Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition

Implementation Guide for Network Storage Protection

APPLICATION VERSION: 8.0 SERVICE PACK 2

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.

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

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

This document and the graphics associated with it may be used exclusively for information, non-commercial or personal purposes.

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.

Kaspersky Lab assumes no liability for the content, quality, relevance or accuracy of any materials used in this document the rights to which are held by third parties, or for potential damages associated with the usage of such documents.

Revision date: 2/28/2015

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

TABLE OF CONTENTS

ABOUT THIS GUIDE

The Implementation Guide for Kaspersky Anti-Virus 8.0 for Windows Servers® Enterprise Edition (further referred to as "Kaspersky Anti-Virus") is intended for those who install and administer Kaspersky Anti-Virus, as well as for those who provide technical support to organizations that use Kaspersky Anti-Virus.

In this Guide you can find information about configuring and using Kaspersky Anti-Virus for network 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 assumed that together with this guide you have available an instance of the application with the RPC: Network storage protection and ICAP: Network storage protection components installed (see *Installation Guide for Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition*) and a key with support for network storage protection added to the application (licensing information is provided in the *Administrator's Guide for Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition*).

IN THIS SECTION

IN THIS DOCUMENT

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

Sources of information about Kaspersky Anti-Virus

This section lists the sources of information about the application.

Kaspersky Anti-Virus

This section describes the features, components, and distribution kit of Kaspersky Anti-Virus.

Hardware and software requirements

This section lists the hardware and software requirements of Kaspersky Anti-Virus.

Application architecture

This section describes the principles of concurrent operation of Kaspersky Anti-Virus and network storage systems.

Managing Kaspersky Anti-Virus Console

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

Viewing network storage protection status

This section provides instructions on how to view information about the current status of network storage protection.

EMC Celerra network storage protection

This section provides information about the protection of EMC Celerra network storage systems and integration of Kaspersky Anti-Virus with EMC Celerra systems.

Protecting RPC-pluggable network storage systems

This section provides information about the task for protection of network storage systems connected via RPC, about the setup of connection between a network storage system and Kaspersky Anti-Virus, as well as instructions on how to configure a protection task and define the security settings for RPC-connected network storage systems.

Protecting ICAP-pluggable network storage systems

This section provides information about the task for protection of network storage systems connected via ICAP, about the setup of connection between a network storage system and Kaspersky Anti-Virus, as well as instructions on how to configure a protection task and define the security settings for ICAP-connected network storage systems.

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.

Kaspersky Lab ZAO

This section provides information about Kaspersky Lab ZAO.

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).

Table 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 yellow background under the heading "Example".
Update means... The *Databases are out of date* event occurs.	The following elements are italicized in the text: • New terms • Names of application statuses and events
Press **ENTER**. Press **ALT**+**F4**.	Names of keyboard keys appear in bold and are capitalized. Names of keys that are connected by a + (plus) sign indicate the use of a key combination. 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 ANTI-VIRUS

This section lists the sources of information about the application. You can select the most suitable information source, depending on the level of importance and urgency of the issue.

IN THIS SECTION

SOURCES FOR INDEPENDENT RETRIEVAL OF INFORMATION

You can use the following sources to find information about Kaspersky Anti-Virus:

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

If you cannot find a solution for your issue on your own, we recommend contacting Kaspersky Lab Technical Support.

An Internet connection is required to use online information sources.

Kaspersky Anti-Virus page on the Kaspersky Lab website

On the Kaspersky Anti-Virus page (http://www.kaspersky.com/business-security/windows-server-antivirus-enterprise-edition), you can view general information about the application, its functions and features.

The Kaspersky Anti-Virus page contains a link to eStore. There you can purchase the application or renew your license.

Kaspersky Anti-Virus page in the Knowledge Base

Knowledge Base is a section on the Technical Support website.

The Kaspersky Anti-Virus page in the Knowledge Base (http://support.kaspersky.com/wsee8) 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 Anti-Virus but also to other Kaspersky Lab applications. Knowledge Base articles can also include Technical Support news.

The deployment guide describes common ways to deploy Kaspersky Anti-Virus on a corporate network.

The installation guide describes how you can perform the following tasks:

- Prepare Kaspersky Anti-Virus for installation, install and activate the application
- Prepare Kaspersky Anti-Virus for operation
- Restore or remove Kaspersky Anti-Virus

The administrator's guide provides information about how to configure and use Kaspersky Anti-Virus.

In the Implementation Guide for Network Storage Protection you can find information about configuring and using Kaspersky Anti-Virus for network 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 ANTI-VIRUS

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

Kaspersky Anti-Virus can be installed on servers in the following roles:

- Terminal servers
- Print servers
- Application servers
- Domain controllers
- Network storage servers
- File servers – these servers are more likely to get infected because they exchange files with user workstations.

Kaspersky Anti-Virus can be managed in the following ways:

- Via Kaspersky Anti-Virus Console installed on the same server with Kaspersky Anti-Virus 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 Anti-Virus.

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

Kaspersky Anti-Virus components and features

The application includes the following components:

- Real-time protection of files

  Kaspersky Anti-Virus scans objects when they are accessed. Kaspersky Anti-Virus scans the following objects:

  - files;
  - alternate file system threads (NTFS threads);
  - master boot record and boot sectors on the local hard drives and removable media.

- Script scanning

  Kaspersky Anti-Virus controls the execution of scripts created using Microsoft Windows Script Technologies (or Active Scripting), for example, VBScript or JScript®. Kaspersky Anti-Virus allows script execution only if this script has been found to be safe. Kaspersky Anti-Virus blocks the execution of a script that has been found to be dangerous. If Kaspersky Anti-Virus finds a script to be potentially dangerous, it performs the action you have specified: blocks or allows script execution.

- Network storage protection

  Kaspersky Anti-Virus installed on a server under a Microsoft Windows operating system protects network storage systems against viruses and other security threats that infiltrate the server through the exchange of files.

- On-demand scan

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

The following functions are implemented in the application:

- Updating databases and application software modules

  Kaspersky Anti-Virus 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 Anti-Virus quarantines probably infected objects by moving such objects from their original location to the *Quarantine storage*. Objects are stored in the Quarantine storage in encrypted form for security considerations.

- Backup

  Kaspersky Anti-Virus 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 Anti-Virus operation and the status of Anti-Virus protection on the server.

- Importing and exporting settings

  You can export Kaspersky Anti-Virus settings to an XML configuration file and import settings into Kaspersky Anti-Virus from the configuration file. All Kaspersky Anti-Virus settings or settings for individual Kaspersky Anti-Virus components can be saved in the configuration file.

HARDWARE AND SOFTWARE REQUIREMENTS

This section lists the hardware and software requirements of Kaspersky Anti-Virus.

IN THIS SECTION

REQUIREMENTS FOR THE SERVER ON WHICH KASPERSKY ANTI-VIRUS IS DEPLOYED

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

Kaspersky Anti-Virus can be installed without prior removal of Kaspersky Anti-Virus 8.0 for Windows Servers® Enterprise Edition or Kaspersky Anti-Virus 6.0 / 8.0 for Windows Servers.

Hardware requirements for the server

General requirements:

- x86-compatible uniprocessor or multiprocessor systems; x86-64-compatible uniprocessor or multiprocessor 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).
    - for storing databases: 2 GB (recommended)

Minimum configuration:

- processor – 1 Intel® Core™ 1.4 GHz
- RAM: 1 GB
- drive subsystem – 4 GB of free space

Recommended configuration:

- CPU: 4 Intel Core 2.4 GHz
- RAM: 2 GB
- drive subsystem – 4 GB of free space

Software requirements for the server

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

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

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

- Windows Server 2003 Standard / Enterprise SP2
- Windows Server 2003 R2 Standard / Enterprise SP2
- Windows Server 2008 Standard / Enterprise / Datacenter SP1 or later
- Windows Server 2008 Core Standard / Enterprise / Datacenter SP1 or later.

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

- Windows Server 2003 Standard / Enterprise SP2
- Windows Server 2003 R2 Standard / Enterprise SP2
- 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 Anti-Virus on the following terminal servers:

- Microsoft Terminal Services based on Windows 2003 Server;
- 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 Presentation Server™ 4.0, 4.5

- Citrix® XenApp® 4.5, 5.0, 6.0, 6.5
- Citrix XenDesktop® 7.0, 7.1, 7.5.

