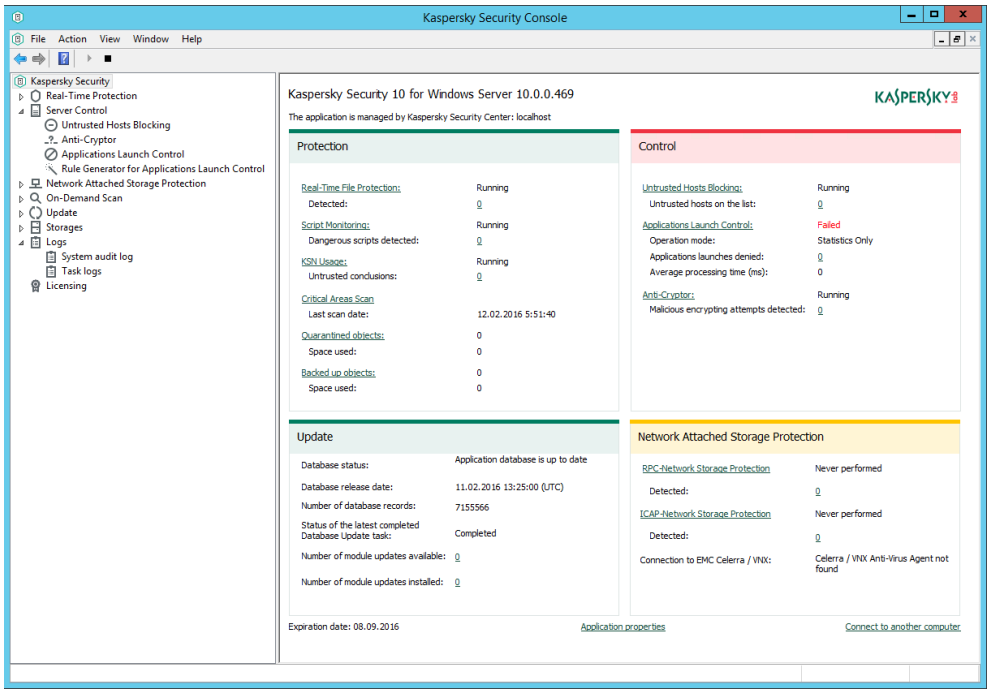
Kaspersky Security Console is displayed in the Microsoft Management Console tree in the form of a node with the name **Kaspersky Security**.

After a connection has been established to Kaspersky Security installed on a different computer, the name of the node is supplemented with the name of the computer on which Kaspersky Security is installed and the name of the user account under which the connection has been established: **Kaspersky Security <computer name> as <account name>**. Upon connection to Kaspersky Security installed on the same computer with the Console, the node name is **Kaspersky Security**.

By default, the Kaspersky Security Console window includes the following elements:

- Console tree
- Details pane
- Quick access bar
- Toolbar

You can also enable the display of the description area and the action panel in the Kaspersky Security Console window.



Console tree

The Console tree displays the Kaspersky Security node and the subnodes of functional components of the application.

The **Kaspersky Security** nodes includes the following subnodes:

- **Real-Time Protection**: manages Real-Time File Protection, Script Monitoring, and KSN services. There is a separate node for each functional area:
  - **Real-Time File Protection**
  - **Script Monitoring**
  - **KSN Usage**
- **Server Control**: controls access to network file resources from remote computers and launches of applications. There is a separate node for each functional area:
  - **Untrusted Hosts Blocking**
  - **Anti-Cryptor**
  - **Applications Launch Control**
  - **Rule Generator for Applications Launch Control**
  - Rule generation group tasks **<Task names>** (if any)
- **Network Attached Storage Protection**: manages protection of network attached storages.
  - **RPC-Network Storage Protection**
  - **ICAP-Network Storage Protection**
- **On-Demand Scan**: manages On-Demand Scan tasks. There is a separate node for each system task:
  - **Scan at Operating System Startup**
  - **Critical Areas Scan**

- **Quarantine Scan**
- **Application Integrity Control**
- Custom tasks **<Task names>** (if any)

A separate control element is created for each custom On-Demand Scan task and for each On-Demand Scan group task created and sent to the server by Kaspersky Security Center Administration Console.

- **Update**: manages updates for Kaspersky Security databases and modules and copies the update to a local update source folder. The node contains subnodes for administering each system update task and last Rollback of Application Database Update task:
  - **Database Update**
  - **Software Modules Update**
  - **Copying Updates**
  - **Rollback of Application Database Update**

  A separate node is created for each task created and sent to the server by Kaspersky Security Center Administration Console.
- **Storages**: management of Quarantine and Backup settings:
  - **Quarantine**
  - **Backup**
- **Logs**: manages logs of Real-Time Protection, Network Attached Storage Protection, On-Demand Scan, Server Control, and Update tasks; manages the Kaspersky Security System audit log. There is a separate control element for each component:
  - **System audit log**
  - **Task logs**
- **Licensing**: add or delete Kaspersky Security keys and activation codes, view license details.

Details pane

The results pane displays information about the selected node. If the **Kaspersky Security** node is selected, the details pane displays information about the current protection status of the server, information about Kaspersky Security, the status of its functional components, as well as license status or key status.

Context menu of the Kaspersky Security node

You can use the items of the context menu of the **Kaspersky Security** node to perform the following operations:

- **Connect to another computer**. Connect to another server to manage Kaspersky Security installed on it. You can also perform this operation by clicking the link in the lower right corner of the details pane of the **Kaspersky Security** node.
- **Start Kaspersky Security** / **Stop Kaspersky Security** (**Start** / **Stop**). Start or stop Kaspersky Security or the selected task. To carry out these operations, you can also use the buttons on the toolbar. You can also perform these operations in context menus of application tasks.
- **Configure trusted zone settings**. View and configure the trusted zone settings.
- **Modify user rights of application management**. View and configure access permissions for managing Kaspersky Security functions.
- **Modify user rights of Kaspersky Security Service management**. View and configure access permissions for managing Kaspersky Security Service.
- **Configure notifications**. View and configure the settings of Kaspersky Security notifications for the administrator and users.
- **Hierarchical storage**. View and configure settings of the hierarchical storage of Kaspersky Security.
- **Export settings**. Export application settings to an XML configuration file. You can also perform this operations in context menus of application tasks.
- **Import settings**. Import application settings from an XML configuration file. You can also perform this operations in context menus of application tasks.

- **About the application**. View information about Kaspersky Security.
- **New window**. Open a new window in Kaspersky Security Console. You can also perform this operations in context menus of application tasks.
- **Refresh**. Refresh the contents of the Kaspersky Security Console window. You can also perform this operations in context menus of application tasks.
- **Properties**. View and configure settings of Kaspersky Security or a selected task. You can also perform this operations in context menus of application tasks.

  > To do so, you can also use the **Application properties** link in the details pane of the **Kaspersky Security** node or use the button on the toolbar.

- **Help**. View information Kaspersky Security Help. You can also perform this operations in context menus of application tasks.

Quick access bar and context menu of Kaspersky Security tasks

You can manage Kaspersky Security tasks using the items of context menus of each task in the Console tree and also do so using the quick access bar located to the right of the details pane of the selected task.

Using links on the quick access bar and context menu items of the selected task, you can perform the following operations:

- **Resume / Pause**. Resume or pause a task. To carry out these operations, you can also use the buttons on the toolbar. This operation is available for Real-Time File Protection and On-Demand Scan tasks.
- **Add task**. Create a new custom task. This operation is available for On-demand scan tasks.
- **Open log**. View and manage a task log The operation is available for all tasks.
- **Save task**. Save and apply modified task settings (see section "Saving task after changing its settings" on page 38). This operation is available for Real-Time File Protection tasks, RPC-Network Storage Protection tasks, On-Demand Scan tasks.
- **Remove task**. Delete a custom task. This operation is available for On-demand scan tasks.
- **Statistics**. View task statistics. This operation is available for the Application Integrity Control task.
- **Settings templates**. Manage templates. This operation is available for Real-Time File Protection, RPC-Network Storage Protection, and On-Demand Scan tasks.

Viewing status information for Network Attached Storage Protection

► *To view information about Network Attached Storage Protection status,*

select the **Kaspersky Security** node in the console tree.

By default, information in the details pane of Kaspersky Security Console is refreshed automatically:

- every 10 seconds in case of a local connection
- every 15 seconds in case of a remote connection

► *To refresh information in the Kaspersky Security node manually,*

select the **Refresh** command in the context menu of the Kaspersky Security node.

Information about the status of protected network attached storages is displayed in the details pane of the **Kaspersky Security** node in the **Network Attached Storage Protection** section (see table below).

Таблица 2. Information about network storage protection

Network Attached Storage Protection section	Information

Network Attached Storage Protection status indicator	The color of the panel with the name of the section reflects the status of tasks described in the section. The indicator can take the following values:
	• Green is displayed in the following cases:
	  ◦ One of the following tasks is running: RPC-Network Storage Protection or ICAP-Network Storage Protection
	  ◦ Kaspersky Security has established connection to EMC software, and the Real-Time File Protection task is running in Kaspersky Security.
	• Yellow is displayed by default in all other cases.

RPC-Network Storage Protection	**Task status** – current task status, for example, *Running* or *Stopped*. **Detected** – the number of objects detected by Kaspersky Security after the task was started. If the number of detected software exceeds 0, the row value is highlighted in red.
ICAP-Network Storage Protection	**Task status** – current task status, for example, *Running* or *Stopped*. **Detected** – the number of objects detected by Kaspersky Security after the task was started. If the number of detected software exceeds 0, the row value is highlighted in red.
Connection to EMC Celerra / VNX	It can take the following values: • **Celerra / VNX Anti-Virus Agent not found** – Kaspersky Security cannot find any EMC software, or an error has occurred in the integration code. • **Protection disabled** – Kaspersky Security has established a connection to EMC software, but the Real-Time File Protection task is not running in Kaspersky Security. • **Protection enabled** – Kaspersky Security has established a connection to EMC software, and the Real-Time File Protection task is running in Kaspersky Security.

