KASPERSKY lab

Kaspersky Security for Windows Server

Implementation guide for Network Attached Storage Protection

Application version: 10.1.2.996

Dear User,

Thank you for choosing Kaspersky Lab as your security software provider. We hope that this document helps you to use our product.

Document revision date: 12.04.2019

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

Contents

About this Guide

The Kaspersky Security for Windows Server 10.1 (hereinafter referred to as "Kaspersky Security for Windows Server") Implementation Guide for Network Attached Storage Protection is intended for specialists who install and administer Kaspersky Security for Windows Server, as well as for specialists who provide technical support to organizations that use Kaspersky Security for Windows Server.

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

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

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

In this chapter

In this document

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

Sources of information about Kaspersky Security for Windows Server

This section lists the sources of information about the application.

Kaspersky Security for Windows Server

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

Hardware and software requirements

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

Integrating Kaspersky Security for Windows Server with network attached storages

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

Managing Kaspersky Security for Windows Server Console

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

Viewing the Network Attached Storage Protection status

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

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

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

RPC Network Storage Protection

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

ICAP Network Storage Protection

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

Anti-Cryptor for NetApp

This section provides information about the Anti-Cryptor for NetApp task and how to configure it.

Contacting Technical Support

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

Glossary

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

AO Kaspersky Lab

This section provides information about Kaspersky Lab AO.

Information about third-party code

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

Document conventions

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

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 blue background under the heading "Example".
Update means... The *Databases are out of date* event occurs.	The following elements are italicized in the text: • New terms • Names of application statuses and events
Press **ENTER**. Press **ALT+F4**.	Names of keyboard keys appear in bold and are capitalized. Names of keys that are connected by a + (plus) sign indicate the use of a key combination. These keys must be pressed simultaneously.
Click the **Enable** button.	Names of application interface elements, such as text boxes, menu items, and buttons, are set off in bold.
► *To configure a task schedule:*	Introductory phrases of instructions are italicized and accompanied by an arrow.
In the command line, type `help` The following message then appears: `Specify the date in dd:mm:yy format.`	The following types of text content are set off with a special font: • Text in the command line • Text of messages displayed on the screen by the application • Data that must be entered from the keyboard
<User name>	Variables are enclosed in angle brackets. Instead of a variable, the corresponding value should be inserted, omitting the angle brackets.

Sources of information about Kaspersky Security for Windows Server

This section lists the sources of information about the application.

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

In this chapter

Sources for independent retrieval of information

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

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

If you did not find a solution to your problem, contact Kaspersky Lab Technical Support.

An Internet connection is required to use online information sources.

Kaspersky Security for Windows Server page on the Kaspersky Lab website

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

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

Kaspersky Security page in Knowledge Base

Knowledge Base is a section on the Technical Support website.

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

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

Kaspersky Security for Windows Server documentation

Kaspersky Security for Windows Server Administrator's Guide describes how to install, uninstall and activate the application, and how to configure and use Kaspersky Security for Windows Server and the Application Console.

In the Implementation Guide for Network Attached Storage Protection you can find information about configuring and using Kaspersky Security for Windows Server for the network attached storage protection.

Discussing Kaspersky Lab applications on the forum

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

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

About Kaspersky Security for Windows Server

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

You can install Kaspersky Security for Windows Server on the following servers:

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

Kaspersky Security for Windows Server can be managed in the following ways:

- Via the Application Console installed on the same server as Kaspersky Security for Windows Server or on a different computer.
- Using commands in the command line.
- Via Kaspersky Security Center Administration Console.

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

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

Kaspersky Security for Windows Server components and functions

The application includes the following components:

- **Real-Time File Protection**. Kaspersky Security for Windows Server scans objects when they are accessed. Kaspersky Security for Windows Server scans the following objects:
  - Files
  - Alternate file system streams (NTFS streams)
  - Master boot record and boot sectors on local hard and removable drives
- **On-Demand Scan**. Kaspersky Security for Windows Server runs a single scan of the specified area for viruses and other computer security threats. Application scans files, RAM, and startup objects on a protected server.
- **Applications Launch Control**. The component tracks users' attempts to launch applications and controls applications launches.

- **RPC Network Storage Protection** and **ICAP Network Storage Protection**. Kaspersky Security for Windows Server installed on a server under a Microsoft Windows operating system protects network attached storages against viruses and other security threats that infiltrate the server through exchange of files.
- **Device Control**. The component controls registration and usage of mass storage devices and CD/DVD drives in order to protect the computer against security threats that may arise while exchanging files with USB-connected flash drives or other types of external device.
- **Anti-Cryptor** and **Anti-Cryptor for NetApp**. The components protect shared folders on servers and network attached storages from malicious encryption, by blocking the hosts that show malicious activity.
- **Script Monitoring**. This component controls the execution of scripts created using Microsoft Windows Script Technologies.
- **Traffic Security**. This component intercepts and scans objects transferred through web traffic (including mail) to detect known computer and other threats on the protected server.
- **Firewall Management**. This component provides the ability to manage the Windows Firewall: configure settings and operating system firewall rules and block any possibility of external firewall configuration.
- **File Integrity Monitor**. Kaspersky Security for Windows Server detects changes in files within the monitoring scopes specified in the task settings. These changes may indicate a security breach on the protected server.
- **Log Inspection**. This component monitors the integrity of the protected environment based on the results of an inspection of Windows event logs.

The following functions are implemented in the application:

- **Database Update** and **Software Modules Update**. Kaspersky Security for Windows Server downloads updates of application databases and modules from FTP or HTTP update servers of Kaspersky Lab, Kaspersky Security Center Administration Server, or other update sources.
- **Quarantine**. Kaspersky Security for Windows Server quarantines probably infected objects by moving such objects from their original location to *Quarantine*. For security purposes, objects are stored in Quarantine in encrypted form.
- **Backup**. Kaspersky Security for Windows Server stores encrypted copies of objects classified as *Infected* or *Probably infected* in *Backup* before disinfecting or deleting them.
- **Administrator and user notifications**. You can configure the application to notify the administrator and users who access the protected server about events in Kaspersky Security for Windows Server operation and the status of Anti-Virus protection on the server.
- **Importing and exporting settings**. You can export Kaspersky Security for Windows Server settings to an XML configuration file and import settings into Kaspersky Security for Windows Server from the configuration file. You can save all application settings or only settings for individual components to a configuration file.
- **Applying templates**. You can manually configure a node's security settings in the tree or in a list of the computer file resources, and save the configured setting values as a template. This template can then be used to configure the security settings of other nodes in Kaspersky Security for Windows Server protection and scan tasks.
- **Managing access permissions for Kaspersky Security for Windows Server functions**. You can configure the rights to manage Kaspersky Security for Windows Server and the Windows services registered by the application, for users and groups of users.

- **Writing events to the application event log**. Kaspersky Security for Windows Server logs information about software component settings, the current status of tasks, events that occur while tasks run, events associated with Kaspersky Security for Windows Server management, and information required to diagnose errors in Kaspersky Security for Windows Server.
- **Hierarchical storage**. Kaspersky Security for Windows Server can operate in hierarchical storage management mode (HSM systems). HSM systems allow data relocation between fast local drives and slow long-term data storage devices.
- **Trusted Zone**. You can generate the list of exclusions from the protection or scan scope, that Kaspersky Security for Windows Server will apply in the on-demand and real-time protection tasks.
- **Exploit Prevention**. You can protect process memory from exploits using an Agent injected into the process.
- **Blocked Hosts**. You can block remote hosts that try to access the server's shared folders if any malicious activity is detected on their side.

Hardware and software requirements

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

In this chapter

Requirements for the server on which Kaspersky Security for Windows Server is deployed

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

Before installing Kaspersky Security for Windows Server 10.1, you must uninstall Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition. You can install Kaspersky Security for Windows Server 10.1 without uninstalling Kaspersky Security 10 for Windows Server or later.

Hardware requirements for the server

General requirements:

- x86/64-compatible single-core or multi-core systems
- disk space requirements:
  - for installing all application components: 100 MB
  - for downloading and storing anti-virus databases of the application: 2 GB (recommended)
  - for storing objects in Quarantine and in Backup: 400 MB (recommended)
  - for storing logs: 1 GB (recommended)

Minimum configuration:

- Processor: 1.4 GHz single-core
- RAM: 1 GB
- Drive subsystem: 4 GB of free space

Recommended configuration:

- Processor: 2.4 GHz quad-core
- RAM: 2 GB

- Drive subsystem: 4 GB of free space

Software requirements for the server

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

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

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

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

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

- Windows Server 2003 Standard / Enterprise / Datacenter SP2 or later
- Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 or later
- Windows Server 2008 Core Standard / Enterprise / Datacenter SP1 or later
- Windows Server 2008 Standard / Premium SP1 or later
- Microsoft Small Business Server 2008 Standard / Premium
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter SP1 or later
- Windows Server 2008 Core R2 Standard / Enterprise / Datacenter SP1 or later
- Windows Hyper-V Server 2008 R2 SP1 or later
- Microsoft Small Business Server 2011 Essentials / Standard
- Microsoft Windows MultiPoint™ Server 2011 Standard / Premium
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter
- Windows Server 2012 Core Foundation / Essentials / Standard / Datacenter
- Microsoft Windows MultiPoint™ Server 2012 Standard / Premium
- Windows Storage Server 2012
- Windows Hyper-V Server 2012
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter
- Windows Server 2012 Core R2 Foundation / Essentials / Standard / Datacenter
- Windows Storage Server 2012 R2
- Windows Hyper-V Server 2012 R2
- Windows Server 2016 Essentials / Standard / Datacenter
- Windows Server 2016 MultiPoint
- Windows Server 2016 Core Standard / Datacenter

- Microsoft Windows MultiPoint™ Server 2016
- Windows Storage Server 2016
- Windows Hyper-V Server 2016
- Windows Server 2019 Essentials / Standard / Datacenter
- Windows Server 2019 Core
- Windows Storage Server 2019
- Windows Hyper-V Server 2019

The following operating systems are no longer supported by Microsoft Windows: Windows Server 2003 Standard / Enterprise / Datacenter SP2, Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 32-bit, 64-bit. There might be limitations for the technical support of servers running these operating systems on the Kaspersky Lab side.