REQUIREMENTS FOR THE PROTECTED NETWORK STORAGE

Kaspersky Anti-Virus can be used to protect the following network 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:
  - operating system EMC DART 6.0.36 or higher;
  - Celerra Anti-Virus Agent (CAVA) 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.

REQUIREMENTS FOR THE COMPUTER ON WHICH KASPERSKY ANTI-VIRUS IS DEPLOYED

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 Anti-Virus 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 Anti-Virus Console.

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

- Windows Server 2003 Standard / Enterprise SP2
- Windows Server 2003 R2 Standard / Enterprise SP2
- 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.

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

- Windows Server 2003 Standard / Enterprise SP2
- Windows Server 2003 R2 Standard / Enterprise SP2
- 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.

INTEGRATING KASPERSKY ANTI-VIRUS WITH NETWORK STORAGE SYSTEMS

This section provides information about the principles of concurrent operation of Kaspersky Anti-Virus and network storage systems.

EMC Celerra network storage protection

Kaspersky Anti-Virus interacts with EMC Celerra network storage systems by means of a software agent named CAVA (Celerra Antivirus Agent), which runs on computers with Kaspersky Anti-Virus installed. When running, Kaspersky Anti-Virus scans the computer for installed CAVA, which must meet the respective requirements (see the section "Requirements to a protected network storage system" on page 14) of Kaspersky Anti-Virus.

When an attempt is made to read or modify a file that is located in the network storage system, the latter initiates a network request and sends that file to CAVA. Then, CAVA saves the received file to the computer's local drive, moving it to 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, e.g., disinfects or deletes the file. CAVA analyzes the activity of Kaspersky Anti-Virus and uses this information to create the scan results and then send them to the network storage system.

Protection of an RPC-connected network storage system

Interaction of Kaspersky Anti-Virus and an RPC-connected network storage system (such as NetApp or Hitachi NAS in RPC mode) involves RPC (Remote Procedure Call) protocol.

Kaspersky Anti-Virus maintains a stable connection with the network storage system and initiates RPC requests to it periodically. When an attempt is made to read or create / modify a file located in the network storage system, the latter provides Kaspersky Anti-Virus with direct access to that file over CIFS protocol. The application's RPC: Network storage protection component scans the file in accordance with the settings defined in the RPC: Network storage protection task. If a threat is detected, Kaspersky Anti-Virus performs on the file the actions that have been defined in the task settings (including disinfection or deletion of that file); then the application sends the scan results to the network storage system.

Protection of an ICAP-connected network storage system

When handling an ICAP-connected network storage system (such as EMC Isilon, IBM NAS, or Hitachi NAS in ICAP mode), Kaspersky Anti-Virus operates as an ICAP-based service.

When an attempt is made to read or create / modify a file located in the network storage system, the latter generates an ICAP request to Kaspersky Anti-Virus and sends the file with that request. The application's ICAP: Network storage protection component scans the file in accordance with the settings defined in the ICAP: Network storage protection task. If a threat is detected, Kaspersky Anti-Virus performs on the file the actions that have been defined in the task settings and then returns the scan results to the network storage system. If the Disinfect action has been defined in the settings, and the file is successfully disinfected, Kaspersky Anti-Virus returns that disinfected file to the network storage system as the response to the request.

MANAGING KASPERSKY ANTI-VIRUS CONSOLE

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

IN THIS SECTION

ABOUT KASPERSKY ANTI-VIRUS CONSOLE

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

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

For detailed information about how to install and configure Kaspersky Anti-Virus Console please refer to the *Installation Guide for Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition.*

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

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

You can start Kaspersky Anti-Virus Console from the **Start** menu. In addition, you can run the msc file of the Kaspersky Anti-Virus snap-in or add the Kaspersky Anti-Virus snap-in to the existing Microsoft Management Console as a new element in its tree (see section "Kaspersky Anti-Virus Console window interface" on page 18).

Under a 64-bit version of Microsoft Windows, the Kaspersky Anti-Virus snap-in can be added only to 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 Anti-Virus snap-ins can be added to a single Microsoft Management Console opened in the authorizing mode, in order to use it to administer the protection of multiple servers on which Kaspersky Anti-Virus is installed.

STARTING KASPERSKY ANTI-VIRUS CONSOLE FROM THE START MENU

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

Make sure that Kaspersky Anti-Virus Console is installed on the computer.

➧ *To start Kaspersky Anti-Virus Console from the Start menu:*

select **Start** → **Programs** → **Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition** → **Administration tools** → **Kaspersky Anti-Virus Console**.

- To add other snap-ins to Kaspersky Anti-Virus Console, open the Console in author mode. To do this, select **Start** → **Programs** → **Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition** → **Administration tools**. Open the context menu of **Kaspersky Anti-Virus Console** and select the **Author** command.

- If Kaspersky Anti-Virus Console has been started on the protected server, the Console window opens (see section "Kaspersky Anti-Virus Console window interface" on page 18).

- If you have started Kaspersky Anti-Virus Console not on a protected server but on a different computer, connect to the protected server. To do so, in the console tree open the context menu of the Kaspersky Anti-Virus node and select the **Connect to another computer** command. In the **Select computer** window that opens, select **Another computer** and type the network name of the protected server in the entry field.

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

KASPERSKY ANTI-VIRUS CONSOLE WINDOW INTERFACE

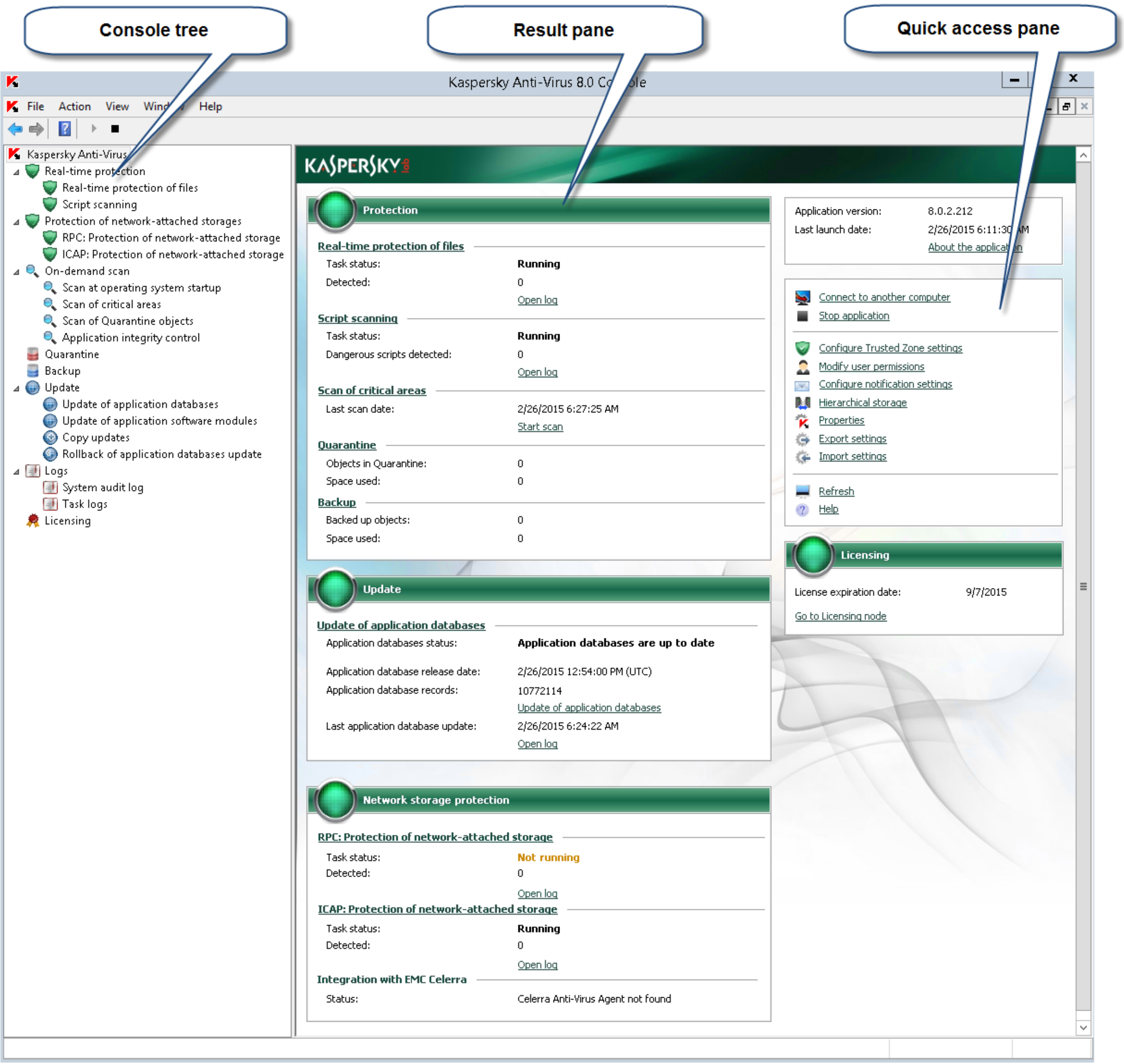
Kaspersky Anti-Virus Console is displayed in the MMC console tree as a node named **Kaspersky Anti-Virus**.