Managing Network Attached Storage Protection tasks

This section provides information about Kaspersky Security tasks, how to create them, define task settings, start and stop tasks, and set up schedules for automatic startup and stop of tasks.

In this section

Saving a task after changing its settings 38

Starting / pausing / resuming / stopping tasks manually 39

Managing task schedules 39

Saving a task after changing its settings

The settings of a task that is running or stopped (paused) can be modified. New settings take effect under the following conditions:

- If you changed the settings of a running task, the new settings are applied immediately after saving the task
- If you changed the settings of a stopped (paused) task, the new settings are applied when the task is next started

► *To save modified task settings,*

in the context menu of the task name, select **Save task**.

If after changing task settings another node in the Console tree is selected without first selecting the **Save task** command, the window for saving the settings appears.

► *To save modified settings when switching to another Console node,*

Click **Yes** in the save settings window.

Starting / pausing / resuming / stopping tasks manually

► *To start or stop a Network Attached Storage Protection task:*

1. Open the context menu of the task name in Kaspersky Security Console.
2. Select one of the items: **Start** or **Stop**.

The operation is performed and logged in the system audit log.

Managing task schedules

You can configure the launch schedule for Kaspersky Security tasks, and configure settings for running tasks by schedule.

In this section

Configuring the task launch schedule settings 39

Enabling and disabling scheduled tasks 41

Configuring the task launch schedule settings

You can configure the launch schedule for local system and custom tasks in the Kaspersky Security Console. You cannot configure the launch schedule for group tasks.

► *To configure task launch schedule settings,* do the following*:*

1. Open the context menu of the name of the task for which you wish to configure the launch schedule.
2. Select **Properties**.

   The **Task settings** window opens.

3. In the window that opens, on the **Schedule** tab, select the **Run by schedule** check box.

   Fields containing the On-demand scan task and Update task schedule settings will be unavailable if the launch of this scheduled task is disabled by the Kaspersky Security Center policy.

4. Configure schedule settings in accordance with your requirements. To do this, perform the following actions:

   a. In the **Frequency** list, select one of the following values:

      - **Hourly**, if you want the task to run every hour for a specified number of hours; specify the number of hours in the **Every <number> hours** field
      - **Daily**, if you want the task to run every day for a specified number of days; specify the number of days in the **Every <number> days** field
      - **Weekly**, if you want the task to run every week for a specified number of weeks; specify the number of weeks in the **Every <number> weeks** field Specify the days of the week on which the task will be launched (by default the task is launched on Mondays)
      - **At application launch**, if you want the task to run every time Kaspersky Security starts
      - **After application database update**, if you want the task to run after every update of the application databases

   b. Specify the time for the first task launch in the **Start time** field.

   c. In the **Start date** field, specify the date from which the schedule applies.

      After the task startup frequency has been specified, the time of the first task launch, and the date from which the schedule applies, information about the calculated time for the next task launch will appear in the top part of the window in the **Next start** field. Updated information about the estimated time of the next task launch will be displayed each time you open the **Task settings** window of the **Schedule** tab.

      The **Blocked by policy** value is displayed in the **Next start** field if the active policy settings of Kaspersky Security Center prohibit launching scheduled system tasks.

5. Using the **Advanced** tab configure the following schedule settings in accordance with your requirements.

   - In the **Task stop settings** section:

     a. Select the **Duration** check box and enter the required number of hours and minutes in the fields to the right to specify the maximum duration of the task execution.

     b. Select the **Pause from ... until** check box and enter the start and end values of the time interval in the fields to the right to specify the interval of time in days during which task execution will be paused.

   - In the **Advanced settings** section:

     a. Select the **Cancel schedule from** check box and specify the date from which the schedule will cease to operate.

     b. Select the **Run skipped tasks** check box to enable the launch of skipped tasks.

     c. Select the **Randomize the task start within interval of** check box and specify the value in minutes.

6. Click the **Apply** button.

The configured task launch settings will be saved.

Enabling and disabling scheduled tasks

You can enable and disable scheduled tasks either before or after configuring the schedule settings.

► *To enable or disable the task launch schedule:*

1. Open the context menu of the name of the task for which you wish to configure the launch schedule.

2. Select **Properties**.

   The **Task settings** window opens.

3. In the window that opens on the **Schedule** tab, do one of the following:

    - Select the **Run by schedule** check box if you want to enable the scheduled launch of the task
    - Select the **Run by schedule** check box if you want to enable scheduled task launch

    > The configured task launch schedule settings are not deleted and will be applied at the next scheduled launch of the task.

4. Click the **Apply** button.

The configured task launch schedule settings are saved.

Protecting EMC network attached storages of the Celerra / VNX group

This section provides information on the protection of EMC network attached storages of the Celerra / VNX group (hereinafter also Celerra / VNX) and on integration of Kaspersky Security with a Celerra / VNX network attached storage.

In this section

About protection of EMC network attached storages of the Celerra / VNX group 43

Integrating Kaspersky Security with an EMC network attached storage of the Celerra / VNX group 44

About protection of EMC network attached storages of the Celerra / VNX group

Kaspersky Security installed on a server under a Microsoft Windows operating system protects EMC network attached storages of the Celerra / VNX group against viruses and other security threats that infiltrate the server through exchange of files.

Kaspersky Security scans files located in network share folders in the EMC network attached storage of the Celerra / VNX group when an attempt is made to read or modify the files from a workstation. The network attached storage allows reading or modifying a file if Kaspersky Security has identified that file as safe. If Kaspersky Security has identified a file as infected or probably infected, the network attached storage blocks that file from being read or modified.

Kaspersky Security allows you to configure the actions that the application will perform on infected and probably infected files.

By default, Kaspersky Security performs the following operations:

- Disinfects infected files
- Deletes infected files if disinfection fails

- Moves probably infected files to Quarantine
- Moves a copy of an infected file to Backup before disinfecting or removing this file

To protect a network attached storage, you have to integrate Kaspersky Security with the Celerra / VNX network attached storage.

Protection of the Celerra / VNX network attached storage is provided by the Real-Time File Protection task.

Detailed information about the Real-Time File Protection task is provided in the *Kaspersky Security 10 for Windows Server Administrator's Guide*.

Integrating Kaspersky Security with an EMC network attached storage of the Celerra / VNX group

To protect a network attached storage, you have to integrate Kaspersky Security with the Celerra / VNX network attached storage.

Integration of Kaspersky Security with a Celerra / VNX network attached storage is performed when the following conditions are met:

1. The CAVA (Celerra Antivirus Agent) software agent that is part of the EMC Celerra / VNX software package is installed on the computer protected by Kaspersky Security. Kaspersky Security interacts with the EMC network attached storage of the Celerra / VNX group through this program agent.
2. Real-Time File Protection task

   For detailed information about the Real-Time File Protection task and instructions on how to configure its settings, refer to the *Kaspersky Security 10 for Windows Server Administrator's Guide*.

The status of Kaspersky Security integration with the Celerra / VNX network attached storage is shown in the details pane of the **Kaspersky Security** node (see section "**Viewing status information for Network Attached Storage Protection**" on page 36).

RPC-Network Storage Protection

This section provides information about the RPC-Network Storage Protection, configuration of connection between a network attached storage and Kaspersky Security, and instructions on how to configure the RPC-Network Storage Protection task settings and the security settings in the task.

In this section

About RPC-Network Storage Protection 45

About scanning symbolic links 47

About scanning snapshots and other read-only volumes and folders 47

Configuring a connection between an RPC-network storage and Kaspersky Security 48

Configuring the RPC-Network Storage Protection task 53

Security levels in the RPC-Network Storage Protection task 60

Viewing statistics of the RPC-Network Storage Protection task 70

About RPC-Network Storage Protection

Kaspersky Security installed on a server under Microsoft Windows protects RPC-network storages (such as NetApp network attached storages) against viruses and other computer security threats that infiltrate the server through the exchange of files.

Kaspersky Security scans files located in network share folders in the RPC-network storage (hereinafter also *network attached storage*) when an attempt is made to read or modify the files from a workstation. The network attached storage allows reading or modifying a file if Kaspersky Security has identified that file as safe. If Kaspersky Security has identified a file as infected or probably infected, the network attached storage performs the action according to the configured settings (e.g., blocks that file from being read or modified).

Kaspersky Security allows you to configure the actions that the application will perform on infected and probably infected files.

By default, Kaspersky Security performs the following operations:

- Disinfects infected files
- Deletes infected files if disinfection fails
- Moves probably infected files to Quarantine
- Moves a copy of an infected file to Backup before disinfecting or removing this file

You can protect one network attached storage or several network attached storages using one server with Kaspersky Security installed on it. To improve the performance of the network attached storage and the server with Kaspersky Security, you can use several servers with Kaspersky Security for protection of a single network attached storage. In this case, the network attached storage distributes the workload among associated servers on which Kaspersky Security is installed.

To ensure real-time protection of a network attached storage, add it to Kaspersky Security as part of the protection scope and then configure a connection between the network attached storage and the server with Kaspersky Security installed on it. Kaspersky Security provides an RPC-network storage protection task called RPC-Network Storage Protection.

The RPC-Network Storage Protection task is created by default; it is a system task of Kaspersky Security. You cannot delete or rename this task. You cannot create custom tasks for RPC-Network Storage Protection.

You can configure the RPC-Network Storage Protection task. Settings configured in the RPC-Network Storage Protection task properties are applied to all protection scopes that are added to the task. You can also configure the security settings for each protection scope.

You can run Network Attached Storage Protection tasks if the active key supports network attached storage protection. If you run a Network Attached Storage Protection task when the active key does not support network attached storage protection, the task returns an error. In this case, Kaspersky Security does not protect network attached storages.

The RPC-Network Storage Protection component is available within Kaspersky Security for Storage.

