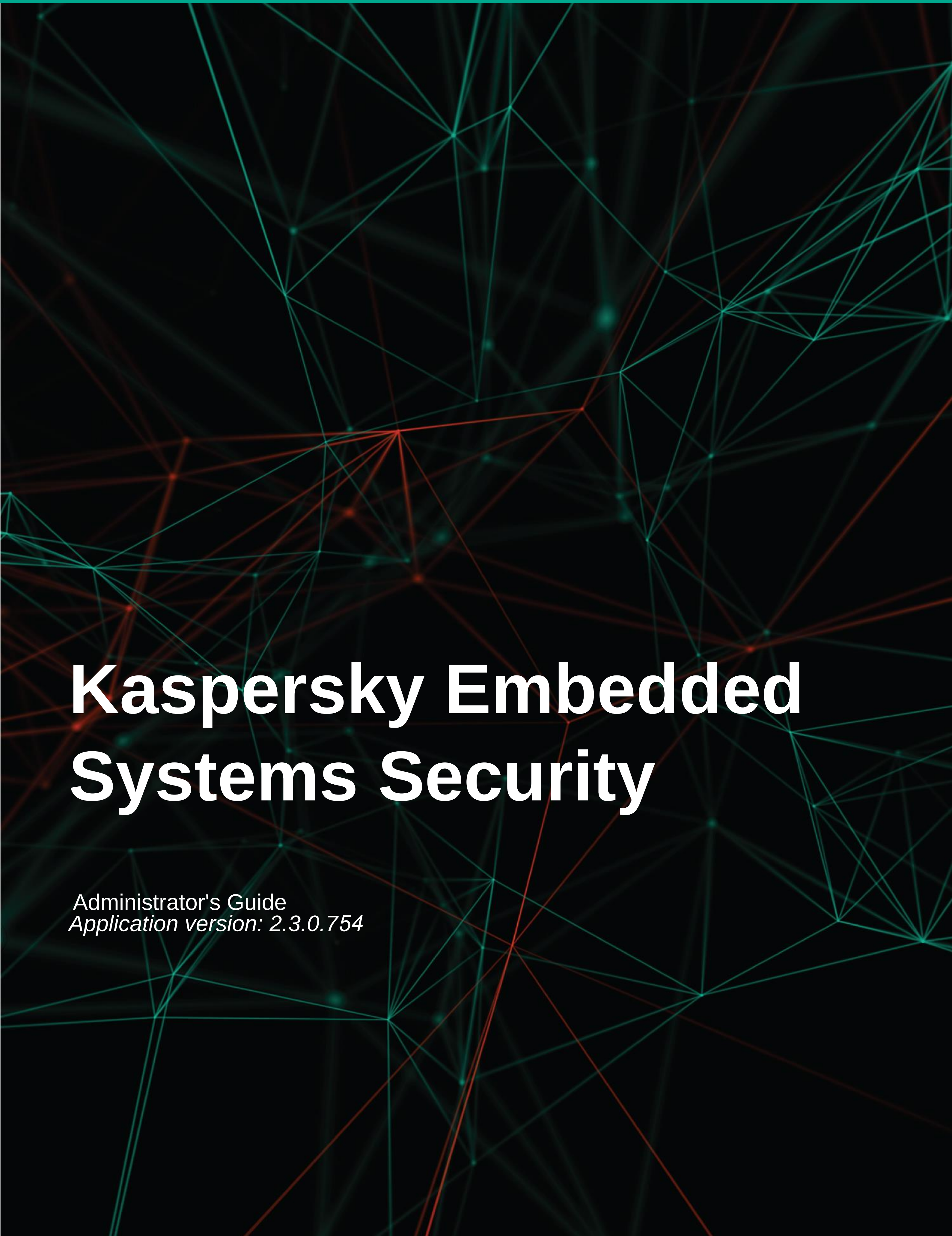


Kaspersky Embedded Systems Security

Administrator's Guide

Application version: 2.3.0.754

Dear User,

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

Attention! This document is the property of AO Kaspersky Lab (herein also referred to as Kaspersky Lab). All rights to this document are reserved by the copyright laws of the Russian Federation and by international treaties. Illegal reproduction and distribution of this document or parts hereof incur civil, administrative, or criminal liability under applicable law.

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

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

Kaspersky Lab reserves the right to amend this document without additional notification.

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

Registered trademarks and service marks used in this document are the property of their respective owners.

Document revision date: 26.04.2019

© 2019 AO Kaspersky Lab. All Rights Reserved.

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

Contents

About this Guide

The Kaspersky Embedded Systems Security 2.3 (hereinafter referred to as "Kaspersky Embedded Systems Security", "the application") Administrator's Guide is intended for specialists who install and administer Kaspersky Embedded Systems Security on all protected devices, and for specialists who provide technical support to organizations using Kaspersky Embedded Systems Security.

This Guide contains information about configuring and using Kaspersky Embedded Systems Security.

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

In this chapter

In this document

The Administrator's Guide for Kaspersky Embedded Systems Security contains the following sections:

Sources of information about Kaspersky Embedded Systems Security

This section lists the sources of information about the application.

Kaspersky Embedded Systems Security

This section describes the functions, components, and distribution kit of Kaspersky Embedded Systems Security, and provides a list of hardware and software requirements of Kaspersky Embedded Systems Security.

Installing and removing the application

This section provides step-by-step instructions for installing and removing Kaspersky Embedded Systems Security.

Application interface

This section contains information about elements of the Kaspersky Embedded Systems Security interface.

Application licensing

This section provides information about the main concepts related to licensing of the application.

Starting and stopping Kaspersky Embedded Systems Security

This section contains information about starting and stopping the Kaspersky Embedded Systems Security Administration Plug-in (hereinafter referred to as Administration Plug-in) and the Kaspersky Security Service.

About access permissions for Kaspersky Embedded Systems Security functions

This section contains information about permissions to manage Kaspersky Embedded Systems Security and Windows® services registered by the application, and instructions on how to configure these permissions.

Creating and configuring policies

This section contains information about using Kaspersky Security Center policies for managing Kaspersky Embedded Systems Security on several computers.

Creating and configuring tasks using Kaspersky Security Center

This section contains information about Kaspersky Embedded Systems Security tasks, and how to create them, configure task settings, and start and stop them.

Managing application settings

This section contains information about configuring Kaspersky Embedded Systems Security general settings in Kaspersky Security Center.

Real-Time Computer Protection

This section provides information about Real-Time Computer Protection components: Real-Time File Protection, KSN Usage and Exploit Prevention. This section also provides instructions on how to configure Real-Time Computer Protection tasks and manage the security settings of a protected computer.

Local Activity Control

This section provides information about Kaspersky Embedded Systems Security functionality that controls applications launches and connections by external devices via USB.

Network Activity Control

This section contains information about the Firewall Management task.

System Inspection

This section contains information about the File Integrity Monitor task and features for inspecting the operating system log.

Integrating with third-party systems

This section describes integration of Kaspersky Embedded Systems Security with third-party features and technologies.

Working with Kaspersky Embedded Systems Security from the command line

This section describes working with Kaspersky Embedded Systems Security from the command line.

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 AO Kaspersky Lab.

Information about third-party code

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

Trademark notices

This section lists trademarks reserved to third-party owners and mentioned in the document.

Index

This section allows you to quickly find required information through the document.

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 may have undesirable consequences.
We recommend that you use...	Notes are set off in a box. Notes contain supplementary and reference information.
Example: …	Examples are given in blocks against a blue background under the heading "Example".

Sample text	Description of document convention
Update means... The *Databases are out of date* event occurs.	The following elements are *italicized* in the text: - New terms - Names of application statuses and events
Press **ENTER**. Press **ALT**+**F4**.	Names of keyboard keys appear in **bold** and are capitalized. Names of keys that are connected by a + (plus) sign indicate the use of a key combination. These keys must be pressed simultaneously.
Click the **Enable** button.	Names of application interface elements, such as text boxes, menu items, and buttons, are set off in **bold**.
► *To configure a task schedule:*	Introductory phrases of instructions are italicized and accompanied by an arrow symbol.
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 the variable name, the corresponding value should be inserted, omitting the angle brackets.

Sources of information about Kaspersky Embedded Systems Security

This section lists the sources of information about the application.

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

In this chapter

Sources for independent retrieval of information

You can use the following sources to find information about Kaspersky Embedded Systems Security:

- Kaspersky Embedded Systems Security page on the Kaspersky Lab website.
- Kaspersky Embedded Systems Security page on the Technical Support website (Knowledge Base).
- Manuals.

If you did not find a solution to your problem, contact Kaspersky Lab Technical Support https://support.kaspersky.com.

An Internet connection is required to use online information sources.

Kaspersky Embedded Systems Security page on the Kaspersky Lab website

On the Kaspersky Embedded Systems Security page https://www.kaspersky.com/enterprise-security/embedded-systems, you can view general information about the application, its functions and features.

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

Kaspersky Embedded Systems Security page in Knowledge Base

Knowledge Base is a section on the Technical Support website.

The Kaspersky Embedded Systems Security page in the Knowledge Base https://support.kaspersky.com/kess2/ 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 Embedded Systems Security but also to other Kaspersky Lab applications. Knowledge Base articles can also include Technical Support news.

Kaspersky Embedded Systems Security documentation

Kaspersky Embedded Systems Security Administrator's Guide contains information about the application installation, uninstallation, settings configuring and usage.

Discussing Kaspersky Lab applications in the community

If your question does not require an immediate answer, you can discuss it with Kaspersky Lab experts and other users in our community https://community.kaspersky.com/.

In this community, you can view existing topics, leave your comments, and create new discussion topics.

Kaspersky Embedded Systems Security

This section describes the functions, components, and distribution kit of Kaspersky Embedded Systems Security, and provides a list of hardware and software requirements of Kaspersky Embedded Systems Security.

In this chapter

About Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security protects computers and other embedded systems under Microsoft® Windows against viruses and other computer threats. Kaspersky Embedded Systems Security users are corporate network administrators and specialists responsible for anti-virus protection of the corporate network.

You can install Kaspersky Embedded Systems Security on a variety embedded systems under Windows, including the following devices types:

- ATM (automated tellers machines);
- POS (points of sales).

Kaspersky Embedded Systems Security can be managed in the following ways:

- Via the Application Console installed on the same computer as Kaspersky Embedded Systems Security, or on a different computer.
- Using commands in the command line.
- Via the Kaspersky Security Center Administration Console.

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

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

Kaspersky Embedded Systems Security components and functions

The application includes the following components:

- **Real-Time Protection**. Kaspersky Embedded Systems Security scans objects when they are accessed. Kaspersky Embedded Systems Security scans the following objects:
    - Files

    - Alternate file system streams (NTFS streams)
    - Master boot records and boot sectors on local hard and removable drives

- **On-Demand Scan**. Kaspersky Embedded Systems Security runs a single scan of the specified area for viruses and other computer security threats. Application scans files, RAM, and autorun objects on a protected computer.
- **Applications Launch Control**. The component tracks users' attempts to launch applications and controls applications launches on a protected computer.
- **Device Control**. The component controls registration and usage of mass storage devices and CD/DVD drives in order to protect the computer against computer security threats that may arise while exchanging files with USB-connected flash drives or other types of external device.
- **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 Embedded Systems Security detects changes in files within the monitoring scopes specified in the task settings. These changes may indicate a security breach on the protected computer.
- **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 Embedded Systems Security downloads updates of application databases and modules from FTP or HTTP update servers of Kaspersky Lab, Kaspersky Security Center Administration Server, or other update sources.
- **Quarantine**. Kaspersky Embedded Systems Security quarantines probably infected objects by moving such objects from their original location to *Quarantine* folder. For security purposes, objects are stored in Quarantine folder in encrypted form.
- **Backup**. Kaspersky Embedded Systems Security stores encrypted copies of objects classified as *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 computer about events in Kaspersky Embedded Systems Security operation and the status of Anti-Virus protection on the computer.
- **Importing and exporting settings**. You can export Kaspersky Embedded Systems Security settings to an XML configuration file and import settings into Kaspersky Embedded Systems Security 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's 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 Embedded Systems Security protection and scan tasks.
- **Managing access permissions for Kaspersky Embedded Systems Security functions**.You can configure the rights to manage Kaspersky Embedded Systems Security and the Windows services registered by the application, for users and groups of users.
- **Writing events to the application event log**. Kaspersky Embedded Systems Security logs information about software component settings, the current status of tasks, events that occur while tasks run, events associated with Kaspersky Embedded Systems Security management, and information required to diagnose errors in Kaspersky Embedded Systems Security.

- **Trusted Zone**. You can generate the list of exclusions from the protection or scan scope, that Kaspersky Embedded Systems Security 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.

What's new

Kaspersky Embedded Systems Security offers the following new features and improvements:

- Support for new versions of Microsoft Windows operating systems.

  Windows 10 Redstone 6 (x32 and x64).
- Complete activation code cannot be viewed in the application GUI.

  The already added activation code is partially hidden while displayed in the application GUI and cannot be viewed in full by any user.

Distribution kit

The distribution kit includes the welcome application that lets you do the following:

- Start the Kaspersky Embedded Systems Security Installation Wizard.
- Start the Kaspersky Embedded Systems Security Console Installation Wizard.
- Start the Installation Wizard that will install Kaspersky Embedded Systems Security Administration Plug-in for managing the application via the Kaspersky Security Center.
- Read the Administrator’s Guide.
- Go to Kaspersky Embedded Systems Security page on the Kaspersky Lab website.
- Visit the Technical Support website https://support.kaspersky.com/.
- Read information about the current version of Kaspersky Embedded Systems Security.

The \console folder contains files for the installation of Application Console ("Kaspersky Embedded Systems Security Administration Tools" set of components).

The \product folder contains:

- Files for the installation of Kaspersky Embedded Systems Security components on a computer running a 32-bit or 64-bit Microsoft Windows operating system.
- File for the installation of the Administration Plug-in for managing Kaspersky Embedded Systems Security via the Kaspersky Security Center.
- Archive of anti-virus databases current at the time the application was released.
- File with the text of the End User License Agreement and Privacy Policy.

The \product_no_avbases folder contains installation files for Kaspersky Embedded Systems Security components and the Administration Plug-in without the antivirus databases.

The \setup folder contains greeting program start files.

The distribution kit files are stored in different folders depending on their intended use (see table below).

Table 2. Kaspersky Embedded Systems Security distribution kit files

File	Purpose
autorun.inf	Autorun file for the Kaspersky Embedded Systems Security Installation Wizard when installing the application from removable media.
ess_admin_guide_en.pdf	Administrator's Guide.
release_notes.txt	The file contains release information.
setup.exe	Greeting program start file (starts setup.hta).
\console\esstools_x86(x64).msi	Windows Installer package; installs the Application Console on the protected computer.
\console\setup.exe	The file that starts the setup wizard for the "Administration tools" set of components (including the Application Console); it starts the esstools.msi installation package file using the settings specified in the setup wizard.
\product\bases.cab	Archive of anti-virus databases current at the time of application release.
\product\setup.exe	The file for installing Kaspersky Embedded Systems Security on the protected computer by means of the wizard; it starts the installation package file ess.msi with the installation settings specified in the wizard.
\product\ess_x86(x64).msi	Windows Installer package; installs Kaspersky Embedded Systems Security on the protected computer.
\product\ess.kud	File in Kaspersky Unicode Definition format with a description of the installation package for remote installation of Kaspersky Embedded Systems Security via Kaspersky Security Center.
\product\klcfginst.exe	Installer for Administration Plug-in for managing Kaspersky Embedded Systems Security via the Kaspersky Security Center. Install the Administration Plug-in on each computer where the Kaspersky Security Center Administration Console is installed if you plan to use it to manage Kaspersky Embedded Systems Security.
\product\license.txt	Text of the End User License Agreement and Privacy Policy.
\product\migration.txt	The file describes migration from previous application versions.
\setup\setup.hta	Greeting program start file.

Hardware and software requirements

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

Software requirements for the protected computer

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

Windows Installer 3.1 is required for a proper application installation and work on a computer under Microsoft Windows XP.

To install and use Kaspersky Embedded Systems Security on the computers with embedded operating systems, Filter Manager component is required.

You can install Kaspersky Embedded Systems Security on a computer under one of the following 32-bit or 64-bit Microsoft Windows operating systems:

- Windows XP Embedded SP3 (32-bit)
- Windows Embedded POSReady 2009 (32-bit)
- Windows XP Professional SP2 / SP3 (32-bit, 64-bit)
- Windows Embedded Standard 7 SP1 (32-bit, 64-bit)
- Windows Embedded Enterprise 7 SP1 (32-bit, 64-bit)
- Windows Embedded POSReady 7 (32-bit, 64-bit)
- Windows 7 Professional / Enterprise SP1 (32-bit, 64-bit)
- Windows Embedded 8.1 Industry Professional / Enterprise (32-bit, 64-bit)
- Windows Embedded 8.0 Standard (32-bit, 64-bit)
- Windows 8 Professional / Enterprise (32-bit, 64-bit)
- Windows 8.1 Professional / Enterprise (32-bit, 64-bit)
- Windows 10 Professional / Enterprise (32-bit, 64-bit)
- Windows 10 IoT Enterprise (32-bit, 64-bit)
- Windows 10 Redstone 1 Professional / Enterprise / IoT Enterprise (32-bit, 64-bit)
- Windows 10 Redstone 2 Professional / Enterprise / IoT Enterprise (32-bit, 64-bit)
- Windows 10 Redstone 3 Professional / Enterprise / IoT Enterprise (32-bit, 64-bit)
- Windows 10 Redstone 4 Professional / Enterprise / IoT Enterprise (32-bit, 64-bit)

- Windows 10 Redstone 5 Professional / Enterprise / IoT Enterprise (32-bit, 64-bit)
- Windows 10 Redstone 6 Professional / Enterprise / IoT Enterprise (32-bit, 64-bit)

Hardware requirements for the protected computer

Hardware requirements for the protected computer vary depending on the installed Windows operating system:

- Hardware requirements for a computer under Windows XP (32 / 64-bit), Windows 7 (32-bit), Windows 8 (32-bit), Windows Embedded XP, Windows Embedded POSReady 2009, or Windows Embedded POSReady 7 operating system:
  - Minimum configuration:
    - Disk space requirements:
      - To install the Applications Launch Control component – 50 MB.
      - To install all Kaspersky Embedded Systems Security components – 2 GB.
    - RAM:
      - 256 MB to install only the Applications Launch Control component on the computer under Microsoft Windows operating system.
      - 512 MB to perform full installation of all components.
    - Processor requirements:
      - for 32-bit Microsoft Windows operating systems: 1.4 GHz single-core processor Intel® Pentium® III.
      - for 64-bit Microsoft Windows operating systems: 1.4 GHz single-core processor Intel Pentium IV.
  - Recommended configuration:
    - Disk space requirements:
      - To install the Applications Launch Control component – 2 GB.
      - To install all Kaspersky Embedded Systems Security components – 4 GB.
    - RAM: 2 GB.
    - Processor requirements:2.4 GHz quad-core processor.
- Hardware requirements for a computer under Windows 7 (64-bit), Windows 8 (64-bit), Windows 10 (64-bit), Windows Embedded 7, or Windows Embedded 8 operating system:
  - Minimum configuration:
    - Disk space requirements:
      - To install the Applications Launch Control component – 50 MB.
      - To install all Kaspersky Embedded Systems Security components – 2 GB.
    - RAM: 1 GB.

        - Processor requirements:
            - for 32-bit Microsoft Windows operating systems: 1.4 GHz single-core processor Intel Pentium III.
            - for 64-bit Microsoft Windows operating systems: 1.4 GHz single-core processor Intel Pentium IV.
    - Recommended configuration
        - Disk space requirements:
            - To install the Applications Launch Control component – 2 GB.
            - To install all Kaspersky Embedded Systems Security components – 4 GB.
        - RAM: 2 GB.
        - Processor requirements:2.4 GHz quad-core processor.

Functional requirements and limitations

This section describes additional functional requirements and existing limitations for Kaspersky Embedded Systems Security components.

In this section

Installation and uninstallation

- During application installation a warning appears, if a new path to the Kaspersky Embedded Systems Security installation folder contains more than 150 symbols. The warning does not affect the installation process: Kaspersky Embedded Systems Security will install and run successfully.
- For installation of the SNMP protocol support component the SNMP service must be restarted, if it is running.
- For installation and functioning of Kaspersky Embedded Systems Security on the device managed by the embedded operating system, the Filter Manager component must be installed.
- The Kaspersky Embedded Systems Security Administration Tools installation is not available via the Microsoft Active Directory® group policies.
- When installing application on computers running on the older operating systems, which cannot receive regular updates, it is required to check the following root certificates: DigiCert Assured ID Root CA, DigiCert_High_Assurance_EV_Root_CA, DigiCertAssuredIDRootCA. Lack of specified certificates can lead to incorrect application functioning. It is recommended to install specified certificates in any possible way.

- Kaspersky Embedded Systems Security Console cannot be uninstalled via the **Start** menu. You can uninstall Kaspersky Embedded Systems Security Console using the link in the Add / Remove Programs window.

File Integrity Monitor

By default, the File Integrity Monitor does not monitor changes in system folders or the file system's housekeeping files, in order to prevent information about routine file changes, which are performed constantly by the operating system, from getting into the task reports. The user cannot manually include such folders in the monitoring scope.

The following folders/files are excluded from the monitoring scope:

- NTFS housekeeping files with file id from 0 to 33
- "%SystemRoot%\\Prefetch\\"
- "%SystemRoot%\\ServiceProfiles\\LocalService\\AppData\\Local\\"
- "%SystemRoot%\\System32\\LogFiles\\Scm\\"
- "%SystemRoot%\\Microsoft.NET\\Framework\\v4.0.30319\\"
- "%SystemRoot%\\Microsoft.NET\\Framework64\\v4.0.30319\\"
- "%SystemRoot%\\Microsoft.NET\\"
- "%SystemRoot%\\System32\\config\\"
- "%SystemRoot%\\Temp\\"
- "%SystemRoot%\\ServiceProfiles\\LocalService\\"
- "%SystemRoot%\\System32\\winevt\\Logs\\"
- "%SystemRoot%\\System32\\wbem\\repository\\"
- "%SystemRoot%\\System32\\wbem\\Logs\\"
- "%ProgramData%\\Microsoft\\Windows\\WER\\ReportQueue\\"
- "%SystemRoot%\\SoftwareDistribution\\DataStore\\"
- "%SystemRoot%\\SoftwareDistribution\\DataStore\\Logs\\"
- "%ProgramData%\\Microsoft\\Windows\\AppRepository\\"
- "%ProgramData%\\Microsoft\\Search\\Data\\Applications\\Windows\\"
- "%SystemRoot%\\Logs\\SystemRestore\\"
- "%SystemRoot%\\System32\\Tasks\\Microsoft\\Windows\\TaskScheduler\\"

The application excludes top-level folders.

The component does not monitor files changes that bypass the ReFS/NTFS file system (file changes made through BIOS, LiveCD, etc.).

Firewall Management

- Working with IP addresses in IPv6 format is not available when specified applied rule scope consists of one address.
- Preset Firewall policy rules provide execution of basic scenarios of interaction between local computers and Administration Server. For full usage of Kaspersky Security Center functions, it is required to set up rules for ports manually. Information about port numbers, protocols and their functions is contained in Kaspersky Security Center Knowledge base (article ID: 9297).
- The application does not control modification of Windows Firewall rules and rule groups during the minutely inquiries of the Firewall management task, if those rules were not added to the task configuration upon the application installation. To update the status and include such rules the Firewall management task must be restarted.
- When the Firewall Management task is started, the following types of rules are automatically removed from the operating system's firewall settings:
    - denying rules;
    - rules monitoring outgoing traffic.

Other limitations

On-Demand Scan, Real-Time File Protection:

- Connected MTP-devices scanning is not available.
- Archive object scanning is not available without SFX-archive scanning: if archive scanning is enabled in the protection settings of Kaspersky Embedded Systems Security, the application automatically scans objects in both archives and SFX-archives. SFX-archives scanning without archives scanning is available.

Licensing:

- Application activation with the key via the Setup wizard is not available, if the key is stored on the disk, which was created with the SUBST command, or if the network path to the key file is specified.

Updates:

- After the installation of Kaspersky Embedded Systems Security critical modules updates, the application icon is hidden by default.
- KLRAMDISK is not supported on computers running Windows XP or Windows 2003 operating system.

Interface:

- If you use filtering in the Application Console in the Quarantine, Backup, System audit log or Task log, the case should be maintained.
- You can use only one mask and only in the path end, when configuring protection or scan scope in the Application Console. Correct mask usage examples: "C:\Temp\Temp*", or "C:\Temp\Temp???.doc", or "C:\Temp\Temp*.doc". Limitation does not affect Trusted Zone configuration.

Security:

- If the User Account Control in the operating system settings is activated, a user account must be a part of KAVWSEE Administrators group to open the Application Console with a double-click on the application icon in the tray notification area. In other case, it will be necessary to login as a user, which is allowed to open the Compact Diagnostic Interface or the Microsoft Management Console snap-in.
- Application uninstallation via the **Programs and Features** window of Microsoft Windows is not available if the User Account Control is activated.

Integration with Kaspersky Security Center:

- Administration Server checks the database updates validity when receiving the update packages, and before sending the updates to network computers. Administration Server does not check validity of the received software module updates.
- Make sure the required check boxes are selected in the Interaction with the Administration Server settings, when you use the components that transmit the dynamically changed data to Kaspersky Security Center with the help of network lists (Quarantine, Backup).

Exploit Prevention:

- Exploit Prevention is not available if apphelp.dll libraries are not loaded in the current environment configuration.
- The Exploit Prevention component is incompatible with Microsoft’s EMET utility on computers running the Microsoft Windows 10 operating system: Kaspersky Embedded Systems Security blocks EMET, if the Exploit Prevention component is being installed on a computer with EMET installed.

Installing and removing the application

This section provides step-by-step instructions for installing and removing Kaspersky Embedded Systems Security.

In this chapter

Kaspersky Embedded Systems Security software component codes for the Windows Installer service

By default, the \product\ess_x86.msi and \product\ess_x64.msi files are designed to install all Kaspersky Embedded Systems Security components. You can install these components by including them in a custom installation.

The \console\esstools_x86.msi and \console\esstools_x64.msi files install all software components in the "Administration Tools" set.

The following sections list the Kaspersky Embedded Systems Security component codes for the Windows Installer service. These codes can be used to define a list of components to be installed when installing Kaspersky Embedded Systems Security from the command line.

In this section

Kaspersky Embedded Systems Security software components

The following table contains codes and descriptions of Kaspersky Embedded Systems Security software components.

Table 3. Description of Kaspersky Embedded Systems Security software components

Component	Identifier	Functions performed
Basic functionality	Core	This component contains the set of basic application functions and ensures their operation.
Applications Launch Control	AppCtrl	This component monitors user attempts to run applications and allows or denies application launch in accordance with specified Applications Launch Control rules. It is implemented in the Applications Launch Control task.
Device Control	DevCtrl	This component tracks attempts to connect USB mass storage devices to a protected computer and allows or denies use of these devices according to the specified device control rules. The component is implemented in the Device Control task.
Anti-Virus protection	AVProtection	This component provides anti-virus protection and contains the following components: • On-Demand Scan • Real-Time File Protection
On-Demand Scan	Ods	This component installs Kaspersky Embedded Systems Security system files and provides On-Demand scan tasks (scanning of objects on the protected computer upon request). If other Kaspersky Embedded Systems Security components are specified when installing Kaspersky Embedded Systems Security from the command line, but the Core component is not specified, the Core component is installed automatically.
Real-Time File Protection	Oas	This component performs anti-virus scans of files on the protected computer when these files are accessed. It implements the Real-Time File Protection task.
Kaspersky Security Network Usage	Ksn	This component provides protection based on Kaspersky Lab cloud technologies. It implements the KSN Usage task (sending requests to and receiving conclusions from the Kaspersky Security Network service).

Component	Identifier	Functions performed
File Integrity Monitor	Fim	This component logs operations performed on files in the specified monitoring scope. The component implements the File Integrity Monitor task.
Exploit Prevention	AntiExploit	This component makes it possible to manage settings to protect memory used by processes in a protected computer's memory.
Firewall Management	Firewall	This component makes it possible to manage Windows Firewall through the Kaspersky Embedded Systems Security graphical user interface. The component implements the Firewall Management task.
Module for integration with Kaspersky Security Center Network Agent	AKIntegration	This component provides a connection between the Kaspersky Embedded Systems Security and the Kaspersky Security Center Network Agent. You can install this component on the protected computer if you intend to manage the application via the Kaspersky Security Center.
Log Inspection	LogInspector	This component monitors the integrity of the protected environment based on the results of an inspection of Windows event logs.
Set of "System Monitor" performance counters	PerfMonCounters	This component installs a set of System Monitor performance counters. Performance counters enable Kaspersky Embedded Systems Security performance to be measured and potential bottlenecks to be located on the computer when Kaspersky Embedded Systems Security is used with other programs.
SNMP counters and traps	SnmpSupport	This component publishes Kaspersky Embedded Systems Security counters and traps via Simple Network Management Protocol (SNMP) on Microsoft Windows. This component may be installed on the protected computer only if Microsoft SNMP service is installed on the same computer.

Component	**Identifier**	**Functions performed**
Kaspersky Embedded Systems Security icon in the notification area	TrayApp	This component displays the Kaspersky Embedded Systems Security icon in the task tray notification area of the protected computer. The Kaspersky Embedded Systems Security icon displays the status of computer protection and can be used to open the Kaspersky Embedded Systems Security Console in Microsoft Management Console (if installed) and the **About the application** window.

"Administration tools" set of software components

The following table contains codes and descriptions of the "Administration tools" set of software components.

Table 4. Description of the "Administration tools" software components

Component	Code	Component functions
Kaspersky Embedded Systems Security snap-ins	MmcSnapin	This component installs the Microsoft Management Console snap-in via Kaspersky Embedded Systems Security Console. If other components are specified during installation of "Administration Tools" from the command line, and the MmcSnapin component is not specified, the component will be installed automatically.
Help	Help	This is a .chm help file saved in the folder with the Kaspersky Embedded Systems Security Administration Tools files. You can open the Help file using the **Start** menu or by clicking the **F1** key with the Application Console window opened.
Documentation	Help	Kaspersky Embedded Systems Security adds a shortcut to the Kaspersky Lab web site where the Administrator's Guide is available in PDF format. The shortcut is available in the **Start** menu.

System changes after Kaspersky Embedded Systems Security installation

When Kaspersky Embedded Systems Security and the set of "Administration Tools" (including the Application Console) are installed together, the Windows Installer service will make the following modifications on the protected computer:

- Kaspersky Embedded Systems Security folders are created on the protected computer and on the computer where the Application Console is installed.
- Kaspersky Embedded Systems Security services are registered.
- A Kaspersky Embedded Systems Security user group is created.
- Kaspersky Embedded Systems Security keys are registered in the system registry.

These changes are described below.

Kaspersky Embedded Systems Security folders on a protected computer

When Kaspersky Embedded Systems Security is installed, the following folders are created on a protected computer:

- Kaspersky Embedded Systems Security default installation folder containing the Kaspersky Embedded Systems Security executable files depend on the operating system bit set. Therefore, the default installation folders are as follows:
  - On the 32-bit version of Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security\
  - On the 64-bit version of Microsoft Windows: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security\
- Management Information Base (MIB) files containing a description of the counters and hooks published by Kaspersky Embedded Systems Security via the SNMP protocol:
  - %Kaspersky Embedded Systems Security%\mibs
- 64-bit versions of Kaspersky Embedded Systems Security executable files (this folder will be created only during installation of Kaspersky Embedded Systems Security on the 64-bit version of Microsoft Windows):
  - %Kaspersky Embedded Systems Security%\x64
- Kaspersky Embedded Systems Security service files:
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Data\
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Settings\
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Dskm\
- Files with settings for update sources:
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Update\
- Updates of databases and software modules downloaded using the Copying Updates task (the folder will be created the first time updates are downloaded using the Copying Updates task):

    - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Update\Distribution\
- Task logs and system audit log:
    - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Reports\
- Set of databases currently in use:
    - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Bases\Current\
- Backup copies of databases; they are overwritten each time the databases are updated:
    - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Bases\Backup\
- Temporary files created during execution of update tasks:
    - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Bases\Temp\
- Quarantined objects (default folder):
    - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Quarantine\
- Objects in backup (default folder):
    - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Backup\
- Objects restored from backup and quarantine (default folder for restored objects):
    - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Restored\

Folder created during installation of Application Console

The Application Console default installation folders containing the "Administration Tools" files depend on the operating system bit set. Therefore, the default installation folders are as follows:

    - On the 32-bit version of Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools\
    - On the 64-bit version of Microsoft Windows: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools\

Kaspersky Embedded Systems Security services

The following Kaspersky Embedded Systems Security services start using the local system (SYSTEM) account:

- Kaspersky Security Service (KAVFS) – essential Kaspersky Embedded Systems Security service that manages Kaspersky Embedded Systems Security tasks and workflows.
- Kaspersky Security Management Service (KAVFSGT) – this service is intended for Kaspersky Embedded Systems Security application management through the Application Console.
- Kaspersky Security Exploit Prevention Service (KAVFSSLP) – a service that acts as an intermediary to communicate security settings to external security agents, and to receive data about security events.

Kaspersky Embedded Systems Security group

ESS Administrators is a group on the protected computer, which users have full access to the Kaspersky Security Management Service and to all Kaspersky Embedded Systems Security functions.

System registry keys

When Kaspersky Embedded Systems Security is installed, the following system registry keys are created:

- Properties of the Kaspersky Embedded Systems Security:
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFS]
- Kaspersky Embedded Systems Security event log settings (Kaspersky Event Log):
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Security]
- Properties of the Kaspersky Embedded Systems Security management service:
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]
- Performance counter settings:
  - On the 32-bit version of Microsoft Windows:
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security\Performance]
  - On the 64-bit version of Microsoft Windows:
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security x64\Performance]
- SNMP Protocol Support component settings:
  - On the 32-bit version of Microsoft Windows:
[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.3\SnmpAgent]
  - On the 64-bit version of Microsoft Windows:
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.3\SnmpAgent]
- Dump file settings:
  - On the 32-bit version of Microsoft Windows:
[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.3\CrashDump]
  - On the 64-bit version of Microsoft Windows:
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.3\CrashDump]
- Trace file settings:
  - On the 32-bit version of Microsoft Windows:
[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.3\Trace]
  - On the 64-bit version of Microsoft Windows:
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.3\Trace]
- Configuration of the application's tasks and functions:
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.3\Environment]

Kaspersky Embedded Systems Security processes

Kaspersky Embedded Systems Security starts processes described in the table below.

Table 5. Kaspersky Embedded Systems Security processes

File name	Purpose
kavfswp.exe	Kaspersky Embedded Systems Security workflow
kavtray.exe	Process for the System Tray Icon
kavfsmui.exe	Process for the Compact Diagnostic Interface component
kavshell.exe	Command line utility process
kavfsrcn.exe	Kaspersky Embedded Systems Security remote management process
kavfs.exe	Kaspersky Security Service process
kavfsgt.exe	Kaspersky Security Management Service process
kavfswh.exe	Kaspersky Security Exploit Prevention Service process

Installation and uninstallation settings and command line options for the Windows Installer service

This section contains descriptions of the settings for installing and uninstalling Kaspersky Embedded Systems Security, their default values, keys for changing the installation settings, and their possible values. These keys can be used in conjunction with standard keys for the Windows Installer service's `msiexec` command when installing Kaspersky Embedded Systems Security from the command line.

Installation settings and command line options in Windows Installer

- Acceptance of the terms of the End User License Agreement: you must accept the terms to install Kaspersky Embedded Systems Security.

  The possible values for `EULA=<value>` command line option are as follows:

  - `0` – you reject the terms of the End User License Agreement (default value).
  - `1` – you accept the terms of the End User License Agreement.

- Acceptance of the terms of the Privacy Policy: you must accept the terms to install Kaspersky Embedded Systems Security.

  The possible values for `PRIVACYPOLICY=<value>` command line option are as follows:

  - `0` – you reject the terms of the Privacy Policy (default value).
  - `1` – you accept the terms of the Privacy Policy.

- Installation of Kaspersky Embedded Systems Security with a preliminary scan of active processes and the boot sectors of local disks.

  The possible values for `PRESCAN=<value>` command line option are as follows:

- `0` – do not perform a preliminary scan of active processes and the boot sectors of local disks during the installation (default value).
- `1` – perform a preliminary scan of active processes and the boot sectors of local disks during the installation.

- Destination folder where Kaspersky Embedded Systems Security files will be saved during installation. A different folder can be specified.

  The default values for `INSTALLDIR=<full path to the folder>` command line option are as follows:

  - Kaspersky Embedded Systems Security: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security
  - Administration tools: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools
  - On the x64-bit version of Microsoft Windows: %ProgramFiles(x86)%

- The Real-Time File Protection task starts immediately after Kaspersky Embedded Systems Security starts. Turn on this setting to start Real-Time File Protection when Kaspersky Embedded Systems Security starts (recommended).

  The possible values for `RUNRTP=<value>` command line option are as follows:

  - `1` – start (default value).
  - `0` – do not start.

- Protection exclusions recommended by Microsoft Corporation. In the Real-Time File Protection task exclude from the protection scope objects on the computer that Microsoft Corporation recommends to exclude. Some applications on the computer may become unstable when an anti-virus application intercepts or modifies the files they use. For example, Microsoft Corporation includes some domain controller applications in the list of such objects.

  The possible values for `ADDMSEXCLUSION=<value>` command line option are as follows:

  - `1` – exclude (default value).
  - `0` – do not exclude.

- Objects excluded from the protection scope according to Kaspersky Lab recommendations. In the Real-Time File Protection task exclude from the protection scope objects on the computer that Kaspersky Lab recommends to exclude.

  The possible values for `ADDKLEXCLUSION=<value>` command line option are as follows:

  - `1` – exclude (default value).
  - `0` – do not exclude.

- Allow remote connection to the Application Console. By default, remote connection is not allowed to the Application Console installed on the protected computer. During the installation, you can allow connection. Kaspersky Embedded Systems Security creates allowing rules for the process kavfsgt.exe using the TCP protocol for all ports.

  The possible values for `ALLOWREMOTECON=<value>` command line option are as follows:

  - `1` – allow.
  - `0` – deny (default value).

- Path to the key file. By default, the Windows Installer attempts to find the file with .key extension in the \product folder of the distribution kit. If the \product folder contains several key files, the Windows Installer will select the key file that has the farthest expiration date. A key file can be saved beforehand in the \product folder or by specifying another path to the key file using the **Add key** setting. You can add a key after Kaspersky Embedded Systems Security is installed using an administrative tool of your choice: for example, the Application Console. If you do not add a key during installation of the application, Kaspersky Embedded Systems Security will not function.
- Path to the configuration file. Kaspersky Embedded Systems Security imports settings from the specified configuration file created in the application. Kaspersky Embedded Systems Security does not import passwords from the configuration file, for example, account passwords for starting tasks, or passwords for connecting to a proxy server. Once the settings are imported, you will have to enter all passwords manually. If the configuration file is not specified, the application will start to work with the default settings after setup.

  The default value for `CONFIGPATH=<configuration file name>` is not specified.
- Enabling network connections for the Application Console. Use this option to install Kaspersky Embedded Systems Security on another computer. You can remotely manage computer protection from another computer with the Kaspersky Embedded Systems Security Console installed. Port 135 (TCP) is opened in Microsoft Windows Firewall, network connections are allowed for the executable file kavfsrcn.exe for remote management of Kaspersky Embedded Systems Security, and access is granted to DCOM applications. When installation is complete, add users to the ESS Administrators group to let them remotely manage the application, and allow network connections to the Kaspersky Security Management Service (kavfsgt.exe file) on the computer. You can read more about additional configuration when the Kaspersky Embedded Systems Security Console is installed on another computer (see Section "Advanced settings after installation of the Application Console on another computer" on page 50).

  The possible values for `ADDWFEXCLUSION=<value>` command line option are as follows:
  - `1` – allow.
  - `0` – deny (default value).
- Disabling the check for incompatible software. Use this setting to enable or disable the check for incompatible software during background installation of the application on the computer.Regardless of the value of this setting, during installation of Kaspersky Embedded Systems Security, the application always warns about other versions of the application installed on the computer.

  The possible values for `SKIPINCOMPATIBLESW=<value>` command line option are as follows:
  - `0` – The check for incompatible software is performed (default value).
  - `1` – The check for incompatible software is not performed.

Uninstallation settings and command line options in Windows Installer

- Restoring quarantined objects.

  The possible values for `RESTOREQTN=<value>` command line option are as follows:

  - `0` – Remove quarantined content (default value).
  - `1` – Restore quarantined content to the folder specified by the RESTOREPATH parameter into the \Quarantine subfolder.

- Restoring the content of backup.

  The possible values for `RESTOREBCK=<value>` command line option are as follows:

  - `0` – Remove backup content (default value).
  - `1` – Restore backup contents to the folder specified by the RESTOREPATH parameter into the \Backup subfolder.

- Enter the current password to confirm the uninstallation (if password protection is enabled).

  The default value for `UNLOCK_PASSWORD=<specified password>` is not specified.

- Folder for restored objects. Restored objects will be saved to the specified folder.

  The default value for `RESTOREPATH=<full path to the folder>` command line option is %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Restored.

Kaspersky Embedded Systems Security install and uninstall logs

If Kaspersky Embedded Systems Security is installed or uninstalled using the Installation (Uninstallation) Wizard, the Windows Installer service creates an install (uninstall) log. A log file named ess_install_<uid>.log (where <uid> is a unique 8-character log identifier) will be saved in the %temp% folder for the user whose account was used to start the setup.exe file.

If you run the **Modify or Remove Kaspersky Embedded Systems Security 2.3 Administration Tools** option for the Application Console or Kaspersky Embedded Systems Security from the **Start** menu, a log file named ess_2.3_maintenance.log is automatically created in the %temp% folder.

If Kaspersky Embedded Systems Security is installed or uninstalled from the command line, the install log file will not be created by default.

► *To install Kaspersky Embedded Systems Security and create a log file on disk C:\:*

- `msiexec /i ess_x86.msi /l*v C:\ess.log /qn EULA=1 PRIVACYPOLICY=1`
- `msiexec /i ess_x64.msi /l*v C:\ess.log /qn EULA=1 PRIVACYPOLICY=1`

Installation planning

This section describes the set of Kaspersky Embedded Systems Security administration tools, and special aspects of installing and uninstalling Kaspersky Embedded Systems Security using a wizard (see Section "Installing and uninstalling the application using a wizard" on page 46), command line (see Section "Installing and uninstalling the application from the command line" on page 59), using Kaspersky Security Center (see Section "Installing and uninstalling the application using Kaspersky Security Center" on page 64) and via an Active Directory group policy (see Section "Installing and uninstalling via Active Directory group policies" on page 69).

Before starting installation of Kaspersky Embedded Systems Security, plan the main stages of the installation.

1. Determine which administration tools will be used to manage and configure Kaspersky Embedded Systems Security.
2. Select the necessary application components for installation (see Section "Kaspersky Embedded Systems Security software component codes for the Windows Installer service" on page 32).
3. Select the installation method.

In this section

Selecting administration tools

Determine the administration tools that will be used to configure Kaspersky Embedded Systems Security settings and to manage the application. Kaspersky Embedded Systems Security can be managed using the Application Console, command-line utility, and Kaspersky Security Center Administration Console.

Kaspersky Embedded Systems Security Console

Kaspersky Embedded Systems Security Console is a standalone snap-in added to the Microsoft Management Console. Kaspersky Embedded Systems Security can be managed via the Application Console installed on the protected computer or on another computer on the corporate network.

Multiple Kaspersky Embedded Systems Security snap-ins can be added to one Microsoft Management Console opened in author mode to use it to manage the protection of multiple computers with Kaspersky Embedded Systems Security installed.

The Application Console is included in the set of "Administration Tools" application components.

Command line utility

You can manage Kaspersky Embedded Systems Security from the command line of a protected computer.

The command line utility is included in the Kaspersky Embedded Systems Security software components group.

Kaspersky Security Center

If Kaspersky Security Center is used for centralized management of anti-virus protection of computers at your company, you can manage Kaspersky Embedded Systems Security via the Kaspersky Security Center Administration Console.

The following components must be installed:

- **Module for integration with Kaspersky Security Center Network Agent**. This component is included in the Kaspersky Embedded Systems Security software components group. It allows Kaspersky Embedded Systems Security to communicate with the Network Agent. Install the module for integration with Kaspersky Security Center Network Agent on the protected computer.
- **Kaspersky Security Center Network Agent**. Install this component on each protected computer. This component supports interaction between Kaspersky Embedded Systems Security installed on the computer and Kaspersky Security Center Administration Console. The Network Agent installation file is included in the Kaspersky Security Center distribution kit folder.
- **Kaspersky Embedded Systems Security 2.3 Administration Plug-in**. Additionally, install the Administration Plug-in for managing Kaspersky Embedded Systems Security via the Administration Console on the computer where the Kaspersky Security Center Administration Server is installed. This provides the interface for application management via Kaspersky Security Center. The Administration Plug-in installation file, \product\klcfginst.exe, is included in the Kaspersky Embedded Systems Security distribution kit.

Selecting the installation type

After specifying the software components for installation of Kaspersky Embedded Systems Security (see Section "Kaspersky Embedded Systems Security software component codes for the Windows Installer service" on page 32), you need to select the application installation method.

Select the installation method depending on the network architecture and the following conditions:

- Whether you need special Kaspersky Embedded Systems Security installation settings, or the recommended installation settings (see Section "Installation and uninstallation settings and command line options for the Windows Installer service" on page 40).
- Whether the installation settings will be the same for all computers or specific to each computer.

Kaspersky Embedded Systems Security can be installed interactively using the Setup Wizard or in silent mode without user involvement, and can be invoked by running the installation package file with installation settings from the command line. A centralized remote installation of Kaspersky Embedded Systems Security can be performed using Active Directory group policies or using the Kaspersky Security Center remote installation task.

Kaspersky Embedded Systems Security can be installed and configured on a single computer with its settings saved to a configuration file; the file can then be used to install Kaspersky Embedded Systems Security on other computers. Note that this ability does not exist when the application is installed using Active Directory group policies.

Starting the Setup Wizard

The Setup Wizard can install the following:

- Kaspersky Embedded Systems Security components (see Section "Kaspersky Embedded Systems Security software components" on page 33) on a protected computer out of a \product\setup.exe file included in the distribution kit.

- Kaspersky Embedded Systems Security Console (see Section "Kaspersky Embedded Systems Security Console installation" on page 49) from the \console\setup.exe file in the distribution kit on the protected computer or another LAN host.

Running the installation package file from the command line with the necessary installation settings

If the installation package file is started without command-line options, Kaspersky Embedded Systems Security will be installed with the default settings. Kaspersky Embedded Systems Security options can be used to modify the installation settings.

The Application Console can be installed on the protected computer and / or administrator's workstation.

You can also use sample commands for the installation of Kaspersky Embedded Systems Security and the Application Console (see Section "Installing and uninstalling the application from the command line" on page 59).

Centralized installation via Kaspersky Security Center

If Kaspersky Security Center is used in your network for managing networked computers' anti-virus protection, Kaspersky Embedded Systems Security can be installed on multiple computers by using the remote installation task.

The computers on which you want to install Kaspersky Embedded Systems Security using Kaspersky Security Center (see Section "Installing and uninstalling the application using Kaspersky Security Center" on page 64) may be in the same domain as Kaspersky Security Center in a different domain, or in no domain at all.

Centralized installation using Active Directory group policies

Active Directory group policies can be used to install Kaspersky Embedded Systems Security on the protected computer. The Application Console can be installed on the protected computer or administrator's workstation.

Kaspersky Embedded Systems Security can be installed using just the recommended installation settings.

The computers on which Kaspersky Embedded Systems Security is installed using Active Directory group policies (see Section "Installing and uninstalling via Active Directory group policies" on page 69) must be located in the same domain and the same organizational unit. Installation is performed at computer start before logging in to Microsoft Windows.

Installing and uninstalling the application using a wizard

This section describes the installation and uninstallation of Kaspersky Embedded Systems Security and the Application Console by means of the Setup Wizard, and contains information about additional configuration of Kaspersky Embedded Systems Security and actions to be performed upon installation.

In this section

Installing using the Setup Wizard

The following sections contain information about installation of Kaspersky Embedded Systems Security and the Application Console.

► *To install and proceed to use Kaspersky Embedded Systems Security, take the following steps:*

1. Install Kaspersky Embedded Systems Security on a protected computer.
2. Install the Application Console on the computers from which you intend to manage Kaspersky Embedded Systems Security.
3. If the Application Console has been installed on any computer in the network, other than protected computer, perform the additional configuration to allow Application Console users to manage Kaspersky Embedded Systems Security remotely.
4. Perform actions after installation of Kaspersky Embedded Systems Security.

In this section

Kaspersky Embedded Systems Security installation

Before installing Kaspersky Embedded Systems Security, take the following steps:

Make sure no other anti-virus programs are installed on the computer.

- Make sure that the account which you are using to start the Setup Wizard belongs to the administrators group on the protected computer.

After completing the actions described above, proceed with the installation procedure. Following the Setup Wizard instructions, specify the installation settings for Kaspersky Embedded Systems Security. The Kaspersky Embedded Systems Security installation process can be stopped at any step of the Setup Wizard. To do so, click the **Cancel** button in the Setup Wizard's window.

You can read more about the installation (uninstallation) settings (see Section "Installation and uninstallation settings and command line options for the Windows Installer service" on page 40).

► *To install Kaspersky Embedded Systems Security using the Setup Wizard:*

1. Start the setup.exe file on the computer.
2. In the window that opens, in the **Installation** section, click the **the terms and conditions of this EULA** link.
3. In the welcome screen of the Kaspersky Embedded Systems Security Setup Wizard, click the **Next** button.

   The **EULA and Privacy Policy** window opens.
4. Review the terms of the License Agreement and Privacy Policy.

5. If you agree to the terms and conditions of End User License Agreement and Privacy Policy, select **the terms and conditions of this EULA** and **Privacy Policy describing the handling of data** check boxes in order to proceed with the installation.

   > If you do not accept the End User License Agreement and/or Privacy Policy the installation will be aborted.

6. Click the **Next** button.

   The **Quick scan of the computer before installation** window opens.

7. In the **Quick scan of the computer before installation**, select the **Scan computer for viruses** check box to scan system memory and the boot sectors of the computer local drives for threats. Click the **Next** button. On completion of the scanning procedure the wizard will open a window reporting the scan results.

   This window displays information about scanned computer objects: the total number of scanned objects, the number of threats detected, the number of infected or probably infected objects detected, the number of dangerous or suspicious processes removed from memory by Kaspersky Embedded Systems Security, and the number of dangerous or suspicious processes that the application was unable to remove.

   To see exactly which objects were scanned, click the **List of processed objects** button.

8. Click the **Next** button in the **Quick scan of the computer before installation** window.

   The **Custom installation** window opens.

9. Select the components to be installed.

   By default, all Kaspersky Embedded Systems Security components are included in recommended installation set, except the Firewall Management component.

   > The SNMP Protocol Support component of Kaspersky Embedded Systems Security will only appear in the list of components suggested for installation if the Microsoft Windows SNMP service is installed on the computer.

10. To cancel all changes, click the **Reset** button in the **Custom installation** window. Click the **Next** button.

11. In the **Select a destination folder** window:

    - If required, specify a folder to which Kaspersky Embedded Systems Security files will be copied.
    - If required, review the information about available space on local drives by clicking the **Disk** button.

    Click the **Next** button.

12. In the **Advanced installation settings** window, configure the following installation settings:

    - **Enable real-time protection after installation of application**.
    - **Add Microsoft recommended files to exclusions list**.
    - **Add Kaspersky Lab recommended files to exclusions list**.

      Click the **Next** button.

13. In the **Import settings from configuration file** window:

    a. Specify the configuration file to import Kaspersky Embedded Systems Security settings from an existing configuration file created in any compatible previous version of the application.

    b. Click the **Next** button.

14. In the **Activation of the application** window, do one of the following:
    - If you want to activate the application, specify a Kaspersky Embedded Systems Security key file for application activation.
    - If you want to activate the application later, click the **Next** button.
    - If a key file was previously saved in the \product folder of the distribution kit, the name of this file will be displayed in the **Key** field.

      > To add a key using a key file stored in another folder, specify the key file.

      Once the key file is added, license information will be shown in the window. Kaspersky Embedded Systems Security displays the license's calculated expiration date. The license term runs from the time when you add a key and expires no later than the expiration date of the key file.

      Click the **Next** button to apply the key file in the application.
15. In the **Ready to install** window, click the **Install** button. The wizard will start the installation of Kaspersky Embedded Systems Security components.
16. The **Installation complete** window opens when installation is complete.
17. Select the **View Release Notes** check box to view information about the release after the Setup Wizard is done.
18. Click **Finish**.

The Setup Wizard closes. Once installation is complete, Kaspersky Embedded Systems Security is ready to use if you have added an activation key.

Kaspersky Embedded Systems Security Console installation

Follow the instructions of the Setup Wizard to configure installation settings for the Application Console. The installation process can be stopped at any step of the wizard. To do so, click the **Cancel** button in the Setup Wizard window.

► *To install the Application Console, take the following steps:*

1. Make sure that the account you use to run the Setup Wizard belongs to the administrators group on the computer.
2. Run the setup.exe file on the computer.

   The welcome window opens.
3. Click on the **Install Kaspersky Embedded Systems Security Console** link.

   The Setup Wizard's welcome window opens.
4. Click the **Next** button.
5. Review the terms of the End User License Agreement in the opened window, and select the **I confirm that I have fully read, understood, and accept the terms and conditions of this End User License Agreement** check box in order to proceed with the installation.
6. Click the **Next** button.

   The **Advanced installation settings** window opens.
7. In the **Advanced installation settings** window:

- If you intend to use the Application Console to manage Kaspersky Embedded Systems Security installed on a remote computer, select the **Allow remote access** check box.
- To open the **Custom installation** window and select components:

  a. Click the **Advanced** button.

     The **Custom installation** window opens.

  b. Select the "Administration Tools" components from the list.

     By default, all the components are installed.

  c. Click the **Next** button.

> You can find more detailed information about Kaspersky Embedded Systems Security components (see Section "Kaspersky Embedded Systems Security software component codes for the Windows Installer service" on page 32).

8. In the **Select a destination folder** window:

   a. If required, specify a different folder to which the files being installed should be saved.

   b. Click the **Next** button.

9. In the **Ready to install** window, click the **Install** button.

   The wizard will begin installing the selected components.

10. Click **Finish**.

The Setup Wizard closes. The Application Console will be installed on the protected computer.

If the "Administration tools" set has been installed on any computer in the network other than protected computer, configure the advanced settings (see Section "Advanced settings after installation of the Application Console on another computer" on page 50).

Advanced settings after installation of the Application Console on another computer

If the Application Console has been installed on any computer in the network, other than a protected computer, perform the following actions to allow users to manage Kaspersky Embedded Systems Security remotely:

- Add Kaspersky Embedded Systems Security users to the ESS Administrators group on the protected computer.
- Allow network connections for the Kaspersky Security Management Service (kavfsgt.exe) (see Section "About access permissions for the Kaspersky Security Management Service" on page 229), if the protected computer uses Windows Firewall or a third-party firewall.
- If the **Allow remote access** check box is not selected during installation of the Application Console on a computer running Microsoft Windows, manually allow network connections for the Application Console via the computer's firewall.

The Application Console on the remote computer uses the DCOM protocol to receive information about Kaspersky Embedded Systems Security events (such as objects scanned, tasks completed, etc.) from the Kaspersky Security Management Service on the protected computer. You need to allow network connections for the Application Console in the Windows Firewall settings in order to establish connections between the Application Console and the Kaspersky Security Management Service.

On the remote computer, where the Application Console is installed, do the following:

- Make sure that anonymous remote access to COM applications is allowed (but not remote start and activation of COM applications).
- In Windows Firewall, open TCP port 135 and allow network connections for kavfsrcn.exe, the executable file of the Kaspersky Embedded Systems Security remote management process.

  The client computer where the Application Console is installed uses TCP port 135 to access the protected computer and to receive a response.
- Configure an outbound rule for Windows Firewall to allow the connection.

  Unlike the traditional TCP/IP and UDP/IP services where a single protocol has a fixed port, DCOM dynamically assigns ports to remote COM objects. If a firewall exists between the client (where the Application Console is installed) and the DCOM endpoint (the protected computer), a large range of ports must be opened.

> The same steps should be applied to configure any other software or hardware firewall.

► *If the Application Console is open while you configure the connection between the protected computer and the computer on which the Application Console is installed:*

1. Close the Application Console.
2. Wait until the Kaspersky Embedded Systems Security remote management process kavfsrcn.exe is finished.
3. Restart the Application Console.

   The new connection settings will be applied.

In this section

Allowing anonymous remote access to COM applications

> The names of settings may vary depending on the installed Windows operating system.

► *To allow anonymous remote access to COM applications, take the following steps:*

1. On the remote computer with the Kaspersky Embedded Systems Security Console installed, open the Component Services console.
2. Select **Start** → **Run**.
3. Enter the command `dcomcnfg`.

4. Click **OK**.
5. Expand the **Computers** node in the **Component Services** console on your computer.
6. Open the context menu on the **My Computer** node.
7. Select **Properties**.
8. On the **COM Security** tab of the **Properties** window, click the **Edit Limits** button in the **Access permissions** settings group.
9. Make sure that the **Allow Remote Access** check box is selected for the ANONYMOUS LOGON user in the **Allow Remote Access** window.
10. Click **OK**.

Allowing network connections for the Kaspersky Embedded Systems Security remote management process

The names of settings may vary depending on the installed Windows operating system.

► *To open TCP port 135 in Windows Firewall and to allow network connections for the Kaspersky Embedded Systems Security remote management process, take the following steps:*

1. Close the Kaspersky Embedded Systems Security Console on the remote computer.
2. Perform one of the following steps:
   - On Microsoft Windows XP SP2 or later:
     a. Select **Start** > **Windows Firewall**.
     b. In the **Windows Firewall** window (or Windows Firewall settings), click the **Add port** button on the **Exclusions** tab.
     c. In the **Name** field, specify the port name RPC (TCP/135) or enter another name, for example Kaspersky Embedded Systems Security DCOM, and specify the port number (135) in the **Port name** field.
     d. Select the **TCP** protocol.
     e. Click **OK**.
     f. Click the **Add** button on the **Exclusions** tab.
   - On Microsoft Windows 7 or later:
     a. Select **Start** > **Control Panel** > **Windows Firewall**.
     b. In the **Windows Firewall** window, select **Allow a program or feature through Windows Firewall**.
     c. In the **Allow programs to communicate through Windows Firewall** window click the **Allow another program...** button.
3. Specify the kavfsrcn.exe file in the **Add Program** window. It is located in the destination folder specified during installation of Kaspersky Embedded Systems Security Console using Microsoft Management Console.
4. Click **OK**.

5. Click the **OK** button in the **Windows Firewall (Windows Firewall settings)** window.

Adding outbound rule for Windows Firewall

> The names of settings may vary depending on the installed Windows operating system.

► *To add the outbound rule for Windows Firewall, take the following steps:*

1. Select **Start** > **Control Panel** > **Windows Firewall**.
2. In the **Windows Firewall** window, click the **Advanced settings** link.

   The **Windows Firewall with Advanced Security** window opens.
3. Select the **Outbound Rules** child node.
4. Click on the **New Rule** option in the **Actions** pane.
5. In the **New Outbound Rule Wizard** window that opens, select the **Port** option and click **Next**.
6. Select the **TCP** protocol.
7. In the **Specific remote ports** field specify the following ports range for allowing outgoing connections: 1024-65535.
8. In the **Action** window, select the **Allow the connection** option.
9. Save the new rule and close the **Windows Firewall with Advanced Security** window.

The Windows Firewall will now allow network connections between the Application Console and Kaspersky Security Management Service.

Actions to perform after Kaspersky Embedded Systems Security installation

Kaspersky Embedded Systems Security starts protection and scan tasks immediately after installation if you have activated the application. If **Enable real-time protection after installation of application** (default option) is selected during installation of Kaspersky Embedded Systems Security, the application scans the computer's file system objects when they are accessed. Kaspersky Embedded Systems Security will run the Critical Areas Scan task every Friday at 8:00 PM.

We recommend taking the following steps after installing Kaspersky Embedded Systems Security:

- Start the application database update task. After installation Kaspersky Embedded Systems Security will scan objects using the database included in the application distribution kit.

  > We recommend updating Kaspersky Embedded Systems Security databases immediately since they may be out of date.

  The application will then update the databases every hour according to the default schedule configured in the task.
- Run a Critical Areas Scan on the computer if no anti-virus software with real-time file protection was installed on the protected computer before installation of Kaspersky Embedded Systems Security.
- Configure administrator notifications about Kaspersky Embedded Systems Security events.

In this section

Starting and configuring Kaspersky Embedded Systems Security Database Update task

► *To update the application database after installation, do the following:*

1. In the Database Update task settings, configure a connection to an update source – Kaspersky Lab HTTP or FTP update servers.
2. Start the Database Update task.

Web Proxy Auto-Discovery Protocol (WPAD) may not be configured on your network to detect proxy server settings automatically in the LAN. At that, your network may require authentication when accessing the proxy server.

► *To specify the optional proxy server settings and authentication settings for accessing the proxy server, do the following:*

1. Open the context menu of the **Kaspersky Embedded Systems Security** node.
2. Select the **Properties** item.

   The **Application settings** window opens.
3. Select the **Connection settings** tab.
4. In the **Proxy server settings** section, select the **Use specified proxy server settings** check box.
5. Enter the proxy server address in the **Address** field, and enter the port number for the proxy server in the **Port** field.
6. In the **Proxy server authentication settings** section, select the necessary authentication method in the drop-down list:
   - **Use NTLM authentication**, if the proxy server supports the built-in Microsoft Windows NTLM authentication. Kaspersky Embedded Systems Security will use the user account specified in the task settings to access the proxy server (by default the task will run under the **local system** (**SYSTEM**) user account).
   - **Use NTLM authentication with user name and password**, if the proxy server supports the built-in Microsoft Windows NTLM authentication. Kaspersky Embedded Systems Security will use the specified account to access the proxy server. Enter a user name and password or select a user from the list.
   - **Apply user name and password**, to select basic authentication. Enter a user name and password or select a user from the list.
7. Click **OK** in the **Application settings** window.

► *To configure the connection to Kaspersky Lab's update servers, in the Database Update task:*

1. Start Application Console in one of the following ways:
   - Open the Application Console on the protected computer. To do this, select **Start** > **All Programs** > **Kaspersky Embedded Systems Security** > **Administration Tools** > **Kaspersky Embedded Systems Security 2.3 Console**.
   - If the Application Console has been started on a computer other than the protected one, connect to the protected computer:
     a. Open the context menu of the **Kaspersky Embedded Systems Security** node in the Application Console tree.
     b. Select the **Connect to another computer** item.
     c. In the **Select computer** window, select **Another computer** and in the text field indicate the network name of the protected computer.

     > If the account you used to sign in to Microsoft Windows does not have access permissions for the Kaspersky Security Management Service (see Section "About access permissions for the Kaspersky Security Management Service" on page 229), indicate an account with the required permissions.

   The Application Console window opens.
2. In the Application Console tree, expand the **Update** node.
3. Select the **Database Update** child node.
4. Click the **Properties** link in the details pane.
5. In the **Task settings** window that opens, open the **Connection settings** tab.
6. Select **Use proxy server settings to connect to Kaspersky Lab update servers**.
7. Click **OK** in the **Task settings** window.

The settings for connecting to the update source in the Database Update task will be saved.

► *To run the Database Update task:*

1. In the Application Console tree, expand the **Update** node.
2. In the context menu on the **Database Update** child node, select the **Start** item.

The Database Update task starts.

After the task has successfully completed, you can view the release date of the latest database updates installed in the details pane of the **Kaspersky Embedded Systems Security** node.

Critical Areas Scan

After you have updated the Kaspersky Embedded Systems Security databases, scan the computer for malware using the Critical Areas Scan task.

► *To run the Critical Areas Scan task, take the following steps:*

1. Expand the **On-Demand Scan** node in the Application Console tree.
2. In the context menu of the **Critical Areas Scan** child node, select the **Start** command.

The task starts; the **Running** task status is displayed in the details pane.

► *To view the task log,*

in the details pane of the **Critical Areas Scan** node, click the **Open task log** link.

Modifying the set of components and repairing Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security components can be added or removed. You need to stop the Real-Time File Protection task before you can remove the Real-Time File Protection component. In other circumstances there is no need to stop the Real-Time File Protection task or Kaspersky Security Service.

> If application management is password protected, Kaspersky Embedded Systems Security requests the password when you attempt to remove components or modify the set of components in the Setup Wizard.

► *To modify the set of Kaspersky Embedded Systems Security components:*

1. In the **Start** menu, select **All programs** > **Kaspersky Embedded Systems Security** > **Modify or Remove Kaspersky Embedded Systems Security**.

   The Setup Wizard's **Modify, repair or remove installation** window opens.
2. Select **Modify components set**. Click the **Next** button.