After a connection has been established to Kaspersky Anti-Virus installed on a different computer, the name of the node is supplemented with the name of the computer on which Kaspersky Anti-Virus is installed and the name of the account under which the connection has been established: **Kaspersky Anti-Virus <Computer name> as <user account name>**. The name of the node does not change after the connection has been established to Kaspersky Anti-Virus installed on the same computer with Kaspersky Anti-Virus Console.

By default, the Kaspersky Anti-Virus 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 Anti-Virus Console window.


Console tree
Result pane
Quick access pane
Kaspersky Anti-Virus 8.0 Console
File
Action
View
Window
Help
Kaspersky Anti-Virus
Real-time protection
Real-time protection of files
Script scanning
Protection of network-attached storages
RPC: Protection of network-attached storage
ICAP: Protection of network-attached storage
On-demand scan
Scan at operating system startup
Scan of critical areas
Scan of Quarantine objects
Application integrity control
Quarantine
Backup
Update
Update of application databases
Update of application software modules
Copy updates
Rollback of application databases update
Logs
System audit log
Task logs
Licensing
KASPERSKY
Protection
Update
Network storage protection
Licensing
Connect to another computer
Stop application
Configure Trusted Zone settings
Modify user permissions
Configure notification settings
Hierarchical storage
Properties
Export settings
Import settings
Refresh
Help

Real-time protection of files
Task status: **Running**
Detected: 0
Open log

Script scanning
Task status: **Running**
Dangerous scripts detected: 0
Open log

Scan of critical areas
Last scan date: 2/26/2015 6:27:25 AM
Start scan

Quarantine
Objects in Quarantine: 0
Space used: 0

Backup
Backed up objects: 0
Space used: 0

Update of application databases
Application databases status: **Application databases are up to date**
Application database release date: 2/26/2015 12:54:00 PM (UTC)
Application database records: 10772114
Update of application databases
Last application database update: 2/26/2015 6:24:22 AM
Open log

RPC: Protection of network-attached storage
Task status: **Not running**
Detected: 0
Open log

ICAP: Protection of network-attached storage
Task status: **Running**
Detected: 0
Open log

Integration with EMC Celerra
Status: Celerra Anti-Virus Agent not found

Application version: 8.0.2.212
Last launch date: 2/26/2015 6:11:30 AM
About the application

License expiration date: 9/7/2015
Go to Licensing node

Figure 1: The Kaspersky Anti-Virus Console main window.

Taskpad

The console tree displays the Kaspersky Anti-Virus node and the nested nodes of functional components of the application.

The **Kaspersky Anti-Virus** nodes includes the following nested nodes:

- **Real-time protection**: manage real-time protection of files and script scanning. There is a separate node for each component:
  - **Real-time file protection**.
  - **Script scanning**.
- **Network storage protection**: manage network storage protection.

  - **RPC: Network storage protection** task.
  - **ICAP: Network storage protection** task.
- **On-demand scan**: manage on-demand scan tasks. There is a separate node for each system task:
  - **Scan at operating system startup**.
  - **Scan of critical areas**.
  - **Scan of Quarantine objects**.
  - **Application integrity check**.

  A separate node is created for each user-defined task and for each group task created and sent to the server by Kaspersky Security Center.
- **Quarantine**: manage Quarantine settings and quarantined objects. The node contains a list of quarantined objects.
- **Backup**: manages Backup settings and handles objects in Backup. The node contains a list of backup copies.
- **Update**: manages updates for Kaspersky Anti-Virus databases and modules and copying updates to a local update source folder. The node contains subnodes for administering each system update task and last application database update rollback task:
  - **Update of application databases**.
  - **Update of application software modules**.
  - **Copy updates**.
  - **Database update rollback**.

  A separate node is created for each task created and sent to the server by Kaspersky Security Center.
- **Logs**: manage logs of real-time protection, network storage protection, on-demand scan, and update tasks; manage the Kaspersky Anti-Virus audit log.
- **Licensing**: add or delete Kaspersky Anti-Virus keys, view license details.

Details pane

The results pane displays information about the selected node. If the Kaspersky Anti-Virus node is selected, the results pane displays information about the current protection status of the server, information about Kaspersky Anti-Virus, and the status of its components.

Quick access bar and context menu for the Kaspersky Anti-Virus node

Using links on the quick access bar and context menu items of the **Kaspersky Anti-Virus** node, you can perform the following operations:

- **Connect to another computer** – connects to another server to manage Kaspersky Anti-Virus installed on it.
- **Start the application / stop the application** – start or stop Kaspersky Anti-Virus. To carry out these operations, you can also use the buttons on the toolbar.
- **Configure trusted zone settings** – specify trusted processes and exclusion rules. You can also specify tasks that use each trusted zone setting.

- **Modify user permissions** – modify permissions that let users or user groups access Kaspersky Anti-Virus functions.
- **Configure notification settings** – configure user and administrator notifications about Anti-Virus events.
- **Hierarchical storage** - configure Tiered storage settings.
- **Export settings** – save application settings to an XML configuration file.
- **Import settings** – restore application settings from an XML configuration file.
- **About the application** – view information about the application: number of the installed application version, details of installed updates. You can also go to the website of Kaspersky Lab and the website of Technical Support and read the End User License Agreement.
- **Properties** - view and configure general Kaspersky Anti-Virus settings.

VIEWING NETWORK STORAGE PROTECTION STATUS

➡ *To view information about network storage protection status,*

select the Kaspersky Anti-Virus node in the console tree.

By default, information in the details pane of Kaspersky Anti-Virus is refreshed automatically every minute. You can refresh information manually.

➡ *To refresh information in the Kaspersky Anti-Virus node manually,*

select the **Refresh** command in the context menu of the Kaspersky Anti-Virus node.

The details pane of Kaspersky Anti-Virus Console displays information about the status of server protection, protected network storages, and information about Kaspersky Anti-Virus.

The lower part of the details panel contains the **Network storage protection** section with information about the status of network storages. The **Network storage protection** section (see table below) is displayed if the active key supports the network storage protection feature (see the *Administrator's Guide for Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition* for detailed information about keys).

Table 2. Information about network storage protection

NETWORK STORAGE PROTECTION SECTION	**INFORMATION**
Network storage protection status indicator	The indicator may appear as follows: 🟢 – in the following cases: • at least one of the following tasks is running: **RPC: Network storage protection** or **ICAP: Network storage protection**; • – Kaspersky Anti-Virus has established connection to EMC software, and the Real-time file protection task is running in Kaspersky Anti-Virus. 🟡 – all other cases.
Status of integration with EMC Celerra	It can take the following values: • **Celerra Anti-Virus Agent not found** – Kaspersky Anti-Virus cannot find any EMC software, or an error has occurred in the integration code. • **Protection disabled** – Kaspersky Anti-Virus has established a connection to EMC software, but the Real-time protection of files task is not running in Kaspersky Anti-Virus. • **Protection enabled** – Kaspersky Anti-Virus has established a connection to EMC software, and the Real-time file protection task is running in Kaspersky Anti-Virus.

EMC CELERRA NETWORK STORAGE PROTECTION

This section provides information about the protection of EMC Celerra network storage systems and integration of Kaspersky Anti-Virus with EMC Celerra systems.