You can install Kaspersky Security for Windows Server on the following terminal servers:

- Microsoft Remote Desktop Services based on Windows Server 2008
- Microsoft Remote Desktop Services based on Windows Server 2008 R2
- Microsoft Remote Desktop Services based on Windows Server 2012
- Microsoft Remote Desktop Services based on Windows Server 2012 R2
- Microsoft Remote Desktop Services based on Windows Server 2016
- Microsoft Remote Desktop Services based on Windows Server 2019
- Citrix XenApp 6.0, 6.5, 7.0, 7.5 - 7.9, 7.15
- Citrix XenDesktop 7.0, 7.1, 7.5 - 7.9, 7.15

The Kaspersky Security for Windows Server is compatible with the following versions of Kaspersky Security Center:

- Kaspersky Security Center 10.4
- Kaspersky Security Center 10.5
- Kaspersky Security Center 11

Requirements for the protected network attached storage

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

- NetApp with one of the following operating systems:
  - Data ONTAP 7.x and Data ONTAP 8.x in 7-mode
  - Data ONTAP 8.2.1 in cluster-mode
  - Data ONTAP 9.0 in cluster-mode
  - Data ONTAP 9.1 in cluster-mode

  - Data ONTAP 9.2 in cluster-mode
  - Data ONTAP 9.3 in cluster-mode
  - Data ONTAP 9.4 in cluster-mode
- Dell™ EMC™ Celerra™ / VNX™ with the following software:
  - EMC DART 6.0.36 or higher
  - Celerra Antivirus Agent (CAVA) 4.5.2.3 or higher
- Dell EMC Isilon™ with the operating system OneFS™ 7.0 or later
- Hitachi/HNAS (ICAP, RPC):
  - 12.0 or later for integration via ICAP
  - 11.2 or later for integration via RPC
- IBM System Storage N series
- Oracle® ZFS Storage Appliance
- Dell NAS on the platform Dell Compellent™ FS8600:
  - FluidFS 6.x
  - FluidFS 5.x
- HPE 3PAR with File Persona 3.3.1:
  - HPE 3PAR STORESERV File Controller
  - HPE 3PAR STORESERV 7000c, 8000, 9000, 20000 Storage

Requirements for the computer on which the Application Console is installed

Hardware requirements for the computer

Recommended RAM amount: at least 128 MB.

Free disk space: 30 MB.

Software requirements for the computer

You can install the Application 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 the Application Console.

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

- Windows Server 2003 Standard / Enterprise / Datacenter SP2 or later
- Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 or later
- Windows Server 2008 Standard / Enterprise / Datacenter SP1 or later
- Microsoft Windows XP Professional SP2 or later

- Microsoft Windows Vista®
- Microsoft Windows 7
- Microsoft Windows 8
- Microsoft Windows 8.1
- Microsoft Windows 10
- Windows 10 Redstone 1
- Windows 10 Redstone 2
- Windows 10 Redstone 3
- Windows 10 Redstone 4
- Windows 10 Redstone 5
- Windows 10 Redstone 6

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

- Windows Server 2003 Standard / Enterprise / Datacenter SP2 or later
- Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 or later
- Windows Server 2008 Core / Standard / Enterprise / Datacenter SP1 or later
- Microsoft Small Business Server 2008 Standard / Premium
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter SP1 or later
- Windows Hyper-V Server 2008 R2 SP1 or later
- Microsoft Small Business Server 2011 Essentials / Standard
- Microsoft Windows MultiPoint Server 2011 Standard / Premium
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter
- Microsoft Windows MultiPoint Server 2012 Standard / Premium
- Windows Storage Server 2012 Foundation / Essentials / Standard / Datacenter
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter
- Windows Storage Server 2012 R2
- Windows Hyper-V Server 2012
- Windows Hyper-V Server 2012 R2
- Windows Server 2016 Essentials / Standard / Datacenter
- Microsoft Windows MultiPoint Server 2016
- Windows Storage Server 2016 Essentials / Standard / Datacenter
- Windows Server 2019 Essentials / Standard / Datacenter
- Windows Storage Server 2019
- Microsoft Windows XP Professional Edition SP2 or later
- Microsoft Windows Vista

- Microsoft Windows 7
- Microsoft Windows 8
- Microsoft Windows 8.1
- Microsoft Windows 10
- Windows 10 Redstone 1
- Windows 10 Redstone 2
- Windows 10 Redstone 3
- Windows 10 Redstone 4
- Windows 10 Redstone 5
- Windows 10 Redstone 6

Integrating Kaspersky Security for Windows Server with network attached storages

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

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

Kaspersky Security for Windows Server interacts with an EMC network attached storage of the Celerra / VNX group using CAVA (Celerra Antivirus Agent) running on the computer with Kaspersky Security for Windows Server installed. When running, Kaspersky Security for Windows Server checks the computer for installed CAVA, which must meet the requirements of Kaspersky Security for Windows Server.

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

RPC Network Storage Protection

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

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

ICAP Network Storage Protection

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

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

Preparing for launch of the Network Attached Storage Protection task

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

If you are planning to use Network Attached Storage Protection on the server running the Microsoft Windows Server 2019 operating system, make sure that the SMB1.0/CIFS File Sharing Support feature is installed. Detailed information about can be found in the Microsoft Windows documentation and corresponding online resources.

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

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

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

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

        The Management Console window opens.
     b. In the window that opens, select **File** > **Add or remove a snap-in**.

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

        The **Group Policy Wizard** starts.
     d. In the Wizard window, click the **Browse** button.

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

   The changes will be saved.
3. Select **Computer configuration** > **Windows configuration** > **Security settings** > **Local policies** > **Security settings**.

4. Specify the following values for network access settings:
    - **Network access: Let For everyone permissions apply to anonymous users – Enabled**
    - **Network access: Do not allow anonymous enumeration of SAM accounts – Disabled**
    - **Network access: Restrict anonymous access to named pipes and shares – Disabled**
5. Restart the server with Kaspersky Security for Windows Server installed.

The applied changes take effect.

Configuring inbound and outbound connections in Windows firewall

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

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

1. Open the settings window of Windows firewall in one of the following ways:
    - If you configure Windows firewall locally, click the **Start** button, enter the `wf.msc` command at the search bar, and press **ENTER**.
    - If you configure Windows firewall from another computer:
        a. Click the **Start** button, enter the `mmc` command at the search bar, and press **ENTER**.

        The **Management Console** window opens.

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

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

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

        The **Select computer window** opens.

        d. In the window that opens, select **Another computer** and specify a server with Kaspersky Security for Windows Server installed, using one of the following methods:
            - In the entry field, specify the domain name of a server with Kaspersky Security for Windows Server installed
            - Click the **Browse** button and, in the integrated security subject selection window that opens, select a server with Kaspersky Security for Windows Server installed, using search by domain or by workgroup.
2. Click **OK**.

    The changes will be saved.
3. Create rules for inbound and outbound connections with the following settings:
    - Allow inbound connections from all remote ports to local ports TCP 137 – 139, TCP 445.
    - Allow outbound connections from all local ports to remote ports TCP 137 – 139, TCP 445.

    If all outbound connections are denied, open the following ports: TCP 443 (RPC(HTTP)), TCP 445 (SMB), TCP 88 (Kerberos), TCP 53 (DNS), UDP 53 (DNS).

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

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

Managing Kaspersky Security for Windows Server Console

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

In this chapter

About the Kaspersky Security for Windows Server Console

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

The application can be managed via the Application Console installed on the protected server or on another computer on the corporate network.

Detailed information about installation and configuration of the Application Console is provided in the *Kaspersky Security for Windows Server Administrator's Guide*.

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

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

You can start the Application Console from the **Start** menu. The Kaspersky Security for Windows Server snap-in msc-file can be run or the Kaspersky Security for Windows Server snap-in can be added to the existing Microsoft Management Console as a new element in the tree.