   The **Custom installation** window opens.
3. In the **Custom installation** window, in the list of available components, select the components that you want to add or remove from Kaspersky Embedded Systems Security. To do this, perform the following actions:

   - To change the set of components, click the button next to the name of the selected component. Then in the context menu, select:
     - **Component will be installed on local hard drive**, if you want to install one component;
     - **Component and its subcomponents will be installed on local hard drive**, if you want to install a group of components.
   - To remove previously installed components, click the button next to the name of the selected component. Then in the context menu, select **Component will be unavailable**.

   Click the **Next** button.

4. In the **Ready to install** window, confirm the change to the set of software components by clicking the **Install** button.
5. In the window that opens when installation is complete, click the **OK** button.

The set of Kaspersky Embedded Systems Security components will be modified based on the specified settings.

If problems occur in the operation of Kaspersky Embedded Systems Security (Kaspersky Embedded Systems Security crashes; tasks crash or do not start), it is possible to attempt to repair Kaspersky Embedded Systems Security. You can perform a repair while saving the current Kaspersky Embedded Systems Security settings, or you can select an option to reset all Kaspersky Embedded Systems Security settings to their default values.

► *To repair Kaspersky Embedded Systems Security after the application or a task crashes, take the following steps:*

1. In the **Start** menu, select **All programs**.
2. Select **Kaspersky Embedded Systems Security**.
3. Select **Modify or Remove Kaspersky Embedded Systems Security**.

   The Setup Wizard's **Modify, repair or remove installation** window opens.
4. Select **Repair installed components**. Click the **Next** button.

   This opens the **Repair installed components** window.
5. In the **Repair installed components** window, select the **Restore recommended application settings** check box if you want to reset the application settings and restore Kaspersky Embedded Systems Security with its default settings. Click the **Next** button.
6. In the **Ready to repair** window, confirm the repair operation by clicking the **Install** button.
7. In the window that opens when the repair operation is complete, click the **OK** button.

Kaspersky Embedded Systems Security will be repaired using the specified settings.

Uninstalling using the Setup Wizard

This section contains instructions on removing Kaspersky Embedded Systems Security and the Application Console from a protected computer using the Setup / Uninstallation Wizard.

In this section

Kaspersky Embedded Systems Security uninstallation

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

Kaspersky Embedded Systems Security can be uninstalled from the protected computer using the Setup / Uninstallation Wizard.

After uninstalling Kaspersky Embedded Systems Security from a protected computer a reboot may be required. The reboot can be postponed.

> Uninstallation, repair and installation of the application is not available via the Windows Control Panel if the operating system uses the UAC feature (User Account Control) or access to the application is password protected.

> If application management is password protected, Kaspersky Embedded Systems Security requests the password when you attempt to remove components or modify the set of components in the Setup Wizard.

► *To uninstall Kaspersky Embedded Systems Security:*

1. In the **Start** menu, select **All programs**.
2. Select **Kaspersky Embedded Systems Security**.
3. Select **Modify or Remove Kaspersky Embedded Systems Security**.

   The Setup Wizard's **Modify, repair or remove installation** window opens.
4. Select **Remove software components**. Click the **Next** button.

   The **Advanced application uninstallation settings** window opens.
5. If necessary, in the **Advanced application uninstallation settings** window:

   a. Select the **Export quarantine objects** check box to make Kaspersky Embedded Systems Security export objects that have been quarantined. The check box is cleared by default.

   b. Check the **Export Backup objects** check box to export objects from Kaspersky Embedded Systems Security Backup. The check box is cleared by default.

   c. Click the **Save to** button and select the folder to which you want to export the objects. By default, the objects will be exported to %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\Uninstall.

      Click the **Next** button.
6. In the **Ready to uninstall** window, confirm the uninstallation by clicking the **Uninstall** button.
7. In the window that opens when the uninstallation is complete, click the **OK** button.

Kaspersky Embedded Systems Security will be uninstalled from the protected computer.

Kaspersky Embedded Systems Security Console uninstallation

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

You can uninstall the Application Console from the computer using the Setup / Uninstallation Wizard.

After uninstalling the Application Console, you do not need to restart the computer.

► *To uninstall the Application Console:*

1. In the **Start** menu, select **All programs**.
2. Select **Kaspersky Embedded Systems Security**.
3. Select **Modify or Remove Kaspersky Embedded Systems Security 2.3 Administration Tools**.

   The wizard's **Modify, repair or remove installation** window opens.
4. Select **Remove software components** and click the **Next** button.
5. The **Ready to uninstall** window opens. Click the **Uninstall** button.

   The **Uninstallation complete** window opens.
6. Click **OK**.

Uninstallation is now complete, and the Setup Wizard closes.

Installing and uninstalling the application from the command line

This section describes the particulars of installing and uninstalling Kaspersky Embedded Systems Security from the command line and contains examples of commands to install and uninstall Kaspersky Embedded Systems Security from the command line, and examples of commands to add and remove Kaspersky Embedded Systems Security components from the command line.

In this section

About installing and uninstalling Kaspersky Embedded Systems Security from command line

Kaspersky Embedded Systems Security can be installed or uninstalled, and its components added or removed, by running the \product\ess_x86(x64).msi installation package files from the command line after the installation settings have been specified using keys.

The "Administration Tools" set can be installed on the protected computer or on another computer on the network to work with the Application Console locally or remotely. To do this, use the \console\esstools.msi installation package.

> Perform the installation using an account included in the administrators group on the computer where the application is installed.

If one of the \product\ess_x86.msi or \product\ess_x64.msi files is run on the protected computer without additional keys, Kaspersky Embedded Systems Security will be installed with the recommended installation settings.

The set of components to be installed can be assigned using the ADDLOCAL command-line option by listing the codes for the selected components or sets of components.

Example commands for installing Kaspersky Embedded Systems Security

This section provides examples of commands used to install Kaspersky Embedded Systems Security.

> On computers running a 32-bit version of Microsoft Windows, run the files with the x86 suffix in the distribution kit. On computers running a 64-bit version of Microsoft Windows, run the files with the x64 suffix in the distribution kit.

Detailed information about the use of Windows Installer's standard commands and command-line options is provided in the documentation supplied by Microsoft.

Examples of installing Kaspersky Embedded Systems Security from the setup.exe file

► *To install Kaspersky Embedded Systems Security with the recommended installation settings without user involvement, run the following command:*

```
\product\setup.exe /s/p EULA=1 PRIVACYPOLICY=1
```

You can install Kaspersky Embedded Systems Security with the following settings:

- only install the Real-Time File Protection and On-Demand Scan components;
- do not run Real-Time File Protection when starting Kaspersky Embedded Systems Security;
- do not exclude files that Microsoft Corporation recommends to exclude from the scan scope;

To do so, run the following command:

```
\product\setup.exe /p "ADDLOCAL=Oas RUNRTP=0 ADDMSEXCLUSION=0"
```

Examples of commands used for installation: running an .msi file

- *To install Kaspersky Embedded Systems Security with the recommended installation settings without user involvement, run the following command:*

  ```
  msiexec /i ess.msi /qn EULA=1 PRIVACYPOLICY=1
  ```

- *To install Kaspersky Embedded Systems Security with the recommended installation settings and display the installation interface, run the following command:*

  ```
  msiexec /i ess.msi /qf EULA=1 PRIVACYPOLICY=1
  ```

- *To install and activate Kaspersky Embedded Systems Security using the key file C:\0000000A.key:*

  ```
  msiexec /i ess.msi LICENSEKEYPATH=C:\0000000A.key /qn EULA=1
  PRIVACYPOLICY=1
  ```

- *To install Kaspersky Embedded Systems Security with a preliminary scan of active processes and the boot sectors of local disks, run the following command:*

  ```
  msiexec /i ess.msi PRESCAN=1 /qn EULA=1 PRIVACYPOLICY=1
  ```

- *To install Kaspersky Embedded Systems Security in the installation folder C:\ESS, run the following command:*

  ```
  msiexec /i ess.msi INSTALLDIR=C:\ESS /qn EULA=1 PRIVACYPOLICY=1
  ```

- *To install Kaspersky Embedded Systems Security and save an installation log file named* `ess`*.log in the folder where the Kaspersky Embedded Systems Security msi file is stored, run the following command:*

  ```
  msiexec /i ess.msi /l*v ess.log /qn EULA=1 PRIVACYPOLICY=1
  ```

- *To install Kaspersky Embedded Systems Security Console, run the following command:*

  ```
  msiexec /i esstools.msi /qn EULA=1
  ```

- *To install and activate Kaspersky Embedded Systems Security using the key file C:\0000000A.key and configure Kaspersky Embedded Systems Security according to the settings in the configuration file C:\settings.xml, run the following command:*

  ```
  msiexec /i ess.msi LICENSEKEYPATH=C:\0000000A.key
  CONFIGPATH=C:\settings.xml /qn EULA=1 PRIVACYPOLICY=1
  ```

- *To install an application patch when Kaspersky Embedded Systems Security is password-protected, run the following command:*

  ```
  msiexec /p "<msp file name with path>" UNLOCK_PASSWORD=<password>
  ```

Actions to perform after Kaspersky Embedded Systems Security installation

Kaspersky Embedded Systems Security starts protection and scan tasks immediately after installation if you have activated the application. If you select **Enable real-time protection after installation of application** during installation of Kaspersky Embedded Systems Security, the application scans the computer's file system objects when they are accessed. Kaspersky Embedded Systems Security will run the Critical Areas Scan task every Friday at 8:00 P.M.

We recommend taking the following steps after installing Kaspersky Embedded Systems Security:

- Start the Kaspersky Embedded Systems Security Databases Update task. After installation Kaspersky Embedded Systems Security will scan objects using the database included in its distribution kit. We recommend updating the Kaspersky Embedded Systems Security database immediately. To do so, you must run the Database Update task. The database will then be updated every hour according to the default schedule.

  For example, you can run the Database Update task by running the following command:

  KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser /PROXYPWD:123456

  In this case, Kaspersky Embedded Systems Security database updates are downloaded from Kaspersky Lab update servers. Connection to an update source is established via a proxy server (proxy server address: proxy.company.com, port: 8080) using built-in Windows NTLM authentication to access the server under an account (username: inetuser; password: 123456).

- Run a Critical Areas Scan of the computer if no anti-virus software with real-time file protection was installed on the protected computer before installation of Kaspersky Embedded Systems Security.

► *To start the Critical Areas Scan task using the command line:*

  KAVSHELL SCANCRITICAL /W:scancritical.log

  This command saves the task log in a file named scancritical.log contained in the current folder.

- Configure administrator notifications about Kaspersky Embedded Systems Security events.

Adding / removing components. Sample commands

The On-Demand Scan component is installed automatically. You do not need to specify it in the list of ADDLOCAL key values by adding or deleting Kaspersky Embedded Systems Security components.

► *To add the Applications Launch Control component to the components that have already been installed, run the following command:*

```
msiexec /i ess.msi ADDLOCAL=Oas,AppCtrl /qn
```

or

```
\product\setup.exe /s /p "ADDLOCAL=Oas,AppCtrl"
```

If you list the components you want to install along with the already installed components, Kaspersky Embedded Systems Security will reinstall the existing components.

► *To remove installed components run the following command:*

```
msiexec /i ess.msi
"ADDLOCAL=Oas,Ods,Ksn,AntiExploit,DevCtrl,Firewall,AntiCryptor,LogInspecto
r,AKIntegration,PerfMonCounters,SnmpSupport,Shell,TrayApp,AVProtection,Ram
Disk REMOVE=AppCtrl,Fim" /qn
```

Kaspersky Embedded Systems Security uninstallation. Sample commands

► *To uninstall Kaspersky Embedded Systems Security from the protected computer, run the following command:*

```
msiexec /x ess.msi /qn
```

or

- For 32-bit operating systems:

```
msiexec /x {51AACF7F-421E-40FA-B2B7-FCFE0BACF505} /qn
```

- For 64-bit operating systems:

```
msiexec /x {673F3697-9D6C-4CF4-BB28-478492F45DDC} /qn
```

► *To uninstall Kaspersky Embedded Systems Security Console, run the following command:*

```
msiexec /x esstools.msi /qn
```

or

- For 32-bit operating systems:

```
msiexec /x {26E7C356-E535-4434-9AB1-F1EA4E8A70F4} /qn
```

- For 64-bit operating systems:

```
msiexec /x {7EC1A40D-52F4-4F8F-93BA-F6E68B152C26} /qn
```

► *To uninstall Kaspersky Embedded Systems Security from a protected computer on which password protection is enabled, perform the following command:*

- For 32-bit operating systems:

```
msiexec /x {51AACF7F-421E-40FA-B2B7-FCFE0BACF505} UNLOCK_PASSWORD=***
/qn
```

- For 64-bit operating systems:

```
msiexec /x {673F3697-9D6C-4CF4-BB28-478492F45DDC} UNLOCK_PASSWORD=***
/qn
```

Return codes

The table below contains a list of command-line return codes.

Table 6. Return codes

Code	Description
1324	The destination folder name contains invalid characters.
25001	Insufficient rights to install Kaspersky Embedded Systems Security. To install the application, start the installation wizard with local administrator rights.
25003	Kaspersky Embedded Systems Security cannot be installed on computers running this version of Microsoft Windows. Please start the installation wizard for 64-bit versions of Microsoft Windows.
25004	Incompatible software detected. To continue the installation, uninstall the following software: <list of incompatible software>.
25010	The indicated path cannot be used to save quarantined objects.
25011	The name of the folder for saving quarantined objects contains invalid characters.
26251	Unable to download the Performance Counters DLL.
26252	Unable to download the Performance Counters DLL.
27300	The driver cannot be installed.
27301	The driver cannot be uninstalled.
27302	The network component cannot be installed. Maximum supported number of filtered devices reached.
27303	Anti-virus databases not found.

Installing and uninstalling the application using Kaspersky Security Center

This section contains general information about installing Kaspersky Embedded Systems Security via Kaspersky Security Center. It also describes how to install and uninstall Kaspersky Embedded Systems Security via Kaspersky Security Center and actions to perform after installing Kaspersky Embedded Systems Security.

In this section

General information about installing via Kaspersky Security Center

You can install Kaspersky Embedded Systems Security via Kaspersky Security Center using the remote installation task.

After the remote installation task is complete, Kaspersky Embedded Systems Security will be installed with identical settings on multiple computers.

All computers can be combined in a single administration group, and a group task can be created to install Kaspersky Embedded Systems Security on the computers in this group.

You can create a task to remotely install Kaspersky Embedded Systems Security on a set of computers that are not in the same administration group. When creating this task, you must generate the list of individual computers that Kaspersky Embedded Systems Security should be installed on.

Detailed information on the remote installation task is provided in *Kaspersky Security Center Help*.

Rights to install or uninstall Kaspersky Embedded Systems Security

The account specified in the remote installation (removal) task must be included in the administrators group on each of the protected computers in all cases except those described below:

- If the Kaspersky Security Center Network Agent is already installed on the computers on which Kaspersky Embedded Systems Security is to be installed (regardless of which domain the computers are in or whether they belong to any domain).

  > If the Network Agent is not yet installed on the computers, you can install it with Kaspersky Embedded Systems Security using a remote installation task. Before installing the Network Agent, make sure that the account you want to specify in the task is included in the administrators group on each of the computers.

- All computers on which you want to install Kaspersky Embedded Systems Security are in the same domain as the Administration Server, and the Administration Server is registered as the **Domain Admin** account (if this account has local administrator's rights on the computers within the domain).

By default, when using the **Forced installation** method, the remote installation task is run from the account running the Administration Server.

When working with group tasks or with tasks for sets of computers under forced installation (uninstallation) mode, an account must have the following rights on the client computer:

- Right to execute applications remotely.
- Rights to the **Admin$** share.
- Right to **Log on as a service**.

Installing Kaspersky Embedded Systems Security via Kaspersky Security Center

> Detailed information about generating an installation package and creating a remote installation task is provided in the Kaspersky Security Center Implementation Guide.

If you intend to manage Kaspersky Embedded Systems Security via Kaspersky Security Center in the future, make sure that the following conditions are met:

- The computer where the Kaspersky Security Center Administration Server is installed also has the Administration Plug-in installed (\product\klcfginst.exe file in the Kaspersky Embedded Systems Security distribution kit).
- Kaspersky Security Center Network Agent is installed on protected computers. If Kaspersky Security Center Network Agent is not installed on protected computers, you can install it together with Kaspersky Embedded Systems Security using a remote installation task.

Computers can also be combined into an administration group in order to later manage the protection settings using Kaspersky Security Center policies and group tasks.

► *To install Kaspersky Embedded Systems Security using a remote installation task:*

1. Start the Kaspersky Security Center Administration Console.
2. In Kaspersky Security Center, expand the **Advanced** node.
3. Expand the **Remote installation** child node.
4. In the details pane of the **Installation packages** child node, click the **Create installation package** button.
5. Select the **Create installation package for a Kaspersky Lab application** installation package type.
6. Enter the installation package name.
7. Specify the `ess`.kud file from the Kaspersky Embedded Systems Security distribution kit as the installation package file.

   The **End User License Agreement and Privacy Policy** window opens.
8. If you agree to the terms and conditions of End User License Agreement and Privacy Policy, select **the terms and conditions of this End User License Agreement** and **Privacy Policy describing the handling of data** check boxes in order to proceed with the installation.

   > You must accept the License Agreement and the Privacy Policy to proceed.

9. To change the set of Kaspersky Embedded Systems Security components to be installed (see Section "Modifying the set of components and repairing Kaspersky Embedded Systems Security" on page 56) and the default installation settings (see Section "Installation and uninstallation settings and command line options for the Windows Installer service" on page 40) in the installation package:

   a. In Kaspersky Security Center, expand the **Remote installation** node.

   b. In the details pane of the **Installation packages** child node, open the context menu of the created Kaspersky Embedded Systems Security installation package and select **Properties**.

   c. In the **Properties: <name of installation package>** window in the **Settings** section, do the following:

      a. In the **Components to install** settings group, select the check boxes next to the names of the Kaspersky Embedded Systems Security components you want to install.

      b. In order to indicate a destination folder other than the default one, specify the folder name and path in the **Destination folder** field.

         The path to the destination folder may contain system environment variables. If the folder does not exist on the computer, it will be created.

      c. In the **Advanced installation settings** group, configure the following settings:

         - **Scan the computer for viruses before installation**.
         - **Enable real-time protection after installation of application**.
         - **Add Microsoft recommended files to exclusions list**.

      d. **Add Kaspersky Lab recommended files to exclusions list**.

   d. In the **Properties: <name of installation package>** dialog window, click **OK**.

10. In the **Installation packages** node create a task to remotely install Kaspersky Embedded Systems Security on the selected computers (administration group). Configure the task settings.

    To learn more about creating and configuring remote installation tasks, see the *Kaspersky Security Center Help*.

11. Run the Kaspersky Embedded Systems Security remote installation task.

Kaspersky Embedded Systems Security will be installed on the computers specified in the task.

Actions to perform after Kaspersky Embedded Systems Security installation

After you install Kaspersky Embedded Systems Security, we recommend that you update Kaspersky Embedded Systems Security databases on the computers, and perform a Critical Areas Scan of the computers if no anti-virus applications with enabled real-time protection were installed on the computers before installation of Kaspersky Embedded Systems Security.

If the computers on which Kaspersky Embedded Systems Security was installed are part of the same administration group in the Kaspersky Security Center, you can perform these tasks using the following methods:

1. Create Database Update tasks for the group of computers on which Kaspersky Embedded Systems Security was installed. Set the Kaspersky Security Center Administration Server as the update source.
2. Create an On-Demand Scan group task with the Critical Areas Scan status. Kaspersky Security Center evaluates the security status of each computer in the group based on the results of this task, not based on the results of the Critical Areas Scan task.

3. Create a new policy for the group of computers. In the policy properties, in the **Application settings** section, deactivate the scheduled start of system on-demand scan tasks and the Database Update tasks on the administration group's computers in the settings of the **Run system tasks** subsection.

You can also configure administrator notifications about Kaspersky Embedded Systems Security events.

Installing the Application Console via Kaspersky Security Center

Detailed information about creating an installation package and a remote installation task is provided in the Kaspersky Security Center Implementation Guide.

► *To install the Application Console using a remote installation task:*

1. In the Kaspersky Security Center Administration Console expand the **Advanced** node.
2. Expand the **Remote installation** child node.
3. In the details pane of the Installation packages child node, click the **Create installation package** button. While creating the new installation package:
    a. In the **New Package Wizard** window, select **Create** an installation package for specified executable file as a package type.

    b. Enter the new installation package name.

    c. Select the \console\setup.exe file from the Kaspersky Embedded Systems Security distribution kit folder and select the **Copy entire folder to the installation package** check box.

    d. If required, use the ADDLOCAL command-line option to modify the set of components to be installed in the **Executable file launch settings (optional)** field and change the destination folder.

    For instance, in order to install the Application Console alone in the folder C:\KasperskyConsole without installing the help file and documentation, use the following command-line options:

    ```
    /s /p "ADDLOCAL=MmcSnapin INSTALLDIR=C:\KasperskyConsole EULA=1"
    ```
4. In the **Installation packages** child node, create a task to remotely install the Application Console on the selected computers (administration group). Configure the task settings.

    To learn more about creating and configuring remote installation tasks, see the Kaspersky Security Center Help.
5. Run the remote installation task.

The Application Console is installed on the computers specified in the task.

Uninstalling Kaspersky Embedded Systems Security via Kaspersky Security Center

> If management of Kaspersky Embedded Systems Security on network computers is password protected, enter the password when creating a task to uninstall multiple applications. If the password protection is not managed centrally by a Kaspersky Security Center policy, Kaspersky Embedded Systems Security will be successfully uninstalled from the protected computers, on which the entered password matched the set value. Kaspersky Embedded Systems Security will not be uninstalled from other computers.

► *In order to uninstall Kaspersky Embedded Systems Security, take the following steps in the Kaspersky Security Center Administration Console:*

1. In the Kaspersky Security Center Administration Console, create and start an application removal task.
2. In the task, select the uninstallation method (similar to selecting the installation method; see the previous section) and specify the account that Administration Server will use to access the computers. You can uninstall Kaspersky Embedded Systems Security with only the default uninstallation settings (see Section "Installation and uninstallation settings and command line options for the Windows Installer service" on page 40).

Installing and uninstalling via Active Directory group policies

This section describes installing and uninstalling Kaspersky Embedded Systems Security via Active Directory group polices. It also contains information about actions to perform after installing Kaspersky Embedded Systems Security through group policies.

In this section

Installing Kaspersky Embedded Systems Security via Active Directory group policies

You can install Kaspersky Embedded Systems Security on several computers via the Active Directory group policy. You can install the Application Console the same way.

The computers on which you want to install Kaspersky Embedded Systems Security or the Application Console must be in the same domain and a single organizational unit.

The operating systems on the computers on which you want to install Kaspersky Embedded Systems Security using the policy must be of the same bitness (32-bit or 64-bit).

You must have domain administrator rights.

To install Kaspersky Embedded Systems Security, use the ess_x86(x64).msi installation packages. To install the Application Console, use the esstools.msi installation packages.

> Detailed information about the use of Active Directory group policies is provided in the documentation supplied by Microsoft.

► *To install Kaspersky Embedded Systems Security (or the Application Console):*

1. Save the msi file corresponding to the bitness (32- or 64-bit) of the installed version of the Microsoft Windows operating system in the public folder on the domain controller.
2. Save the key file (see Section "About the key file" on page 78) in the same public folder on the domain controller.
3. In the same public folder on the domain controller, create an install_props.json file with the contents below, which means that you accept the terms of the License Agreement and the Privacy Policy.

   ```
   {
   "EULA": "1",
   "PRIVACYPOLICY": "1"
   }
   ```

4. On the domain controller create a new policy for the group that the computers belong to.
5. Using the **Group Policy Object Editor**, create a new installation package in the **Computer Configuration** node. Specify the path to the msi file for Kaspersky Embedded Systems Security (or Application Console) in UNC (Universal Naming Convention) format.
6. Select the Windows Installer's **Always install with elevated privileges** check box in both the **Computer Configuration** node and in the **User Configuration** node of the selected group.
7. Apply the changes using the `gpupdate /force` command.

Kaspersky Embedded Systems Security will be installed on the computers of the group after they have been restarted.

Actions to perform after Kaspersky Embedded Systems Security installation

After installing Kaspersky Embedded Systems Security on the protected computers, it is recommended that you immediately update the application databases and run a Critical Areas Scan. You can perform these actions (see Section "Actions to perform after Kaspersky Embedded Systems Security installation" on page 53) from the Application Console.

You can also configure administrator notifications about Kaspersky Embedded Systems Security events.

Uninstalling Kaspersky Embedded Systems Security via Active Directory group policies

If you used an Active Directory group policy to install Kaspersky Embedded Systems Security (or the Application Console) on the group of computers, you can use this policy to uninstall Kaspersky Embedded Systems Security (or the Application Console).

You can uninstall the application only with the default uninstallation parameters.

Detailed information about the use of Active Directory group policies is provided in the documentation supplied by Microsoft.

If application management is password protected, you cannot uninstall Kaspersky Embedded Systems Security using Active Directory group policies.

► *To uninstall Kaspersky Embedded Systems Security (or the Application Console):*

1. On the domain controller, select the organizational unit from whose computers you want to uninstall Kaspersky Embedded Systems Security or the Application Console.
2. Select the policy created for the installation of Kaspersky Embedded Systems Security and in the **Group Policies Object Editor**, in the **Software installation** node (**Computer Configuration** > **Software Settings** > **Software installation**) open the context menu of the Kaspersky Embedded Systems Security (or the Application Console) installation package and select the **All tasks > Remove** command.
3. Select the uninstallation method **Immediately uninstall the software from users and computers**.
4. Apply the changes using the `gpupdate / force` command.

Kaspersky Embedded Systems Security is removed from the computers after they are restarted and before logging in to Microsoft Windows.

Checking Kaspersky Embedded Systems Security functions. Using the EICAR test virus

This section describes the EICAR test virus and how to use the EICAR test virus to check the Real-Time Protection and On-Demand Scan features of Kaspersky Embedded Systems Security.

In this section

About the EICAR test virus

This test virus is designed to verify the operation of anti-virus applications. It was developed by the European Institute for Computer Antivirus Research (EICAR).

> The test virus is not a malicious object and does not contain executable code for your computer, but most vendors' anti-virus applications identify it as a threat.

The file containing this test virus is called eicar.com. You can download it from the EICAR website http://www.eicar.org/anti_virus_test_file.htm.

> Before saving the file in a folder on the computer's hard drive, make sure that Real-Time File Protection is disabled on that drive.

The eicar.com file contains a line of text. When scanning the file Kaspersky Embedded Systems Security detects the test threat in this line of text, assigns the **Infected** status to the file, and deletes it. Information about the threat detected in the file will appear in the Application Console and in the task log.

You can use the eicar.com file to check how Kaspersky Embedded Systems Security disinfects infected objects and how it detects probably infected objects. To do this, open the file using a text editor, add one of the prefixes listed in the table below to the beginning of the line of text in the file, and save the file under a new name, e.g. eicar_cure.com.

> To make sure that Kaspersky Embedded Systems Security processes the eicar.com file with a prefix, in the **Objects protection** security settings section, set the **All objects** value for the Real-Time File Protection tasks and Default On-Demand Scan tasks of Kaspersky Embedded Systems Security.

Table 7. Prefixes in EICAR files

Prefix	File status after the scan and Kaspersky Embedded Systems Security action
No prefix	Kaspersky Embedded Systems Security assigns the **Infected** status to the object and deletes it.
SUSP–	Kaspersky Embedded Systems Security assigns the **Probably infected** status to the object detected by the heuristic analyzer and deletes it since probably infected objects are not disinfected.
WARN–	Kaspersky Embedded Systems Security assigns the **Probably infected** status to the object (the object's code partly matches the code of a known threat) and deletes it since probably infected objects are not disinfected.
CURE–	Kaspersky Embedded Systems Security assigns the **Infected** status to the object and disinfects it. If disinfection is successful, the entire text in the file is replaced with the word "CURE".

Checking the Real-Time Protection and On-Demand Scan features

After installing Kaspersky Embedded Systems Security, you can confirm that Kaspersky Embedded Systems Security finds objects containing malicious code. To check this, you can use a test virus from EICAR (see Section "About the EICAR test virus" on page 72).

► *To check the Real-Time Protection feature, take the following steps:*

1. Download the eicar.com file from the EICAR website http://www.eicar.org/anti_virus_test_file.htm. Save it in a public folder on the local drive of any computer on the network.

   > Before you save the file to the folder, make sure that Real-Time File Protection is disabled for the folder.

2. If you want to check that network user notifications are working, make sure that the Microsoft Windows Messenger Service is enabled both on the protected computer and on the computer where you saved the eicar.com file.
3. Open the Application Console.
4. Copy the saved eicar.com file to the local drive of the protected computer using one of the following methods:
   - To test notifications through a Terminal Services window, copy the eicar.com file to the computer after connecting to the computer using the Remote Desktop Connection utility.
   - To test notifications through the Microsoft Windows Messenger Service, use the computer's network places to copy the eicar.com file from the computer where you saved it.

Real-Time File Protection is working correctly if the following conditions are met:

- The eicar.com file is deleted from the protected computer.
- In the Application Console, the task log is given the *Critical* status. The log has a new line with information about a threat in the eicar.com file. (To view the task log, in the Application Console tree, expand the **Real-Time Computer Protection** node, select the **Real-Time File Protection** task and in the details panel of the node click the **Open task log** link).
  - The following Microsoft Windows Messenger Service message appears on the computer from which you copied the file: `Kaspersky Embedded Systems Security blocked access to <path to file on the computer>\eicar.com on computer <network name of computer> at <time that event occurred>. Reason: Threat detected. Virus: EICAR-Test-File. User name: <user name>. Computer name: <network name of the computer from which you copied the file>`.

  > Make sure that the Microsoft Windows Messenger Service is running on the computer from which you copied the eicar.com file.

► *To check the On-Demand Scan feature, take the following steps:*

1. Download the eicar.com file from the EICAR website http://www.eicar.org/anti_virus_test_file.htm. Save it in a public folder on the local drive of any computer on the network.

   > Before you save the file to the folder, make sure that Real-Time File Protection is disabled for the folder.

2. Open the Application Console.
3. Do the following:
   a. Expand the **On-Demand Scan** node in the Application Console tree.
   b. Select the **Critical Areas Scan** child node.
   c. On the **Scan scope settings** tab, open the context menu on the **Network** node and select **Add network file**.
   d. Enter the network path to the eicar.com file on the remote computer in UNC (Universal Naming Convention) format.
   e. Select the check box to include the added network path in the scan scope.
   f. Run the Critical Areas Scan task.

The On-Demand Scan is working as it should if the following conditions are met:

- The eicar.com file is deleted from the computer's hard drive.
- In the Application Console, the task log is given the *Critical* status. The Critical Areas Scan task log has a new line with information about a threat in the eicar.com file. (To view the task log, in the Application Console tree, expand the **On-Demand Scan** child node, select the Critical Areas Scan task and in the details panel, click the **Open task log** link).

Application interface

You can control Kaspersky Embedded Systems Security using the Administration Plug-in and the local Application Console.

Actions in the local Application Console interface are described in the Working with the Application Console section (see Section "Working with the Kaspersky Embedded Systems Security Console" on page 134).

The Kaspersky Security Center Administration Console interface is used to perform actions with the Administration Plug-in. See detailed information about the Kaspersky Security Center interface in the *Kaspersky Security Center Help.*

Application licensing

This section provides information about the main concepts related to licensing of the application.

In this chapter

About the End User License Agreement

The *End User License Agreement* is a binding agreement between you and AO Kaspersky Lab, stipulating the terms on which you may use the application.

Carefully review the terms of the End User License Agreement before you start using the application.

You can review the terms of the End User License Agreement in the following ways:

- During the Kaspersky Embedded Systems Security installation
- By reading the file license.txt. This document is included in the application's distribution kit

By confirming that you agree with the End User License Agreement when installing the application, you signify your acceptance of the terms of the End User License Agreement. If you do not accept the terms of the End User License Agreement, you must abort application installation and must not use the application.

About the license

A license is a time-limited right to use the application, granted to you under the End User License Agreement.

A valid license entitles you to receive the following services:

- Use of the application in accordance with the terms of the End User License Agreement
- Technical support

The scope of service and the period of application use depend on the type of license used to activate the application.

The application is activated using a key file or an activation code for a purchased commercial license.

A commercial license is a paid license granted upon purchase of the application.

Kaspersky Embedded Systems Security implies the following commercial licenses:

- Kaspersky Embedded Systems Security standard license.
- Kaspersky Embedded Systems Security Compliance Edition extended license, which includes two additional system inspection components: File Integrity Monitor and Log Inspection.

When a commercial license expires, the application continues to run but some of its features become unavailable (for example, Kaspersky Embedded Systems Security databases cannot be updated). To continue using all the features of Kaspersky Embedded Systems Security, you must renew your commercial license.

To ensure maximum protection of your computer against security threats, we recommend renewing the license before it expires.

Make sure the additional key that you add has a later expiration date than the active one.

About license certificate

A *license certificate* is a document that you receive along with a key file or an activation code (if applicable).

A license certificate contains the following information about the license provided:

- Order number
- Information about the user who has been granted the license
- Information about the application that can be activated under the license provided
- Limit of the number of licensing units (e.g., devices on which the application can be used under the license provided)
- License validity start date
- License expiration date or license term
- License type

About key

A *key* is a sequence of bits with which you can activate and subsequently use the application in accordance with the terms of the End User License Agreement. A key is generated by Kaspersky Lab.

You can add a key to the application by using a key file. After you add a key to the application, the key is displayed in the application interface as a unique alphanumeric sequence.

Kaspersky Lab can black-list a key over violations of the License Agreement. If your key is blocked, a different key must be added in order for the application to work.

A key may be an "active key" or an "additional key".

An *active key* is the key that the application currently uses to function. A key for a commercial or trial license may be added as the active key. The application can have no more than one active key.

An *additional key* is a key that confirms the right to use the application but is not currently in use. An additional key automatically becomes active when the license associated with the current active key expires. An additional key may be added only if there is an active key.

About the key file

A *key file* is a file with the .key extension provided to you by Kaspersky Lab. Key files are designed to activate the application by adding a license key.

You receive a key file at the email address that you provided when you bought Kaspersky Embedded Systems Security or ordered the trial version of Kaspersky Embedded Systems Security.

You do not need to connect to Kaspersky Lab activation servers in order to activate the application with a key file.

You can restore a key file if it has been accidentally deleted. You may need a key file to register a Kaspersky CompanyAccount, for example.

To restore your key file, perform any of the following actions:

- Contact the license seller.
- Receive a key file through Kaspersky Lab website (https://keyfile.kaspersky.com/en/) by using your available activation code.

About activation code

An *activation code* is a unique sequence of 20 letters and numbers. You have to enter an activation code in order to add a key for activating Kaspersky Embedded Systems Security. You receive the activation code at the email address that you provided when you bought Kaspersky Embedded Systems Security.

To activate the application with an activation code, you need Internet access in order to connect to Kaspersky Lab activation servers.

If you have lost your activation code after installing the application, it can be recovered. You may need the activation code to register a Kaspersky CompanyAccount, for example. To recover your activation code, contact Kaspersky Lab Technical Support.

About data provision

The License Agreement for Kaspersky Embedded Systems Security, specifically the section entitled “Terms of data processing”, specifies the terms, liability, and procedure for sending and processing the data indicated in this Guide. Before accepting the License Agreement, carefully review its terms as well as all documents linked to by the License Agreement.

The data Kaspersky Lab receives from you when you use the application is protected and processed in accordance with the Privacy Policy available at www.kaspersky.com/Products-and-Services-Privacy-Policy.

By accepting the terms of the License Agreement, you agree to automatically send the following data to Kaspersky Lab:

- To support the mechanism for receiving updates – information about the installed application and its activation: identifier of the application being installed and its full version, including build number, type, and license identifier, installation identifier, update task identifier.
- To use the ability to navigate to Knowledge Base articles when application errors occur (Redirector service) – information about the application and link type, specifically: the name, locale, and full version number of the application, type of redirecting link, and error identifier.
- To manage confirmations for data processing – information about the status of acceptance of license agreements and other documents, that stipulate data transferring terms: identifier and version of the License Agreement or other document, as a part of which the data processing terms are accepted or declined; an attribute, signifying the user’s action (confirmation or recall of the terms acceptance); date and time of status changes of the data processing terms acceptance.

You can review the terms of the End User License Agreement in the following ways:

- During the application installation Kaspersky Embedded Systems Security Installation Wizard displays full text of the License Agreement on a step of requesting the acceptance of the terms of the License Agreement.
- At any moment in the TXT file (license.txt), which contains the full License Agreement text. The file is included in the Kaspersky Embedded Systems Security distribution kit, along with the application installation files.

Local data processing

While executing the application’s primary functions described in this Guide, Kaspersky Embedded Systems Security locally processes and stores a sequence of data types on the protected computer. The data processed by the application locally is not automatically sent to Kaspersky Lab or other third-party systems.

Kaspersky Embedded Systems Security locally processes and stores the following data:

- Information about scanned files and detected objects, for example, names and attributes of processed files and full paths to them on the scanned media, file types, actions taken on scanned files, accounts of users performing any actions on the protected network or protected computer, names and data about scanned devices, information about processes running on the system, checksums (MD5, SHA-256), timestamps, digital certificate attributes, data about executed scripts.
- Information about operating system activity and settings, for example, Windows Firewall settings, Windows Event Log entries, names of user accounts, starts of executable files, their checksums and attributes.

Kaspersky Embedded Systems Security processes and stores data as part of the application's basic functionality, including to log application events and receive diagnostic data. Locally processed data is protected in accordance with the configured and applied application settings.

Kaspersky Embedded Systems Security lets you configure the level of protection for data processed locally: you can change user privileges to access process data, change data retention periods for such data, entirely or partially disable functionality that involves data logging, and change the path and attributes of the folder where the data is logged.

Detailed information about configuring application functionality that involves data processing and default settings of processed data storage, can be found in the corresponding sections of this Guide.

By default, all data locally processed by the application during operation is removed after Kaspersky Embedded Systems Security removal from the computer.

Exception applies to files with diagnostics information (trace and dump files) and the application events in the Windows Event Log - it is recommended to manually remove these files.

You can find the detailed information about working with files containing diagnostic data of the application in the corresponding sections of this Guide.

You can delete Windows Event Log files containing the program events of Kaspersky Embedded Systems Security via standard means of the operating system.

Local data processing by means of the application auxiliary components

The Kaspersky Embedded Systems Security installation package comprises the application auxiliary components, which can be installed on your server or computer even if Kaspersky Embedded Systems Security is not installed on it. Such auxiliary components are:

- The Application Console. This component is included in the Kaspersky Embedded Systems Security Administration Tools set and is represented by a Microsoft Management Console snap-in.
- The Administration Plug-in. This component provides a full integration with Kaspersky Security Center application.

While performing the main functions of the application described in this Guide, the application auxiliary components locally process and store a set of data on the computer where they are installed, even if they are installed separately from Kaspersky Embedded Systems Security.

The application components locally process and store the following data:

- The Application Console: the name of the computer with installed Kaspersky Embedded Systems Security (IP address or domain name) to which the Application Console last connected remotely; display parameters configured in the Microsoft Management Console snap-in; data about the last folder in which the user selected objects via the Application Console (by means of system dialog opened by clicking the **Browse** button). The Application Console trace files can also contain the following data: the name of the computer with installed Kaspersky Embedded Systems Security application to which the remote connection was established, the name of the user account under which the remote connection was established.
- The Administration Plug-in can process and temporarily store data processed by Kaspersky Embedded Systems Security; for example, configured parameters of the application tasks and components, parameters of Kaspersky Security Center policies, data sent in network lists.

The data processed by the auxiliary components is not automatically sent to Kaspersky Lab or other third-party systems.

By default, all data locally processed by the application auxiliary components during the operation is deleted after removal of these components.

The exceptions are trace files of the application auxiliary components, it is recommended to delete this files manually.

You can find the detailed information about working with files containing diagnostic data of the application auxiliary components in the corresponding sections of this Guide.

Activating the application with a license key

You can activate Kaspersky Embedded Systems Security by applying a key file.

If an active key has already been added to Kaspersky Embedded Systems Security and you add another key as the active key, the new key replaces the previously added key. The previously added key is removed.

If an additional key has already been added to Kaspersky Embedded Systems Security and you add another key as an additional key, the new key replaces the previously added key. The previously added additional key is removed.

If an active key and an additional key have already been added to Kaspersky Embedded Systems Security and you add a new key as the active key, the new key replaces the previously added active key; the additional key is not removed.

► *To activate Kaspersky Embedded Systems Security using a key file, take the following steps::*

1. In the Application Console tree, expand the **Licensing** node.
2. In the details pane of the **Licensing** node, click the **Add key** link.
3. In the window that opens, click the **Browse** button and select a key file with the .key extension.

   You can also add a key as an additional key. To add a key as an additional key, select the **Use as additional key** check box.

4. Click **OK**.

The selected key file will be applied. Information about the added key will be available on the **Licensing** node.

Activating the application with an activation code

To activate the application using an activation code, the computer must be connected to the Internet.

You can activate Kaspersky Embedded Systems Security by using an activation code.

When activating the application with this method, Kaspersky Embedded Systems Security sends data to the activation server to verify the entered code:

- If the activation code verification is successful, the application is activated.
- If the activation code verification fails, the corresponding notification is displayed. In this case, you must contact the software vendor from whom you purchased your Kaspersky Embedded Systems Security license.

- If the number of activations with the activation code is exceeded, the corresponding notification is displayed. The application activation procedure is interrupted, and the application suggests that you contact Kaspersky Lab Technical Support.

► *To obtain a key to activate Kaspersky Embedded Systems Security using an activation code, take the following steps:*

1. In the Application Console tree, expand the **Licensing** node.
2. In the details pane of the **Licensing** node, click the **Add activation code** link.
3. In the window that opens, enter the activation code in the **Activation code** field.
    - If you want to use the activation code as an additional key, enable **Use as additional key** check box.
    - If you want to view the license information, click the **Show license information** button; it will be displayed in the **License information** group box.
4. Click **OK**.

    Kaspersky Embedded Systems Security sends information about the applied activation code to the activation server.

Viewing information about the current license

Viewing licensing information

Information about the current license is displayed in the details pane of the **Kaspersky Embedded Systems Security** node of the Application Console. A key can have the following statuses:

- **Checking the key status** – Kaspersky Embedded Systems Security is checking the applied key file or activation code and waiting for a response about the current key status.
- **License expiration date** – Kaspersky Embedded Systems Security has been activated until the specified date and time. The key status is highlighted in yellow in the following cases:
    - The license will expire in 14 days and no additional key has been applied.
    - The added key has been blacklisted and is about to be blocked.
- **License has expired** – Kaspersky Embedded Systems Security is not activated because the license has expired. The status is highlighted in red.
- **End User License Agreement has been violated** – Kaspersky Embedded Systems Security is not activated because the terms of the End User License Agreement (see Section "About the End User License Agreement" on page 76) have been violated. The status is highlighted in red.
- **Key is blacklisted** – The added key has been blocked and blacklisted by Kaspersky Lab, for example, if the key has been used by third parties to activate the application illegally. The status is highlighted in red.

Viewing information about the current license

► *To view information about the current license,*

in the Application Console tree, expand the **Licensing** node.

General information about the current license is displayed in the details pane of the **Licensing** node (see the table below).

Table 8. General information about the license in the Licensing node

Field	Description
Activation code	The activation code. This field is filled in if you activate the application using an activation code.
Activation status	Information about the activation status of the application. The **Activation** column of the **Licensing** node's details pane can have the following statuses: • **Applied** – if you have activated the application using an activation code or key file. **Activation** – if you have applied an activation code to activate the application, but the activation process has not been finalized yet. The status changes to *Applied* after activation of the application is complete and the contents of the node's details pane are refreshed. • **Activation error** – if application activation failed. You can view the cause of unsuccessful activation in the task log.
Key	The key used to activate the application.
License type	License type: commercial or trial.
Expiration date	Expiration date and time of the license associated with the active key.
Activation code status or key status	Activation code status or key status: Active or Additional.

► *To view detailed information about the license,*

on the **Licensing** node, open the context menu on the line with license data that you want to expand and select **Properties**.

In the **Properties: <Activation code status or key status>** window, the **General** tab displays detailed information about the current license, and the **Advanced** tab displays information about the customer and the contact details of Kaspersky Lab or the retailer from whom you purchased Kaspersky Embedded Systems Security (see the table below).

Table 9. Detailed license information in the Properties: <Activation code status or key status> window

Field	Description
General tab	
Key	The key used to activate the application.
Key addition date	Date when the key was added to the application.
License type	License type: commercial or trial.
Days till expiration	Number of days remaining until the expiration of the license associated with the active key.
Expiration date	Expiration date and time of the license associated with the active key. If you activate the application under an unlimited subscription, the field value is *Unlimited*. If Kaspersky Embedded Systems Security is unable to determine the license expiration date, the field value is *Unknown*.
Application	The name of the application activated with the key file or activation code.
Key usage restriction	Restriction on use of the key (if any).
Eligible for technical support	Information on whether Kaspersky Lab or one of its partners will provide technical support under the license terms.
Advanced tab	
Information about the license	Current license number.
Support information	Contact details of Kaspersky Lab or its partner providing technical support. This field may be empty if technical support is not provided.
Owner information	Information about the license owner: a customer name and the name of the organization for which the license was acquired.

Functional limitations when the license expires

When the current license expires, the following limitations are applied to the functional components:

- All tasks are stopped, except the Real-Time File Protection, On-Demand Scan and Application Integrity Control tasks.
- You cannot start any tasks except the Real-Time File Protection, On-Demand Scan and Application Integrity Control. These tasks continue to run using the old anti-virus databases.
- Exploit Prevention functionality is limited:
  - Processes are protected until they are restarted.
  - New processes cannot be added to the protection scope.

Other functions (repositories, logs, diagnostic information) are still available.

Renewing the license

By default, when the license has 14 days remaining before expiration, Kaspersky Embedded Systems Security notifies you about the approaching expiration. In this case, the **License expiration date** status is highlighted in yellow in the details pane of the **Kaspersky Embedded Systems Security** node.

You can renew the license before the expiration date using an additional key file or an activation code. This ensures that your computer remains protected after expiration of the current license and before you activate the application with a new license.

► *To renew a license, take the following steps:*

1. Obtain a new activation code or a key file.
2. In the Application Console tree, open the **Licensing** node.
3. Perform one of the following actions in the details pane of the **Licensing** node:
   - If you want to renew a license using an additional key:
     a. Click the **Add** key link.
     b. In the window that opens, click the **Browse** button and select a new key file with the .key extension.
     c. Select the **Use as additional key** check box.
   - If you want to renew a license using an activation code:
     a. Click the **Add activation code** link.
     b. Enter the purchased activation code in the window that opens.
     c. Select the **Use as additional key** check box.

   > An Internet connection is required to apply an activation code.

4. Click **OK**.

The additional key will be added and automatically applied upon expiration of the current Kaspersky Embedded Systems Security license.

Deleting key

You can remove the added key.

If an additional key has been added to Kaspersky Embedded Systems Security and you remove the active key, the additional key automatically becomes the active key.

> If you delete an added key, you can restore it by re-applying the key file.

► *To remove a key that has been added:*

1. In the Application Console tree, select the **Licensing** node.
2. In the details pane of the **Licensing** node in the table containing information on added keys, select the key that you want to remove.
3. In the context menu of the line containing information on the selected key, select **Remove**.
4. Click the **Yes** button in the confirmation window to confirm that you want to delete the key.

The selected key will be removed.

Working with the Administration Plug-in

This section provides information about the Kaspersky Embedded Systems Security Administration Plug-in and describes how to manage the application installed on a protected computer or on a group of computers.

In this chapter

Managing Kaspersky Embedded Systems Security from Kaspersky Security Center

You can centrally manage several computers with Kaspersky Embedded Systems Security installed and included in an administration group by means of the Kaspersky Embedded Systems Security Administration Plug-in. Kaspersky Security Center also lets you separately configure the operation settings of each computer included in the administration group.

The administration group is created on the side of Kaspersky Security Center manually and includes several computers with Kaspersky Embedded Systems Security installed, for which you want to configure the same control and protection settings. For details on using administration groups, see the *Kaspersky Security Center Help*.

> Application settings for one computer are unavailable if the operation of Kaspersky Embedded Systems Security on that computer is controlled by an active Kaspersky Security Center policy.

Kaspersky Embedded Systems Security can be managed from Kaspersky Security Center in the following ways:

- **Using Kaspersky Security Center policies**. Kaspersky Security Center policies can be used to remotely configure the same protection settings for a group of computers. Task settings specified in the active policy have priority over task settings configured locally in the Application Console or remotely in the **Properties: <Computer name>** window of Kaspersky Security Center.

  You can use policies to configure general application settings, Real-Time Protection task settings, Local Activity Control tasks settings, scheduled system task start settings, and profile usage settings.
- **Using Kaspersky Security Center group tasks**. Kaspersky Security Center group tasks allow remote configuration of common settings of tasks with an expiration period for a group of computers.
- You can use group tasks to activate the application, configure On-Demand Scan task settings, update task settings, and Rule Generator for Applications Launch Control task settings.

- **Using tasks for a set of devices**. Tasks for a set of devices allow remote configuration of common task settings with a limited execution period for computers that do not belong to any one of the administration groups.
- **Using the properties window of a single computer**. In the **Properties: <Computer name>** window, you can remotely configure the task settings for a single computer included in the administration group. You can configure both general application settings and settings of all Kaspersky Embedded Systems Security tasks if the selected computer is not controlled by an active Kaspersky Security Center policy.

Kaspersky Security Center makes it possible to configure application settings, advanced features, and lets you work with logs and notifications. You can configure these settings for a group of computers as well as for an individual computer.

Managing application settings

This section contains information about configuring Kaspersky Embedded Systems Security general settings in Kaspersky Security Center.

In this chapter

Managing Kaspersky Embedded Systems Security from Kaspersky Security Center

You can centrally manage several computers with Kaspersky Embedded Systems Security installed and included in an administration group by means of the Kaspersky Embedded Systems Security Administration Plug-in. Kaspersky Security Center also lets you separately configure the operation settings of each computer included in the administration group.

The administration group is created on the side of Kaspersky Security Center manually and includes several computers with Kaspersky Embedded Systems Security installed, for which you want to configure the same control and protection settings. For details on using administration groups, see the *Kaspersky Security Center Help*.

> Application settings for one computer are unavailable if the operation of Kaspersky Embedded Systems Security on that computer is controlled by an active Kaspersky Security Center policy.

Kaspersky Embedded Systems Security can be managed from Kaspersky Security Center in the following ways:

- **Using Kaspersky Security Center policies**. Kaspersky Security Center policies can be used to remotely configure the same protection settings for a group of computers. Task settings specified in the active policy have priority over task settings configured locally in the Application Console or remotely in the **Properties: <Computer name>** window of Kaspersky Security Center.

  You can use policies to configure general application settings, Real-Time Protection task settings, Local Activity Control tasks settings, scheduled system task start settings, and profile usage settings.
- **Using Kaspersky Security Center group tasks**. Kaspersky Security Center group tasks allow remote configuration of common settings of tasks with an expiration period for a group of computers.
- You can use group tasks to activate the application, configure On-Demand Scan task settings, update task settings, and Rule Generator for Applications Launch Control task settings.
- **Using tasks for a set of devices**. Tasks for a set of devices allow remote configuration of common task settings with a limited execution period for computers that do not belong to any one of the administration groups.

- **Using the properties window of a single computer**. In the **Properties: <Computer name>** window, you can remotely configure the task settings for a single computer included in the administration group. You can configure both general application settings and settings of all Kaspersky Embedded Systems Security tasks if the selected computer is not controlled by an active Kaspersky Security Center policy.

Kaspersky Security Center makes it possible to configure application settings, advanced features, and lets you work with logs and notifications. You can configure these settings for a group of computers as well as for an individual computer.

Navigation

Learn how to navigate to the required task settings via the interface.

In this section

Opening the general settings via the policy

► *To open the application settings of the Kaspersky Embedded Systems Security via the policy:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure the task.
3. Select the **Policies** tab.
4. Double-click the policy name you want to configure.
5. In the **Properties: <Policy name>** window that opens, select the **Application settings** section.
6. Click the **Settings** button in the subsection of the setting, that you want to configure.

Opening the general settings in the application properties window

► *To open the properties window of the Kaspersky Embedded Systems Security for a single computer:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure the task.
3. Select the **Devices** tab.
4. Open the **Properties: <Computer name>** window in one of the following ways:
   - Double-click the name of the protected computer.
   - Select the **Properties** item in the context menu of the protected computer.

   The **Properties: <Computer name>** window opens.
5. In the **Applications** section, select the **Kaspersky Embedded Systems Security**.
6. Click the **Properties** button.

The **"Kaspersky Embedded Systems Security" application settings** window opens.

7. Select the **Application settings** section.

Configuring general application settings in Kaspersky Security Center

You can configure general Kaspersky Embedded Systems Security settings from Kaspersky Security Center for a group of computers or for one computer.

In this section

Configuring scalability and the interface in Kaspersky Security Center

► *To configure scalability settings and the application interface:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.
3. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring a policy" on page 112).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in the Application settings window of the Kaspersky Security Center" on page 117).

   > If an active Kaspersky Security Center policy is applied to a device, and this policy blocks changes to application settings, then these settings cannot be edited in the **Application settings** window.

4. In the **Application settings** section, in the **Scalability and interface** block, click **Settings**.

5. In the **Advanced application settings** window on the **General** tab, configure the following settings:
    - In the **Scalability settings** section, configure the settings that define the number of processes used by Kaspersky Embedded Systems Security:
        - **Automatically detect scalability settings**.

          Kaspersky Embedded Systems Security automatically regulates the number of processes used.

          This is the default value.
        - **Set the number of working processes manually**.

          Kaspersky Embedded Systems Security regulates the number of active working processes according to the values specified.
            - **Maximum number of active processes.**

              Maximum number of processes that Kaspersky Embedded Systems Security uses. The entry field is available if the **Set the number of working processes manually** option is selected.
            - **Number of processes for real-time protection.**

              Maximum number of processes that are used by the Real-Time Protection task components. The entry field is available if the **Set the number of working processes manually** option is selected.
            - **Number of processes for background on-demand scan tasks.**

              Maximum number of processes used by the On-Demand Scan component when running On-Demand Scan tasks in background mode. The entry field is available if the **Set the number of working processes manually** option is selected.
        - In the **Interaction with user** section, configure the display of the application System Tray Icon in the notification area: clear or select the **Display System Tray Icon in the taskbar** check box.
6. On the **Hierarchical storage** tab, select the option for accessing the hierarchical storage.
7. Click **OK**.

The configured application settings are saved.

Configuring security settings in Kaspersky Security Center

► *To configure security settings manually, take the following steps:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.
3. Perform one of the following actions in the details pane of the selected administration group:
    - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring a policy" on page 112).

- To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in the Application settings window of the Kaspersky Security Center" on page 117).

  > If an active Kaspersky Security Center policy is applied to a device, and this policy blocks changes to application settings, then these settings cannot be edited in the **Application settings** window.

4. In the **Application settings** section, click the **Settings** button under the **Security** settings.
5. In the **Security settings** window, configure the following settings:

- In the **Reliability settings** section, configure the settings for recovery of Kaspersky Embedded Systems Security tasks when the application returns an error or terminates.
  - **Perform task recovery**

    This check box enables or disables the recovery of Kaspersky Embedded Systems Security tasks when the application returns an error or terminates.

    If the check box is selected, Kaspersky Embedded Systems Security automatically recovers Kaspersky Embedded Systems Security tasks when the application returns an error or terminates.

    If the check box is cleared, Kaspersky Embedded Systems Security does not recover Kaspersky Embedded Systems Security tasks when the application returns an error or terminates.

    The check box is selected by default.
  - **Recover on-demand scan tasks no more than (times)**

    The number of attempts to recover an On-Demand Scan task after Kaspersky Embedded Systems Security returns an error. The entry field is available if the **Perform task recovery** check box is selected.
- In the **Actions when switching to UPS backup power** section, specify limitations on computer load created by Kaspersky Embedded Systems Security after switching to UPS power:
  - **Do not start scheduled scan tasks**

    This check box enables or disables the start of a scheduled scan task after the computer switches to a UPS source until the standard power supply mode is restored.

    If the check box is selected, Kaspersky Embedded Systems Security does not start scheduled scan tasks after the computer switches to a UPS source until the standard power supply mode is restored.

    If the check box is cleared, Kaspersky Embedded Systems Security starts scheduled scan tasks regardless of the power supply mode.

    The check box is selected by default.
  - **Stop current scan tasks**

    The check box enables or disables the execution of running scan tasks after the computer switches to a UPS source.

    If the check box is selected, Kaspersky Embedded Systems Security pauses running scan tasks after the computer switches to a UPS source.

If the check box is cleared, Kaspersky Embedded Systems Security continues running scan tasks after the computer switches to a UPS source.

The check box is selected by default.

- In the **Password protection settings** section, set a password to protect access to Kaspersky Embedded Systems Security functions.

6. Click **OK**.

The scalability and reliability settings are saved.

Configuring connection settings using Kaspersky Security Center

The configured connection settings are used to connect Kaspersky Embedded Systems Security to update and activation servers and during integration of applications with KSN services.

► *To configure the connection settings take the following steps:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.
3. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring a policy" on page 112).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in the Application settings window of the Kaspersky Security Center" on page 117).

   > If an active Kaspersky Security Center policy is applied to a device, and this policy blocks changes to application settings, then these settings cannot be edited in the **Application settings** window.

4. In the **Application settings** section click the **Settings** button in the **Connections** block.

   The **Connection settings** window opens.

5. In the **Connection settings** window, configure the following settings:
   - In the **Proxy server settings** section, select the proxy server usage settings:
     - **Do not use proxy server**.

       If this option is selected, Kaspersky Embedded Systems Security connects to KSN services directly, without using any proxy server.

     - **Use specified proxy server settings**.

       If this option is selected, Kaspersky Embedded Systems Security connects to KSN using proxy server settings specified manually.

     - IP address or the symbol name of the proxy server and the port number.

    - **Do not use proxy server for local addresses**.

      The check box enables or disables the use of a proxy server when accessing computers located in the same network as the computer with Kaspersky Embedded Systems Security installed.

      If this check box is selected, computers are accessed directly from the network, which hosts the computer with Kaspersky Embedded Systems Security installed. No proxy server is used.

      If the check box is cleared, the proxy server is applied to connect to local computers.

      The check box is selected by default.

  - In the **Proxy server authentication settings** section, specify the authentication settings:
    - Select the authentication settings in the drop-down list.
      - **Do not use authentication** – authentication is not performed. This mode is selected by default.
      - **Use NTLM authentication** – authentication is performed using the NTLM network authentication protocol developed by Microsoft.
      - **Use NTLM authentication with user name and password** – authentication is performed using the name and password through the NTLM network authentication protocol developed by Microsoft.
      - **Apply user name and password** – authentication is performed using the user name and password.
    - Enter user name and password, if needed.
  - In the **Licensing** block clear or select the **Use Kaspersky Security Center as a proxy server when activating the application**.

6. Click **OK**.

The configured connection settings are saved.

Configuring scheduled start of local system tasks

You can use policies to allow or block start of the local system On-Demand Scan task and the Update task according to the following schedule configured locally on each computer in the administration group:

- If the scheduled start of a specific type of local system task is prohibited by a policy, these tasks will not be performed on the local computer as per the schedule. You can start the local system tasks manually.
- If the scheduled start of a specific type of local system task is allowed by a policy, these tasks will be performed in accordance with the scheduled parameters configured locally for this task.

By default, start of local system tasks is prohibited by policy.

> We recommend that you do not allow local system tasks to start if updates or on-demand scans are being administered by Kaspersky Security Center group tasks.

If you do not use group update or on-demand scan tasks, allow local system tasks to be started in the policy: Kaspersky Embedded Systems Security will perform application database and module updates, and start all local system on-demand scan tasks in accordance with the default schedule.

You can use policies to allow or block the scheduled start of the following local system tasks:

- On-Demand Scan tasks: Critical Areas Scan, Quarantine Scan, Scan at Operating System Startup, Application Integrity Control.
- Update tasks: Database Update, Software Modules Update and Copying Updates.

> If the protected computer is excluded from the administration group, the system tasks schedule will be enabled automatically.

► *To allow or block the scheduled start of Kaspersky Embedded Systems Security system tasks in a policy take the following steps:*

1. In the **Managed devices** node in the Administration Console tree, expand the required group and select the **Policies** tab.
2. On the **Policies** tab in the context menu of the policy with which you want to configure the scheduled start of Kaspersky Embedded Systems Security system tasks on the group of computers, select the **Properties** item
3. In the **Properties: <Policy name>** window, open the **Application settings** section. In the **Run system tasks** section, click the **Settings** button and perform the following:
   - Select the **Allow on-demand scan tasks launch** and **Allow update tasks and Copying Update task launch** check boxes to allow the scheduled launch of the listed tasks.
   - Clear the **Allow on-demand scan tasks launch** and **Allow update tasks and Copying Update task launch** check boxes to disable the scheduled launch of the listed tasks.

   > Selecting or clearing the check box will not affect the start settings of any local custom tasks of this type.
4. Make certain that the policy you are configuring is active and applied to the selected group of computers.
5. Click **OK**.

The configured scheduled task start settings are applied for the selected tasks.

Configuring Quarantine and Backup settings in Kaspersky Security Center

► *To configure general Backup settings in Kaspersky Security Center:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.

3. Perform one of the following actions in the details pane of the selected administration group:

   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring a policy" on page 112).

   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in the Application settings window of the Kaspersky Security Center" on page 117).

   > If an active Kaspersky Security Center policy is applied to a device, and this policy blocks changes to application settings, then these settings cannot be edited in the **Application settings** window.

4. In the **Supplementary** section, click the **Settings** button in the **Storages** subsection.
5. Use the **Backup** tab of the **Storages** settings window to configure the following Backup settings:

   - To specify the backup folder, use the **Backup folder** field to select the required folder on the local drive of the protected computer, or enter its full path.

   - To set the maximum size of Backup, select the **Maximum Backup size (MB)** check box and specify the relevant value in megabytes in the entry field.

   - To set the threshold of free space in Backup, define the value of the **Maximum Backup size (MB)** setting, select the **Threshold value for space available (MB)** check box, and specify the minimum value of free space in the Backup folder in megabytes.

   - To specify a folder for restored objects, select the relevant folder on a local drive of the protected computer in the **Restoration settings** section, or enter the name of the folder and the full path to it in the **Target folder for restoring objects** field.

6. In the **Storages** settings window on the **Quarantine** tab, configure the following Quarantine settings:

   - To change the quarantine folder, in the **Quarantine folder** entry field specify the complete path to the folder on the local drive of the protected computer.

   - To set the maximum Quarantine size, select the **Maximum Quarantine size (MB)** check box and specify the value of this parameter in megabytes in the entry field.

   - To set the minimum amount of free space in Quarantine, select the **Maximum Quarantine size (MB)** check box and the **Threshold value for space available (MB)** check box, and then specify the value of this parameter in megabytes in the entry field.

   - To change the folder to which objects are restored from Quarantine, in the **Target folder for restoring objects** entry field specify the complete path to the folder on the local drive of the protected computer.

7. Click **OK**.

The configured Quarantine and Backup settings are saved.

Configuring logs and notifications

The Kaspersky Security Center Administration Console can be used to configure notifications for administrator and users about the following events related to Kaspersky Embedded Systems Security and the status of Anti-Virus protection on the protected computer:

- The administrator can receive information about events of selected types;
- LAN users who access the protected computer and terminal computer users can receive information about events of the *Object detected* type.

Notifications about Kaspersky Embedded Systems Security events can be configured either for a single computer using the **Properties: <Computer name>** window of the selected computer, or for a group of computers in the **Properties: <Policy name>** window of the selected administration group.

On the **Event notifications** tab or in the **Notification settings** window, you can configure the following types of notifications:

- Administrator notifications about events of selected types can be configured using the **Event notifications** tab (the standard tab of the Kaspersky Security Center application). For details on notification methods, see the *Kaspersky Security Center Help*.
- Both administrator and user notifications can be configured in the **Notification settings** window.

You can configure notifications for some events types in the window or on the tab only; you can use both the window and the tab for configuring notifications for other events types.

> If you configure notifications about events of the same type using the same mode on the **Event notifications** tab and in the **Notification settings** window, the system administrator will receive notifications of those events twice but in the same mode.

In this section

Configuring log settings

► *To configure Kaspersky Embedded Systems Security logs, perform the following steps:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.
3. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring a policy" on page 112).

- To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in the Application settings window of the Kaspersky Security Center" on page 117).

  > If an active Kaspersky Security Center policy is applied to a device, and this policy blocks changes to application settings, then these settings cannot be edited in the **Application settings** window.