IN THIS SECTION

ABOUT PROTECTING EMC CELERRA NETWORK STORAGE SYSTEMS

Kaspersky Anti-Virus installed on a server under a Microsoft Windows operating system protects EMC Celerra network storage systems against viruses and other security threats that infiltrate the server through the exchange of files.

Kaspersky Anti-Virus scans files located in network share folders in the EMC Celerra network storage system when an attempt is made to read or modify those files from a workstation. The network storage system allows reading or modifying a file if Kaspersky Anti-Virus has identified that file as safe. If Kaspersky Anti-Virus has identified a file as infected or probably infected, the network storage system blocks that file from being read or modified.

Kaspersky Anti-Virus allows you to configure actions that the application will perform on infected and probably infected files. By default, Kaspersky Anti-Virus attempts to disinfect infected files and moves probably infected files to Quarantine. Before disinfecting a file, Kaspersky Anti-Virus places a copy of the file in backup storage.

To protect an EMC Celerra network storage system, you must integrate it with Kaspersky Anti-Virus.

Actions to protect the EMC Celerra network storage system are performed by the Real-time file protection task. For detailed information about how to configure the Real-time file protection task please refer to the *Administrator's Guide for Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition*.

INTEGRATING KASPERSKY ANTI-VIRUS WITH AN EMC CELERRA NETWORK STORAGE

To integrate Kaspersky Anti-Virus with an EMC Celerra network storage system:

1. Install a software agent named Celerra Antivirus Agent (CAVA) on a computer with Kaspersky Anti-Virus installed. CAVA is part of the EMC Celerra software suite. Kaspersky Anti-Virus interacts with the EMC Celerra network storage system through this software agent.

2. Run the Real-time file protection task if it has been stopped. The task is started by default.

The status of integration of Kaspersky Anti-Virus with the EMC Celerra network storage system is displayed (see the section "Viewing the protection status of network storage systems" on page 22) in the details pane of the **Kaspersky Anti-Virus** node.

PROTECTING RPC-PLUGGABLE NETWORK STORAGE SYSTEMS

This section provides information about the task for protection of network storage systems connected via RPC, about the setup of connection between a network storage system and Kaspersky Anti-Virus, as well as instructions on how to configure a protection task and define the security settings for RPC-connected network storage systems.

IN THIS SECTION

ABOUT PROTECTING RPC-PLUGGABLE NETWORK STORAGE SYSTEMS

Kaspersky Anti-Virus installed on a server under a Microsoft Windows operating system protects RPC-pluggable network storage systems (such as NetApp) against viruses and other security threats that infiltrate the server through the exchange of files.

Kaspersky Anti-Virus scans files located in network share folders in the RPC-pluggable network storage system (hereinafter also *network storage system*) when an attempt is made to read or modify the files from a workstation. The network storage system allows reading or modifying a file if Kaspersky Anti-Virus has identified that file as safe. If Kaspersky Anti-Virus has identified a file as infected or probably infected, the network storage system blocks that file from being read or modified. Kaspersky Anti-Virus lets you configure actions that the application takes on infected and probably infected files. By default Kaspersky Anti-Virus disinfects infected files, and if disinfection is not possible it deletes them; probably infected files are placed in quarantine. Before disinfecting or deleting a file, Kaspersky Anti-Virus places a copy of the file in backup storage..

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

To ensure real-time protection of a network storage system, add it to Kaspersky Anti-Virus as part of the protection scope and then configure a connection between the network storage system and the server with Kaspersky Anti-Virus installed on it. Kaspersky Anti-Virus provides an RPC-pluggable network storage protection task called **RPC: Network storage protection** task.

You can run network storage protection tasks if the active key supports network storage protection. If you run a network storage protection task when the active key does not support network storage protection, the task returns an error. In this case, the network storage systems are not protected by Kaspersky Anti-Virus.

The **RPC: Network protection task** is created by default. You cannot delete or rename this task. Nor can you create another RPC-pluggable network storage protection task. You can configure the properties of the **RPC: Network storage protection** task. The settings configured in the properties of the **RPC: Network storage protection** task are applied to all protection scopes added. You can also configure the security settings of each protection area.

ABOUT SCANNING SYMBOLIC LINKS. NETAPP STORAGE SYSTEM

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 storage system.

Scanning symbolic links in NetApp storage systems typically occurs as follows. Kaspersky Anti-Virus 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 Anti-Virus does not scan that file. If the settings of the NetApp storage system 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 NetApp storage system, 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 NETAPP STORAGE SYSTEM

Kaspersky Anti-Virus 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-PLUGGABLE NETWORK STORAGE SYSTEM AND KASPERSKY ANTI-VIRUS

You can run network storage protection tasks if the active key supports network storage protection. If you run a network storage protection task when the active key does not support network storage protection, the task returns an error. In this case, the network storage systems are not protected by Kaspersky Anti-Virus.

To protect RPC-pluggable network storage systems, you need to configure a connection between the network storage system and Kaspersky Anti-Virus.

To do this, perform the following actions:

- On the server with Kaspersky Anti-Virus installed:

  - add the network storage system to Kaspersky Anti-Virus
  - specify the account from which the **RPC: Network storage protection** task is started in Kaspersky Anti-Virus
  - Define the security settings of local policies in the local group policy editor
  - Configure rules for inbound and outbound connections in Windows firewall
  - Install a connector application for the NetApp storage system managed by the NetApp Clustered Data ONTAP operating system.

    For more details on how to install a connector application for the NetApp storage system managed by the NetApp Clustered Data ONTAP operating system, please refer to the documentation shipped with the network storage system.

- In the network storage system:
  - Enable the anti-virus scan feature (vscan)
  - Add the account from which the **RPC: Network storage protection** task is started to the Backup Operators group.

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

IN THIS SECTION

ADDING AN RPC-PLUGGABLE NETWORK STORAGE SYSTEM TO KASPERSKY ANTI-VIRUS

To add an RPC-pluggable network storage system to Kaspersky Anti-Virus:

1. In the Kaspersky Anti-Virus Console tree, select the **Protection of network-attached storages** → **RPC: Network storage protection** task.
2. In the details pane, select the **Protection scope settings** tab.
3. Right-click in the **Protection scope** table and select **Add protection scope**.

   The **Add protection scope** window opens.
4. In the **Add protection scope** window, enter the domain name or IP address of the network storage system.

   > 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.

5. Click **OK** to add the network storage system to Kaspersky Anti-Virus.

The network storage system appears in the list of protected network storage systems.

6. Save the changes that have been made using one of the following methods:

   - In the toolbar of Kaspersky Anti-Virus Console, click the 💾 button.
   - Open the context menu on the task name and select **Save task**.

Kaspersky Anti-Virus connects to the network storage system when the **RPC: Network storage protection** task. If you have specified an incorrect domain name or incorrect IP address for the network storage system, the task returns an error. Kaspersky Anti-Virus records information about this event in the system audit log and the task execution log.

If you are using a NetApp storage system managed by the NetApp Clustered Data ONTAP operating system, Kaspersky Anti-Virus connects to the connector application. 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 storage system is protected by Kaspersky Anti-Virus.

SELECTING THE ACCOUNT FROM WHICH THE RPC: NETWORK STORAGE PROTECTION

The account from which the **RPC: Network storage protection** task is started must have administrator rights on the server with Kaspersky Anti-Virus installed and be included in the Backup Operators group on the network storage system.

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

➡ *To specify the account from which the RPC: Network storage protection task:*

1. Expand the **Protection of network-attached storages** node in the Kaspersky Anti-Virus Console tree.
2. Open the context menu of the **RPC: Network storage protection** task and select the **Properties** item.

   The **Properties: RPC: Network storage protection** task.
3. In the window that opens, go to the **General** tab, and in the **Network storage systems connection settings** section enter the name of the account under which the task starts, the account password, and the password confirmation.
4. Click **OK** to save changes and close the **Properties: RPC: Network storage protection** task.

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 Anti-Virus installed, using one of the following methods:

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

  a. Click **OK** to save changes and close the window.

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

3. 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**.

4. Reboot the server to apply changes.

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 Anti-Virus installed, using one of the following methods:

     - In the entry field, specify the domain name of a server with Kaspersky Anti-Virus installed

     - Click the **Browse** button and, in the integrated security subject selection window that opens, select a server with Kaspersky Anti-Virus installed, using search by domain or by workgroup.

     a. Click **OK** to save changes and close the window.