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

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

Starting the Kaspersky Security for Windows Server Console from Start menu

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

► *To start the Application Console from the **Start** menu:*

in the **Start** menu select **All Programs** > **Kaspersky Security for Windows Server** > **Administration Tools** > **Kaspersky Security for Windows Server Console**.

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

► *To start the Application Console in author mode, take the following steps:*

1. In the **Start** menu select **Programs** > **Kaspersky Security for Windows Server** > **Administration Tools**.
2. In the context menu of the Application Console, select the **Author** command.

The Application Console is started in author mode.

If the Application Console has been started on the protected server, the Application Console window opens.

If you have started the Application Console not on a protected server but on a different one, connect to the protected server.

► *To connect to a protected server:*

1. In the Application Console tree, open the context menu of the **Kaspersky Security** node.
2. Select the **Connect to another computer** command.

   The **Select computer** window opens.
3. Select **Another computer** in the window that opens.
4. Specify the network name of the protected server in the entry field on the right.
5. Click **OK**.

The Application Console will be connected to a protected server.

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

Kaspersky Security for Windows Server Console interface

The Kaspersky Security for Windows Server Console is displayed in the Microsoft Management Console tree in the form of a node with the name Kaspersky Security.

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

By default, the Application Console window includes the following elements:

- Application Console tree
- Details pane
- Toolbar

The Application Console tree

The Application Console tree displays the **Kaspersky Security** node and the child nodes of functional components of the application.

The **Kaspersky Security** node includes the following child nodes:

- **Real-Time Server Protection**: manages real-time protection tasks and KSN services. The **Real-Time Server Protection** node allows to configure the following tasks:
  - **Real-Time File Protection**
  - **Script Monitoring**
  - **KSN Usage**
  - **Traffic Security**
  - **Anti-Cryptor**
- **Server Control**: controls launches of applications installed on a protected server, as well as external devices connections. The **Server Control** node allows to configure the following tasks:
  - **Applications Launch Control**
  - **Device Control**
  - **Firewall Management**
- **Automated rule generators**: configuring automatic generation of group and system rules for the Applications Launch Control task and the Device Control task.
  - **Rule Generator for Applications Launch Control**
  - **Rule Generator for Device Control**
  - Rule generation group tasks **<Task names>** (if any)

    Group tasks are created using Kaspersky Security Center. You cannot manage group tasks through the Application Console.
- **System Inspection**: configuring file operations control and Windows Event Log inspection settings.
  - **File Integrity Monitor**

    - **Log Inspection**
- **Network Attached Storage Protection**: configure the network storage protection tasks.
    - **RPC Network Storage Protection**
    - **ICAP Network Storage Protection**
    - **Anti-Cryptor for NetApp**
- **On-Demand Scan**: manages On-Demand Scan tasks. There is a separate node for each task:
    - **Scan at Operating System Startup**
    - **Critical Areas Scan**
    - **Quarantine Scan**
    - **Application Integrity Control**
    - Custom tasks **<Task names>** (if any)

    The node displays system tasks created when the application is installed, custom tasks, and group on-demand scan tasks created and sent to a computer using Kaspersky Security Center.
- **Update**: manages updates for Kaspersky Security for Windows Server databases and modules and copies the update to a local update source folder. The node contains child nodes for administering each update task and the last Rollback of Database Update task:
    - **Database Update**
    - **Software Modules Update**
    - **Copying Updates**
    - **Rollback of Database Update**

    The node displays all custom and group update tasks created and sent to a computer using Kaspersky Security Center.
- **Storages**: Management of Quarantine, Backup and Blocked Hosts settings.
    - **Quarantine**
    - **Backup**
    - **Blocked Hosts**
- **Logs and notifications**: manages local task logs, Security log and Kaspersky Security for Windows Server System audit log.
    - **Security log**
    - **System audit log**
    - **Task logs**
- **Licensing**: add or delete Kaspersky Security for Windows Server keys and activation codes, view license details.

Details pane

The details pane displays information about the selected node. If the **Kaspersky Security** node is selected, the details pane displays information about the current server protection status and information about Kaspersky Security for Windows Server, the protection status of its functional components, and the license expiration date.

Context menu of the Kaspersky Security node

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

- **Connect to another computer**. Connect to another computer to manage Kaspersky Security for Windows Server installed on it. You can also perform this operation by clicking the link in the lower right corner of the details pane of the **Kaspersky Security** node.
- **Start the service** / **Stop the service**. Start or stop application or a selected task. To carry out these operations, you can also use the buttons on the toolbar. You can also perform these operations in context menus of application tasks.
- **Configure removable drives scan settings**. Configure scanning of removable drives connected to the protected server via the USB port.
- **Exploit Prevention: general settings**. Configure the Exploit Prevention mode and set up preventing actions.
- **Exploit Prevention: processes protection settings**. Add processes for protection and select the exploit prevention techniques.
- **Configure Trusted Zone settings**. View and configure Trusted Zone settings.
- **Modify user rights of the application management**. View and configure permissions to access Kaspersky Security for Windows Server functions.
- **Modify user rights of Kaspersky Security Service management**. View and configure user rights to manage Kaspersky Security Service.
- **Hierarchical storage**. Configure access method of the HSM system.
- **Export settings**. Save the application settings in a configuration file in XML format. You can also perform this operation in context menus of application tasks.
- **Import settings**. Import application settings from a configuration file in XML format. You can also perform this operation in context menus of application tasks.
- **Information about the application and available module updates**. See information about Kaspersky Security for Windows Server and currently available application modules updates.
- **Refresh**. Refresh the contents of the Application Console window. You can also perform this operation in context menus of application tasks.
- **Properties**. View and configure settings of Kaspersky Security for Windows Server or a selected task. You can also perform this operation in context menus of application tasks.

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

- **Help**. View information Kaspersky Security for Windows Server Help. You can also perform this operation in context menus of application tasks.

Toolbar and context menu of Kaspersky Security for Windows Server tasks

You can manage Kaspersky Security for Windows Server tasks using the items of context menus of each task in the Application Console tree.

You can use the items of the context menu to perform the following operations:

- **Resume** / **Pause**. Resume or pause task execution. To carry out these operations, you can also use the buttons on the toolbar. This operation is available for the Real-Time Protection tasks and the On-Demand Scan tasks.
- **Add task**. Create new custom task. This operation is available for On-demand scan tasks.
- **Open log**. View and manage a task log. This operation is available for all tasks.
- **Save task**. Save and apply modified task settings. This operation is available for Real-Time File Protection and On-Demand Scan tasks.
- **Remove task**. Delete custom task. This operation is available for On-demand scan tasks.
- **Statistics**. View task statistics. This operation is available for the Application Integrity Control task.
- **Settings templates**. Manage templates. This operation is available for Real-Time File Protection and On-Demand Scan.

Viewing status information for Network Attached Storage Protection

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

select the **Kaspersky Security** node in the Application Console tree.

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

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

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

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

Information about the status of protected network attached storages is displayed in the details pane of the **Kaspersky Security** node on the **Network Attached Storage Protection** tab.

The **Real-Time Protection** section displays information about the RPC and ICAP Network Storage Protection tasks, and the Celerra / VNX integration status (see table below).

Table 2. Information about network storage protection

Network Attached Storage Protection section	Information

Network Attached Storage Protection status indicator	The color of the panel with the name of the section reflects the status of tasks described in the section. The indicator can take the following values:
	• *Green* is displayed in the following case: RPC Network Storage Protection and ICAP Network Storage Protection tasks are running.
	• *Yellow* is displayed in the following cases:
	  ◦ One of the following tasks is running: RPC Network Storage Protection or ICAP Network Storage Protection.
	  ◦ Celerra / VNX Anti-Virus Agent is found.
	• *Red* is displayed in the following case: no protection tasks are running and Celerra / VNX Anti-Virus Agent is found.

RPC Network Storage Protection	**Task status** field displays current task status, for example, Running or Stopped. **Detected** field displays the number of malicious objects detected on RPC network storage shared folders. If the number of detected software exceeds 0, the row value is highlighted in red.
ICAP Network Storage Protection	**Task status** field displays current task status, for example, Running or Stopped. **Detected** field specifies the number of malicious objects detected on ICAP network storage shared folders. If the number of detected software exceeds 0, the row value is highlighted in red.
Connection to EMC Celerra / VNX	The following values are possible: • **Celerra / VNX Anti-Virus Agent not found**. Kaspersky Security for Windows Server cannot find any EMC software, or an error has occurred in the integration code. • **Protection disabled**. Kaspersky Security for Windows Server has established a connection to EMC software, but the Real-Time File Protection task is not running in Kaspersky Security for Windows Server. • **Protection enabled**. Kaspersky Security for Windows Server has established a connection to EMC software, and the Real-Time File Protection task is running in Kaspersky Security for Windows Server.

The **Anti-Cryptor protection** section (see the table below) displays information about the Anti-Cryptor for NetApp task status.

Table 3. Information about Anti-Cryptor protection status

Control section	Information
Anti-Cryptor protection status indicator	The color of the panel with the name of the section reflects the status of tasks being performed in the section. The indicator can take the following values: • Green color of the panel – the Anti-Cryptor for NetApp task is running. • Red color of the panel – the Anti-Cryptor for NetApp task is not running.
Anti-Cryptor for NetApp	**Task status** – current task status, for example, *Running* or *Stopped*. **Mode** – one of the two available modes for the Anti-Cryptor for NetApp task. **Hosts blocked** – the number of compromised hosts that were blocked when attempting to access the network shared folders on the protected server.