For more details on solutions for protection of organizations that include Kaspersky Security for Windows Server, see the *Administrator's Guide* of *Kaspersky Security 10 for Windows Server.*

About scanning symbolic links

Symbolic link is a specific type of file that contains an indicator redirecting to another object and presented as an absolute or relative path. A symbolic link can point to, for example, an object that is located in a shared network folder of another network attached storage.

Scanning symbolic links in network attached storages typically occurs as follows. Kaspersky Security scans the file that the symbolic link indicates, only if that file is included in the protection scope. If the file that the symbolic link indicates is located beyond the protection scope, Kaspersky Security does not scan that file. If the settings of the network attached storage allow using the link to leave the folder storing that link, you are recommended to make sure that the destination folder makes part of the protection scope. For example, if the settings allow using the symbolic link to browse between shared network folders within the protected network attached storage, you are recommended to make sure that anti-virus scanning is enabled for all shared network folders.

About scanning snapshots and other read-only volumes and folders

Kaspersky Security scans files stored in snapshots and other volumes and folders that are set up in read-only mode, but does not perform any actions on files in those volumes and folders: for example, it does not block access to infected files. To prevent any risk of infection of workstations, you are recommended to mark snapshots and other volumes and folders in read-only mode as hidden form users and provide access to snapshots and other volumes and folders in read-only mode by requesting the administrator.

Configuring a connection between an RPC-network storage and Kaspersky Security

You can run Network Attached Storage Protection tasks if the active key supports network attached storage protection. If you run a Network Attached Storage Protection task when the active key does not support network attached storage protection, the task returns an error. In this case, Kaspersky Security does not protect network attached storages.

To protect an RPC-network storage, you need to configure the connection of the network attached storage to Kaspersky Security.

► *To configure a connection between a network attached storage and Kaspersky Security:*

1. Configure the following settings on the server with Kaspersky Security installed:
   - Add a network attached storage to Kaspersky Security (see section "Adding an RPC-network storage to Kaspersky Security" on page 50).
   - In Kaspersky Security Console, specify the user account under which you want to run the RPC-Network Storage Protection task (see section "Selecting a user account for running the RPC-Network Storage Protection task" on page 49).
   - In the local group policy editor, configure the security settings of local policies (see section "Configuring the security settings of local policies in the local group policy editor" on page 25).
   - In the Windows firewall settings window, configure the rules of outbound and inbound connections in Windows firewall (see section "Configuring inbound and outbound connections in Windows firewall" on page 26).
   - If necessary, install a connector application for the RPC-network storage to be protected by Kaspersky Security.

     You can find information on how to install the connector application for the protected network attached storage in the accompanying manual.

2. In the network attached storage, configure the following settings:

   - Enable the anti-virus protection feature (vscan).
   - Add the user account under which the RPC-Network Storage Protection task must be run to the Backup Operators group.

   You can find information on how to configure your network attached storage in the accompanying manual.

The connection between an RPC-network storage and Kaspersky Security is established.

Selecting a user account for running the RPC-Network Storage Protection task

The user account under which the RPC-Network Storage Protection task will be run must have administrator rights on the server with Kaspersky Security installed and must be included in the Backup Operators group in the network attached storage.

If the network attached storage and the server with Kaspersky Security installed are in the same domain, you can use the domain account. If the network attached storage and the server with Kaspersky Security installed are in the same work group, you can use local accounts with the same user name and the same password.

Only a domain account can be used for network storages running under the Data ONTAP operating system of version 8.2.1 or later in cluster mode.

► *To specify a user account under which the RPC-Network Storage Protection task is started:*

1. Expand the **Network Attached Storage Protection** node in the Kaspersky Security Console tree.
2. Select the **RPC-Network Storage Protection** subnode.
3. In the details pane of the **RPC-Network Storage Protection** node, click the **Properties** link.

   The **Task settings** window opens.

4. In the window that opens, go to the **General** tab, and in the **Network attached storage systems connection settings** section enter the name of the user account under which the task starts, the account password, and the password confirmation.

5. Click **OK**.

The modified settings to run the task with user account permissions are saved.

Creating the protection scope in the RPC-Network Storage Protection task

This section provides instructions on creating and managing a protection scope in the RPC-Network Storage Protection task.

In this section

Adding an RPC-network storage to Kaspersky Security 50

Disabling and enabling protection of an added RPC-network storage 52

Removing an RPC-network storage from the protection scope 53

Adding an RPC-network storage to Kaspersky Security

► *To add an RPC-network storage to the protection scope of Kaspersky Security:*

1. Expand the **Network Attached Storage Protection** node in the Kaspersky Security Console tree.

2. Select the **RPC-Network Storage Protection** subnode.

3. In the details pane of the **RPC-Network Storage Protection** node, click the **Configure protection scope** link.

4. In the window that opens, click the **Add** button.

   The **Add protection scope** window opens.

5. In the **Add protection scope** window, enter the domain name or IP address of the network attached storage.

   If you are using a NetApp storage system managed by NetApp Clustered Data ONTAP operating system, fill in this field by specifying the IP address of the computer on which the connector application is installed, i.e. 127.0.0.1.

6. Click **OK** to add the network attached storage to Kaspersky Security.

   The network attached storage appears in the list of protected network attached storages.

7. Click the **Save** button.

The configured protection scope settings are saved.

Kaspersky Security connects to the network attached storage when the RPC-Network Storage Protection task is launched. If you have specified an incorrect domain name or incorrect IP address for the network attached storage, the task returns an error. Kaspersky Security records information about this event in the system audit log and the task log.

If you are using a NetApp storage system managed by the NetApp Clustered Data ONTAP operating system, Kaspersky Security connects to the connector application installed on the protected server. You are recommended to make sure that the connection between the connector application and the NetApp storage system is configured correctly and that the added network attached storage is protected by Kaspersky Security.

Disabling and enabling protection of an added RPC-network storage

► *To disable protection of an added RPC-network storage:*

1. Expand the **Network Attached Storage Protection** node in the Kaspersky Security Console tree.
2. Select the **RPC-Network Storage Protection** subnode.
3. In the details pane of the **RPC-Network Storage Protection** node, click the **Configure protection scope** link.
4. In the list of protected network attached storages, clear the check box next to the name of the network attached storage for which you want to temporarily disable protection.
5. Click the **Save** button.

Kaspersky Security interrupts the connection with the selected network attached storage.

If you disable the protection feature for all added network attached storages, Kaspersky Security stops the RPC-Network Storage Protection task.

► *To enable protection of an added RPC-network storage:*

1. Expand the **Network Attached Storage Protection** node in the Kaspersky Security Console tree.
2. Select the **RPC-Network Storage Protection** subnode.
3. In the details pane of the **RPC-Network Storage Protection** node, click the **Configure protection scope** link.
4. In the list of protected network attached storages, select the check box next to the name of the network attached storage for which you want to enable protection.
5. Click the **Save** button.

If RPC-Network Storage Protection is enabled, Kaspersky Security establishes a connection to the network attached storage. If the RPC-Network Storage Protection task is not running, you need to start it so that Kaspersky Security establishes a connection with the network attached storage.

Removing an RPC-network storage from the protection scope

► *To delete an RPC-network storage from the RPC-Network Storage Protection task:*

1. Expand the **Network Attached Storage Protection** node in the Kaspersky Security Console tree.
2. Select the **RPC-Network Storage Protection** subnode.
3. In the details pane of the **RPC-Network Storage Protection** node, click the **Configure protection scope** link.
4. In the list of protected network attached storages, select the network attached storage that you want to remove from the protection scope.
5. In the context menu of the name or IP address of the network attached storage that you want to remove from the protection scope, select **Remove from the list**.

The selected network attached storage is removed from the list of protected network attached storages.

Configuring the RPC-Network Storage Protection task

By default, the RPC-Network Storage Protection task has the settings described in the table below. You can change the values of these settings.

When task settings are modified (for example, a different protection scope is specified), Kaspersky Security immediately applies new settings in the running task. Kaspersky Security logs the date and time when task settings were modified in the system audit log.

Таблица 3. Settings of the RPC-Network Storage Protection task

Setting	Default value	Comment
Protection scope	Not available.	You need to add the network attached storage to Kaspersky Security.
Security level	The **Recommended** security level is applied.	You can apply one of the preset security levels to the protected network attached storage, or specify the values of the security settings manually.
Heuristic Analyzer	The **Medium** analysis level is applied.	The Heuristic Analyzer can be enabled or disabled and the analysis level configured.
Trusted zone	Applied.	You can enable and disable the use of the trusted zone and configure it.
KSN Usage	Applied.	You can enable or disable the use of KSN services in the RPC-Network Storage Protection task.
Network storage connection settings	• The **User name** and the **Password** of the user account under which the task is started: none; • **Timeout between reconnection attempts (sec.)** : 5; • **Maximum number of reconnection attempts**: 3; • **Clear cache of scanned files on network attached storage after application database update** – the check box is cleared.	You need to specify the user account under which the RPC-Network Storage Protection task is started. You can also modify other network storage connection settings.
Scheduled task launch	Not applied. The **Run by schedule** check box is cleared. The task is run manually.	You can configure the task to run by schedule, for example at Kaspersky Security startup.

► *To configure settings of the RPC-Network Storage Protection task:*

1. Expand the **Network Attached Storage Protection** node in the Kaspersky Security Console tree.
2. Select the **RPC-Network Storage Protection** subnode.
3. In the details pane of the **RPC-Network Storage Protection** node, click the **Properties** link.

   The **Task settings** window opens.
4. On the **General** tab in the window that opens, configure the following task settings:
   - Using the Heuristic Analyzer (see page 56).
   - Task launch with user account permissions (see section "Selecting an account for running the RPC-Network Storage Protection task" on page 49).
   - Connection to an PRC-network storage (see section "Configuring general settings for PRC-network storage connection" on page 59).
   - Integration with other Kaspersky Security components (see page 57).
5. On the **Schedule** and **Advanced** tabs, configure the scheduled task launch settings (see section "Configuring the task launch schedule settings" on page 39).
6. Click **OK** in the **Task settings** window.