4. In the **Logs and notifications** section, click the **Settings** button in the **Task logs** block.
5. In the **Logs settings** window define the following settings of Kaspersky Embedded Systems Security according to your requirements:
   - Configure the level of detail of events in logs. To do this, perform the following actions:
     a. In the **Component** list select the component of Kaspersky Embedded Systems Security for which you want to set the detail level.
     b. To define level of detail in the task logs and System audit log for the selected component, choose the level you need from **Importance level**.
   - To change the default location for logs, specify full path to the folder or click the **Browse** button to select it.
   - Specify how many days task logs will be stored.
   - Specify how many days information displayed in the **System audit log** node will be stored.
6. Click **OK**.

The configured log settings are saved.

Security log

Kaspersky Embedded Systems Security maintains a log of events associated with security breaches or attempted security breaches on the protected computer. The following events are recorded in this log:

- Exploit Prevention events.
- Critical Log Inspection events.
- Critical events that indicate an attempted security breach (for the Real-Time Computer Protection, On-Demand Scan, File Integrity Monitor, Applications Launch Control, and Device Control tasks).

You can clear the Security log as well as the System audit log (see Section "Deleting events from the system audit log" on page 202). Moreover, Kaspersky Embedded Systems Security records system audit events regarding clearing the Security log.

Configuring SIEM integration settings

To reduce the load on low-performance devices and to reduce the risk of system degradation as a result of increased volumes of application logs, you can configure the publication of audit events and task performance events to the *syslog server* via the Syslog protocol.

A syslog server is an external server for aggregating events (SIEM). It collects and analyzes received events and also performs other actions for managing logs.

You can use SIEM integration in two modes:

- Duplicate events on the syslog server: this mode prescribes that all task performance events whose publication is configured in the settings of logs as well as all system audit events continue to be stored on the local computer even after they are sent to SIEM.

  It is recommended to use this mode to maximally reduce the load on the protected computer.
- Delete local copies of events: this mode prescribes that all events that are registered during application operation and published to SIEM will be deleted from the local computer.

  > The application never deletes local versions of the security log.

Kaspersky Embedded Systems Security can convert events in application logs into formats supported by the syslog server so that those events can be transmitted and successfully recognized by SIEM. The application supports conversion into structured data format and into JSON format.

To reduce the risk of unsuccessful transmission of events to SIEM, you can define the settings for connecting to the mirror syslog server.

A mirror syslog server is an additional syslog server to which the application switches automatically if the connection to the main syslog server is unavailable or if the main server cannot be used.

By default, SIEM integration is not used. You can enable and disable SIEM integration, and configure functionality settings (see the table below).

Table 10. SIEM integration settings

Setting	Default Value	Description
Send events to a remote syslog server via syslog protocol	Not applied	You can enable or disable SIEM integration by selecting or clearing the check box, respectively.
Remove local copies for events that have been sent to a remote syslog server	Not applied	You can configure the settings for storing local copies of logs after they are sent to SIEM by selecting or clearing the check box.
Events format	Structured data	You can select one of two formats to which the application converts its events prior to sending them to the syslog server for better recognition of these events by SIEM.
Connection protocol	TCP	You can use the drop-down list to configure the connection to the main syslog server via the UDP or TCP protocols; to the mirror syslog server via the TCP protocol.
Main syslog server connection settings	IP address: 127.0.0.1 Port: 514	You can use the appropriate fields to configure the IP address and port used to connect to the main syslog server. You can specify the IP address only in IPv4 format.
Use mirror syslog server if the main server is not accessible	Not applied	You can use the check box to enable or disable the use of a mirror syslog server.
Mirror syslog server connection settings	IP address: 127.0.0.1 Port: 514	You can use the appropriate fields to configure the IP address and port used to connect to the mirror syslog server. You can specify the IP address only in IPv4 format.

► *To configure SIEM integration settings:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.
3. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring a policy" on page 112).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in the Application settings window of the Kaspersky Security Center" on page 117).

   > If an active Kaspersky Security Center policy is applied to a device, and this policy blocks changes to application settings, then these settings cannot be edited in the **Application settings** window.

4. In the **Logs and notifications** section click the **Settings** button in the **Task logs** block.

   The **Logs and notifications settings** window opens.

5. Select the **SIEM integration** tab.
6. In the **Integration settings** section, select the **Send events to a remote syslog server via syslog protocol** check box.

   The check box enables or disables the functionality for sending published events to an external syslog server.

   If the check box is selected, the application sends published events to SIEM according to the configured SIEM integration settings.

   If the check box is cleared, the application does not perform SIEM integration. You cannot configure SIEM integration settings if the check box is cleared.

   The check box is cleared by default.
7. If necessary, in the **Integration settings** section, select the **Remove local copies for events that have been sent to a remote syslog server** check box.

   The check box enables or disables deletion of local copies of logs when they are sent to SIEM.

   If the check box is selected, the application deletes the local copies of events after they have been successfully published to SIEM. This mode is recommended on low-performance computers.

   If the check box is cleared, the application only sends events to SIEM. Copies of logs continue to be stored locally.

   The check box is cleared by default.

   > The status of the **Remove local copies for events that have been sent to a remote syslog server** check box does not affect the settings for storing events of the security log: the application never automatically deletes security log events.
8. In the **Events format** section, specify the format to which you want to convert application operation events so that they can be sent to SIEM.

   By default, the application converts them into structured data format.
9. In the **Connection settings** section:
   - Specify the SIEM connection protocol.
   - Specify the settings for connecting to the main syslog server.

     You can specify an IP address in IPv4 format only.
   - Select the **Use mirror syslog server if the main server is not accessible** check box if you want the application to use other connection settings when unable to send events to the main syslog server.
     - Specify the following settings for connecting to the mirror syslog server: **IP address** and **Port**.

       The **IP address** and **Port** fields for the mirror syslog server cannot be edited if the **Use mirror syslog server if the main server is not accessible** check box is cleared.

       You can specify an IP address in IPv4 format only.
10. Click **OK**.

The configured SIEM integration settings will be applied.

Configuring notification settings

► *To configure Kaspersky Embedded Systems Security notifications, perform the following steps:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.
3. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring a policy" on page 112).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in the Application settings window of the Kaspersky Security Center" on page 117).

   > If an active Kaspersky Security Center policy is applied to a device, and this policy blocks changes to application settings, then these settings cannot be edited in the **Application settings** window.

4. In the **Logs and notifications** section, click the **Settings** button in the **Event notifications** subsection.
5. In the **Notification settings** window, define the following settings of Kaspersky Embedded Systems Security according to your requirements:
   - In the **Notification settings** list select the type of notification whose settings you want to configure.
   - In the **Notify users** section configure the user notification method. If necessary, enter the text of the notification message.
   - In the **Notify administrators** section configure the administrator notification method. If necessary, enter the text of the notification message. If necessary, configure additional notification settings by clicking the **Settings** button.
   - In the **Event generation thresholds** section, specify the time intervals after which Kaspersky Embedded Systems Security logs the events *Application database is out of date, Application database is extremely out of date* and *Critical Areas Scan has not been performed for a long time*.
     - **Application database is out of date (days)**

       The number of days that have passed since the last Database Update.

       The default value is 7 days.
     - **Application database is extremely out of date (days)**

       The number of days that have passed since the last Database Update.

       The default value is 14 days.
     - **Critical Areas Scan has not been performed for a long time (days)**

       The number of days after the last successful Critical Areas Scan.

       The default value is 30 days.
6. Click **OK**.

The configured notification settings are saved.

Configuring interaction with the Administration Server

► *To select the types of objects about which Kaspersky Embedded Systems Security sends information to the Kaspersky Security Center Administration Server:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.
3. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring a policy" on page 112).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in the Application settings window of the Kaspersky Security Center" on page 117).

   > If an active Kaspersky Security Center policy is applied to a device, and this policy blocks changes to application settings, then these settings cannot be edited in the **Application settings** window.

4. In the **Logs and notifications** section, click the **Settings** button in the **Interaction with Administration Server** block.

   The **Administration Server Network lists** window opens.
5. In the **Administration Server Network lists** window, select the types of objects about which Kaspersky Embedded Systems Security will send information to the Kaspersky Security Center Administration Server:
   - Quarantined objects.
   - Backed up objects.
6. Click **OK**.

   Kaspersky Embedded Systems Security will send information about the selected object types to the Administration Server.

Creating and configuring policies

This section provides information on using Kaspersky Security Center policies for managing Kaspersky Embedded Systems Security on several computers.

Global Kaspersky Security Center policies can be created for managing protection on several computers where Kaspersky Embedded Systems Security is installed.

A policy enforces the Kaspersky Embedded Systems Security settings, functions and tasks specified in it on all the protected computers for one administration group.

Several policies for one administration group can be created and enforced in turns. The policy currently active for a group has the *active* status in Administration Console.

Information on policy enforcement is logged in the Kaspersky Embedded Systems Security system audit log. This information can be viewed in the Application Console in the **System audit log** node.

Kaspersky Security Center offers one way to apply policies on local computers: *Prohibit changing the settings*. After a policy has been applied, Kaspersky Embedded Systems Security uses the values for settings next to which you have selected the 🔒 icon in the policy properties on local computers instead of the values for those settings that had been actual before the policy was applied. Kaspersky Embedded Systems Security does not apply the values of active policy settings next to which the 🔓 icon is selected in the policy properties.

If a policy is active, the values of settings marked with the 🔒 icon in the policy are displayed in the Application Console but cannot be edited. The values of other settings (marked with the 🔓 icon in the policy) can be edited in the Application Console.

The settings configured in the active policy and marked with the 🔒 icon also block changes in Kaspersky Security Center for one computer in the **Properties: <Computer name>** window.

The settings, that are specified and sent to the local computer using an active policy, are saved in the local tasks settings after the active policy is disabled.

If the policy defines the settings for any Real-Time Computer Protection task, and if such a task is currently running, then the settings defined by the policy will be modified as soon as the policy is applied. If the task is not running, the settings are applied when it starts.

In this chapter

Creating policy

The process of creating a policy involves the following steps:

1. Creating a policy using the policy wizard. Real-Time Computer Protection tasks settings can be configured using the wizard dialogs.
2. Configuring policy settings. In the **Properties: <Policy name>** window of the created policy, you can define the Real-Time Computer Protection tasks settings, the general settings of Kaspersky Embedded Systems Security, the Quarantine and Backup settings, the level of detail for task logs, as well as user and administrator notifications about Kaspersky Embedded Systems Security events.

► *To create a policy for a group of computers running the installed Kaspersky Embedded Systems Security, take the following steps:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree, then select the administration group containing the computers for which you wish to create a policy.
2. In the details pane of the selected administration group, select the **Policies** tab and click the **Create a policy** link to start the wizard and create a policy.

   The **New Policy Wizard** window opens.
3. In the **Select the application for which you want to create a group policy** window, select Kaspersky Embedded Systems Security and click **Next**.
4. Enter a group policy name in the **Name** field.

   > The policy name cannot contain the following symbols: `" * < : > ? \ | .`

5. To apply policy configuration used for the previous application version:

   a. Select the **Use settings from policy for previous versions of application** check box.

   b. Click the **Select** button.

   c. Select the policy you want to apply.

   d. Click **Next**.
6. In the **Operation type selection** window, select one of the following options:
   - **New**, to create new policy with default settings.
   - **Import policy created with previous versions of Kaspersky Embedded Systems Security**, to use that version policy as a template.
   - Click **Browse** and select a configuration file where an existing policy is stored.
7. In the **Real-time computer protection** window, configure the Real-Time File Protection, KSN Usage tasks and Exploit Prevention functionality as required. Allow or block the use of configured policy tasks on local computers on the network:
   - Click the 🔒 button to allow changes to task settings on network computers and block the application of task settings configured in the policy.
   - Click the 🔓 button to deny changes to task settings on network computers and allow the application of task settings configured in the policy.

   The newly created policy uses the default settings of Real-Time Computer Protection tasks.

- To edit the default settings of the Real-Time File Protection task, click the **Settings** button in the **Real-Time File Protection** subsection. In the window that opens, configure the task according to your needs. Click **OK**.
- To edit the default settings of the KSN Usage task, click the **Settings** button in the **KSN Usage** subsection. In the window that opens, configure the task according to your needs. Click **OK**.

  > To start the KSN Usage task, you need to accept the KSN Statement in the Data handling window (see Section "Configuring Data Handling via the Administration Plug-in" on page 280).

- To edit the default settings of the Exploit Prevention component, click the **Settings** button in the **Exploit Prevention** subsection. In the window that opens, configure the functionality according to your needs. Click **OK**.

8. Select one of the following policy statuses in the **Create the group policy for the application** window:
   - **Active policy** if you want to apply the policy immediately after it is created. If an active policy already exists in the group, it is deactivated and a new policy is applied.
   - **Inactive policy** if you do not want to apply the created policy immediately. In this case the policy may be activated later.
   - Select the **Open policy properties immediately after they are created** check box to automatically close the **New Policy Wizard** and configure the newly created policy after clicking the **Next** button.
9. Click the **Finish** button.

The created policy appears in the list of policies on the **Policies** tab of the selected administration group. In the **Properties: <Policy name>** window, you can configure other settings, tasks and functions of Kaspersky Embedded Systems Security.

Kaspersky Embedded Systems Security policy settings sections

General

In the **General** section, you can configure the following policy settings:

- Indicate policy status.
- Configure the inheritance of settings from parent policies and for child policies.

Event configuration

In the **Event configuration** section, you can configure settings for the following event categories:

- *Critical events*
- *Functional failure*
- *Warning*
- *Informational message*

You can use the **Properties** button to configure the following settings for the selected events:

- Indicate the storage location and retention period of information about logged events.
- Indicate the method of notification about logged events.

Application settings

Table 11. Settings of the Application Settings section

Section	Options
Scalability and interface	In the **Scalability and interface** subsection, you can click the **Settings** button to configure the following settings: • Choose whether to configure scalability settings automatically or manually. • Configure the application icon display settings.
Security	In the **Security** subsection, you can click the **Settings** button to configure the following settings: • Configure the task run settings. • Specify how the application should behave when the computer is running on UPS power. • Enable or disable password-protection of application functions.
Connections	In the **Connections** subsection, you can use the **Settings** button to configure the following proxy server settings for connecting with update servers, activation servers, and KSN: • Configure the proxy server settings. • Specify the proxy server authentication settings.
Run system tasks	In the **Run system tasks** subsection, you can use the **Settings** button to allow or block the starting of the following system tasks according to a schedule configured on local computers: • On-Demand Scan task. • Update and Copying Updates tasks.

Supplementary

Table 12. Settings of the Supplementary section

Section	Options
Trusted Zone	Click the **Settings** button on the **Trusted Zone** subsection to configure the following Trusted Zone application settings: • Create a list of Trusted Zone exclusions. • Enable or disable scanning of file backup operations. • Create a list of trusted processes.
Removable Drives Scan	In the **Removable Drives Scan** subsection, you can use the **Settings** button to configure scan settings for removable USB drives.
User access permissions for application management	In the **User access permissions for application management** subsection, you can configure user rights and user group rights to manage Kaspersky Embedded Systems Security.
User access permissions for Security Service management	In the **User access permissions for Security Service management** subsection, you can configure user rights and user group rights to manage the Kaspersky Security Service.
Storages	In the **Storages** subsection, click the **Settings** button to configure the following Quarantine, Backup and Blocked Hosts settings: • Specify the path to the folder into which you want to place Quarantine or Backup objects. • Configure the maximum size of Backup and Quarantine and also specify the free space threshold. • Specify the path to the folder into which you want to place objects restored from Quarantine or Backup. • Configure the host blocking term.

Real-Time Computer Protection

Table 13. Settings of the Real-Time Computer Protection section

Section	Options
Real-Time File Protection	In the **Real-Time File Protection** subsection, you can click the **Settings** button to configure the following task settings: • Indicate the protection mode. • Configure use of the Heuristic Analyzer. • Configure use of the Trusted Zone. • Indicate 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 task start settings.
KSN Usage	In the **KSN Usage** subsection, you can click the **Settings** button to configure the following task settings: • Indicate the actions to perform on KSN untrusted objects. • Configure data transfer and usage of Kaspersky Security Center as a KSN proxy server. Click the **Data handling** button to accept or reject the KSN Statement and KMP statement, and configure dependable data exchange settings.
Exploit Prevention	In the **Exploit Prevention** subsection, you can click the **Settings** button to configure the following task settings: • Select the process memory protection mode. • Indicate the actions to reduce exploit risks. • Add to and edit the list of protected processes.

Local activity control

Table 14. Settings of the Local Activity Control section

Section	Options
Applications Launch Control	In the **Applications Launch Control** subsection, you can use the **Settings** button to configure the following task settings: • Select the task operating mode. • Configure settings for controlling subsequent application launches. • Indicate the scope for application of the Applications Launch Control rules. • Configure use of KSN. • Configure the task start settings.
Device Control	In the **Device Control** subsection, you can click the **Settings** button to configure the following task settings: • Select the task operating mode. • Configure the task start settings.

Network activity control

Table 15. Settings of the Network activity control section

Section	Options
Firewall Management	In the **Firewall Management** subsection, you can click the **Settings** button to configure the following task settings: • Configure firewall rules. • Configure the task start settings.

System Inspection

Table 16. Settings of the System Inspection section

Section	Options
File Integrity Monitor	In the **File Integrity Monitor** subsection you can configure control over the changes in files that can signify a security violation on a protected computer.
Log Inspection	In the **Log Inspection** section you can configure a protected computer integrity control basing on the results of the Windows Event Log analysis.

Logs and notifications

Table 17. Settings of the Logs and Notifications section

Section	Options
Task logs	In the **Task logs** subsection, you can click the **Settings** button to configure the following settings: • Specify the importance level of the logged events for the selected software components. • Specify the task log storage settings. • Specify the SIEM integration with Kaspersky Security Center settings.
Event notifications	In the **Event notifications** subsection, you can click the **Settings** button to configure the following settings: • Specify the user notification settings for the *Object detected* event, *Untrusted mass storage detected and restricted* event and *Host listed as untrusted* event. • Specify the administrator notification settings for any event selected in the event list in the **Notification settings** section.
Interaction with Administration Server	In the **Interaction with Administration Server** section, you can click the **Settings** button to select the types of objects that Kaspersky Embedded Systems Security will report to Administration Server. You can also configure transmission of information about Quarantine and Backup objects to Administration Server.

> To review the detailed information about Network Attached Storage Protection tasks, see the *Kaspersky Embedded Systems Security Implementation Guide for Network Storages Protection*.

Revision history

In the **Revision history** section, you can manage revisions: compare with the current revision or other policy, add descriptions of revisions, save revisions to a file or perform a rollback.

Configuring a policy

In the **Properties: <Policy name>** window of an existing policy, you can configure general Kaspersky Embedded Systems Security settings, quarantine and backup settings, Trusted Zone settings, Real-Time Computer Protection settings, Local Activity Control settings, the level of detail for task logs, as well as user and administrator notifications about the Kaspersky Embedded Systems Security events, access privileges for managing the application and the Kaspersky Security Service, and policy profile application settings.

► *To configure the policy settings:*

1. Expand the **Managed devices** node in the tree of the Administration Console of Kaspersky Security Center.
2. Expand the administration group, for which you want to configure the associated policy settings, and open the **Policies** tab in the details pane.
3. Select a policy you want to configure and open the **Properties: <Policy name>** window using one of the following ways:
   - By selecting the **Properties** option in the policy context menu.
   - By clicking the **Configure policy** link in the right details pane of the selected policy.
   - By double-clicking the selected policy.
4. On the **General** tab in the **Policy status** section, enable or disable the policy. To do so, select one of the options below:
   - **Active policy**, if you want the policy to be applied on all computers within the selected administration group.
   - **Inactive policy**, if you want to activate the policy later on all computers within the selected administration group.

   > The **Out-of-office policy** setting is not available when you manage Kaspersky Embedded Systems Security.

5. In the **Event configuration**, **Application settings**, **Supplementary**, **Logs and notifications**, and **Revision history** sections, you can modify the application configuration (see table below).
6. In the **Real-Time Computer Protection**, **Local activity control**, **Network activity control**, and **System Inspection** sections, configure the application settings and application launch settings (see the table below).

You can enable or disable the execution of any task on all computers within the administration group by means of a Kaspersky Security Center policy.
You can configure the application of policy settings on all network computers for each individual software component.

7. Click **OK**.

The configured settings are applied in the policy.

Creating and configuring tasks using Kaspersky Security Center

This section contains information about Kaspersky Embedded Systems Security tasks, and how to create them, configure task settings, and start and stop them.

In this chapter

About task creation in Kaspersky Security Center

You can create group tasks for administration groups and sets of computers. You can create the following task types:

- Activation of the application
- Copying Updates
- Database Update
- Software Modules Update
- Rollback of Database Update
- On-Demand Scan
- Application Integrity Control
- Rule Generator for Applications Launch Control
- Rule Generator for Device Control

You can create local and group tasks in the following ways:

- for one computer: in the **Properties <Computer name>** window in the **Tasks** section.
- for an administration group: in the details pane of the node of the selected group of computers on the **Tasks** tab.
- for a set of computers: in the details pane of the **Device selections** node.

Using policies you can disable schedules for update and On-Demand Scan local system tasks (see Section "Configuring scheduled start of local system tasks" on page 95) on all protected computers, from the same administration group.

General information on tasks in Kaspersky Security Center is provided in the *Kaspersky Security Center Help*.

Creating task using Kaspersky Security Center

► *To create a new task in the Kaspersky Security Center Administration Console:*

1. Start the task wizard in one of the following ways:
   - To create a local task:
     a. Expand the **Managed devices** node in the tree of the Administration Console and select the group that the protected computer belongs to.
     b. In the details pane, on the **Devices** tab open the context menu of the protected computer and select **Properties**.
     c. In the window that opens, click the **Add** button in the **Tasks** section.
   - To create a group task:
     a. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
     b. Select the administration group for which you want to create a task.
     c. In the details pane, open the **Tasks** tab and select **Create a task**.
   - To create a task for a custom set of computers:
     a. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
     b. Select the administration group containing the computers.
     c. Select a computer or a custom set of computers.
     d. From the **Perform action** drop-down list, select **Create a task** option.

   The task wizard window opens.
2. In the **Select the task type** window under the heading **Kaspersky Embedded Systems Security**, select the type of the task to be created.
3. If you selected any task type except Rollback of Database Update, Application Integrity Control or Activation of Application, the **Settings** window opens. Depending on the task type, the settings may vary:
   - Create an On-Demand Scan task (see Section "Creating an On-Demand Scan task" on page 411).
   - To create an update task, configure task settings based on your requirements:
     a. Select updates source in the **Update source** window.
     b. Click the **Connection settings** button. The **Connection settings** window opens.
     c. On the **Connection settings** window:

        Specify the FTP server mode for connecting to the protected computer.

        Modify the connection timeout when connecting to the update source, if required.

Configure proxy server access settings when connecting to the update source.

Specify protected computer(s) location, to optimize update downloads.

- To create a Software Modules Update task, configure the required program modules update settings in the **Settings for application software module updates** window:

  a. Select either to copy and install critical software module updates, or only to check for their availability without installation.

  b. If **Copy and install critical software modules updates** is selected: a computer restart may be required to apply the installed software modules. If you wish Kaspersky Embedded Systems Security to restart the computer automatically upon task completion, select the **Allow operating system restart** check box.

  c. To obtain information about Kaspersky Embedded Systems Security module upgrades, select **Receive information about available scheduled software modules updates**.

  Kaspersky Lab does not publish planned update packages on the update servers for automatic installation; these can be downloaded manually from the Kaspersky Lab website. An administrator notification about the event **New scheduled software modules update is available** can be configured. This will contain the URL of our website from which scheduled updates can be downloaded.

- To create the Copying Updates task, specify the set of updates and the destination folder in the **Copying updates settings** window.

- To create the Activation of Application task:

  a. In the **Activation Settings** window, specify the key file that you want to use to activate the application.

  b. Select the **Use as additional key** check box if you want to create a task for renewing the license.

- Create the Rule Generator for Applications Launch Control task (see Section "Creating a Rule Generator for Applications Launch Control task" on page 316).

- Create the Rule Generator for Device Control task (see Section "Creating rules using the Rule Generator for Device Control task" on page 353).

4. Configure the task schedule (see Section "Configuring the task start schedule settings" on page 129) (you can configure a schedule for all task types except Rollback of Database Update task).
5. Click **OK**.
6. If the task created for a set of computers, select the network (or group) of computers on which this task will be executed.
7. In the **Selecting an account to run the task** window, specify the account under which you want to run the task.
8. In the **Define the task name** window, enter the task name (no longer than 100 characters) not containing the symbols **" * < > ? \ | :** .

   It is recommended that the task type is added to its name (for example, "On-demand scan of shared folders").
9. In the **Finishing creating the task** window, select the **Run task after Wizard finishes** check box if you want the task to be started as soon as it has been created. Click the **Finish** button.

The task created is displayed in the **Tasks** list.

Configuring local tasks in the Application settings window of the Kaspersky Security Center

► *To configure local tasks or general application settings for a single network computer:*

1. Expand the **Managed devices** node in the tree of the Administration Server of Kaspersky Security Center and select the group that the protected computer belongs to.
2. In the details pane, select the **Devices** tab.
3. Open the **Properties: <Computer name>** window in one of the following ways:
   - Double-click the name of the protected computer.
   - Open the context menu of the protected computer name and select the **Properties** item.

   The **Properties: <Computer name>** window opens.
4. To configure the local task settings perform the following steps:
   a. Go to the **Tasks** section.
      - In the task list, select a local task to configure.
      - Double-click the task name in the list of tasks.
      - Select the task name and click the **Properties** button.
      - Select **Properties** in the context menu of the selected task.

      The **Properties: <Task name>** window opens.
5. To configure the application settings perform the following steps:
   a. Go to the **Applications** section.
      - In the installed applications list, select an application to configure.
      - Double-click the application name in the list of installed applications.
      - Select the application name in the list of installed applications and click the **Properties** button.
      - Open the context menu of the application name in the list of installed applications and select the **Properties** item.

      The **<Application name> settings** window opens.

> If the application is currently under the Kaspersky Security Center policy and this policy prohibits changing the application settings, these settings cannot be edited via the **<Application name> settings** window.

Configuring group tasks in Kaspersky Security Center

► *To configure group task for multiple computers:*

1. In the Kaspersky Security Center Administration Console tree expand the **Managed devices** node and select the administration group for which you want to configure the application tasks.
2. On the details pane of a selected administration group, open **Tasks** tab.

3. In the list of previously created group tasks, select a task you want to configure. Open the **Properties: <Task name>** window in one of the following ways:
   - Double-click the name of the task in the list of created tasks.
   - Select the name of the task in the list of created tasks and click **Configure task** link.
   - Open the context menu of the task name in the list of created tasks and select the **Properties** item.
4. In the **Notification** section, configure the task event notification settings.

   > For detailed information regarding configuring settings in this section, see the *Kaspersky Security Center Help*.

5. Depending on the type of configured task, do one of the following actions:
   - To configure an On-Demand Scan task:
     a. In the **Scan scope** section, configure a scan scope.
     b. In the **Options** section, configure task priority level and integration with other software components.
   - To configure an update task, adjust task settings based on your requirements:
     a. In the **Settings** section, configure update source settings and disk subsystem usage optimization.
     b. Click the **Connection settings** button to configure update source connection settings.
   - To configure Software Modules Update task, in the **Settings for application software module updates** section choose an action to perform: copy and install critical updates of software modules or only check for them.
   - To configure the Copying Updates task, specify the set of updates and the destination folder in the **Copying updates settings** section.
   - To configure the Activation of Application task, in the **Activation Settings** section apply the key file that you want to use to activate the application. Select the **Use as additional key** check box if you want to add an activation code or key file for renewing the license.
   - To configure the automatic generation of allowing rules for computer control, in the **Settings** section specify the settings based on which the list of allowing rules will be created.
6. Configure the task schedule in the **Schedule** section (you can configure a schedule for all task types except Rollback of Database Update).
7. In the **Account** section specify the account which rights will be used for the task execution. For detailed information regarding configuring settings in this section, see the *Kaspersky Security Center Help*.
8. If required, specify the objects to exclude from the task scope in the **Exclusions from task scope** section. For detailed information regarding configuring settings in this section, see the *Kaspersky Security Center Help.*
9. In the **Properties: <Task name>** window, click **OK**.

The newly configured group tasks settings are saved.

Group tasks settings that are available for configuring are summarized in the table below.

Table 18. Kaspersky Embedded Systems Security group tasks settings

Kaspersky Embedded Systems Security task types	Section in the Properties: <Task name> window	Task settings
Rule Generator for Applications Launch Control	**Settings**	While configuring the Rule Generator for Applications Launch Control task settings you can: • Create allowing rules based on running applications; • Create allowing rules for applications from the specific folders.
	Options	You can specify actions to perform while creating allowing rules for applications launch control: • **Use digital certificate** • **Use digital certificate subject and thumbprint** • **If the certificate is missing, use** • **Use SHA256 hash** • **Generate rules for user or group of users** You can configure settings for configuration files with allowing rules lists that Kaspersky Embedded Systems Security creates upon the task completion.
	Schedule	You can configure the settings of scheduled startup of the task.
Rule Generator for Device Control	**Settings**	• Select the operation mode: consider system data about all mass storages that have ever been connected or consider currently connected mass storages only. • Configure settings for configuration files with allowing rules lists that Kaspersky Embedded Systems Security creates upon the task completion.
	Schedule	You can configure the settings of scheduled startup of the task.
Activation of Application (see Section "Activation of the Application task" on page 122)	**Activation settings**	To activate the application or to renew the license, you can add a key file.
	Schedule	You can configure the settings of scheduled startup of the task.

Kaspersky Embedded Systems Security task types	Section in the Properties: <Task name> window	Task settings
Copying Updates (see Section "Update tasks" on page 124)	**Update source**	You can specify Kaspersky Security Center Administration Server or Kaspersky Lab update servers as application update source. You can also create a customized list of update sources: by adding custom HTTP and FTP servers or network folders manually and setting them as update sources. You can specify the usage of Kaspersky Lab update servers, if manually customized servers are not available.
	Connection settings window	In the **Connection settings** window linked from the **Update source** section, you can specify if connection to Kaspersky Lab update servers or any other server should be established via proxy server.
	Copying updates settings	You can specify the set of updates intended for copying. In the **Folder for local storage of copied updates** field, specify a path to a folder, which will be used by Kaspersky Embedded Systems Security to store copied updates.
	Schedule	You can configure the settings of scheduled startup of the task.
Database Update (see Section "Update tasks" on page 124)	**Settings**	You can specify Kaspersky Security Center Administration Server or Kaspersky Lab update servers as application update source in the **Update source** group box. You can also create a customized list of update sources: by adding custom HTTP and FTP servers or network folders manually and setting them as update sources. You can specify the usage of Kaspersky Lab update servers, if manually customized servers are not available. In the Disk I/O usage optimization section you can configure the feature that reduces the workload on the disk subsystem: • **Lower the load on the disk I/O** • **RAM used for optimization (MB)**
	Connection settings window	In the **Connection settings** window linked from the **Update source** section, you can specify if connection to Kaspersky Lab update servers or any other server should be established via proxy server.
	Schedule	You can configure the settings of scheduled start of the task.

Kaspersky Embedded Systems Security task types	Section in the Properties: <Task name> window	Task settings
Software Modules Update (see Section "Update tasks" on page 124)	**Update source**	You can specify Kaspersky Security Center Administration Server or Kaspersky Lab update servers as application update source. You can also create a customized list of update sources: by adding custom HTTP and FTP servers or network folders manually and setting them as update sources. You can specify the usage of Kaspersky Lab update servers, if manually customized servers are not available.
	Connection settings window	In the **Update source connection settings** group box you can specify if connection to Kaspersky Lab update servers or any other server should be established via proxy server.
	Settings for application software module updates	You can specify which actions should Kaspersky Embedded Systems Security perform when critical software module updates are available or have already been installed, and also if Kaspersky Embedded Systems Security should receive information regarding scheduled updates.
	Schedule	You can configure the settings of scheduled startup of the task.
On-Demand Scan Settings (see Section "Creating an On-Demand Scan task" on page 411)	**Scan scope**	You can specify a Scan scope for On-Demand Scan task and configure security level settings.
	On-demand scan settings window	In the **On-demand scan settings** window linked from the **Scan scope** section, you can select one of predefined security levels, or customize security level manually.
	Options	You can activate or deactivate heuristic analyzer usage for On-Demand Scan task, and set analysis level using a slider In the **Heuristic analyzer** group box. In the **Integration with other components** group box, you can configure the following settings: • Apply Trusted Zone for On-Demand Scan tasks. • Apply KSN usage for On-Demand Scan tasks. • Set a priority for On-Demand Scan task: perform task in background mode (low priority) or consider task a Critical Areas Scan.

Kaspersky Embedded Systems Security task types	Section in the Properties: <Task name> window	Task settings
	Schedule	You can configure the settings of scheduled startup of the task.
Application Integrity Control (on page 125)	**Schedule**	You can configure the settings of scheduled startup of the task.

> For Rollback of Database Update task, you can configure only standard task settings in the **Notification** and **Exclusions from task scope** sections, controlled by Kaspersky Security Center.

For detailed information regarding settings configuration of these sections, see the *Kaspersky Security Center Help*.

In this section

Activation of the Application task

► *To configure an Activation of the Application task, take the following steps:*

1. In the Kaspersky Security Center Administration Console tree expand the **Managed devices** node and select the administration group for which you want to configure the application tasks.
2. On the details pane of a selected administration group, open **Tasks** tab.
3. In the list of previously created group tasks, select a task you want to configure. Open the **Properties: <Task name>** window in one of the following ways:
   - Double-click the name of the task in the list of created tasks.
   - Select the name of the task in the list of created tasks and click **Configure task** link.
   - Open the context menu of the task name in the list of created tasks and select the **Properties** item.
4. In the **Notification** section, configure the task event notification settings.

   > For detailed information regarding configuring settings in this section, see the *Kaspersky Security Center Help*.

5. In the **Activation Settings** section, specify the key file that you want to use to activate the application. Select the **Use as additional key** check box if you want to add a key to extend the license.

6. Configure the task schedule in the **Schedule** section (you can configure a schedule for all task types except Rollback of Database Update).
7. In the **Account** section specify the account which rights will be used for the task execution.
8. If required, specify the objects to exclude from the task scope in the **Exclusions from task scope** section.

> For detailed information regarding configuring settings in these sections, see the *Kaspersky Security Center Help*.

9. In the **Properties: <Task name>** window, click **OK**.

   The newly configured group tasks settings are saved.

Update tasks

► *To configure the Copying Updates, Database Update, or Software Modules Update tasks, do the following:*

1. In the Kaspersky Security Center Administration Console tree expand the **Managed devices** node and select the administration group for which you want to configure the application tasks.
2. On the details pane of a selected administration group, open **Tasks** tab.
3. In the list of previously created group tasks, select a task you want to configure. Open the **Properties: <Task name>** window in one of the following ways:
   - Double-click the name of the task in the list of created tasks.
   - Select the name of the task in the list of created tasks and click **Configure task** link.
   - Open the context menu of the task name in the list of created tasks and select the **Properties** item.
4. In the **Notification** section, configure the task event notification settings.

   > For detailed information regarding configuring settings in this section, see the *Kaspersky Security Center Help*.

5. Depending on the type of configured task, do one of the following actions:
   - In the **Update source** section, configure update source settings and disk subsystem usage optimization.
     a. You can specify Kaspersky Security Center Administration Server or Kaspersky Lab update servers as application update source in the **Update source** section. You can also create a customized list of update sources: by adding custom HTTP and FTP servers or network folders manually and setting them as update sources.

        You can specify the usage of Kaspersky Lab update servers, if manually customized servers are not available.

     b. In the **Disk I/O usage optimization** section for the Database Update task, you can configure the feature that reduces the workload on the disk subsystem:
        - **Lower the load on the disk I/O**

          This check box enables or disables the feature of the disk subsystem optimization through storing update files on a virtual drive in the RAM.

          If the check box is selected, this function is enabled.

          The check box is cleared by default.
        - **RAM used for optimization (MB)**

          The size of the RAM (in MB) that the application uses for storing update files. The default RAM size is 512 MB. The minimum RAM size is 400 MB.

     c. Click the **Connection settings** button, and in the **Connection settings** window that opens, configure the use of a proxy server for connecting to Kaspersky Lab update servers and other servers.

- In the **Settings for application software module updates** section for the Software Modules Update task, you can specify which actions Kaspersky Embedded Systems Security should perform when critical software module updates are available or information about planned updates is available, and you can also specify which actions Kaspersky Embedded Systems Security should perform when critical updates are installed.
- Specify the set of updates and the destination folder in the **Copying updates settings** section for the Copying Updates task.

6. Configure the task schedule in the **Schedule** section (you can configure a schedule for all task types except Rollback of Database Update).
7. In the **Account** section specify the account which rights will be used for the task execution.

> For detailed information regarding configuring settings in these sections, see the *Kaspersky Security Center Help*.

8. In the **Properties: <Task name>** window, click **OK**.

The newly configured group tasks settings are saved.

For the Rollback of Database Update task, you can configure only standard task settings controlled by Kaspersky Security Center in the **Notifications** and **Exclusions from task scope** sections. For detailed information regarding configuring the settings in these sections, see the *Kaspersky Security Center Help*.

Application Integrity Control

► *To configure the Application Integrity Control group task:*

1. In the Kaspersky Security Center Administration Console tree expand the **Managed devices** node and select the administration group for which you want to configure the application tasks.
2. On the details pane of a selected administration group, open **Tasks** tab.
3. In the list of previously created group tasks, select a task you want to configure. Open the **Properties: <Task name>** window in one of the following ways:
   - Double-click the name of the task in the list of created tasks.
   - Select the name of the task in the list of created tasks and click **Configure task** link.
   - Open the context menu of the task name in the list of created tasks and select the **Properties** item.
4. In the **Notification** section, configure the task event notification settings.

> For detailed information regarding configuring settings in this section, see the *Kaspersky Security Center Help*.

5. In the **Devices** section, select the devices for which you want to configure the Application Integrity Control task.
6. Configure the task schedule in the **Schedule** section (you can configure a schedule for all task types except Rollback of Database Update).
7. In the **Account** section specify the account which rights will be used for the task execution.

8. If required, specify the objects to exclude from the task scope in the **Exclusions from task scope** section.

   For detailed information regarding configuring settings in these sections, see the *Kaspersky Security Center Help*.

9. In the **Properties: <Task name>** window, click **OK**.

   The newly configured group tasks settings are saved.

Configuring crash diagnostics settings in Kaspersky Security Center

If a problem occurs during Kaspersky Embedded Systems Security operation (for example, Kaspersky Embedded Systems Security crashes) and you want to diagnose it, you can enable the creation of trace files and the dump file of Kaspersky Embedded Systems Security process and send these files for analysis to Kaspersky Lab Technical Support.

Kaspersky Embedded Systems Security does not send any trace or dump files automatically. Diagnostics data can only be sent by the user with the corresponding permissions.

Kaspersky Embedded Systems Security writes information to trace files and the dump file in unencrypted form. The folder where files are saved is selected by the user and managed by the operating system configuration and Kaspersky Embedded Systems Security settings. You can configure access permissions (see Section "Managing access permissions for Kaspersky Embedded Systems Security functions" on page 225) and allow access to logs, trace and dump files only for required users.

► *To configure crash diagnostics settings in Kaspersky Security Center:*

1. In the Kaspersky Security Center Administration Console, open the **Application settings** (see Section "**Configuring local tasks in the Application settings window of the Kaspersky Security Center**" on page 117) window.
2. Open the **Malfunction diagnosis** section and do the following:
   - If you want the application to write debug information to file, select the **Write debug information to trace file** check box.
     - In the field below specify the folder in which Kaspersky Embedded Systems Security will save trace files.
     - Configure the level of detail of debug information.

       This drop-down list lets you select the level of detail of debug information that Kaspersky Embedded Systems Security saves to the trace file.

       You can select one of the following detail levels:

       - **Critical events** – Kaspersky Embedded Systems Security saves information only about critical events to the trace file.

  - **Errors** – Kaspersky Embedded Systems Security saves information about critical events and errors to the trace file.
  - **Important events** – Kaspersky Embedded Systems Security saves information about critical events, errors, and important events to the trace file.
  - **Informational events** – Kaspersky Embedded Systems Security saves information about critical events, errors, important events, and informational events to the trace file.
  - **All debug information** – Kaspersky Embedded Systems Security saves all debug information to the trace file.

  A Technical Support representative determines the detail level that needs to be set in order to resolve the issue that arose.

  The default level of detail is set to **All debug information**.

  The drop-down list is available if the **Write debug information to trace file** check box is selected.

- Specify the maximum size of trace files.

- Specify the components to be debugged. Component codes must be separated with a semicolon. The codes are case sensitive (see table below).

Table 19. Kaspersky Embedded Systems Security subsystem codes

Component Code	Name of component
*	All components.
gui	User interface subsystem, Kaspersky Embedded Systems Security snap-in in Microsoft Management Console.
ak_conn	Subsystem for integrating Network Agent and Kaspersky Security Center.
bl	Control process, implements Kaspersky Embedded Systems Security control tasks.
wp	Work process, handles anti-virus protection tasks.
blgate	Kaspersky Embedded Systems Security remote management process.
ods	On-Demand Scan subsystem.
oas	Real-Time File Protection subsystem.
qb	Quarantine and Backup subsystem.
scandll	Auxiliary module for anti-virus scans.
core	Subsystem for basic anti-virus functionality.
avscan	Anti-virus processing subsystem.
avserv	Subsystem for controlling the anti-virus kernel.
prague	Subsystem for basic functionality.
updater	Subsystem for updating databases and software modules.
snmp	SNMP protocol support subsystem.
perfcount	Performance counter subsystem.

The trace settings of the Kaspersky Embedded Systems Security snap-in (gui) and the Administration Plug-in for Kaspersky Security Center (ak_conn) are applied after these components are restarted. The trace settings of the SNMP protocol support subsystem (snmp) are applied after the SNMP service is restarted. The trace settings of the performance counters subsystem (perfcount) are applied after all processes that use performance counters are restarted. Trace settings for other Kaspersky Embedded Systems Security subsystems are applied as soon as the crash diagnostics settings are saved.

By default, Kaspersky Embedded Systems Security logs debug information for all Kaspersky Embedded Systems Security components.

The entry field is available if the **Write debug information to trace file** check box is selected.

- If you want the application to create a dump file, select the **Create dump file** check box.
  - In the field below, specify the folder in which Kaspersky Embedded Systems Security will save the dump file.

3. Click **OK**.

The configured application settings are applied on the protected computer.

Managing task schedules

You can configure the start schedule for Kaspersky Embedded Systems Security tasks, and configure settings for running tasks by schedule.

In this section

Configuring the task start schedule settings

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

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

1. In the Kaspersky Security Center Administration Console tree, expand the **Managed devices** node.
2. Select the group that the protected server belongs to.
3. In the details pane, select the **Tasks** tab.
4. Open the **Properties: <Task name>** window in one of the following ways:
   - Double-click the name of the task.
   - Open the context menu of the task name and select the Properties item.
5. Select **Schedule** section.
6. In the **Schedule settings** block, select the **Run by schedule** check box.

   > Fields with the schedule settings for the On-Demand Scan and Update tasks are unavailable if their scheduled start is blocked by a policy of Kaspersky Security Center.

7. 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 at intervals of 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 at intervals of 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 at intervals of 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 started (by default the task runs on Mondays).
   - **At application launch**, if you want the task to run every time Kaspersky Embedded Systems Security starts.
   - **After application database update**, if you want the task to run after every update of the application databases.

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

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

> After you have specified the task start frequency, the time of the first task start, and the date from which the schedule applies, information about the estimated time for the next task start will appear in the top part of the window in the **Next start** field. Updated information about the estimated time of the next task start 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 start of scheduled system tasks (see Section "Configuring scheduled start of local system tasks" on page 95).

8. Use the **Advanced** tab to 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 a time interval under 24 hours 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 start of skipped tasks.

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

9. Click **OK**.

10. Click the **Apply** button to save the task start settings.

> If you want to configure application settings for a single task using Kaspersky Security Center, perform the steps described in Configuring local tasks in the Application settings window of the Kaspersky Security Center (on page 117) section.

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 start schedule, take the following steps:*

1. In the Application Console tree open the context menu on the task name for which you wish to configure the start 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 scheduled task start.
   - Clear the **Run by schedule** check box if you want to disable scheduled task start.

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

The configured task start schedule settings are saved.

Reporting in Kaspersky Security Center

Reports in Kaspersky Security Center contain information about the status of managed devices. Reports are based on information stored on Administration Server.

Starting from the Kaspersky Security Center 11 the following types of reports are available for the Kaspersky Embedded Systems Security :

- Report on the status of application components
- Report on prohibited applications
- Report on prohibited applications in test mode

> See *Kaspersky Security Center Help* for detailed information about all Kaspersky Security Center reports and how to configure them.

Report on the application components status

You can monitor the protection status of all network devices and get a structured overview of the component set on each device.

Report displays one of the following states for each component: *Running, Paused, Stopped, Malfunction, Not installed, Starting*.

The *Not Installed* status refers to the component, not the application itself. If the application is not installed the Kaspersky Security Center assigns the N/A (Not available) status.

You can create component selections and use filtering to display network devices with the defined set of components and their state.

See *Kaspersky Security Center Help* for detailed information about creating and using selections.

► *To review the components statuses in the application settings:*

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. Select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in the Application settings window of the Kaspersky Security Center" on page 117).
3. Select the **Components** section.
4. Review the status table.

► *To review a Kaspersky Security Center standard report:*

1. Select the **Administration Server <computer name>** node in the Administration Console tree.
2. Open the **Reports** tab.
3. Double-click the **Report on the status of application components** list item.

   A report is generated.
4. Review the following report details:
   - A graphical diagram.
   - A summary table of components and aggregated numbers of network devices where each of the components is installed, and groups they belong to.
   - A detailed table specifying component status, version, device and group.

Reports on blocked applications in active and statistics modes

Based on the results of the Application Launch Control task execution, two types of report can be generated: report on prohibited applications (if the task is started in the Active mode), report on prohibited applications in test mode (if the task is started in the Statistics only mode). These reports display information about blocked applications on the protected computers of the network. Each report is generated for all administration groups and accumulates data from all the Kaspersky Lab applications installed on the protected devices.

► *To review a report on prohibited applications in test mode:*

1. Start the Application Control task in the Statistics only mode (see Section "Configuring Applications Launch Control task settings" on page 301).
2. Select the **Administration Server <computer name>** node in the Administration Console tree.
3. Open the **Reports** tab.

4. Double-click the **Report on prohibited applications in test mode** list item.

   A report is generated.

5. Review the following report details:

   - A graphical diagram that displays top ten applications with most amount of blocked starts.
   - A summary table of occurred application blocks specifying the executable file name, reason, time of blocking and number of devices where it occurred.
   - A detailed table specifying data about the device, file path and criteria for blocking.

► *To review a report on prohibited applications in the Active mode:*

1. Start the Application Control task in the Active mode (see Section "Configuring Applications Launch Control task settings" on page 301),
2. Select the **Administration Server <computer name>** node in the Administration Console tree.
3. Open the **Reports** tab.
4. Double-click a **Report on prohibited applications** list item.

   A report is generated.

This report consists of the same data blocks as the report on prohibited applications in test mode.

Working with the Kaspersky Embedded Systems Security Console

This section provides information about the Kaspersky Embedded Systems Security Console and describes how to manage the application using the Application Console installed on the protected computer or another computer.

In this chapter

Kaspersky Embedded Systems Security settings in the Application Console

General settings and malfunction diagnostics settings of Kaspersky Embedded Systems Security settings establish the general conditions on which the application operates. These settings allow you to control the number of working processes used by Kaspersky Embedded Systems Security, enable Kaspersky Embedded Systems Security task recovery after an abnormal termination, maintain the tracking log, enable creating dump file of Kaspersky Embedded Systems Security processes in case of an abnormal termination, and configure other general settings.

> Application settings cannot be configured in the Application Console if the Kaspersky Security Center active policy blocks changes to these settings.

► *To configure Kaspersky Embedded Systems Security settings:*

1. In the Application Console tree, select the **Kaspersky Embedded Systems Security** node and do one of the following:
    - Click the **Application properties** link in the details pane of the node.
    - Select **Properties** in the node's context menu.

    The **Application settings** window opens.
2. In the window that opens, configure general Kaspersky Embedded Systems Security settings according to your preferences:
    - The following settings can be configured on the **Scalability and interface** tab:
        - In the **Scalability settings** section:
            - Maximum number of working processes that Kaspersky Embedded Systems Security can run

Table 20. Maximum number of active processes

<table>
<tr><th>Setting</th><th>Maximum number of active processes</th></tr>
<tr><td><b>Description</b></td><td>This setting belongs to the <b>Scalability settings</b> group in Kaspersky Embedded Systems Security. It sets the maximum number of active processes that application can run simultaneously.
Increasing the number of processes running in parallel increases the speed of file scanning and improves the fail-safety of Kaspersky Embedded Systems Security. However, if the value of this setting is too high, it may reduce the general computer performance and increase RAM usage.
In the Administration Console of the Kaspersky Security Center application you can change the <b>Maximum number of active processes</b> setting only for Kaspersky Embedded Systems Security installed on a stand-alone computer (using the <b>Application settings</b> dialog box); however, you cannot modify this setting in the policy settings for group of computers.</td></tr>
<tr><td><b>Possible values</b></td><td>1 – 8</td></tr>
<tr><td><b>Default Value</b></td><td>The application handles scalability automatically depending on the number of processors on the computer:
<table>
<tr><th>Number of processors</th><th>Maximum number of active processes</th></tr>
<tr><td>1</td><td>1</td></tr>
<tr><td>1&lt; number of processors &lt; 4</td><td>2</td></tr>
<tr><td>4 or more</td><td>4</td></tr>
</table></td></tr>
</table>

- Number of processes for Real-Time Computer Protection

Table 21. Number of processes for Real-Time Protection

<table>
<tr><td><b>Setting</b></td><td><b>Number of processes for Real-Time Protection</b></td></tr>
<tr><td><b>Description</b></td><td>This setting belongs to the <b>Scalability settings</b> group in Kaspersky Embedded Systems Security.
Using this setting you can specify the fixed number of processes in which Kaspersky Embedded Systems Security will execute Real-Time Protection tasks.
A higher value of this setting will increase the scan speed in the Real-Time Protection tasks. However, the more processes Kaspersky Embedded Systems Security uses, the greater its influence will be on the general performance of the protected computer and usage of RAM resources.
In the Administration Console of the Kaspersky Security Center application you can change the <b>Number of processes for Real-Time Protection</b> setting only for Kaspersky Embedded Systems Security installed on a stand-alone computer (using the <b>Application settings</b> window); however, you cannot modify this setting in the policy settings for group of computers.</td></tr>
<tr><td><b>Possible values</b></td><td>Possible values: 1-N where N is the value specified using the <b>Maximum number of active processes</b> setting.
If you set the value of the <b>Number of processes for Real-Time Protection</b> setting as equal to the maximum number of active processes, you will reduce the impact of Kaspersky Embedded Systems Security on the rate of the file exchange between the computers and the computer, thus further improving its performance during Real-Time Protection. However, update tasks and On-Demand Scan tasks with the <b>Medium (Normal)</b> basic priority will be executed in Kaspersky Embedded Systems Security processes which are already running. On-Demand Scan tasks will be executed with less speed. If the execution of a task causes an abnormal termination of a process, it will take more time to restart it.
On-Demand Scan tasks with the <b>Low</b> basic priority are always executed in a separate process or processes.</td></tr>
<tr><td><b>Default Value</b></td><td>Kaspersky Embedded Systems Security handles scalability automatically depending on the number of processors on the computer:
<table>
<tr><th>Number of processors</th><th>Number of processes for Real-Time Protection</th></tr>
<tr><td>=1</td><td>1</td></tr>
<tr><td>&gt;1</td><td>2</td></tr>
</table></td></tr>
</table>

- Number of working processes for background On-Demand Scan tasks

Table 22. Number of processes for background On-Demand Scan tasks

Setting	**Number of processes for background On-Demand Scan tasks**
Description	This setting belongs to the **Scalability settings** group in Kaspersky Embedded Systems Security. You can use this setting to specify the maximum number of processes which the application will use to run On-Demand Scan tasks in the background mode. The number of processes specified by this setting is not included in the total number of Kaspersky Embedded Systems Security processes specified by the **Maximum number of active processes** setting. For example, of you specify the following values of settings: • Maximum number of active processes – 3; • Number of processes for Real-Time Protection tasks – 3; • Number of processes for background On-Demand Scan tasks – 1; and then start Real-Time Protection tasks and one On-Demand Scan task in background mode, the total number of kavfswp.exe processes of Kaspersky Embedded Systems Security will be 4. Several On-Demand Scan tasks can be running in one process with low priority. You can increase the number of processes, for example, if you run several tasks in background mode in order to allocate a separate process for each task. Allocating separate processes for tasks increases the reliability and speed of task execution.
Possible values	1-4
Default Value	1

- In the **Interaction with user** section select if the System Tray Icon will be displayed in the taskbar after each application start (see Section "System Tray Icon in notification area" on page 145).

- The following settings can be configured on the **Security and reliability** tab:
  - In the **Reliability settings** section, specify the number of attempts to recover an On-Demand Scan task after it crashed.

Table 23. Task recovery

Setting	Task recovery (**Perform task recovery**)
Description	This setting belongs to the **Reliability settings** group in Kaspersky Embedded Systems Security. It enables recovery of tasks in case of their emergency termination and defines the number of attempts used to recover On-Demand Scan tasks. When a task crashes, the kavfs.exe process of Kaspersky Embedded Systems Security attempts to restart the process in which that task was running at the time of the crash. If task recovery is disabled, the application does not restore the Real-Time Protection and On-Demand Scan tasks. If task recovery is enabled, the application attempts to restore the Real-Time Protection tasks until they are started successfully and tries to restore On-Demand Scan tasks using the number of attempts specified in the setting.
Possible values	Enabled / disabled. The number of On-Demand Scan tasks recovery attempts: 1 - 10.
Default Value	Task recovery is enabled. The number of On-Demand Scan tasks recovery attempts: 2.

  - In the **Actions when switching to UPS backup power** section, specify actions that Kaspersky Embedded Systems Security performs after switching to UPS power:

Table 24. Use of uninterruptible power supply

Setting	Actions when switching to UPS backup power.
Description	This setting determines the actions that Kaspersky Embedded Systems Security performs when the computer switches to an uninterruptible power supply source.
Possible values	Run or do not run On-Demand Scan tasks to be started according to schedule. Perform or stop all active On-Demand Scan tasks.
Default Value	By default, if uninterruptible power supply is used to power the computer, Kaspersky Embedded Systems Security: • Does not run On-Demand Scan tasks that run according to schedule. • Automatically stops all active On-Demand Scan tasks.

  - In the **Password protection settings** section, configure the settings for password-protection of the application's functions (see Section "Password-protected access to Kaspersky Embedded Systems Security functions" on page 233).

- On the **Connection settings** tab:
    - In the **Proxy server settings** section, specify the proxy server usage settings.
    - In the **Proxy server authentication settings** section specify authentication type and details required for authentication on the proxy server.
    - In the **Licensing** section, indicate whether Kaspersky Security Center will be used as a proxy-server for application activation.
- On the **Malfunction diagnosis** tab:
    - If you want the application to write debug information to file, select the **Write debug information to trace file** check box.
        - In the field below specify the folder in which Kaspersky Embedded Systems Security will save trace files.
        - Configure the level of detail of debug information.

          This drop-down list lets you select the level of detail of debug information that Kaspersky Embedded Systems Security saves to the trace file.

          You can select one of the following detail levels:

            - **Critical events** – Kaspersky Embedded Systems Security saves information only about critical events to the trace file.
            - **Errors** – Kaspersky Embedded Systems Security saves information about critical events and errors to the trace file.
            - **Important events** – Kaspersky Embedded Systems Security saves information about critical events, errors, and important events to the trace file.
            - **Informational events** – Kaspersky Embedded Systems Security saves information about critical events, errors, important events, and informational events to the trace file.
            - **All debug information** – Kaspersky Embedded Systems Security saves all debug information to the trace file.

          A Technical Support representative determines the detail level that needs to be set in order to resolve the issue that arose.

          The default level of detail is set to **All debug information**.

          The drop-down list is available if the **Write debug information to trace file** check box is selected.
        - Specify the maximum size of trace files.
        - Specify the components to be debugged.

          A list of codes of Kaspersky Embedded Systems Security components for which application saves debug information in the trace file. Component codes must be separated with a semicolon. The codes are case sensitive (see table below).

Table 25. Kaspersky Embedded Systems Security subsystem codes

Component Code	Name of component
*	All components.
gui	User interface subsystem, Kaspersky Embedded Systems Security snap-in in Microsoft Management Console.
ak_conn	Subsystem for integrating Network Agent and Kaspersky Security Center.
bl	Control process, implements Kaspersky Embedded Systems Security control tasks.
wp	Work process, handles anti-virus protection tasks.
blgate	Kaspersky Embedded Systems Security remote management process.
ods	On-Demand Scan subsystem.
oas	Real-Time File Protection subsystem.
qb	Quarantine and Backup subsystem.
scandll	Auxiliary module for anti-virus scans.
core	Subsystem for basic anti-virus functionality.
avscan	Anti-virus processing subsystem.
avserv	Subsystem for controlling the anti-virus kernel.
prague	Subsystem for basic functionality.
updater	Subsystem for updating databases and software modules.
snmp	SNMP protocol support subsystem.
perfcount	Performance counter subsystem.

The trace settings of the Kaspersky Embedded Systems Security snap-in (gui) and the Kaspersky Embedded Systems Security Administration Plug-in for Kaspersky Security Center (ak_conn) are applied after these components are restarted. The trace settings of the SNMP protocol support subsystem (snmp) are applied after the SNMP service is restarted. The trace settings of the performance counters subsystem (perfcount) are applied after all processes that use performance counters are restarted. Trace settings for other Kaspersky Embedded Systems Security subsystems are applied as soon as the crash diagnostics settings are saved.

By default, Kaspersky Embedded Systems Security logs debug information for all Kaspersky Embedded Systems Security components.

The entry field is available if the **Write debug information to trace file** check box is selected.

- If you want the application to create a dump file, select the **Create crash dump file** check box.

Kaspersky Embedded Systems Security does not send any trace or dump files automatically. Diagnostics data can only be sent by the user with the corresponding permissions.

- In the field below, specify the folder in which Kaspersky Embedded Systems Security will save the memory dump file.

Kaspersky Embedded Systems Security writes information to trace files and the dump files in unencrypted form. The folder where files are saved is selected by the user and is managed by the operating system configuration and Kaspersky Embedded Systems Security settings. You can configure access permissions (see Section "Managing access permissions for Kaspersky Embedded Systems Security functions" on page 225) and allow access to logs, trace and dump files only for required users.

3. Click **OK**.

Kaspersky Embedded Systems Security settings are saved.

About the Kaspersky Embedded Systems Security Console

Kaspersky Embedded Systems Security 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 computer or on another computer on the corporate network.

After the Application Console has been installed on another computer, advanced configuration is required.

If the Application Console and Kaspersky Embedded Systems Security 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 Embedded Systems Security snap-in to the list of isolated Microsoft Windows snap-ins.

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

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

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

Kaspersky Embedded Systems Security Console interface

The Kaspersky Embedded Systems Security Console is displayed in the Microsoft Management Console tree in the form of a node.

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

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

- **Real-Time Computer Protection**: manages real-time protection tasks and KSN services. The **Real-Time Computer Protection** node allows to configure the following tasks:
    - **Real-Time File Protection**
    - **KSN Usage**
- **Computer Control**: controls launches of applications installed on a protected computer, as well as external devices connections. The **Computer 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 (see Section "Kaspersky Embedded Systems Security task categories" on page 147) 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**
- **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 (see Section "Kaspersky Embedded Systems Security task categories" on page 147) 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 Embedded Systems Security 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 (see Section "Kaspersky Embedded Systems Security task categories" on page 147) created and sent to a computer using Kaspersky Security Center.
- **Storages**: Management of Quarantine and Backup settings.
  - **Quarantine**
  - **Backup**
- **Logs and notifications**: manages local task logs, Security log and Kaspersky Embedded Systems Security System audit log.
  - **Security log**
  - **System audit log**
  - **Task logs**
- **Licensing**: add or delete Kaspersky Embedded Systems Security keys and activation codes, view license details.

Details pane

The details pane displays information about the selected node. If the **Kaspersky Embedded Systems Security** node is selected, the details pane displays information about the current computer protection status (see Section "Viewing protection status and Kaspersky Embedded Systems Security information" on page 159) and information about Kaspersky Embedded Systems Security, the protection status of its functional components, and the license expiration date.

Context menu of the Kaspersky Embedded Systems Security node

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

- **Connect to another computer**. Connect to another computer (see Section "Managing Kaspersky Embedded Systems Security via the Application Console on another computer" on page 146) to manage Kaspersky Embedded Systems Security installed on it. You can also perform this operation by clicking the link in the lower right corner of the details pane of the **Kaspersky Embedded Systems Security** node.
- **Start the service** / **Stop the service**. Start or stop application or a selected task (see Section "Starting / pausing / resuming / stopping tasks manually" on page 148). 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 (see Section "About the Removable Drives Scan" on page 406) connected to the protected computer 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 (see Section "Exploit prevention techniques" on page 466).
- **Configure Trusted Zone settings**. View and configure Trusted Zone settings (see Section "About the Trusted Zone" on page 443).
- **Modify user rights of the application management**. View and configure permissions to access Kaspersky Embedded Systems Security functions (see Section "Managing access permissions for Kaspersky Embedded Systems Security functions" on page 225).
- **Modify user rights of Kaspersky Security Service management**. View and configure user rights to manage Kaspersky Security Service (see Section "Configuring access permissions for managing Kaspersky Embedded Systems Security and Kaspersky Security Service" on page 231).
- **Export settings**. Save the application settings in a configuration file in XML format (see Section "Exporting settings" on page 154). You can also perform this operation in context menus of application tasks.
- **Import settings**. Import application settings from a configuration file in XML format (see Section "Importing settings" on page 155). You can also perform this operation in context menus of application tasks.
- **Information about the application and available module updates**. See information about Kaspersky Embedded Systems Security 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 Embedded Systems Security 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 Embedded Systems Security** node or use the button on the toolbar.

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

Toolbar and context menu of Kaspersky Embedded Systems Security tasks

You can manage Kaspersky Embedded Systems Security 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:

- **Start** / **Stop**. Start or stop task (see Section "Starting / pausing / resuming / stopping tasks manually" on page 148) execution. To carry out these operations, you can also use the buttons on the toolbar.
- **Resume** / **Pause**. Resume or pause task (see Section "Starting / pausing / resuming / stopping tasks manually" on page 148) 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 (see Section "Creating and configuring an On-Demand Scan task" on page 426). This operation is available for On-demand scan tasks.
- **Open log**. View and manage a task log (see Section "About task logs" on page 203). This operation is available for all tasks.
- **Remove task**. Delete custom task. This operation is available for On-demand scan tasks.
- **Settings templates**. Manage templates (see Section "Using security settings templates" on page 156). This operation is available for Real-Time File Protection and On-Demand Scan.

System Tray Icon in notification area

Every time Kaspersky Embedded Systems Security automatically starts after a computer reboot, the System Tray Icon is displayed in the toolbar notification area K. It is displayed by default if the System Tray Icon component was installed during application setup.

The appearance of the System Tray Icon reflects the current status of computer protection. The two statuses are possible:

K	active (colored icon) if at least one of the tasks is currently running: Real-Time File Protection, Applications Launch Control
K	inactive (black-and-white icon) if none of the tasks are currently running: Real-Time File Protection, Applications Launch Control

You can open the context menu of the System Tray Icon by right-clicking it.

The context menu offers several commands which can be used to display application windows (see the table below).

Table 26. Context menu commands displayed in the System Tray Icon

Command	Description
Open the Application Console	Opens Kaspersky Embedded Systems Security Console (if installed).
Open Compact Diagnostic Interface	Open the Compact Diagnostic Interface.
About the application	Opens the About the application window containing information about Kaspersky Embedded Systems Security. For registered Kaspersky Embedded Systems Security users, the About the application window contains information about urgent updates that have been installed.
Hide	Hides the System Tray Icon in the toolbar notification area.

You can display the hidden System Tray Icon again at any time.

► *To display the application icon again,*

in the **Start** menu of Microsoft Windows, select **All Programs** > **Kaspersky Embedded Systems Security** > **System Tray Icon**.

The names of settings may vary depending on the installed operating system.

In the general settings of Kaspersky Embedded Systems Security, you can enable or disable the display of the System Tray Icon every time the application starts automatically following a computer reboot.

Managing Kaspersky Embedded Systems Security via the Application Console on another computer

You can manage Kaspersky Embedded Systems Security via the Application Console installed on a remote computer.

To manage the application using Kaspersky Embedded Systems Security Console on a remote computer, make sure that:

- The Application Console users on the remote computer are added to the ESS Administrators group on the protected computer.
- Network connections are allowed for the Kaspersky Security Management Service process (kavfsgt.exe) if Windows Firewall is enabled on the protected computer.

- During installation of Kaspersky Embedded Systems Security, the **Allow remote access** check box was selected in the Installation Wizard window.