2. 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 blocking 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.

DEFAULT SETTINGS OF THE RPC: NETWORK STORAGE PROTECTION TASK

By default, the **RPC: Network storage protection** task has the following settings described in the table below. You can change the values of these settings.

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

Table 3. Default settings of the RPC: Network storage protection task

SETTING	DEFAULT VALUE	Comment
Protection scope.	Not available.	You need to add the network storage system to Kaspersky Anti-Virus.
Security level.	The **Recommended** security level is applied.	You can apply one of the preset security levels to the protected network storage system, 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.
Network storage connection settings	• The **User name** and the **Password** of the 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 storage system after updates of application databases** – the check box is selected.	You need to specify the account from which the **RPC: Network storage protection** task. 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 Anti-Virus startup.

REMOVING AN RPC-PLUGGABLE NETWORK STORAGE SYSTEM FROM AN RPC TASK: NETWORK STORAGE PROTECTION

To delete an RPC-pluggable network storage system from the RPC: Network storage protection task:

1. In the Kaspersky Anti-Virus Console tree, select the **Protection of network-attached storages** → **RPC: Network storage protection** task.

2. In the details pane, select the **Protection scope settings** tab.

3. In the list of protected systems, open the context menu of the network storage system that you want to delete from the task, and select the **Remove from the list** item.

   The selected network storage system is removed from the list of protected network storage systems.

DISABLING AND ENABLING PROTECTION OF AN ADDED RPC-PLUGGABLE NETWORK STORAGE SYSTEM

To disable protection of an added RPC-pluggable network storage system:

1. In the Kaspersky Anti-Virus Console tree, select the **Protection of network-attached storages** → **RPC: Network storage protection** task.

2. In the details pane, select the **Protection scope settings** tab.

3. In the list of protected network storage systems, clear the check box next to the name of the network storage system for which you want to temporarily disable protection.

4. Save the changes that have been made using one of the following methods:

   - In the toolbar of Kaspersky Anti-Virus Console, click the 💾 button.

   - Open the context menu on the task name and select **Save task**.

Kaspersky Anti-Virus interrupts the connection with the selected network storage system.

If you disable protection for all added network storage systems, Kaspersky Anti-Virus stops the **RPC: Network storage protection** task.

To enable protection of an added RPC-pluggable network storage system:

1. In the Kaspersky Anti-Virus Console tree, select the **Protection of network-attached storages** → **RPC: Network storage protection** task.

2. In the details pane, select the **Protection scope settings** tab.

3. In the list of protected network storage systems, select the check box next to the name of the network storage system for which you want to enable protection.

4. Save the changes that have been made using one of the following methods:

   - In the toolbar of Kaspersky Anti-Virus Console, click the 💾 button.

   - Open the context menu on the task name and select **Save task**.

If the **RPC: Network storage protection** task is running, Kaspersky Anti-Virus establishes a connection with the network storage system. If the **RPC: Network storage protection** task is not running, you need to start it so that Kaspersky Anti-Virus establishes a connection with the network storage system.

CONFIGURING THE RPC: NETWORK STORAGE PROTECTION

This section describes how to configure the **RPC: Network storage protection** task.

IN THIS SECTION

ENABLING OR DISABLING THE HEURISTIC ANALYZER. RPC: NETWORK STORAGE PROTECTION

In the **RPC: Network storage protection** task, you can enable the Heuristic Analyzer.

➧ *To enable or disable the Heuristic Analyzer in the RPC: Network storage protection task:*

1. Expand the **Protection of network-attached storages** node in the Kaspersky Anti-Virus Console tree.
2. Open the context menu of the **RPC: Network storage protection** task and select the **Properties** item.

   The **Properties: RPC: Network storage protection** task.
3. In the window that opens, go to the **General** tab and do one of the following in the **Heuristic Analyzer** section:
   - To use the heuristic analyzer, select the **Use heuristic analyzer** check box and configure the analysis level using the slider.
   - To disable the Heuristic Analyzer, clear the **Use Heuristic Analyzer** check box.
4. Click **OK** to save changes and close the **Properties: RPC: Network storage protection** task.

ENABLING OR DISABLING THE USE OF A TRUSTED ZONE. RPC: NETWORK STORAGE PROTECTION

Trusted zone is a precompiled list of exclusions from the protection / scan scope (for detailed information about the trusted zone please refer to the *Administrator's Guide for Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition*).

You can enable or disable 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.

➧ *To enable or disable a trusted zone in the RPC: Network storage protection task:*

1. Expand the **Protection of network-attached storages** node in the Kaspersky Anti-Virus Console tree.
2. Open the context menu of the **RPC: Network storage protection** task and select the **Properties** item.

   The **Properties: RPC: Network storage protection** task.
3. In the window that opens, go to the **General** tab and do one of the following in the **Trusted zone** section:
   - To apply the trusted zone in the task, select the **Apply trusted zone** check box.
   - To disable the use of the trusted zone in the task, clear the **Apply trusted zone** check box.
4. Click **OK** to save changes and close the **Properties: RPC: Network storage protection** task.

CONFIGURING RECOVERY OF THE CONNECTION WITH AN RPC-PLUGGABLE NETWORK STORAGE SYSTEM AFTER A CONNECTION INTERRUPTION

➧ *To configure the recovery of the connection to an RPC-pluggable network storage system after a connection interruption:*

1. Expand the **Protection of network-attached storages** node in the Kaspersky Anti-Virus Console tree.
2. Open the context menu of the **RPC: Network storage protection** task and select the **Properties** item.

   The **Properties: RPC: Network storage protection** task.
3. In the window that opens, go to the **General** tab and do the following in the **Network storage systems connection settings** section:
   - In this field, enter a value for the timeout between attempts to recover the connection with the network storage system.
   - In this field, enter a value for the maximum number of attempts to recover the connection with the network storage system.

   You are recommended to keep default values or specify larger values.
4. Click **OK** to save changes and close the **Properties: RPC: Network storage protection** task.

ENABLING AND DISABLING CACHE CLEARING OF SCANNED FILES IN AN RPC-PLUGGABLE NETWORK STORAGE SYSTEM AFTER AN APPLICATION DATABASES UPDATE

➧ *To enable or disable cache clearing of scanned files in an RPC-pluggable network storage system after an application databases update:*

1. Expand the **Protection of network-attached storages** node in the Kaspersky Anti-Virus Console tree.

2. Open the context menu of the **RPC: Network storage protection** task and select the **Properties** item.

   The **Properties: RPC: Network storage protection** task.

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

   - If you want Kaspersky Anti-Virus to clear the cache of scanned files of the network storage system after each update of the application databases, select the **Clear cache of scanned files on network storage system after updates of application databases** check box.

   - If you want Kaspersky Anti-Virus to save the cache of scanned files of the network storage system after each update of the application databases, clear the **Clear cache of scanned files on network storage system after updates of application databases** check box.

4. Click **OK** to save changes and close the **Properties: RPC: Network storage protection** task.

STARTING THE RPC: NETWORK STORAGE PROTECTION TASK BY SCHEDULE

You can configure a scheduled start of the **RPC: Network storage protection** task.

You can enable or disable the scheduled start of the task and configure the task start schedule.

➧ *To configure the task start schedule*:

1. Open the context menu of the name of the task for which you wish to configure the launch schedule, and select the **Properties** item.

2. In the **Properties** window: **<Task name>** on the **Schedule** tab, enable task launch by schedule: select the **Run by schedule** check box.

3. Configure schedule settings in accordance with your requirements. To do this*:*

   a. Specify the task launch frequency: In the **Frequency** list, select one of the following values: **Hourly**, **Daily**, **Weekly**, **At application startup**, **After database update**. Define the following settings:

      - if **Hourly** is selected, specify the number of hours in the **Every <number> h** in the **Task start settings** group;

      - if **Daily** is selected, specify the number of days in the **Every <number> d** in the **Task start settings** group;

      - if **Weekly** is selected, specify the number of weeks in the **Every <number> w** in the **Task start settings** group. Specify the days of the week on which the task will be launched (by default the task is launched on Mondays).

   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 **Properties: <Task name>** window on the **Schedule** tab.
   >
   > The value **Blocked by policy** is displayed in the **Next start** field if the active policy settings of Kaspersky Security Center prohibit starting system tasks by schedule.