   The modified settings are saved.
7. In the details pane of the **RPC-Network Storage Protection** node, select the **Protection scope settings** tab.
8. Do the following:
   i. Add network attached storage via RPC protocol to the protection scope of Kaspersky Security (see section "Adding an RPC-network storage to Kaspersky Security" on page 50).
   ii. In the list of added network attached storages connected via the PRC protocol, select the network attached storages whose protection you want to activate.
   iii. Select one of the preset security levels (see section "Applying a preset security level in the RPC-Network Storage Protection systems task" on page 62) or configure the security settings of objects manually (see section "Manually configuring the security level settings in the RPC-Network Storage Protection systems task" on page 63).
9. In the context menu of the name of the **RPC-Network Storage Protection** node, select the **Save task** item.

Kaspersky Security immediately applies the new values of settings to the running task. Information about the date and time when the settings were modified and the values of task settings before and after modification are saved in the task log.

Using the Heuristic Analyzer

The RPC-Network Storage Protection task can use the Heuristic Analyzer with a configured level of analysis.

► *To configure the settings of Heuristic Analyzer used in the RPC-Network Storage Protection task:*

1. Expand the **Network Attached Storage Protection** node in the Kaspersky Security Console tree.
2. Select the **RPC-Network Storage Protection** subnode.
3. In the details pane of the **RPC-Network Storage Protection** node, click the **Properties** link.

   The **Task settings** window opens.
4. In the window that opens, go to the **General** tab and do the following in the **Heuristic Analyzer** section:

   - Clear or select the **Use Heuristic Analyzer** check box.
   - If necessary, adjust the level of analysis using the slider.

     The slider allows you to adjust the heuristic analysis level. The scanning intensity level sets the balance between the thoroughness of searches for threats, the load on the operating system's resources and the time required for scanning.

     The following scanning intensity levels are available:

     - **Light**. Heuristic analyzer performs fewer operations found inside executable files. The probability of threat detection in this mode is somewhat lower. Scanning is faster and less resource-intensive.
     - **Medium**. Heuristic Analyzer performs the number of instructions found within executable files recommended by the experts of Kaspersky Lab.

       This level is selected by default.

- **Deep**. Heuristic analyzer performs more operations found in executable files. The probability of threat detection in this mode is higher. The scan uses up more system resources, takes more time, and can cause a higher number of false alarms.

The slider is available if the **Use Heuristic Analyzer** check box is selected.

5. Click **OK**.

The newly configured settings are applied.

Integration with other components of Kaspersky Security

You can use the RPC-Network Storage Protection task together with the following functional components of Kaspersky Security:

- Trusted zone
- KSN Usage task

Trusted zone is a predefined list of exclusions for protection scope or scan scope.

You can enable or disable the use of the trusted zone in the RPC-Network Storage Protection task. After the trusted zone is enabled or disabled, exclusions in this zone will be applied or removed immediately.

Kaspersky Security Network (KSN) is an infrastructure of online services providing access to Kaspersky Lab's online knowledge base on the reputation of files, web resources and programs.

You can enable or disable the KSN usage in the RPC-Network Storage Protection task. After you enable or disable the KSN usage, the task starts or stops showing verdicts about the reputation of files being scanned based on information received from KSN.

To start the KSN Usage task, you must accept the KSN Statement. The KSN Usage task does not start automatically at startup of Kaspersky Security by default.

Detailed information about the trusted zone and the KSN Usage task is provided in the *Kaspersky Security 10 for Windows Server Administrator's Guide*.

► *To enable or disable the use of other application components in the RPC-Network Storage Protection task:*

1. Expand the **Network Attached Storage Protection** node in the Kaspersky Security Console tree.
2. Select the **RPC-Network Storage Protection** subnode.
3. In the details pane of the **RPC-Network Storage Protection** node, click the **Properties** link.

   The **Task settings** window opens.
4. In the window that opens, go to the **General** tab and do the following in the **Integration with other Kaspersky Security components** section:
   - Select or clear the **Apply trusted zone** check box.

     This check box enables / disables use of the trusted zone for a task.

     If the check box is selected, Kaspersky Security adds file operations of trusted processes to the scan exclusions configured in the task settings.

     If the check box is cleared, Kaspersky Security disregards the file operations of trusted processes when forming the protection scope for the Real-Time File Protection task.

     The check box is selected by default.
   - Select or clear the **Use KSN for protection** check box.

     This check box enables or disables the use of KSN services in the RPC-Network Storage Protection task.

     If the check box is selected, the application uses Kaspersky Security Network data to ensure a faster response time by the application to new threats and reduces the likelihood of false positives.

     If the check box is cleared, the RPC-Network Storage Protection task does not use KSN services.

     The check box is selected by default.
5. Click **OK**.

The newly configured settings are saved.

Configuring general settings for RPC-Network Storage connection

► *To configure general settings of the connection to an RPC-network storage:*

1. Expand the **Network Attached Storage Protection** node in the Kaspersky Security Console tree.

2. Select the **RPC-Network Storage Protection** subnode.

3. In the details pane of the **RPC-Network Storage Protection** node, click the **Properties** link.

   The **Task settings** window opens.

4. In the window that opens, go to the **General** tab and do the following in the **Network attached storage systems connection settings** section:

   - In this field, enter a value for the timeout between attempts to recover the connection with the network attached storage.

   - In this field, enter a value for the maximum number of attempts to recover the connection with the network attached storage.

     > You are recommended to keep default values or specify larger values.

   - If you want Kaspersky Security to clear the cache of scanned files of the network attached storage after each update of the application databases, select the **Clear cache of scanned files on network attached storage after application database update** check box.

   - If you want Kaspersky Security to save the cache of scanned files of the network attached storage after each update of the application databases, clear the **Clear cache of scanned files on network attached storage after application database update** check box.

5. Click **OK**.

The newly configured settings are saved.

Security levels in the RPC-Network Storage Protection task

This section describes the security settings and provides instructions on applying preset security levels and configuring security settings manually in the RPC-Network Storage Protection task.

In this section

About security levels in the RPC-Network Storage Protection task 60

Applying a preset security level in the RPC-Network Storage Protection task 62

Manually configuring the security level settings in the RPC-Network Storage Protection task ... 63

Using security level settings templates in the RPC-Network Storage Protection task..... 67

About security levels in the RPC-Network Storage Protection task

In the RPC-Network Storage Protection task, you can apply any of the following preset security levels to every protected storage system: **Maximum performance**, **Recommended**, or **Maximum protection**. Each of these levels contains its own pre-defined set of security settings (see the table below). You can also specify the values of the security settings manually; in this case, the security level of the network attached storage changes to **Custom**.

Maximum performance

The **Maximum performance** security level is recommended if, apart from using Kaspersky Security on servers and workstations, there are additional computer security measures on your network, for example, firewalls are set up, network users comply with existing security policies.

Recommended

The **Recommended** security level ensures an optimum combination of protection quality and degree of impact on the performance of protected servers. This level is recommended by

Kaspersky Lab experts as sufficient for protection of file servers on most corporate networks. The **Recommended** security level is set by default.

Maximum Protection

The **Maximum protection** security level is recommended if you have higher requirements for computer security on your organization's network.

Таблица 4. Settings of preset security levels in the RPC-Network Storage Protection task

Options	Security level		
	Maximum performance	Recommended	Maximum Protection
Objects protection	Objects scanned according to list of extensions specified in anti-virus database	Objects scanned by format	Objects scanned by format
Compound objects protection	Packed objects	• SFX archives • Packed objects • OLE objects	• SFX archives • Packed objects • OLE objects
Action to perform on infected objects	Block access and disinfect. Delete if disinfection fails	Block access and perform recommended action	Block access and disinfect. Delete if disinfection fails
Action to perform on probably infected objects	Block access and quarantine	Block access and perform recommended action	Block access and quarantine

Options	Security level		
	Maximum performance	Recommended	Maximum Protection
Actions depending on the detected object type	No	No	No
Exclude files	No	No	No
Do not detect	No	No	No
Stop scanning if it takes longer than (sec.)	60	60	60
Do not scan compound objects larger than (MB)	8	8	No

Applying a preset security level in the RPC-Network Storage Protection task

► *To apply one of the preset security levels to an RPC-network storage:*

1. Expand the **Network Attached Storage Protection** node in the Kaspersky Security Console tree.
2. Select the **RPC-Network Storage Protection** subnode.
3. In the details pane of the **RPC-Network Storage Protection** node, click the **Configure protection scope** link.
4. In the list of protected network attached storages, select the network attached storage for which you want to select a preset security level.

5. On the **Security level** tab, select one of the following preset security levels in the list:

   - **Maximum Protection**;
   - **Recommended**;
   - **Maximum performance**.

   The **Security level** tab displays the main values for settings of the selected security level. The applied security level is displayed next to the name of the network attached storage in the list of protected network attached storages.

6. Click the **Save** button.

The configured security level settings are saved and applied to the running task.

You can also configure the security settings for a protected network attached storage manually (see section "Manually configuring the security level settings in the RPC-Network Storage Protection task" on page 63).

See also

About security levels in the RPC-Network Storage Protection task 60

Manually configuring the security level settings in the RPC-Network Storage Protection task ... 63

Manually configuring the security level settings in the RPC-Network Storage Protection task

► *To manually configure the security settings of an RPC-network storage:*

1. Expand the **Network Attached Storage Protection** node in the Kaspersky Security Console tree.

2. Select the **RPC-Network Storage Protection** subnode.

3. In the details pane of the **RPC-Network Storage Protection** node, click the **Configure protection scope** link.

4. In the list of protected network attached storages, select the network attached storage whose security settings you want to configure.

   You can apply a preset security settings template.