> If Kaspersky Embedded Systems Security on the remote computer is password protected, enter the password to get access for application management via the Application Console.

Managing Kaspersky Embedded Systems Security tasks

This section contains information about Kaspersky Embedded Systems Security tasks, and how to create them, configure task settings, and start and stop them.

In this section

Kaspersky Embedded Systems Security task categories

Real-Time Computer Protection, Computer Control, On-Demand Scan, and Update functions in Kaspersky Embedded Systems Security are implemented as tasks.

You can manage tasks using the task's context menu in the Application Console tree, the toolbar, and the quick access bar. You can view task status information in the details pane. Task management operations are recorded in the system audit log.

There are two types of Kaspersky Embedded Systems Security tasks: *local* and *group*.

Local tasks

Local tasks are executed only on the protected computer for which they are created. Depending on the start method, the following types of local tasks exist:

- **Local system tasks**. Created automatically during installation of Kaspersky Embedded Systems Security. You can edit the settings of all system tasks, except for the Quarantine Scan and Rollback of Database Update tasks. System tasks cannot be renamed or deleted. You can run system and custom On-Demand Scan tasks simultaneously.

- **Local custom tasks**. In the Application Console, you can create On-Demand Scan tasks. In Kaspersky Security Center you can create On-Demand Scan, Database Update, Rollback of Database Update, and Copying Updates tasks. Such tasks are called custom tasks. Custom tasks can be renamed, configured, and deleted. You can run several custom tasks simultaneously.

Group tasks

Group tasks and tasks for sets of computers created using Kaspersky Security Center are displayed in the Application Console. Such tasks are called group tasks. Group tasks can be managed and configured from the Kaspersky Security Center. In the Application Console, you can only view the status of group tasks.

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, 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 Application Console node,*

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

Starting / pausing / resuming / stopping tasks manually

You can pause and resume only Real-Time Computer Protection and On-Demand Scan tasks.

► *To start / pause / resume / stop a task, take the following steps:*

1. Open the context menu of the task in the Application Console.
2. Select one of the following: **Start**, **Pause**, **Resume** or **Stop**.

The operation is executed and registered in the system audit log (on page 201).

> When an On-Demand Scan task is resumed, Kaspersky Embedded Systems Security continues with the object that was being scanned when the task was paused.

Managing task schedules

You can configure the start schedule for Kaspersky Embedded Systems Security tasks, and configure settings for running tasks by schedule.

In this section

Configuring the task start schedule settings

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

► *To configure task start schedule settings:*

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

   The **Task settings** window opens.
3. In the window that opens, on the **Schedule** tab, select the **Run by schedule** check box.
4. Configure schedule settings in accordance with your requirements. To do this, perform the following actions:

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

   - **Hourly**, if you want the task to run at intervals of 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 at intervals of 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 at intervals of a specified number of weeks; specify the number of weeks in the **Every <number> week(s) on** field. Specify the days of the week on which the task will be started (by default the task runs on Mondays).
   - **At application launch**, if you want the task to run every time Kaspersky Embedded Systems Security starts.
   - **After application database update**, if you want the task to run after every update of the application databases.

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

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

> After you have specified the task start frequency, the time of the first task start, and the date from which the schedule applies, information about the estimated time for the next task start will appear in the top part of the window in the **Next start** field. Updated information about the estimated time of the next task start will be displayed each time you open the **Task settings** window of the **Schedule** tab.
> **Blocked by policy** is displayed in the **Next start** field if starting system tasks on a schedule is set in the Kaspersky Security Center policy settings.

5. Use the **Advanced** tab to 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 a time interval under 24 hours 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 start of skipped tasks.
     c. Select the **Randomize the task start within interval of** check box and specify a value in minutes.
6. Click **OK**.

The configured task start 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 start schedule, take the following steps:*

1. In the Application Console tree open the context menu on the task name for which you wish to configure the start 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 scheduled task start.
   - Clear the **Run by schedule** check box if you want to disable scheduled task start.

   > The configured task start schedule settings are not deleted and will be applied at the next scheduled start of the task.
4. Click **OK**.

The configured task start schedule settings are saved.

Using user accounts to start tasks

You can start tasks under the system account or specify a different account.

In this section

About using accounts to start tasks

You can specify the account under which you want to run the selected task for the following functional components of Kaspersky Embedded Systems Security:

- Rule Generator for Applications Launch Control and Rule Generator for Device Control tasks
- On-Demand Scan task
- Update tasks

By default, these tasks are run using system account permissions.

A different account with proper access permissions is recommended in the following cases:

- In the Update task, if you specified a public folder on a different computer on the network as the update source.

- In the Update task, if a proxy server with built-in Windows NTLM authentication is used to access the update source.
- In On-Demand Scan tasks, if the system account does not possess permissions to access any of the scanned objects (for example, to files in shared folders on the computer).
- In the Rule Generator for Applications Launch Control task, if after completion of the task the generated rules are exported to a configuration file located at a path that the system account cannot access (for example, in one of the shared folders on the computer).

You can run Update, On-Demand Scan, and Rule Generator tasks with system account permissions. During execution of these tasks, Kaspersky Embedded Systems Security accesses shared folders on another computer in the network if this computer is registered in the same domain as the protected computer. In this case, the system account must possess access permissions for these folders. Kaspersky Embedded Systems Security will access the computer using permissions of the account **<domain name \ computer_name>**.

Specifying a user account to start a task

► *To specify an account to start a task, take the following steps:*

1. In the Application Console tree, open the context menu of the task for which you want to configure start with account permissions.
2. Select **Properties**.

   The **Task settings** window opens.
3. In the window that opens, do the following on the **Run as** tab:
   a. Select **User name**.
   b. Enter the user name and password for the account you want to use.

      The selected user must be registered on the protected computer or in the same domain as this computer.

   c. Confirm the password that has been entered.
4. Click **OK**.

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

Importing and exporting settings

This section provides information about how to export the settings of Kaspersky Embedded Systems Security or the settings of specific software components to a configuration file in XML format and how to import those settings from that configuration file back to the application.

In this section

About importing and exporting settings

You can export Kaspersky Embedded Systems Security settings to an XML configuration file and import settings into Kaspersky Embedded Systems Security from the configuration file. You can save all application settings or only settings for individual components to a configuration file.

When you export all settings of Kaspersky Embedded Systems Security to a file, the general application settings and settings of the following Kaspersky Embedded Systems Security components and functions are saved:

- Real-Time File Protection
- KSN Usage
- Device Control
- Applications Launch Control
- Rule Generator for Device Control
- Rule Generator for Applications Launch Control
- On-Demand Scan tasks
- File Integrity Monitor
- Log Inspector
- Kaspersky Embedded Systems Security database and software modules update
- Quarantine
- Backup
- Logs
- Administrator and user notifications
- Trusted Zone
- Exploit Prevention
- Password protection

Also, you can save the general settings of Kaspersky Embedded Systems Security in the file, as well as the rights of user accounts.

You cannot export group task settings.

Kaspersky Embedded Systems Security exports all passwords used by the application, for example, account data for running tasks or connecting to a proxy server. Exported passwords are saved in encrypted form in the configuration file. You can import passwords only using Kaspersky Embedded Systems Security installed on this computer if it has not been reinstalled or updated.

You cannot import previously saved passwords using Kaspersky Embedded Systems Security installed on a different computer. After settings have been imported on another computer, all passwords must be entered manually.

If a Kaspersky Security Center policy is active at the time of export, the application exports the specified values used by that policy.

Settings from a configuration file containing parameters for individual components of Kaspersky Embedded Systems Security (e.g., from a file created in Kaspersky Embedded Systems Security installed with incomplete set of components) can be imported. After the settings are imported, only those Kaspersky Embedded Systems Security settings that were contained in the configuration file are changed. All other settings remain the same.

> Settings of an active Kaspersky Security Center policy that have been blocked do not change when importing the settings.

Exporting settings

► *To export settings to a configuration file, take the following steps:*

1. In the Application Console tree, do one of the following:
   - In the context menu of the **Kaspersky Embedded Systems Security** node, select **Export settings** to export all Kaspersky Embedded Systems Security settings.
   - In the context menu for the task whose settings you want to export, select **Export settings** to export the settings of an individual functional component of the application.
   - To export the settings of the Trusted Zone component:
     a. In the Application Console tree, open the context menu of the **Kaspersky Embedded Systems Security** node.
     b. Select **Configure Trusted Zone settings**.

        The **Trusted Zone** window opens.
     c. Click the **Export** button.

        The welcome window of the settings export wizard opens.
2. Follow the instructions in the **Wizard**: specify the name of the configuration file for saving settings and the path to it.

   System environment variables can be used when specifying the path; user environment variables are not allowed.

   > If a Kaspersky Security Center policy is active at the time of export, the application exports the settings' values used by that policy.
3. Click the **Close** button in the **Export of application settings complete** window.

The export settings are saved when the wizard closes.

Importing settings

► *To import settings from a saved configuration file, take the following steps:*

1. In the Application Console tree, do one of the following:
   - In the context menu of the **Kaspersky Embedded Systems Security** node, select **Import settings** to import all Kaspersky Embedded Systems Security settings.
   - In the context menu for the task whose settings you want to import, select **Import settings** to import the settings of an individual functional component of the application.
   - To import the settings of the Trusted Zone component:
     a. In the Application Console tree, open the context menu of the **Kaspersky Embedded Systems Security** node.
     b. Select **Configure Trusted Zone settings**.

        The **Trusted Zone** window opens.
     c. Click the **Import** button.

        The welcome window of the settings import wizard opens.
2. Follow the instructions in the Wizard: specify the configuration file from which you want to import settings.

   After you have imported the general settings of Kaspersky Embedded Systems Security or its functional components on the computer, you will not be able return to the previous setting values.
3. Click the **Close** button in the **Application settings import completed** window.

   The imported settings are saved when the wizard closes.
4. In the toolbar of the Application Console, click the **Refresh** button.

The imported settings are displayed in the Application Console window.

Kaspersky Embedded Systems Security does not import passwords (account data to start tasks or connect to the proxy server) from the file created on another computer or on the same computer, after Kaspersky Embedded Systems Security has been re-installed or updated on it. After the importing operation is completed, passwords must be entered manually.

Using security settings templates

This section contains information about using security settings templates in Kaspersky Embedded Systems Security protection and scan tasks.

In this section

About security settings templates

You can manually configure a node's security settings in the tree or in a list of the computer's 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 Embedded Systems Security protection and scan tasks.

Templates can be used to configure the security settings of the following Kaspersky Embedded Systems Security tasks:

- Real-Time File Protection
- Scan at Operating System Startup
- Critical Areas Scan
- On-Demand Scan tasks

Security settings from a template applied to a parent node in the computer's file resource tree are applied to all child nodes. A parent node's template is not applied to child nodes in the following cases:

- If the security settings of the child nodes were configured separately (see Section "Applying a security settings template" on page 157).
- If the child nodes are virtual. You must apply the template to each virtual node separately.

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 apply the security setting 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 computer'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.

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**.

   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.

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 apply the security setting 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 computer's network file resources, open the context menu of the node or item to which you want to apply the template.
4. Select **Apply template** → **<Template name>**.
5. Click the **Save** button.

The security settings template is applied to the selected node in the tree of the computer's file resources. The **Security level** tab of the selected node now has the value **Custom**.

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

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

► *To apply security settings from a template to all selected nodes, take the following steps:*

1. In the Application Console tree, select the task for which you want to apply the security setting 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 computer's network file resources, select a parent node in order to apply the template to the selected node and to all of its child nodes.
4. In the context menu, select **Apply template** → **<Template name>**.
5. Click the **Save** button.

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

Deleting a security settings template

► *To delete a security settings template, take the following steps:*

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 view settings templates 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 is deleted.

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

Viewing protection status and Kaspersky Embedded Systems Security information

► *To view information about the computer protection status Kaspersky Embedded Systems Security,*

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

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

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

You can refresh the information manually.

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

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

The following application information is displayed in the details pane of the Application Console:

- Kaspersky Security Network Usage status.
- Computer protection status.
- Information about database and application module updates.
- Actual diagnostic data.
- Data about computer control tasks.
- License information.
- Status of integration with Kaspersky Security Center: details of the computer with Kaspersky Security Center installed and to which the application is connected; information about application tasks controlled by the active policy.

Different colors are used to indicate the protection status:

- *Green*. The task is being run in accordance with the configured settings. Protection is active.
- *Yellow*. The task was not started, has been paused, or has been stopped. Security threats may occur. You are advised to configure and start the task.
- *Red*. The task completed with an error or a security threat was detected while the task was running. You are advised to start the task or take measures to eliminate the detected security threat.

Some details in this block (for example, task names or the number of threats detected) are links that, when clicked, take you to the node of the relevant task or open the task log.

The **Kaspersky Security Network Usage** section displays current task status, for example, *Running*, *Stopped* or *Never performed*. The indicator can take the following values:

- Green color signifies that the KSN Usage task is running and file requests for statuses are being send to KSN.
- Yellow color signifies that one of the Statements is accepted, but the task is not running; or the task is running, but file requests are not sent to KSN.

Computer **protection**

The **Computer protection** section (see the table below) displays information about the computer's current protection status.

Table 27. Information about computer protection status

Protection section	Information
Computer protection status indicator	The color of the panel with the section name reflects the status of tasks being performed in the section. The indicator can take the following values: • Green – This color is displayed by default and signifies that Real-Time File Protection component is installed and the task is running. • Yellow – The Real-Time File Protection component is not installed, and the Critical Areas Scan task has not been performed for a long time. • Red – Real-Time File Protection task is not running.
Real-Time File Protection	**Task status** – Current task status, for example, *Running* or *Stopped*. **Detected** – Number of objects detected by Kaspersky Embedded Systems Security. For example, if Kaspersky Embedded Systems Security detects one malware program in five files, the value in this field increases by one. If the number of detected malware programs exceeds 0, the value is highlighted in red.
Critical Areas Scan	**Last scan date** – Date and time of the last Critical Areas Scan for viruses and other computer security threats. *Never performed* – An event that occurs when the Critical Areas Scan task has not been performed in the last 30 days or longer (default value). You can change the threshold for generating this event.
Exploit prevention	**Status** – current status of exploit prevention techniques, for example, *Applied* or *Not Applied*. **Prevention mode** – one of two available modes, selected during configuration of process memory protection: • Terminate on exploit. • Statistics only. **Processes protected** – the total number of processes added to the protection scope and handled in accordance with the selected mode.
Backed up objects	*Backup free space threshold exceeded* – This event occurs when the amount of free space in Backup is approaching the specified limit. Kaspersky Embedded Systems Security continues to move objects to Backup. In this case, the value in the **Space used** field is highlighted in yellow. *Maximum Backup size exceeded* – This event occurs when the Backup size has reached the specified limit. Kaspersky Embedded Systems Security continues to move objects to Backup. In this case, the value in the **Space used** field is highlighted in red. **Backed up objects** – Number of objects currently in Backup. **Space used** – Amount of Backup space used.

Update

The **Update** section (see the table below) displays information about how up-to-date the anti-virus databases and application modules are.

Table 28. Information about the status of Kaspersky Embedded Systems Security databases and modules

Updates section	Information
Status indicator for databases and software modules	The color of the panel with the section name reflects the status of application databases and modules. The indicator can take the following values: • Green – This color is displayed by default and signifies that application databases are up to date and that the last database update task was completed successfully. • Yellow – Databases are out of date, or the last database update task failed. • Red – The event *Application databases are extremely out of date* or *Application databases are corrupted* has occurred.
Database Update and **Software Modules Update**	**Database status** – An evaluation of the Database Update status. It can take the following values: • **Application database is up to date** – Application databases were updated no more than 7 days ago (default). • **Application database is out of date** – Application databases were updated between 7 and 14 days ago (default). • **Application database is extremely out of date** – Application databases were updated more than 14 days ago (default). You can change the thresholds for generating the events *Application databases are out of date* and *Application databases are outdated*. **Database release date** – Date and time of the release of the latest database update. The date and time are specified in UTC format. **Status of the latest completed Database Update task** – Date and time of the latest database update. The date and time are specified according to the local time of the protected computer. The field is red if the *Failed* event occurred. **Number of module updates available** – Number of Kaspersky Embedded Systems Security module updates available to be downloaded and installed. **Number of module updates installed** – Number of installed Kaspersky Embedded Systems Security module updates.

Control

The **Control** section (see table below) displays information about the Applications Launch Control, Device Control and Firewall Management tasks.

Table 29. Information about computer control status

Control section	Information
Computer Control status indicator	The color of the panel with the section name reflects the status of tasks being performed in the section. The indicator can take the following values: • Green – This color is displayed by default and signifies that the Applications Launch Control component is installed and the task is running in the **Active** mode. • Yellow – Applications Launch Control is running in the **Statistics only** mode. • Red – The Applications Launch Control task is not running or failed.
Applications Launch Control	**Task status** – Current task status, for example, *Running* or *Stopped*. **Mode** – One of the two available Applications Launch Control task modes: • Active • Statistics only **Applications launches denied** – Number of attempts to start applications blocked by Kaspersky Embedded Systems Security during the Applications Launch Control task. If the number of blocked application launches exceeds 0, the field is red. **Average processing time (ms)** – Time taken by Kaspersky Embedded Systems Security to process an attempt to start applications on the protected computer.
Device Control	**Task status** – Current task status, for example, *Running* or *Stopped*. **Mode** – One of two available Device Control task modes: • **Active** • **Statistics only** **Devices blocked** – Number of attempts to connect a mass storage device that were blocked by Kaspersky Embedded Systems Security during the Device Control task. If the number of blocked mass storage devices exceeds 0, the field is red.
Firewall Management	**Task status** – Current task status, for example, *Running* or *Stopped*. **Connection attempts blocked** – Number of connections to a protected computer that were blocked by the specified firewall rules.

Diagnostics

The **Diagnostics** section (see the table below) displays information about the File Integrity Monitor and Log Inspection tasks.

Table 30. Information about System Inspection status

Diagnostics section	Information
Diagnostics status indicator	The color of the panel with the section name reflects the status of tasks being performed in the section. The indicator can take the following values: • Green – This color is displayed by default and signifies that one or both system inspection components are installed and tasks are running. • Yellow – Both components are installed, but one of the system inspection tasks is not running; the *Not running* event occurred. • Red – One of the tasks failed.
File Integrity Monitor	**Task status** – Current task status, for example, *Running* or *Stopped*. **Non-sanctioned file operations** – Number of changes to files within the monitoring scope. These changes may indicate that the security of a protected computer has been breached.
Log Inspection	**Task status** – Current task status, for example, *Running* or *Stopped*. **Possible violations** – Number of recorded violations based on data from the Windows Event Log. This number is determined based on the specified task rules or using the heuristic analyzer.

The Kaspersky Embedded Systems Security licensing information is displayed in the row in the bottom left corner of the details pane of the **Kaspersky Embedded Systems Security** node.

You can configure Kaspersky Embedded Systems Security properties by following the Application Properties link (see Section "Kaspersky Embedded Systems Security settings in the Application Console" on page 134).

You can connect to a different computer by following the **Connect to another computer** link (see Section "Managing Kaspersky Embedded Systems Security via the Application Console on another computer" on page 146).

Compact Diagnostic Interface

This section describes how to use the Compact Diagnostic Interface for reviewing computer status or current activity, and how to configure writing of dump and trace files.

In this chapter

About the Compact Diagnostic Interface

The Compact Diagnostic Interface component (also referred to as the "CDI") is installed and uninstalled along with the System Tray Icon component independently from the Application Console, and can be used when the Application Console is not installed on the protected computer. The CDI is started from the System Tray Icon or by running kavfsmui.exe from the application folder on the computer.

From the CDI window, you can do the following:

- Review information about general application status (see Section "Reviewing Kaspersky Embedded Systems Security status via the Compact Diagnostic Interface" on page 166).
- Review security incidents that have occurred (see Section "Reviewing security event statistics" on page 167).
- Review current activity on the protected (see Section "Reviewing current application activity" on page 167) computer.
- Start or stop writing dump and trace files (see Section "Configuring writing of dump and trace files" on page 168).
- Open the Application Console.
- Open the **About the application** window with the list of installed updates and available patches.

The CDI is available even if access to Kaspersky Embedded Systems Security functions is password-protected. No password is required.

> The CDI component cannot be configured via Kaspersky Security Center.

Reviewing Kaspersky Embedded Systems Security status via the Compact Diagnostic Interface

► *To open the Compact Diagnostic Interface window, perform the following actions:*

1. Right-click the Kaspersky Embedded Systems Security System Tray Icon in the toolbar notification area.
2. Select the **Open Compact Diagnostic Interface** option.

   The **Compact Diagnostic Interface** window opens.

Review the current status of the key, Real-Time Computer Protection tasks, and Update tasks on the **Protection status** tab.Different colors are used to notify the user about the protection status (see table below).

Table 31. Compact Diagnostic Interface protection status.

Section	Status
Real-Time Computer Protection	The panel is *green* for either of the following scenarios (any number of the conditions can be met): • Recommended configuration: • The Real-Time File Protection task is started with the default settings. • The Applications Launch Control task is started in **Active** mode with the default settings. • Acceptable configuration: • The Real-Time File Protection task is configured by the user. • Applications Launch Control task settings are modified.
	The panel is *yellow* if one or more of the following conditions are met: • The Real-Time File Protection task is paused (by the user or schedule). • The Applications Launch Control task is started in **Statistics only** mode. • Exploit Protection and Applications Launch Control are started in **Statistics only** mode.
	The panel is *red* if both of the following conditions are met: • The Real-Time File Protection component is not installed or the task is stopped or paused. • The Applications Launch Control component is not installed or the task is started in **Statistics only** mode.
Licensing	The panel is *green* if the current license is valid.
	A *yellow* panel signifies that one of the following events has occurred: • **Checking the license status**. • **The license will expire in 14 days and no additional key or activation code have been added**. • **The added key has been black-listed and is about to be blocked**.

	A *red* panel signifies that one of the following events has occurred: • **Application not activated.** • **License has expired.** • **End User License Agreement has been violated.** • **Key is blacklisted.**
Update	The panel is *green* when Application databases are up-to-date.
	The panel is *yellow* when Application databases are out of date.
	The panel is *red* when Application databases are extremely out of date.

Reviewing security event statistics

The **Statistics** tab displays all security events. Each protection task statistic is displayed in a separate block specifying the number of incidents and the date, and time when the last incident occurred. When an incident is logged, the block color changes to red.

► *To review the statistics:*

1. Right-click the Kaspersky Embedded Systems Security System Tray Icon in the toolbar notification area.
2. Select the **Open Compact Diagnostic Interface** option.

   The **Compact Diagnostic Interface** window opens.
3. Open the **Statistics** tab.
4. Review the security incidents for the protection tasks.

Reviewing current application activity

On this tab, you can review the status of current tasks and application processes, and promptly get notifications about critical events that occur.

Different colors are used to indicate the application activity status:

- In the **Tasks** section:
  - *Green*. No conditions for yellow or red.
  - *Yellow*. Critical areas have not been scanned for a long time.
  - *Red*. Any of the following conditions is true:
    - No tasks are started and a start schedule is not set up for any of the tasks.
    - Application launch errors are logged as critical events.
- In the **Kaspersky Security Network** section:
  - *Green*. The KSN Usage task is started.
  - *Yellow*. The KSN Statement is accepted, but the task is not started.

► *To review the current application activity on the computer:*

1. Right-click the Kaspersky Embedded Systems Security System Tray Icon in the toolbar notification area.
2. Select the **Open Compact Diagnostic Interface** option.

   The **Compact Diagnostic Interface** window opens.
3. Open the **Current application activity** tab.
4. Review the following information in the **Tasks** section:
   - **Critical areas not scanned for a long time**

     > This field is displayed only if the application returns a corresponding warning about critical areas scans.
   - **Running now**
   - **Execution failed**
   - **Next start defined by a schedule**
5. Review the following information in the **Kaspersky Security Network** section:
   - **KSN is on. File reputation services are enabled** or **Protection is off**.
   - **Application statistics is being sent to KSN**.

     The application sends information about malware, including fraudulent software, detected during execution of the Real-Time File Protection task and the On-Demand Scan tasks, as well as debugging information about errors during scanning.

     The field is displayed if the **Send Kaspersky Security Network statistics** check box is selected in the KSN Usage task settings.
6. Review the following information in the **Integration with Kaspersky Security Center** section:
   - Local management is allowed.
   - Policy is applied: <Kaspersky Security Center server name>.

Configuring writing of dump and trace files

You can configure the writing of dump and trace files via the CDI.

> You can also configure malfunction diagnostics via the Application Console (see Section "Kaspersky Embedded Systems Security settings in the Application Console" on page 134).

► *To start writing dump and trace files, perform the following actions:*

1. Right-click the Kaspersky Embedded Systems Security System Tray Icon in the toolbar notification area.
2. Select the **Open Compact Diagnostic Interface** option.

   The **Compact Diagnostic Interface** window opens.
3. Open the **Troubleshooting** tab.

4. Change the following trace settings if necessary:

   a. Select the **Write debug information to the trace file in this folder** check box.

   b. Click the **Browse** button to specify the folder where Kaspersky Embedded Systems Security will save trace files.

      Tracing will be enabled for all components with the default parameters using the **Debug** level of detail and the default maximum log size of 50 MB.

5. Change the following dump-file settings if necessary:

   a. Select the **Create dump file on malfunction in this folder** check box.

   b. Click the **Browse** button to specify the folder where Kaspersky Embedded Systems Security will save the dump file.

6. Click the **Apply** button.

   A new configuration will be applied.

Updating Kaspersky Embedded Systems Security databases and software modules

This section provides information about databases and software modules update tasks of Kaspersky Embedded Systems Security, copying updates and rolling back databases updates of Kaspersky Embedded Systems Security, as well as instructions on how to configure databases and software modules update tasks.

In this chapter

About Update tasks

Kaspersky Embedded Systems Security provides four system update tasks: Database Update, Software Modules Update, Copying Updates, and Rollback of Database Update.

By default Kaspersky Embedded Systems Security connects to the updates source (one of Kaspersky Lab's update computers) every hour. You can configure all Update tasks (see Section "Configuring Update tasks" on page 176), except for the Rollback of Database Update task. When task settings are modified, Kaspersky Embedded Systems Security will apply the new values at the next task start.

You are not allowed to pause and resume Update tasks.

Database Update

By default, Kaspersky Embedded Systems Security copies databases from the update source to the protected computer and immediately starts using them in the running Real-Time Computer Protection task. The On-Demand Scan tasks start using the updated database at the next start.

By default, Kaspersky Embedded Systems Security runs the Database Update task every hour.

Software Modules Update

By default, Kaspersky Embedded Systems Security checks availability of software modules updates on the update source. In order to start using installed software modules, a computer restart and / or a restart of Kaspersky Embedded Systems Security is required.

By default, Kaspersky Embedded Systems Security runs the Software Modules Update task on a weekly basis on Fridays at 04:00 PM (time according to the regional settings of the protected computer). During task execution, the application checks for availability of important and scheduled updates of Kaspersky Embedded Systems Security modules without distributing them.

Copying Updates

By default, during task execution, Kaspersky Embedded Systems Security downloads Database Update files and saves them to the specified network or local folder without applying them.

The Copying Updates task is disabled by default.

Rollback of Database Update

During task execution, Kaspersky Embedded Systems Security returns to using databases with previously installed updates.

The Rollback of Database Update task is disabled by default.

About Kaspersky Embedded Systems Security software modules update

Kaspersky Lab can issue update packages for Kaspersky Embedded Systems Security modules. The update packages can be *urgent* (or *critical*) and planned. Critical update packages repair vulnerabilities and errors; planned packages add new features or enhance existing features.

Urgent (critical) update packages are uploaded to Kaspersky Lab's update servers. Their automatic installation can be configured using the Software Modules Update task. By default, Kaspersky Embedded Systems Security runs the Software Modules Update task on a weekly basis on Fridays at 04:00 PM (time according to the regional settings of the protected computer).

Kaspersky Lab does not publish planned update packages on its update servers for automatic update; these can be downloaded from the Kaspersky Lab website. The Software Modules Update task can be used to receive information about the release of scheduled Kaspersky Embedded Systems Security updates.

Critical updates can be updated from the Internet to each protected computer, or one computer can be used as intermediary by copying all updates onto it and then distributing them to the network computers. In order to copy and save updates without installing them use the Copying Updates task.

Before updates of modules are installed Kaspersky Embedded Systems Security creates backup copies of the previously installed modules. If the software modules updating process is interrupted or results in an error, Kaspersky Embedded Systems Security will automatically return to using the previously installed software modules. Software modules can be rolled back manually to the previously installed updates.

During the installation of downloaded updates the Kaspersky Security Service automatically stops and then restarts.

About Kaspersky Embedded Systems Security Database Updates

Kaspersky Embedded Systems Security databases stored on the protected computer quickly become outdated. Kaspersky Lab's virus analysts detect hundreds of new threats daily, create identifying records for them, and include them in application database updates. Database updates are a file or set of files containing records that identify threats discovered during the time since the last update was created. To maintain the required level of computer protection, we recommend that database updates are received regularly.

By default, if the Kaspersky Embedded Systems Security databases are not updated within a week from the time at which the installed database updates were last created, the *Application database is out of date* event occurs. If the databases are not updated for a period of two weeks, the *Application database is extremely out of date* event occurs. Information about the up-to-date status of the databases (see Section "Viewing protection status and Kaspersky Embedded Systems Security information" on page 159) is displayed in the details pane of the **Kaspersky Embedded Systems Security** node of the Application Console tree. You can use Kaspersky Embedded Systems Security general settings to indicate a different number of days before these events occur. You can also configure administrator notifications about these events (see Section "Configuring administrator and user notifications" on page 215).

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

Updates can be downloaded to every protected computer, or one computer can be used as intermediary by copying all updates onto it and then distributing them to the computers. If you use Kaspersky Security Center for centralized administration of protection of computers in an organization, you can use Kaspersky Security Center Administration Server as an intermediary for downloading updates.

Database Update tasks can be started manually or based on a schedule (see Section "Configuring the task start schedule settings" on page 149). By default, Kaspersky Embedded Systems Security runs the Database Update task every hour.

If the update downloading process is interrupted or results in an error Kaspersky Embedded Systems Security will automatically switch back to using the databases with the last installed updates. If the Kaspersky Embedded Systems Security databases become corrupted, they can be manually rolled back (see Section "Rolling back Kaspersky Embedded Systems Security database updates" on page 182) to previously installed updates.

Schemes for updating databases and modules of anti-virus applications used within organization

Selection of updates source in the update tasks depends on the databases and program modules update scheme used in the organization.

Kaspersky Embedded Systems Security databases and modules can be updated on the protected computers using the following schemes:

- Download updates directly from the Internet to each protected computer (Scheme 1).
- Download updates from the Internet to an intermediary computer and distribute updates to computers from the computer.

  Any computer with the software listed below installed can serve as an intermediary computer:

  - Kaspersky Embedded Systems Security (Scheme 2).
  - Kaspersky Security Center Administration Server (Scheme 3).

Updating using an intermediary computer will not only allow Internet traffic to be decreased, but will also ensure additional network computers security.

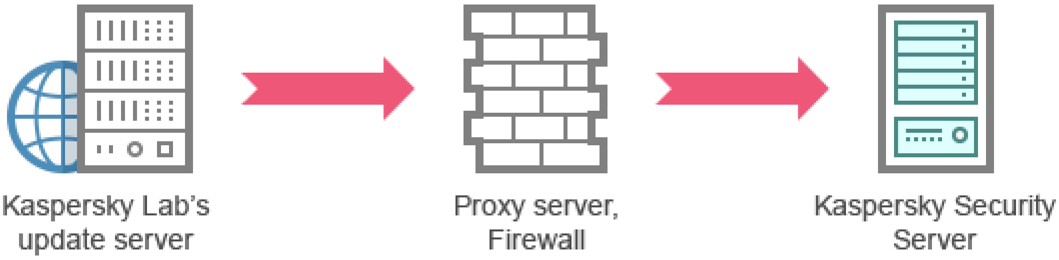
Description of update schemes listed is provided below.

Scheme 1. Updating databases and modules directly from the Internet

► *To configure Kaspersky Embedded Systems Security updates directly from the Internet:*

on each protected computer in the settings of the Database Update task and the Software Modules Update task, specify Kaspersky Lab's update servers as the source of updates.

Other HTTP or FTP servers which have an update folder can be configured as the updates source.



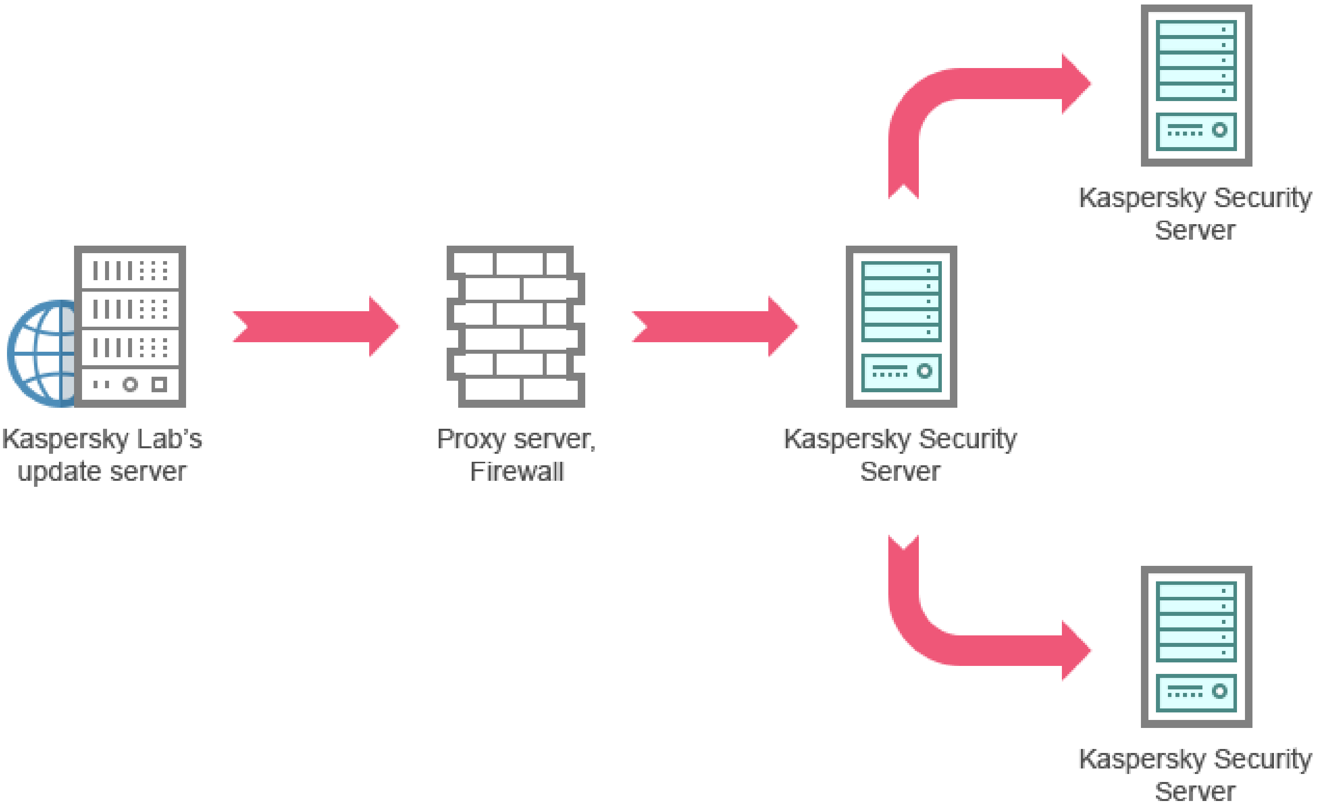
Scheme 2. Updating databases and modules via one of the protected computers

► *To configure Kaspersky Embedded Systems Security updates via one of the protected computers:*

1. Copy updates to the selected protected computer. To do this, perform the following actions:
    - Configure the Copying Updates task settings on the selected computer:
        a. Specify Kaspersky Lab's update server as the updates source.

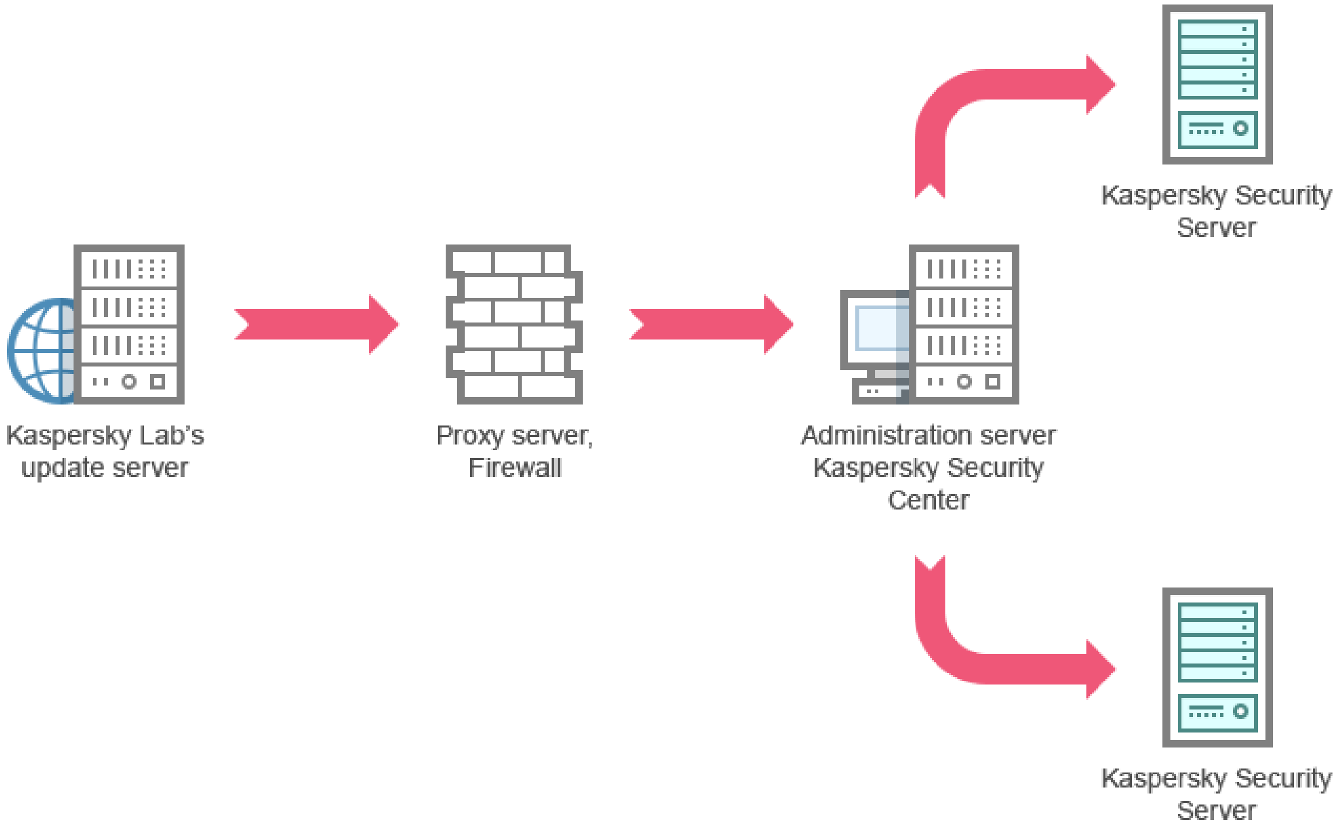
        b. Specify a shared folder to be used as the folder where updates are saved.
2. Distribute updates to other protected computers. To do this, perform the following actions:
    - On each protected computer, configure the settings for the Database Update task and the Software Modules Update task (see figure below).
        a. For the update source, specify a folder on the intermediary computer's drive to which updates will be downloaded.

Kaspersky Embedded Systems Security will obtain updates via one of the protected computers.


Kaspersky Security Server
Kaspersky Lab's update server
Proxy server, Firewall
Kaspersky Security Server
Kaspersky Security Server

Scheme 3. Updating databases and modules via Kaspersky Security Center Administration Server

If the Kaspersky Security Center application is used for the centralized administration of Anti-Virus computer protection, updates can be downloaded via the Kaspersky Security Center Administration Server installed in the local area network (see figure below).


Kaspersky Lab's update server
Proxy server, Firewall
Administration server Kaspersky Security Center
Kaspersky Security Server
Kaspersky Security Server

► *To configure Kaspersky Embedded Systems Security updates via the Kaspersky Security Center Administration Server:*

1. Download updates from Kaspersky Lab's update servers to Kaspersky Security Center Administration Server. To do this, perform the following actions:
   - Configure the Retrieve updates by Administration Server task for the specified set of computers:
     a. Specify Kaspersky Lab's update servers as the updates source.
2. Distribute updates to protected computers. To do so, perform one of the following actions:
   - On the Kaspersky Security Center configure an Anti-Virus database (application module) update group task to distribute updates to protected computers:
     a. In the task schedule specify **After Administration Server has retrieved updates** as start frequency.

        Administration Server will start the task each time it receives updates (recommended method).

The start frequency of **After Administration Server has retrieved updates** cannot be specified in the Application Console.

- On each protected computer, configure the Database Update task and the Software Modules Update task:

  a. Specify the Kaspersky Security Center Administration Server as the update source.

  b. Configure the task schedule if necessary.

  > If Kaspersky Embedded Systems Security anti-virus databases are rarely updated (from once a month to once a year), the likelihood of detecting threats decreases and the frequency of false alarms raised by application components increases.

Kaspersky Embedded Systems Security will obtain updates via the Kaspersky Security Center Administration Server.

If you plan to use Kaspersky Security Center administration server for updates distribution, install Network Agent, an application component included in the Kaspersky Security Center distribution kit, onto each of the protected computers. This ensures interaction between the Administration Server and Kaspersky Embedded Systems Security on the protected computer. Detailed information about the Network Agent and its configuration using Kaspersky Security Center is provided in the *Kaspersky Security Center Help*.

Configuring Update tasks

This section provides instructions on how to configure Kaspersky Embedded Systems Security update tasks.

In this section

Configuring settings for working with Kaspersky Embedded Systems Security update sources

For each update task except the Rollback of Database Update task, you can specify one or several update sources, add user-defined update sources, and configure the settings for connection with the specified sources.

> After update task settings are modified, the new settings will not be immediately applied in the running update tasks. The configured settings will be applied only when the task is restarted.

► *To specify the type of update source:*

1. In the Application Console tree, expand the **Update** node.
2. Select the child node corresponding to the update task that you want to configure.
3. Click the **Properties** link in the details pane of the selected node.

   The **Task settings** window opens on the **General** tab.
4. In the **Update source** section, select the type of Kaspersky Embedded Systems Security update source:
   - **Kaspersky Security Center Administration Server**

     Kaspersky Embedded Systems Security uses Kaspersky Security Center Administration Server as the update source.

     You can only select this option if Kaspersky Lab applications on your network are administered using the Kaspersky Security Center remote access system and if Network Agent (the Kaspersky Security Center component that provides the connection between computers and Administration Server) is installed on the protected computer.
   - **Kaspersky Lab update servers**

     Kaspersky Embedded Systems Security uses Kaspersky Lab websites as update sources, hosting updates for the databases and software modules of all of the company's products.

     This option is selected by default.
   - **Custom HTTP or FTP servers, or network folders**

     Kaspersky Embedded Systems Security uses the administrator-specified HTTP or FTP server or folders on local network folder as the update source.

     You can create a list of sources with the current updates by clicking the **Custom HTTP or FTP servers, or network folders** link.
5. If required, configure the advanced settings for user-defined update sources:

   a. Click on the **Custom HTTP or FTP servers, or network folders** link.

      i. In the **Update servers** window that opens, select or clear the check boxes next to the user-defined update sources in order to begin or terminate their use.

      ii. Click **OK**.

   b. In the **Update source** section on the **General** tab, select or clear the **Use Kaspersky Lab update servers if specified servers are not available** check box.

      This check box enables or disables the option of using Kaspersky Lab update servers as the update source if the user-defined update sources are unavailable.

      If the check box is selected, this function is enabled.

      The check box is selected by default.

      You can select the **Use Kaspersky Lab update servers if specified servers are not available** check box when the **Custom HTTP or FTP servers, or network folders** option is enabled.

6. In the **Task settings** window, select the **Connection settings** tab to configure the settings for connecting to update sources:
    - Clear or select the **Use proxy server settings to connect to Kaspersky Lab update servers** check box.

        The check box enables / disables the use of proxy server settings if updates are received from Kaspersky Lab servers or if the **Use Kaspersky Lab update servers if specified servers are not available** check box is selected.

        If the check box is selected, the proxy server settings are used.

        If the check box is cleared, the proxy server settings are not used.

        The check box is selected by default.

    - Clear or select the **Use proxy server settings to connect to other servers** check box.

        The check box enables or disables the use of proxy server settings if the option **Custom HTTP or FTP servers, or network folders** is selected as the update source.

        If the check box is selected, the proxy server settings are used.

        The check box is cleared by default.

    > For information about configuring the optional proxy server settings and authentication settings for accessing the proxy server, see Starting and configuring Kaspersky Embedded Systems Security Database Update task section.

7. Click **OK**.

The configured settings for the Kaspersky Embedded Systems Security update source will be saved and applied at the next task start.

You can manage the list of user-defined Kaspersky Embedded Systems Security update sources.

► *To edit the list of user-defined application update sources:*

1. In the Application Console tree, expand the **Update** node.
2. Select the child node corresponding to the update task that you want to configure.
3. Click the **Properties** link in the details pane of the selected node.

    The **Task settings** window opens on the **General** tab.
4. Click on the **Custom HTTP or FTP servers, or network folders** link.

    The **Update servers** window opens.
5. Do the following:
    - To add a new user-defined update source, in the entry field specify the address of the folder containing update files on the FTP or HTTP server; specify a local or network folder in the UNC (Universal Naming Convention) format. Press **ENTER**.

        By default, the added folder is used as the source of updates.
    - To disable use of a user-defined source, clear the check box next to the source in the list.
    - To enable use of a user-defined source, select the check box next to the source in the list.

- In order to change the order in which Kaspersky Embedded Systems Security accesses user-defined update sources, use the **Move Up** and **Move Down** buttons to move the selected source to the beginning or to the end of the list, depending on whether it is to be used before or after other sources.
- To change the path to the user-defined source, select the source in the list and click the **Edit** button, make the required changes in the entry field and press the **ENTER** key.
- To remove a user-defined source, select it in the list and press the **Remove** button.

  > You cannot delete the only remaining user-defined source from the list.

6. Click **OK**.

The changes in the list of user-defined application update sources will be saved.

Optimizing use of disk I/O when running Database Update task

When running the Database Update task, Kaspersky Embedded Systems Security stores update files on the local disk of the computer. You can lower the workload on the disk I/O subsystem of the computer through storing update files on a virtual drive in the RAM when running the update task.

> This feature is available for Microsoft Windows 7 operating systems and higher.

> When using this feature while running the Database Update task, an extra logical drive may appear in the operating system. This logical drive will be removed from the operating system after the task is completed.

► *To lower the workload on your computer's disk I/O subsystem during Database Update task, take the following steps:*

1. In the Application Console tree, expand the **Update** node.
2. Select the **Database Update** child node.
3. Click the **Properties** link in the details pane of the **Database Update** node.
4. The **Task settings** window opens on the **General** tab.
5. In the Disk I/O usage optimization section, define the following settings:
   - Clear or select the **Lower the load on the disk I/O** check box.

     This check box enables or disables the feature of the disk subsystem optimization through storing update files on a virtual drive in the RAM.

     If the check box is selected, this function is enabled.

     The check box is cleared by default.
   - In the **RAM used for optimization** field, specify the RAM volume (in MB). The operating system temporarily allocates the specified RAM volume to store update files while running the task. The default RAM size is 512 MB. The minimum RAM size is 400 MB.

6. Click **OK**.

The configured settings will be saved and applied at the next task start.

Configuring Copying Updates task settings

► *To configure the Copying Updates task:*

1. In the Application Console tree, expand the **Update** node.
2. Select the **Copying Updates** child node.
3. Click the **Properties** link in the details pane of the **Copying Updates** node.

   The **Task settings** window opens.
4. On the **General** and **Connection settings** tabs, configure the settings for working with update sources (see Section "Configuring settings for working with Kaspersky Embedded Systems Security update sources" on page 176).
5. On the **General** tab in the **Copying updates settings** section:
   - Specify the conditions for copying updates:
     - **Copy database updates**.

       Kaspersky Embedded Systems Security downloads only software database updates.

       This option is selected by default.
     - **Copy critical software modules updates**.

       Kaspersky Embedded Systems Security downloads only urgent Kaspersky Embedded Systems Security software module updates.
     - **Copy database updates and critical software modules updates**.

       Kaspersky Embedded Systems Security downloads software database updates and critical software module updates of Kaspersky Embedded Systems Security.
   - Specify the local or network folder to which Kaspersky Embedded Systems Security will be distributing downloaded updates.
6. On the **Schedule** and **Advanced** tabs configure the task start schedule (see Section "Configuring the task start schedule settings" on page 149).
7. On the **Run as** tab, configure the task to start using account permissions (see Section "Specifying a user account to start a task" on page 152).
8. Click **OK**.

The configured settings will be saved and applied at the next task start.

Configuring Software Modules Update task settings

► *To configure the Software Modules Update task:*

1. In the Application Console tree, expand the **Update** node.
2. Select the **Software Modules Update** child node.
3. Click the **Properties** link in the details pane of the **Software Modules Update** node.

The **Task settings** window opens.

4. On the **General** and **Connection settings** tabs, configure the settings for working with update sources (see Section "Configuring settings for working with Kaspersky Embedded Systems Security update sources" on page 176).
5. On the **General** tab in the **Application update settings** section, configure the settings for updating application modules:
   - **Only check for critical software updates available**

     Kaspersky Embedded Systems Security displays a notification about urgent updates to software modules available in the update source without downloading the updates. The notification is displayed if notifications about events of this type are enabled.

     This option is selected by default.
   - **Copy and install critical software modules updates**

     Kaspersky Embedded Systems Security downloads and installs critical updates to software modules.
   - **Allow operating system restart**

     The operating system is restarted after installing updates that require a restart.

     If the check box is selected, Kaspersky Embedded Systems Security reboots the operating system after installing updates that require a reboot.

     This check box is active if the **Copy and install critical software modules updates** option is selected.

     The check box is cleared by default.
   - **Receive information about available scheduled software modules updates**

     Notifications about all scheduled updates to Kaspersky Embedded Systems Security software modules available in the update source are displayed. The application displays a notification if notifications are enabled for events of this type.

     If the check box is selected, Kaspersky Embedded Systems Security displays a notification about all scheduled updates to software modules available in the update source.

     The check box is selected by default.
6. On the **Schedule** and **Advanced** tabs configure the task start schedule (see Section "Configuring the task start schedule settings" on page 149). By default, Kaspersky Embedded Systems Security runs the Software Modules Update task on a weekly basis on Fridays at 04:00 PM (time according to the regional settings of the protected computer).
7. On the **Run as** tab, configure the task start using account permissions (see Section "Specifying a user account to start a task" on page 152).
8. Click **OK**.

The configured settings will be saved and applied at the next task start.

Kaspersky Lab does not publish planned update packages on the update servers for automatic installation; these can be downloaded manually from the Kaspersky Lab website. Administrator notification about the *New scheduled update of application software modules is available* event can be configured; this will contain the URL of the page on the website from which scheduled updates can be downloaded.

Rolling back Kaspersky Embedded Systems Security database updates

Before database updates are applied, Kaspersky Embedded Systems Security creates backup copies of the previously used databases. If the update has been interrupted or has resulted in an error, Kaspersky Embedded Systems Security will automatically return to using the previously installed databases.

If any problems arise after you have updated the databases, they can be rolled back to the previously installed updates through the Rollback of Database Update task.

► *To start the Rollback of Database Update task:*

click the **Start** link in the details pane of the **Rollback of Database Update** node.

Rolling back application module updates

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

Before applying updates of software modules, Kaspersky Embedded Systems Security creates backup copies of the modules currently in use. If the modules updating process has been interrupted or has resulted in an error, Kaspersky Embedded Systems Security will automatically return to using modules with the latest installed updates.

In order to roll back the software modules use the Microsoft Windows component **Install and delete applications**.

Update task statistics

While the update task is running, real-time information can be viewed about the amount of data downloaded since the task has been started until the present moment, and also other task execution statistics.

When the task is completed or stopped, you can view this information in the task log.

► *To view update task statistics take the following steps:*

1. In the Application Console tree, expand the **Update** node.
2. Select the child node that corresponds to the task whose statistics you want to view.

Task statistics are displayed in the **Statistics** section of the details pane of the selected node.

If you are viewing the Database Update task or the Copying Updates task the **Statistics** block shows the volume of data downloaded by Kaspersky Embedded Systems Security on the present moment (**Received data**).

If you are viewing the Software Modules Update task, you will see the information described in the table below.

Table 32. Information about the Software Modules Update task

Field	Description
Received data	Total amount of downloaded data.
Available critical updates	Number of critical updates available for installation.
Available scheduled updates	Number of planned updates available for installation.
Errors applying updates	If the value of this field is non-zero, the update was not applied. The name of the update, which caused an error during its application, can be viewed in the task log (see Section "Viewing statistics and information about a Kaspersky Embedded Systems Security task in task logs" on page 205).

Objects isolating and backup copying

This section provides information about backing up of the detected malicious objects before they are disinfected or removed, and information about quarantining of the probably infected objects.

In this chapter

Isolating probably infected objects. Quarantine

This section describes how to isolate probably infected objects by quarantining them and how to configure Quarantine settings.

In this section

About quarantining of probably infected objects

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

Viewing Quarantine objects

Quarantined objects can be viewed in the **Quarantine** node of the Application Console.

► *To view quarantined objects, take the following steps:*

1. In the Application Console tree, expand the **Storages** node.
2. Select the **Quarantine** child node.

Information about quarantined objects is displayed in the details pane of the selected node.

► *To find the required object in the list of Quarantined objects,*

sort the objects (see Section "Sorting quarantined objects" on page 185) or filter the objects (see Section "Filtering quarantined objects" on page 185).

In this section

Sorting quarantined objects

By default, objects in the list of quarantined objects are sorted by date of quarantining in reverse chronological order. To find the desired object you may sort objects by columns with information about the objects. Sorted results will be saved if you close and then re-open the **Quarantine** node, or if you close the Application Console, save the msc file and then re-open it from this file.

► *To sort objects, take the following steps:*

1. In the Application Console tree, expand the **Storages** node.
2. Select the **Quarantine** child node.
3. In the details pane of the **Quarantine** node, select the column heading that you wish to use to sort objects in the list.

Objects in the list will be sorted based on the selected setting.

Filtering quarantined objects

To find the required quarantined object you can filter objects in the list - display only those objects that satisfy the filtering criteria (filters) that you specify. Filtered results are saved if you leave and then reopen the **Quarantine** node or if you close the Application Console, save the msc file and then reopen it from this file.

► *To specify one or multiple filters, take the following steps:*

1. In the Application Console tree, expand the **Storages** node.
2. Select the **Quarantine** child node.
3. Select **Filter** in the context menu of the node's name.

   The **Filter settings** window opens.

4. To add a filter, perform the following steps:

   a. In the **Field name**, select an item to which the filter value will be compared.

   b. In the **Operator** list, select the filtering condition. The values of the filtering conditions in the list may differ depending on the value you have selected in the **Field name** list.

   c. Enter the filter value in the **Field value** field or select it from the list.

   d. Click the **Add** button.

   The filter you have added will appear in the list of filters in the **Filter settings** window. Repeat steps a-d for each filter you add. Use the following guidelines while working with filters:

   - To combine multiple filters using the logical operator "AND", select **If all conditions are met**.
   - To combine multiple filters using the logical operator "OR", select **If any condition is met**.
   - In order to delete a filter, select the filter you wish to delete in the filter list, and click the **Remove** button.
   - In order to edit a filter, select the filter in the list in the **Filter settings** window. Then change the required values in the **Field name**, **Operator** or **Field value** fields and click the **Replace** button.

5. After all filters have been added, click the **Apply** button.

The created filters will be saved.

► *In order to re-display all objects in the list of quarantined objects,*

select **Remove** filter in the context menu of the **Quarantine** node.

Quarantine Scan

By default, after each database update, Kaspersky Embedded Systems Security performs the Quarantine Scan system task. Task settings are described in the table below. The Quarantine Scan task settings cannot be modified.

You can configure the task start schedule (see Section "Configuring the task start schedule settings" on page 149), start it manually, and modify the permissions of the account (see Section "Specifying a user account to start a task" on page 152) used to start the task.

Having scanned Quarantine objects after updating the databases, Kaspersky Embedded Systems Security can reclassify some of them as not infected: the status of such objects is changed to **False alarm**. Other objects can be reclassified as infected, in which case Kaspersky Embedded Systems Security handles such objects as specified by the Quarantine Scan task settings: disinfect, or delete if disinfection failed.

Table 33. Quarantine Scan task settings

Quarantine Scan task setting	Value
Scan scope	Quarantine folder
Security settings	Common for the entire scan area; their values are provided in the next table

Table 34. Scan settings in the Quarantine Scan task

Security setting	Value
Scan objects	All objects included into scan scope
Optimization	Disabled
Action to be performed with infected and other detected objects	Disinfect, delete if disinfection is impossible
Action to be performed on infected objects	Skip
Exclude objects	No
Do not detect	No
Stop scan if takes longer than (sec)	Not configured
Do not scan objects larger than (MB)	Not configured
Scan alternate NTFS streams	Enabled
Boot sectors of drives and MBR	Disabled
Using iChecker technology	Disabled
Using iSwift technology	Disabled
Scan compound objects	• Archives* • SFX archives* • Packed objects* • Embedded OLE objects* * Scan only new and modified files is disabled.
Checking files for Microsoft signatures	Not performed
Use heuristic analyzer	Enabled with **Deep** analysis level
Trusted zone	Not applied

Restoring quarantined objects

Kaspersky Embedded Systems Security places probably infected objects into the quarantine folder in encrypted form to shield the protected computer against their possible harmful effect.

You can restore any object from the quarantine. This may be required in the following cases:

- If after the quarantine scan using the updated database the status of the object changed to **False alarm** or **Disinfected**.
- If you consider the object harmless for the computer and wish to use it. If you do not want Kaspersky Embedded Systems Security to isolate this object during the subsequent scans you can exclude this object from the processing in the Real-Time File Protection task and in the On-Demand Scan tasks. To do this, specify the object as the value of the **Exclude files** (by filename) or **Do not detect** security setting in those tasks, or add it to the Trusted Zone (on page 443).

When you restore objects you can select where the object being restored will be saved to: original location (by default), special folder for restored objects on the protected computer or custom folder on computer where the Application Console is installed or on another computer in the network.

The **Restore to folder** option is used for storing restored objects on the protected computer. You can configure special security settings for it to be scanned. The path to this folder is set by the Quarantine settings.

Restoring objects from the quarantine may lead to computer infection.

You can restore the object and save its copy in the quarantine folder to use it later, for example in order to rescan the object after the database has been updated.

If a quarantined object was contained in a compound object (for example in an archive), Kaspersky Embedded Systems Security will not include into this compound object during the restoration, rather it will save separately into a selected folder.

You can restore one or several objects.

► *To restore quarantined objects, perform the following steps:*

1. In the Application Console tree, expand the **Storages** node.
2. Select the **Quarantine** child node.
3. Perform one of the following actions in the details pane of the **Quarantine** node:
   - To restore one object, select **Restore** from the context menu of the object that you want to restore.
   - To restore multiple objects select the objects you wish to restore using the **CTRL** or **SHIFT** key, right-click one of the selected objects and select **Restore** from the context menu.

   The **Restore object** window opens.
4. In the **Restore object** window, specify folder into which the object being restored will be saved for each of the selected object.

The name of the object is displayed in the **Object** field in the upper part of the window. If you selected several objects, the name of the first object in the list of selected objects will be displayed.

5. Perform one of the following steps:
   - To restore an object to its original location, select **Restore to the source folder**.
   - To restore an object to the folder specified as the location for restored objects in the settings, select **Restore to the default folder for restoration**.
   - To save an object to a different folder on computer where the Application Console is installed or to a shared folder, select **Restore to folder on your local computer or on network resource** and then select required folder or specify path to it.
6. If you wish to save a copy of the object in the Quarantine folder after this objects is restored, clear the **Remove objects from storage after they are restored** check box.
7. In order to apply the specified restoration conditions to the rest of the selected objects, check the **Apply to all selected objects** box.

   All selected objects are restored and saved in the specified location: if you selected **Restore to the source folder**, each of the objects will be saved into its original location if you selected **Restore to the default folder for restoration** or **Restore to folder on your local computer or on network resource -** all objects will then be saved into one specified folder.
8. Click **OK**.

   Kaspersky Embedded Systems Security will start restoring the first of the selected objects.
9. If an object with this name already exists in the specified location, the **Object with this name already exists** window opens.

   a. Select one of the following Kaspersky Embedded Systems Security actions:
      - **Replace**, in order to restore an object instead of the existing one.
      - **Rename**, to save the restored object under a different name. In the entry field enter a new object's filename and full path to it.
      - **Rename by adding suffix**, to rename the object by adding a suffix to its filename. Enter suffix in the entry field.

   b. If you have selected several objects to be restored, then in order to apply the selected action, such as **Replace** or **Rename**, by adding suffix to the rest of the selected objects, select the **Apply to all selected objects** check box. (If you have selected the **Rename** value, the **Apply to all selected objects** check box will be unavailable).

   c. Click **OK**.

   The object will be restored. Information about the restoration operation will be entered into the system audit log.

   If you did not select option **Apply to all selected objects** in the **Restore object** window, the **Restore object** window will open again. Using this window you can specify the location into which next selected object will be saved (see Step 4 of this procedure).

Moving objects to Quarantine

You can quarantine files manually.

► *To quarantine a file take the following steps:*

1. In the Application Console tree, open the context menu of the **Quarantine** node.
2. Select **Add**.
3. In the **Open** window, select the file on the disk that you wish to quarantine.
4. Click **OK**.

Kaspersky Embedded Systems Security will quarantine the selected file.

Deleting objects from Quarantine

According to the settings of the Quarantine Scan task, Kaspersky Embedded Systems Security automatically deletes objects from the Quarantine folder if their status has changed to *Infected* during the scan of Quarantine with the updated databases and if Kaspersky Embedded Systems Security has failed to disinfect them. Kaspersky Embedded Systems Security does not remove other objects from Quarantine.

One or multiple objects can be deleted from Quarantine.

► *To delete one or multiple objects from the Quarantine take the following steps:*

1. In the Application Console tree, expand the **Storages** node.
2. Select the **Quarantine** child node.
3. Perform one of the following steps:
   - To remove one object, select **Remove** in the context menu of the name of the object.
   - To delete multiple objects, select the objects that you want to delete using the **Ctrl** or **Shift** key, open the context menu on any one of the selected objects and select **Remove**.
4. In the confirmation window, click the **Yes** button to confirm operation.

The selected objects will be removed from quarantine.

Sending probably infected objects to Kaspersky Lab for analysis

If the behavior of a file gives you a reason to suspect that it contains a threat, and Kaspersky Embedded Systems Security considers this file to be clean, you may have encountered an unknown threat whose signature has not yet been added to the databases. You may send this file to Kaspersky Lab for analysis. Kaspersky Lab's Anti-Virus analysts will analyze it and, if they detect a new threat in it, will add a record identifying it in the databases. It is likely that when you rescan the object after the database has been updated Kaspersky Embedded Systems Security will find this object to be infected and will be able to disinfect it. You will not only be able to keep the object, but will prevent a virus outbreak.

Only quarantined files can be sent for analysis. Quarantined files are stored in encrypted form and are not deleted by the Anti-Virus application installed on the mail server during transfer.

Quarantined object cannot be sent for analysis to Kaspersky Lab after the license expires.

► *To send a file for analysis to Kaspersky Lab take the following steps:*

1. If the file was not quarantined, first move it into **Quarantine**.
2. In the **Quarantine** node, open the context menu on the file which you wish to send for analysis and select **Send object for analysis** in the context menu.
3. In the confirmation window that opens, click **Yes** if you are sure you want to send the selected object for analysis.
4. If a mail client is configured on the computer on which the Application Console is installed, a new email message is created. Review it and click the **Send** button.

   The **Receiver** field contains the Kaspersky Lab email address newvirus@kaspersky.com. The Subject field will contain the text "Quarantined object".

   The body of the message will contain the following text: "This file will be sent to Kaspersky Lab for analysis". Any additional information about the file, why you considered it probably infected or dangerous, how it behaves, or how it affects the system, can be included in the body of the message.

   Archive <object name>.cab will be attached to the message. This archive will contain file <uuid>.klq with the object in encrypted form, file <uuid>.txt with information about the object extracted by Kaspersky Embedded Systems Security, as well as the file Sysinfo.txt, which contains the following information about Kaspersky Embedded Systems Security and the operation system installed on the computer:

   - Name and version of the operating system.
   - Name and version of Kaspersky Embedded Systems Security.
   - Release date of the latest database update installed.
   - Active key.