Managing Network Attached Storage Protection tasks

This section provides information about Kaspersky Security for Windows Server tasks: how to create, start and stop tasks manually or automatically, and define task settings.

Saving a task after changing its settings

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

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

► *To save modified task settings,*

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

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

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

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

Starting / pausing / resuming / stopping tasks manually

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

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

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

Managing task schedules

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

Configuring the task launch schedule settings

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

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

1. Open the context menu of the name of the task for which you wish to configure the launch schedule.
2. Select **Properties**.
3. The **Task settings** window opens.
4. In the window that opens, on the **Schedule** tab, select the **Run by schedule** check box.

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

5. Configure schedule settings in accordance with your requirements. To do this, perform the following actions:
   a. In the **Frequency** list, select one of the following values:
      - **Hourly**, if you want the task to run every hour for a specified number of hours; specify the number of hours in the **Every <number> hour(s)** field.
      - **Daily**, if you want the task to run every day for a specified number of days; specify the number of days in the **Every <number> day(s)** field.
      - **Weekly**, if you want the task to run every week for a specified number of weeks; specify the number of weeks in the **Every <number> week(s)** field Specify the days of the week on which the task will be launched (by default the task is launched on Mondays).
      - **At application launch**, if you want the task to run every time Kaspersky Security for Windows Server starts.
      - **After application database update**, if you want the task to run after every update of the application databases.

   b. Specify the time for the first task launch in the **Start time** field.
   c. In the **Start date** field, specify the date from which the schedule applies.

   After the task startup frequency has been specified, the time of the first task launch, and the date from which the schedule applies, information about the calculated time for the next task launch will appear in the top part of the window in the Next start field. Updated information about the estimated time of the next task launch will be displayed each time you open the Task settings window of the Schedule tab.
   The Blocked by policy value is displayed in the Next start field if the active policy settings of Kaspersky Security Center prohibit launching scheduled system tasks.

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

- In the **Task stop settings** section:
  a. Select the **Duration** check box and enter the required number of hours and minutes in the fields to the right to specify the maximum duration of the task execution.
  b. Select the **Pause from** check box and enter the start and end values of the time interval in the fields to the right to specify the interval of time in days during which task execution will be paused.
- In the **Advanced settings** section:
  a. Select the **Cancel schedule from** check box and specify the date from which the schedule will cease to operate.
  b. Select the **Run skipped tasks** check box to enable the launch of skipped tasks.
  c. Select the **Randomize the task start within interval of** check box and specify the value in minutes.

7. Click the **Apply** button.

The configured task launch settings will be saved.

Enabling and disabling scheduled tasks

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

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

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

   The **Task settings** window opens.
3. In the window that opens on the **Schedule** tab, do one of the following:
   - Select the **Run by schedule** check box if you want to enable the scheduled launch of the task
   - Select the **Run by schedule** check box if you want to enable scheduled task launch

   The configured task launch schedule settings are not deleted and will be applied at the next scheduled launch of the task.
4. Click the **Apply** button.

The configured task launch schedule settings are saved.

Protecting EMC network attached storages of the Celerra / VNX group

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

In this chapter

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

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

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

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

By default, Kaspersky Security for Windows Server performs the following operations:

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

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

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

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

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

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

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

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

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

The status of Kaspersky Security for Windows Server (see Section "Viewing status information for Network Attached Storage Protection" on page 29) integration with the Celerra / VNX network attached storage is shown in the details pane of the **Kaspersky Security** node.

RPC Network Storage Protection

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

In this chapter

About the RPC Network Storage Protection

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

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

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

By default, Kaspersky Security for Windows Server performs the following operations:

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

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

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

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

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

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

The RPC Network Storage Protection component is available within Kaspersky Security for Windows Server for Network attached storages.

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

About scanning symbolic links

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

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

About scanning snapshots and other read-only volumes and folders

Kaspersky Security for Windows Server scans files stored in snapshots and other volumes and folders that are set up in read-only mode, but does not perform any actions on files in those volumes and folders: for example, it does not block access to infected files. To prevent any risk of infection of workstations, you are recommended

to mark snapshots and other volumes and folders in read-only mode as hidden form users and provide access to snapshots and other volumes and folders in read-only mode by requesting the administrator.

Configuring a connection between an RPC network storage and Kaspersky Security for Windows Server

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

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

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

1. Configure the following settings on the server with Kaspersky Security for Windows Server installed:
   - Add a network attached storage to Kaspersky Security for Windows Server (see Section "Adding an RPC network storage to Kaspersky Security for Windows Server" on page 40).
   - In Kaspersky Security for Windows Server Console, specify the user account under which you want to run the RPC Network Storage Protection task (see Section "Selecting a user account for running the RPC Network Storage Protection task" on page 39).
   - In the local group policy editor, configure the security settings of local policies (see Section "Configuring security settings of local policies in the local group policy editor" on page 21).
   - In the Windows firewall settings window, configure the rules of outbound and inbound connections in Windows firewall (see Section "Configuring inbound and outbound connections in Windows firewall" on page 22).
   - If necessary, install a connector application for the RPC network storage to be protected by Kaspersky Security for Windows Server.

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

2. In the network attached storage, configure the following settings:
   - Enable the anti-virus protection feature (vscan).
   - Add the user account under which the RPC Network Storage Protection task must be run to the Backup Operators group.

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

The connection between an RPC network storage and Kaspersky Security for Windows Server is established.

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

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

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

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

If more than one user account exists on the Kaspersky Security for Windows Server side, make sure the user under which you configure and start the RPC Network Storage Protection task is added to the privileged users list for working with NetApp. If the user account does not have required privileges, files on the network attached storage shared folders can be accessed, but no scanning will be performed by the running protection tasks.

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

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

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

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

Creating the protection scope in the RPC Network Storage Protection task

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

In this section

Adding an RPC network storage to Kaspersky Security for Windows Server

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

1. Expand the **Network Attached Storage Protection** node in the Application Console tree.
2. Select the **RPC Network Storage Protection** child node.
3. In the details pane of the **RPC Network Storage Protection** node, click the **Configure protection scope** link.
4. In the window that opens, click the **Add** button.

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

   If you are using a NetApp storage system managed by NetApp Clustered Data ONTAP operating system, fill in this field by specifying the IP address of the computer on which the connector application is installed, i.e. 127.0.0.1.
6. Click **OK** to add the network attached storage to Kaspersky Security for Windows Server.

   The network attached storage appears in the list of protected network attached storages.
7. Click the **Save** button.

The configured protection scope settings are saved.

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

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

Disabling and enabling protection of an added RPC network storage

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

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

Kaspersky Security for Windows Server interrupts the connection with the selected network attached storage.

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

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

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

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

Removing an RPC network storage from the protection scope

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

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

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

Configuring the RPC Network Storage Protection task

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

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

Table 4. Settings of the RPC Network Storage Protection task

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

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

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

   The **Task settings** window opens.
4. On the **General** tab in the window that opens, configure the following task settings:
   - Using the Heuristic Analyzer (on page 43).
   - Task launch with user account permissions (see Section "Selecting a user account for running the RPC Network Storage Protection task" on page 39).
   - Connection to an PRC network storage (see Section "Configuring general settings for RPC Network Storage connection" on page 45).
   - Integration with other Kaspersky Security for Windows Server components (see Section "Preparing for launch of the Network Attached Storage Protection task" on page 21).

5. On the **Schedule** and **Advanced** tabs, configure the scheduled task launch settings (see Section "Configuring the task launch schedule settings" on page 32).
6. Click **OK** in the **Task settings** window.

   The modified settings are saved.
7. In the details pane of the **RPC Network Storage Protection** node, select the **Protection scope settings** tab.
8. Do the following:
   - Add network attached storage via RPC protocol to the protection scope (see Section "Adding an RPC network storage to Kaspersky Security for Windows Server" on page 40) of Kaspersky Security for Windows Server.
   - In the list of added network attached storages connected via the PRC protocol, select the network attached storages whose protection you want to activate.
   - Select one of the preset security levels (see Section "Applying a preset security level in the RPC Network Storage Protection task" on page 47) or configure the security settings of objects manually (see Section "Manually configuring the security level settings in the RPC Network Storage Protection task" on page 48).
9. Click **OK** in the **Task settings** window.

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

Using the Heuristic Analyzer

The ICAP Network Storage Protection task can use heuristic analyzer with a configured level of analysis.

► *To configure the settings of heuristic analyzer used in the ICAP Network Storage Protection task:*

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

   The **Task settings** window opens.

4. In the window that opens, go to the **General** tab and do the following in the **Heuristic analyzer** section:
   - Clear or select the **Use heuristic analyzer** check box.
   - If necessary, adjust the level of analysis using the slider.

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

     The following scanning intensity levels are available:

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

and less resource-intensive.

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

  This level is selected by default.

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

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

5. Click **OK**.

The newly configured settings are applied.