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

   a. To specify the maximum duration of a task, enter the number of hours and minutes you wish in the **Duration** field in the **Task stop settings** group.

   b. To specify time interval within a 24-hour period in which a task execution is be paused, in the group **Task stop settings** enter the start and end values of the interval in the **Pause from… until** field.

   c. To specify the date at which the schedule will be disabled: select the **Cancel schedule from** check box and select the date when schedule will be disabled using the **Calendar** window.

   d. To enable launching of missed tasks: select the **Run skipped tasks** check box.

   e. To enable the use of the "Randomize the task start within internal, min" setting, check the Randomize the task start within interval **of** and specify the value for this setting in minutes.

5. Click the **Apply** button to save the changes that you have made in the **Settings <Task>**.

After a task launch schedule has been configured once, it can be enabled and disabled. After a schedule has been disabled, its settings (frequency, start time, etc.) will not be deleted and the schedule can be enabled again, if required.

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

1. Open the context menu on the name of the task for which you want to configure the launch schedule, and select **Properties**.
2. In the **Properties: <Task name>** window, perform one of the following actions on the **Schedule** tab:
   - select the **Run by schedule** check box to enable the schedule;
   - clear the **Run by schedule** check box to disable the schedule.
3. Press the **OK** or **Apply** button.

SECURITY LEVELS. RPC: NETWORK STORAGE PROTECTION

This section describes the security settings and provides instructions for applying preset security levels and configuring security settings manually in the **RPC: Network storage protection** task.

IN THIS SECTION

ABOUT SECURITY LEVELS. RPC: NETWORK STORAGE PROTECTION

In the **RPC: Network storage protection** task, you can apply one of the following preset security levels for each 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 storage system changes to **Custom**.

Maximum performance

The **Maximum performance** security level is recommended if, apart from using Kaspersky Anti-Virus 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.

Table 4. Settings of preset security levels. RPC: Network storage protection

SETTINGS	SECURITY LEVEL		
	MAXIMUM PERFORMANCE	RECOMMENDED	MAXIMUM PROTECTION
Objects protection	**Objects scanned according to list of extensions specified in anti-virus databases**	**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**
Actions depending on the detected object type	No	No	No
Exclude objects	No	No	No
Do not detect	No	No	No
Stop scan 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. RPC: NETWORK STORAGE PROTECTION

To apply one of the preset security levels to an RPC-pluggable network storage system:

1. In the Kaspersky Anti-Virus Console tree, select the **Protection of network-attached storages** → **RPC: Network storage protection** task.

2. In the details pane, select the **Protection scope settings** tab.

3. In the list of protected network storage systems, select the network storage system for which you want to select a preset security level.

4. On the **Security level** tab, in the **Selecting security level** section, 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 storage system in the list of protected network storage systems.

5. Save the changes that have been made using one of the following methods:

   - In the toolbar of Kaspersky Anti-Virus Console, click the 💾 button.
   - Open the context menu on the task name and select **Save task**.

You can also edit the security settings of the protected network storage system manually.

SEE ALSO

About security levels. RPC: Network storage protection 36

Configuring security level settings manually. RPC: Network storage protection 38

CONFIGURING SECURITY LEVEL SETTINGS MANUALLY. RPC: NETWORK STORAGE PROTECTION

➡ *To manually configure the security settings of an RPC-pluggable network storage system:*

1. In the Kaspersky Anti-Virus Console tree, select the **Protection of network-attached storages → RPC: Network storage protection** task.
2. In the details pane, select the **Protection scope settings** tab.
3. In the list of protected network storage systems, select the network storage system whose security settings you want to configure.
4. On the **Security level** tab, in the **Selecting security level** section, click the **Settings** button in the lower part of the tab.

   > You can apply a preset template of security settings.

5. Configure the settings of the selected network storage system in accordance with your computer security requirements. To do so:

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

       Kaspersky Anti-Virus scans only objects that can be potentially infected based on file format.

       Kaspersky Lab compiles the list of formats. It is included in the Kaspersky Anti-Virus databases.

       This option is selected by default for the **Maximum Protection** and **Recommended** security levels.
     - **Objects scanned according to the list of extensions specified in antivirus databases**.

       Kaspersky Anti-Virus scans only objects that can be potentially infected based on file extension.

Kaspersky Lab compiles the list of extensions. It is included in the Kaspersky Anti-Virus databases.

This option is selected by default for the **Maximum performance** security level.

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

  Kaspersky Anti-Virus scans files based on file extension. You have to specify manually the extensions of files to be scanned.

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

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

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

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

  - In the **Exclusions** section, specify the objects that you want Kaspersky Anti-Virus 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 masks of names of detectable objects, according to the Virus Encyclopedia classification (http://www.securelist.com/en/).

> You can also define these settings for the entire task in the settings of the exclusion rule in the Trusted Zone.

  - In the **Advanced settings** section, specify the maximum duration of an object scan and the maximum size of a compound file being scanned:

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

6. On the **General** tab, click the **Security level** button to save changes and exit the mode of configuring security settings for the protected network storage system.

SEE ALSO

MANAGING TEMPLATES OF SECURITY LEVEL SETTINGS. RPC: NETWORK STORAGE PROTECTION

This section provides instructions on how to manage templates of security level settings in the **RPC: Network storage protection** task.

IN THIS SECTION

SAVING SECURITY LEVEL SETTINGS TO A TEMPLATE. RPC: NETWORK STORAGE PROTECTION

➧ *To save the security level settings of a protected RPC-pluggable network storage system to a template:*

1. In the Kaspersky Anti-Virus Console tree, select the **Protection of network-attached storages** → **RPC: Network storage protection** task.
2. In the details pane, select the **Protection scope settings** tab.
3. In the list of protected network storage systems, select the network storage system whose security settings you want to save to a template.
4. On the **Security level** tab, click the **Settings** button in the lower part of the tab.
5. On the **General** tab, click the **Save as template** button.

   The **Template properties** window opens.
6. In the **Template properties** window, in the **Template name** field, enter the name of the security settings template.
7. If necessary, in the **Description** field, enter additional information about the security settings template.
8. Click **OK** to save the security settings template and close the **Template properties** window.

VIEWING SECURITY SETTINGS IN A TEMPLATE. RPC: NETWORK STORAGE PROTECTION

➧ *To view the security settings of an RPC-pluggable network storage system:*

1. Expand the **Protection of network-attached storages** node in the Kaspersky Anti-Virus Console tree.
2. Open the context menu of the **RPC: Network storage protection** task, and select the **Settings templates** item.

   The **Templates** window opens.
3. The **Templates** window displays the security settings templates that you can apply to a protected network storage system.
4. Open the window with details of a security settings template using one of the following methods:
   - Double-click the name of a settings template in the list
   - Select the name of a security template in the list and click the **View** button.
5. In the window that opens, the following details are displayed:
   - The **General** tab displays the template name and description
   - The **Properties** tab displays the list of security settings.

You cannot modify the template that has been saved.

APPLYING A TEMPLATE OF SECURITY SETTINGS. RPC: NETWORK STORAGE PROTECTION

By default, the list of security settings templates that you can apply to a protected RPC-pluggable network storage system is blank. Before applying a security settings template to a protected network storage system, you must create it.

➧ *To apply a security settings template to a protected RPC-pluggable network storage system:*

1. In the Kaspersky Anti-Virus Console tree, select the **Protection of network-attached storages** → **RPC: Network storage protection** task.
2. In the details pane, select the **Protection scope settings** tab.
3. Open the context menu of the protected network storage system to which you want to apply the security settings template, and select **Apply template** → **<Template name>**.

   The selected security settings template is applied to the protected network storage system. The security level applied to the protected network storage system changes to **Custom**.

SEE ALSO

Saving security level settings to a template. RPC: Network storage protection 40

DELETING A TEMPLATE OF SECURITY SETTINGS. RPC: NETWORK STORAGE PROTECTION

➧ *To delete a template of security settings:*

1. Expand the **Protection of network-attached storages** node in the Kaspersky Anti-Virus Console tree.
2. Open the context menu of the **RPC: Network storage protection** task, and select the **Settings templates** item.

   The **Templates** window opens.
3. In the **Templates** window, select the security settings template to be deleted and click the **Delete** button.
4. Click **Yes** in the window of template deletion confirmation.