   This information is required by Kaspersky Lab's anti-virus analysts in order analyze your file faster and more efficiently. If, however, you do not wish to transfer this information you can delete Sysinfo.txt file from the archive.

If a mail client is not installed on the computer with the Application Console, the application prompts you to save the selected encrypted object to file. This file can be sent to Kaspersky Lab manually.

► *To save an encrypted object to a file, take the following steps:*

1. In the window that opens with a prompt to save the object, click **OK**.
2. Select a folder on the drive of the protected computer or a network folder where the file containing the object will be saved.

The object will be saved to a CAB file.

Configuring Quarantine settings

You can configure quarantine settings. New Quarantine settings are applied immediately after saving.

► *To configure Quarantine settings take the following steps:*

1. In the Application Console tree, expand the **Storages** node.
2. Open the context menu of the **Quarantine** child node.
3. Select **Properties**.

4. In the **Quarantine Properties** window, configure the necessary quarantine settings in accordance with your requirements:
   - In the **Quarantine settings** section:
     - **Quarantine folder**

       Path to the Quarantine folder in UNC (Universal Naming Convention) format.

       The default path is C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Quarantine\.
     - **Maximum Quarantine size**

       This check box enables or disables the function that monitors the total size of objects stored in the Quarantine folder. If the specified value is exceeded (the default value being 200 MB), Kaspersky Embedded Systems Security logs the *Maximum Quarantine size exceeded* event and issues a notification according to the settings for notifications about events of this type.

       If the check box is selected, Kaspersky Embedded Systems Security monitors the total size of objects placed in Quarantine.

       If the check box is cleared, Kaspersky Embedded Systems Security does not monitor the total size of objects placed in Quarantine.

       The check box is cleared by default.
     - **Threshold value for space available**

     > If the size of objects in Quarantine exceeds the maximum quarantine size or exceeds the available space threshold, Kaspersky Embedded Systems Security will notify you about this while continuing to place objects in Quarantine.
   - In the **Restoration settings** section:
     - **Target folder for restoring objects**
5. Click **OK**.

The newly configured settings for Quarantine will be saved.

Quarantine statistics

You can view information about the number of quarantined objects - quarantine statistics.

► *In order to view quarantine statistics,*

in the context menu of the **Quarantine** node in the Application Console tree, select **Statistics**.

The **Statistics** window displays information about the number of objects currently stored in Quarantine (see the following table):

Field	Description
Probably infected objects	Number of objects found by Kaspersky Embedded Systems Security to be probably infected.
Used quarantine space	Total size of data in the quarantine folder.
False alarms	The number of objects that received *False alarm* status because they were classified as non-infected during the quarantine scan using updated databases.
Objects disinfected	The number of objects that received *Disinfected* status after the quarantine scan.
Total number of objects	Total number of objects in Quarantine.

Making backup copies of objects. Backup

This section provides information about backup of detected malicious objects before disinfection or deletion, as well as instructions for configuring Backup.

In this section

About backing up objects before disinfection or deletion

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

If the object is a part of a compound object (for example, part of an archive), Kaspersky Embedded Systems Security will save such a compound object in its entirety in Backup. For example, if Kaspersky Embedded Systems Security has detected that one of the objects from a mail database is infected, it will back up the entire mail database.

Large objects placed in Backup by Kaspersky Embedded Systems Security can slow down the system and reduce disk space on the hard drive.

Files can be restored from Backup either to their original folder or to a different folder on the protected computer or on another computer in the local area network. A file can be restored from Backup, for example, if an infected file contained important information, but during the disinfection of this file Kaspersky Embedded Systems Security was unable to maintain its integrity and therefore the information became unavailable.

Restoring files from Backup may lead to computer infection.

Viewing objects stored in Backup

Objects can be stored in the Backup folder only by using the Application Console in **Backup** node. They cannot be viewed using Microsoft Windows file managers.

► *In order to view the objects in Backup,*

1. In the Application Console tree, expand the **Storages** node.
2. Select the **Backup** child node.

Information about objects placed into Backup is displayed in the details pane of the selected node.

► *To find the necessary object in the list of objects in Backup,*

sort the objects or filter the objects.

In this section

Sorting files in Backup

By default, files in Backup are sorted by the date of saving in reverse chronological order. To find the required file, you can sort files according to the content of any column in the details pane.

Sorted results are saved if you leave and then reopen the **Backup** node or if you close the Application Console, save the msc file and then reopen it from this file.

► *To sort files in Backup, take the following steps:*

1. In the Application Console tree, expand the **Storages** node.
2. Select the **Backup** child node.
3. In the list of files in **Backup** select the column heading which you wish to use to sorting the objects.

Files in Backup will be sorted based on the selected criterion.

Filtering files in Backup

To find the required file in Backup you can filter files: display in the **Backup** node only those files which satisfy the filtering criteria you have specified (filters).

The sorting result will be saved if you leave and then re-open the **Backup** node or if you close the Application Console, save the msc file and then re-open it from this file.

► *To filter files in Backup, take the following steps:*

1. In the Application Console tree, open the context menu of the **Backup** node and select **Filter**.

   The **Filter settings** window opens.

2. To add a filter, perform the following steps:

   a. From the **Field name** list select the field against whose values the filter values will be compared during selection.

   b. In the **Operator** list select the filtering condition. The values of the filtering conditions in the list may differ depending on the value you have selected in the **Field name** field.

   c. Enter the filter value in the **Field value** field or select filter value.

   d. Click the **Add** button.

   The filter you have added will appear in the list of filters in the **Filter settings** window. Repeat these steps for each filter you add. The following guidelines can be used while working with the filters:

   - To combine multiple filters using the logical operator "AND", select **If all conditions are met**.
   - To combine multiple filters using the logical operator "OR", select **If any condition is met**.
   - In order to delete a filter, select the filter you wish to delete in the filter list, and click the **Remove** button.
   - To edit the filter, select it from the filter list in the **Filter settings** window, modify the required values in the **Field name**, **Operator** or **Field value** fields and click the **Replace** button.

   When all filters have been added, click the **Apply** button. Only files selected by the filters you have specified will then be displayed in the list.

► *In order to display all files included in the list of objects stored in Backup,*

select **Remove filter** in the context menu of the **Backup** node.

Restoring files from Backup

Kaspersky Embedded Systems Security stores files in the Backup folder in encrypted form in order to protect the protected computer against their possible harmful effect.

Any file can be restored from Backup.

A file may need to be restored in the following cases:

- If the original file, which appeared to be infected, had been containing important information and Kaspersky Embedded Systems Security failed to keep its integrity so, as a result, the information in the file became unavailable.
- If you consider the file harmless to the computer and wish to use it. If you do not wish Kaspersky Embedded Systems Security to consider this file infected or probably infected, during subsequent scans you can exclude it from processing in the Real-Time File Protection task and in the On-Demand Scan tasks. To do this, specify the file as the **Exclude files** setting or as the **Do not detect** setting in the corresponding tasks.

  Restoring files from Backup may lead to computer infection.

When you restore a file you can select where it will be saved: in the original location (by default), the special folder for restored objects on the protected computer, or a custom folder on the computer where the Application Console is installed or another computer in the network.

The **Restore to folder** is used for storing restored objects on the protected computer. You can configure special security settings for it to be scanned. The path to this folder is specified by Backup settings (see Section "Configuring Backup settings" on page 198).

By default when Kaspersky Embedded Systems Security is restoring a file it makes a copy of it in Backup. The file copy can be deleted from Backup after it is restored.

► *To restore files from Backup take the following steps:*

1. In the Application Console tree, expand the **Storages** node.
2. Select the **Backup** child node.
3. Perform one of the following actions in the details pane of the **Backup** node:
   - To restore one object, select **Restore** from the context menu of the object that you want to restore.
   - To restore multiple objects select the objects you wish to restore using the **CTRL** or **SHIFT** key, right-click one of the selected objects and select **Restore** from the context menu.

   The **Restore object** window opens.
4. In the **Restore object** window, specify folder into which the object being restored will be saved for each of the selected object.

> The name of the object is displayed in the **Object** field in the upper part of the window. If you selected several objects, the name of the first object in the list of selected objects will be displayed.

5. Perform one of the following steps:
   - To restore an object to its original location, select **Restore to the source folder**.
   - To restore an object to the folder specified as the location for restored objects in the settings, select **Restore to the default folder for restoration**.
   - To save an object to a different folder on computer where the Application Console is installed or to a shared folder, select **Restore to folder on your local computer or on network resource** and then select required folder or specify path to it.
6. If you do not want to save a copy of the file in the Backup folder after it is restored, select the **Remove objects from storage after they are restored** check box (by default, this check box is cleared).
7. In order to apply the specified restoration conditions to the rest of the selected objects, check the **Apply to all selected objects** box.

   All selected objects are restored and saved in the specified location: if you selected **Restore to the source folder**, each of the objects will be saved into its original location if you selected **Restore to the default folder for restoration** or **Restore to folder on your local computer or on network resource** - all objects will then be saved into one specified folder.
8. Click **OK**.

   Kaspersky Embedded Systems Security will start restoring the first of the selected objects.
9. If an object with this name already exists in the specified location, the **Object with this name already exists** window opens.

   a. Select one of the following Kaspersky Embedded Systems Security actions:
      - **Replace**, in order to restore an object instead of the existing one.
      - **Rename**, to save the restored object under a different name. In the entry field enter a new object's filename and full path to it.
      - **Rename by adding suffix**, to rename the object by adding a suffix to its filename. Enter suffix in the entry field.

   b. If you have selected several objects to be restored, then in order to apply the selected action, such as **Replace** or **Rename**, by adding suffix to the rest of the selected objects, select the **Apply to all selected objects** check box. (If you have selected the **Rename** value, the **Apply to all selected objects** check box will be unavailable).

   c. Click **OK**.

   The object will be restored. Information about the restoration operation will be entered into the system audit log.

If you did not select option **Apply to all selected objects** in the **Restore object** window, the **Restore object** window will open again. Using this window you can specify the location into which next selected object will be saved (see Step 4 of this procedure).

Deleting files from Backup

► *To delete one or multiple files from Backup, take the following steps:*

1. In the Application Console tree, expand the **Storages** node.
2. Select the **Backup** child node.
3. Perform one of the following steps:
   - To remove one object, select **Remove** in the context menu of the name of the object.
   - To delete multiple objects, select the objects that you want to delete using the **Ctrl** or **Shift** key, open the context menu on any one of the selected objects and select **Remove**.
4. In the confirmation window, click the **Yes** button to confirm operation.

The selected files will be deleted from Backup.

Configuring Backup settings

► *To configure Backup settings, take the following steps:*

1. In the Application Console tree, expand the **Storages** node.
2. Open the context menu of the **Backup** child node.
3. Select **Properties**.
4. In the **Backup Properties** window, configure the necessary Backup settings in accordance with your requirements:

   In the **Backup settings** section:

   - **Backup folder**

     Path to the Backup folder in UNC (Universal Naming Convention) format.

     The default path is C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Backup\.

   - **Maximum Backup size (MB)**

     This check box enables or disables the function that monitors the total size of objects stored in the Backup folder. If the specified value is exceeded (the default value being 200 MB), Kaspersky Embedded Systems Security logs the *Maximum Backup size exceeded* event and issues a notification according to the settings for notifications about events of this type.

     If the check box is selected, Kaspersky Embedded Systems Security monitors the total size of objects placed in Backup.

     If the check box is cleared, Kaspersky Embedded Systems Security does not monitor the total size of objects placed in Backup.

     The check box is cleared by default.

- **Threshold value for space available (MB)**

  The check box enables or disables the function that monitors the minimum amount of free space in Backup (the default value being 50 MB). If the amount of free space decreases below the specified threshold, Kaspersky Embedded Systems Security logs the *Backup free space threshold exceeded* event and issues a notification according to the settings for notifications about events of this type.

  If the check box is selected, Kaspersky Embedded Systems Security monitors the amount of free space in Backup.

  The Threshold value for space available (MB) check box is active if the Maximum Backup size (MB) check box is selected.

  The check box is selected by default.

> If the size of objects in Backup exceeds the maximum Backup size or exceeds the available space threshold, Kaspersky Embedded Systems Security will notify you about this while continuing to place objects in Backup.

In the **Restoration settings** section:

- **Target folder for restoring objects**

  Path to the folder for restoring objects, in UNC (Universal Naming Convention) format.

  Default path: C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Restored\.

5. Click **OK**.

The configured Backup settings will be saved.

Backup statistics

You can view information about the current status of Backup: Backup statistics.

► *To view Backup statistics,*

open the context menu on the **Backup** node in the Application Console tree and select **Statistics**. The **Backup statistics** window opens.

The **Backup statistics** window displays information about the current Backup status (see table below).

Table 35. Information about current Backup status

Field	Description
Current Backup size	Data size in the Backup folder; application calculates the file size in encrypted form
Total number of objects	Current total number of objects in Backup

Event registration. Kaspersky Embedded Systems Security logs

This section provides information about working with Kaspersky Embedded Systems Security logs: the system audit log, task execution logs, and the event log.

In this chapter

Ways to register Kaspersky Embedded Systems Security events

Events of Kaspersky Embedded Systems Security are divided into two groups:

- Events related to the processing of objects in Kaspersky Embedded Systems Security tasks.
- Events related to the administration of Kaspersky Embedded Systems Security, such as start of application, creation or deletion of tasks, or edition of task settings.

Kaspersky Embedded Systems Security uses the following methods of logging events:

- **Task logs**. A task log contains information about current task status and events that occurred during its execution.
- **System audit log**. The system audit log contains information about events that are related to the administration of Kaspersky Embedded Systems Security.
- **Event Log**. The Event Log contains information about events that are required for diagnostics of failures in the operation of Kaspersky Embedded Systems Security. The Event Log is available in Microsoft Windows Event Viewer.
- **Security log**. The Security log contains information about events that are associated with the security breaches or attempted security breaches on the protected computer.

If a problem occurs during Kaspersky Embedded Systems Security operation (for example, Kaspersky Embedded Systems Security or an individual task terminates abnormally or does not start), you can create a trace file and memory dump of Kaspersky Embedded Systems Security processes and send files with this information for analysis to Kaspersky Lab Technical Support in order to diagnose the problem encountered.

> Kaspersky Embedded Systems Security does not send any trace or dump files automatically. Diagnostics data can only be sent by the user with the corresponding permissions.

Kaspersky Embedded Systems Security writes information to trace files and the dump file in unencrypted form. The folder where files are saved is selected by the user and managed by the operating system configuration and Kaspersky Embedded Systems Security settings. You can configure access permissions (see Section "Managing access permissions for Kaspersky Embedded Systems Security functions" on page 225) and allow access to logs, trace and dump files only for required users.

System audit log

Kaspersky Embedded Systems Security performs the system audit of events related to the administration of Kaspersky Embedded Systems Security. The application logs information about, for example, start of the application, starts and stops of Kaspersky Embedded Systems Security tasks, changes in task settings, creation and deletion of On-Demand Scan tasks. Records of all those events are displayed in the details pane when you select the **System audit log** node in the Application Console.

By default Kaspersky Embedded Systems Security stores records in the System audit log for an unlimited period of time. You specify the storage period for records in the System audit log.

You can specify a folder which Kaspersky Embedded Systems Security will use to store files containing System audit log other than the default one.

In this section

Sorting events in the System audit log

By default, events in the system audit log node are displayed in reverse chronological order.

Events can be sorted by the contents of any column except the **Event** column.

► *To sort events in the System audit log:*

1. In the Application Console tree, expand the **Logs and notifications** node.
2. Select the **System audit log** child node.
3. In the details pane, select the header of the column that you want to use to sort the events in the list.

The sorted results will be saved until your next viewing session in the System audit log.

Filtering events in the System audit log

You can configure the System audit log to display only the records of events that meet the filtering conditions (filters) that you have specified.

► *To filter events in the System audit log, take the following steps:*

1. In the Application Console tree, expand the **Logs and notifications** node.
2. Open the context menu of the **System audit log** child node and select **Filter**.

   The **Filter settings** window opens.
3. To add a filter, perform the following steps:
   a. In the **Field name** list, select a column by which events will be filtered.
   b. In the **Operator** list select the filtering condition. Filtering conditions vary depending on the item selected in the **Field name** list.
   c. In the **Field value** list, select a value for the filter.
   d. Click the **Add** button.

      The filter you have added will appear in the list of filters in the **Filter settings** window.
4. If necessary, perform one of the following actions:
   - If you want to combine multiple filters using the logical operator "AND", select **If all conditions are met**.
   - If you want to combine multiple filters using the logical operator "OR", select **If any condition is met**.
5. Click the **Apply** button to save the filtering conditions in the system audit log.

   The list of events of the System audit log displays only events that meet the filtering conditions. The filtering results will be saved until your next viewing session in the System audit log.

► *To disable the filter:*

1. In the Application Console tree, expand the **Logs and notifications** node.
2. Open the context menu of the **System audit log** child node and select **Remove filter**.

   The list of events of the System audit log will then display all events.

Deleting events from the system audit log

By default Kaspersky Embedded Systems Security stores records in the system audit log for an unlimited period of time. You specify the storage period for records in the System audit log.

You can manually delete all events from System audit log.

► *To delete events from the System audit log:*

1. In the Application Console tree, expand the **Logs and notifications** node.
2. Open the context menu of the **System audit log** child node and select **Clear**.

3. Perform one of the following steps:
   - If you want to save the log contents as a file in CSV or TXT format before deleting events from the system audit log, click the **Yes** button in the deletion confirmation window. In the window that opens, specify the name and location of the file.
   - If you do not want to save the log contents as a file, click the **No** button in the deletion confirmation window.

The System audit log will be cleared.

Task logs

This section provides information about task logs of Kaspersky Embedded Systems Security and instructions on how to manage them.

In this section

About task logs

Information about the execution of Kaspersky Embedded Systems Security tasks is displayed in the details pane when you select the **Task logs** node in the Application Console.

In the log of each task, you can view the statistics of the task execution, details of each of the objects that have been processed by the application since the start of the task until the present moment, and the task settings.

By default, Kaspersky Embedded Systems Security stores records in task logs during 30 days since the task completion. You can change the storage period for records in task logs.

You can specify a folder that Kaspersky Embedded Systems Security will use to store files containing task logs other than the default one. You can also select events that Kaspersky Embedded Systems Security will record into task logs.

Viewing the list of events in task logs

► *To view the list of events in task logs:*

1. In the Application Console tree, expand the **Logs and notifications** node.
2. Select the **Task logs** subnode.

   The list of events saved in task logs of Kaspersky Embedded Systems Security will be displayed in the details pane.

Events can be sorted by any column or filtered.

Sorting events in task logs

By default, events in task logs are displayed in reverse chronological order. They can be sorted by any column.

► *To sort events in task logs:*

1. In the Application Console tree, expand the **Logs and notifications** node.
2. Select the **Task logs** subnode.
3. In the details pane, select the header of the column that you want to use to sort events in task logs of Kaspersky Embedded Systems Security.

   The sorted results will be saved until your next viewing session in the task logs.

Filtering events in task logs

You can configure the list of task logs to display only the records of events that meet the filtering conditions (filters) that you have specified.

► *To filter events in the task logs:*

1. In the Application Console tree, expand the **Logs and notifications** node.
2. Open the context menu of the **Task logs** child node and select **Filter**.

   The **Filter settings** window opens.
3. To add a filter, perform the following steps:
   a. In the **Field name** list, select a column by which events will be filtered.
   b. In the **Operator** list select the filtering condition. Filtering conditions vary depending on the item selected in the **Field name** list.
   c. In the **Field value** list, select a value for the filter.
   d. Click the **Add** button.

      The filter you have added will appear in the list of filters in the **Filter settings** window.

4. If necessary, perform one of the following actions:
   - If you want to combine multiple filters using the logical operator "AND", select **If all conditions are met**.
   - If you want to combine multiple filters using the logical operator "OR", select **If any condition is met**.
5. Click the **Apply** button to save the filtering conditions in the list of task logs.

The list of events of task logs displays only events that meet the filtering conditions. The filtered results will be saved until your next viewing session in the task logs.

► *To disable the filter:*

1. In the Application Console tree, expand the **Logs and notifications** node.
2. Open the context menu of the **Task logs** child node and select **Remove filter**.

The list of events of the task logs will then display all events.

Viewing statistics and information about a Kaspersky Embedded Systems Security task in task logs

In task logs, you can view detailed information about all events that have occurred in tasks since they had been started until the present moment, as well as task execution statistics and task settings.

► *To view statistics and information about a Kaspersky Embedded Systems Security task:*

1. In the Application Console tree, expand the **Logs and notifications** node.
2. Select the **Task logs** subnode.
3. In the results pane, open the **Logs** window using one of the following methods:
   - By double-clicking the event that has occurred in the task for which you want to view the log.
   - Open the context menu of the event that has occurred in the task for which you want to view the log, and select **View log**.
4. In the window that opens, the following details are displayed:
   - The **Statistics** tab displays the time of the task start and completion, as well as the task statistics.
   - The **Events** tab displays a list of events that have been logged during the task run.
   - The **Options** tab displays the task settings.
5. If necessary, click the **Filter** button to filter the events in the task log.
6. If necessary, click the **Export** button to export data from the task log into a file in CSV or TXT format.
7. Press the **Close** button.

The **Logs** window will be closed.

Exporting information from a task log

You can export data from a task log into a file in CSV or TXT format.

► *To export data from a task log:*

1. In the Application Console tree, expand the **Logs and notifications** node.
2. Select the **Task logs** subnode.
3. In the results pane, open the **Logs** window using one of the following methods:
   - By double-clicking the event that has occurred in the task for which you want to view the log.
   - Open the context menu of the event that has occurred in the task for which you want to view the log, and select **View log**.
4. In the lower part of the **Logs** window, click the **Export** button.

   The **Save as** window opens.
5. Specify the name, location, type, and encoding of the file into which you want to export data from the task log.
6. Click the **Save** button.

The specified settings are saved.

Deleting events from task logs

By default, Kaspersky Embedded Systems Security stores records in task logs during 30 days since the task completion. You can change the storage period for records in task logs.

You can manually delete all events from logs of tasks that have been already completed for the present moment.

Events from logs of tasks that are currently running and tasks being used by other users will not be deleted.

► *To delete the events from task logs:*

1. In the Application Console tree, expand the **Logs and notifications** node.
2. Select the **Task logs** subnode.
3. Perform one of the following steps:
   - If you want to delete the events from the logs of all tasks that have been already completed for the present moment, open the context menu of the **Task logs** child node and select **Clear**.
   - If you want to clear the log of an individual task, in the details pane, open the context menu of an event that has occurred in the task for which you want to clear the log, and select **Remove**.
   - If you want to clear the logs for several tasks:
     a. In the details pane, use the **Ctrl** or **Shift** keys to select events that have occurred in the tasks for which you want to clear the logs.
     b. Open the context menu of any selected event and select **Remove**.
4. Click the **Yes** button in the deletion confirmation window to confirm that you want to delete the logs.

The task logs that you have selected will be cleared. The deletion of events from the task logs will be registered with the system audit log.

Security log

Kaspersky Embedded Systems Security maintains a log of events associated with security breaches or attempted security breaches on the protected computer. The following events are recorded in this log:

- Exploit Prevention events.
- Critical Log Inspection events.
- Critical events that indicate an attempted security breach (for the Real-Time Computer Protection, On-Demand Scan, File Integrity Monitor, Applications Launch Control, and Device Control tasks).

You can clear the Security log as well as the System audit log (see Section "Deleting events from the system audit log" on page 202). Moreover, Kaspersky Embedded Systems Security records system audit events regarding clearing the Security log.

Viewing the event log of Kaspersky Embedded Systems Security in Event Viewer

You can view the event log of Kaspersky Embedded Systems Security using Microsoft Windows Event Viewer snap-in for Microsoft Management Console. The log contains events registered by Kaspersky Embedded Systems Security and required for diagnostics of failures in its operation.

Events that will be registered in the events log can be selected based on the following criteria:

- **by event types**
- **by level of detail**. The level of detail corresponds to the importance level of the events registered in the log (informational, important, or critical events). The most detailed is the Informational events level, which registers all events, and the least detailed is the Critical events level, which registers critical events only. By default, all components except for the Update component have the level of detail Important events selected (only important and critical events are logged); for the Update component the level Informational events is selected.

► *To view the Kaspersky Embedded Systems Security event log:*

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

   The window of Microsoft Management Console opens.

2. Select **File** > **Add or remove snap-in**.

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

3. In the list of available snap-ins, select the **Event Viewer snap-in** and click the **Add** button.

   The **Select computer** window opens.

4. In the **Select computer** window, specify the computer on which Kaspersky Embedded Systems Security is installed, and click **OK**.

5. In the **Add and remove snap-ins** window, click **OK**.

   In the Microsoft Management Console tree, the **Event Viewer** node appears.

6. Expand the **Event Viewer** node and select the **Applications and Services Logs** > **Kaspersky Embedded Systems Security** child node.

The Kaspersky Embedded Systems Security event log opens.

Configuring log settings in Kaspersky Embedded Systems Security Console

You can edit the following settings of logs of Kaspersky Embedded Systems Security:

- Length of the storage period for events in task logs and the system audit log.
- Location of the folder in which Kaspersky Embedded Systems Security stores files of task logs and the system audit log.
- Events generation thresholds for *Application database is out of date*, *Application database is extremely out of date* and *Critical Areas Scan has not been performed for a long time.*
- Events that Kaspersky Embedded Systems Security saves in task logs, the system audit log, and the event log of Kaspersky Embedded Systems Security in Event Viewer.
- Settings for publishing audit events and task performance events to the syslog server via the Syslog protocol.

► *To configure Kaspersky Embedded Systems Security logs, perform the following steps:*

1. In the Application Console tree, open the context menu of the **Logs and Notifications** node and select **Properties**.

   The **Logs and Notifications settings** window opens.

2. In the **Logs and notifications settings** window, configure the logs in accordance with your requirements. To do this, perform the following actions:

   - On the **General** tab, if necessary, select events that Kaspersky Embedded Systems Security will save in task logs, the system audit log, and the event log of Kaspersky Embedded Systems Security in Event Viewer. To do this, perform the following actions:

     - In the **Component** list, select the component of Kaspersky Embedded Systems Security for which you want to set the detail level.

       > For the Real-Time File Protection, On-Demand Scan, and Update components, registration of events via tasks logs and the event log is provided. For these components, the table of event list contains the **Task log** and **Windows Event Log** columns. Events for the Quarantine and Backup components are registered in the system audit log and the event log. For these components, the table of event list contains the **Audit** and **Windows Event Log** columns.

     - In the **Importance level** list, select a detail level for events in task logs, the system audit log, and the event log for the selected component.

       In the following table with a list of events, the check boxes are selected next to events that are registered with task logs, the system audit log, and the event log, according to the current detail level.

     - If you want to manually enable registration of specific events for a selected component, perform the following actions:

a. In the **Importance level** list, select **Custom**.

b. In the table with the list of events, select the check boxes next to events that you want to be registered in task logs, the system audit log, and the event log.

- On the **Advanced** tab, configure the log storage settings and event generation thresholds for computer protection status:
  - In the **Log storage** section:
    - **Logs folder**

      Path to the log folder in UNC (Universal Naming Convention) format.

      Default path: C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Reports\.

      If the default path is changed, a folder with corresponding name is created. The new logs will be stored in the new folder. The old logs will be preserved.

    - **Remove task logs older than (days)**

      The check box enables / disables a function that deletes logs with the results of execution of completed tasks and events published in logs of running tasks after the specified period of time (default value: 30 days).

      If the check box is selected, Kaspersky Embedded Systems Security deletes logs with the results of execution of completed tasks and events published in logs of running tasks after the specified period of time.

      The check box is selected by default.

    - **Remove from the system audit log events older than (days)**

      The check box enables / disables a function that deletes events recorded in the system audit log after the specified period of time (default value: 60 days).

      If the check box is selected, Kaspersky Embedded Systems Security deletes events recorded in the system audit log after the specified period of time.

      The check box is cleared by default.

  - In the **Event generation thresholds** section:
    - Specify the number of days after which the events *Application database is out of date*, *Application database is extremely out of date* and *Critical Areas Scan has not been performed for a long time* will occur.

Table 36. Event generation thresholds

Setting	Event generation thresholds.
Description	You can specify thresholds for generation of the following event types: *Application database is out of date* and *Application database is extremely out of date*. This event occurs if Kaspersky Embedded Systems Security database has not been updated during the period (in days) specified by the setting since the release date of the most recently installed database updates. You can configure administrator notifications about this event. *Critical Areas Scan has not been performed for a long time*. This event occurs if none of the tasks marked with the **Consider task as Critical Areas Scan** check box are performed during the specified number of days.
Possible values	Number of days from 1 to 365.
Default Value	Application databases are obsolete – 7 days. Application databases are extremely out of date – 14 days. Critical Areas Scan has not been performed for a long time – 30 days.

- On the **SIEM integration** tab, configure the settings for publishing audit events and task performance events to the syslog server (see Section "Configuring SIEM integration settings" on page 211).

3. Click **OK** to save the changes.

In this section

About SIEM integration

To reduce the load on low-performance devices and to reduce the risk of system degradation as a result of increased volumes of application logs, you can configure the publication of audit events and task performance events to the *syslog server* via the Syslog protocol.

A syslog server is an external server for aggregating events (SIEM). It collects and analyzes received events and also performs other actions for managing logs.

You can use SIEM integration in two modes:

- Duplicate events on the syslog server: this mode prescribes that all task performance events whose publication is configured in the settings of logs as well as all system audit events continue to be stored on the local computer even after they are sent to SIEM.

  It is recommended to use this mode to maximally reduce the load on the protected computer.

- Delete local copies of events: this mode prescribes that all events that are registered during application operation and published to SIEM will be deleted from the local computer.

The application never deletes local versions of the security log.

Kaspersky Embedded Systems Security can convert events in application logs into formats supported by the syslog server so that those events can be transmitted and successfully recognized by SIEM. The application supports conversion into structured data format and into JSON format.

It is recommended to select the format of events based on the configuration of the utilized SIEM.

Reliability settings

You can reduce the risk of unsuccessful relay of events to SIEM by defining the settings for connecting to the mirror syslog server.

A mirror syslog server is an additional syslog server to which the application switches automatically if the connection to the main syslog server is unavailable or if the main server cannot be used.

Kaspersky Embedded Systems Security also notifies you about unsuccessful attempts to connect to SIEM and about errors sending events to SIEM using system audit events.

Configuring SIEM integration settings

By default, SIEM integration is not used. You can enable and disable SIEM integration, and configure functionality settings (see the table below).

Table 37. SIEM integration settings

Setting	Default value	Description
Send events to a remote syslog server via syslog protocol	Not applied	You can enable or disable SIEM integration by selecting or clearing the check box, respectively.
Remove local copies for events that have been sent to a remote syslog server	Not applied	You can configure the settings for storing local copies of logs after they are sent to SIEM by selecting or clearing the check box.
Events format	Structured data	You can select one of two formats to which the application converts its events prior to sending them to the syslog server for better recognition of these events by SIEM.
Connection protocol	TCP	You can use the drop-down list to configure the connection to the main and mirror syslog servers via the UDP or TCP protocols.
Main syslog server connection settings	IP address: 127.0.0.1 Port: 514	You can use the appropriate fields to configure the IP address and port used to connect to the main syslog server. You can specify the IP address only in IPv4 format.
Use mirror syslog server if the main server is not accessible	Not applied	You can use the check box to enable or disable the use of a mirror syslog server.
Mirror syslog server connection settings	IP address: 127.0.0.1 Port: 514	You can use the appropriate fields to configure the IP address and port used to connect to the mirror syslog server. You can specify the IP address only in IPv4 format.

► *To configure SIEM integration settings:*

1. In the Application Console tree, open the context menu of the **Logs and Notifications** node.
2. Select **Properties**.

   The **Logs and notifications settings** window opens.
3. Select the **SIEM integration** tab.
4. In the **Integration settings** section, select the **Send events to a remote syslog server via syslog protocol** check box.

   The check box enables or disables the functionality for sending published events to an external syslog server.

   If the check box is selected, the application sends published events to SIEM according to the configured SIEM integration settings.

   If the check box is cleared, the application does not perform SIEM integration. You cannot configure SIEM integration settings if the check box is cleared.

The check box is cleared by default.

5. If necessary, in the **Integration settings** section, select the **Remove local copies for events that have been sent to a remote syslog server** check box.

   The check box enables or disables deletion of local copies of logs when they are sent to SIEM.

   If the check box is selected, the application deletes the local copies of events after they have been successfully published to SIEM. This mode is recommended on low-performance computers.

   If the check box is cleared, the application only sends events to SIEM. Copies of logs continue to be stored locally.

   The check box is cleared by default.

> The status of the **Remove local copies for events that have been sent to a remote syslog server** check box does not affect the settings for storing events of the security log: the application never automatically deletes security log events.

6. In the **Events format** section, specify the format to which you want to convert application operation events so that they can be sent to SIEM.

   By default, the application converts them into structured data format.

7. In the **Connection settings** section:

   - Specify the SIEM connection protocol.
   - Specify the settings for connecting to the main syslog server.

     You can specify an IP address in IPv4 format only.
   - Select the **Use mirror syslog server if the main server is not accessible** check box if you want the application to use other connection settings when unable to send events to the main syslog server.
     - Specify the following settings for connecting to the mirror syslog server: **IP address** and **Port**.

       The **IP address** and **Port** fields for the mirror syslog server cannot be edited if the **Use mirror syslog server if the main server is not accessible** check box is cleared.

       You can specify an IP address in IPv4 format only.

8. Click **OK**.

   The configured SIEM integration settings will be applied.

Notification settings

This section provides information about ways in which users and administrators of Kaspersky Embedded Systems Security can be notified about application events and the computer protection status, as well as instructions on how to configure notifications.

In this chapter

Administrator and user notification methods

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

The application ensures performance of the following tasks:

- The administrator can receive information about events of selected types.
- LAN users who access a protected computer and terminal computer users can receive information about events of the type *Object detected* in the Real-Time File Protection task.

In the Application Console, administrator or user notifications can be activated using several methods:

- User notification methods:

  a. Terminal service tools.

     You can apply this method for notifying terminal computer users if the protected computer is used as terminal.

  b. Message service tools.

     You can apply this method for notification via Microsoft Windows message services.

- Administrator notification methods:

  a. Message service tools.

     You can apply this method for notification via Microsoft Windows message services.

  b. Running an executable file.

     This method runs an executable file stored on the local drive of the protected computer, when the event occurs.

  c. Sending by email.

     This method uses email to transmit messages.

You can create a message text for individual event types. It can include an information field to describe an event. By default, the application uses a predefined text to notify users.

Configuring administrator and user notifications

Event notification settings give you a choice of methods for configuring and composing a message text.

► *To configure event notification settings, take the following steps:*

1. In the Application Console tree, open the context menu of the **Logs and notifications** node and select **Properties**.

   The **Logs and notifications settings** window opens.

2. On the **Notifications** tab select the notification mode:

   a. Select the event for which you wish to select a notification method from the **Event type** list.

   b. In the **Notify administrators** or **Notify users** group settings, select the check box next to the notification methods that you wish to configure.

   > You can configure user notifications for the **Object detected** event, **Untrusted mass storage detected and restricted** event, and **Host listed as untrusted** event only.

3. To add the text of a message:

   a. Click the **Message text** button.

   b. In the window that opens, enter text to be displayed in the corresponding event message.

   > You can create one message text for several event types: after you have selected a notification method for one event type, select the other event types for which you want to use the same message text by using the **Ctrl** or **Shift** key, and then click the **Message text** button.

   c. To add fields with information about an event, click the **Macro** button and select the relevant fields from the drop-down list. Fields with event information are described in the table in this section.

   d. To restore the default event message text, click the **By default** button.

4. To configure the selected methods of administrator notification of selected event, select the **Notifications** tab, click the **Settings** button in the **Notify administrators** section and configure the selected methods in the **Advanced settings** window. To do this, perform the following actions:

   a. For email notifications, open the **Email** tab and specify the email addresses of recipients (delimit addresses with semicolon), name or network address of SMTP server, and port number in the appropriate fields. If necessary, specify the text that will be displayed in the **Subject** and **From** fields. The text in the **Subject** field can also include variables with information about the event (see table below).

   If you want to apply user account authentication when connecting to the SMTP server, select **Use SMTP authentication** in the **Authentication settings** group and specify the name and password of the user whose user account will be authenticated.

   b. For notifications using **Windows Messenger Service** create a list of recipient computers for notifications on the **Windows Messenger Service** tab: for each computer that you wish to add, press the **Add** button and enter its network name in the input field.

c. To run an executable file, select the file on a local drive of the protected computer that will be executed on the computer triggered by the event or enter the full path to it on the **Executable file** tab. Enter the user name and password which will be used to execute the file.

   System environment variables can be used when the path to the executable file is specified; user environment variables are not allowed.

   If you wish to limit the number of messages for one event type over a period of time, on the **Advanced** tab select **Do not send the same notification more than** and specify the number of times and time unit.

5. Click **OK**.

The configured notification settings are saved.

Table 38. Fields with event information

Variable	Description
%EVENT_TYPE%	Event type.
%EVENT_TIME%	Event time.
%EVENT_SEVERITY%	Importance level.
%OBJECT%	Object name (in Real-Time Computer Protection and On-Demand Scan tasks). The Software Modules Update task includes the name of the update and the address of the web page with information on the update.
%VIRUS_NAME%	The name of the object according to the Virus Encyclopedia https://encyclopedia.kaspersky.com/knowledge/classification/ classification. This name is included in the full name of the detected object that Kaspersky Embedded Systems Security returns on detecting an object. You can view the full name of the detected object in the task log (see Section "Viewing statistics and information about a Kaspersky Embedded Systems Security task in task logs" on page 205).
%VIRUS_TYPE%	The type of detected object according to the Kaspersky Lab classification, such as "virus" or "trojan". It is included in the full name of the detected object, which is returned by Kaspersky Embedded Systems Security when it finds an object to be infected or probably infected. You can view the full name of the detected object in the task log.
%USER_COMPUTER%	In the Real-time File Protection task the computer name for the user who accessed the object on the computer.
%USER_NAME%	In the Real-Time File Protection task the name of the user who accessed the object on the computer.
%FROM_COMPUTER%	Name of the protected computer where the notification originated.
%EVENT_REASON%	Reason event occurred (some events do not have this field).
%ERROR_CODE%	Error code (used only for the "internal task error" event).
%TASK_NAME%	Task name (only for events related to task performance).

Starting and stopping Kaspersky Embedded Systems Security

This section contains information about starting Application Console, and also about starting and stopping Kaspersky Security Service.

In this chapter

Starting the Kaspersky Embedded Systems Security Administration Plug-in

No additional actions are required to start the Kaspersky Embedded Systems Security Administration Plug-in in Kaspersky Security Center. After the Plug-in is installed on the administrator's computer, it is started simultaneously with Kaspersky Security Center. Detailed information about starting Kaspersky Security Center can be found in the *Kaspersky Security Center Help*.

Starting the Kaspersky Embedded Systems Security Console from Start menu

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

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

1. In the **Start** menu, select **Programs** > **Kaspersky Embedded Systems Security** > **Administration Tools** > **Kaspersky Embedded Systems Security 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 Embedded Systems Security** > **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 computer, the Application Console window opens.

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

► *To connect to a protected computer:*

1. In the Application Console tree, open the context menu of the **Kaspersky Embedded Systems 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 computer in the entry field on the right.
5. Click **OK**.

The Application Console will be connected to a protected computer.

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 computer, select the **Connect as user** check box and specify a different user account that has such permissions.

Starting and stopping Kaspersky Security Service

By default, Kaspersky Security Service starts automatically immediately after the operating system. Kaspersky Security Service manages working processes in which Real-Time Computer Protection, Computer Control, On-Demand Scan and update tasks are executed.

By default when Kaspersky Embedded Systems Security is started, the Real-Time File Protection and Scan at Operating System Startup tasks are started, as well as other tasks that are scheduled to start **At application launch**.

If the Kaspersky Security Service is stopped, all running tasks are stopped. After you restart Kaspersky Security Service, the application automatically starts only those tasks whose schedule has the launch frequency set to **At application launch**, while the other tasks have to be started manually.

You can start and stop Kaspersky Security Service using the context menu of the **Kaspersky Embedded Systems Security** node or using the Microsoft Windows Services snap-in.

You can start and stop Kaspersky Embedded Systems Security if you are a member of the Administrators group on the protected computer.

► *To stop or start application using the Application Console take the following steps:*

1. In the Application Console tree, open the context menu of the **Kaspersky Embedded Systems Security** node.
2. Select one of the following items:
   - **Stop the service**.
   - **Start the service**.

The Kaspersky Security Service will be started or stopped.

Starting the Kaspersky Embedded Systems Security components in the operating system safe mode

This section provides information about Kaspersky Embedded Systems Security working in the operating system safe mode.

In this chapter

About Kaspersky Embedded Systems Security working in the operating system safe mode

Kaspersky Embedded Systems Security components can be started upon loading of the operating system in safe mode. Besides Kaspersky Security Service (kavfs.exe), klam.sys driver is loaded, which is used for registering Kaspersky Security service as a protected service during the start of the operating system. For more details, see section Registering the Kaspersky Security Service as a protected service.

Kaspersky Embedded Systems Security can be started in the following safe modes of the operating system:

- Safe Mode Minimal – this mode is started when the standard option of the operating system safe mode is selected. At that, Kaspersky Embedded Systems Security can start the following components:
  - Real-Time File Protection.
  - On-Demand Scan.
  - Applications Launch Control and Rule Generator for Applications Launch Control.
  - Log Inspection.
  - File Integrity Monitor.
  - Application Integrity Control.
- Safe Mode Network – this mode is started when the operating system is loaded in safe mode with network drivers. Besides the components starting in Safe Mode Minimal, Kaspersky Embedded Systems Security can start the following components:
  - Databases Update.
  - Software Modules Update.

Starting Kaspersky Embedded Systems Security in safe mode

By default, Kaspersky Embedded Systems Security is not started upon loading of the operating system in safe mode.

► *To make Kaspersky Embedded Systems Security start in the operating system safe mode, perform the following actions:*

1. Start Windows registry editor (C:\Windows\regedit.exe).
2. Open the [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam\Parameters] key of the system registry.
3. Open LoadInSafeMode parameter.
4. Set value `1`.
5. Click **OK**.

► *To cancel start of Kaspersky Embedded Systems Security in the operating system safe mode, perform the following actions:*

1. Start Windows registry editor (C:\Windows\regedit.exe).
2. Open the [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam\Parameters] key of the system registry.
3. Open LoadInSafeMode parameter.
4. Set value `0`.
5. Click **OK**.

Kaspersky Embedded Systems Security self-defense

This section provides information about Kaspersky Embedded Systems Security self-defense mechanisms.

In this chapter

About Kaspersky Embedded Systems Security self-defense

Kaspersky Embedded Systems Security comprises self-defense mechanisms that protect the application against modification or deletion of its folders on the hard drive, memory processes, and system registry entries.

Protection from changes of folders with installed Kaspersky Embedded Systems Security components

Kaspersky Embedded Systems Security restricts renaming and deletion of folders with the installed application components for any user account. By default, the paths to the application installation folders are as follows:

- On the 32-bit version of Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security\
- On the 64-bit version of Microsoft Windows: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security\

Protection from changes of Kaspersky Embedded Systems Security registry keys

Kaspersky Embedded Systems Security restricts rights of access to the following registry branches and keys, which provide loading of the application drivers and services:

- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfs]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsgt]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsslp]

- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klelaml]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klflltdev]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klramdisk]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.3\CrashDump]
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.3\CrashDump] (on the 64-bit version of Microsoft Windows)
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.3\Trace]
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.3\Trace] (on the 64-bit version of Microsoft Windows)

The rights to change these registry branches and keys are granted to Local System (SYSTEM) account only. User and Administrator accounts are granted with read-only rights.

Registering the Kaspersky Security Service as a protected service

Protected Process Light (also referred to as "PPL") technology ensures that the operating system only loads trusted services and processes. For a service to run as a protected service, an *Early Launch Antimalware* driver must be installed on the protected computer.

An *Early Launch Antimalware* (also referred to as "ELAM") driver provides protection for the computers in your network when they start and before third-party drivers are initialized.

The ELAM driver is automatically installed during the Kaspersky Embedded Systems Security installation and is used for registering the Kaspersky Security Service as PPL when the operating system starts. When the Kaspersky Security Service (KAVFS) is started as a system protected process, other non-protected processes on the system are not able to inject threads, write into the virtual memory of the protected process, or stop the service.

When a process is started as PPL, it cannot be managed by user disregarding the assigned user permissions. The Kaspersky Security Service registration as PPL using the ELAM driver is supported on the Microsoft Windows 10 and higher operating systems. If you install Kaspersky Embedded Systems Security on a server running PPL-supporting operating system, the permission management for Kaspersky Security Service (KAVFS) will not be available.

► *To install Kaspersky Embedded Systems Security as PPL, run the following command:*

```
msiexec /i ess_x64.msi NOPPL=0 EULA=1 PRIVACYPOLICY=1 /qn
```

Managing access permissions for Kaspersky Embedded Systems Security functions

This section contains information about permissions to manage Kaspersky Embedded Systems Security and Windows services registered by the application, and instructions on how to configure these permissions.

In this chapter

About permissions to manage Kaspersky Embedded Systems Security

By default, access to all Kaspersky Embedded Systems Security functions is granted to users of the Administrators group on the protected computer, users of the ESS Administrators group created on the protected computer during installation of Kaspersky Embedded Systems Security, and the SYSTEM group.

Users who have access to the **Edit** permissions function of Kaspersky Embedded Systems Security can grant access to Kaspersky Embedded Systems Security functions to other users registered on the protected computer or included in the domain.

Users who are not registered in the list of Kaspersky Embedded Systems Security users cannot open the Application Console.

You can choose one of the following preset access levels for a user or group of users:

- **Full control** – access to all application functions: the ability to view and edit Kaspersky Embedded Systems Security general settings, component settings,and Kaspersky Embedded Systems Security user permissions; and the ability to view Kaspersky Embedded Systems Security statistics.
- **Edit** – access to all application functions except editing of user permissions: the ability to view and edit Kaspersky Embedded Systems Security general settings and Kaspersky Embedded Systems Security component settings.
- **Read** – the ability to view Kaspersky Embedded Systems Security general settings, Kaspersky Embedded Systems Security component settings, Kaspersky Embedded Systems Security statistics, and Kaspersky Embedded Systems Security user permissions.

You can also configure advanced access permissions: allow or block access to specific functions of Kaspersky Embedded Systems Security.

If you have manually configured access permissions for a user or group, then the **Special permissions** access level is set for this user or group.

Table 39. About access permissions for Kaspersky Embedded Systems Security functions

User rights	Description
Task management	Ability to start / stop / pause / resume Kaspersky Embedded Systems Security tasks.
Create and delete On-Demand Scan tasks	Ability to create and delete On-Demand Scan tasks.
Edit settings	Ability to: • Import Kaspersky Embedded Systems Security settings from a configuration file. • Edit the application settings.
Read settings	Ability to: • View Kaspersky Embedded Systems Security general settings and task settings. • Export Kaspersky Embedded Systems Security settings to a configuration file. • View settings for task logs, system audit log, and notifications.
Manage repositories	Ability to: • Move objects to Quarantine. • Remove objects from Quarantine and Backup. • Restore objects from Quarantine and Backup.
Manage logs	Ability to delete task logs and clear the system audit log.
Read logs	Ability to view Anti-Virus events in task logs and the system audit log.
Read statistics	Ability to view statistics for each Kaspersky Embedded Systems Security task.
Application licensing	Ability to activate Kaspersky Embedded Systems Security.
Uninstalling the application	Ability to uninstall Kaspersky Embedded Systems Security.
Read permissions	Ability to view the list of Kaspersky Embedded Systems Security users and user access privileges.
Edit permissions	Ability to: • Edit the list of users with access to application management. • Edit user access permissions for Kaspersky Embedded Systems Security functions.

About permissions to manage registered services

During installation, Kaspersky Embedded Systems Security registers in Windows the Kaspersky Security Service (KAVFS), the Kaspersky Security Management Service (KAVFSGT) and Kaspersky Security Exploit Prevention (KAVFSSLP).

The Kaspersky Security Service registration as a Protected Process Light using the ELAM driver is supported on the Microsoft Windows 10 and higher operating systems. When a process is started as PPL, it cannot be managed by user disregarding the assigned user permissions. If you install Kaspersky Embedded Systems Security on a computer running PPL-supporting operating system, the permission management for Kaspersky Security Service (KAVFS) will not be available.

Kaspersky Security Service

By default, access permissions for managing the Kaspersky Security Service are granted to users in the Administrators group on the protected computer, as well as to the SERVICE and INTERACTIVE groups with read permissions and to the SYSTEM group with read and execute permissions.

Users who have access to functions of the Edit permissions level (see Section "Password-protected access to Kaspersky Embedded Systems Security functions" on page 233) can grant access permissions for managing Kaspersky Security Service to other users registered on the protected computer or included in the domain.

Kaspersky Security Management Service

To manage the application via the Application Console installed on a different computer, the account whose permissions are used to connect to Kaspersky Embedded Systems Security must have full access to Kaspersky Security Management Service on the protected computer.

By default, access to the Kaspersky Security Management Service is granted to users of the Administrators group on the protected computer and users of the ESS Administrators group created on the protected computer during Kaspersky Embedded Systems Security installation.

You can only manage the Kaspersky Security Management Service via the Microsoft Windows Services snap-in.

Kaspersky Security Exploit Prevention

By default, access permissions for managing the Kaspersky Security Exploit Prevention service are granted to users in the Administrators group on the protected computer, as well as to the SYSTEM group with read and execute permissions.

About permissions to manage the Kaspersky Security Service

During installation, Kaspersky Embedded Systems Security registers the Kaspersky Security Service (KAVFS) in Windows, and internally enables the functional components that are started at operating system startup. To reduce the risk of third-party access to application functions and security settings on a protected computer through management of the Kaspersky Security Service, you can restrict permissions for managing the Kaspersky Security Service from the Application Console or the Administration Plug-in.

By default, access permissions for managing the Kaspersky Security Service are granted to users in the Administrators group on the protected computer. Read permissions are granted to the SERVICE and INTERACTIVE groups, and read and execute permissions are granted to the SYSTEM group.

You cannot delete the SYSTEM user account or edit permissions for this account. If the permissions for the SYSTEM account are edited, the maximum privileges are restored for this account when you save the changes.

Users who have access to functions (see Section "About permissions to manage Kaspersky Embedded Systems Security" on page 225) that require Edit permissions can grant access permissions for managing the Kaspersky Security Service to other users registered on the protected computer or included in the domain.

You can choose one of the following preset permission levels for a user or group of users of Kaspersky Embedded Systems Security to manage the Kaspersky Security Service:

- **Full control**: ability to view and edit general settings and user permissions for the Kaspersky Security Service, and to start and stop the Kaspersky Security Service.
- **Read**: ability to view Kaspersky Security Service general settings and user permissions.
- **Modification**: ability to view and edit Kaspersky Security Service general settings and user permissions.
- **Execution**: ability to start and stop the Kaspersky Security Service.

You can also configure advanced access permissions: allow or deny access to specific Kaspersky Embedded Systems Security functions (see the table below).

If you have manually configured access permissions for a user or group, then the **Special permissions** access level is set for this user or group.

Table 40. Access permissions for Kaspersky Security Service functions

Feature	Description
View service configurations	Ability to view Kaspersky Security Service general settings and user permissions.
Request service status from Service Control Manager	Ability to request the execution status of the Kaspersky Security Service from Microsoft Windows Service Control Manager.
Request status from service	Ability to request the service execution status from the Kaspersky Security Service.
Read list of dependent services	Ability to view a list of services that the Kaspersky Security Service depends on and which depend on the Kaspersky Security Service.
Editing service settings	Ability to view and edit Kaspersky Security Service general settings and user permissions.
Start the service	Ability to start the Kaspersky Security Service.
Stop the service	Ability to stop the Kaspersky Security Service.
Pause / Resume the service	Ability to pause and resume the Kaspersky Security Service.
Read permissions	Ability to view the list of Kaspersky Security Service users and each user's access privileges.
Edit permissions	Ability to: • Add and remove Kaspersky Security Service users. • Edit user access permissions for the Kaspersky Security Service.
Delete the service	Ability to unregister the Kaspersky Security Service in the Microsoft Windows Service Control Manager.
User defined requests to service	Ability to create and send user requests to the Kaspersky Security Service.

About access permissions for the Kaspersky Security Management Service

You can review the list of Kaspersky Embedded Systems Security services.

During installation, Kaspersky Embedded Systems Security registers the Kaspersky Security Management Service (KAVFSGT). To manage the application via the Application Console installed on a different computer, the account used to connect to Kaspersky Embedded Systems Security must have full access to the Kaspersky Security Management Service on the protected computer.

By default, access to the Kaspersky Security Management Service is granted to users of the Administrators group on the protected computer and users of the ESS Administrators group created on the protected computer during installation of Kaspersky Embedded Systems Security.

You can manage the Kaspersky Security Management Service only via the Microsoft Windows Services snap-in.

You cannot allow or block user access to the Kaspersky Security Management Service by configuring Kaspersky Embedded Systems Security.

You can connect to Kaspersky Embedded Systems Security from a local account if an account with the same user name and password is registered on the protected computer.

Configuring access permissions for managing Kaspersky Embedded Systems Security and Kaspersky Security Service

You can edit the list of users and user groups allowed to access Kaspersky Embedded Systems Security functions and manage the Kaspersky Security Service. You can also edit the access permissions of those users and user groups.

► *To add or remove a user or group from the list:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.
3. Perform one of the following actions in the details pane of the selected administration group:
    - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring a policy" on page 112).
    - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in the Application settings window of the Kaspersky Security Center" on page 117).

    > If an active Kaspersky Security Center policy is applied to a device, and this policy blocks changes to application settings, then these settings cannot be edited in the **Application settings** window.

4. In the **Supplementary** section, perform one of the following steps:
    - Click **Settings** in the **User access permissions for application management** subsection if you want to edit the list of users who have access permissions for managing Kaspersky Embedded Systems Security functions.
    - Click **Settings** in the **User access permissions for Kaspersky Security Service management** subsection if you want to edit the list of users who have access permissions for managing the Kaspersky Security Service.

      The **Permissions for Kaspersky Embedded Systems Security** group window opens.
5. In the window that opens, perform the following operations:
    - In order to add a user or group to the list, click the **Add** button and select the user or group that you want to grant privileges to.
    - To remove a user or group from the list, select the user or group whose access you want to restrict, and click the **Remove** button.
6. Click the **Apply** button.

The selected users (groups) are added or removed.

► *To edit the permissions of a user or group to manage Kaspersky Embedded Systems Security or the Kaspersky Security Service:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.
3. Perform one of the following actions in the details pane of the selected administration group:

- To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring a policy" on page 112).
- To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in the Application settings window of the Kaspersky Security Center" on page 117).

> If an active Kaspersky Security Center policy is applied to a device, and this policy blocks changes to application settings, then these settings cannot be edited in the **Application settings** window.

4. In the **Supplementary** section, perform one of the following steps:
   - Click **Settings** in the **Modify user rights of application management** subsection if you want to edit the list of users who have access permissions for managing Kaspersky Embedded Systems Security functions.
   - Click **Settings** in the **Modify user rights of Kaspersky Security Service management** subsection if you want to edit the list of users who have access permissions for managing the application via the Kaspersky Security Service.

     The **Permissions for Kaspersky Embedded Systems Security** group window opens.
5. In the window that opens, in the **Group or user names** list, select the user or group of users whose permissions you want to change.
6. In the **Permissions for <User (Group)>** section, select the **Allow** or **Deny** check boxes for the following access levels:
   - **Full control**: full set of permissions to manage Kaspersky Embedded Systems Security or the Kaspersky Security Service.
   - **Read**:
     - The following permissions to manage Kaspersky Embedded Systems Security: **Retrieve statistics**, **Read settings**, **Read logs** and **Read permissions**.
     - The following permissions to manage the Kaspersky Security Service: **Read service settings**, **Request service status from Service Control Manager**, **Request status from service**, **Read list of dependent services**, **Read permissions**.
   - **Modification**:
     - All permissions to manage Kaspersky Embedded Systems Security, except **Edit permissions**.
     - The following permissions to manage Kaspersky Security Service: **Modify service settings**, **Read permissions**.
   - **Special permissions**: the following permissions to manage the Kaspersky Security Service: **Start service**, **Stop service**, **Pause / Resume service**, **Read permissions**, **User defined requests to service**.
7. To configure advanced permissions for a user or group (**Special permissions**), click the **Advanced** button.

   a. In the **Advanced security settings for Kaspersky Embedded Systems Security** window that opens, select the desired user or group.

   b. Click the **Edit** button.

   c. In the drop-down list in the top part of the window, select the type of access control (**Allow** or **Block**).

d. Select the check boxes next to the functions that you want to allow or block for the selected user or group.

e. Click **OK**.

f. In the **Advanced security settings for Kaspersky Embedded Systems Security** window, click **OK**.

8. In the **Permissions for Kaspersky Embedded Systems Security** group window, click the **Apply** button.
9. The configured permissions for managing Kaspersky Embedded Systems Security or the Kaspersky Security Service are saved.

Password-protected access to Kaspersky Embedded Systems Security functions

You can restrict access to application management and registered services by configuring user permissions (see Section "Managing access permissions for Kaspersky Embedded Systems Security functions" on page 225). You can also set password protection in the Kaspersky Embedded Systems Security settings for additional protection. Password protection allows you to additionally limit access to the Application Console management and execution of the command line commands. If the password protection is applied, Kaspersky Embedded Systems Security requires all users to enter the password when starting the Application Console or executing command line commands.

► *To protect access to Kaspersky Embedded Systems Security functions:*

1. In the Application Console tree, select the **Kaspersky Embedded Systems Security** node and do one of the following:
   - Click the **Application properties** link in the details pane of the node.
   - Select **Properties** in the node's context menu.

   The **Application settings** window opens.
2. On the **Security and reliability** tab in the **Password protection settings** click the **Apply password protection** check box.

   The **Password** and **Confirm password** fields become active.
3. In the **Password** field, enter the value you want to use to protect access to Kaspersky Embedded Systems Security functions.
4. In the **Confirm password** field, enter your password again.
5. Click **OK**.

This password cannot be recovered. Losing your password results in complete loss of control of the application. Additionally, it will be impossible to uninstall the application from the protected computer.

You can reset the password at any time. To do that, clear the **Apply password protection** check box and save changes. Password protection will be disabled and old password checksum removed. Repeat the password entering process with a new password.

Configuring access permissions in Kaspersky Security Center

You can configure access permissions for managing the application and Kaspersky Security Service in Kaspersky Security Center for a group of computers or for a separate computer.

► *To access permissions for managing the application and Kaspersky Security Service:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.
3. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring a policy" on page 112).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in the Application settings window of the Kaspersky Security Center" on page 117).

   > If an active Kaspersky Security Center policy is applied to a device, and this policy blocks changes to application settings, then these settings cannot be edited in the **Application settings** window.

4. Open the **Supplementary** section and do the following:
   - To configure access permissions for managing Kaspersky Embedded Systems Security for a user or group of users, in the **User access permissions for application management** section click the **Settings** button.
   - To configure access permissions for managing Kaspersky Security Service for a user or group of users, in the **User access permissions for Security Service management** section click the **Settings** button.
5. In the window that opens, configure the access privileges (see Section "Managing access permissions for Kaspersky Embedded Systems Security functions" on page 225) according to your needs.

The specified settings are saved.

Real-Time File Protection

This section contains information about the Real-Time File Protection task and how to configure it.

In this chapter

About Real-Time File Protection task

When the Real-Time File Protection task is running, Kaspersky Embedded Systems Security scans the following protected computer objects when they are accessed:

- Files.
- Alternate file system streams (NTFS streams).
- Master boot records and boot sectors on the local hard drives and external devices.

When any application writes a file to a computer or reads a file from it, Kaspersky Embedded Systems Security intercepts this file, scans it for threats, and, if a threat is detected, performs a default action or an action you have specified: tries to disinfect it, moves it to Quarantine, or deletes it if disinfection is impossible. Before disinfection or deletion, Kaspersky Embedded Systems Security saves an encrypted copy of the source file to the Backup folder. Kaspersky Embedded Systems Security restores the file from Quarantine in the original folder if it has been successfully disinfected.

Kaspersky Embedded Systems Security also detects malware for processes running under Windows Subsystem for Linux®. For such processes, the Real-Time File Protection task applies action defined by the current configuration.

About the task protection scope and security settings

By default, the Real-Time File Protection task protects all objects of the computer file system. If there is no security requirement to protect all objects of the file system or you want to exclude any objects from the task scope, you can limit the protection scope.

In the Application Console, the protection scope is displayed as a tree or in the list of the computer file resources that Kaspersky Embedded Systems Security can control. By default, the network file resources of the protected computer are displayed in a list-view mode.

In the Administration Plug-in only the list view is available.

► *To display network file resources in the tree-view mode in the Application Console,*

open the drop down list in the **Protection scope settings** window upper left sector and select **Tree-view**.

The items or nodes are displayed in a list-view or in a tree-view mode of the computer file resources as follows:

☑ The node is included in the protection scope.

□ The node is excluded from the protection scope.

▣ At least one of the child nodes of this node is excluded from the protection scope, or the security settings of the child node(s) differ(s) from the setting of a parental node (for a tree-view mode only).

The ▣ icon is displayed if all child nodes are selected, but the parent node is not selected. In this case, changes in the composition of files and folders of the parent node are disregarded automatically when the protection scope for the selected child node is being created.

Using the Application Console, you can also add virtual drives (see Section "Creating virtual protection scope" on page 265) to the protection scope. The names of the virtual nodes are displayed in blue font.

Security settings

The task security settings can be configured as common settings for all nodes or items included in the protection scope, or as different settings for each node or item in the computer file resource tree or list.

Security settings configured for the selected parent node are automatically applied to all its child nodes. The security settings of the parent node are not applied to child nodes that are configured separately.

The settings for a selected protection scope can be configured using one of the following methods:

- Selecting one of three predefined security levels (on page 238).
- Configuring the security settings manually (see Section "Configuring security settings manually" on page 251) for the selected nodes or items in the file resources tree or list (the security level changes to **Custom**).

A set of settings for a node or item can be saved in a template in order to be applied later to other nodes or items.

About virtual protection scope

Kaspersky Embedded Systems Security can scan not only existing folders and files on hard and removable drives, but also drives that are dynamically created on the computer by various applications and services.

If all computer objects are included in the protection scope, these dynamic nodes will automatically be included in the protection scope. However, if you want to specify special values for the security settings of these dynamic nodes or if you have selected not the entire computer for protection, but discrete areas of it, then in order to include dynamic drives, files or folders in the protection scope, you will first have to create them in the Application Console: that is, specify the virtual protection scope. The drives, files and folders created will exist only in the Application Console, but not in the file structure of the protected computer.

If, while creating a protection scope, all subfolders or files are selected without the parent folder being selected, then all dynamic folders or files which will appear in it will not automatically be included in the protected scope. "Virtual copies" of these should be created in the Application Console and added to the protection scope.

Predefined protection scopes

The file resources tree or list displays the nodes to which you have read-access based on the configured security settings of Microsoft Windows.

Kaspersky Embedded Systems Security covers the following predefined protection scopes:

- **Local hard drives**. Kaspersky Embedded Systems Security protects files on the computer hard drives.
- **Removable drives**. Kaspersky Embedded Systems Security protects files on external devices, such as CDs or USB drives. All removable disks, individual disks, folders or files can be included in or excluded from the protection scope.
- **Network**. Kaspersky Embedded Systems Security protects files that are written to network folders or read from them by applications running on the computer. Kaspersky Embedded Systems Security does not protect files when such files are accessed by applications from other computers.
- **Virtual drives**. Dynamic folders and files and drives that are temporarily connected to the computer can be included in the protection scope, for example, common cluster drives.

By default, you can view and configure predefined protection scopes in the scope list; you can also add predefined scopes to the list during its formation in the protection scope settings.

By default, the protection scope includes all predefined areas except virtual drives.

Virtual drives created using a SUBST command are not displayed in the computer file resource tree in the Application Console. To include objects on the virtual drive in the protection scope, include the computer folder with which this virtual drive is associated in the protection scope.

Connected network drives will also not be displayed in the computer file resources list. To include objects on network drives in the protection scope, specify the path to the folder which corresponds to this network drive in UNC format.

Predefined security levels

One of the following predefined security levels for the nodes selected either in the computer file resources tree or file resources list can be applied: **Maximum performance**, **Recommended**, and **Maximum protection**. Each of these levels contains its own predefined set of security settings (see the table below).

Maximum performance

The **Maximum performance** security level is recommended if, beyond using Kaspersky Embedded Systems Security on computers, there are additional computer security measures inside your network, for example, firewalls and existing security policies.

Recommended

The **Recommended** security level ensures an optimum combination of protection and performance impact on protected computers. This level is recommended by Kaspersky Lab experts as sufficient to protect computers on most corporate networks. The **Recommended** security level is set by default.

Maximum protection

The **Maximum protection** security level is recommended if your organization’s network has elevated computer security requirements.