Integration with other components of Kaspersky Security for Windows Server

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

- Trusted zone
- KSN Usage task

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

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

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

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

To start the KSN Usage task, you must accept the Kaspersky Security Network Statement.

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

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

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

   The **Task settings** window opens.

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

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

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

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

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

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

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

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

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

The newly configured settings are saved.

Configuring general settings for RPC Network Storage connection

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

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

   The **Task settings** window opens.
4. In the window that opens, go to the **General** tab and do the following in the Network attached storage systems connection settings section:
   - Enter a value for the timeout between attempts to recover the connection with the network attached storage.
   - Enter a value for the maximum number of attempts to recover the connection with the network attached storage.

     It is recommended to keep default values or specify larger values.
   - If you want Kaspersky Security for Windows Server to clear the cache of scanned files of the network attached storage after each update of the application databases, select the **Clear cache of scanned files on network attached storage after application database update** check box.

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

5. Click **OK**.

The newly configured settings are saved.

Security levels in the RPC Network Storage Protection task

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

About security levels in the RPC Network Storage Protection task

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

Maximum performance

The **Maximum performance** security level is recommended if, apart from using Kaspersky Security for Windows Server 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 5. Settings of preset security levels in the RPC Network Storage Protection task

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

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

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

1. Expand the **Network Attached Storage Protection** node in the Application Console tree.
2. Select the **RPC Network Storage Protection** child node.
3. In the details pane of the **RPC Network Storage Protection** node, click the **Configure protection scope** link.
4. In the list of protected network attached storages, select the network attached storage for which you want to select a preset security level.
5. On the **Security level** tab, select one of the following preset security levels in the list:
   - **Maximum Protection**
   - **Recommended**
   - **Maximum performance**

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

6. Click the **Save** button.

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

You can also configure the security settings for a protected network attached storage manually (see Section "Manually configuring the security level settings in the RPC Network Storage Protection task" on page 48).

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

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

1. Expand the **Network Attached Storage Protection** node in the Application Console tree.
2. Select the **RPC Network Storage Protection** child node.
3. In the details pane of the **RPC Network Storage Protection** node, click the **Configure protection scope** link.
4. In the list of protected network attached storages, select the network attached storage whose security settings you want to configure.

   You can apply a preset security settings template.

5. Configure the settings of the selected network attached storage in accordance with your computer security requirements. To do this, perform the following actions:
   - On the **General** tab take the following actions:
     - In the **Objects protection** section, specify objects to be scanned by Kaspersky Security for Windows Server:
       - **All objects**.

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

         Kaspersky Security for Windows Server scans only infectable objects based on file format.

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

         Kaspersky Security for Windows Server scans only infectable objects based on file extension.

         Kaspersky Lab compiles the list of extensions. It is included in the Kaspersky Security for Windows Server databases.
       - **Objects scanned by specified list of extensions**.

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

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

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

- On the **Actions** tab take the following actions:
  - In the **Action to perform on infected and other objects** section, select the action to be performed by Kaspersky Security for Windows Server on detecting an infected object.
  - In the **Action to perform on probably infected objects** section, select the action to be performed by Kaspersky Security for Windows Server on detecting a probably infected object.
  - Configure actions to be performed on objects depending on the type of object detected.
  - Select the actions to perform on unmodifiable compound files: select or clear the **Entirely remove compound file that cannot be modified by the application in case of embedded object detection** check box.

    This check box enables or disables forced removal of the parent compound file when a malicious, probably infected or other detected child embedded object is detected.

    If the check box is selected and the task is configured to remove infected and probably infected objects, Kaspersky Security for Windows Server forcibly removes the entire parent compound object when a malicious or other embedded object is detected.Enforced removal of a parent file along with all of its contents happens if the application cannot remove only the detected child object (for example, if the parent object is unmodifiable).

    If this check box is cleared and the task is configured to remove infected and probably infected objects, Kaspersky Security for Windows Server does not perform the selected action, if the parent object is unmodifiable.

    By default, the check box is selected for the **Maximum protection** security level and cleared for the **Recommended** and **Maximum performance** security levels.

- On the **Performance** tab take the following actions:
  - In the **Exclusions** section, specify objects that you want Kaspersky Security for Windows Server to exclude from scanning:
    - To exclude files from scanning, select the **Exclude files** check box and specify the names or name masks of files to be excluded.

- To exclude detectable objects (such as remote administration utilities), select the **Do not detect** check box and specify the names or name masks of detectable objects, according to the Virus Encyclopedia http://www.securelist.com classification.

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

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

6. Click the **Save** button.

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

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

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

Creating a security settings template

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

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

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

The template with the set of security settings is saved.

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

Applying a security settings template

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

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

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

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

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

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

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

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

Viewing security settings in a template

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

1. In the Application Console tree, select the task for which you want to view the security template.
2. In the context menu of the selected task, select **Settings templates**.

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

The **Templates** window opens.

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

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

Deleting a security settings template

► *To delete a security settings template:*

1. In the Application Console tree, select the task for which you no longer want to use a security settings template for configuration.
2. In the context menu of the selected task, select **Settings templates**.

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

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

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

The selected template will be deleted.

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

Viewing statistics of the RPC Network Storage Protection task

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

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

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

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

Table 6. Full statistics of the RPC Network Storage Protection task

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

ICAP Network Storage Protection

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

In this chapter

About the ICAP Network Storage Protection

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

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

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

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

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

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

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

The ICAP Network Storage Protection component is available within Kaspersky Security for Windows Server for network attached storages.

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

Configuring a connection between an ICAP network storage and Kaspersky Security for Windows Server

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

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

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

1. Configure the following settings on the server with Kaspersky Security for Windows Server installed:
   - In Application Console, specify the settings of the connection to an ICAP network storage (see Section "Configuring the settings of the connection to an ICAP network storage" on page 57) to be protected by Kaspersky Security for Windows Server.
   - In the local group policy editor, configure the security settings of local policies (see Section "Configuring security settings of local policies in the local group policy editor" on page 21).
   - In the Windows firewall settings window, configure the rules of outbound and inbound connections in Windows firewall (see Section "Configuring inbound and outbound connections in Windows firewall" on page 22).
2. In the network attached storage, configure the following settings:
   - Enable anti-virus protection.
   - Specify the address of the connection to Kaspersky Security for Windows Server in the network attached storage settings.

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

The connection between an ICAP network storage and Kaspersky Security for Windows Server is established.

Configuring the ICAP Network Storage Protection task

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

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

Table 7. Settings of the ICAP Network Storage Protection task

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

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

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

   The **Task settings** window opens.
4. On the **General** tab in the window that opens, configure the following task settings:
   - Connection to an ICAP network storage (see Section "Configuring the settings of the connection to an ICAP network storage" on page 57).
   - Using the Heuristic Analyzer (on page 58).

- KSN Usage for protection (see Section "Using KSN for protection" on page 58).

In the **Security level** section:

- Select one of the preset security levels (see Section "About security levels in the ICAP Network Storage Protection task" on page 59) or configure the security settings of objects manually (see Section "Manually configuring the security level settings in the ICAP Network Storage Protection task" on page 61).

5. On the **Schedule** and **Advanced** tabs, configure the scheduled task launch settings (see Section "Managing task schedules" on page 32).
6. Click **OK**.

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

Configuring the settings of the connection to an ICAP network storage

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

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

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

     The number of the ICAP server network port used to connect the network attached storage to the application.
   - **Service ID**.

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

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

The newly configured settings are saved.

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

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

Using the Heuristic Analyzer

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

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

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

   The **Task settings** window opens.
4. In the window that opens, go to the **General** tab and do the following in the **Heuristic analyzer** section:
   - Clear or select the **Use heuristic analyzer** check box.
   - If necessary, adjust the level of analysis using the slider.

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

     The following scanning intensity levels are available:

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

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

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

The newly configured settings are applied.

Using KSN for protection

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

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

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

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

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

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

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

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

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

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

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

The newly configured settings are saved.

Security levels in the ICAP Network Storage Protection task

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

About security levels in the ICAP Network Storage Protection task

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

Maximum performance

The **Maximum performance** security level is recommended if, apart from using Kaspersky Security for Windows Server 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 8. Settings of preset security levels in the ICAP Network Storage Protection task

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

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

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

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

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

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

You can also configure the security settings for a protected network attached storage manually (see Section "Manually configuring the security level settings in the ICAP Network Storage Protection task" on page 61).

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

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

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

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

   The **Security settings** window opens.
5. Configure the settings in accordance with your computer security requirements. To do this, perform the following actions:
   - On the **General** tab take the following actions:
     - In the **Objects protection** section, specify objects to be scanned by Kaspersky Security for Windows Server:
       - **All objects**.

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

         Kaspersky Security for Windows Server scans only infectable objects based on file format.

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

         Kaspersky Security for Windows Server scans only infectable objects based on file extension.

         Kaspersky Lab compiles the list of extensions. It is included in the Kaspersky Security for Windows Server databases.
       - **Objects scanned by specified list of extensions**.