5. Configure the settings of the selected network attached storage in accordance with your computer security requirements. To do this, perform the following actions:

   - On the **General** tab take the following actions:

     - In the **Objects protection** section, specify objects to be scanned by Kaspersky Security:

       - **All objects**.

       Kaspersky Security scans all objects.

       - **Objects scanned by format**.

       Kaspersky Security scans only infectable objects based on file format.

       Kaspersky Lab compiles the list of formats. It is included in the Kaspersky Security databases.

       - **Objects scanned according to list of extensions specified in anti-virus database**.

       Kaspersky Security scans only infectable objects based on file extension.

       Kaspersky Lab compiles the list of extensions. It is included in the Kaspersky Security databases.

       - **Objects scanned by specified list of extensions.**

       Kaspersky Security scans files based on file extension. List of file extensions can be manually customized in the **List of extensions** window, which can be opened by clicking **Edit** button.

This setting can be also configured in the network attached storage. If the setting is configured in Kaspersky Security, the network attached storage sends the object for scanning, and Kaspersky Security declares the object safe without running a virus scan. If the setting is configured in the network attached storage, the network attached storage does not send the object for scanning. To reduce network traffic and the load on the server with Kaspersky Security installed, it is recommended to configure settings that limit the number of objects scanned in the network attached storage.

- In the **Compound objects protection** section, specify compound objects to be scanned by Kaspersky Security.

- On the **Actions** tab take the following actions:

  - In the **Action to perform on infected objects** section, select the action to be performed by Kaspersky Security on detecting an infected object.
  - In the **Action to perform on probably infected objects** section, select the action to be performed by Kaspersky Security on detecting a probably infected object.
  - In the **Actions depending on the detected object type** section, specify the actions to be performed by Kaspersky Security on objects depending on the type of object detected.

- On the **Performance** tab take the following actions:

  - In the **Exclusions** section, specify objects that you want Kaspersky Security to exclude from scanning:
    - To exclude files from scanning, select the **Exclude files** check box and specify the names or name masks of files to be excluded.
    - To exclude detectable objects (such as remote administration utilities), select the **Do not detect** check box and specify the names or name masks of detectable objects, according to the Virus Encyclopedia classification (http://www.securelist.com).

You can also define these settings for the task as a whole in the exclusion settings in the trusted zone.

- In the **Advanced settings** section, specify the maximum duration of object scanning and the maximum size of the compound file being scanned.

If you are using a network attached storage under the Clustered Data ONTAP operating system, this setting can be also configured in the network attached storage. If the setting is configured in Kaspersky Security, the network attached storage sends the object for scanning, and Kaspersky Security declares the object safe without running a virus scan. If the setting is configured in the network attached storage, the network attached storage does not send the object for scanning. To reduce network traffic and the load on the server with Kaspersky Security installed, it is recommended to configure settings that limit the number of objects scanned in the network attached storage.

6. Click the **Save** button.

The configured custom security level settings are saved and applied to the running task.

Using security level settings templates in the RPC-Network Storage Protection task

This section provides instructions on how to manage security level settings templates in the RPC-Network Storage Protection task.

In this section

Creating a security settings template 67

Applying a security settings template 68

Viewing security settings in a template 69

Deleting a security settings template 69

Creating a security settings template

► *To manually save the security settings of a node and save those settings to a template:*

1. In the Kaspersky Security Console tree, select the task for which you want to save the security settings to a template.
2. In the details pane of the selected task, click the **Configure protection scope** or **Configure scan scope** link.
3. In the tree or in the list of the server's network file resources choose the node which settings you want to save as a template.
4. On the **Security level** tab click the **Save as template** button.

   The **Template properties** window opens.
5. In the **Template name** field, enter the name of the template.
6. Enter additional template information in the **Description** field.
7. Click **OK**.

The template with the set of security values for settings will be saved.

Applying a security settings template

► *To apply security settings from a template for a selected node:*

1. In the Kaspersky Security Console tree, select the task for which you want to save the security settings to a template.
2. In the details pane of the selected task, click the **Configure protection scope** or **Configure scan scope** link.
3. In the tree or in the list of the server's network file resources select the node for which you want to apply the template.
4. Select **Apply template** → **<Template name>**.
5. In the Console tree, open the context menu of the configurable task.
6. Select **Save task**.

The security settings template is applied to the selected node in the server file resource tree. The **Security level** tab of the selected node will now have the value **Custom**.

Security settings from a template applied to a parent node in the server file resource tree are installed in all subnodes.

If the protection scope or scan scope of the subnodes in the server file resource tree was configured separately, the security settings from the template applied to the parent node are not set automatically for such subnodes.

► *To apply security settings from a template for all selected nodes:*

1. In the Kaspersky Security Console tree, select the task for which you want to save the security settings to a template.
2. In the details pane of the selected task, click the **Configure protection scope** or **Configure scan scope** link.
3. In the tree or in the list of the server's network file resources select the node for which you want to apply the template.
4. Select **Apply template** → **<Template name>**.

5. In the Console tree, open the context menu of the configurable task.

6. Select **Save task**.

The security settings template is applied to the parent and all subnodes in the server file resource tree. The **Security level** tab of the selected node will now have the value **Custom**.

Viewing security settings in a template

► *To view security settings in a template that you have created, perform the following steps:*

1. In the Kaspersky Security Console tree, select the task for which you want to view the security template.

2. In the context menu of the selected task, select **Settings templates**.

   > You can create a settings template for On-Demand Scan tasks from the details pane of the **On-Demand Scan** parent node.

   The **Templates** window opens.

3. In the list of templates in the window that opens, select the template that you want to view.

4. Click the **View** button.

The **<Template name>** window opens. The **General** tab displays the template name and additional information about the template; the **Options** tab lists security settings saved in the template.

Deleting a security settings template

► *To delete a security settings template:*

1. In the Kaspersky Security Console tree, select the task for which you no longer want to use a security settings template for configuration.

2. In the context menu of the selected task, select **Settings templates**.

You can create a settings template for On-Demand Scan tasks from the details pane of the **On-Demand Scan** parent node.

The **Templates** window opens.

3. In the list of templates in the window that opens, select the template that you want to delete.
4. Click the **Remove** button.

   A window opens to confirm the deletion.
5. In the window that opens, click **Yes**.

The selected template will be deleted.

If the security settings template was applied to protect or to scan nodes of server file resources, the configured security settings for such nodes are preserved after the template is deleted.

Viewing statistics of the RPC-Network Storage Protection task

If the RPC-Network Storage Protection task is running, you can view real-time information about the number of objects processed by Kaspersky Security since the task was started up till now (i.e., task execution statistics).

► *To view statistics of the RPC-Network Storage Protection task:*

1. Expand the **Network Attached Storage Protection** node in the Kaspersky Security Console tree.
2. Select the **RPC-Network Storage Protection** subnode.
3. In the details pane, select the **Overview and management** tab.

The **Statistics** section shows a table with information about objects processed by Kaspersky Security since it was started until the current moment (see the table below).

Таблица 5. Full statistics of the RPC-Network Storage Protection task

Field	Description
Detected	Number of objects detected by Kaspersky Security. For example, if Kaspersky Security detects one software program in five files, the value in this field increases by one.
Infected and other objects detected	Number of objects that Kaspersky Security found and classified as infected or number of found legitimate software files, which were not excluded from the real-time protection and on-demand tasks scope and were classified as riskware.
Probably infected objects detected	Number of objects found by Kaspersky Security to be probably infected.
Objects not disinfected	Number of objects which Kaspersky Security did not disinfect for the following reasons: • the type of detected object cannot be disinfected; • an error occurred during disinfection.
Objects not moved to quarantine	The number of objects that Kaspersky Security attempted to quarantine but was unable to do so, for example, due to insufficient disk space.
Objects not removed	The number of objects that Kaspersky Security attempted but was unable to delete, because, for example, access to the object was blocked by another application.
Objects not scanned	The number of objects in the protection scope that Kaspersky Security failed to scan because, for example, access to the object was blocked by another application.
Objects not backed up	The number of objects the copies of which Kaspersky Security attempted to save in Backup but was unable to do so, for example, due to insufficient disk space.
Processing errors	Number of objects whose processing resulted in an error.
Objects disinfected	Number of objects disinfected by Kaspersky Security.
Moved to quarantine	Number of objects quarantined by Kaspersky Security.

Field	Description
Moved to Backup	The number of object copies that Kaspersky Security saved to Backup.
Objects removed	Number of objects deleted by Kaspersky Security.
Password-protected objects	Number of objects (archives, for example) that Kaspersky Security missed because they were password protected.
Corrupted objects	The number of objects skipped by Kaspersky Security as their format was corrupted.
Objects processed	Total number of objects processed by Kaspersky Security.

ICAP-Network Storage Protection

This section contains information about the ICAP-Network Storage Protection task, and how to connect a network attached storage to Kaspersky Security, as well as instructions on how to configure protection task settings and ICAP-network storage security settings.

In this section

About ICAP-Network Storage Protection 73

Configuring a connection between an ICAP-network storage and Kaspersky Security..... 75

Configuring the ICAP-Network Storage Protection task..... 76

Security levels in the ICAP-Network Storage Protection task..... 81

Viewing statistics of the ICAP-Network Storage Protection task 87

About ICAP-Network Storage Protection

Kaspersky Security installed on a server under Microsoft Windows protects ICAP-network storages (such as EMC Isilon) against viruses and other security threats that infiltrate the server through the exchange of files.

Kaspersky Security has no direct access to files in an ICAP-network storage (hereinafter also referred to as *network attached storage*). When an attempt is made to read or write to a file, the network attached storage generates an ICAP request to Kaspersky Security and sends the file inside this request. The application performs an anti-virus scan of this file in accordance with the settings defined in the ICAP-Network Storage Protection task. When a threat is detected, Kaspersky Security performs the actions defined in the task settings on the file, and then it sends the scan result to the network attached storage. If the Disinfect action is specified in the task settings, and the file is successfully disinfected, Kaspersky Security returns the disinfected file to the network attached storage as the response to the request.