Table 41. Preset security levels and corresponding setting values

Options	Security level		
	Maximum performance	Recommended	Maximum protection
Objects protection	By extension	By format	By format
Protect only new and modified files	Enabled	Enabled	Disabled
Action to perform on infected and other objects	Block access and disinfect. Remove if disinfection fails	Block access and perform recommended action	Block access and disinfect. Remove if disinfection fails
Action to perform on probably infected objects	Block access and quarantine	Block access and perform recommended action	Block access and quarantine
Exclude files	No	No	No
Do not detect	No	No	No
Stop scanning if it takes longer than (sec.)	60 sec.	60 sec.	60 sec.
Do not scan compound objects larger than (MB)	8 MB	8 MB	Not set
Scan alternate NTFS streams	Yes	Yes	Yes
Scan disk boot sectors and MBR	Yes	Yes	Yes
Compound objects protection	• Packed objects* *New and modified objects only	• SFX archives* • Packed objects* • Embedded OLE objects* *New and modified objects only	• SFX archives* • Packed objects* • Embedded OLE objects* *All objects
Entirely remove compound file that cannot be modified by the application in case of embedded object detect	No	No	Yes

The **Objects protection**, **Use iChecker technology**, **Use iSwift technology**, and **Use heuristic analyzer** settings are not included in the settings of the predefined security levels. If you edit the **Objects protection**, **Use iChecker technology**, **Use iSwift technology**, or **Use heuristic analyzer** security settings after selecting one of the predefined security levels, the security level that you have selected will not change.

File extensions scanned by default in Real-Time File Protection task

Kaspersky Embedded Systems Security scans files with the following extensions by default:

- *386;*
- *acm;*
- *ade, adp;*
- *asp;*
- *asx;*
- *ax;*
- *bas;*
- *bat;*
- *bin;*
- *chm;*
- *cla, clas*;*
- *cmd;*
- *com;*
- *cpl;*
- *crt;*
- *dll;*
- *dpl;*
- *drv;*
- *dvb;*
- *dwg;*
- *efi;*
- *emf;*
- *eml;*
- *exe;*
- *fon;*
- *fpm;*
- *hlp;*
- *hta;*
- *htm, html*;*
- *htt;*
- *ico;*

- *inf;*
- *ini;*
- *ins;*
- *isp;*
- *jpg, jpe;*
- *js, jse;*
- *lnk;*
- *mbx;*
- *msc;*
- *msg;*
- *msi;*
- *msp;*
- *mst;*
- *nws;*
- *ocx;*
- *oft;*
- *otm;*
- *pcd;*
- *pdf;*
- *php;*
- *pht;*
- *phtm*;*
- *pif;*
- *plg;*
- *png;*
- *pot;*
- *prf;*
- *prg;*
- *reg;*
- *rsc;*
- *rtf;*
- *scf;*
- *scr;*
- *sct;*
- *shb;*

- *shs;*
- *sht;*
- *shtm*;*
- *swf;*
- *sys;*
- *the;*
- *them*;*
- *tsp;*
- *url;*
- *vb;*
- *vbe;*
- *vbs;*
- *vxd;*
- *wma;*
- *wmf;*
- *wmv;*
- *wsc;*
- *wsf;*
- *wsh;*
- *do?;*
- *md?;*
- *mp?;*
- *ov?;*
- *pp?;*
- *vs?;*
- *xl?.*

Default Real-Time File Protection task settings

By default, the Real-Time File Protection task uses the settings described in the table below. You can change the values of these settings.

Table 42. Default Real-Time File Protection task settings

Setting	Default Value	Description
Protection scope	The entire computer, excluding virtual drives.	You can limit the protection scope.
Objects protection mode	**On access and modification**	You can select protection mode, i.e. define type of access at which Kaspersky Embedded Systems Security will scan objects.
Heuristic analyzer	The **Medium** security level is applied.	The Heuristic Analyzer can be enabled or disabled and the analysis level configured.
Apply Trusted Zone	Applied.	General list of exclusions which can be used in selected tasks.
Use KSN for protection	Applied.	You can improve your server protection using the Kaspersky Security Network infrastructure of cloud services (available if the KSN Statement is accepted).
Task start schedule	At application start.	You can configure scheduled task start.
Block access to network shared resources for the hosts that show malicious activity	Not applied.	You can add hosts showing malicious activity to the list of blocked hosts.

Managing Real-Time File Protection task via the Administration Plug-in

In this section, learn how to navigate the Administration Plug-In interface and configure task settings for one or all computers on the network.

In this section

Navigation

Learn how to navigate to the required task settings via the interface.

In this section

Opening policy settings for the Real-Time File Protection task

► *To open the Real-Time File Protection task settings via the Kaspersky Security Center policy:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure the task.
3. Select the **Policies** tab.
4. Double-click the policy name you want to configure.
5. In the **Properties: <Policy name>** window that opens, select the **Real-time computer protection** section.
6. Click the **Settings** button in the **Real-Time File Protection** subsection.

   The **Real-time file protection** window opens.

If a computer is being managed by an active Kaspersky Security Center policy and this policy blocks changes to the application settings, these settings cannot be edited via the Application Console.

Opening the Real-Time File Protection task properties

► *To open the Real-Time File Protection task settings window for a single network computer:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure the task.
3. Select the **Devices** tab.
4. Open the **Properties: <Computer name>** window in one of the following ways:
   - Double-click the name of the protected computer.
   - Select the **Properties** item in the context menu of the protected computer.

   The **Properties: <Computer name>** window opens.
5. In the **Tasks** section, select the **Real-Time File Protection** task.
6. Click the **Properties** button.

   The **Properties: Real-Time File Protection** window opens.

Configuring the Real-Time File Protection task

► *To configure the Real-Time File Protection task settings:*

1. Open the **Real-time file protection** window (see Section "Opening policy settings for the Real-Time File Protection task" on page 244).
2. Configure the following task settings:
   - On the **General** tab:
     - **Objects protection mode** (see Section "**Selecting protection mode**" on page 246)
     - **Heuristic analyzer**
     - **Integration with other components** (see Section "**Configuring Heuristic Analyzer and integration with other application components**" on page 246)
   - On the **Task management** tab:
     - Scheduled task start settings (see Section "Configuring the task start schedule settings" on page 129).
3. Select the **Protection scope** tab and do the following:
   - Click the **Add** or **Edit** button to edit the protection scope (see Section "Creating protection scope" on page 263).
     - In the window that opens, choose what you want to include in the task protection scope:
       - **Predefined scope**
       - **Disk, folder or network location**
       - **File**
     - Select one of the predefined security levels (on page 238) or manually configure the protection (see Section "Configuring security settings manually" on page 251) settings.
4. Click **OK** in the **Real-time file protection** window.

Kaspersky Embedded Systems Security immediately applies the new 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 system audit log.

In this section

Selecting protection mode

In the Real-Time File Protection task, the protection mode can be selected. The **Objects protection mode** section lets you specify the type of access to objects upon which Kaspersky Embedded Systems Security should scan the objects.

The **Objects protection mode** setting has the common value for the entire protection scope specified in the task. You cannot specify different values for the setting for individual nodes within the protection scope.

► *To select the protection mode:*

1. Open the **Real-time file protection** window (see Section "Opening policy settings for the Real-Time File Protection task" on page 244).
2. In the window that opens, open the **General** tab and select the protection mode that you want to set:
   - **Smart mode**

     Kaspersky Embedded Systems Security selects objects to be scanned on its own. The object is scanned on being opened and then again after being saved if the object has been modified. If multiple calls to the object were made by the process while it was running and if the process modified it, Kaspersky Embedded Systems Security rescans the object only after the object was saved by the process for the last time.
   - **On access and modification**

     Kaspersky Embedded Systems Security scans the object when it is opened and rescans after it is saved if the object was modified.

     This option is selected by default.
   - **On access**

     Kaspersky Embedded Systems Security scans all objects when they are opened for reading or for execution or modification.
   - **When run**

     Kaspersky Embedded Systems Security scans the file only when it is accessed to be executed.
3. Click **OK**.

The selected protection mode will take effect.

Configuring Heuristic Analyzer and integration with other application components

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

► *To configure the Heuristic Analyzer and Integration with other components:*

1. Open the **Real-time file protection** window (see Section "Opening policy settings for the Real-Time File Protection task" on page 244).
2. On the **General** tab, 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.

3. 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.

4. In the **Integration with other components** section, configure the following settings:

   - 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 Embedded Systems Security adds file operations of trusted processes to the scan exclusions configured in the task settings.

     If the check box is cleared, Kaspersky Embedded Systems Security disregards the file operations of trusted processes when forming the protection scope for the task.

     The check box is selected by default.

   - Select or clear the **Use KSN for protection** check box.

     This check box enables or disables the use of KSN services.

     If the check box is selected, the application uses Kaspersky Security Network data to ensure that the application responds more quickly to new threats and to reduce the likelihood of false positives.

     If the check box is cleared, the task does not use KSN services.

     The check box is selected by default.

     The **Send data about scanned files** check box must be selected in the KSN Usage task settings.

   - Select or clear the **Block access to network shared resources for the hosts that show malicious activity** check box.

5. Click **OK**.

Configured task settings are applied immediately to the running task. If the task is not running, the modified settings are applied at next start.

Configuring the task start schedule settings

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

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

1. In the Kaspersky Security Center Administration Console tree, expand the **Managed devices** node.
2. Select the group that the protected server belongs to.
3. In the details pane, select the **Tasks** tab.
4. Open the **Properties: <Task name>** window in one of the following ways:
   - Double-click the name of the task.
   - Open the context menu of the task name and select the Properties item.
5. Select **Schedule** section.
6. In the **Schedule settings** block, select the **Run by schedule** check box.

   > Fields with the schedule settings for the On-Demand Scan and Update tasks are unavailable if their scheduled start is blocked by a policy of Kaspersky Security Center.

7. 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 at intervals of 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 at intervals of 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 at intervals of 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 started (by default the task runs on Mondays).
      - **At application launch**, if you want the task to run every time Kaspersky Embedded Systems Security starts.
      - **After application database update**, if you want the task to run after every update of the application databases.

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

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

   > After you have specified the task start frequency, the time of the first task start, and the date from which the schedule applies, information about the estimated time for the next task start will appear in the top part of the window in the **Next start** field. Updated information about the estimated time of the next task start 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 start of scheduled system tasks (see Section "Configuring scheduled start of local system tasks" on page 95).

8. Use the **Advanced** tab to 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 a time interval under 24 hours 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 start of skipped tasks.
     c. Select the **Randomize the task start time within the interval of** of check box and specify a value in minutes.
9. Click **OK**.
10. Click the **Apply** button to save the task start settings.

If you want to configure application settings for a single task using Kaspersky Security Center, perform the steps described in Configuring local tasks in the Application settings window of the Kaspersky Security Center (on page 117) section.

Creating and configuring the task protection scope

► *To create and configure the task protection scope via the Kaspersky Security Center:*

1. Open the **Real-time file protection** window (see Section "Opening policy settings for the Real-Time File Protection task" on page 244).
2. Select the **Protection scope** tab.
3. All items already protected by the task are listed in the **Protection scope** table.
4. Click the **Add** button to add new item to the list.

   The **Add objects to protection scope** window opens.
5. Select an object type to add it to a protection scope:
   - **Predefined scope** to include one of the predefined scopes into protection scope on the server. Then in the drop down list select a necessary protection scope.
   - **Disk, folder or network location** to include individual drive, folder or a network object into a protection scope. Then select a necessary protection scope by clicking the **Browse** button.
   - **File** to include an individual file into protection scope. Then select a necessary protection scope by clicking the **Browse** button.

You cannot add an object into protection scope if it has already been added as an exclusion out of a protection scope.

6. To exclude individual items from the protection scope, clear check boxes next to the names of these items or take the following steps:

   a. Open the context menu on the protection scope by right-clicking it.

   b. In the context menu select **Add exclusion** option.

   c. In the **Add exclusion** window select an object type that you want to add as an exclusion out of the protection scope following the logic of the adding object to a protection scope procedure.

7. To modify the protection scope or an exclusion added, select the **Edit scope** option in the context menu for the necessary protection scope.

8. To hide the previously added protection scope or an exclusion in the list of network file resources, select the **Remove scope** option in the context menu for the necessary protection scope.

   The protection scope is excluded out of the Real-Time File Protection task scope on its removal from the network file resources list.

9. Click the **Save** button.

Protection scope settings window is closed. Your newly configured settings are saved.

The **Real-Time File Protection** task can be started if at least one of the computer file resource nodes is included into a protection scope.

Configuring security settings manually

By default, the Real-Time File Protection task uses common security settings for the entire protection scope. These settings correspond to the **Recommended** predefined security level (see Section "Predefined security levels" on page 238).

The default values of security settings can be modified by configuring them as common settings for the entire protection scope or as different settings for different items in the computer file resource list or nodes in the tree.

► *To configure the security settings of the selected node manually:*

1. Open the **Real-time file protection** window (see Section "Opening policy settings for the Real-Time File Protection task" on page 244).
2. On the **Protection scope** tab, select the node whose security settings you want to configure, and click **Configure**.

   The **Real-time file protection settings** window opens.
3. On the **Security level** tab click the **Settings** button to set custom configuration.
4. You can configure the custom security settings of the selected node in accordance with your requirements:
   - General settings (see Section "Configuring general task settings" on page 251)
   - Actions (see Section "Configuring actions" on page 254)
   - Performance (see Section "Configuring performance" on page 256)
5. Click **OK** in the **Real-time file protection** window.

New protection scope settings are saved.

In this section

Configuring general task settings

► *To configure the general security settings of the Real-Time File Protection task:*

1. Open the **Real-time file protection settings** window (see Section "Opening policy settings for the Real-Time File Protection task" on page 244).
2. Select the **General** tab.

3. In the **Objects protection** section, specify the objects types that you want to include in the protection scope:

   - **All objects**

     Kaspersky Embedded Systems Security scans all objects.

   - **Objects scanned by format**

     Kaspersky Embedded Systems Security scans only infectable objects based on file format.

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

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

     Kaspersky Embedded Systems Security scans only infectable objects based on file extension.

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

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

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

   - **Scan disk boot sectors and MBR**

     Enables protection of boot sectors and master boot records.

     If the check box is selected, Kaspersky Embedded Systems Security scans boot sectors and master boot records on hard drives and removable drives of the computer.

     The check box is selected by default.

   - **Scan alternate NTFS streams**

     Scanning of alternative file and folder streams on the NTFS file system drives.

     If the check box is selected, the application scans a probably infected object and all NTFS streams associated with that object.

     If the check box is cleared, the application scans only the object that was detected and considered as probably infected.

     The check box is selected by default.

4. In the **Performance** section, select or clear the **Protect only new and modified files** check box.

   This check box enables / disables scanning and protection of files that have been recognized by Kaspersky Embedded Systems Security as new or modified since the last scan.

   If the check box is selected, Kaspersky Embedded Systems Security scans and protects only the files that it has recognized as new or modified since the last scan.

   If the check box is cleared, you can select if you want to scan and protect only new files or all files disregarding their modification status.

   By default, the check box is selected for the **Maximum performance** security level. If the **Maximum protection** or **Recommended** security levels are set, the check box is cleared.

> To switch between available options when the check box is cleared, click on the **All** / **Only new** link for each of the compound object types.

5. In the **Compound objects protection** section, specify the compound objects that you want to include in the protection scope:

   - **All / Only new archives**

     Scanning of ZIP, CAB, RAR, ARJ archives and other archive formats.

     If this check box is selected, Kaspersky Embedded Systems Security scans archives.

     If this check box is cleared, Kaspersky Embedded Systems Security skips archives during scanning.

     The default value depends on the selected protection level.

   - **All / Only new SFX archives**

     Scanning of self-extracting archives.

     If this check box is selected, Kaspersky Embedded Systems Security scans SFX archives.

     If this check box is cleared, Kaspersky Embedded Systems Security skips SFX archives during scanning.

     The default value depends on the selected protection level.

     This option is active when the **Archives** check box is cleared.

   - **All / Only new email databases**

     Scanning of Microsoft Outlook and Microsoft Outlook Express mail database files.

     If this check box is selected, Kaspersky Embedded Systems Security scans mail database files.

     If this check box is cleared, Kaspersky Embedded Systems Security skips mail database files during scanning.

     The default value depends on the selected security level.

   - **All / Only new packed objects**

     Scanning of executable files packed by binary code packers, such as UPX or ASPack.

     If this check box is selected, Kaspersky Embedded Systems Security scans executable files packed by packers.

     If this check box is cleared, Kaspersky Embedded Systems Security skips executable files packed by packers during scanning.

     The default value depends on the selected protection level.

   - **All / Only new plain email**

     Scanning of files of mail formats, such as Microsoft Outlook and Microsoft Outlook Express messages.

     If this check box is selected, Kaspersky Embedded Systems Security scans files of mail formats.

     If this check box is cleared, Kaspersky Embedded Systems Security skips files of mail formats during scanning.

The default value depends on the selected security level.

- **All / Only new embedded OLE objects**

  Scanning of objects embedded into files (such as Microsoft Word macros, or email message attachments).

  If this check box is selected, Kaspersky Embedded Systems Security scans objects embedded into files.

  If this check box is cleared, Kaspersky Embedded Systems Security skips objects embedded into files during scanning.

  The default value depends on the selected protection level.

6. Click **Save**.

New task configuration will be saved.

Configuring actions

► *To configure the actions on infected and other detected objects for the Real-Time File Protection task:*

1. Open the **Real-time file protection settings** (see Section "**Opening policy settings for the Real-Time File Protection task**" on page 244) window.
2. Select the **Actions** tab.
3. Select the action to be performed on infected and other detected objects:
   - **Notify only**.

     When this mode is selected, Kaspersky Embedded Systems Security does not block access to detected or other detected objects, or perform any actions on them. The following event is registered in the task log: *Object not disinfected. Reason: no action was taken to neutralize detected object due to user-defined settings.* The event specifies all available information about the detected object.

     The **Notify only** mode should be separately configured for each protection or scan area. This mode is not used by default on any of the security levels. If you select this mode, Kaspersky Embedded Systems Security automatically changes the security level to **Custom**.

   - **Block access**.

     When this option is selected Kaspersky Embedded Systems Security blocks access to the detected or probably infected object. You can select additional action over blocked objects in the drop-down list.

   - **Perform additional action**.

     Select the action from the drop-down list:

     - **Disinfect**.
     - **Disinfect. Remove if disinfection fails**.
     - **Remove**.
     - **Recommended**.
4. Select the action to be performed on probably infected objects:

- **Notify only**.

  When this mode is selected, Kaspersky Embedded Systems Security does not block access to detected or other detected objects, or perform any actions on them. The following event is registered in the task log: *Object not disinfected. Reason: no action was taken to neutralize detected object due to user-defined settings.* The event specifies all available information about the detected object.

  The **Notify only** mode should be separately configured for each protection or scan area. This mode is not used by default on any of the security levels. If you select this mode, Kaspersky Embedded Systems Security automatically changes the security level to **Custom**.

- **Block access**.

  When this option is selected Kaspersky Embedded Systems Security blocks access to the detected or probably infected object. You can select additional action over blocked objects in the drop-down list.

- **Perform additional action**.

  Select the action from the drop-down list:

  - **Quarantine**.
  - **Remove**.
  - **Recommended**.

5. Configure actions to be performed on objects depending on the type of object detected:

   a. Clear or select the **Perform actions depending on the type of object detected** check box.

   If the check box is selected, you can independently set primary and secondary action for each detected object type by clicking the **Settings** button next to the check box. At that, Kaspersky Embedded Systems Security will not allow to open or execute an infected object regardless of your choice.

   If the check box is cleared, Kaspersky Embedded Systems Security performs actions that are selected in the **Action to perform on infected and other objects** and **Action to perform on probably infected objects** sections for named object types respectively.

   The check box is cleared by default.

   b. Click the **Settings** button.

   c. In the window that opens select first and secondary action (if the first action fails) for each type of the detected object.

   d. Click **OK**.

6. Select the action 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 detect** 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 Embedded Systems Security 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 Embedded Systems Security does not perform the selected action, if the parent object is unmodifiable.

7. Click **Save**.

New task configuration will be saved.

Configuring performance

► *To configure the performance for the Real-Time File Protection task:*

1. Open the **Real-time file protection settings (see Section "Opening policy settings for the Real-Time File Protection task" on page** 244**)** window.
2. Select the **Performance** tab.
3. In the **Exclusions** section:
   - Clear or select the **Exclude files** check box.

     Excluding files from scanning by file name or file name mask.

     If this check box is selected, Kaspersky Embedded Systems Security skips specified objects during scanning.

     If this check box is cleared, Kaspersky Embedded Systems Security scans all objects.

     The check box is cleared by default.
   - Clear or select the **Do not detect** check box.

     Objects are excluded from scanning by the name or name mask of the detectable object. The list of names of detectable objects is available on the Virus Encyclopedia https://encyclopedia.kaspersky.com/knowledge/classification/ website.

     If this check box is selected, Kaspersky Embedded Systems Security skips specified detectable objects during scanning.

     If the check box is cleared, Kaspersky Embedded Systems Security detects all objects specified in the application by default.

     The check box is cleared by default.
   - Click the **Edit** button for each setting to add exclusions.
4. In the **Advanced settings** section:
   - **Stop scanning if it takes longer than (sec.)**

     Limits the duration of object scanning. The default value is 60 seconds.

     If the check box is cleared, scan duration is limited to the specified value.

     If the check box is cleared, scan duration is unlimited.

     By default, the check box is selected for the **Maximum performance** security level.
   - **Do not scan compound objects larger than (MB)**

     Excludes objects larger than the specified size from the scanning.

     If the check box is selected, Kaspersky Embedded Systems Security skips compound objects whose size exceeds the specified limit during virus scan.

If this check box is cleared, Kaspersky Embedded Systems Security scans compound objects of any size.

By default, the check box is selected for the **Maximum performance** security level.

- **Use iSwift technology**

  iSwift compares file NTFS identifier, that is stored in a database, with a current identifier. The scanning is performed only for files, whose identifiers has changed (new files and files modified since the last scan of NTFS system objects).

  If the check box is selected, Kaspersky Embedded Systems Security scans only new files or those modified since the last scan of NTFS system objects.

  If the check box is cleared, Kaspersky Embedded Systems Security scans objects of NTFS file system disregarding the date of file creation or modification except for files from network folders.

  The check box is selected by default.

- **Use iChecker technology**

  iChecker calculates and remembers checksums of scanned files. If an object is modified the checksum changes. The application compares all checksums during the scan task and scans only new and modified since the last scan files.

  If the check box is selected, Kaspersky Embedded Systems Security scans only new and modified files.

  If the check box is cleared, Kaspersky Embedded Systems Security scans files disregarding the date of file creation or modification.

  The check box is selected by default.

Managing Real-Time File Protection task via the Application Console

In this section, learn how to navigate the Application Console interface and configure task settings on a local computer.

In this section

Navigation

Learn how to navigate to the required task settings via the interface.

Opening the Real-Time File Protection scope settings

► *To open the Protection scope settings window for the Real-Time File Protection task:*

1. In the Application Console tree, expand the **Real-Time Computer Protection** node.
2. Select the **Real-Time File Protection** child node.
3. Click the **Configure protection scope** link in the details pane.

   The **Protection scope settings** window opens.

Opening the Real-Time File Protection task settings

► *To open the general task settings window:*

1. In the Application Console tree, expand the **Real-Time Computer Protection** node.
2. Select the **Real-Time File Protection** child node.
3. Click the **Properties** link in the details pane.

   The **Task settings** window opens.

Configuring the Real-Time File Protection task

► *To configure the Real-Time File Protection task settings:*

1. Open the **Task settings** window (see Section "Opening the Real-Time File Protection task settings" on page 258).
2. On the **General** tab, configure the following task settings:
   - **Objects protection mode** (see Section "**Selecting protection mode**" on page 259)
   - **Heuristic analyzer**
   - **Integration with other components** (see Section "**Configuring Heuristic Analyzer and integration with other application components**" on page 260)
3. On the **Schedule** and **Advanced** tabs, specify the scheduled start settings (see Section "Configuring the task start schedule settings" on page 149).
4. Click **OK** in the **Task settings** window.

   The modified settings are saved.
5. In the details pane of the **Real-Time File Protection** node click the **Configure protection scope** link.
6. Do the following:
   - In the tree or in the list of file resources of the computer, select the nodes or items that you want to be included in the task protection scope.
   - Select one of the predefined security levels or configure the object protection settings manually (see Section "Configuring security settings manually" on page 432).
7. In the **Protection scope settings** window, click the **Save** button.

Kaspersky Embedded Systems Security immediately applies the new settings to the running task. Information about the date and time of the settings modification, and the values of task settings set before and after modification, are saved in the system audit log.

In this section

Selecting protection mode

In the Real-Time File Protection task, the protection mode can be selected. The **Objects protection mode** section lets you specify the type of access to objects upon which Kaspersky Embedded Systems Security should scan the objects.

The **Objects protection mode** setting has the common value for the entire protection scope specified in the task. You cannot specify different values for the setting for individual nodes within the protection scope.

► *To select protection mode, take the following steps:*

1. Open the **Task settings** window (see Section "Opening the Real-Time File Protection task settings" on page 258).
2. In the window that opens, open the **General** tab and select the protection mode that you want to set:
   - **Smart mode**

     Kaspersky Embedded Systems Security selects objects to be scanned on its own. The object is scanned on being opened and then again after being saved if the object has been modified. If multiple calls to the object were made by the process while it was running and if the process modified it, Kaspersky Embedded Systems Security rescans the object only after the object was saved by the process for the last time.
   - **On access and modification**

     Kaspersky Embedded Systems Security scans the object when it is opened and rescans after it is saved if the object was modified.

     This option is selected by default.
   - **On access**

     Kaspersky Embedded Systems Security scans all objects when they are opened for reading or for execution or modification.
   - **When run**

     Kaspersky Embedded Systems Security scans the file only when it is accessed to be executed.
3. Click **OK**.

The selected protection mode will take effect.

Configuring Heuristic Analyzer and integration with other application components

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

► *To configure the Heuristic Analyzer and Integration with other components:*

1. Open the **Task settings** (see Section "**Opening the Real-Time File Protection task settings**" on page 258) window.
2. On the **General** tab, 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.

3. 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.

4. In the **Integration with other components** section, configure the following settings:

   - 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 Embedded Systems Security adds file operations of trusted processes to the scan exclusions configured in the task settings.

     If the check box is cleared, Kaspersky Embedded Systems Security disregards the file operations of trusted processes when forming the protection scope for the task.

     The check box is selected by default.

     Click the **Trusted Zone** link to open the Trusted Zone settings.
   - Select or clear the **Use KSN for protection** check box.

     This check box enables or disables the use of KSN services.

     If the check box is selected, the application uses Kaspersky Security Network data to ensure that the application responds more quickly to new threats and to reduce the likelihood of false positives.

     If the check box is cleared, the task does not use KSN services.

     The check box is selected by default.

     > The **Send data about scanned files** check box must be selected in the KSN Usage task settings.
   - Select or clear the **Block access to network shared resources for the hosts that show malicious activity** check box.

5. Click **OK**.

The newly configured settings will be applied.

Configuring the task start schedule settings

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

► *To configure task start schedule settings:*

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

   The **Task settings** window opens.
3. In the window that opens, on the **Schedule** tab, select the **Run by schedule** check box.
4. Configure schedule settings in accordance with your requirements. To do this, perform the following actions:

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

      - **Hourly**, if you want the task to run at intervals of 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 at intervals of 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 at intervals of a specified number of weeks; specify the number of weeks in the **Every <number> week(s) on** field. Specify the days of the week on which the task will be started (by default the task runs on Mondays).
      - **At application launch**, if you want the task to run every time Kaspersky Embedded Systems Security starts.
      - **After application database update**, if you want the task to run after every update of the application databases.

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

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

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

   Blocked by policy is displayed in the **Next start** field if starting system tasks on a schedule is set in the Kaspersky Security Center policy settings.
5. Use the **Advanced** tab to 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 a time interval under 24 hours 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 start of skipped tasks.

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

6. Click **OK**.

The configured task start settings will be saved.

Creating protection scope

This section provides instructions on creating and managing a protection scope in the Real-Time File Protection task.

In this section

Creating protection scope

The procedure of creating the Real-Time File Protection task scope depends on the network file resources view mode (see Section "About the task protection scope and security settings" on page 236). You can configure network file resources view mode as a tree or as a list (set as default).

> To apply the new protection scope settings to the task, the Real-Time File Protection task must be restarted.

► *To create a protection scope using the network file resources tree:*

1. Open the **Protection scope settings** window (see Section "Opening the Real-Time File Protection scope settings" on page 258).
2. In the left section of the window open the network file resources tree to display all the nodes and child nodes.
3. Do the following:
   - To exclude individual nodes from the protection scope, clear check boxes next to the names of these nodes.
   - To include individual nodes in the protection scope, clear the **My Computer** check box and do the following:
     - If all drives of one type are to be included in the protection scope, select the check box opposite the name of the required disk type (for example, to add all removable drives on the computer, select the **Removable drives** check box).

- If an individual disk of a certain type is to be included in the protection scope, expand the node that contains the list of drives of this type and check the box next to the name of the required drive. For example, in order to select removable drive F:, expand node **Removable drives** and check the box for drive **F:**.
- If you would like to include only a single folder or file on the drive, select the check box next to the name of that folder or file.

4. Click the **Save** button.

Protection scope settings window will be closed. Your newly configured settings have been saved.

► *To create a protection scope using the network file resources list:*

1. Open the **Protection scope settings** window (see Section "Opening the Real-Time File Protection scope settings" on page 258).
2. To include individual nodes in the protection scope, clear the **My Computer** check box and do the following:

   a. Open the context menu on the protection scope by right-clicking it.

   b. In the context menu of the button, select **Add protection scope**.

   c. In the **Add protection scope** window select an object type to add it to a protection scope:

   - **Predefined scope** to include one of the predefined scopes into protection scope on the computer. Then in the drop down list select a necessary protection scope.
   - **Disk, folder or network location** to include individual drive, folder or a network object into a protection scope. Then select a necessary scope by clicking the **Browse** button.
   - **File** to include an individual file into protection scope. Then select a necessary scope by clicking the **Browse** button.

   > You cannot add an object into protection scope if it has already been added as an exclusion out of a protection scope.

3. To exclude individual nodes from the protection scope, clear check boxes next to the names of these nodes or take the following steps:

   a. Open the context menu on the protection scope by right-clicking it.

   b. In the context menu select **Add exclusion** option.

   c. In the **Add exclusion** window select an object type that you want to add as an exclusion out of the protection scope following the logic of the adding object to a protection scope procedure.

4. To modify the protection scope or an exclusion added, select the **Edit scope** option in the context menu for the necessary protection scope.
5. To hide the previously added protection scope or an exclusion in the list of network file resources, select the **Remove from the list** option in the context menu for the necessary protection scope.

   > The protection scope is excluded out of the Real-Time File Protection task scope on its removal from the network file resources list.

6. Click the **Save** button.

Protection scope settings window will be closed. Your newly configured settings have been saved.

The *Real-Time File Protection* task can be started if at least one of the computer file resource nodes is included into a protection scope.

If a complex protection scope is specified, for example, if different security values for settings for multiple nodes in the computer file resource tree are specified, this may slow the scanning of objects when they are accessed.

Creating virtual protection scope

You can expand the protection / scan scope by adding individual virtual drives, folders, or files only if the protection / scan scope is presented as a tree of file resources (see Section "Configuring view mode for network file resources" on page 429).

► *To add a virtual drive to the protection scope:*

1. Open the **Protection scope settings** window (see Section "Opening the Real-Time File Protection scope settings" on page 258).
2. Open the drop-down list in the window upper left sector and select **Tree-view**.
3. Open the context menu of the **Virtual drives**.
4. Select the **Add virtual drive** option.
5. In the list of available names, select the name for the virtual drive that is being created.
6. Enable the check box next to the drive added to include the drive in the protection scope.
7. In the **Protection scope settings** window, click the **Save** button.

Your newly configured settings have been saved.

► *To add a virtual folder or virtual file to the protection scope:*

1. Open the **Protection scope settings** window (see Section "Opening the Real-Time File Protection scope settings" on page 258).
2. Open the drop-down list in the window upper left sector and select **Tree-view**.
3. Open the context menu for the virtual drive to which you want to add a folder or a file, and select one of the following options:
   - **Add virtual folder** if you want to add a virtual folder to the protection scope.
   - **Add virtual file** if you want to add a virtual file to the protection scope.
4. In the entry field specify the name of the folder or file.

5. In the line containing the name of the created folder or file, select the check box to include the folder or file in the protection scope.
6. In the **Protection scope settings** window, click the **Save** button.

The modified task settings are saved.

Configuring security settings manually

By default Real-Time Computer Protection tasks use common security settings for the entire protection scope. These settings correspond to the **Recommended** predefined security level (see Section "Predefined security levels" on page 238).

The default values of security settings can be modified by configuring them as common settings for the entire protection scope or as different settings for different items in the computer file resource list or nodes in the tree.

When working with the server file resources tree, security settings that are configured for the selected parent node are automatically applied to all child nodes. The security settings of the parent node are not applied to child nodes that are configured separately.

► *To configure security settings manually:*

1. Open the **Protection scope settings** window (see Section "Opening the Real-Time File Protection scope settings" on page 258).
2. In the left window section select the node to configure security settings.

> A predefined template containing security settings (see Section "About security settings templates" on page 156) can be applied for a selected node or item in the protection scope.

3. Configure the required security settings of the selected node or item in accordance with your requirements:
   - **General** (see Section "**Configuring general task settings**" on page 267)
   - **Actions** (see Section "**Configuring actions**" on page 269)
   - **Performance** (see Section "**Configuring performance**" on page 271)
4. In the **Protection scope settings** window, click the **Save** button.

New protection scope settings are saved.

In this section

Configuring general task settings

► *To configure the general security settings of the Real-Time File Protection task:*

1. Open the **Protection scope settings** window (see Section "Opening the Real-Time File Protection scope settings" on page 258).
2. Select the **General** tab.
3. In the **Objects protection** section, specify the objects that you want to include in the protection scope:
   - **All objects**

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

     Kaspersky Embedded Systems Security scans only infectable objects based on file format.

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

     Kaspersky Embedded Systems Security scans only infectable objects based on file extension.

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

     Kaspersky Embedded Systems Security scans files based on file extension. List of file extensions can be manually customized in the **List of extensions** window, which can be opened by clicking the **Edit** button.
   - **Scan disk boot sectors and MBR**

     Enables protection of boot sectors and master boot records.

     If the check box is selected, Kaspersky Embedded Systems Security scans boot sectors and master boot records on hard drives and removable drives of the computer.

     The check box is selected by default.
   - **Scan alternate NTFS streams**

     Scanning of alternative file and folder streams on the NTFS file system drives.

     If the check box is selected, the application scans a probably infected object and all NTFS streams associated with that object.

     If the check box is cleared, the application scans only the object that was detected and considered as probably infected.

     The check box is selected by default.
4. In the **Performance** section, select or clear the **Protect only new and modified files** check box.

   This check box enables / disables scanning and protection of files that have been recognized by Kaspersky Embedded Systems Security as new or modified since the last scan.

   If the check box is selected, Kaspersky Embedded Systems Security scans and protects only the files that it has recognized as new or modified since the last scan.

If the check box is cleared, you can select if you want to scan and protect only new files or all files disregarding their modification status.

By default, the check box is selected for the **Maximum performance** security level. If the **Maximum protection** or **Recommended** security levels are set, the check box is cleared.

> To switch between available options when the check box is cleared, click on the **All** / **Only new** link for each of the compound object types.

5. In the **Compound objects protection** section, specify the compound objects that you want to include in the protection scope:

   - **All / Only new archives**

     Scanning of ZIP, CAB, RAR, ARJ archives and other archive formats.

     If this check box is selected, Kaspersky Embedded Systems Security scans archives.

     If this check box is cleared, Kaspersky Embedded Systems Security skips archives during scanning.

     The default value depends on the selected protection level.

   - **All / Only new SFX archives**

     Scanning of self-extracting archives.

     If this check box is selected, Kaspersky Embedded Systems Security scans SFX archives.

     If this check box is cleared, Kaspersky Embedded Systems Security skips SFX archives during scanning.

     The default value depends on the selected protection level.

     This option is active when the **Archives** check box is cleared.

   - **All / Only new email databases**

     Scanning of Microsoft Outlook and Microsoft Outlook Express mail database files.

     If this check box is selected, Kaspersky Embedded Systems Security scans mail database files.

     If this check box is cleared, Kaspersky Embedded Systems Security skips mail database files during scanning.

     The default value depends on the selected security level.

   - **All / Only new packed objects**

     Scanning of executable files packed by binary code packers, such as UPX or ASPack.

     If this check box is selected, Kaspersky Embedded Systems Security scans executable files packed by packers.

     If this check box is cleared, Kaspersky Embedded Systems Security skips executable files packed by packers during scanning.

     The default value depends on the selected protection level.

- **All / Only new plain email**

  Scanning of files of mail formats, such as Microsoft Outlook and Microsoft Outlook Express messages.

  If this check box is selected, Kaspersky Embedded Systems Security scans files of mail formats.

  If this check box is cleared, Kaspersky Embedded Systems Security skips files of mail formats during scanning.

  The default value depends on the selected security level.

- **All / Only new embedded OLE objects**

  Scanning of objects embedded into files (such as Microsoft Word macros, or email message attachments).

  If this check box is selected, Kaspersky Embedded Systems Security scans objects embedded into files.

  If this check box is cleared, Kaspersky Embedded Systems Security skips objects embedded into files during scanning.

  The default value depends on the selected protection level.

6. Click **Save**.

New task configuration will be saved.

Configuring actions

► *To configure the actions on infected and other detected objects for the Real-Time File Protection task:*

1. Open the **Protection scope settings** window (see Section "Opening the Real-Time File Protection scope settings" on page 258).
2. Select the **Actions** tab.
3. Select the action to be performed on infected and other detected objects:

   - **Notify only**.

     When this mode is selected, Kaspersky Embedded Systems Security does not block access to detected or other detected objects, or perform any actions on them. The following event is registered in the task log: *Object not disinfected. Reason: no action was taken to neutralize detected object due to user-defined settings.* The event specifies all available information about the detected object.

     The **Notify only** mode should be separately configured for each protection or scan area. This mode is not used by default on any of the security levels. If you select this mode, Kaspersky Embedded Systems Security automatically changes the security level to **Custom**.

   - **Block access**.

     When this option is selected Kaspersky Embedded Systems Security blocks access to the detected or probably infected object. You can select additional action over blocked objects in the drop-down list.

   - **Perform additional action**.

Select the action from the drop-down list:

  - **Disinfect**.
  - **Disinfect. Remove if disinfection fails**.
  - **Remove**.
  - **Recommended**.

4. Select the action to be performed on probably infected objects:

   - **Notify only**.

     When this mode is selected, Kaspersky Embedded Systems Security does not block access to detected or other detected objects, or perform any actions on them. The following event is registered in the task log: *Object not disinfected. Reason: no action was taken to neutralize detected object due to user-defined settings.* The event specifies all available information about the detected object.

     The **Notify only** mode should be separately configured for each protection or scan area. This mode is not used by default on any of the security levels. If you select this mode, Kaspersky Embedded Systems Security automatically changes the security level to **Custom**.

   - **Block access**.

     When this option is selected Kaspersky Embedded Systems Security blocks access to the detected or probably infected object. You can select additional action over blocked objects in the drop-down list.

   - **Perform additional action**.

     Select the action from the drop-down list:

     - **Quarantine**.
     - **Remove**.
     - **Recommended**.

5. Configure actions to be performed on objects depending on the type of object detected:

   a. Clear or select the **Perform actions depending on the type of object detected** check box.

   If the check box is selected, you can independently set primary and secondary action for each detected object type by clicking the **Settings** button next to the check box. At that, Kaspersky Embedded Systems Security will not allow to open or execute an infected object regardless of your choice.

   If the check box is cleared, Kaspersky Embedded Systems Security performs actions that are selected in the **Action to perform on infected and other objects** and **Action to perform on probably infected objects** sections for named object types respectively.

   The check box is cleared by default.

   b. Click the **Settings** button.

   c. In the window that opens select first and secondary action (if the first action fails) for each type of the detected object.

   d. Click **OK**.

6. Select the action 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 detect** 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 Embedded Systems Security 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 Embedded Systems Security does not perform the selected action, if the parent object is unmodifiable.

7. Click **Save**.

New task configuration will be saved.

Configuring performance

► *To configure the performance for the Real-Time File Protection task:*

1. Open the **Protection scope settings** window (see Section "Opening the Real-Time File Protection scope settings" on page 258).
2. Select the **Performance** tab.
3. In the **Exclusions** section:
   - Clear or select the **Exclude files** check box.

     Excluding files from scanning by file name or file name mask.

     If this check box is selected, Kaspersky Embedded Systems Security skips specified objects during scanning.

     If this check box is cleared, Kaspersky Embedded Systems Security scans all objects.

     The check box is cleared by default.
   - Clear or select the **Do not detect** check box.

     Objects are excluded from scanning by the name or name mask of the detectable object. The list of names of detectable objects is available on the Virus Encyclopedia https://encyclopedia.kaspersky.com/knowledge/classification/ website.

     If this check box is selected, Kaspersky Embedded Systems Security skips specified detectable objects during scanning.

     If the check box is cleared, Kaspersky Embedded Systems Security detects all objects specified in the application by default.

     The check box is cleared by default.
   - Click the **Edit** button for each setting to add exclusions.
4. In the **Advanced settings** section:
   - **Stop scanning if it takes longer than (sec.)**

Limits the duration of object scanning. The default value is 60 seconds.

If the check box is cleared, scan duration is limited to the specified value.

If the check box is cleared, scan duration is unlimited.

By default, the check box is selected for the **Maximum performance** security level.

- **Do not scan compound objects larger than (MB)**

  Excludes objects larger than the specified size from the scanning.

  If the check box is selected, Kaspersky Embedded Systems Security skips compound objects whose size exceeds the specified limit during virus scan.

  If this check box is cleared, Kaspersky Embedded Systems Security scans compound objects of any size.

  By default, the check box is selected for the **Maximum performance** security level.

- **Use iSwift technology**

  iSwift compares file NTFS identifier, that is stored in a database, with a current identifier. The scanning is performed only for files, whose identifiers has changed (new files and files modified since the last scan of NTFS system objects).

  If the check box is selected, Kaspersky Embedded Systems Security scans only new files or those modified since the last scan of NTFS system objects.

  If the check box is cleared, Kaspersky Embedded Systems Security scans objects of NTFS file system disregarding the date of file creation or modification except for files from network folders.

  The check box is selected by default.

- **Use iChecker technology**

  iChecker calculates and remembers checksums of scanned files. If an object is modified the checksum changes. The application compares all checksums during the scan task and scans only new and modified since the last scan files.

  If the check box is selected, Kaspersky Embedded Systems Security scans only new and modified files.

  If the check box is cleared, Kaspersky Embedded Systems Security scans files disregarding the date of file creation or modification.

  The check box is selected by default.

Real-Time File Protection task statistics

While the Real-Time File Protection task is being executed, you can view detailed real-time information about the number of objects processed by Kaspersky Embedded Systems Security since the task was started until the current moment.

► *To view the statistics of a Real-Time File Protection task, take the following steps:*

1. In the Application Console tree, expand the **Real-Time Computer Protection** node.

2. Select the **Real-Time File Protection** child node.

Task statistics are displayed in the **Statistics** section of the details pane of the selected node.

The information can be viewed about objects processed by Kaspersky Embedded Systems Security since it was started until the current moment (see the table below):

Table 43. Real-Time File Protection task statistics

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

You can view the Real-Time File Protection task statistics in the task log by clicking the **Open task log** in the **Management** section in the detail pane.

If the value of the **Total events** field in the Real-Time Protection task log window exceeds 0, it is recommended to process the events appeared in the task log on the **Events** tab manually.

KSN Usage

This section contains information about the KSN Usage task and how to configure it.

In this chapter

About the KSN Usage task

Kaspersky Security Network (also referred to as "KSN") is an infrastructure of online services providing access to Kaspersky Lab's operative knowledge base on the reputation of files, web resources and programs. Kaspersky Security Network allows Kaspersky Embedded Systems Security to react very promptly to new threats, improves the performance of several protection components, and reduces the likelihood of false positives.

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

Information received by Kaspersky Embedded Systems Security from Kaspersky Security Network pertains only to the reputation of programs.

Participation in KSN allows Kaspersky Lab to receive real-time information about types and sources of new threats, develop ways to neutralize them, and reduce the number of false positives in application components.

More detailed information about the transferring, processing, storage, and destruction of information about application usage is available in the **Data handling** window of the KSN Usage task, and in the Privacy Policy on the Kaspersky Lab's website.

Participation in Kaspersky Security Network is voluntary. The decision regarding participation in Kaspersky Security Network is made after installation of Kaspersky Embedded Systems Security. You can change your decision about participation in Kaspersky Security Network at any time.

Kaspersky Security Network can be used in the following Kaspersky Embedded Systems Security tasks:

- Real-Time File Protection.
- On-Demand Scan.
- Applications Launch Control.

Kaspersky Private Security Network

> See details about how to configure Kaspersky Private Security Network (hereinafter referred to "Private KSN") in the *Kaspersky Security Center Help*.

If you use Private KSN on the protected computer, in the **Data handling** window (see Section "Configuring Data Handling via the Administration Plug-in" on page 280) of the KSN Usage task you can read the KSN Statement and enable the task by selecting the **I accept the Kaspersky Private Security Network Statement** check box. By accepting the terms you agree to send all types of data mentioned in KSN Statement (security requests, statistical data) to KSN services.

> After accepting the Private KSN terms, the check boxes that adjust the Global KSN usage are not available.

If you disable Private KSN when the KSN Usage task is running, the *License violation* error occurs and the task stops. To continue protecting the computer you need to accept the KSN Statement in the **Data handling** window and restart the task.

Withdrawal of the KSN Statement acceptance

You can withdraw the acceptance and stop any data exchange with the Kaspersky Security Network at any moment. The following actions are considered as the full or partial withdrawal of KSN Statement:

- Clearing the **Send data about scanned files** check box: the application stops sending checksums of scanned files to KSN service for analysis.
- Clearing the **Send Kaspersky Security Network statistics** check box: the application stops processing data with additional KSN statistics.
- Clearing the **I accept the terms of the Kaspersky Security Network Statement** check box: the application stops all KSN-related data processing, the KSN Usage task stops.
- Uninstalling the KSN Usage component: all KSN-related data processing stops.
- Uninstalling the Kaspersky Embedded Systems Security: all KSN-related data processing stops.

Default KSN Usage task settings

You can change the default settings of the KSN Usage task (see the table below).

Table 44. Default KSN Usage task settings

Setting	Default Value	Description
Action to perform on KSN untrusted objects	Remove	You can specify actions that Kaspersky Embedded Systems Security will take on objects identified by KSN as untrusted.
Data transfer	The file checksum (MD5 hash) is calculated for files that do not exceed 2 MB in size.	You can specify the maximum size of files for which a checksum is calculated using the MD5 algorithm for delivery to KSN. If the check box is cleared, Kaspersky Embedded Systems Security calculates the MD5 hash for files of any size.
Task start schedule	First run is not scheduled.	You can start the task manually or configure a scheduled start.
Use Kaspersky Security Center as KSN Proxy	Selected	By default the data is sent to KSN via Kaspersky Security Center. You can change this setting only via the Administration Plug-in.
I accept the terms of the Kaspersky Security Network Statement	Cleared	If selected, participation in KSN after the installation is accepted. You can change your decision at any moment.
Send Kaspersky Security Network statistics	Selected (applied only if the KSN Statement is accepted)	If the KSN Statement is accepted, the KSN Statistics will be sent automatically, unless you clear the check box.
Send data about scanned files	Selected (applied only if the KSN Statement is accepted)	If the KSN Statement is accepted, the data about files that were scanned and analyzed since the task has been started, is sent. You can clear the check box at any time.
Send data about scanned URLs	Selected (applied only if the KSN Statement is accepted)	If the KSN Statement is accepted, the application sends information about the accessed URLs to Kaspersky Lab.
Accept the terms of the Kaspersky Managed Protection Statement	Cleared	You can enable or disable the KMP service. The service available only if the additional agreement has been signed during the application purchase process.

Managing KSN Usage via the Administration Plug-In

In this section, learn how configure the KSN Usage task and Data Handling via the Administration Plug-In.

In this section

Configuring the KSN Usage task via the Administration Plug-in

► *To configure the KSN Usage task, take the following steps:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.
3. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring a policy" on page 112).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in the Application settings window of the Kaspersky Security Center" on page 117).

   > If an active Kaspersky Security Center policy is applied to a device, and this policy blocks changes to application settings, then these settings cannot be edited in the **Application settings** window.

4. In the **Real-Time Computer Protection** section, click the **Settings** button in the **KSN Usage** block.

   The **KSN Usage** window opens.

5. On the **General** tab, configure the following task settings:
   - In the **Action to perform on KSN untrusted objects** section, specify the action that Kaspersky Embedded Systems Security is to perform if it detects an object identified by KSN as untrusted:
     - **Remove**

       Kaspersky Embedded Systems Security deletes the object with KSN-untrusted status and places a copy of it in Backup.

       This option is selected by default.

     - **Log information**

       Kaspersky Embedded Systems Security records information about the object with KSN-untrusted status in the task log. Kaspersky Embedded Systems Security does not delete the untrusted object.

- In the **Data transfer** section, restrict the size of files for which the checksum is calculated:
  - Clear or select the **Do not calculate checksum before sending to KSN if file size exceeds (MB)** check box.

    This check box enables or disables calculation of the checksum for files of the specified size for delivery of this information to the KSN service.

    The duration of the checksum calculation depends on the file size.

    If this check box is selected, Kaspersky Embedded Systems Security does not calculate the checksum for files that exceed the specified size (in MB).

    If the check box is cleared, Kaspersky Embedded Systems Security calculates the checksum for files of any size.

    The check box is selected by default.
  - If required, in the field to the right, change the maximum size of files for which Kaspersky Embedded Systems Security calculates the checksum.
- In the **KSN Proxy** section, clear or select the **Use Kaspersky Security Center as KSN Proxy** check box.

  The check box allows to manage the data transfer between the protected computers and KSN.

  If the check box is cleared the data from the Administration Server and protected computers is sent to KSN directly (not via the Kaspersky Security Center). The active policy defines which type of data can be sent to KSN directly.

  If the check box is selected, all data is sent to KSN via the Kaspersky Security Center.

  The check box is selected by default.

> To enable KSN Proxy the KSN Statement must be accepted and Kaspersky Security Center properly configured. See *Kaspersky Security Center Help* for more details.

6. If needed, configure the task start schedule on the **Task management** tab. For example, you can start the task by schedule and specify the **At application launch** frequency, if you want the task to run automatically when the server is restarted.

   The application will automatically start the KSN Usage task by schedule.
7. Configure the data handling (see Section "Configuring Data Handling via the Administration Plug-in" on page 280) before starting the task.
8. Click **OK**.

The modified settings are applied. The date and time of modifying the settings, as well as information about the task settings before and after modification, are saved in the system audit log.

Configuring Data Handling via the Administration Plug-in

► *To configure what data will be processed by the KSN services and accept the KSN Statement:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.

3. Perform one of the following actions in the details pane of the selected administration group:

   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring a policy" on page 112).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in the Application settings window of the Kaspersky Security Center" on page 117).

   > If an active Kaspersky Security Center policy is applied to a device, and this policy blocks changes to application settings, then these settings cannot be edited in the **Application settings** window.

4. In the **Real-Time Computer Protection** section click the **Data handling** button in the **KSN Usage** block.

   The **Data handling** window opens.

5. On the **Statistics and services** tab, read the Statement and select the **I accept the terms of the Kaspersky Security Network Statement** check box.
6. To increase the protection level, the following check boxes are automatically selected:

   - **Send data about scanned files**.

     If the check box is selected, Kaspersky Embedded Systems Security sends the checksum of scanned files to the Kaspersky Lab. Conclusion about each file security is based on the reputation received from KSN.

     If the check box is cleared, Kaspersky Embedded Systems Security does not send checksum of files to KSN.

     Note, than the file reputation requests might be sent in a limited mode. The limitations are used for protection of the Kaspersky Lab reputation servers from the DDoS attacks. In this scenario, the parameters of file reputation requests, that are being sent, are defined by the rules and methods established by the Kaspersky Lab experts and cannot be configured by user on a protected computer. Updates of these rules and methods are received along with the application database updates. If the limitations are applied, the *Enabled by Kaspersky Lab for protecting KSN servers against DDoS* status is displayed in the KSN Usage task statistics.

     The check box is selected by default.

   - **Send Kaspersky Security Network statistics.**

     If the check box is selected the Kaspersky Embedded Systems Security sends additional statistics, which may contain personal data. The list of all data, that is sent as KSN statistics, is specified in the KSN Statement. The data received by Kaspersky Lab is used to improve the quality of applications and level of threat detection rates.

     If the check box is cleared, Kaspersky Embedded Systems Security does not send additional statistics.

     The check box is selected by default.

   You can clear these check boxes and stop sending additional data at any moment.

7. On the **Kaspersky Managed Protection** tab, read the Statement and select the **I accept the terms of the Kaspersky Managed Protection Statement** check box.

   If the check box is selected, you agree to send statistics on the protected computer activity to the Kaspersky Lab specialists. Received data is used for around-the-clock analysis and reporting, required to prevent security breach incidents.

   The check box is cleared by default.

   The changes of **I accept the terms of the Kaspersky Managed Protection Statement** check box state do not start or stop the processing of data immediately. To apply the changes you must restart Kaspersky Embedded Systems Security.

   To use the KMP service you need to sign the corresponding agreement and execute configuration files on a protected computer.

   To use the KMP service the data processing terms of KSN Statement on the **Statistics and services** tab must be accepted.

8. Click **OK**.

   The data processing configuration will be saved.

Managing KSN Usage via the Application Console

In this section, learn how configure the KSN Usage task and Data handling via the Application Console.

In this section

Configuring KSN Usage task via the Application Console

► *To configure the KSN Usage task, take the following steps:*

1. In the Application Console tree, expand the **Real-Time Computer Protection** node.
2. Select the **KSN Usage** child node.
3. Click the **Properties** link in the details pane.

   The **Task settings** window opens on the **General** tab.

4. Configure the task:
    - In the **Action to perform on KSN untrusted objects** section, specify the action that Kaspersky Embedded Systems Security is to perform if it detects an object identified by KSN as untrusted:
        - **Remove**

          Kaspersky Embedded Systems Security deletes the object with KSN-untrusted status and places a copy of it in Backup.

          This option is selected by default.
        - **Log information**

          Kaspersky Embedded Systems Security records information about the object with KSN-untrusted status in the task log. Kaspersky Embedded Systems Security does not delete the untrusted object.
    - In the **Data transfer** section, restrict the size of files for which the checksum is calculated:
        - Clear or select the **Do not calculate checksum before sending to KSN if file size exceeds (MB)** check box.

          This check box enables or disables calculation of the checksum for files of the specified size for delivery of this information to the KSN service.

          The duration of the checksum calculation depends on the file size.

          If this check box is selected, Kaspersky Embedded Systems Security does not calculate the checksum for files that exceed the specified size (in MB).

          If the check box is cleared, Kaspersky Embedded Systems Security calculates the checksum for files of any size.

          The check box is selected by default.
        - If required, in the field to the right, change the maximum size of files for which Kaspersky Embedded Systems Security calculates the checksum.
5. If needed, configure the task start schedule on the **Schedule** and **Advanced** tabs. For example, you can enable task start by schedule and specify the start frequency of the **At application launch** if you want the task to run automatically when the computer is restarted.

   The application will automatically start the KSN Usage task by schedule.
6. Configure the Data handling (see Section "Configuring Data handling via the Application Console" on page 283) before starting the task.
7. Click **OK**.

The modified settings are applied. The date and time of modifying the settings, as well as information about the task settings before and after modification, are saved in the system audit log.

Configuring Data handling via the Application Console

► *To configure what data will be processed by the KSN services and accept the KSN Statement:*

1. In the Application Console tree, expand the **Real-Time Computer Protection** node.
2. Select the **KSN Usage** child node.

3. Click the **Data handling** link in the details pane.

   The **Data handling** window opens.

4. On the **Statistics and services** tab, read the Statement and select the **I accept the terms of the Kaspersky Security Network Statement** check box.

5. To increase the protection level, the following check boxes are automatically selected:

   - **Send data about scanned files**.

     If the check box is selected, Kaspersky Embedded Systems Security sends the checksum of scanned files to the Kaspersky Lab. Conclusion about each file security is based on the reputation received from KSN.

     If the check box is cleared, Kaspersky Embedded Systems Security does not send checksum of files to KSN.

     Note, than the file reputation requests might be sent in a limited mode. The limitations are used for protection of the Kaspersky Lab reputation servers from the DDoS attacks. In this scenario, the parameters of file reputation requests, that are being sent, are defined by the rules and methods established by the Kaspersky Lab experts and cannot be configured by user on a protected computer. Updates of these rules and methods are received along with the application database updates. If the limitations are applied, the *Enabled by Kaspersky Lab for protecting KSN servers against DDoS* status is displayed in the KSN Usage task statistics.

     The check box is selected by default.

   - **Send Kaspersky Security Network statistics.**

     If the check box is selected the Kaspersky Embedded Systems Security sends additional statistics, which may contain personal data. The list of all data, that is sent as KSN statistics, is specified in the KSN Statement. The data received by Kaspersky Lab is used to improve the quality of applications and level of threat detection rates.

     If the check box is cleared, Kaspersky Embedded Systems Security does not send additional statistics.

     The check box is selected by default.

   You can clear these check boxes and stop sending additional data at any moment.

6. On the **Kaspersky Managed Protection** tab, read the Statement and select the **I accept the terms of the Kaspersky Managed Protection Statement** check box.

   If the check box is selected, you agree to send statistics on the protected computer activity to the Kaspersky Lab specialists. Received data is used for around-the-clock analysis and reporting, required to prevent security breach incidents.

   The check box is cleared by default.

The changes of **I accept the terms of the Kaspersky Managed Protection Statement** check box state do not start or stop the processing of data immediately. To apply the changes you must restart Kaspersky Embedded Systems Security.

To use the KMP service you need to sign the corresponding agreement and execute configuration files on a protected computer.

> To use the KMP service the data processing terms of KSN Statement on the **Statistics and services** tab must be accepted.

7. Click **OK**.

The data processing configuration will be saved.

Configuring additional data transfer

Kaspersky Embedded Systems Security can be configured to send the following data to Kaspersky Lab:

- Checksums of scanned files (**Send data about scanned files** check box).
- Additional statistics, including personal data (**Send Kaspersky Security Network statistics** check box).

> See the "Local data handling" section of this guide for detailed information about data that is sent to Kaspersky Lab.

The corresponding check boxes can be selected or cleared (see Section "Configuring Data handling via the Application Console" on page 283) only if the **I accept the terms of the Kaspersky Security Network Statement** check box is selected.

By default Kaspersky Embedded Systems Security sends checksums of files and additional statistics after you accept the KSN Statement.

Table 45. Possible check box states and corresponding conditions

Check box state	**Conditions for the** Send data about scanned files **check box state**	**Conditions for the** Send Kaspersky Security Network statistics **check box state**	**Conditions for the** Send data about scanned URLs **check box state**	**Conditions for the** I accept the terms of the Kaspersky Managed Protection Statement **check box state**	**Conditions for the** I accept the terms of the Kaspersky Security Network Statement **check box state**
☑	• reputation requests are sent • check box is editable	• additional statistics is sent • check box is editable	• data about scanned URLs is sent • check box is editable	• the terms of the Kaspersky Managed Protection Statement are accepted • check box is editable	• the terms of the Kaspersky Security Network Statement are accepted • check box is editable
☑	• reputation requests are sent • check box is not editable	• additional statistics is sent • check box is not editable	• data about scanned URLs is sent • check box is not editable	• the terms of the Kaspersky Managed Protection Statement are accepted • check box is not editable	• the terms of the Kaspersky Security Network Statement are accepted • check box is not editable
□	• reputation requests are not sent • check box is editable	• additional statistics is not sent • check box is editable	• data about scanned URLs is not sent • check box is editable	• the terms of the Kaspersky Managed Protection Statement are not accepted • check box is editable	• the terms of the Kaspersky Security Network Statement are not accepted • check box is editable
□	• reputation requests are not sent • check box is not editable	• additional statistics is not sent • check box is not editable	• data about scanned URLs is not sent • check box is not editable	• the terms of the Kaspersky Managed Protection Statement are not accepted • check box is not editable	• the terms of the Kaspersky Security Network Statement are not accepted • check box is not editable

KSN Usage task statistics

While the KSN Usage task is being executed, detailed information can be viewed in real time about the number of objects processed by Kaspersky Embedded Systems Security since it was started up till now. Information about all events that occur during the task performing is recorded in the task log (see Section "About task logs" on page 203).

► *To view KSN Usage task statistics take the following steps:*

1. In the Application Console tree, expand the **Real-Time Computer Protection** node.
2. Select the **KSN Usage** child node.

Task statistics are displayed in the **Statistics** section of the details pane of the selected node.

You can view information about objects processed by Kaspersky Embedded Systems Security since the task was started (see the table below).

Table 46. KSN Usage task statistics

Field	Description
Request sending errors	Number of KSN requests whose processing resulted in a task error.
Statistics formed	Number of generated statistic packages sent to KSN.
Objects removed	Number of objects that Kaspersky Embedded Systems Security deleted when running the KSN Usage task.
Moved to Backup	The number of object copies that Kaspersky Embedded Systems Security saved to Backup.
Objects not removed	The number of objects that Kaspersky Embedded Systems Security attempted but was unable to delete, because, for example, access to the object was blocked by another application. Information about such objects is recorded in the task log.
Objects not backed up	The number of objects the copies of which Kaspersky Embedded Systems Security attempted to save in Backup but was unable to do so, for example, due to insufficient disk space. The application does not disinfect or delete files that it could not move to Backup. Information about such objects is recorded in the task log.
Limited mode	The status signifies whether the application sends file reputation requests in a limited mode.

Applications Launch Control

This section contains information about the Applications Launch Control task and how to configure it.

In this chapter

About the Applications Launch Control task

When running the Applications Launch Control task, Kaspersky Embedded Systems Security monitors user's attempts to start applications and allows or denies start of these applications. The Applications Launch Control task relies on the Default Deny principle, which means that any applications that are not allowed in the task settings will be blocked automatically.

You can allow applications to start using one of the following methods:

- Set allowing rules for trusted applications.
- Check trusted applications reputation in KSN on launch.

The task gives top priority to denying the start of applications. For example, if an application is prevented from starting by one of the blocking rules, the application start will be denied regardless of the trusted conclusion for KSN. At that, if the application is not trusted by the KSN services but is included in the scope of an allowing rule, the application start will be denied.

All attempts to start applications are recorded in the task log (see Section "About task logs" on page 203).

The Applications Launch Control task can operate in one of two modes:

- **Active**. Kaspersky Embedded Systems Security uses a set of rules to control the start of applications that fall within the scope of the Applications Launch Control rules. The scope of the Applications Launch Control rules is specified in the settings of this task. If an application falls within the scope of the Applications Launch Control rules, and the task settings do not satisfy any specified rule, the application launch will be denied.

  Launches of applications that do not fall within the scope of any rule specified in the Applications Launch Control task settings are allowed regardless of the Applications Launch Control task settings.

The **Applications Launch Control** task cannot be started in Active mode if no rules have been created or if there are more than 65,535 rules for one computer.

- **Statistics only**. Kaspersky Embedded Systems Security does not use Applications Launch Control rules to allow or deny the start of applications. Instead, it only records information about application starts, rules satisfied by running applications, and actions that would have been performed if the task was running in **Active** mode. All applications are allowed to start. This mode is set by default.

  You can use this mode to create Applications Launch Control rules (see Section "Creating allowing rules from Applications Launch Control task events" on page 332) based on information recorded in the task log.

You can configure the Applications Launch Control task according to one of the following scenarios:

- Advanced rule configuration (see Section "About Applications Launch Control rules" on page 289) and usage for Application Launch Control.
- Basic rules configuration and KSN usage (see Section "Configuring KSN usage" on page 325) for Application Launch Control.

If operating system files fall within the scope of the Applications Launch Control task, we recommend that when creating Applications Launch Control rules you make sure that such applications are allowed by the newly created rules. Otherwise, the operating system may fail to start.

Kaspersky Embedded Systems Security also intercepts processes launched under the Windows Subsystem for Linux (except for scripts run from the UNIX™ shell, or command line interpreters). For such processes, the Applications Launch Control task applies the action defined by the current configuration. The Rule Generator for Applications Launch Control task detects application launches and generates corresponding rules for applications running under the Windows Subsystem for Linux.

About Applications Launch Control rules

How Applications Launch Control rules work

The operation of Applications Launch Control rules is based on the following components:

- Type of rule.

  Applications Launch Control rules can allow or deny the start of application. Accordingly, they are called *allowing* or *denying* rules. To create a list of allowing rules for Applications Launch Control, you can use the the Rule Generator for generating allowing rules or use the Applications Launch Control task in **Statistics only** mode. You can also add allowing rules manually.
- User and / or user group.