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

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

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

- On the **Actions** tab take the following actions:
  - In the **Action to perform on infected and other objects** section, select the action to be performed by Kaspersky Security for Windows Server on detecting an infected object.
  - In the **Action to perform on probably infected objects** section, select the action to be performed by Kaspersky Security for Windows Server on detecting a probably infected object.
  - Configure actions to be performed on objects depending on the type of object detected.
- On the **Performance** tab take the following actions:
  - In the **Exclusions** section, specify objects that you want Kaspersky Security for Windows Server to exclude from scanning:
    - To exclude files from scanning, select the **Exclude files** check box and specify the names or name masks of files to be excluded.
    - To exclude detectable objects (such as remote administration utilities), select the **Do not detect** check box and specify the names or name masks of detectable objects, according to the Virus Encyclopedia http://www.securelist.com classification.
  - In the **Advanced settings** section, specify the maximum duration of object scanning and the maximum size of the compound file being scanned.

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

   The **Security settings** window closes.

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

The configured custom security level settings are saved.

Viewing statistics of the ICAP Network Storage Protection task

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

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

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

2. Select the **ICAP Network Storage Protection** child node.

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

Table 9. Statistics of the RPC Network Storage Protection task

Field	Description
Detected	Number of objects detected by Kaspersky Security for Windows Server. For example, if Kaspersky Security for Windows Server detects one malware program in five files, the value in this field increases by one.
Infected and other objects detected	Number of objects that Kaspersky Security for Windows Server found and classified as infected or number of found legitimate software files, which were not excluded from the real-time protection and on-demand tasks scope and can be used by intruders to damage your computer.
Probably infected objects detected	Number of objects found by Kaspersky Security for Windows Server to be probably infected.
Objects not disinfected	Number of objects which Kaspersky Security for Windows Server did not disinfect for the following reasons: • The type of detected object cannot be disinfected. • An error occurred during disinfection.
Objects not moved to quarantine	The number of objects that Kaspersky Security for Windows Server attempted to quarantine but was unable to do so, for example, due to insufficient disk space.
Objects not removed	The number of objects that Kaspersky Security for Windows Server attempted but was unable to delete, because, for example, access to the object was blocked by another application.
Objects not scanned	The number of objects in the protection scope that Kaspersky Security for Windows Server failed to scan because, for example, access to the object was blocked by another application.
Objects not backed up	The number of objects the copies of which Kaspersky Security for Windows Server attempted to save in Backup but was unable to do so, for example, due to insufficient disk space.
Processing errors	Number of objects whose processing resulted in an error.
Objects disinfected	Number of objects disinfected by Kaspersky Security for Windows Server.
Moved to quarantine	Number of objects quarantined by Kaspersky Security for Windows Server.
Moved to Backup	The number of object copies that Kaspersky Security for Windows Server saved to Backup.
Objects removed	Number of objects deleted by Kaspersky Security for Windows Server.
Password-protected objects	Number of objects (archives, for example) that Kaspersky Security for Windows Server missed because they were password protected.
Corrupted objects	The number of objects skipped by Kaspersky Security for Windows Server as their format was corrupted.
Objects processed	Total number of objects processed by Kaspersky Security for Windows Server.

Anti-Cryptor for NetApp

This section provides information about the Anti-Cryptor for NetApp task and how to configure it.

In this section

About the Anti-Cryptor for NetApp

The Anti-Cryptor for NetApp provides encryption protection for the folders on the Network Attached Storages. If any malicious encrypting is detected, Kaspersky Security for Windows Server blocks access to the folders of the protected network attached storage.

To operate on network attached storage, Kaspersky Security for Windows Server must to be connected to a protected storage as an *external engine*. The connection implies receiving notifications about file operations that have been performed on a protected network attached storage by the external engine; analyzing the patterns on the file operations received and sending conclusions about the file activity (whether it can be estimated as an encryption attempt or not); blocking the compromised hosts. In order to start the Anti-Cryptor for NetApp task the server (with Kaspersky Security for Windows Server installed) must be specified as the primary FPolicy server on the network attached storage side. *FPolicy* is a file access notification framework that is used to monitor and manage file access events on Storage Virtual Machines (SVMs) with FlexVol volumes. The framework generates notifications that are sent to external FPolicy servers.

The Fpolicy is not supported for FlexGroup volumes, hence the Anti-Cryptor for NetApp component cannot be configured to protect the network attached storages with FlexGroup volumes.

Notifications from network attached storage to an external server are sent via the FPolicy protocol, only in a synchronous mode. The server analyzes each notification before allowing a file operation.

The external engine (Kaspersky Security for Windows Server) and a protected network attached storage are connected using the FPolicy protocol.

To configure the protection you need to:

1. Create and configure the FPolicy on the protected network attached storage side.
2. Specify Kaspersky Security for Windows Server as an FPolicy server on a protected network attached storage side. Kaspersky Security for Windows Server will be recognized as an external server.
3. Configure the Anti-Cryptor for NetApp task settings in Kaspersky Security for Windows Server.

To complete the required configuration you need the following data:

- SVM machine name.
- External server IP address and the name assigned to it.
- Full list of cluster nodes of the protected network attached storage along with their names.

- Cluster management interface address.
- Created FPolicy name.
- Port for establishing a secure connection between the protected network attached storage an the external server.
- Credentials (login and password):
  - for a user allowed to access network attached storage shared folders;
  - for the CDOT Local Administrator.

All these settings must be specified during the FPolicy creation (see Section "Creating and configuring FPolicy" on page 66) and when the Anti-Cryptor for NetApp task is configured on the Kaspersky Security for Windows Server (see Section "Configuring Anti-Cryptor for NetApp task settings" on page 70).

For detailed instructions on how to create the FPolicy please see the following article: https://library.netapp.com/ecmdocs/ECMP12454941/html/GUID-DDFB957B-CE0F-4603-9629-669653B1E922.html.

Creating and configuring FPolicy

While creating the FPolicy for the first time, Kaspersky Lab experts recommend to apply the configuration specified in the table below.

Table 10. FPolicy settings

Parameter	String	Value	Note
_EVENT CREATE This parameter identifies the file operations that will be intercepted and reported to Kaspersky Security for Windows Server for analysis and detection encryption attempts.	**Vserver name**	<svm_name>	Must coincide with the value specified in the Anti-Cryptor for NetApp task settings on the external engine side (Kaspersky Security for Windows Server).
	Event	<events_source>	Will be used as a source for the FPolicy.
	Protocol	cifs	
	File operations	create, open, rename, write, close, setattr, delete	
	Filters	close-with-modification, first-write, write-with-size-change, open-with-delete-intent, open-with-write-intent	
	Is volume operation required	false	

Parameter	String	Value	Note
_ENGINE CREATE This parameter determines the settings for the connection to an external engine (or FPolicy server).	**Vserver name**	<svm_name>	Must coincide with the value specified in the Anti-Cryptor for NetApp task settings on the external engine.
	Engine	<engine_name>	External engine name. Must coincide with the value specified in the Anti-Cryptor for NetApp task settings on the external engine.
	Primary FPolicy servers	<primary_server_ip>	Only one server is allowed.
	Port Number of FPolicy Service	<port_number>	1346 is recommended. Must coincide with the value specified in the Anti-Cryptor for NetApp task settings on the external engine.
	Secondary FPolicy servers	<secondary_server_ip>	If a primary server is selected, the secondary server is not available.
	External Engine Type	Synchronous	Asynchronous mode is not supported.
	SSL option for external communication	No-auth	
	FQDN or CCN	-	
	Serial Number of Certificate	-	
	Certificate Authority	-	
_POLICY CREATE This parameter determines the future FPolicy settings.	**Vserver name**	<svm_name>	Must coincide with the value specified in the Anti-Cryptor for NetApp task settings on the external engine.
	Fpolicy	<fpolicy_name>	Must coincide with the value specified in the Anti-Cryptor for NetApp task settings on the external engine.
	Events to Monitor	<events_source>	

Parameter	String	Value	Note
	FPolicy Engine	<engine_name>	External engine string name. Must coincide with the value specified in the Anti-Cryptor for NetApp task settings on the external engine.
	Is mandatory screening required	true	
	Allow privileged access	yes	
	User name for privileged access	<user_name>	The same value must be specified in the Anti-Cryptor for NetApp task settings for the Credentials field to access shared folders on network attached storage.
	Is passthrough read enabled	false	
_SCOPE CREATE This parameter determines the protection scope covered by the external engine.	**Vserver name**	<svm_name>	We recommend that you specify the widest possible area for protecting the network attached storage. We recommend that you add exclusions in the Anti-Cryptor for NetApp task settings.
	Policy	<fpolicy_name>	

We recommend that you specify the highlighted values in the table. Other values may vary depending on your requirements.

If FPolicy settings are changed on the network attached storage while the Anti-Cryptor for NetApp task is running, the Anti-Cryptor for NetApp task must be restarted to apply the new settings.

Configuring the Kaspersky Security for Windows Server

To establish the connection between the Kaspersky Security for Windows Server Anti-Cryptor for NetApp component and a protected network attached storage, the Anti-Cryptor for NetApp settings (see table below).