Kaspersky Security allows you to configure the actions that the application will perform on infected and probably infected files.

When using KSN in the ICAP-Network Storage Protection task, Kaspersky Security cannot delete or block files used by an ICAP-network storage because the application has no direct access to network folders of the storage system when an untrusted verdict is received from KSN services. Information about receiving an untrusted verdict is recorded in the KSN Usage task log.

You can protect one network attached storage using one server with Kaspersky Security installed. To improve the performance of the network attached storage and the server with Kaspersky Security, you can use several servers with Kaspersky Security for protection of a single network attached storage. In this case, the network attached storage distributes the workload among associated servers on which Kaspersky Security is installed.

The ICAP-Network Storage Protection task is created by default; it is a system task of Kaspersky Security. You cannot delete or rename this task. You cannot create custom tasks for ICAP-Network Storage Protection. You can configure the ICAP-Network Storage Protection task.

You can run Network Attached Storage Protection tasks if the active key supports network attached storage protection. If you run a Network Attached Storage Protection task when the active key does not support network attached storage protection, the task returns an error. In this case, Kaspersky Security does not protect network attached storages.

The ICAP-Network Storage Protection component is available within Kaspersky Security for Storage.

For more details on solutions for protection of organizations that include Kaspersky Security for Windows Server, see the *Administrator's Guide* of *Kaspersky Security 10 for Windows Server.*

Configuring a connection between an ICAP-network storage and Kaspersky Security

You can run Network Attached Storage Protection tasks if the active key supports network attached storage protection. If you run a Network Attached Storage Protection task when the active key does not support network attached storage protection, the task returns an error. In this case, Kaspersky Security does not protect network attached storages.

To protect an ICAP-network storage, you need to configure the connection of the network attached storage to Kaspersky Security.

► *To configure a connection between a network attached storage and Kaspersky Security:*

1. Configure the following settings on the server with Kaspersky Security installed:
   - In Kaspersky Security Console, specify the settings of the connection to an ICAP-network storage to be protected by Kaspersky Security (see section "Configuring general settings of the connection to an PRC-network storage" on page 78).
   - In the local group policy editor, configure the security settings of local policies (see section "Configuring the security settings of local policies in the local group policy editor" on page 25).
   - In the Windows firewall settings window, configure the rules of outbound and inbound connections in Windows firewall (see section "Configuring inbound and outbound connections in Windows firewall" on page 26).
2. In the network attached storage, configure the following settings:
   - Enable anti-virus protection
   - Specify the address of the connection to Kaspersky Security in the network attached storage settings

   You can find information on how to configure your network attached storage in the accompanying manual.

The connection between an ICAP-network storage and Kaspersky Security is established.

Configuring the ICAP-Network Storage Protection task

By default, the ICAP-Network Storage Protection task has the settings described in the table below. You can change the values of these settings.

When the task settings are modified (for example, a different security level is specified), Kaspersky Security immediately applies the new settings in the running task. Kaspersky Security logs the date and time when task settings were modified in the system audit log.

Таблица 6. Settings of the ICAP-Network Storage Protection task

Setting	Default value	Comment
Security level.	The **Recommended** security level is applied.	You can apply one of the preset security levels to the protected network attached storage, or specify the values of the security settings manually.
Heuristic analyzer.	The **Medium** analysis level is applied.	The Heuristic Analyzer can be enabled or disabled and the analysis level configured.
Using KSN for protection	Applied.	You can enable or disable the use of KSN services for ICAP-Network Storage Protection.
Network storage connection settings	• **ICAP server port** – 1344 • **Service ID** – avscan.	You can also modify other network storage connection settings. These changes should be incorporated on the network attached storages.
Scheduled task launch.	Not applied. The **Run by schedule** check box is cleared. The task is run manually.	You can configure the task to run by schedule, for example at Kaspersky Security startup.

► *To configure settings of the ICAP-Network Storage Protection task:*

1. Expand the **Network Attached Storage Protection** node in the Kaspersky Security Console tree.
2. Select the **ICAP-Network Storage Protection** subnode.
3. In the details pane of the **ICAP-Network Storage Protection** node, click the **Properties** link.

   The **Task settings** window opens.
4. On the **General** tab in the window that opens, configure the following task settings:

   - Connection to an ICAP-network storage (see section "Configuring settings of the connection to an ICAP-network storage" on page 78).
   - Using the Heuristic Analyzer (see page 79).
   - KSN Usage for protection (see page 80).

   In the **Security level** section:

   - Select one of the preset security levels (see section "Applying a preset security level in the ICAP-Network Storage Protection systems task" on page 84) or configure the security settings of objects manually (see section "Manually configuring the security level settings in the ICAP-Network Storage Protection systems task" on page 85).
5. On the **Schedule** and **Advanced** tabs, configure the scheduled task launch settings (see section "Configuring the task launch schedule settings" on page 39).
6. Click **OK**.

Kaspersky Security immediately applies the new values of settings to the running task. Information about the date and time when the settings were modified and the values of task settings before and after modification are saved in the task log.

In this section

Configuring the settings of the connection to an ICAP-network storage 78

Using the Heuristic Analyzer 79

Using KSN for protection 80

Configuring the settings of the connection to an ICAP-network storage

► *To configure settings of the connection to an ICAP-network storage:*

1. Expand the **Network Attached Storage Protection** node in the Kaspersky Security Console tree.
2. Select the **ICAP-Network Storage Protection** subnode.
3. In the details pane of the **ICAP-Network Storage Protection** node, click the **Properties** link.

   The **Task settings** window opens.
4. On the **General** tab in the fields of the **Connection settings** section specify the following settings:

   - Number of ICAP server network port

     The number of the ICAP server network port used to connect the network attached storage to the application.

   - Service ID.

     An ID that makes part of the RESPMOD URI parameter of ICAP (see document RFC 3507). RESPMOD URI designates the address of an anti-virus ICAP server installed for the network storage area.

     For example, if the IP address of the protected server is 192.168.10.10, the port number is 1344, and the ID of ICAP service is avscan, those parameters result in the following RESPMOD URI address – `icap://192.168.10.10/avscan:1344`.
5. Click **OK**.

The newly configured settings are saved.

Once you have configured the connection settings, on the network attached storage you need to set the address of the connection to Kaspersky Security. The connection settings are included in this address. For example, if the default settings are used, the connection address looks as follows:

```
icap://<IP address of computer with Kaspersky Security installed>/avscan:1344
```

Using the Heuristic Analyzer

The ICAP-Network Storage Protection task can use the Heuristic Analyzer with a configured level of analysis.

► *To configure the settings of Heuristic Analyzer used in the ICAP-Network Storage Protection task:*

1. Expand the **Network Attached Storage Protection** node in the Kaspersky Security Console tree.

2. Select the **ICAP-Network Storage Protection** subnode.

3. In the details pane of the **ICAP-Network Storage Protection** node, click the **Properties** link.

   The **Task settings** window opens.

4. In the window that opens, go to the **General** tab and do the following in the **Heuristic Analyzer** section:

   - Clear or select the **Use Heuristic Analyzer** check box.

   - If necessary, adjust the level of analysis using the slider.

     The slider allows you to adjust the heuristic analysis level. The scanning intensity level sets the balance between the thoroughness of searches for threats, the load on the operating system's resources and the time required for scanning.

     The following scanning intensity levels are available:

     - **Light**. Heuristic analyzer performs fewer operations found inside executable files. The probability of threat detection in this mode is somewhat lower. Scanning is faster and less resource-intensive.

     - **Medium**. Heuristic Analyzer performs the number of instructions found within executable files recommended by the experts of Kaspersky Lab.

       This level is selected by default.

- **Deep**. Heuristic analyzer performs more operations found in executable files. The probability of threat detection in this mode is higher. The scan uses up more system resources, takes more time, and can cause a higher number of false alarms.

  The slider is available if the **Use Heuristic Analyzer** check box is selected.

5. Click **OK**.

The newly configured settings are applied.

Using KSN for protection

Kaspersky Security Network (KSN) is an infrastructure of online services providing access to Kaspersky Lab's online knowledge base on the reputation of files, web resources and programs.

You can enable or disable the KSN usage in the RPC-Network Storage Protection task. After you enable or disable the KSN usage, the task starts or stops showing verdicts about the reputation of files being scanned based on information received from KSN.

To start the KSN Usage task, you must accept the KSN Statement. The KSN Usage task does not start automatically at startup of Kaspersky Security by default.

> Detailed information about the KSN Usage task is provided in the *Kaspersky Security 10 for Windows Server Administrator's Guide*.

► *To enable or disable KSN usage in the ICAP-Network Storage Protection task:*

1. Expand the **Network Attached Storage Protection** node in the Kaspersky Security Console tree.
2. Select the **ICAP-Network Storage Protection** subnode.
3. In the details pane of the **ICAP-Network Storage Protection** node, click the **Properties** link.

   The **Task settings** window opens.

4. In the window that opens, go to the **General** tab and in the **KSN usage** section clear or select the **Use KSN for protection** check box.

   The check box enables or disables the use of Kaspersky Security Network (KSN) services in the ICAP-Network Storage Protection task.

   If the check box is selected, the application uses Kaspersky Security Network data to ensure a faster response time by the application to new threats and reduces the likelihood of false positives.

   If the check box is cleared, the ICAP-Network Storage Protection task does not use KSN services.

   The check box is selected by default.

5. Click **OK**.

The newly configured settings are saved.

Security levels in the ICAP-Network Storage Protection task

This section describes the security settings and provides instructions for applying preset security levels and configuring security settings manually in the ICAP: Network Attached Storage Protection

In this section

About security levels in the ICAP-Network Storage Protection task 82

Applying a preset security level in the ICAP-Network Storage Protection task..... 84

Manually configuring the security level settings in the ICAP-Network Storage Protection task .. 85

About security levels in the ICAP-Network Storage Protection task

In the ICAP-Network Storage Protection task, you can apply any of the following preset security levels to every protected storage system: **Maximum performance**, **Recommended**, or **Maximum protection**. Each of these levels contains its own pre-defined set of security settings (see the table below). You can also specify the values of the security settings manually; in this case, the security level of the network attached storage changes to **Custom**.