  Applications Launch Control rules can control the start of specified applications by a user and / or user group.
- Rule usage scope.

  Applications Launch Control rules can be applied to *executable files, scripts,* and *MSI packages*.
- Rule-triggering criterion.

Applications Launch Control rules control the launch of files that satisfy one of the criteria specified in the rule settings: signed by the specified *digital certificate*, matching the specified *SHA256 hash*, or located at the specified *path*.

If **Digital certificate** is set as the rule-triggering criterion, the created rule controls the start of all trusted applications in the operating system. You can set stricter conditions for this criterion by selecting the following check boxes:

- **Use subject**

  The check box either enables or disables the use of the subject of the digital certificate as a rule-triggering criterion.

  If the check box is selected, the specified digital certificate subject is used as a rule-triggering criterion. The created rule will control the start of applications only for the vendor specified in the subject.

  If the check box is cleared, the application will not use the subject of the digital certificate as a rule-triggering criterion. If the **Digital certificate** criterion is selected, the created rule will control the start of applications signed with a digital certificate containing any subject.

  The subject of the digital certificate used to sign the file can be specified only from the properties of the selected file using the **Set rule triggering criterion from file properties** button located above the **Rule triggering criterion** section.

  The check box is cleared by default.

- **Use thumb**

  The check box enables / disables the use of the thumbprint of the digital certificate as a rule-triggering criterion.

  If the check box is selected, the specified digital certificate thumbprint is used as a rule-triggering criterion. The created rule will control the start of applications signed with a digital certificate with the specified thumbprint.

  If the check box is cleared, the application will not use the thumbprint of the digital certificate as a rule-triggering criterion. If the **Digital certificate** criterion is selected, the application will control the start of applications signed with a digital certificate with any thumbprint.

  The thumbprint of the digital certificate used to sign the file can be specified only from the properties of the selected file using the **Set rule triggering criterion from file properties** button located above the **Rule triggering criterion** section.

  The check box is cleared by default.

Thumbprints allow for the most restrictive triggering of application start rules based on a digital certificate, because a thumbprint uniquely identifies a digital certificate and cannot be forged, unlike the subject of a digital certificate.

You can specify exclusions for Applications Launch Control rules. Exclusions to Applications Launch Control rules are based on the same criteria used to trigger rules: digital certificate, SHA256 hash, and file path. Exclusions to Applications Launch Control rules may be required for certain allowing rules: for example, if you want to allow users to start applications from the C:\Windows path, while blocking launch of the Regedit.exe file.

If operating system files fall within the scope of the Applications Launch Control task, we recommend that when creating Applications Launch Control rules you make sure that such applications are allowed by the newly created rules. Otherwise, the operating system may fail to start.

Managing Applications Launch Control rules

You can perform the following actions with Applications Launch Control rules:

- Add rules manually.
- Generate and add rules automatically.
- Remove rules.
- Export rules to file.
- Check selected files for rules that allow execution of these files.
- Filter the rules in the list according to specified criterion.

About Software Distribution Control

Generating Applications Launch Control rules can be complicated if you also need to control software distribution on a protected computer, for example, on computers where installed software is periodically automatically updated. In this case, the list of allowing rules must be updated after each software update for newly created files to be considered in the Applications Launch Control task settings. To simplify launch control in software distribution scenarios, you can use the Software Distribution Control subsystem.

A software distribution package (hereinafter referred to as “package”) represents a software application to be installed on a computer. Each package contains at least one application and may also contain individual files, updates, or even an individual command, in addition to applications, particularly when you are installing a software application or update.

The Software Distribution Control subsystem is implemented as an additional list of exclusions. When you add a software distribution package to this list, the application allows these trusted packages to be decompressed and allows software installed or modified by a trusted package to be started automatically. The extracted files can inherit the trusted attribute of the primary distribution package. *A primary distribution package* is a package that has been added to the list of Software Distribution Control exclusions by a user and has become a trusted package.

Kaspersky Embedded Systems Security controls only full software distribution cycles. The application cannot correctly process the launch of files modified by a trusted package if, when the package is started for the first time, software distribution control is turned off or the Application Launch Control component is not installed.

Software distribution control is not available if the **Apply rules to executable files** check box is cleared in the Applications Launch Control task settings.

Software distribution cache

Kaspersky Embedded Systems Security uses a dynamically generated software distribution cache (“distribution cache”) to establishes the relationship between trusted packages and files created during software distribution. When a package is first started, Kaspersky Embedded Systems Security detects all files created by the package during the software distribution process and stores file checksums and paths in the distribution cache. Then all files in the distribution cache are allowed to start by default.

You cannot review, clear or manually modify the distribution cache via the user interface. The cache is populated and controlled by Kaspersky Embedded Systems Security.

You can export the distribution cache to a configuration file (XML format) and clear the cache using command line options.

► *To export the distribution cache to a configuration file, execute the following command:*

```
kavshell appcontrol /config /savetofile:<full path> /sdc
```

► *To clear the distribution cache, execute the following command:*

```
kavshell appcontrol /config /clearsdc
```

Kaspersky Embedded Systems Security updates the distribution cache every 24 hours. If the checksum of a previously allowed file is changed, the application deletes the record for this file from the distribution cache. If the Applications Launch Control task is started in Active mode, subsequent attempts to start this file will be blocked. If the full path to the previously allowed file is changed, subsequent attempts to start this file will not be blocked, because the checksum is stored within the distribution cache.

Processing the extracted files

All files extracted from a trusted package inherit the trusted attribute upon first launch of the package. If you clear the check box after first launch, all files extracted from the package will retain the inherited attribute. To reset the inherited attribute on all extracted files, you need to clear the distribution cache and clear the **Allow launching to all files from this distribution package extraction chain** check box before starting the trusted distribution package again.

Extracted files and packages created by a trusted primary distribution package inherit the trusted attribute when their checksums are added to the distribution cache when the software distribution package in the exclusion list is opened for the first time. Hence, the distribution package itself and all files extracted from this package will also be trusted. By default, the number of levels of inheritance of the trusted attribute is unlimited.

Extracted files will retain the trusted attribute after the operating system restarts.

The processing of files is configured in the Software Distribution Control settings (see Section "Configuring Software Distribution Control" on page 304) by selecting or clearing the **Allow launching to all files from this distribution package extraction chain** check box.

For example, suppose you add a test.msi package containing several other packages and applications to the exclusions list and select the check box. In this case, all packages and applications contained in the test.msi package are allowed to run or be extracted if they contain other files. This scenario works for extracted files on all nested levels.

If you add a test.msi package to the exclusions list and clear the **Allow launching to all files from this distribution package extraction chain** check box, the application will assign the trusted attribute only to the packages and executable files extracted directly from the primary trusted package (on the first level of nesting). The checksums of such files are stored in the distribution cache. All files on the second level of nesting and beyond will be blocked by the Default Deny principle.

Working with the Applications Launch Control rule list

The list of trusted packages of software distribution control subsystem is a list of exclusions, which amplifies, but does not replace the general list of applications launch control rules.

Denying applications launch control rules have the highest priority: trusted package decompression and start of new or modified files will be blocked, if these packages and files are affected by the applications launch control denying rules.

Software distribution control exclusions are applied both for trusted packages and files created or modified by these packages, if no denying rules in the applications launch control list are applied for those packages and files.

Using KSN conclusions

KSN conclusions that a file is untrusted have a higher priority than the software distribution control exclusions: decompression of trusted packages and start of files created or modified by these packages will be blocked if KSN reports that these files are untrusted.

After unpacking from a trusted package, all child files will be allowed to run regardless of KSN usage within the Applications Launch Control scope. At that, states of **Deny applications untrusted by KSN** and **Allow applications trusted by KSN** check boxes do not affect the operation of the **Allow launching to all files from this distribution package extraction chain** check box.

About KSN usage for the Applications Launch Control task

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

If KSN data about an application’s reputation is used by the Applications Launch Control task, the KSN application reputation is considered a criterion for allowing or denying launch of that application. If KSN reports to Kaspersky Embedded Systems Security that an application is untrusted when the user attempts to launch the application, the application launch is denied. If KSN reports to Kaspersky Embedded Systems Security that the application is trusted when the user attempts to launch the application, the application launch is allowed. KSN can be used along with Applications Launch Control rules or as an independent criterion for denying launch of applications.

Using KSN conclusions as independent criterion for denying application launch

This scenario lets you securely control application launches on a protected computer without requiring advanced configuration of the rule list.

You can apply KSN conclusions to Kaspersky Embedded Systems Security together with the only specified rule. The application will only allow the start of applications that are trusted in KSN or are allowed by a specified rule.

> For such a scenario, we recommend that you set a rule allowing start of the application based on a digital certificate.

All other applications are denied in accordance with the Default Deny policy. Using KSN when no rules are applied protects a computer from applications that KSN considers to be a threat.

Using KSN conclusions simultaneously with Applications Launch Control rules

When using KSN conclusions simultaneously with Applications Launch Control rules, the following conditions apply:

- Kaspersky Embedded Systems Security always denies launch of an application if it is included in the scope of at least one denying rule. If the application is considered trusted by KSN, the corresponding conclusion has a lower priority and is not considered; the application launch will still be denied. This lets you expand the list of unwanted applications.
- Kaspersky Embedded Systems Security always denies the launch of an application if the launch of applications not trusted in KSN is prohibited and the application is not trusted in KSN. If an allowing rule is set for the application, it has a lower priority and is not considered; the application launch will still be denied. This protects the computer from applications that KSN considers to be a threat but were not considered during initial configuration of the rules.

Generating Applications Launch Control rules

You can create lists of Applications Launch Control rules using Kaspersky Security Center tasks and policies simultaneously for all computers and groups of computers on the corporate network. This scenario is recommended if the corporate network does not have a reference machine and you are unable to create a list of allowing rules based on applications installed on the reference machine.You can also run the Rule Generator for Applications Launch Control task locally via the Application Console to create a list of rules based on the applications running on a single computer.

The Applications Launch Control component is installed with two preset allowing rules:

- Allowing rule for scripts and MSI files with a certificate trusted by the operating system.
- Allowing rule for executable files with a certificate trusted by the operating system.

You can create lists of Applications Launch Control rules on the side of Kaspersky Security Center in one of the following ways:

- Using a Rule Generator for Applications Launch Control group task.

  Under this scenario, a group task generates its own list of Applications Launch Control rules for each computer on the network and saves those lists to an XML file in the specified shared folder. The XML file generated by the Rule Generator for Applications Launch Control task contains the allowing rules specified in task settings before the task starts.No rules will be created for applications that are not allowed to start in the specified task settings. The start of such applications is denied by default. You can then manually import the created list of rules into the Applications Launch Control task for the Kaspersky Security Center policy. You can configure a Kaspersky Security Center policy to automatically add the created rules to the Applications Launch Control rule list when the Rule Generator for Applications Launch Control group task is finished.

You can configure the generated rules to be automatically imported into the list of rules for the Applications Launch Control task.

This scenario is recommended when you need to quickly create lists of Applications Launch Control rules. We recommend that you configure the scheduled launch of the Rule Generator for Applications Launch Control task only if the applied allowing rules include folders and files you know to be safe.

> Before using the Applications Launch Control task in the network, make sure that all protected computers have access to a shared folder. If the organization’s policy does not provide for the use of a shared folder in the network, we recommend that you start the Rule Generator for Applications Launch Control task on a computer in the test computers group or on a reference machine.

- Based on a report of task events generated in Kaspersky Security Center by the Applications Launch Control task running in **Statistics only** mode.

  Under this scenario, Kaspersky Embedded Systems Security does not deny the launch of applications. Instead, with Applications Launch Control running in the **Statistics only** mode, it reports all allowed and denied application launches across all network computers in the **Events** tab of the Administration Server node's workspace in the Kaspersky Security Center. Kaspersky Security Center uses the task log to generate a single list of events in which application launches were denied.

  You need to configure the task execution period so that all possible scenarios involving the protected computers and computer groups, and at least one computer restart are performed during the specified time period. After rules are added to the Applications Launch Control task, you can import application launch data from the saved Kaspersky Security Center event report (TXT format) and generate Applications Launch Control allowing rules for such applications based on this data.

  This scenario is recommended if a corporate network includes a large number of computers of different type (with a different software installed).

- Based on denied application launch events received through Kaspersky Security Center, without creating and importing a configuration file.

  To use this feature, the Applications Launch Control task on the local computer must be running under an active Kaspersky Security Center policy. In this case, all events on the local computer are sent to the Administration Server.

We recommend that you update the list of rules when the set of applications installed on network computers changes (for example, when updates are installed or operating systems are reinstalled). We recommend that you generate an updated list of rules by running the Rule Generator for Applications Launch Control task or the Applications Launch Control task in **Statistics only** mode on computers in the test administration group. The test administration group includes the computers required to test the launch of new applications before they are installed on network computers.

> XML files containing lists of allowing rules are created based on an analysis of tasks started on the protected computer. To account for all applications used on the network when generating lists of rules you are advised to start the Rule Generator for Applications Launch Control task and the Applications Launch Control task in **Statistics only** mode on a reference machine.

Before generating allowing rules based on the applications launched on a reference machine, make sure that the reference machine is secure and there is no malware on it.

Before adding allowing rules, select one of the available rule application modes. The list of Kaspersky Security Center policy rules displays only rules specified by the policy, regardless of the rule application mode. The local rule list includes all applied rules — both local rules and rules added through a policy.

Default Applications Launch Control task settings

By default, the Applications Launch Control task has the settings described in the table below. You can change the values of these settings.

Table 47. Default Applications Launch Control task settings

Setting	Default Value	Description
Task mode	**Statistics only**. The task records denied launch events and allowed launch events based on the set rules. Application launch is not actually denied.	You can select **Active** mode after the final list of rules is generated.
Repeat actions taken for the first file launch on all the subsequent launches for this file	Applied	You can repeat actions taken for the first file launch on all the subsequent launches for this file.
Deny the command line interpreters launch with no command to execute	Not applied.	You can deny launch of command interpreters with no command to execute.
Rules managing	**Replace local rules with policy rules**	You can select a mode in which rules specified in a policy are applied together with the rules on the local computer.

Setting	Default Value	Description
Rules usage scope	The task controls the launch of executable files, scripts, and MSI packages. It also monitors loading of DLL modules.	You can specify the file types for which launch is controlled by rules.
KSN Usage	KSN application reputation data is not used.	You can use KSN application reputation data when running the Applications Launch Control task.
Automatically allow software distribution for applications and packages listed	Not applied.	You can allow software distribution using the installers and applications specified in the settings. By default, software distribution is only allowed using the Windows Installer service.
Always allow software distribution via Windows Installer	Applied (can be changed only when the **Automatically allow software distribution for applications and packages listed** setting is enabled).	You can allow any software installation or update if the operations are performed via Windows Installer.
Always allow software distribution via SCCM using the Background Intelligent Transfer Service	Not applied (can be changed only when the **Automatically allow software distribution for applications and packages listed** setting is enabled).	You can turn on or off automatic software distribution using the System Center Configuration Manager.
Task start	First run is not scheduled.	The Applications Launch Control task does not start automatically at start of Kaspersky Embedded Systems Security. You can start the task manually or configure a scheduled start.

Table 48. Rule Generator for Applications Launch Control task default settings

Setting	Default Value	Description
Prefix for allowing rules names	Identical to the name of the computer on which Kaspersky Embedded Systems Security is installed.	You can change the prefix for names of allowing rules.
Allowing rules usage scope	The scope of allowing rules includes the following file categories by default: • Files with the EXE extension located in the folders C:\Windows, C:\Program Files (x86) and C:\Program Files • MSI packages stored in the C:\Windows folder • Scripts stored in the C:\Windows folder The task also creates rules for all running applications, regardless of their location and format.	You can change the protection scope by adding or removing folder paths and specifying the types of files that will be allowed to launch by the automatically generated rules. You can also ignore running applications when creating allowing rules.
Criteria for generation of allowing rules	The digital certificate subject and thumbprint are used; rules are generated for all users and groups of users.	You can use the SHA256 hash when generating allowing rules. You can select a user and group of users for which allowing rules need to be automatically generated.
Actions upon task completion	Allowing rules are added to the list of Applications Launch Control rules; new rules are merged with existing rules; duplicate rules are removed.	You can add rules to the existing rules without merging them and without deleting duplicate rules, or replace existing rules with the new allowing rules, or configure export of the allowing rules to a file.
Task launch settings with permissions	The task is started under a system account.	You can allow the Rule Generator for Applications Launch Control task to start under a system account or using the permissions of a specified user.
Task start schedule	First run is not scheduled.	The Rule Generator for Applications Launch Control task does not start automatically when Kaspersky Embedded Systems Security starts. You can start the task manually or configure a scheduled start.

Managing Applications Launch Control via the Administration Plug-in

In this section, learn how to navigate the Administration Plug-In interface and configure task settings for one or all computers on the network.

In this section

Navigation

Learn how to navigate to the required task settings via the interface.

In this section

Opening policy settings for the Applications Launch Control task

► *To open the Applications Launch Control task settings via the Kaspersky Security Center policy:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure the task.
3. Select the **Policies** tab.
4. Double-click the policy name you want to configure.
5. In the **Properties: <Policy name>** window that opens, select the **Local activity control** section.
6. Click the **Settings** button in the **Applications Launch Control** subsection.

   The **Applications Launch Control** window opens.

Configure the policy as required.

Opening the Applications Launch Control rules list

► *To open the Applications Launch Control rules list via the Kaspersky Security Center:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure the task.
3. Select the **Policies** tab.
4. Double-click the policy name you want to configure.
5. In the **Properties: <Policy name>** window that opens, select the **Local activity control** section.
6. Click the **Settings** button in the **Applications Launch Control** subsection.

   The **Applications Launch Control** window opens.
7. On the **General** tab, click the **Rules list** button.

   The **Applications Launch Control rules** window opens.

Configure the rules list as required.

Opening the Rule Generator for Applications Launch Control task wizard and properties

► *To start creating a Rule Generator for Applications Launch Control task:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure the task.
3. Select the **Tasks** tab.
4. Click **Create a task** button.

   The **New Task Wizard** window opens.
5. Select the **Rule Generator for Applications Launch Control** task.
6. Click **Next**.

   The **Settings** window opens.

► *To configure the existing Rule Generator for Applications Launch Control task:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure the task.
3. Select the **Tasks** tab.
4. Double-click the task name in the list of Kaspersky Security Center tasks.

   The **Properties: Rule Generator for Applications Launch Control** window opens.

See the Configuring the Rule Generator for Applications Launch Control task section for details on configuring the task.

Configuring Applications Launch Control task settings

► *To configure general Applications Launch Control task settings:*

1. Open the **Applications Launch Control** (see Section "**Opening policy settings for the Applications Launch Control task**" on page 299) window.
2. On the **General** tab, select the following settings in the **Task mode** section:
   - In the **Task mode** drop-down list, specify the task mode.

     In this drop-down list, you can select the Applications Launch Control task's mode:

     - **Active**. Kaspersky Embedded Systems Security uses the specified rules to control the launch of any application.
     - **Statistics only**. Kaspersky Embedded Systems Security does not use the specified rules to control application launches. Instead, it simply records information about launch events in the task log. All applications are allowed to start. You can use this mode to generate a list of Applications Launch Control rules based on the information about denied application launches recorded in the task log.

     By default, the Applications Launch Control task runs in **Statistics only** mode.
   - Clear or select the **Repeat action taken for the first file launch on all the subsequent launches for this file** check box.

     The check box enables or disables launch control for the second and subsequent attempts to start applications based on the event information stored in the cache.

     If the check box is selected, Kaspersky Embedded Systems Security allows or denies subsequent launches of an application based on the task's conclusion regarding the first launch of the application. For example, if the first application launch was allowed by the rules, information about this decision will be stored in the cache, and the second and all subsequent launches will also be allowed without rechecking.

     If the check box is cleared, Kaspersky Embedded Systems Security analyzes an application every time a launch is attempted.

     The check box is selected by default.
   - Clear or select the **Deny the command line interpreters launch with no command to execute** check box.

     If the check box is selected, Kaspersky Embedded Systems Security denies the launch of command line interpreters even if launching interpreters is allowed. A command interpreter can only be launched with no command if both of the following conditions are met:

     - Launch of the command line interpreter is allowed.
     - The command to be executed is allowed.

     If the check box is cleared, Kaspersky Embedded Systems Security only considers allowing rules when launching a command line interpreter. The launch is denied if no allowing rule applies or the executable process is not trusted by KSN. If an allowing rule applies or the process is trusted by KSN, a command line interpreter can be launched with or without a command to execute.

Kaspersky Embedded Systems Security recognizes the following command line interpreters:

- cmd.exe
- powershell.exe
- python.exe
- perl.exe

The check box is cleared by default.

3. In the **Rules managing** section, configure settings for applying rules:

   a. Click the **Rules list** button to add allowing rules for the Applications Launch Control task.

   > Kaspersky Embedded Systems Security does not recognize paths that contain slashes ("/"). Use backslash ("\") to enter the path correctly.

   b. Select the mode for applying rules:

   - **Replace local rules with policy rules**.

     The application applies the rule list specified in the policy for centralized application launch control on a group of computers. Local rule lists cannot be created, edited, or applied.

   - **Add policy rules to the local rules**.

     The application applies the rule list specified in a policy together with local rule lists. You can edit the local rule lists using the Rule Generator for Applications Launch Control task.

   > By default, Kaspersky Embedded Systems Security applies two preset rules that allow a list of scripts, MSI packages, and executable files if these objects are signed with a trusted digital signature.

4. In the **Rules usage scope** section, specify the following settings:

   - **Apply rules to executable files**.

     The check box either enables or disables launch control of executable files.

     If this check box is selected, Kaspersky Embedded Systems Security allows or blocks start of executable files using the specified rules whose settings specify **Executable files** as the scope.

     If the check box is cleared, Kaspersky Embedded Systems Security does not control start of executable files using the specified rules. Startup of executable files is allowed.

     The check box is selected by default.

   - **Monitor loading of DLL modules**.

     The check box either enables or disables control of loading of DLL modules.

     If this check box is selected, Kaspersky Embedded Systems Security allows or blocks loading of DLL modules using the specified rules whose settings specify **Executable files** as the scope.

     If this check box is cleared, Kaspersky Embedded Systems Security does not control loading of DLL modules using the specified rules. Loading of DLL modules is allowed.

The check box is active if the **Apply rules to executable files** check box is selected.

The check box is cleared by default.

> Controlling loading of DLL modules may affect the performance of the operating system.

- **Apply rules to scripts and MSI packages**.

  The check box either enables or disables launch of scripts and MSI packages.

  If this check box is selected, Kaspersky Embedded Systems Security allows or blocks start of scripts and MSI packages using the specified rules whose settings specify Scripts and MSI packages as the scope.

  If the check box is cleared, Kaspersky Embedded Systems Security does not control start of scripts and MSI packages using specified rules. Start of scripts and MSI packages is allowed.

  The check box is selected by default.

5. In the **KSN Usage** group box, configure the following application launch settings:

   - **Deny applications untrusted by KSN**.

     The check box either enables or disables Applications Launch Control according to application reputation data in KSN.

     If this check box is selected, Kaspersky Embedded Systems Security blocks any application from running if it is not trusted in KSN. Applications Launch Control allowing rules that apply to applications not trusted in KSN will not be triggered. Selecting the check box provides additional protection from malware.

     If the check box is cleared, Kaspersky Embedded Systems Security does not consider the reputation of applications not trusted in KSN and allows or blocks start in accordance with the rules that apply to such applications.

     The check box is cleared by default.

   - **Allow applications trusted by KSN**.

     The check box either enables or disables Applications Launch Control according to application reputation data in KSN.

     If this check box is selected, Kaspersky Embedded Systems Security allows applications to run if they are trusted in KSN. Denying application launch control rules that apply to KSN-trusted applications have higher priority: if an application is trusted by KSN services, the application launch will be denied.

     If the check box is cleared, Kaspersky Embedded Systems Security does not consider the reputation of KSN-trusted applications and allows or denies launch in accordance with rules that apply to such applications.

     The check box is cleared by default.

   - Users and / or user groups allowed to launch applications trusted in KSN.

6. On the **Software Distribution Control** tab, configure the settings for software distribution control (see Section "Configuring Software Distribution Control" on page 304).

7. On the **Task management** tab, configure the scheduled task start settings (see Section "Configuring the task start schedule settings" on page 129).

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

Kaspersky Embedded Systems Security immediately applies the new 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 system audit log.

Configuring Software Distribution Control

► *To add a trusted distribution package:*

1. Open the **Applications Launch Control** window (see Section "Opening policy settings for the Applications Launch Control task" on page 299).
2. On the **Software Distribution Control** tab, select the **Automatically allow software distribution for applications and packages listed** check box.

   The check box enables and disables automatic creation of exclusions for all files started using the distribution packages specified in the list.

   If the check box is selected, the application automatically allows files in the trusted distribution packages to start. The list of applications and distribution packages allowed to start can be edited.

   If the check box is cleared, the application does not apply the exclusions specified in the list.

   The check box is cleared by default.

   > You can select the **Automatically allow software distribution for applications and packages listed**, if the **Apply rules to executable files** check box in the **General** tab is selected in the **Applications Launch Control** task settings.

3. Clear the **Always allow software distribution via Windows Installer** check box if required.

   The check box enables and disables automatic creation of exclusions for all files executed via Windows Installer.

   If the check box is selected, files installed via Windows Installer will always be allowed to start.

   If the check box is cleared, files will not be allowed to start unconditionally, even if they are started via Windows Installer.

   The check box is selected by default.

   The check box is not editable if the **Automatically allow software distribution for applications and packages listed** check box is not selected.

   > Clearing the **Always allow software distribution via Windows Installer** check box is only recommended if it is absolutely necessary. Turning off this function may cause issues with updating operating system files and also prevent the launch of files extracted from a distribution package.

4. If required, select the **Always allow software distribution via SCCM using the Background Intelligent Transfer Service** check box.

   The check box turns on or off automatic software distribution using the System Center Configuration Manager.

   If the check box is selected, Kaspersky Embedded Systems Security automatically allows Microsoft Windows deployment using the System Center Configuration Manager. The application allows software distribution only via the Background Intelligent Transfer Service.

   The application controls start of objects with the following extensions:

   - .exe
   - .msi

   The check box is cleared by default.

> The application controls the software distribution cycle on the computer — from package delivery to installation or update. The application does not control processes if any stage of distribution was performed before installation of the application on the computer.

5. To edit the list of trusted distribution packages, click **Change packages list** and select one of the following methods in the window that opens:

- **Add one distribution package**.

  a. Click the **Browse** button and select the executable file or distribution package.

     The **Trusting criteria** section is automatically populated with data about the selected file.

  b. Clear or select the **Allow launching to all files from this distribution package extraction chain** check box.

  c. Select one of two available options for criteria to use to determine whether a file or distribution package is trusted:

     - **Use digital certificate**
     - Use SHA256 hash]

- **Add several packages by hash**.

  > You can select an unlimited number of executable files and distribution packages, and add them to the list all at the same time. Kaspersky Embedded Systems Security examines the hash and allows the operating system to launch the specified files.

- **Change selected package**.

  Use this option to select a different executable file or distribution package, or to change the trust criteria.

- **Import distribution packages list from file**.

  You can import the list of trusted distribution packages from a configuration file. To be recognized by Kaspersky Embedded Systems Security, such a file must satisfy the following parameters:

  - The file extension is TXT.
  - The file contains information structured as a list of lines, where each line includes data for one of the trusted files.
  - The file must contain a list in one of the following formats:
    - <file name>:<SHA256 hash>.
    - <SHA256 hash>*<file name>.

  In the **Open** window, specify the configuration file containing a list of trusted distribution packages.

6. If you want to remove a previously added application or distribution package for the trusted list, click the **Delete distribution packages** button. Extracted files will be allowed to run.

   > To prevent extracted files from starting, uninstall the application on the protected computer or create a denying rule in the Applications Launch Control task settings.

7. Click **OK**.

Your newly configured settings are saved.

Configuring the Rule Generator for Applications Launch Control task

► *To configure the Rule Generator for Applications Launch Control task, do the following:*

1. Open the **Properties: Rule Generator for Applications Launch Control** (see Section "**Opening the Rule Generator for Applications Launch Control task wizard and properties**" on page 300) window.
2. In the **Notification** section, configure the task event notification settings.

   > For detailed information regarding configuring settings in this section, see the *Kaspersky Security Center Help*.

3. In the **Settings** section, you can configure the following settings:
   - Add prefix for rule names.
   - Configure the allowing rules usage scope:
     - Create allowing rules based on running applications;
     - Create allowing rules for applications from the specific folders.

4. In the **Options** section, you can specify actions to perform while creating allowing rules for applications launch control:

   - **Use digital certificate**

If this option is selected, the presence of a digital certificate is specified as a rule-triggering criterion in the settings of the newly generated allowing rules for Applications Launch Control. The application will now allow start of programs launched using files with a digital certificate. We recommend this option if you want to allow the start of any applications that are trusted in the operating system.

This option is selected by default.

- **Use digital certificate subject and thumbprint**

  The check box enables or disables the use of the subject and thumbprint of the file's digital certificate as a criterion for triggering the allowing rules for Applications Launch Control. Selecting this check box lets you specify stricter digital certificate verification conditions.

  If this check box is selected, the subject and thumbprint values of the digital certificate of files for which the rules are generated are set as a criterion for triggering the allowing rules for Applications Launch Control. Kaspersky Embedded Systems Security will allow applications that are launched using files with the specified thumbprint and digital certificate.

  Selecting this check box highly restricts the triggering of allowing rules based on a digital certificate because a thumbprint is a unique identifier of a digital certificate and cannot be forged.

  If this check box is cleared, the existence of any digital certificate that is trusted in the operating system is set as a criterion for triggering the allowing rules for Applications Launch Control.

  This check box is active if the **Use digital certificate** option is selected.

  The check box is selected by default.

- **If the certificate is missing, use**

  This is a drop-down list that allows you to select the criterion for triggering an allowing rule for Applications Launch Control if the file used to generate the rule, has no digital certificate.

  - **SHA256 hash**. The checksum of the file used to generate the rule is set as a criterion for triggering the allowing rule for Applications Launch Control. The application will allow start of programs launched using files with the specified checksum.

  - **path to file**. The path to the file used to generate the rule is set as a criterion for triggering the allowing rule for Applications Launch Control. The application will now allow start of programs launched using files located in the folders specified in the **Create allowing rules for applications from the folders** table in the **Settings** section.

- **Use SHA256 hash**

If this option is selected, the checksum of the file used to generate the rule is specified as a rule-triggering criterion in the settings of the newly generated allowing rules for Applications Launch Control. The application will allow start of programs launched using files with the specified checksum.

We recommend this option for cases when the generated rules must achieve the highest level of security: a SHA256 checksum may be used as a unique file ID. Using a SHA256 checksum as a rule-triggering criterion restricts the rule usage scope to one file.

This option is cleared by default.

- **Generate rules for user or group of users**.

  This is a field that displays a user or group of users. The application will control any applications run by the specified user or group of users.

  The default selection is **Everyone**.

You can configure settings for configuration files with allowing rules lists that Kaspersky Embedded Systems Security creates upon the task completion.

1. Configure the task schedule in the **Schedule** section (you can configure a schedule for all task types except Rollback of Database Update).
2. In the **Account** section specify the account which rights will be used for the task execution.
3. If required, specify the objects to exclude from the task scope in the **Exclusions from task scope** section.

   > For detailed information regarding configuring settings in these sections, see the *Kaspersky Security Center Help*.

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

   The newly configured group tasks settings are saved.

Configuring Applications Launch Control rules via the Kaspersky Security Center

Learn how to generate a list of rules based on various criteria or manually create allowing or denying rules using the Application Launch Control task.

In this section

Adding an Applications Launch Control rule

► *To add an Applications Launch Control rule:*

1. Open the **Applications Launch Control rules** window (see Section "Opening the Applications Launch Control rules list" on page 300).
2. Click the **Add** button.
3. In the context menu of the button, select **Add one rule**.

   The **Rule settings** window opens.
4. Specify the following settings:
   a. In the **Name** field, enter the name of the rule.

   b. In the **Type** drop-down list, select the rule type:
      - **Allowing** if you want the rule to allow launch of applications in accordance with the criteria specified in the rule settings.
      - **Denying** if you want the rule to block launch of applications in accordance with the criteria specified in the rule settings.

   c. In the **Scope** drop-down list, select the type of files whose execution will be controlled by the rule:
      - **Executable files** if you want the rule to control launch of executable files.
      - **Scripts and MSI packages** if you want the rule to control launch of scripts and MSI packages.

   d. In the **User or user group** field, specify the users who will be allowed or not allowed to start programs based on the type of rule. To do this, perform the following actions:

      i. Click the **Browse** button.

      ii. The standard Microsoft Windows **Select user or groups** window opens.

      iii. Specify the list of users and/or user groups.

      iv. Click **OK**.

   e. If you want to take the values of the rule-triggering criteria listed in the **Rule triggering criterion** section from a specific file:

      i. Click the **Set rule triggering criterion from file properties** button.

      The standard Microsoft Windows **Open** window opens.

      ii. Select the file.

      iii. Click the **Open** button.

      The criteria values in the file are displayed in the fields in the **Rule triggering criterion** section. The criterion for which data are available in the file properties is selected by default.

   f. In the **Rule triggering criterion** section, select one of the following options:
      - **Digital certificate** if you want the rule to control the start of applications launched using files signed with a digital certificate:
        - Select the **Use subject** check box if you want the rule to control the launch of files signed with a digital certificate only with the specified header.

- Select the **Use thumb** check box if you want the rule to only control the launch of files signed with a digital certificate with the specified thumbprint.

- **SHA256 hash** if you want the rule to control the start of programs launched using files whose checksum matches the one specified.
- **Path to file** if you want the rule to control the start of programs launched using files located at the specified path.

> Kaspersky Embedded Systems Security does not recognize paths that contain slashes ("/"). Use backslash ("\") to enter the path correctly.

g. If you want to add rule exclusions:

i. In the **Exclusions from rule** section, click the **Add** button.

The **Exclusion from rule** window opens.

ii. In the **Name** field, enter the name of the exclusion.

iii. Specify the settings for exclusion of application files from the Applications Launch Control rule. You can fill out the settings fields from the file properties by clicking the **Set exclusion based on file properties** button.

- **Digital certificate**

If this option is selected, the presence of a digital certificate is specified as a rule-triggering criterion in the settings of the newly generated allowing rules for Applications Launch Control. The application will now allow start of programs launched using files with a digital certificate. We recommend this option if you want to allow the start of any applications that are trusted in the operating system.

This option is selected by default.

- **Use subject**

  The check box either enables or disables the use of the subject of the digital certificate as a rule-triggering criterion.

  If the check box is selected, the specified digital certificate subject is used as a rule-triggering criterion. The created rule will control the start of applications only for the vendor specified in the subject.

  If the check box is cleared, the application will not use the subject of the digital certificate as a rule-triggering criterion. If the **Digital certificate** criterion is selected, the created rule will control the start of applications signed with a digital certificate containing any subject.

  The subject of the digital certificate used to sign the file can be specified only from the properties of the selected file using the **Set rule triggering criterion from file properties** button located above the **Rule triggering criterion** section.

  The check box is cleared by default.

- **Use thumb**

  The check box enables / disables the use of the thumbprint of the digital certificate as a rule-triggering criterion.

  If the check box is selected, the specified digital certificate thumbprint is used as a rule-triggering criterion. The created rule will control the start of applications signed with a digital certificate with the specified thumbprint.

  If the check box is cleared, the application will not use the thumbprint of the digital certificate as a rule-triggering criterion. If the **Digital certificate** criterion is selected, the application will control the start of applications signed with a digital certificate with any thumbprint.

The thumbprint of the digital certificate used to sign the file can be specified only from the properties of the selected file using the **Set rule triggering criterion from file properties** button located above the **Rule triggering criterion** section.

The check box is cleared by default.

- **SHA256 hash**

If this option is selected, the checksum of the file used to generate the rule is specified as a rule-triggering criterion in the settings of the newly generated allowing rules for Applications Launch Control. The application will allow start of programs launched using files with the specified checksum.

We recommend this option for cases when the generated rules must achieve the highest level of security: a SHA256 checksum may be used as a unique file ID. Using a SHA256 checksum as a rule-triggering criterion restricts the rule usage scope to one file.

This option is cleared by default.

- **Path to file**

  If the check box is selected, Kaspersky Embedded Systems Security uses the full path to the file to determine whether the process is trusted.

  If the check box is cleared, the path to the file is not used to determine whether the process is trusted.

  The check box is cleared by default.

i. Click **OK**.

ii. If necessary, repeat steps (i)-(iv) to add additional exclusions.

1. Click **OK** in the **Rule settings** window.

   The created rule is displayed in the list in the **Applications Launch Control rules** window.

Enabling the Default Allow mode

Default Allow mode allows all applications to start if they are not blocked by rules or by a conclusion from KSN that they are not trusted. Default Allow mode can be enabled by adding specific allowing rules. You can enable Default Allow for only scripts or for all executable files.

► *To add a Default Allow rule:*

1. Open the **Applications Launch Control rules** (see Section "**Opening the Applications Launch Control rules list**" on page 300) window.
2. Click the **Add** button and, in the button’s context menu, select **Add one rule**.

   The **Rule settings** window opens.
3. In the **Name** field, enter the name of the rule.
4. In the **Type** drop-down list, select the **Allowing** rule type.

5. In the **Scope** drop-down list, select the type of files whose execution will be controlled by the rule:
   - **Executable files** if you want the rule to control the launch of executable files.
   - **Scripts and MSI packages** if you want the rule to control the launch of scripts and MSI packages.
6. In the **Rule triggering criterion** section, select the **Path to file** option.
7. Enter the following mask: `?:\`
8. Click **OK** in the **Rule settings** window.

Kaspersky Embedded Systems Security applies the Default Allow mode.

Creating allowing rules from Kaspersky Security Center events

► *To generate allowing rules for applications from Kaspersky Security Center events in Applications Launch Control:*

1. Open the **Applications Launch Control rules** (see Section "**Opening the Applications Launch Control rules list**" on page 300) window.
2. Click the **Add** button and, in the button’s context menu, select **Create allowing rules for applications from Kaspersky Security Center events**.
3. Select the principle for adding the rules to the list of previously created Application Launch Control rules:
   - **Add to existing rules** if you want to add the imported rules to the list of existing rules. Rules with identical settings are duplicated.
   - **Replace existing rules** if you want to replace the existing rules with the imported rules.
   - **Merge with existing rules** if you want to add the imported rules to the list of existing rules. Rules with identical settings are not added; the rule is added if at least one rule parameter is unique.

   The **Applications launch control rules generation** window opens.
4. Configure the following request settings:
   - **Administration Server address**
   - **Port**
   - **User**
   - **Password**
5. Select the types of events that you want the rule generation task to use:
   - **Statistics only mode: application launch denied**.
   - **Application launch denied**.
6. Select the time period from the **Request events that were generated within the period** drop-down list.
7. Click the **Generate rules** button.

8. Click the **Save** button in the **Applications Launch Control rules** window.

   The rule list in the Applications Launch Control task will be populated with new rules generated based on system data from the computer with the Kaspersky Security Center Administration Console installed.

   If the list of Application Launch Control rules is already specified in the policy, Kaspersky Embedded Systems Security adds the selected rules from the blocking events to the already specified rules. Rules with the same hash are not added, because all rules in the list must be unique.

Importing rules from a Kaspersky Security Center report on blocked applications

You can import data on blocked application launches from a report generated in Kaspersky Security Center after the Applications Launch Control task is run in **Statistics only** mode and use this data to generate a list of Applications Launch Control allowing rules in the policy being configured.

When generating a report on events occurring during the Applications Launch Control task, you can keep track of the applications whose launch is blocked.

When importing data from a report on blocked applications into policy settings, make sure that the list you are using contains only applications whose launch you want to allow.

► *To specify Applications Launch Control allowing rules for a group of computers based on a blocked applications report from Kaspersky Security Center:*

1. Open the **Applications Launch Control** window (see Section "Opening policy settings for the Applications Launch Control task" on page 299).
2. In the **Task mode** section, select **Statistics only** mode.
3. In the policy properties in the **Event notification** section, make sure that:
   - For **Critical Events**, the task log retention period for **Application launch denied** events exceeds the planned period for running the task in **Statistics only** mode (the default value is 30 days).
   - For events with an importance level of **Warning**, the task log retention period for **Statistics only mode: application launch denied** events exceeds the planned period for running the task in **Statistics only** mode (the default value is 30 days).

   When the retention period for events elapses, information about the logged events is deleted and is not reflected in the report file. Before running the Applications Launch Control task in **Statistics only** mode, make sure that the task run time does not exceed the configured period for the specified events.
4. When the task has finished, export the logged events to a TXT file:

   a. In the workspace of the **Administration Server** node in Kaspersky Security Center, select the **Events** tab.

   b. Click the **Create a selection** button to create a selection of events based on the *Blocked* criterion to view the applications whose start will be blocked by the Applications Launch Control task.

c. In the details pane of the selection, click **Export events** to file list to save the blocked application starts report to a TXT file.

> Before importing and applying the generated report in a policy, make sure that the report only contains data on the applications whose start you want to allow.

5. Import data on blocked application starts into the Applications Launch Control task. To do so, in the policy properties in the Applications Launch Control task settings:

   a. On the **General** tab, click the **Rules list** button.

      The **Applications Launch Control rules** window opens.

   b. Click the **Add** button and, in the button's context menu, select **Import data of blocked applications from Kaspersky Security Center report**.

   c. Select the principle for adding rules from the list created based on a Kaspersky Security Center report to the list of previously configured Applications Launch Control rules:

      - **Add to existing rules** if you want to add the imported rules to the list of existing rules. Rules with identical settings are duplicated.
      - **Replace existing rules** if you want to replace the existing rules with the imported rules.
      - **Merge with existing rules** if you want to add the imported rules to the list of existing rules. Rules with identical settings are not added; the rule is added if at least one rule parameter is unique.

   d. In the standard Microsoft Windows window that opens, select the TXT file to which events from the blocked application launch report have been exported.

   e. Click **OK** in the Applications Launch Control rules and in the **Task settings** window.

Rules created based on the Kaspersky Security Center report on blocked applications are added to the list of Applications Launch Control rules.

Importing Applications Launch Control rules from an XML file

You can import reports generated by the Rule Generator for Applications Launch Control group task and apply them as a list of allowing rules in the policy you are configuring.

When the Rule Generator for Applications Launch Control group task finishes, the application exports the created allowing rules into XML files saved in the specified shared folder. Each file with a rule list is created by analyzing files executed and applications launched on each separate computer on the corporate network. The lists contain allowing rules for files and applications whose type matches the type specified in the Rule Generator for Applications Launch Control group task.

► *To specify Applications Launch Control allowing rules for a group of computers based on an automatically generated list of allowing rules:*

1. On the **Tasks** tab in the control panel of the group of computers you are configuring, create a Rule Generator for Applications Launch Control group task or select an existing task (see Section "Opening the Rule Generator for Applications Launch Control task wizard and properties" on page 300).
2. In the properties of the created Rule Generator for Applications Launch Control group task or in the task wizard, specify the following settings:
   - In the **Notification** section, configure the settings for saving the task execution report.

> For detailed instructions on configuring settings in this section, see the *Kaspersky Security Center Help.*

- In the **Settings** section, specify the types of applications whose start will be allowed by the rules that are created. You can edit the set of folders containing allowed applications: exclude default folders from the task scope or add new folders manually.
- In the **Options** section, specify the operations to be performed by the task while it is running and after it is finished. Specify the rule-generating criterion and the name of the file to which the generated rules will be exported.
- In the **Schedule** section, configure the task start schedule settings.
- In the **Account** section, specify the user account under which the task will be executed.
- In the **Exclusions from task scope** section, specify the groups of computers to be excluded from the task scope.

> Kaspersky Embedded Systems Security does not create allowing rules for applications launched on excluded computers.

3. On the **Tasks** tab on the control panel of the group of computers being configured, in the list of group tasks select the Rule Generator for Applications Launch Control task that you have created, and click the **Start** button to start the task.

   When the task is finished, the automatically generated lists of allowing rules are saved in XML files in a shared folder.

   > Before using the Applications Launch Control task in the network, make sure that all protected computers have access to a shared folder. If the organization's policy does not provide for the use of a shared folder in the network, we recommend that you start the Rule Generator for Applications Launch Control task on a computer in the test computers group or on a reference machine.

4. To add the generated lists of allowing rules to the Applications Launch Control task:

   a. Open the **Applications Launch Control rules** window (see Section "Opening the Applications Launch Control rules list" on page 300).

   b. Click the **Add** button and in the list that opens select **Import rules from XML file**.

   c. Select the principle for adding the automatically generated allowing rules to the list of previously created Applications Launch Control rules:

      - **Add to existing rules** if you want to add the imported rules to the list of existing rules. Rules with identical settings are duplicated.
      - **Replace existing rules** if you want to replace the existing rules with the imported rules.
      - **Merge with existing rules** if you want to add the imported rules to the list of existing rules. Rules with identical settings are not added; the rule is added if at least one rule parameter is unique.

   d. In the standard Microsoft Windows window that opens, select XML files created after completion of the Rule Generator for Applications Launch Control group task.

   e. Click **OK** in the **Applications Launch Control rules** and in the **Task settings** window.

5. If you want to apply the created rules to control the launch of application, in the policy in the properties of the Applications Launch Control task, select the **Active** mode for the task.

Allowing rules automatically generated based on task runs on each separate computer are applied to all network computers covered by the policy being configured. On these computers, the application will allow the launch of only those applications for which allowing rules have been created.

Checking application launches

Before applying the configured Applications Launch Control rules, you can test any application to determine which Applications Launch Control rules are triggered by that application.

By default, Kaspersky Embedded Systems Security denies the launch of applications whose launch is not allowed by a single rule. To avoid the denial of the launch of important applications, you need to create allowing rules for them.

If the launch of an application is controlled by several rules of different types, denying rules are given priority: the launch of an application will be denied if it falls under even one denying rule.

► *To test Applications Launch Control rules:*

1. Open the **Applications Launch Control rules** window (see Section "Opening the Applications Launch Control rules list" on page 300).
2. In the window that opens, click the **Show rules for the file** button.

   The standard Microsoft Windows window opens.
3. Select the file whose start control you want to test.

The path to the specified file is displayed in the search field. The list contains all rules that will be triggered when the selected file is started.

Creating a Rule Generator for Applications Launch Control task

► *To create and configure the Rule Generator for Applications Launch Control task settings:*

1. Open the **Settings** window in the New Task Wizard (see Section "Opening the Rule Generator for Applications Launch Control task wizard and properties" on page 300).
2. Configure the following:
   - Specify **Prefix for rule names**.

     This is the first part of a rule name. The second part of the name of the rule is formed from the name of the object that will be allowed to start.

     The default prefix is the name of the computer on which Kaspersky Embedded Systems Security is installed. You can change the prefix for names of allowing rules.
   - Configure the allowing-rules usage scope (see Section "Restricting the task usage scope" on page 335).
3. Click **Next**.
4. Specify the actions that must be performed by Kaspersky Embedded Systems Security:
   - When generating allowing rules (see Section "Actions to perform during automatic rule generation" on page 336).

- Upon task completion (see Section "Actions to perform upon completion of automatic rule generation" on page 337).

5. In the **Schedule** window, set the scheduled task start settings.
6. Click **Next**.
7. In the **Selecting an account to run the task** window, specify the account you want to use.
8. Click **Next**.
9. Define a task name.
10. Click **Next**.

    > The task name should be no longer than 100 characters and cannot contain the following symbols: " * < > & \ : |

    The **Finish task creation** window opens.

11. You can optionally run the task after the Wizard finishes by selecting the **Run task after Wizard finishes** check box.
12. Click **Finish** to finish creating the task.

► *To configure an existing rule in Kaspersky Security Center,*

open the **Properties: Rule Generator for Applications Launch Control** window and adjust the settings described above.

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 system audit log.

In this section

Restricting the task usage scope

► *To restrict the scope of the Rule Generator for Applications Launch Control task:*

1. Open the **Properties: Rule Generator for Applications Launch Control** window (see Section "Opening the Rule Generator for Applications Launch Control task wizard and properties" on page 300).
2. Configure the following task settings:
   - **Create allowing rules based on running applications**.

     This check either box enables or disables generation of Applications Launch Control rules for applications that are already running. This option is recommended if the computer has a reference set of applications based on which you want to create allowing rules.

     If this check box is selected, allowing rules for Applications Launch Control are generated based on running applications.

     If this check box is cleared, running applications are not taken into account when generating allowing rules.

     The check box is selected by default.

     This check box cannot be cleared if none of the folders are selected in the **Create allowing rules for applications from the folders** table.
   - **Create allowing rules for applications from the folders**.

     You can use the table to select or specify folders for the task and the types of executable files to be taken into account when creating Applications Launch Control rules. The task will generate allowing rules for files of the selected types that are located in the specified folders.
3. Click **OK**.

The specified settings are saved.

Actions to perform during automatic rule generation

► *To configure the actions that Kaspersky Embedded Systems Security while the Rule Generator for Applications Launch Control task is running:*

1. Open the **Properties: Rule Generator for Applications Launch Control** (see Section "**Opening the Rule Generator for Applications Launch Control task wizard and properties**" on page 300) window.
2. Open the **Options** tab.
3. In the **While generating allowing rules** section, configure the following settings:
   - **Use digital certificate**

     If this option is selected, the presence of a digital certificate is specified as a rule-triggering criterion in the settings of the newly generated allowing rules for Applications Launch Control. The application will now allow start of programs launched using files with a digital certificate. We recommend this option if you want to allow the start of any applications that are trusted in the operating system.

     This option is selected by default.

- **Use digital certificate subject and thumbprint**

  The check box enables or disables the use of the subject and thumbprint of the file's digital certificate as a criterion for triggering the allowing rules for Applications Launch Control. Selecting this check box lets you specify stricter digital certificate verification conditions.

  If this check box is selected, the subject and thumbprint values of the digital certificate of files for which the rules are generated are set as a criterion for triggering the allowing rules for Applications Launch Control. Kaspersky Embedded Systems Security will allow applications that are launched using files with the specified thumbprint and digital certificate.

  Selecting this check box highly restricts the triggering of allowing rules based on a digital certificate because a thumbprint is a unique identifier of a digital certificate and cannot be forged.

  If this check box is cleared, the existence of any digital certificate that is trusted in the operating system is set as a criterion for triggering the allowing rules for Applications Launch Control.

  This check box is active if the **Use digital certificate** option is selected.

  The check box is selected by default.

- **If the certificate is missing, use**

  This is a drop-down list that allows you to select the criterion for triggering an allowing rule for Applications Launch Control if the file used to generate the rule, has no digital certificate.

  - **SHA256 hash**. The checksum of the file used to generate the rule is set as a criterion for triggering the allowing rule for Applications Launch Control. The application will allow start of programs launched using files with the specified checksum.

  - **path to file**. The path to the file used to generate the rule is set as a criterion for triggering the allowing rule for Applications Launch Control. The application will now allow start of programs launched using files located in the folders specified in the **Create allowing rules for applications from the folders** table in the **Settings** section.

- **Use SHA256 hash**

If this option is selected, the checksum of the file used to generate the rule is specified as a rule-triggering criterion in the settings of the newly generated allowing rules for Applications Launch Control. The application will allow start of programs launched using files with the specified checksum.

We recommend this option for cases when the generated rules must achieve the highest level of security: a SHA256 checksum may be used as a unique file ID. Using a SHA256 checksum as a rule-triggering criterion restricts the rule usage scope to one file.

This option is cleared by default.

- **Generate rules for user or group of users**.

  This is a field that displays a user or group of users. The application will control any applications run by the specified user or group of users.

  The default selection is **Everyone**.

4. Click **OK**.

The specified settings are saved.

Actions to perform upon completion of automatic rule generation

► *To configure the actions to be taken by Kaspersky Embedded Systems Security after the Rule Generator for Applications Launch Control task is finished:*

1. Open the **Properties: Rule Generator for Applications Launch Control** window (see Section "Opening the Rule Generator for Applications Launch Control task wizard and properties" on page 300).
2. Open the **Options** tab.
3. In the **After task completes** section, configure the following settings:
   - **Add allowing rules to the list of Applications Launch Control rules**.

     The check box enables or disables adding the newly generated allowing rules to the list of Applications Launch Control rules. The list of Applications Launch Control rules is displayed when you click the **Applications Launch Control rules** link in the details pane of the Applications Launch Control node.

     If this check box is selected, Kaspersky Embedded Systems Security adds the rules generated by the Rule Generator for Applications Launch Control task to the list of Applications Launch Control rules based on the selected principle for adding rules.

     If this check box is cleared, Kaspersky Embedded Systems Security does not add the newly generated allowing rules to the list of Applications Launch Control rules. The generated rules are only exported to a file.

     The check box is selected by default.
   - **Principle of adding**.

     This drop-down list is used to specify the method used to add the newly generated allowing rules to the list of Applications Launch Control rules.

     - **Add to existing rules**. The rules are added to the list of existing rules. Rules with identical settings are duplicated.
     - **Replace existing rules**. The rules replace the existing rules in the list.
     - **Merge with existing rules**. The rules are added to the list of existing rules. Rules with identical settings are not added; the rule is added if at least one rule parameter is unique.

     By default, the **Merge with existing rules** method is selected.
   - **Export allowing rules to file**.
   - **Add computer details to file name**.

     The check box enables or disables adding information about the protected computer to the name of the file to which the allowing rules will be exported.

     If this check box is selected, the application adds the protected computer name and the file creation date and time to the name of the export file.

     If the check box is cleared, the application does not add information about the protected computer to the name of the export file.

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

The specified settings are saved.

Managing Applications Launch Control via the Application Console

In this section, learn how to navigate the Application Console interface and configure task settings on a local computer.

In this section

Navigation

Learn how to navigate to the required task settings via the interface.

In this section

Opening the Applications Launch Control task settings

► *To open the Applications Launch Control general task settings via the Application Console:*

1. In the Application Console tree, expand the **Computer Control** node.
2. Select the **Applications Launch Control** child node.
3. In the details pane of the **Applications Launch Control** child node, click the **Properties** link.

   The **Task settings** window opens.

Opening the Applications Launch Control rules window

► *To open the Applications Launch Control rule list via the Application Console:*

1. In the Application Console tree, expand the **Computer Control** node.
2. Select the **Applications Launch Control** child node.

3. In the details pane of the **Applications Launch Control** node, click the **Applications Launch Control rules** link.

   The **Applications Launch Control rules** window opens.

4. Configure the rules list as required.

Opening the Rule Generator for Applications Launch Control task settings

► *To configure the Rule Generator for Applications Launch Control task:*

1. In the Application Console tree, expand the **Automated rule generators** node.
2. Select the **Rule Generator for Applications Launch Control** child node.
3. In the details pane of the **Rule Generator for Applications Launch Control** child node, click the **Properties** link.

   The **Task settings** window opens.

4. Configure the task as required.

Configuring Applications Launch Control task settings

► *To configure general Applications Launch Control task settings:*

1. Open the **Task settings** window (see Section "Opening the Applications Launch Control task settings" on page 321).
2. Configure the following task settings:
   - On the **General** tab:
     - Applications Launch Control task mode (see Section "Selecting the mode of the Applications Launch Control task" on page 323).
     - Rule usage scope in the task (see Section "Configuring the scope of the Applications Launch Control task" on page 324).
     - KSN Usage (see Section "Configuring KSN usage" on page 325).
   - Software Distribution Control settings (see Section "Software Distribution Control" on page 326) on the **Software Distribution Control** tab.
   - Task start schedule settings (see Section "Configuring the task start schedule settings" on page 149) on the **Schedule** and **Advanced** tabs.
3. Click **OK** in the **Task settings** window.

   The modified settings are saved.

Kaspersky Embedded Systems Security immediately applies the new 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 system audit log.

In this section

Selecting the mode of the Applications Launch Control task

► *To configure the mode of the Applications Launch Control task:*

1. Open the **Task settings** (see Section "**Opening the Applications Launch Control task settings**" on page 321) window.
2. On the **General** tab, in the **Task mode** drop-down list, specify the task mode.

   In this drop-down list you can select an Applications Launch Control task mode:

   - **Active**. Kaspersky Embedded Systems Security uses the specified rules to control any applications that are launched.
   - **Statistics only**. Kaspersky Embedded Systems Security does not use the specified rules to control application launches. Instead, it simply records information about those launches in the task log. All programs are allowed to start. You can use this mode to generate a list of Applications Launch Control rules based on the information about blocking recorded in the task log.

   By default, the Applications Launch Control task runs in **Statistics only** mode.
3. Clear or select the **Repeat action taken for the first file launch on all the subsequent launches for this file** check box.

   The check box enables or disables launch control for the second and subsequent attempts to start applications based on the event information stored in the cache.

   If the check box is selected, Kaspersky Embedded Systems Security allows or denies subsequent launches of an application based on the task's conclusion regarding the first launch of the application. For example, if the first application launch was allowed by the rules, information about this decision will be stored in the cache, and the second and all subsequent launches will also be allowed without rechecking.

   If the check box is cleared, Kaspersky Embedded Systems Security analyzes an application every time a launch is attempted.

   The check box is selected by default.

> Kaspersky Embedded Systems Security creates a new list of cached events every time the Applications Launch Control task settings are modified. This means that Applications Launch Control is performed according to the current security settings.

4. Clear or select the **Deny the command line interpreters launch with no command to execute**.

   If the check box is selected, Kaspersky Embedded Systems Security denies the launch of command line interpreters even if launching interpreters is allowed. A command interpreter can only be launched with no command if both of the following conditions are met:

   - Launch of the command line interpreter is allowed.
   - The command to be executed is allowed.

   If the check box is cleared, Kaspersky Embedded Systems Security only considers allowing rules when launching a command line interpreter. The launch is denied if no allowing rule applies or the executable process is not trusted by KSN. If an allowing rule applies or the process is trusted by KSN, a command line interpreter can be launched with or without a command to execute.

   Kaspersky Embedded Systems Security recognizes the following command line interpreters:

   - cmd.exe
   - powershell.exe
   - python.exe
   - perl.exe

   The check box is cleared by default.

5. Click **OK**.

The specified settings are saved.

All attempts to start applications are recorded in the task log.

Configuring the scope of the Applications Launch Control task

► *To define the scope of the Applications Launch Control task:*

1. Open the **Task settings** (see Section "**Opening the Applications Launch Control task settings**" on page 321) window.
2. On the **General** tab, in the **Rules usage scope** section, specify the following settings:

   - **Apply rules to executable files**

     The check box either enables or disables launch control of executable files.

     If this check box is selected, Kaspersky Embedded Systems Security allows or blocks start of executable files using the specified rules whose settings specify **Executable files** as the scope.

     If the check box is cleared, Kaspersky Embedded Systems Security does not control start of executable files using the specified rules. Startup of executable files is allowed.

     The check box is selected by default.

- **Monitor loading of DLL modules**

  The check box either enables or disables control of loading of DLL modules.

  If this check box is selected, Kaspersky Embedded Systems Security allows or blocks loading of DLL modules using the specified rules whose settings specify **Executable files** as the scope.

  If this check box is cleared, Kaspersky Embedded Systems Security does not control loading of DLL modules using the specified rules. Loading of DLL modules is allowed.

  The check box is active if the **Apply rules to executable files** check box is selected.

  The check box is cleared by default.

  > Controlling loading of DLL modules may affect the performance of the operating system.

- **Apply rules to scripts and MSI packages**

  The check box either enables or disables launch of scripts and MSI packages.

  If this check box is selected, Kaspersky Embedded Systems Security allows or blocks start of scripts and MSI packages using the specified rules whose settings specify Scripts and MSI packages as the scope.

  If the check box is cleared, Kaspersky Embedded Systems Security does not control start of scripts and MSI packages using specified rules. Start of scripts and MSI packages is allowed.

  The check box is selected by default.

3. Click **OK**.

The specified settings are saved.

Configuring KSN usage

► *To configure the use of KSN services for the Applications Launch Control task:*

1. Open the **Task settings** (see Section "**Opening the Applications Launch Control task settings**" on page 321) window.
2. On the **General** tab, in the **KSN Usage** section, specify the settings for use of KSN services:
   - If necessary, select the **Deny applications untrusted by KSN** check box.

     The check box either enables or disables Applications Launch Control according to application reputation data in KSN.

     If this check box is selected, Kaspersky Embedded Systems Security blocks any application from running if it is not trusted in KSN. Applications Launch Control allowing rules that apply to applications not trusted in KSN will not be triggered. Selecting the check box provides additional protection from malware.

     If the check box is cleared, Kaspersky Embedded Systems Security does not consider the reputation of applications not trusted in KSN and allows or blocks start in accordance with the rules that apply to such applications.

     The check box is cleared by default.

   - If necessary, select the **Allow applications trusted by KSN** check box.

The check box either enables or disables Applications Launch Control according to application reputation data in KSN.

If this check box is selected, Kaspersky Embedded Systems Security allows applications to run if they are trusted in KSN. Denying application launch control rules that apply to KSN-trusted applications have higher priority: if an application is trusted by KSN services, the application launch will be denied.

If the check box is cleared, Kaspersky Embedded Systems Security does not consider the reputation of KSN-trusted applications and allows or denies launch in accordance with rules that apply to such applications.

The check box is cleared by default.

- If the **Allow applications trusted by KSN** check box is selected, indicate the users and/or groups of users allowed to start applications trusted in KSN. To do this, perform the following actions:

  a. Click the **Edit** button.

     The standard Microsoft Windows **Select users or groups** window opens.

  b. Specify the list of users and/or user groups.

  c. Click **OK**.

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

The specified settings are saved.

Software Distribution Control

► *To add a trusted distribution package:*

1. Open the **Task settings** (see Section "**Opening the Applications Launch Control task settings**" on page 321) window.
2. On the **Software Distribution Control** tab, select the **Automatically allow software distribution for applications and packages listed** check box.

   The check box enables and disables automatic creation of exclusions for all files started using the distribution packages specified in the list.

   If the check box is selected, the application automatically allows files in the trusted distribution packages to start. The list of applications and distribution packages allowed to start can be edited.

   If the check box is cleared, the application does not apply the exclusions specified in the list.

   The check box is cleared by default.

> You can select the **Automatically allow software distribution for applications and packages listed**, if the **Apply rules to executable files** check box in the **General** tab is selected in the **Applications Launch Control** task settings.

3. Clear the **Always allow software distribution via Windows Installer** check box if required.

   The check box enables and disables automatic creation of exclusions for all files executed via Windows Installer.

   If the check box is selected, files installed via Windows Installer will always be allowed to start.

   If the check box is cleared, files will not be allowed to start unconditionally, even if they are started via Windows Installer.

   The check box is selected by default.

   The check box is not editable if the **Automatically allow software distribution for applications and packages listed** check box is not selected.

> Clearing the **Always allow software distribution via Windows Installer** check box is only recommended if it is absolutely necessary. Turning off this function may cause issues with updating operating system files and also prevent the launch of files extracted from a distribution package.

4. If required, select the **Always allow software distribution via SCCM using the Background Intelligent Transfer Service** check box.

   The check box turns on or off automatic software distribution using the System Center Configuration Manager.

   If the check box is selected, Kaspersky Embedded Systems Security automatically allows Microsoft Windows deployment using the System Center Configuration Manager. The application allows software distribution only via the Background Intelligent Transfer Service.

   The application controls start of objects with the following extensions:

   - .exe
   - .msi

   The check box is cleared by default.

> The application controls the software distribution cycle on the computer — from package delivery to installation or update. The application does not control processes if any stage of distribution was performed before installation of the application on the computer.

5. To edit the list of trusted distribution packages, click **Change packages list** and select one of the following methods in the window that opens:

   - **Add one distribution package**.

     a. Click the **Browse** button and select the executable file or distribution package.

        The **Trusting criteria** section is automatically populated with data about the selected file.

     b. Clear or select the **Allow launching to all files from this distribution package extraction chain** check box.

c. Select one of two available options for criteria to use to determine whether a file or distribution package is trusted:

   - **Use digital certificate**
   - Use SHA256 hash]

- **Add several packages by hash**.

  > You can select an unlimited number of executable files and distribution packages, and add them to the list all at the same time. Kaspersky Embedded Systems Security examines the hash and allows the operating system to launch the specified files.

- **Change selected package**.

  Use this option to select a different executable file or distribution package, or to change the trust criteria.

- **Import distribution packages list from file**.

  You can import the list of trusted distribution packages from a configuration file. To be recognized by Kaspersky Embedded Systems Security, such a file must satisfy the following parameters:

  - The file extension is TXT.
  - The file contains information structured as a list of lines, where each line includes data for one of the trusted files.
  - The file must contain a list in one of the following formats:
    - <file name>:<SHA256 hash>.
    - <SHA256 hash>*<file name>.

  In the **Open** window, specify the configuration file containing a list of trusted distribution packages.

6. If you want to remove a previously added application or distribution package for the trusted list, click the **Delete distribution packages** button. Extracted files will be allowed to run.

   > To prevent extracted files from starting, uninstall the application on the protected computer or create a denying rule in the Applications Launch Control task settings.