Table 11. Anti-Cryptor for NetApp configuration

Setting	Possible values	Default
Mode	• Statistic Only • Active	Active
Heuristic Analyzer	Light – Medium – Deep	Applied with the “medium” heuristic level.
Exclusions	Applied for all protected shares. Exclusion criteria: • Mask (folder, object, extension) • Client computer IP address • Trusted user	Not defined
Addressing	• Cluster IP-address • Full list of clusters • Credentials (login and password) for the CDOT local Administrator. The following setting double value that have been configured for _POLICY CREATE parameter (User name for privileged access string) Credentials (login and password) for the user that is allowed to access the network attached storage shared folders. The following settings double values that have been configured for _ENGINE CREATE parameter on network attached storage side. • FPolicy name • SVM (Vserver) name • Port (1346)	Not defined
Schedule settings	-	Not defined

Blocked hosts storage usage

The Blocked hosts storage is populated when the following conditions are met:

- The Anti-Cryptor for NetApp task is started in an **Active** mode.
- Anti-Cryptor for NetApp detects an encryption attempt on protected NetApp shares.

After the encryption attempt is detected, the Anti-Cryptor for NetApp component sends information about the compromised host to the **Blocked Host Storage**. After that, Kaspersky Security for Windows Server creates a critical event for the host blocking and blocks any file operation executed from this host.

By default Kaspersky Security for Windows Server automatically unblocks hosts in 30 minutes after they were added to the list. Computers' access to network file resources is restored automatically after they are deleted from the list of untrusted hosts.

You can modify the blocked hosts list:

- Unblock hosts manually.

- Configure blocking term.

When configuring the Anti-Cryptor for NetApp task, please pay attention to the external engine type that is used in the FPolicy settings (_ENGINE CREATE parameter).

Kaspersky Security for Windows Server logs the event with the result of received conclusion and performs an action according to the task mode.

Kaspersky Security for Windows Server supports two possible configurations:

#	Network Attached Storage mode	Anti-Cryptor for NetApp task mode	Description
1	Synchronous	Statistic Only	This configuration provides protection from encryption in the audit mode: the application only logs encryption events. You can switch to configuration 2 from Kaspersky Security for Windows Server.
2	Synchronous	Active	This configuration provides full protection: all compromised hosts are stored in the Blocked Hosts storage, any file operations executed by these hosts are blocked. You can switch to configuration 1 from protected network attached storage or from an external server.

See detailed information on how to configure the Blocked Hosts Storage in the Kaspersky Security for Windows Server Administrator's Guide.

Configuring Anti-Cryptor for NetApp task settings

Set up external server and Network Attached Storage settings to start and configure the Anti-Cryptor for NetApp task.

Configuring task settings via the Kaspersky Security for Windows Server Console

► *To configure the Anti-Cryptor for NetApp task settings:*

1. In the Application Console tree, expand the **Network Attached Storage Protection** node.
2. Select the **Anti-Cryptor for NetApp** child node.
3. Click the **Properties** link in the details pane.

   The **Task settings** window opens.

4. On the **General** tab configure the following settings:
   - Select the task mode in the **Task mode** section.
   - Configure the heuristic analyzer usage and the level of analysis in the **Heuristic analyzer** section.
5. On the **Addressing** tab, configure connection and authentication settings (see Section "Configuring addressing" on page 72).
6. On the **Schedule** and **Advanced** tab, configure the task start schedule.
7. Click **OK**.

► *To set up the exclusion list for the Anti-Cryptor for NetApp task:*

1. In the Application Console tree, expand the **Network Attached Storage Protection** node.
2. Select the **Anti-Cryptor for NetApp** child node.
3. Click the **Exclusion list** link in the details pane.

   The **Exclusion list** window opens.
4. Set up the exclusion list (see Section "Modifying the list of exclusions" on page 73).

Configuring task settings via Kaspersky Security Center

► *To configure the Anti-Cryptor for NetApp task:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree and select the administration group for which you want to configure application settings.
2. To configure application settings for a group of servers, select the **Policies** tab and open the properties of the policy you want to configure.
3. In the **Network Attached Storage Protection** section click the **Settings** button the **Anti-Cryptor for NetApp** block.
4. On the **General** tab, configure the task mode and the heuristic analyzer.
5. On the **Addressing** tab, configure connection and authentication settings (see Section "Configuring addressing" on page 72).
6. On the **Exclusions** tab, add exclusions from the protection scope (see Section "Modifying the list of exclusions" on page 73).
7. On the **Task Management** tab, start the task based on a schedule.
8. Click **OK**.

Configuring general task settings

► *To configure the Anti-Cryptor for NetApp task:*

1. On the **General** tab, configure the following settings:
   - Task mode:
     - **Statistic only**

       Select this option to receive notifications about detected file encryption attempts.

The application generates events in the task log.

- **Active**

  Select this option to block file operations performed by the compromised hosts on a protected network storage. The application adds hosts to the Blocked hosts storage if a file encryption attempt has been detected. Any file operations from this host will be blocked for a period of time specified in the storage settings.

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

    This check box enables / disables Heuristic Analyzer during object scanning.

    If the check box is selected, Heuristic Analyzer is enabled.

    If the check box is cleared, Heuristic Analyzer is disabled.

    The check box is selected by default.

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

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

    The following scanning intensity levels are available:

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

      This level is selected by default.

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

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

2. On the **Addressing** tab, configure connection and authentication settings (see Section "Configuring addressing" on page 72).
3. On the **Exclusions** tab, add exclusions from the protection scope (see Section "Modifying the list of exclusions" on page 73).
4. On the **Task Management** tab, start the task based on a schedule.
5. Click **OK**.

Configuring addressing

► *To set up a connection with protected clusters and gain access to network attached storage:*

1. Open the **Addressing** tab in the task settings.
2. In the **Connection** section configure the following:
   - **IP address of protected cluster**

Specify the IP address of the cluster. A cluster contains the following types of Vservers:

- Admin Vserver
- Node Vserver
- Cluster Vserver

- **Vserver name**

  Specify a name of a virtual storage server.

- **FPolicy name**

  Specify the name of the FPolicy. Before FPolicy can monitor file access, an FPolicy configuration must be created and enabled on the Vserver for which FPolicy services are required.

- **Port**

3. To edit the list of protected cluster nodes:
   a. Click the **Cluster nodes list** in the **Connection** section.
   b. Enter the node name.
   c. Click **Add**.
   d. Click **OK**.

   All existing nodes of a protected cluster must be added to the list.

4. In the **Authentication** section enter:
   - Credentials of a user with a privileged access to network attached storage folders: login and password.

     This account should coincide with the account that has been defined during _POLICY CREATE operation on network attached storage side.

   - Credentials of a CDOT Administrator: login and password.
5. Click **OK** In the **Anti-Cryptor for NetApp** window.

The configured addressing settings are saved.

Modifying the list of exclusions

You can add exclusions based on three criteria:

- Path
- IP address
- User ID

You can use any combination of these criteria for exclusion. The more criteria are specified, the more strict the exclusion parameters are. Kaspersky Security for Windows Server does not analyze file operations for specified exclusions. Note that exclusions added to this list are used for all folders on network attached storage.

If you simultaneously configure anti-virus protection and FPolicy on the same network attached storage, access to the storage shared folders will be possible only if the RPC Network Storage Protection and Anti-Cryptor for NetApp tasks are running.

The external engine should have only one network interface card with one IP address.

► *To add or modify the list of exclusion:*

1. Open the **Exclusion list** tab in the task settings.
2. Select the **Do not detect encryption for the specified exclusions** check box.

   If the check box is selected, all file operations executed by the user / IP address / path specified in the list below are allowed.

   If the check box is cleared, Kaspersky Security for Windows Server detects encryption activity from all hosts, users and paths.

   The check box is cleared by default.

   The list of exclusions becomes active.
3. Click the **Add** button.

   The **Exclusion settings** window opens.
4. To add a mask-based exclusion:
   a. On the **Path** tab, select the **Exclude by path mask** check box.
   b. Enter the path.
   c. Click the **Add** button.
5. To add an IP address-based exclusion:
   a. On the **IP-addresses** tab, select the **Exclude by IP-address of client computer** check box.
   b. Enter IP address.
   c. Click the **Add** button.
6. To add a user-based exclusion:
   a. On the **Users** tab, select the **Exclude by user** check box.
   b. Click the **Add** button.

      The **Select Users** window opens.
   c. Select a user or group you want to exclude.
   d. Click **OK**.
7. Click **OK** in the **Exclusion settings** window.

   The list of exclusions is populated with the specified exceptions.

Managing Network Attached Storage Protection tasks from Kaspersky Security Center

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

In this chapter

About Network Attached Storage Protection from Kaspersky Security Center

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

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

Configuring Network Attached Storage Protection settings using policies

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

Table 12. Network Attached Storage Protection tasks settings in the Kaspersky Security Center policies

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

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

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree and select the administration group for which you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of servers select a policy you want to configure and open the **Properties: <Policy name>** window using one of the following ways:
     a. By selecting the **Properties** option in the policy context menu.
     b. By clicking the **Configure policy** link in the right details pane of the selected policy.
     c. By double-clicking the selected policy.
   - To configure the application for a single server:
     a. On the **Devices** tab open the **Properties: <Computer name>** window in one of the following ways:
        - Double-click the name of the protected server.
        - Open the context menu of the protected server name and select the Properties item.