Maximum performance

The **Maximum performance** security level is recommended if, apart from using Kaspersky Security on servers and workstations, there are additional computer security measures on your network, for example, firewalls are set up, network users comply with existing security policies.

Recommended

The **Recommended** security level ensures an optimum combination of protection quality and degree of impact on the performance of protected servers. This level is recommended by Kaspersky Lab experts as sufficient for protection of file servers on most corporate networks. The **Recommended** security level is set by default.

Maximum Protection

The **Maximum protection** security level is recommended if you have higher requirements for computer security on your organization's network.

Таблица 7. Settings of preset security levels in the ICAP-Network Storage Protection task

Options	Security level		
	Maximum performance	Recommended	Maximum Protection
Objects protection	Objects scanned according to list of extensions specified in anti-virus database	Objects scanned by format	Objects scanned by format
Compound objects protection	Packed objects	• SFX archives • Packed objects • OLE objects	• SFX archives • Packed objects • OLE objects
Action to perform on infected objects	Block access and disinfect.	Block access and perform recommended action	Block access and disinfect.
Action to perform on probably infected objects	Block access and quarantine	Block access and perform recommended action	Block access and quarantine
Exclude files	No	No	No
Do not detect	No	No	No
Stop scanning if it takes longer than (sec.)	60	60	60
Do not scan compound objects larger than (MB)	8	8	No

Applying a preset security level in the ICAP-Network Storage Protection task

► *To apply one of the preset security levels to an ICAP-network storage:*

1. Expand the **Network Attached Storage Protection** node in the Kaspersky Security Console tree.
2. Select the **ICAP-Network Storage Protection** subnode.
3. In the details pane of the **ICAP-Network Storage Protection** node, click the **Properties** link.

   The **Task settings** window opens.
4. On the **General** tab, in the **Security level** section, select one of the following preset security levels in the list:

   - **Maximum Protection**
   - **Recommended**
   - **Maximum performance**

   The main values of the settings of the selected security level are displayed under the list.
5. Click **OK**.

The newly configured settings are saved.

You can also configure the security settings for a protected network attached storage manually (see section "Manually configuring the security level settings in the ICAP-Network Storage Protection task" on page 85).

See also

About ICAP-Network Storage Protection 73

Configuring the ICAP-Network Storage Protection task 76

Manually configuring the security level settings in the ICAP-Network Storage Protection task

► *To manually configure the security settings of an ICAP-network storage:*

1. Expand the **Network Attached Storage Protection** node in the Kaspersky Security Console tree.
2. Select the **ICAP-Network Storage Protection** subnode.
3. In the details pane of the **ICAP-Network Storage Protection** node, click the **Properties** link.

   The **Task settings** window opens.
4. On the **General** tab in the **Security level** section, click the **Settings** button.

   The **Security settings** window opens.
5. Configure the settings in accordance with your computer security requirements. To do this, perform the following actions:

   - On the **General** tab take the following actions:
     - In the **Objects protection** section, specify objects to be scanned by Kaspersky Security:
       - **All objects**.

       Kaspersky Security scans all objects.
       - **Objects scanned by format**.

       Kaspersky Security scans only infectable objects based on file format.

       Kaspersky Lab compiles the list of formats. It is included in the Kaspersky Security databases.
       - **Objects scanned according to list of extensions specified in anti-virus database**.

       Kaspersky Security scans only infectable objects based on file extension.

       Kaspersky Lab compiles the list of extensions. It is included in the Kaspersky Security databases.

- **Objects scanned by specified list of extensions**.

  Kaspersky Security scans files based on file extension. List of file extensions can be manually customized in the **List of extensions** window, which can be opened by clicking **Edit** button.

- In the **Compound objects protection** section, specify compound objects to be scanned by Kaspersky Security.

- On the **Actions** tab take the following actions:

  - In the **Action to perform on infected objects** section, select the action to be performed by Kaspersky Security on detecting an infected object.
  - In the **Action to perform on probably infected objects** section, select the action to be performed by Kaspersky Security on detecting a probably infected object.

- On the **Performance** tab take the following actions:

  - In the **Exclusions** section, specify objects that you want Kaspersky Security to exclude from scanning:
    - To exclude files from scanning, select the **Exclude files** check box and specify the names or name masks of files to be excluded.
    - To exclude detectable objects (such as remote administration utilities), select the **Do not detect** check box and specify the names or name masks of detectable objects, according to the Virus Encyclopedia classification (http://www.securelist.com).
  - In the **Advanced settings** section, specify the maximum duration of object scanning and the maximum size of the compound file being scanned.

6. Click **OK** in the **Security settings** window.

   The **Security settings** window closes.

7. Click **OK** in the **Task settings** window.

The configured custom security level settings are saved.

Viewing statistics of the ICAP-Network Storage Protection task

If the ICAP-Network Storage Protection task is running, you can view real-time information about the number of objects processed by Kaspersky Security since the task was started up till now (i.e., task execution statistics).

► *To view statistics of the ICAP-Network Storage Protection task:*

1. Expand the **Network Attached Storage Protection** node in the Kaspersky Security Console tree.

2. Select the **ICAP-Network Storage Protection** subnode.

The **Overview and management** tab of the details pane in the **Statistics** section displays a table with information about objects processed by Kaspersky Security since the task was started (see table below).

Таблица 8. Statistics of the RPC-Network Storage Protection task

Field	Description
Detected	Number of objects detected by Kaspersky Security. For example, if Kaspersky Security detects one malware program in five files, the value in this field increases by one.
Infected and other objects detected	Number of objects that Kaspersky Security found and classified as infected or number of found legitimate software files, which were not excluded from the real-time protection and on-demand tasks scope and were classified as riskware.
Probably infected objects detected	Number of objects found by Kaspersky Security to be probably infected.
Objects not disinfected	• Number of objects which Kaspersky Security did not disinfect for the following reasons: • the type of detected object cannot be disinfected; • an error occurred during disinfection.

Field	Description
Objects not moved to quarantine	The number of objects that Kaspersky Security attempted to quarantine but was unable to do so, for example, due to insufficient disk space.
Objects not removed	The number of objects that Kaspersky Security attempted but was unable to delete, because, for example, access to the object was blocked by another application.
Objects not scanned	The number of objects in the protection scope that Kaspersky Security failed to scan because, for example, access to the object was blocked by another application.
Objects not backed up	The number of objects the copies of which Kaspersky Security attempted to save in Backup but was unable to do so, for example, due to insufficient disk space.
Processing errors	Number of objects whose processing resulted in an error.
Objects disinfected	Number of objects disinfected by Kaspersky Security.
Moved to quarantine	Number of objects quarantined by Kaspersky Security.
Moved to Backup	The number of object copies that Kaspersky Security saved to Backup.
Objects removed	Number of objects deleted by Kaspersky Security.
Password-protected objects	Number of objects (archives, for example) that Kaspersky Security missed because they were password protected.
Corrupted objects	The number of objects skipped by Kaspersky Security as their format was corrupted.
Objects processed	Total number of objects processed by Kaspersky Security.

Managing Network Attached Storage Protection tasks from Kaspersky Security Center

This section provides information on how to manage Network Attached Storage Protection tasks using the Kaspersky Security Center Administration Server as well as instructions on how to configure task settings for a server group and for one server from Kaspersky Security Center.

In this section

About Network Attached Storage Protection from Kaspersky Security Center 89

Configuring Network Attached Storage Protection settings using policies 90

Configuring Network Attached Storage Protection settings for one server in Kaspersky Security Center 92

About Network Attached Storage Protection from Kaspersky Security Center

You can manage Network Attached Storage Protection tasks from Kaspersky Security Center in the following ways:

- **Using Kaspersky Security Center policies**. You can configure common Network Attached Storage Protection settings and apply them to tasks for the selected server group.
- **In the Application settings window**. You can configure Network Attached Storage Protection settings separately for each server where Kaspersky Security is installed.

Configuring Network Attached Storage Protection settings using policies

By default, Network Attached Storage Protection tasks in the Kaspersky Security Center policy have the settings described in the table below. You can change the values of these settings.

Таблица 9. Network Attached Storage Protection tasks settings in the Kaspersky Security Center policies

Network Attached Storage Protection task	Options
RPC-Network Storage Protection	In the RPC-Network Storage Protection task, click the **Settings** button to configure the following task run settings: • Specify the protection scope • Set the security level for the selected protection scope: you can select a predefined security level or configure the security settings manually • Configure the use of Heuristic Analyzer • Configure usage of the Trusted zone and KSN • Configure the network attached storage connection settings • Configure the task run settings
ICAP-Network Storage Protection	In the ICAP-Network Storage Protection task, click the **Settings** button to configure the following task run settings: • Configure the use of Heuristic Analyzer • Configure the network attached storage connection settings • Set the security level for the selected protection scope: you can select a predefined security level or configure the security settings manually • Configure the use of KSN • Configure the task run settings

► *To configure settings of the Network Attached Storage Protection task in the Kaspersky Security Center policy:*

1. Expand the **Managed computers** node in the Administration console tree, then expand the administration group, for which you want to configure the associated policy settings, and open the **Policies** subnode in the details pane.

2. In the context menu of the policy whose settings you want to configure, select **Properties** and in the window that opens select **Network Attached Storage Protection** in the list of sections.

3. In the window that opens, perform the following operations:

   - To configure settings of the RPC-Network Storage Protection task, in the **RPC-Network Storage Protection** section click the **Settings** button.

     In the **Options** window that opens, configure the task settings according to your requirements (see section "Configuring the RPC-Network Storage Protection task" on page 53). Click **OK** to save changes made to the settings in the policy.