   The selected security settings template will be deleted.

VIEWING STATISTICS. RPC: NETWORK STORAGE PROTECTION

If the **RPC: Network storage protection** task is running, you can view real-time information about the number of objects processed by Kaspersky Anti-Virus since the task was started (task statistics).

➧ *To view task statistics for the RPC: Network storage protection task:*

1. In the Kaspersky Anti-Virus Console tree, select the **Protection of network-attached storages** → **RPC: Network storage protection** task.
2. In the details pane, select the **Overview and management** tab.
3. On the **Overview and management** tab of the details pane in the **Statistics** section, click the **Complete statistics** link.

   This opens a table with the following information about objects processed by Kaspersky Anti-Virus since the task was started (see the table below).

Table 5. Full RPC: Network storage protection

FIELD	DESCRIPTION
Detected	Number of objects detected by Kaspersky Anti-Virus. For example, if Kaspersky Anti-Virus detects one malware program in five files, the value in this field increases by one.
Infected objects detected	Number of objects found by Kaspersky Anti-Virus to be infected.
Probably infected objects detected	Number of objects found by Kaspersky Anti-Virus to be probably infected.
Objects not disinfected	Number of objects which Kaspersky Anti-Virus 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 Anti-Virus attempted to quarantine but was unable to do so, for example, due to insufficient disk space.
Objects not deleted	The number of objects that Kaspersky Anti-Virus 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 Anti-Virus 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 Anti-Virus 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 Anti-Virus.
Moved to Quarantine	Number of objects quarantined by Kaspersky Anti-Virus.
Moved to Backup	The number of object copies that Kaspersky Anti-Virus saved to Backup.
Objects deleted	Number of objects deleted by Kaspersky Anti-Virus.
Password-protected objects	Number of objects (archives, for example) that Kaspersky Anti-Virus missed because they were password protected.
Corrupted objects	The number of objects skipped by Kaspersky Anti-Virus as their format was corrupted.
Objects processed	Total number of objects processed by Kaspersky Anti-Virus.

PROTECTING ICAP-PLUGGABLE NETWORK STORAGE SYSTEMS

This section provides information about the task for protection of network storage systems connected via ICAP, about the setup of connection between a network storage system and Kaspersky Anti-Virus, as well as instructions on how to configure a protection task and define the security settings for ICAP-connected network storage systems.

IN THIS SECTION

ABOUT PROTECTING ICAP-PLUGGABLE NETWORK STORAGE SYSTEMS

Kaspersky Anti-Virus installed on a server under a Microsoft Windows operating system protects ICAP-pluggable network storage systems (such as EMC Isilon) against viruses and other security threats that infiltrate the server through the exchange of files.

Kaspersky Anti-Virus scans files located in network share folders in the ICAP-pluggable network storage system (hereinafter also *network storage system*) when an attempt is made to read or modify the files from a workstation. The network storage system allows reading or modifying a file if Kaspersky Anti-Virus has identified that file as safe. If Kaspersky Anti-Virus has identified a file as infected or probably infected, the network storage system blocks that file from being read or modified. Kaspersky Anti-Virus lets you configure actions that the application takes on infected and probably infected files. By default, Kaspersky Anti-Virus attempts to disinfect infected files and places probably infected files in Quarantine. Before disinfecting a file, Kaspersky Anti-Virus places a copy of the file in backup storage.

You can protect one network storage system or several network storage systems using one server with Kaspersky Anti-Virus installed on it.

To protect the network storage system, you need to configure the connection of the network storage system to Kaspersky Anti-Virus. Kaspersky Anti-Virus provides an ICAP-pluggable network storage protection task called **ICAP: Network storage protection** task.

You can run network storage protection tasks if the active key supports network storage protection. If you run a network storage protection task when the active key does not support network storage protection, the task returns an error. In this case, the network storage systems are not protected by Kaspersky Anti-Virus.

The **ICAP: Network protection task** is created by default. You cannot delete or rename this task. Nor can you create another ICAP-pluggable network storage protection task. You can configure the properties of the **ICAP: Network storage protection** task.

CONFIGURING AN ICAP-PLUGGABLE NETWORK STORAGE SYSTEM TO KASPERSKY ANTI-VIRUS

To protect an ICAP-pluggable network storage system, you need to configure the connection of the network storage system to Kaspersky Anti-Virus.

To do this, perform the following actions:

- On the server with Kaspersky Anti-Virus installed:
  - configure the connection settings – **Number of ICAP server network port** and **ICAP service ID**
  - open the ICAP server port in the Windows firewall and on all network devices between the network storage system and Kaspersky Anti-Virus.
- In the network storage system:
  - enable anti-virus protection
  - specify the address of the connection to Kaspersky Anti-Virus in the network storage settings

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

➧ *To configure the connection settings:*

1. Select the **Protection of network-attached storages** node in the Kaspersky Anti-Virus Console tree.
2. Open the context menu of the **IPAC: Network storage protection** task and select the **Properties** item.
3. The **Properties: ICAP: Network storage protection** task.
4. On the **General** tab in the **Connection settings** section, define the following settings:
   - **Number of ICAP server network port**

     Number of ICAP server network port.
   - **ICAP 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 an anti-virus application 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** to save changes and close the **Properties: ICAP: Network storage protection** task.