The **Properties: <Computer name>** window opens.

b. In the **Tasks** section select a task you want to configure.

3. When configuring a policy, select **Network Attached Storage Protection** in the list of sections in the **Properties: <Policy name>** window.
4. In the window that opens, perform the following operations:
   - To configure settings of the RPC Network Storage Protection task, in the **RPC Network Storage Protection** section click the **Settings** button.

     In the **Options** window that opens, configure the task settings according to your requirements. Click **OK** to save changes made to the settings in the policy.
   - To configure settings of the ICAP Network Storage Protection task, in the **ICAP Network Storage Protection** section click the **Settings** button.

     In the **Options** window that opens, configure the task settings (see Section "Configuring the ICAP Network Storage Protection task" on page 56) according to your requirements. Click **OK** to save changes made to the settings in the policy.
   - To configure settings of the Anti-Cryptor for NetApp task, in the **Anti-Cryptor for NetApp** section click the **Settings** button.

     In the **Options** window that opens, configure the task settings (see Section "Configuring Anti-Cryptor for NetApp task settings" on page 70) according to your requirements. Click **OK** to save changes made to the settings in the policy.
5. In the **Properties: <Policy name>** window, click **OK**.

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

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

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

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

1. Expand the **Managed Devices** node in the Administration Console tree and select the group that the protected server belongs to.
2. In the details pane, on the **Devices** tab open the context menu on the line with information about the protected server and select **Properties**.

3. In the **Properties: <Computer name>** window of the **Tasks** section, open the context menu of the Network Attached Storage Protection task that you want to configure and select the **Properties** item.
4. In the window that opens, configure the settings of the Network Attached Storage Protection task according to your requirements:
   - RPC Network Storage Protection task (see Section "Configuring the RPC Network Storage Protection task" on page 41).
   - ICAP Network Storage Protection task.
5. Click **OK**.

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

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

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

Contacting Technical Support

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

In this chapter

How to get technical support

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

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

Before contacting Technical Support, please read through the Technical Support rules.

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

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

Technical Support via Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) is a portal for companies that use Kaspersky Lab applications. Kaspersky CompanyAccount is designed to facilitate interaction between users and Kaspersky Lab specialists via online requests. Kaspersky CompanyAccount lets you monitor the progress of electronic request processing by Kaspersky Lab specialists and store a history of electronic requests.

You can register all of your organization's employees under a single user account on Kaspersky CompanyAccount. A single account lets you centrally manage electronic requests from registered employees to Kaspersky Lab and also manage the privileges of these employees via Kaspersky CompanyAccount.

Kaspersky CompanyAccount is available in the following languages:

- English
- Spanish
- Italian
- German

- Polish
- Portuguese
- Russian
- French
- Japanese

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

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 Security for Windows Server 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.

For more effective support and troubleshooting of application problems, Technical Support specialists may ask you to change application settings temporarily for purposes of debugging during diagnostics. This may require doing the following:

- Activating the functionality that processes and stores extended diagnostic information.
- Fine-tuning the settings of individual software components, which are not available via standard user interface elements.
- Changing the settings of storage and transmission of diagnostic information that was processed.
- Configuring the interception and logging of network traffic.

AO Kaspersky Lab

Kaspersky Lab is a world-renowned vendor of systems protecting computers against digital threats, including viruses and other malware, unsolicited email (spam), and network and hacking attacks.

In 2008, Kaspersky Lab was rated among the world's top four leading vendors of information security software solutions for end users (IDC Worldwide Endpoint Security Revenue by Vendor). Kaspersky Lab is the preferred vendor of computer protection systems for home users in Russia (IDC Endpoint Tracker 2014).

Kaspersky Lab was founded in Russia in 1997. It has since grown into an international group of companies with 38 offices in 33 countries. The company employs more than 3,000 skilled professionals.

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

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

The company offers protection and control solutions and technologies for workstations and mobile devices, virtual machines, file and web servers, mail gateways, and firewalls. The company's portfolio also features specialized products providing protection against DDoS attacks, protection for industrial control systems, and prevention of financial fraud. Used in conjunction with centralized management tools, these solutions ensure effective automated protection for companies and organizations of any size against computer threats. Kaspersky Lab products are certified by major test laboratories, compatible with software from diverse vendors, and optimized to run on many hardware platforms.

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

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

Achievements. Over the years, Kaspersky Lab has won hundreds of awards for its services in combating computer threats. Following tests and research conducted by the reputed Austrian test laboratory AV-Comparatives in 2014, Kaspersky Lab ranked among the top two vendors by the number of Advanced+ certificates earned and was ultimately awarded the Top Rated certificate. But Kaspersky Lab's main achievement is the loyalty of its users worldwide. The company's products and technologies protect more than 400 million users, and its corporate clients number more than 270,000.

Kaspersky Lab website:	https://www.kaspersky.com
Virus encyclopedia:	https://securelist.com
Virus Lab:	https://virusdesk.kaspersky.com (for analyzing suspicious files and websites)
Kaspersky Lab's web forum:	https://forum.kaspersky.com

Information about third-party code

Information about third-party code is contained in the file legal_notices.txt, in the application installation folder.

Trademark notices

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

Citrix, XenApp, and XenDesktop are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries.

Dell and Dell Compellent are trademarks of Dell, Inc.

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

Hitachi is a trademark of Hitachi, Ltd.

IBM and System Storage are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide.

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

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

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

Glossary

A

Administration Server

A component of Kaspersky Security Center that centrally stores information about all Kaspersky Lab applications that are installed within the corporate network. It can also be used to manage these applications.

Anti-virus databases

Databases that contain information about computer security threats known to Kaspersky Lab as of when the anti-virus databases are released. Entries in anti-virus databases allow malicious code to be detected in scanned objects. Anti-virus databases are created by Kaspersky Lab specialists and updated hourly.

Archive

One or more file(s) packaged into a single file through compression. A dedicated application, called an archiver, is required for packing and unpacking the data.

B

Backup

A special storage for backup copies of files, which are created before disinfection or deletion is attempted.

E

Event severity

Property of an event encountered during the operation of a Kaspersky Lab application. There are four severity levels:

- Critical event.
- Error.
- Warning.
- Info.

Events of the same type can have different severity levels depending on the situation in which the event occurred.

H

Heuristic analyzer

A technology for detecting threats about which information has not yet been added to Kaspersky Lab databases. The heuristic analyzer detects objects whose behavior in the operating system may pose a security threat. Objects detected by the heuristic analyzer are considered to be probably infected. For example, an object may be considered probably infected if it contains sequences of commands that are typical of malicious objects (open file, write to file).

I

Infectable file

A file that, due to its structure or format, can be used by criminals as a "container" to store and spread malicious code. As a rule, these are executable files, with such file extensions as .com, .exe, and .dll. The risk of penetration of malicious code into such files is quite high.

Infected object

An object of which a portion of code completely matches part of the code of known malware. Kaspersky Lab does not recommend accessing such objects.

K

Kaspersky Security Network (KSN)

An infrastructure of cloud services that provides access to the Kaspersky Lab database with constantly updated information about the reputation of files, web resources, and software. Kaspersky Security Network ensures faster responses by Kaspersky Lab applications to threats, improves the performance of some protection components, and reduces the likelihood of false positives.

O

OLE object

An object attached to another file or embedded into another file through the use of the Object Linking and Embedding (OLE) technology. An example of an OLE object is a Microsoft Office Excel® spreadsheet embedded into a Microsoft Office Word document.

P

Policy

A policy determines the settings of an application and manages the access to configuration of an application installed on computers within an administration group. An individual policy must be created for each application. You can create an unlimited number of various policies for applications installed on computers in each administration group, but only one policy can be applied to each application at a time within an administration group.

Protection status

Current protection status, which reflects the level of computer security.

Q

Quarantine

The folder to which the Kaspersky Lab application moves probably infected objects that have been detected. Objects are stored in Quarantine in encrypted form in order to avoid any impact on the computer.

R

Real-time protection

The application's operating mode under which objects are scanned for the presence of malicious code in real time.

The application intercepts all attempts to open any object (read, write, or execute) and scans the object for threats. Uninfected objects are passed on to the user; objects containing threats or probably infected objects are processed according to the task settings (disinfected, deleted or quarantined).

S

Security level

The security level is defined as a pre-configured set of application component settings.

Startup objects

A set of applications needed for the operating system and software that is installed on the computer to start and operate correctly. These objects are executed every time the operating system is started. There are viruses capable of infecting such objects specifically, which may lead, for example, to blocking of operating system startup.

U

Update

The procedure of replacing / adding new files (databases or application modules) retrieved from the Kaspersky Lab update servers.

V

Vulnerability

A flaw in an operating system or an application that may be exploited by malware makers to penetrate the operating system or application and corrupt its integrity. Presence of a large number of vulnerabilities in an operating system makes it unreliable, because viruses that penetrate the operating system may cause disruptions in the operating system itself and in installed applications.

Index

A

C

M