   - To configure settings of the ICAP-Network Storage Protection task, in the **ICAP-Network Storage Protection** section click the **Settings** button.

     In the **Options** window that opens, configure the task settings according to your requirements (see section "Configuring the RPC-Network Storage Protection task" on page 53). Click **OK** to save changes made to the settings in the policy.

4. In the **Properties: <Policy name>** window, click **OK**.

The configured settings of the Network Attached Storage Protection tasks are saved and applied to the active policy.

Detailed information about the operation of Kaspersky Security with Kaspersky Security Center policies and information about Kaspersky Security Center policies is provided in the *Kaspersky Security Center Administrator's Guide* and *Kaspersky Security 10 for Windows Server Administrator's Guide*.

Configuring Network Attached Storage Protection settings for one server in Kaspersky Security Center

► *To configure Network Attached Storage Protection settings for one server in Kaspersky Security Center:*

1. Expand the **Managed Computers** node in the Administration Console tree and select the group that the protected server belongs to.
2. In the details pane, on the **Computers** tab open the context menu on the line with information about the protected server and select **Properties**.
3. In the **Properties: <Computer name>** window of the **Tasks** section, open the context menu of the Network Attached Storage Protection task that you want to configure and select the **Properties** item.
4. In the window that opens, configure the settings of the Network Attached Storage Protection task according to your requirements:
   - RPC-Network Storage Protection (see section "Configuring the RPC-Network Storage Protection task" on page 53).
   - ICAP-Network Storage Protection (see section "Configuring the ICAP-Network Storage Protection task" on page 76).
5. Click **OK**.

The configured task settings are saved and applied to the running task for one server.

If an application is covered by a Kaspersky Security Center policy and this policy prohibits changing the task settings, these settings cannot be edited via the **Properties: <Computer name>** window.

Detailed information about the operation of Kaspersky Security with Kaspersky Security Center policies and information about Kaspersky Security Center policies is provided in the *Kaspersky Security Center Administrator's Guide* and *Kaspersky Security 10 Administrator's Guide*.

Contacting Technical Support

This section describes the ways to receive technical support and the conditions on which it is available.

In this section

How to get Technical support 93

Technical Support via Kaspersky CompanyAccount 94

Technical support by phone..... 95

Using trace files and AVZ scripts 95

How to get 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 Technical Support. Technical Support specialists will answer your questions about installing and using the application.

Technical support is available only to users who have purchased a commercial license for the application. Technical support is not available to users who have a trial license.

Before contacting Technical Support, please read through the Technical Support rules (http://support.kaspersky.com/support/rules).

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

- By calling Technical Support (http://support.kaspersky.com/support/contacts);
- By sending a request to Technical Support through the Kaspersky CompanyAccount portal (https://companyaccount.kaspersky.com).

Technical Support via Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) is a portal for companies that use Kaspersky Lab applications. Kaspersky CompanyAccount is designed to facilitate interaction between users and Kaspersky Lab specialists via online requests. Kaspersky CompanyAccount lets you 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 user account on Kaspersky CompanyAccount. A single user account gives you centralized management of online requests from these employees to Kaspersky Lab, as well as control over the rights of these employees in your Kaspersky CompanyAccount.

Kaspersky CompanyAccount is available in the following languages:

- English
- Spanish
- Italian
- German
- Polish
- Portuguese
- Russian
- French
- Japanese

To learn more about Kaspersky CompanyAccount, visit the Technical Support website (http://support.kaspersky.com/faq/companyaccount_help).

Technical support by phone

In most regions worldwide, you can contact Technical Support by phone. Information about how to contact Technical Support in your region is available on the Kaspersky Lab Technical Support website (http://support.kaspersky.com/support/contacts).

Before contacting Technical Support, please read through the Technical Support rules (http://support.kaspersky.com/support/rules).

Using trace files and AVZ scripts

After you report a problem to Technical Support specialists, they may ask you to generate a report with information about the operation of Kaspersky Security and to send it to Technical Support. Technical Support specialists may also ask you to generate a *trace file*. The trace file allows following the process of how application commands are performed, step by step, in order to determine the stage of application operation at which an error occurs.

After Technical Support Service specialists analyze the data that you have sent, they can create an AVZ script and send it to you. With AVZ scripts, it is possible to analyze active processes for threats, scan the computer for threats, disinfect or delete infected files, and create system scan reports.

Glossary

A

Anti-virus databases

Databases that contain information about computer security threats known to Kaspersky Lab as of the anti-virus database release date. Anti-virus database signatures help to detect malicious code in scanned objects. Anti-virus databases are created by Kaspersky Lab specialists and updated hourly.

Application settings

Application settings that are common to all types of tasks and determine how the application operates in general. For example, performance, reports, and Backup settings.

Archive

A file that contains inside itself one or several other files, which, in their turn, may also be archives.

B

Backup

A dedicated storage area intended for storing backup copies of files that have been created before their first disinfection or deletion.

D

Disinfection of objects

A method of processing infected objects that results in a complete or partial recovery of data. Not every infected object can be disinfected.

F

False alarm

A situation when a non-infected object is identified by a Kaspersky Lab application as infected because its code is similar to that of a virus.

File mask

Representation of the name and extension of a file by means of wildcards.

To create a file mask, you can use any symbols that are allowed to use in file names, including special ones:

- ***** – the symbol that substitutes zero or more characters
- **?** – the symbol that substitutes any single character

Please note that the name and the extension of a file are always separated with a dot.

H

Heuristic analysis

A technology intended for detection of threats that cannot be detected using current version of Kaspersky Lab applications databases. It allows finding files that may contain some unknown virus or a new modification of a known virus.

Files in which malicious code is detected during heuristic analysis are marked as *probably infected*.

Heuristic Analyzer

A module of Kaspersky Security that performs heuristic analysis.

I

Infected file

A file that contains malicious code (i.e., when scanning the file, code of a known application that poses a threat has been detected). Kaspersky Lab specialists recommend that you abstain from handling such files since this may lead to an infection of your computer.

O

OLE object

A file that has been merged or integrated into another one. Kaspersky Lab applications allow scanning OLE objects for viruses. For example, if you embed a Microsoft Office Excel® spreadsheet into a Microsoft Office Word document, the former will be scanned as OLE object.

P

Potentially infectable file

A file with a specific structure or format that may be used by criminals to convert this file into a container for storing and spreading malicious code. As a rule, they include executable files, for example, those with com, exe, dll, and other similar extensions. The risk of malicious code penetration into such files is rather high.

Probably infected file

A file that contains either modified code of a known virus, or code that is similar to one but still unknown to Kaspersky Lab. Probably infected files can be detected by the means of the heuristic analyzer.

Q

Quarantine

A dedicated storage area intended for storing backup copies of objects that have been created before their first disinfection or deletion. The Kaspersky Lab application also moves to Quarantine probably infected objects that have been detected. Objects are stored in Quarantine in encrypted form in order to avoid affecting the computer.

S

Signature analysis

Threat detection technology , which uses Kaspersky Security databases that contain the descriptions of known threats and the methods of neutralizing them. Protection with signature analysis ensures the minimum admissible security level. According to recommendations of Kaspersky Lab specialists, this analysis method is always enabled.

Startup objects

A set of applications that are required for start and proper operation of the operating system and software installed on the computer. Every time the operating system boots, it runs those objects. There are viruses aimed at infecting such objects, which may result, for example, in blocked booting of the operating system.

T

Task

Functions performed by the Kaspersky Lab application as tasks, for example: Real-Time File Protection, Full scan, Application databases update.

Task settings

Settings of the application that are specific for each task type.

V

Vulnerability

A flaw in the operating system or in an application that may be exploited by malicious programs in order to intrude into the operating system or application and corrupt its integrity. A large number of vulnerabilities in the operating system makes its operation unreliable, because viruses that have intruded into the operating system may provoke failures in the system's operation or errors in the operation of installed applications.

AO Kaspersky Lab

Kaspersky Lab is a world-renowned vendor of systems for protection of computers against various threats, including viruses and other malware, spam, network and hacking 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 is now employing more than 3,000 skilled professionals.

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

The personal product range includes information security applications for desktop, laptop, and tablet computers, and 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 products are certified by major testing laboratories, compatible with the applications of most software vendors, and optimized for work on most hardware platforms.

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

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

ACHIEVEMENTS. Over the years, Kaspersky Lab has won hundreds of awards for its services in combating computer threats. For example, in 2014, tests and researches conducted by the renowned Austrian anti-virus lab AV-Comparatives brought Kaspersky Lab one of the two leading positions in the number of Advanced+ certificates awarded, which gave 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 website:	http://www.kaspersky.com
Virus Encyclopedia	http://www.securelist.com
Virus Lab:	http://newvirus.kaspersky.com (for scanning suspicious files and websites)
Kaspersky Lab web forum:	http://www.kaspersky.com

Information about third-party code

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

Trademark notices

Registered trademarks and service marks are the property of their respective owners.

Citrix, XenApp, and XenDesktop are registered trademarks of Citrix Systems, Inc. and/or subsidiaries in the United States and/or elsewhere.

Dell, Dell Compellent - are registered trademarks of Dell, Inc.

Celerra, EMC, Isilon, OneFS, and VNX are either registered trademarks or trademarks of EMC Corporation in the United States and/or elsewhere.

Hitachi - is a registered trademark of Hitachi, Ltd.

IBM and System Storage are trademarks of International Business Machines Corporation registered all over the world.

Excel, Hyper-V, Microsoft, Windows, Windows Server, and Windows Vista are trademarks of Microsoft Corporation registered in the United States and/or elsewhere.

Data ONTAP and NetApp are either registered trademarks or trademarks of NetApp, Inc. in the United States and/or elsewhere.

Oracle – is registered trademark of Oracle and/or its affiliates.

Index

A

AVZ script 95

D

Databases

automatic update 39

L

Launching missed tasks 39

M

MMC 29

T

Tasks schedule 39, 41

Tracing

trace file 95

U

Update

by schedule 39