Once you have configured the connection settings, on the network storage system you need to set the address of the connection to Kaspersky Anti-Virus. 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 Anti-Virus installed>/avscan:1344
```

DEFAULT SETTINGS OF THE ICAP: NETWORK STORAGE PROTECTION TASK

By default, the **ICAP: Network storage protection** task has the following 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 Anti-Virus immediately applies the new settings in the running task. Kaspersky Anti-Virus logs the date and time when the task settings were modified in the system audit log.

Table 6. Default 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 storage system, 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.
Network storage connection settings	• **Number of ICAP server network port** – 1344 • **ICAP service ID** – avscan.	You can also modify other network storage connection settings. These changes should be incorporated on the network storage systems.
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 Anti-Virus startup.

CONFIGURING THE ICAP: NETWORK STORAGE PROTECTION

This section describes how to configure the **IPAC: Network storage protection** task.

IN THIS SECTION

ENABLING OR DISABLING THE HEURISTIC ANALYZER

In the ICAP: Network storage protection task, you can enable the Heuristic Analyzer.

➧ *To enable or disable the Heuristic Analyzer in the ICAP: Network storage protection task:*

1. Expand the **Protection of network-attached storages** node in the Kaspersky Anti-Virus Console tree.
2. Open the context menu of the **IPAC: Network storage protection** task and select the **Properties** item.

3. The **Properties: ICAP: Network storage protection** task.
4. In the window that opens, go to the **General** tab and do one of the following in the **Heuristic Analyzer** section:
   - To use the heuristic analyzer, select the **Use heuristic analyzer** check box and configure the analysis level using the slider.
   - To disable the Heuristic Analyzer, clear the **Use Heuristic Analyzer** check box.
5. Click **OK** to save changes and close the **Properties: ICAP: Network storage protection** task.

STARTING THE ICAP: NETWORK STORAGE PROTECTION TASK BY SCHEDULE

You can configure a scheduled start of the **ICAP: Network storage protection** task.

You can enable or disable the scheduled start of the task and configure the task start schedule (see section "Starting the RPC: Network storage protection task by schedule" on page 34).

SECURITY LEVELS. ICAP: NETWORK STORAGE PROTECTION

This section describes the security settings and provides instructions for applying preset security levels and configuring security settings manually in the **ICAP: Network storage protection** task.

IN THIS SECTION

ABOUT SECURITY LEVELS. ICAP: NETWORK STORAGE PROTECTION

In the **ICAP: Network storage protection** task, you can apply one of the following preset security levels for each 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 storage system changes to **Custom**.

Maximum performance

The **Maximum performance** security level is recommended if, apart from using Kaspersky Anti-Virus 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.

Table 7. Settings of preset security levels. ICAP: Network storage protection

SETTINGS	SECURITY LEVEL		
	MAXIMUM PERFORMANCE	RECOMMENDED	MAXIMUM PROTECTION
Objects protection	**Objects scanned according to list of extensions specified in anti-virus databases**	**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 objects	No	No	No
Do not detect	No	No	No
Stop scan 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. ICAP: NETWORK STORAGE PROTECTION

To apply one of the preset security levels to an ICAP-pluggable network storage system:

1. Select the **Protection of network-attached storages** node in the Kaspersky Anti-Virus Console tree.
2. Open the context menu of the **IPAC: Network storage protection** task and select the **Properties** item.
3. The **Properties: ICAP: Network storage protection** task.
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 selected security level settings are displayed under the list.

5. Click **OK** to save changes and close the **Properties: ICAP: Network storage protection** task.

You can also edit the security settings of the protected network storage system manually.

SEE ALSO

CONFIGURING SECURITY LEVEL SETTINGS MANUALLY. ICAP: NETWORK STORAGE PROTECTION

To manually configure the security settings of an ICAP-pluggable network storage system:

1. Select the **Protection of network-attached storages** node in the Kaspersky Anti-Virus Console tree.
2. Open the context menu of the **IPAC: Network storage protection** task and select the **Properties** item.
3. The **Properties: ICAP: Network storage protection** task.
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 so:

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

     - In the **Objects protection** section, specify the objects to be scanned by Kaspersky Anti-Virus:
     - **All objects**.
     - **Objects scanned by format**.

       Kaspersky Anti-Virus scans only objects that can be potentially infected based on file format.

       Kaspersky Lab compiles the list of formats. It is included in the Kaspersky Anti-Virus databases.

       This option is selected by default for the **Maximum Protection** and **Recommended** security levels.

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

       Kaspersky Anti-Virus scans only objects that can be potentially infected based on file extension.

       Kaspersky Lab compiles the list of extensions. It is included in the Kaspersky Anti-Virus databases.

       This option is selected by default for the **Maximum performance** security level.

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

       Kaspersky Anti-Virus scans files based on file extension. You have to specify manually the extensions of files to be scanned.

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

- 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 Anti-Virus when detecting an infected object.
  - In the **Action to perform on probably infected objects** section, select the action to be performed by Kaspersky Anti-Virus when detecting a probably infected object.
- On the **Performance** tab take the following actions:
  - In the **Exclusions** section, specify the objects that you want Kaspersky Anti-Virus 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 the masks of names of detectable objects, according to the Virus Encyclopedia classification (http://www.securelist.com/en/).
  - In the **Advanced settings** section, specify the maximum duration of an object scan and the maximum size of a compound file being scanned:

6. Click **OK** to open the **Security settings** window. Click **OK** to save changes and close the **Properties: ICAP: Network storage protection** task.

VIEWING STATISTICS. ICAP: NETWORK STORAGE PROTECTION

If the **IPAC: Network storage protection** task is running, you can view real-time information about the number of objects processed by Kaspersky Anti-Virus since the task was started (task statistics).

➧ *To view task statistics for the IPAC: Protection of network-attached storages:*

In the Kaspersky Anti-Virus Console tree, select the **Protection of network-attached storages** → **ICAP: Network storage protection** task.

On the **View and manage** tab of the results pane, in the **Statistics** section, a table is displayed in which you can view information about the objects that Kaspersky Anti-Virus has processed since the task start until the present moment. The settings displayed in the table are analogous to those displayed for the **RPC: Network storage protection** (see section "**Viewing statistics. RPC: Network storage protection**" on page 42).

CONTACTING TECHNICAL SUPPORT

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

IN THIS SECTION

ABOUT TECHNICAL SUPPORT

If you do not find a solution to your problem in the application documentation or in one of the sources of information about the application, we recommend that you contact Kaspersky Lab Technical Support. Technical Support specialists will answer your questions about installing and using the application.

Technical support is 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, we recommend that you read through the support rules (http://support.kaspersky.com/support/rules).

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

- By calling Kaspersky Lab Technical Support.
- By sending a request to Technical Support through the Kaspersky CompanyAccount web service.

Technical Support via Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) is a web service for companies that use Kaspersky Lab applications. The Kaspersky CompanyAccount web service is designed to facilitate interaction between users and Kaspersky Lab specialists via online requests. You can use Kaspersky CompanyAccount to track the status of your online requests and store a history of them as well.

You can register all of your organization's employees under a single account on Kaspersky CompanyAccount. A single 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.

The Kaspersky CompanyAccount web service 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

If an urgent issue arises, you can call Kaspersky Lab Technical Support representatives (http://support.kaspersky.com/support/contacts).

Before contacting Technical Support, you are advised to read the technical support rules (http://support.kaspersky.ru/support/rules). These rules contain information about the working hours of Kaspersky Lab Technical Support and about the information that you must provide so that Kaspersky Lab Technical Support specialists can help you.

Using trace files and AVZ scripts

After you report a problem to Kaspersky Lab Technical Support specialists, they may ask you to generate a report with information about the operation of Kaspersky Anti-Virus and to send it to Kaspersky Lab Technical Support. Kaspersky Lab Technical Support specialists may also ask you to create 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 analyzing the data you send, Kaspersky Lab Technical Support specialists 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

Settings of the application that are common for tasks of all the types and responsible for the operation of the application itself, for example: application performance settings, settings of reports, 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, which substitutes zero or more characters
- **?** – the symbol, which 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 the current version of the databases of Kaspersky Lab applications. It allows finding files that may contain some unknown virus or a new modification of a known virus.

The *Probably-infected* status is assigned to files in which the heuristic analysis has detected malicious code.

Heuristic Analyzer

A module of Kaspersky Anti-Virus 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

POSSIBLY 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. Possibly files can be detected by means of the heuristic analyzer.

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.

Q

QUARANTINE

The folder to which Kaspersky Anti-Virus moves possibly infected objects that have been detected. Files are stored in Quarantine in encrypted form in order to avoid any impact on the computer.

S

SIGNATURE ANALYSIS

The technology of threat detection, which uses databases of Kaspersky Anti-Virus that contain descriptions of known threats and 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 a Kaspersky Lab application are implemented as tasks, for example: Real-time protection of files, Full Scan, Update application databases.

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.

KASPERSKY LAB ZAO

Kaspersky Lab software is internationally renowned for its protection against viruses, malware, spam, network and hacker attacks, and other threats.

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). Kaspersky Lab is the preferred developer of computer protection systems among home users in Russia, according to the COMCON survey "TGI-Russia 2009".

Kaspersky Lab was founded in Russia in 1997. Today Kaspersky Lab is an international group of companies headquartered in Moscow and comprising five regional divisions, which manage the company's operations in Russia, Western and Eastern Europe, the Middle East, Africa, Northern and Southern America, Japan, China, and other countries of the Asia-Pacific region. The company employs more than 2,000 skilled professionals.

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

The personal product range includes anti-virus applications for desktop, laptop, and tablet computers, and for smartphones and other mobile devices.

Kaspersky Lab delivers applications and services to protect workstations, file and web servers, mail gateways, and firewalls. Used in conjunction with Kaspersky Lab's centralized management system, these solutions ensure effective automated protection for companies and organizations against computer threats. 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 new computer threats, create tools to detect and disinfect them, and include them in the databases used by Kaspersky Lab applications. *Kaspersky Lab's Anti-Virus database is updated hourly*; and the *Anti-Spam database every five minutes*.

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 many other developers use the Kaspersky Anti-Virus kernel in their products, including: SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Israel), Clearswift (UK), CommuniGate Systems (USA), Openwave Messaging (Ireland), D-Link (Taiwan), M86 Security (USA), GFI Software (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), Netasq+Arkoon (France), NETGEAR (USA), Parallels (USA), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Taiwan). 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 2010 Kaspersky Anti-Virus received several top Advanced+ awards in a test administered by AV-Comparatives, a reputed Austrian anti-virus laboratory. But Kaspersky Lab's main achievement is the loyalty of its users worldwide. The company's products and technologies protect more than 300 million users, and its corporate clients number more than 200,000.

Kaspersky Lab website:	http://www.kaspersky.com
Virus Encyclopedia	http://www.securelist.com/en/
Virus Lab:	newvirus@kaspersky.com (only for sending probably infected files in archives)
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, Citrix Presentation Server, XenApp, and XenDesktop are registered trademarks of Citrix Systems, Inc. and/or subsidiaries in the United States and/or elsewhere.

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

Core and Intel are trademarks of Intel Corporation registered in the United States and/or elsewhere.

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

Excel, Hyper-V, JScript, 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.

INDEX