7. Click **OK**.

Your newly configured settings are saved.

Configuring Applications Launch Control rules

Learn how to generate, import and export a list of rules, or manually create allowing or denying rules using the Application Launch Control task.

In this section

Adding an Applications Launch Control rule

► *To add an Applications Launch Control rule, take the following steps:*

1. Open the **Applications Launch Control rules** window.
2. Click the **Add** button.
3. In the context menu of the button, select **Add one rule**.

   The **Rule settings** window opens.
4. Specify the following settings:
   a. In the **Name** field, enter the name of the rule.

   b. In the **Type** drop-down list, select the rule type:

   - **Allowing** if you want the rule to allow launch of applications in accordance with the criteria specified in the rule settings.
   - **Denying** if you want the rule to block launch of applications in accordance with the criteria specified in the rule settings.

   c. In the **Scope** drop-down list, select the type of files whose execution will be controlled by the rule:

   - **Executable files** if you want the rule to control launch of executable files.
   - **Scripts and MSI packages** if you want the rule to control launch of scripts and MSI packages.

   d. In the **User or user group** field, specify the users who will be allowed or not allowed to start programs based on the type of rule. To do this, perform the following actions:

   i. Click the **Browse** button.

   ii. The standard Microsoft Windows **Select user or groups** window opens.

iii. Specify the list of users and/or user groups.

iv. Click **OK**.

e. If you want to take the values of the rule-triggering criteria listed in the **Rule triggering criterion** section from a specific file:

i. Click the **Set rule triggering criterion from file properties** button.

The standard Microsoft Windows **Open** window opens.

ii. Select the file.

iii. Click the **Open** button.

The criteria values in the file are displayed in the fields in the **Rule triggering criterion** section. The criterion for which data are available in the file properties is selected by default.

f. In the **Rule triggering criterion** section, select one of the following options:

- **Digital certificate** if you want the rule to control the start of applications launched using files signed with a digital certificate:
    - Select the **Use subject** check box if you want the rule to control the launch of files signed with a digital certificate only with the specified header.
    - Select the **Use thumb** check box if you want the rule to only control the launch of files signed with a digital certificate with the specified thumbprint.
- **SHA256 hash** if you want the rule to control the start of programs launched using files whose checksum matches the one specified.
- **Path to file** if you want the rule to control the start of programs launched using files located at the specified path.

> Kaspersky Embedded Systems Security does not recognize paths that contain slashes ("/"). Use backslash ("\") to enter the path correctly.

g. If you want to add rule exclusions:

i. In the **Exclusions from rule** section, click the **Add** button.

The **Exclusion from rule** window opens.

ii. In the **Name** field, enter the name of the exclusion.

iii. Specify the settings for exclusion of application files from the Applications Launch Control rule. You can fill out the settings fields from the file properties by clicking the **Set exclusion based on file properties** button.

- **Digital certificate**

  If this option is selected, the presence of a digital certificate is specified as a rule-triggering criterion in the settings of the newly generated allowing rules for Applications Launch Control. The application will now allow start of programs launched using files with a digital certificate. We recommend this option if you want to allow the start of any applications that are trusted in the operating system.

  This option is selected by default.

- **Use subject**

  The check box either enables or disables the use of the subject of the digital certificate as a rule-triggering criterion.

If the check box is selected, the specified digital certificate subject is used as a rule-triggering criterion. The created rule will control the start of applications only for the vendor specified in the subject.

If the check box is cleared, the application will not use the subject of the digital certificate as a rule-triggering criterion. If the **Digital certificate** criterion is selected, the created rule will control the start of applications signed with a digital certificate containing any subject.

The subject of the digital certificate used to sign the file can be specified only from the properties of the selected file using the **Set rule triggering criterion from file properties** button located above the **Rule triggering criterion** section.

The check box is cleared by default.

- **Use thumb**

  The check box enables / disables the use of the thumbprint of the digital certificate as a rule-triggering criterion.

  If the check box is selected, the specified digital certificate thumbprint is used as a rule-triggering criterion. The created rule will control the start of applications signed with a digital certificate with the specified thumbprint.

  If the check box is cleared, the application will not use the thumbprint of the digital certificate as a rule-triggering criterion. If the **Digital certificate** criterion is selected, the application will control the start of applications signed with a digital certificate with any thumbprint.

  The thumbprint of the digital certificate used to sign the file can be specified only from the properties of the selected file using the **Set rule triggering criterion from file properties** button located above the **Rule triggering criterion** section.

  The check box is cleared by default.

- **SHA256 hash**

  If this option is selected, the checksum of the file used to generate the rule is specified as a rule-triggering criterion in the settings of the newly generated allowing rules for Applications Launch Control. The application will allow start of programs launched using files with the specified checksum.

  We recommend this option for cases when the generated rules must achieve the highest level of security: a SHA256 checksum may be used as a unique file ID. Using a SHA256 checksum as a rule-triggering criterion restricts the rule usage scope to one file.

  This option is cleared by default.

- **Path to file**

  If the check box is selected, Kaspersky Embedded Systems Security uses the full path to the file to determine whether the process is trusted.

  If the check box is cleared, the path to the file is not used to determine whether the process is trusted.

  The check box is cleared by default.

   iv. Click **OK**.

   v. If necessary, repeat steps (i)-(iv) to add additional exclusions.

5. Click **OK** in the **Rule settings** window.

The created rule is displayed in the list in the **Applications Launch Control rules** window.

Enabling the Default Allow mode

Default Allow mode allows all applications to start if they are not blocked by rules or by a conclusion from KSN that they are not trusted. Default Allow mode can be enabled by adding specific allowing rules. You can enable Default Allow for only scripts or for all executable files.

► *To add a Default Allow rule:*

1. Open the **Applications Launch Control rules** window.
2. Click the **Add** button.
3. In the context menu of the button, select **Add one rule**.

   The **Rule settings** window opens.
4. In the **Name** field, enter the name of the rule.
5. In the **Type** drop-down list, select the **Allowing** rule type.
6. In the **Scope** drop-down list, select the type of files whose execution will be controlled by the rule:
   - **Executable files** if you want the rule to control the launch of executable files.
   - **Scripts and MSI packages** if you want the rule to control the launch of scripts and MSI packages.
7. In the **Rule triggering criterion** section, select the **Path to file** option.
8. Enter the following mask: `?:\`
9. Click **OK** in the **Rule settings** window.

Kaspersky Embedded Systems Security applies the Default Allow mode.

Creating allowing rules from Applications Launch Control task events

► *To create a configuration file that contains allowing rules generated from Applications Launch Control task events:*

1. Start the Applications Launch Control task in **Statistics only** mode (see Section "Selecting the mode of the Applications Launch Control task" on page 323) to record information about all applications launches on a protected computer in the task log.
2. After the task finishes running in **Statistics only** mode, open the task log by clicking the **Open task log** button in the **Management** section of the **Applications Launch Control** node's detail pane.
3. In the **Logs** window, click **Generate rules based on events**.

Kaspersky Embedded Systems Security will generate an XML configuration file containing a rule list based on events of the Applications Launch Control task in **Statistics only** mode. You can apply this rule list (see Section "Importing Applications Launch Control rules from an XML file" on page 333) in the Applications Launch Control task.

Before applying the rule list generated from the logged task events, we recommend that you review and manually process the list to be certain that the launch of critical files (for example, system files) is allowed by the specified rules.

All task events are recorded in the task log regardless of the task mode. You can generate a configuration file with a rule list based on the log created while the task is running in **Active** mode. This scenario is not recommended except for urgent cases, because a final rule list must be generated before the task is run in **Active** mode in order to make it efficient.

Exporting Applications Launch Control rules

► *To export Applications Launch Control rules to a configuration file:*

1. Open the **Applications Launch Control rules** window.
2. Click the **Export to a file** button.

   The standard Microsoft Windows window opens.
3. In the window that opens, specify the file to which you want to export the rules. If no such file exists, it will be created. If a file with the specified name already exists, its contents will be overwritten when the rules are exported.
4. Click the **Save** button.

The rule settings will be exported to the specified file.

Importing Applications Launch Control rules from an XML file

► *To import Applications Launch Control rules:*

1. Open the **Applications Launch Control rules** window.
2. Click the **Add** button.
3. In the context menu of the button, select **Import rules from XML file**.
4. Specify the method for adding the imported rules. To do so, select one of the options from the context menu of the **Import rules from XML file** button:
   - **Add to existing rules** if you want to add the imported rules to the list of existing rules. Rules with identical settings are duplicated.
   - **Replace existing rules** if you want to replace the existing rules with the imported rules.
   - **Merge with existing rules** if you want to add the imported rules to the list of existing rules. Rules with identical settings are not added; the rule is added if at least one rule parameter is unique.

   The standard Microsoft Windows **Open** window opens.
5. In the **Open** window, select the XML file that contains the Applications Launch Control rules.
6. Click the **Open** button.

The imported rules will be displayed in the list in the **Applications Launch Control rules** window.

Removing Applications Launch Control rules

► *To remove Applications Launch Control rules:*

1. Open the **Applications Launch Control rules** window.
2. In the list, select one or more rules that you want to delete.
3. Click the **Remove Selected** button.
4. Click the **Save** button.

The selected Applications Launch Control rules are deleted.

Configuring a Rule Generator for Applications Launch Control task

► *To configure the Rule Generator for Applications Launch Control task settings:*

1. Open the **Task settings** (see Section "**Opening the Rule Generator for Applications Launch Control task settings**" on page 322) window of the **Rule Generator for Applications Launch Control** task.
2. Configure the following settings:
   - On the **General** tab:
     - Specify **Prefix for rule names**.

       This is the first part of a rule name. The second part of the name of the rule is formed from the name of the object that will be allowed to start.

       The default prefix is the name of the computer on which Kaspersky Embedded Systems Security is installed. You can change the prefix for names of allowing rules.
     - Configure the allowing-rules usage scope (see Section "Restricting the task usage scope" on page 335).
   - On the **Action** tab, specify the actions that must be performed by Kaspersky Embedded Systems Security:
     - When generating allowing rules (see Section "Actions to perform during automatic rule generation" on page 336).
     - Upon task completion (see Section "Actions to perform upon completion of automatic rule generation" on page 337).
   - On the **Schedule** and **Advanced** tabs, configure Schedule task start settings (see Section "Configuring the task start schedule settings" on page 149).
   - On the **Run as** tab, configure Task start settings with account permission (see Section "Specifying a user account to start a task" on page 152).
3. Click **OK**.

Kaspersky Embedded Systems Security immediately applies the new 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.

In this section

Restricting the task usage scope

► *To restrict the scope of the Rule Generator for Applications Launch Control task:*

1. Open the **Task settings** (see Section "**Opening the Rule Generator for Applications Launch Control task settings**" on page 322) window of the **Rule Generator for Applications Launch Control** task.
2. Configure the following task settings:
   - **Create allowing rules based on running applications**.

     This check either box enables or disables generation of Applications Launch Control rules for applications that are already running. This option is recommended if the computer has a reference set of applications based on which you want to create allowing rules.

     If this check box is selected, allowing rules for Applications Launch Control are generated based on running applications.

     If this check box is cleared, running applications are not taken into account when generating allowing rules.

     The check box is selected by default.

     This check box cannot be cleared if none of the folders are selected in the **Create allowing rules for applications from the folders** table.
   - **Create allowing rules for applications from the folders**.

     You can use the table to select or specify folders for the task and the types of executable files to be taken into account when creating Applications Launch Control rules. The task will generate allowing rules for files of the selected types that are located in the specified folders.
3. Click **OK**.

The specified settings are saved.

Actions to perform during automatic rule generation

► *To configure the actions that Kaspersky Embedded Systems Security while the Rule Generator for Applications Launch Control task is running:*

1. Open the **Task settings** (see Section "**Opening the Rule Generator for Applications Launch Control task settings**" on page 322) window of the **Rule Generator for Applications Launch Control** task.
2. Open the **Options** tab.
3. In the **While generating allowing rules** section, configure the following settings:
   - **Use digital certificate**

     If this option is selected, the presence of a digital certificate is specified as a rule-triggering criterion in the settings of the newly generated allowing rules for Applications Launch Control. The application will now allow start of programs launched using files with a digital certificate. We recommend this option if you want to allow the start of any applications that are trusted in the operating system.

     This option is selected by default.
   - **Use digital certificate subject and thumbprint**

     The check box enables or disables the use of the subject and thumbprint of the file's digital certificate as a criterion for triggering the allowing rules for Applications Launch Control. Selecting this check box lets you specify stricter digital certificate verification conditions.

     If this check box is selected, the subject and thumbprint values of the digital certificate of files for which the rules are generated are set as a criterion for triggering the allowing rules for Applications Launch Control. Kaspersky Embedded Systems Security will allow applications that are launched using files with the specified thumbprint and digital certificate.

     Selecting this check box highly restricts the triggering of allowing rules based on a digital certificate because a thumbprint is a unique identifier of a digital certificate and cannot be forged.

     If this check box is cleared, the existence of any digital certificate that is trusted in the operating system is set as a criterion for triggering the allowing rules for Applications Launch Control.

     This check box is active if the **Use digital certificate** option is selected.

     The check box is selected by default.
   - **If the certificate is missing, use**

     This is a drop-down list that allows you to select the criterion for triggering an allowing rule for Applications Launch Control if the file used to generate the rule, has no digital certificate.

     - **SHA256 hash**. The checksum of the file used to generate the rule is set as a criterion for triggering the allowing rule for Applications Launch Control. The application will allow start of programs launched using files with the specified checksum.

    - **path to file**. The path to the file used to generate the rule is set as a criterion for triggering the allowing rule for Applications Launch Control. The application will now allow start of programs launched using files located in the folders specified in the **Create allowing rules for applications from the folders** table in the **Settings** section.

- **Use SHA256 hash**

  If this option is selected, the checksum of the file used to generate the rule is specified as a rule-triggering criterion in the settings of the newly generated allowing rules for Applications Launch Control. The application will allow start of programs launched using files with the specified checksum.

  We recommend this option for cases when the generated rules must achieve the highest level of security: a SHA256 checksum may be used as a unique file ID. Using a SHA256 checksum as a rule-triggering criterion restricts the rule usage scope to one file.

  This option is cleared by default.

- **Generate rules for user or group of users**.

  This is a field that displays a user or group of users. The application will control any applications run by the specified user or group of users.

  The default selection is **Everyone**.

4. Click **OK**.

The specified settings are saved.

Actions to perform upon completion of automatic rule generation

► *To configure the actions to be taken by Kaspersky Embedded Systems Security after the Rule Generator for Applications Launch Control task is finished:*

1. Open the **Task settings** (see Section "**Opening the Rule Generator for Applications Launch Control task settings**" on page 322) window of the **Rule Generator for Applications Launch Control** task.
2. Open the **Options** tab.
3. In the **After task completes** section, configure the following settings:

   - **Add allowing rules to the list of Applications Launch Control rules**.

     The check box enables or disables adding the newly generated allowing rules to the list of Applications Launch Control rules. The list of Applications Launch Control rules is displayed when you click the **Applications Launch Control rules** link in the details pane of the Applications Launch Control node.

     If this check box is selected, Kaspersky Embedded Systems Security adds the rules generated by the Rule Generator for Applications Launch Control task to the list of Applications Launch Control rules based on the selected principle for adding rules.

     If this check box is cleared, Kaspersky Embedded Systems Security does not add the newly generated allowing rules to the list of Applications Launch Control rules. The generated rules are only exported to a file.

     The check box is selected by default.

- **Principle of adding**.

  This drop-down list is used to specify the method used to add the newly generated allowing rules to the list of Applications Launch Control rules.

  - **Add to existing rules**. The rules are added to the list of existing rules. Rules with identical settings are duplicated.
  - **Replace existing rules**. The rules replace the existing rules in the list.
  - **Merge with existing rules**. The rules are added to the list of existing rules. Rules with identical settings are not added; the rule is added if at least one rule parameter is unique.

  By default, the **Merge with existing rules** method is selected.

- **Export allowing rules to file**.
- **Add computer details to file name**.

  The check box enables or disables adding information about the protected computer to the name of the file to which the allowing rules will be exported.

  If this check box is selected, the application adds the protected computer name and the file creation date and time to the name of the export file.

  If the check box is cleared, the application does not add information about the protected computer to the name of the export file.

  The check box is selected by default.

4. Click **OK**.

The specified settings are saved.

Device Control

This section contains information about the Device Control task, as well as instruction to configure the task settings.

In this chapter

About Device Control task

Kaspersky Embedded Systems Security controls registration and usage of the mass storage devices and CD/DVD drives in order to protect computer against computer security threats, that may occur in process of file exchange with flash drives or other type of external device connected via USB. Mass storage device is an external device that may be connected to a computer in order to copy or store files.

Kaspersky Embedded Systems Security controls the following USB external devices connections:

- USB-connected flash drives
- CD/DVD ROM drives
- USB-connected floppy disk drives
- USB-connected MTP-mobile devices

> Kaspersky Embedded Systems Security informs you about all devices connected via USB with the corresponding event in the task and event logs. The event details include device type and connection path. When the Device Control task is started, Kaspersky Embedded Systems Security checks and lists all devices connected via USB. You can configure the notifications in the Kaspersky Security Center notification settings section.

The Device Control task monitors all the attempts of external devices connections to a protected computer via USB and blocks connection, if there are no allowing rules for such devices. After the connection is blocked, the device is not available.

The application prescribes one of the following statuses to each connected mass storage device:

- *Trusted*. Device for which you want to allow files exchange. Upon rules list generation, the *Device Instance Path* value is included into usage scope for at least one rule.
- *Untrusted*. Device for which you want to restrict files exchange. Device instance path is not included into any allowing rule usage scope.

You can create allowing rules for external devices to allow data exchange using the Rule Generator for Device Control task. You can also expand the usage scope for already specified rules. You cannot create allowing rules manually.

Kaspersky Embedded Systems Security identifies mass storage devices that are registered in the system, by using the Device Instance Path value. Device Instance Path is a default feature uniquely specified for each external device. The Device Instance Path value is specified for each external device in its Windows properties and is automatically determined by Kaspersky Embedded Systems Security during rule generation.

The Device Control task can operate in two modes:

- **Active**. Kaspersky Embedded Systems Security applies rules to control the connection of flash drives and other external devices, and allows or blocks the use of all devices according to the Default Deny principle and specified allowing rules. The use of trusted external devices is allowed. The use of untrusted external devices is blocked by default.

  > If an external device you consider to be untrusted is connected to a protected computer before the Device Control task is run in the **Active** mode, the device is not blocked by the application. We recommend that you disconnect the untrusted device manually or restart the computer. Otherwise, the Default Deny principle will not be applied to the device.

- **Statistics only**. Kaspersky Embedded Systems Security does not control the connection of flash drives and other external devices, but only logs information about the connection and registration of external devices on a protected computer, and about the Device Control allowing rules triggered by the connected devices. The use of all external devices is allowed. This mode is set by default.

  You can apply this mode for rules generation on the basis of the information about blocking logged during the task running (see Section "Filling rules list basing on Device Control task events" on page 359).

About Device Control rules

The rules are generated uniquely for each device that is currently connected or has ever been connected to a protected computer if the information about this device is stored in the system registry.

To generate allowing rules for device control, you can do the following:

- Apply the Rule Generator for Device Control task (see Section "About Rule Generator for Device Control task" on page 344).
- Run the Device Control task in the Statistics only mode (see Section "Filling rules list basing on Device Control task events" on page 359).

- Apply system information about previously connected devices (see Section "Adding an allowing rule for one or several external devices" on page 360).
- Expand the usage scope for already specified rules (see Section "Expanding Device Control rules usage scope" on page 361).

> The maximum number of the Device Control rules supported by Kaspersky Embedded Systems Security is 3072.

Device Control rules are described below.

Rule type

Rule type is always *allowing*. By default, the Device Control task blocks all flash drives and other external devices connections if these devices are not included into any allowing rule usage scope.

Triggering criterion and rule usage scope

Device Control rules identify flash drives and other external devices basing on *Device Instance Path*. Device instance path is a unique criterion that is assigned to a device by the system when the device is connected and is registered as a Mass Storage Device or CD/DVD drive (for example, IDE or SCSI).

> Kaspersky Embedded Systems Security controls connection of the CD/DVD drives regardless of the bus used for connection. When mounting such device via USB, operating system registers two path values to the device instance: for the mass storage device and for CD/DVD drive (for example, IDE or SCSI). To connect such devices correctly, allowing rules for each path value to the instance must be set.

Kaspersky Embedded Systems Security automatically defines the device instance path and parses the value obtained into the following elements:

- Device manufacturer (VID)
- Device controller type (PID)
- Device serial number

You cannot set the device instance path manually. Allowing rule triggering criteria define the rule usage scope. By default, newly created rule usage scope includes one initial device, basing on whose properties Kaspersky Embedded Systems Security had generated the rule. You can configure the values in the created rule settings by using a mask to expand the rule usage scope (see Section "Expanding Device Control rules usage scope" on page 361).

Initial device values

Device properties that Kaspersky Embedded Systems Security used for allowing rule generation and that are displayed in Windows Device Manager for each device connected.

Initial device values contain the following information:

- **Device instance path**. Basing on this property Kaspersky Embedded Systems Security defines rule triggering criteria and fills the following fields: **Manufacturer (VID)**, **Controller type (PID)**, **Serial number** in the **Rule usage scope** section of the **Rule properties** window.
- **Friendly name**. Device clear name that is set in the device properties by its manufacturer.

Kaspersky Embedded Systems Security automatically defines initial device values when the rule is generating. Later on you can use these values to recognize the device that was used as a base for the rule generating. Initial device values are not available for editing.

Description

You can add additional information for each created device control rule in the **Description** field, for example, you can note name of the connected flash driver or define its owner. The description is displayed in a corresponding graph in the **Device Control rules** window.

Description and initial device values are not allowed for rule triggering and are prescribed only to simplify device identification by user.

About Device Control rules list filling

You can import device control allowing rules from the XML files that were automatically generated during the Device Control or the Rule Generator for Device Control tasks running.

By default, Kaspersky Embedded Systems Security restricts connections of any flash drives and other external devices, if they are not included into the usage scope of specified device control rules.

Table 49. Targets and scenarios for list generation of device control rules

Rule generation scenario	Target
The Rule Generator for Device Control task	• Add allowing rules for previously connected trusted devices before the first start of the Device Control task. • Generate rules list for devices trusted in the protected computers network.
Rules generation based on system data	Add allowing rules for one or several newly connected devices.
The Device Control task in the **Statistics only** mode	Generate allowing rules for a large number of trusted devices.

The rule Generator for Device Control task usage

XML file, generated upon the Rule Generator for Device Control task completion, contains allowing rules for those flash drives and other external devices whose data have been stored in a system registry.

During the task running, Kaspersky Embedded Systems Security receives system data about all mass storage devices that have ever been connected or are currently connected to a protected computer and generates allowing rules list basing on system data for detected devices. Upon task completion the application creates XML file in folder that is situated by path specified in the task settings. You can configure automatic import of the generated rules into the list of rules for the Device Control task.

This scenario is recommended to generate allowing rules list before the first start of the Device Control task, so that allowing rules generated cover all trusted external devices that are used on a protected computer.

Usage of system data about all connected devices

During the task running, Kaspersky Embedded Systems Security receives system data about all external devices that have ever been connected or that are currently connected to a protected computer, and displays detected devices in the list of the **Generate rules based on the system information** window.

For each detected device Kaspersky Embedded Systems Security parses the values of manufacturer (VID), controller type (PID), friendly name, serial number and device instance path. You can generate allowing rules for any mass storage device, whose data have been stored in the system, and straightly add newly created rules to the list of the device control rules.

This scenario is recommended to renew an already specified rules list when it is necessary to trust a little amount of new mass storage devices.

> Kaspersky Embedded Systems Security does not get access to system data about mobile devices connected via MTP. You cannot generate allowing rules for MTP-connected mobile devices.

Usage of the Device Control task in the Statistics only mode

XML file received upon the Device Control task completion in the **Statistics only** mode is generated basing on the task log.

During the task running Kaspersky Embedded Systems Security logs information about all connections of flash drives and other mass storage devices to a protected computer. You can generate allowing rules based on task events and export them to an XML file. Before starting the task in the **Statistics only** mode, it is recommended to configure the task running period so that during the term specified all the possible external devices connections to a protected computer would be performed.

This scenario is recommended to renew an already generated rules list if it is required to allow a large number of new external devices.

If the rule list generation according to this scenario is performed on a template machine, you can apply a generated allowing rules list while configuring the Device Control task via the Kaspersky Security Center. This way you will be able to allow to use the external devices that are connected to a template machine on all the computers included into a protected network.

About Rule Generator for Device Control task

The Rule Generator for Device Control task can automatically create a list of allowing rules for connected flash drives and other mass storage devices basing on the system data about all external devices that have ever been connected to a protected computer.

> Kaspersky Embedded Systems Security does not get access to system data about mobile devices connected via MTP. You cannot generate allowing rules for MTP-connected mobile devices.

Upon the task completion Kaspersky Embedded Systems Security creates an XML configuration file that contains allowing rules list for all detected external devices or straightly adds generated rules in the Device Control task depending on the Rule Generator for Device Control settings. The application will subsequently allow devices for which allowing rules were automatically generated.

Generated and added in the task rules are displayed in the **Device Control rules** window.

Device Control rules generation scenarios

You can generate rules (see Section "Generating Device Control rules for all computers via Kaspersky Security Center" on page 349) basing on Windows data about all mass storage devices that have ever been connected or are currently connected by three scenarios:

- Using the Rule Generator for Device Control group task. Use this scenario during the rule generation process to take into account all ever connected mass storage devices that are registered by the systems on all network computers.
- Using the **Generate rules based on system data** option. Use this scenario during the rule generation process to take into account all ever connected mass storage devices that are and registered by the system of the computer with a Kaspersky Security Center Administration Console installed.
- Using the **Generate rules based on connected devices** in the **Device Control rules** window and the Rule Generator for Device Control task settings. Use this method if you want to consider only data about devices currently connected to the protected computer when generating allowing rules.

> Kaspersky Embedded Systems Security does not get access to system data about mobile devices connected via MTP. You cannot generate allowing rules for trusted MTP-connected mobile devices using scenarios for rules list filling on the base of system data about all connected devices.

Device Control default task settings

By default, the Device Control task has the settings described in the table below. You can change the values of these settings.

Table 50. Default Device Control task settings

Setting	Default Value	Description
Task mode	**Statistics only**	The task logs information about external devices that were blocked or allowed according to the specified rules. External devices are not actually blocked. You can select the **Active** mode for computer protection to actually block the use of external devices.
Allow using all mass storage devices when the Device Control task is not running	Not applied	Kaspersky Embedded Systems Security blocks use of external devices, regardless of the Device Control task state. This provides maximum protection level against computer security threats arising when exchanging files with external devices. You can adjust the setting so that Kaspersky Embedded Systems Security allows use of all external devices when the Device Control task is not running.
Task start schedule	First run is not scheduled.	The Device Control task does not start automatically at the start of Kaspersky Embedded Systems Security. You can configure the task start schedule.

Table 51. Rule Generator for Device Control task default settings

Setting	Default Value	Description
Task mode	**Consider system data about all mass storages that have ever been connected**	The task operation mode. You can select the **Consider currently connected mass storages only** task mode.
Actions upon task completion	Allowing rules are added to the list of Device Control rules; new rules are merged with existing ones; duplicated rules are removed.	You can add rules to existing ones without merging them and without deleting duplicated rules, or replace existing rules with new allowing rules, or configure export of allowing rules to a file.
Task start schedule	First run is not scheduled.	The Rule Generator for Device Control task does not start automatically at startup of Kaspersky Embedded Systems Security. You can start the task manually or configure a scheduled start.

Managing Device Control via the Administration Plug-in

In this section, learn how to navigate through the Administration Plug-in interface and manage connections of any mass storage devices to all computers on the network by generating rule lists via the Kaspersky Security Center for the groups of computers.

In this section

Navigation

Learn how to navigate to the required task settings via the interface.

In this section

Opening policy settings for the Device Control task

► *To open the Device Control task settings via the Kaspersky Security Center policy:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure the task.
3. Select the **Policies** tab.
4. Double-click the policy name you want to configure.
5. In the **Properties: <Policy name>** window that opens, select the **Local activity control** section.
6. Click the **Settings** button in the **Device Control** subsection.

   The **Device Control** window opens.
7. Configure the policy as required.

Opening the Device Control rules list

► *To open the Device Control rules list via the Kaspersky Security Center:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure the task.
3. Select the **Policies** tab.
4. Double-click the policy name you want to configure.
5. In the **Properties: <Policy name>** window that opens, select the **Local activity control** section.
6. Click the **Settings** button in the **Device Control** subsection.

   The **Device Control** window opens.
7. On the **General** tab, click the **Rules list** button.

   The **Device Control rules** window opens.
8. Configure the policy as required.

Opening the Rule Generator for Device Control task wizard and properties

► *To initialize creation of a Rule Generator for Device Control task:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure the task.
3. Select the **Tasks** tab.
4. Click **Create a task** button.

   The **New Task Wizard** window opens.
5. Select the **Rule Generator for Device Control** task.
6. Click **Next**.

   The **Settings** window opens.

► *To configure the existing Rule Generator for Device Control task:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure the task.
3. Select the **Tasks** tab.
4. Double-click the task name in the list of Kaspersky Security Center tasks.

   The **Properties: Rule Generator for Device Control** window opens.

See the Configuring the Rule Generator for Device Control task section for for details on configuring the task.

Configuring the Device Control task

► *To configure the Device Control task settings:*

1. Open the **Device Control** window (see Section "Opening policy settings for the Device Control task" on page 346).
2. On the **General** tab, configure the following task settings:
   - In the **Task mode** section, select one of the task modes:
     - **Active**.

       Kaspersky Embedded Systems Security applies rules to control the connection of flash-drives and other external devices, and allows or blocks the use of all devices according to the Default Deny principle and specified allowing rules. The use of trusted external devices is allowed. The use of untrusted external devices is blocked by default.

       If an external device you consider to be untrusted is connected to a protected computer before the Device Control task is run in the Active mode, the device is not blocked by the application. We recommend that you disconnect the untrusted device manually or restart the computer. Otherwise, the Default Deny principle will not be applied to the device.

     - **Statistics only**.

       Kaspersky Embedded Systems Security does not control the connection of flash-drives and other external devices, but only logs information about the connection and registration of external devices on a protected computer, and about the Device Control allowing rules triggered by the connected devices. The use of all external devices is allowed. This mode is set by default.
   - Select or clear the **Allow using all mass storage devices when the Device Control task is not running** check box.

     The check box allows or blocks the use of mass storage devices when the Device Control task is not running.

     If the check box is selected and Device Control task is not running, Kaspersky Embedded Systems Security allows using any mass storage devices on a protected computer.

     If the check box is cleared, the application blocks the use of untrusted mass storage devices on a protected computer in the following cases: the Device Control task is not running or the Kaspersky Security Service is turned off. This option is recommended to maximize the level of protection against computer security threats arising when exchanging files with external devices.

     The check box is cleared by default.
3. Click the **Rules list** button to edit the list of Device control rules (see Section "Configuring Device Control rules via the Kaspersky Security Center" on page 351).
4. If necessary, configure the scheduled task start settings on the **Task management** tab.
5. Click **OK**.

Kaspersky Embedded Systems Security immediately applies the new 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.

Generating Device Control rules for all computers via Kaspersky Security Center

You can create lists of Device Control rules using Kaspersky Security Center tasks for all computers and groups of computers on the corporate network at once.

You can create lists of Device Control rules on the side of Kaspersky Security Center in the following ways:

- Using the Rule Generator for Device Control group task.

  According to this scenario the group task generates rules lists basing on each computer system data about all mass storage devices that have ever been connected to protected computers. The task also allows for all mass storage devices that a connected at the moment of task running. Upon the group task completion Kaspersky Embedded Systems Security generates allowing rules lists for all mass storage devices registered in the network and saves these lists in an XML file in a specified folder. Then you can manually import generated rules in the Device Control task settings. Unlike a task on a local computer, the policy does not allow configuring the automatic addition of the created rules to the list of Device Control rules when the Rule Generator for Device Control group task is completed.

  This scenario is recommended to generate allowing rules list before the first Device Control task start in the mode of **Active** rules application.

  > Before using the Device Control policy in the network, make certain that all protected computers have access to a shared network folder. If the organization’s policy does not provide for the use of a shared network folder in the network, it is recommended to start the Rule Generator for Device Control task for computer control rules on the test computer group or on a template machine.

- Based on a report on task events generated in Kaspersky Security Center for the Device Control task in the **Statistics only** mode.

  According to this scenario Kaspersky Embedded Systems Security does not restrict mass storage devices connections but logs information about all devices connections and mass storage devices registration on all network computers during the Device Control task running in the **Statistics only** mode. The information logged may be found in the **Events** tab of the **Administration Server** node's workspace in the Kaspersky Security Center. Kaspersky Security Center generates unified list of mass storage devices restricting and allowing events, based on the task log.

  You should configure the task running period the way that all the mass storage devices connections would be performed during the set period. Then as rules are added to the Device Control task you can import data on devices connections from the saved Kaspersky Security Center event report file (in TXT format) and generate Device Control allowing rules for such devices basing on this data. The type of events, that an imported log is based on, does not influence the generated rules type; only allowing rules are generated.

  This scenario is recommended to add allowing rules for a large number of new mass storage devices, as well as to generate rules for MTP-connected trusted mobile devices.

- Based on system data about connected mass storage devices (using the **Generate rules based on system data** option in the Device Control task settings).

  According to this scenario Kaspersky Embedded Systems Security generates allowing rules for mass storage devices that have ever been connected or are currently connected to a computer with Kaspersky Security Center installed.

  This scenario is recommended to generate rules for a little number of new mass storage devices that you want to trust on all computers in the network.

- Based on data about the currently connected devices (using the **Generate rules based on connected devices**).

  In this scenario, Kaspersky Embedded Systems Security generates allowing rules only for currently connected devices. You can select one or more devices for which you want to generate allowing rules.

  > Kaspersky Embedded Systems Security does not get access to system data about mobile devices connected via MTP. You cannot generate allowing rules for trusted MTP-connected mobile devices using scenarios for rules list filling on the base of system data about all connected devices.

Configuring the Rule Generator for Device Control task

► *To configure the Rule Generator for Device Control task, do the following:*

1. Open the **Properties: Rule Generator for Device Control** (see Section "**Opening the Rule Generator for Device Control task wizard and properties**" on page 347) window.
2. In the **Notification** section, configure the task event notification settings.

   > For detailed information regarding configuring settings in this section, see the *Kaspersky Security Center Help*.

3. In the **Settings** section, you can configure the following settings:
   - Select the operation mode: consider system data about all mass storages that have ever been connected or consider currently connected mass storages only.
   - Configure settings for configuration files with allowing rules lists that Kaspersky Embedded Systems Security creates upon the task completion.
4. Configure the task schedule in the **Schedule** section (you can configure a schedule for all task types except Rollback of Database Update).
5. In the **Account** section specify the account which rights will be used for the task execution.
6. If required, specify the objects to exclude from the task scope in the **Exclusions from task scope** section.

   > For detailed information regarding configuring settings in these sections, see the *Kaspersky Security Center Help*.

7. In the **Properties: <Task name>** window, click **OK**.

   The newly configured group tasks settings are saved.

Configuring Device Control rules via the Kaspersky Security Center

Learn how to generate a list of rules based on various criteria or manually create allowing or denying rules using the Device Control task.

In this section

Creating allowing rules based on system data in a Kaspersky Security Center policy

► *To specify allowing rules using the **Generate rules based on system data** option in the Device Control task:*

1. If necessary, connect a new mass storage device that you want to make trusted to a computer with the Kaspersky Security Center Administration Console installed.
2. Open the **Device Control rules** window (see Section "Opening the Device Control rules list" on page 347).
3. Click the **Add** button and in the context menu that opens select the **Generate rules based on system data** option.
4. Select the principle for adding the allowing rules to the list of previously created Device Control rules:
   - In the device list of **Generate rules based on the system information** window, select a device.
   - Click **Add rules for devices selected**.
5. Click the **Save** button in the **Device Control rules** window.

Rules list in the Device Control task will be filled up with new rules generated basing on a system data of the computer with the Kaspersky Security Center Administration Console installed.

Generating rules for connected devices

► *To specify allowing rules using the **Generate rules based on connected devices** option in the Device Control task:*

1. Open the **Device Control rules** (see Section "**Opening the Device Control rules list**" on page 347) window.
2. Click the **Add** button and in the context menu, select **Generate rules based on connected devices**.

   The **Generate rules based on the system information** window opens.
3. In the list of detected devices connected to the protected computer, select the devices you want to generate allowing rules for.
4. Click the **Add rules for devices selected** button.

5. Click the **Save** button in the **Device Control rules** window.

Rules list in the Device Control task will be filled up with new rules generated basing on a system data of the computer with the Kaspersky Security Center Administration Console installed.

Importing rules from the Kaspersky Security Center report on blocked devices

You can import data on blocked device connections from the report generated in Kaspersky Security Center after completion of the Device Control task in **Statistics only** mode (see Section "Configuring the Device Control task" on page 348) and use this data to generate a list of Device Control allowing rules in the policy being configured.

When generating the report on events occurring during the Device Control task, you can keep track of the devices whose connection is restricted.

► *To specify allowing rules for devices connection for a group of computers based on the Kaspersky Security Center report on blocked devices:*

1. In the policy properties, in the **Event notification** section, make sure that:
   - For the **Critical Events** importance level the period of time for storing the task log for the *Mass storage restricted* event exceeds the planned period of operation in the **Statistics only** mode (the default value is 30 days).
   - For the **Warning** importance level the period of time for storing the task log for the *Statistics only: untrusted mass storage detected* event exceeds the planned period of task operation in the **Statistics only** mode (the default value is 30 days).

   When the period for storing the events elapses, information about logged events is deleted and is not reflected in the report file. Before running the Device Control task in **Statistics only** mode, make sure that the task run time does not exceed the configured storage time for the specified events.

2. Start the Device Control task in the **Statistics only** mode. In the workspace of the **Administration Server** node in Kaspersky Security Center**,** select the **Events** tab. Click the **Create a selection** button and create a selection of events based on the *Untrusted mass storage detected* criterion to view the devices whose connections will be restricted by the Device Control task. In the details pane of the selection, click the **Export events to file** link to save the report on restricted connections to a TXT file.

   Before importing and applying the generated report in a policy, make sure that the report contains data only on those devices whose connection you want to allow.

3. Import data about restricted devices connections into the Device Control task:

   a. Open the **Device Control rules** window (see Section "Opening the Device Control rules list" on page 347).

   b. Click the **Add** button and in the context menu of the button select **Import data of blocked devices from Kaspersky Security Center report**.

c. Select the principle for adding rules from the list created on the basis of the Kaspersky Security Center report to the list of previously configured Device Control rules:

  - **Add to existing rules** if you want to add the imported rules to the list of existing rules. Rules with identical settings are duplicated.
  - **Replace existing rules** if you want to replace the existing rules with the imported rules.
  - **Merge with existing rules** if you want to add the imported rules to the list of existing rules. Rules with identical settings are not added; the rule is added if at least one rule parameter is unique.

d. In the standard window of Microsoft Windows that opens, select the TXT file to which events from the report about restricted devices have been exported.

e. Click the **Save** button in the **Device Control rules** window.

4. Click **OK** the **Device Control** window.

Rules created on the basis of the Kaspersky Security Center report on restricted devices are added to the list of Device Control rules.

Creating rules using the Rule Generator for Device Control task

► *To specify allowing device control rules for a group of computers using the Rule Generator for Device Control task:*

1. Open the **Settings** window in the **New Task Wizard** (see Section "**Opening the Rule Generator for Device Control task wizard and properties**" on page 347).
2. Configure the following:
   - In the **Mode** section:
     - **Consider system data about all mass storages that have ever been connected**.
     - **Consider currently connected mass storages only**.
   - In the **After task completes** section:
     - **Add allowing rules to the list of Device Control rules**.

       The check box enables or disables adding the newly generated allowing rules to the list of Device Control rules. The list of Device Control rules is displayed when you click the **Device Control rules** link in the details pane of the **Device Control** node.

       If this check box is selected, Kaspersky Embedded Systems Security adds the rules generated by the Rule Generator for Device Control task to the list of Device Control rules based on the selected principle for adding rules.

       If this check box is cleared, Kaspersky Embedded Systems Security does not add the newly generated allowing rules to the list of Device Control rules. The generated rules are only exported to a file.

       The check box is selected by default.

       The check box cannot be selected if the **Export allowing rules to file** check box has not been selected.

- **Principle of adding**.

  This drop-down list is used to specify the method used to add the newly generated allowing rules to the list of Applications Launch Control rules.

  - **Add to existing rules**. The rules are added to the list of existing rules. Rules with identical settings are duplicated.
  - **Replace existing rules**. The rules replace the existing rules in the list.
  - **Merge with existing rules**. The rules are added to the list of existing rules. Rules with identical settings are not added; the rule is added if at least one rule parameter is unique.

  By default, the **Merge with existing rules** method is selected.

- **Export allowing rules to file**.

  The check box enables or disables export of allowing rules for Device Control to a file.

  If the check box is selected, Kaspersky Embedded Systems Security exports the allowing rules to the file specified in the field below when the Rule Generator for Device Control task is finished.

  If this check box is cleared, the application does not export the generated allowing rules to a file when the Rule Generator for Device Control task is finished. Instead, it only adds them to the list of Device Control rules.

  The check box is cleared by default.

  The check box cannot be selected if the **Add allowing rules to the list of Device Control rules** check box has not been selected.

- **Add computer details to file name**.

  The check box enables or disables adding information about the protected computer to the name of the file to which the allowing rules will be exported.

  If this check box is selected, the application adds the protected computer name and the file creation date and time to the name of the export file.

  If the check box is cleared, the application does not add information about the protected computer to the name of the export file.

  The check box is selected by default.

3. Click **Next**.
4. In the **Schedule** window, set the scheduled task start settings.
5. Click **Next**.
6. In the **Selecting an account to run the task** window, specify the account you want to use.
7. Click **Next**.
8. Define a task name.
9. Click **Next**.

> The task name should be no longer than 100 characters and cannot contain the following symbols: " * < > & \ : |

The **Finish task creation** window opens.

10. You can optionally run the task after the Wizard finishes by selecting the **Run task after Wizard finishes** check box.
11. Click **Finish** to finish creating the task.
12. On the **Tasks** tab on the workspace of the group of computers being configured, in the list of group tasks select the Rule Generator for Device Control you have created.
13. Click the **Start** button to start the task.

    When the task is completed, automatically generated lists of allowing rules are saved in a shared folder in XML files.

    > Before using the Device Control policy in the network, make certain that all protected computers have access to a shared network folder. If the organization's policy does not provide for the use of a shared network folder in the network, it is recommended to start the Rule Generator for Device Control task for computer control rules on the test computer group or on a template machine.

Adding generated rules to the Device Control rules list

► *To add the generated lists of allowing rules to the Device Control task:*

1. Open the **Device Control rules** window (see Section "Opening the Device Control rules list" on page 347).
2. Click the **Add** button.
3. In the **Add** button context menu select the **Import rules from XML file** option.
4. Select the principle for adding the automatically generated allowing rules to the list of previously created Device Control rules:
   - **Add to existing rules** if you want to add the imported rules to the list of existing rules. Rules with identical settings are duplicated.
   - **Replace existing rules** if you want to replace the existing rules with the imported rules.
   - **Merge with existing rules** if you want to add the imported rules to the list of existing rules. Rules with identical settings are not added; the rule is added if at least one rule parameter is unique.
5. In the standard window of Microsoft Windows that opens, select XML files created after completion of the Rule Generator for Device Control group task.
6. Click **Open**.

   All generated rules from the XML file are added to the list according to the selected principle.
7. Click the **Save** button in the **Device Control rules** window.
8. If you want to apply generated device control rules, select the **Active** task mode in the **Device Control** policy settings.

Allowing rules automatically generated based on system data on each separate computer are applied to all network computers covered by the policy being configured. On these computers, the application will allow connection of only those devices for which allowing rules have been created.

Managing Device Control via the Application Console

In this section, learn how to navigate the Application Console interface and configure task settings on a local computer.

In this section

Navigation

Learn how to navigate to the required task settings via the interface.

In this section

Opening the Device Control task settings

► *To open the Device Control task settings via the Application Console:*

1. In the Application Console tree, expand the **Computer Control** node.
2. Select the **Device Control** child node.
3. In the details pane of the **Device Control** child node, click the **Properties** link.

   The **Task settings** window opens.
4. Configure the task as required.

Opening the Device Control rules window

► *To open the Device Control rules list via the Application Console:*

1. In the Application Console tree, expand the **Computer Control** node.
2. Select the **Device Control** child node.

3. In the details pane of the **Device Control** node, click the **Device Control rules** link.

   The **Device Control rules** window opens.

4. Configure the rules list as required.

Opening the Rule Generator for Device Control task settings

► *To configure the Rule Generator for Device Control task:*

1. In the Application Console tree, expand the **Automated rule generators** node.
2. Select the **Rule Generator for Device Control** child node.
3. In the details pane of the **Rule Generator for Device Control** child node, click the **Properties** link.

   The **Task settings** window opens.

4. Configure the task as required.

Configuring Device Control task settings

► *To configure the Device Control task settings:*

1. Open the **Task settings** window (see Section "Opening the Device Control task settings" on page 356).
2. On the **General** tab, configure the following task settings:
   - In the **Task mode** section, select one of the task modes:
     - **Active**.

       Kaspersky Embedded Systems Security applies rules to control the connection of flash-drives and other external devices, and allows or blocks the use of all devices according to the Default Deny principle and specified allowing rules. The use of trusted external devices is allowed. The use of untrusted external devices is blocked by default.

       If an external device you consider to be untrusted is connected to a protected computer before the Device Control task is run in the Active mode, the device is not blocked by the application. We recommend that you disconnect the untrusted device manually or restart the computer. Otherwise, the Default Deny principle will not be applied to the device.

     - **Statistics only**.

       Kaspersky Embedded Systems Security does not control the connection of flash-drives and other external devices, but only logs information about the connection and registration of external devices on a protected computer, and about the Device Control allowing rules triggered by the connected devices. The use of all external devices is allowed. This mode is set by default.

   - Select or clear the **Allow using all mass storage devices when the Device Control task is not running** check box.

     The check box allows or blocks the use of mass storage devices when the Device Control task is not running.

     If the check box is selected and Device Control task is not running, Kaspersky Embedded Systems Security allows using any mass storage devices on a protected computer.

If the check box is cleared, the application blocks the use of untrusted mass storage devices on a protected computer in the following cases: the Device Control task is not running or the Kaspersky Security Service is turned off. This option is recommended to maximize the level of protection against computer security threats arising when exchanging files with external devices.

The check box is cleared by default.

3. If necessary, on the **Schedule** and **Advanced** tabs, configure the scheduled task start settings (see Section "Configuring the task start schedule settings" on page 149).
4. To edit the list of device control rules (see Section "About Device Control rules list filling" on page 342), click the **Device Control rules** link in the lower part of the details pane of the **Device Control** node.

Kaspersky Embedded Systems Security immediately applies the new 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 system audit log.

Configuring Device Control rules

Learn how to generate, import and export a list of rules, or manually create allowing or denying rules using the Device Control task.

In this section

Importing Device Control rules from XML file

► *To import the Device Control rules, take the following steps:*

1. Open the **Device Control rules** (see Section "**Opening the Device Control rules window**" on page 356) window.
2. Click the **Add** button.
3. In the context menu of the button, select **Import rules from XML file**.

4. Specify the method for adding the imported rules. To do so, select one of the options from the context menu of the **Import rules from XML file** button:

    - **Add to existing rules** if you want to add the imported rules to the list of existing ones. Rules with identical settings are duplicated.
    - **Replace existing rules** if you want to replace the existing rules with the imported ones.
    - **Merge with existing rules** if you want to add the imported rules to the list of existing ones. Rules with identical settings are not added; the rule is added if at least one rule parameter is unique.

    The standard Microsoft Windows **Open** window opens.

5. In the **Open** window, select the XML file that contains the settings of the Device Control rules.
6. Click the **Open** button.

The imported rules will be displayed in the list of the **Device Control rules** window.

Filling rules list basing on Device Control task events

► *To create a configuration file that contains device control rules list basing on the Device Control task events:*

1. Start the Device Control task in the **Statistics only** (see Section "**Configuring Device Control task settings**" on page 357) mode, to log all events of flash drives and other external devices connections to a protected computer.
2. Upon the completion of the task in the **Statistics only** mode, open the task log by clicking the **Open task log** button in the **Management** section of the **Device Control** node details pane.
3. In the **Logs** window click the **Generate rules based on events**.

Kaspersky Embedded Systems Security will create an XML configuration file that contains a rules list generated basing on events of the Device Control task in the **Statistics only** mode. You can apply this list in the Device Control task (see Section "Importing Device Control rules from XML file" on page 358).

Before applying a rules list generated basing on the task events, it is recommended to review and then manually process the rules list to make certain that there are no untrusted devices allowed by the specified rules.

During the conversion of an XML file with the task events to a rules list, the application generates allowing rules for all registered events, including the devices restrictions.

All the task events are registered in the task log regardless of the task mode. You can create a configuration file with a rules list basing on the events of the task in the **Active** mode. This scenario is not recommended except urgent cases, as far as the task efficiency requires to generate a final rule list version before the task is run in the active mode.

Adding an allowing rule for one or several external devices

The function of manual adding rules by ones is not supported in the Device Control task. However, in cases when you need to add rules for one or several new external devices you can use the **Generate rules basing on system data** option. If this scenario is applied, the application uses Windows data about all ever connected external devices and also allows for currently connected devices for filling an allowing rules list.

> Kaspersky Embedded Systems Security does not get access to system data about mobile devices connected via MTP. You cannot generate allowing rules for MTP-connected mobile devices.

► *To add an allowing rule for one or several external devices that are currently connected:*

1. Open the **Device Control rules** window (see Section "Opening the Device Control rules window" on page 356).
2. Click the **Add** button.
3. In the context menu that opens select the **Generate rules based on system data** option.
4. In the window that opens, review the detected devices list and select a single device or several devices that you want to trust on a protected computer.
5. Click the **Add rules for devices selected** button.

New rules will be generated and added to the device control rules list.

Removing Device Control rules

► *To remove the Device Control rules:*

1. Open the **Device Control rules** (see Section "**Opening the Device Control rules window**" on page 356) window.
2. In the list, select one or several rules that you want to delete.
3. Click the **Remove Selected** button.
4. Click the **Save** button.

The selected Device Control rules will be removed.

Exporting Device Control rules

► *To export Device Control rules to a configuration file:*

1. Open the **Device Control rules** (see Section "**Opening the Device Control rules window**" on page 356) window.
2. Click the **Export to a file** button.

   The standard Microsoft Windows window opens.
3. In the window that opens, specify the file to which you want to export the rules. If no such file exists, it will be created. If a file with the specified name already exists, its contents will be rewritten after the rules are exported.

4. Click the **Save** button.

The rules and its settings will be exported in the specified file.

Activating and deactivating of Device Control rules

You can activate and deactivate created device control rules without removing them.

► *To activate or deactivate a created device control rule, take the following steps:*

1. Open the **Device Control rules** (see Section "**Opening the Device Control rules window**" on page 356) window.
2. In the list of specified rules open the **Rule properties** window by double clicking on the rule whose properties you want to configure.
3. In the window that opens, select or clear the **Apply rule** check box.

   The check box enables or disables a device control rule.

   If the check box is selected for a rule, the rule is activated. Connection for the external devices that are included into the rule usage scope is allowed.

   If the check box is cleared in the rule properties, the rule is inactive. Connection for the external devices that are included into the rule usage scope is blocked.

   By default the check box is selected in the settings for each created rule.
4. Click **OK**.

Rule apply status will be saved and displayed for a specified rule.

Expanding Device Control rules usage scope

Each automatically generated device control rule covers only one external device. You can manually expand a rule usage scope by setting the device instance path mask in properties of any specified rule.

Device instance path application reduces the total number of rules specified and simplifies rules processing. But expanding of a rule usage scope can lead to decreasing of mass storage devices control efficiency.

► *To apply a device instance path mask in a device control rule properties:*

1. Open the **Device Control rules** (see Section "**Opening the Device Control rules window**" on page 356) window.
2. In the window that opens, select a rule to use its properties for mask application.
3. Open the **Rule properties** window by double clicking on a selected device control rule.
4. In the window that opens, perform the following operations:
   - Select the **Use mask** check box next to the **Controller type (PID)** field if you want a rule selected to allow connections for all mass storage devices that fit the specified information about device manufacturer and device serial number.

- Select the **Use mask** check box next to the **Serial number** field if you want a rule selected to allow connections for all mass storage devices that fit the specified information about device manufacturer and controller type.
- Select the **Use mask** check boxes next to the **Controller type (PID)** field and the **Serial number** field if you want a rule selected to allow connections for all mass storage devices that fit the specified information about device manufacturer.

If the **Use mask** check box is selected in at least one of the fields, the data from the fields with the selected check box is replaced with the * sign and is not considered when the rule is applied.

5. If necessary, specify additional information about rule in the **Description** field. For example, specify the devices affected by the rule.
6. Click **OK**.

The newly configured rule properties will be saved. The rule usage scope will be expanded according to a device instance path mask specified.

Configuring Rule Generator for Device Control task

► *To configure the Rule Generator for Device Control task:*

1. In the Application Console tree, expand the **Automated rule generators** node.
2. Select the **Rule Generator for Device Control** child node.
3. Click the **Properties** link in the details pane of the **Rule Generator for Device Control** node.

   The **Task settings** window opens.
4. On the **General** tab, select the task operation mode in the **Task mode** section:
   - **Consider system data about all mass storages that have ever been connected**.
   - **Consider currently connected mass storages only**.
5. In the **After task completes** section, specify the actions that must be performed by Kaspersky Embedded Systems Security upon task completion:
   - **Add allowing rules to the list of Device Control rules**.

     The check box enables or disables adding the newly generated allowing rules to the list of Device Control rules. The list of Device Control rules is displayed when you click the **Device Control rules** link in the details pane of the **Device Control** node.

     If this check box is selected, Kaspersky Embedded Systems Security adds the rules generated by the Rule Generator for Device Control task to the list of Device Control rules based on the selected principle for adding rules.

     If this check box is cleared, Kaspersky Embedded Systems Security does not add the newly generated allowing rules to the list of Device Control rules. The generated rules are only exported to a file.

     The check box is selected by default.

     The check box cannot be selected if the **Export allowing rules to file** check box has not been selected.

- **Principle of adding**.

  This drop-down list is used to specify the method used to add the newly generated allowing rules to the list of Applications Launch Control rules.

  - **Add to existing rules**. The rules are added to the list of existing rules. Rules with identical settings are duplicated.
  - **Replace existing rules**. The rules replace the existing rules in the list.
  - **Merge with existing rules**. The rules are added to the list of existing rules. Rules with identical settings are not added; the rule is added if at least one rule parameter is unique.

  By default, the **Merge with existing rules** method is selected.

- **Export allowing rules to file**.

  The check box enables or disables export of allowing rules for Device Control to a file.

  If the check box is selected, Kaspersky Embedded Systems Security exports the allowing rules to the file specified in the field below when the Rule Generator for Device Control task is finished.

  If this check box is cleared, the application does not export the generated allowing rules to a file when the Rule Generator for Device Control task is finished. Instead, it only adds them to the list of Device Control rules.

  The check box is cleared by default.

  The check box cannot be selected if the **Add allowing rules to the list of Device Control rules** check box has not been selected.

- **Add computer details to file name**.

  The check box enables or disables adding information about the protected computer to the name of the file to which the allowing rules will be exported.

  If this check box is selected, the application adds the protected computer name and the file creation date and time to the name of the export file.

  If the check box is cleared, the application does not add information about the protected computer to the name of the export file.

  The check box is selected by default.

6. On the **Schedule** and **Advanced** tabs, configure the scheduled task start settings (see Section "Configuring the task start schedule settings" on page 149).
7. Click **OK**.

Kaspersky Embedded Systems Security immediately applies the new 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 system audit log.

Firewall Management

This section contains information about the Firewall Management task and how to configure it.

In this chapter

About the Firewall Management task

Kaspersky Embedded Systems Security provides a reliable and ergonomic solution for protecting network connections using the Firewall Management task.

The Firewall Management task does not perform independent network traffic filtering, but it allows you to manage Windows Firewall through the Kaspersky Embedded Systems Security graphical interface. During the Firewall Management task Kaspersky Embedded Systems Security takes over management of the settings and policies of the operation system's firewall and blocks any possibility of external firewall configuration.

During installation of the application, the Firewall Management component reads and copies the Windows Firewall status and all specified rules. After that, the set of rules and the rule parameters may only be changed, and the firewall may only be turned on or off in Kaspersky Embedded Systems Security.

If Windows Firewall is turned off during installation of Kaspersky Embedded Systems Security, the Firewall Management task will not be executed after the installation completes. If Windows Firewall is turned on during installation of the application, the Firewall Management task is executed after the installation completes, blocking all network connections that are not allowed by the specified rules.

The Firewall Management component is not installed by default, as it is not included in the set of components for the Recommended Installation.

The Firewall Management task enforces blocking of all incoming and outgoing connections not allowed by the task's specified rules.

The task polls the Windows Firewall regularly and monitors its status. By default, the polling interval is set to 1 minute and cannot be changed. If during polling Kaspersky Embedded Systems Security detects a mismatch between the Windows Firewall settings and the Firewall Management task settings, the application forcibly applies the task settings on the operating system firewall.

With minute-by-minute polling of the Windows Firewall, Kaspersky Embedded Systems Security monitors the following:

- Operating status of the Windows Firewall.
- Status of rules added after installation of Kaspersky Embedded Systems Security by other applications or tools (for example, the addition of a new application rule for a port/application using wf.msc).

When applying the new rules to Windows Firewall, Kaspersky Embedded Systems Security creates a Kaspersky Security Group rule set in the **Windows Firewall** snap-in. This rule set unites all the rules created by Kaspersky Embedded Systems Security using the Firewall Management task. The rules in the Kaspersky Security Group are not monitored by the application during the polling each minute and are not automatically synchronized with the list of rules specified in the Firewall Management task settings.

► *To update the Kaspersky Security Group rules manually,*

restart the Kaspersky Embedded Systems Security Firewall Management task.

You can also edit the Kaspersky Security Group rules manually using the **Windows Firewall** snap-in.

If Windows Firewall is managed by the Kaspersky Security Center group policy, the Firewall Management task cannot be started.

About Firewall rules

The Firewall Management task controls filtration of incoming and outgoing network traffic using allowing rules forcibly applied to the Windows Firewall during task execution.

The first time the task is started Kaspersky Embedded Systems Security reads and copies all the incoming network traffic rules specified in the Windows Firewall settings to the Firewall Management task settings. Then the application operates according to the following rules:

- If a new rule is created in the Windows Firewall settings (manually or automatically during a new application installation), Kaspersky Embedded Systems Security deletes the rule.
- If an existing rule is deleted from the Windows Firewall settings, Kaspersky Embedded Systems Security restores the rule when the task is restarted.
- If the parameters of an existing rule are changed in the Windows Firewall settings, Kaspersky Embedded Systems Security rolls back the changes.
- If a new rule is created in the Firewall Management settings, Kaspersky Embedded Systems Security forcibly applies the rule to Windows Firewall.
- If an existing rule is deleted from the Firewall Management settings, Kaspersky Embedded Systems Security forcibly deletes the rule from the Windows Firewall settings.

Kaspersky Embedded Systems Security does not work with blocking rules or rules controlling outgoing network traffic. Upon start of the Firewall Management task, Kaspersky Embedded Systems Security deletes all such rules from the Windows Firewall settings.

You can set, delete and edit filtration rules for incoming network traffic.

> You cannot specify a new rule to control outgoing network traffic in the Firewall Management task settings. All Firewall rules specified in Kaspersky Embedded Systems Security control only incoming network traffic.

You can manage the following types of Firewall rules:

- Application rules.
- Port rules.

Application rules

This type of rule allows targeted network connections for specified applications. The triggering criterion for these rules is based on a path to an executable file.

You can manage application rules:

- Add new rules.
- Remove existing rules.
- Enable or disable specified rules.
- Edit the parameters of the specified rules: specify the rule name, path to the executable file, and the rule usage scope.

Port rules

This type of rule allows network connections for specified ports and protocols (TCP / UDP). The triggering criteria for these rules are based on the port number and protocol type.

You can manage port rules:

- Add new rules.
- Remove existing rules.
- Enable or disable specified rules.
- Edit the parameters of the specified rules: set the rule name, port number, protocol type, and scope for application of the rule.

> Port rules imply a broader scope than application rules. By allowing connections based on port rules, you lower the security level of the protected computer.

Default Firewall Management task settings

The Firewall Management task uses the default settings described in the table below. You can change the values of these settings.

Table 52. Default Firewall Management task settings

Setting	Default value	Description
Firewall rules for application	Two default rules for application enabled	You can disable the default rules or add new rules.
Firewall rules for ports	Six default rules for ports enabled	You can disable the default rules or add new rules.
Task start schedule	First run is not scheduled.	The Firewall Management task does not start automatically at the start of Kaspersky Embedded Systems Security. You can configure the task start schedule.

Managing Firewall rules via the Administration Plug-in

In this section, learn how to manage Firewall rules via the Application Console interface.

In this section

Enabling and disabling Firewall rules

► *To enable or disable an existing rule for filtering incoming network traffic, perform the following actions:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.
3. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring a policy" on page 112).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in the Application settings window of the Kaspersky Security Center" on page 117).

   > If an active Kaspersky Security Center policy is applied to a device, and this policy blocks changes to application settings, then these settings cannot be edited in the **Application settings** window.

4. In the **Network activity control** section click the **Settings** button in the **Firewall Management** subsection.
5. Click the **Rules list** button in the window that opens.

   The **Firewall rules** window opens.
6. Depending on the type of the rule whose status you want to modify, select **Applications** or **Ports**.
7. In the rule list, select the rule whose status you want to modify and perform one of the following actions:
   - If you want to enable a disabled rule, select the check box to the left of the rule name.

     The selected rule is enabled.
   - If you want to disable an enabled rule, clear the check box to the left of the rule name.

     The selected rule is disabled.
8. Click **OK** in the **Firewall rules** window.
9. Click **OK** in the **Firewall Management** window.
10. Click **OK** in the **Properties: <Policy name>** window.

The specified task settings are saved. The new rule parameters will be sent to Windows Firewall.

Adding Firewall rules manually

> You can only add and edit rules for applications and ports. You cannot add new or edit existing group rules.

► *To add a new or edit an existing rule for filtering incoming network traffic, do the following:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.
3. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring a policy" on page 112).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in the Application settings window of the Kaspersky Security Center" on page 117).

   > If an active Kaspersky Security Center policy is applied to a device, and this policy blocks changes to application settings, then these settings cannot be edited in the **Application settings** window.
4. In the **Network activity control** section click the **Settings** button in the **Firewall Management** subsection.
5. Click the **Rules list** button in the window that opens.

   The **Firewall rules** window opens.
6. Depending on the type of rule you want to add, select the **Applications** or **Ports** tab and perform one of the following actions:
   - To edit an existing rule, select the rule you want to edit in the rule list and click **Edit**.

- To add a new rule, click **Add**.

  Depending on the type of rule being configured, the **Port rule** window or **Application rule** window opens.

7. In the window that opens, perform the following operations:
   - If you are working with an application rule, do the following:
     a. Enter the **Rule name** of the edited rule.
     b. Specify the **Application path** to the executable file of the application for which you are allowing a connection by modifying this rule.

        You can set the path manually or by using the **Browse** button.
     c. In the **Rule application scope** field, specify the network addresses for which the modified rule will be applied.

     > You can only use IPv4 IP-addresses.

   - If you are working with a port rule, do the following:
     a. Enter the **Rule name** of the edited rule.
     b. Specify the **Port number** for which the application will allow connections.
     c. Select the type of protocol (TCP / UDP) for which the application will allow connections.
     d. In the **Rule application scope** field, specify the network addresses for which the modified rule will be applied.

     > You can only use IPv4 IP-addresses.

8. Click **OK** in the **Application rule** or **Port rule** window.
9. Click **OK** in the **Firewall Management** window.
10. Click **OK** in the **Properties: <Policy name>** window.

The specified task settings are saved. The new rule parameters will be sent to Windows Firewall.

Deleting Firewall rules

> You can only delete application and port rules. You cannot delete existing group rules.

► *To delete an existing rule for filtering incoming network traffic, perform the following actions:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.
3. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring a policy" on page 112).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in the Application settings window of the Kaspersky Security Center" on page 117).

   > If an active Kaspersky Security Center policy is applied to a device, and this policy blocks changes to application settings, then these settings cannot be edited in the **Application settings** window.

4. In the **Network activity control** section click the **Settings** button in the **Firewall Management** subsection**.**
5. Click the **Rules list** button in the window that opens.

   The **Firewall rules** window opens.
6. Depending on the type of rule whose status you want to modify, select the **Applications** or **Ports** tab.
7. In the rule list, select the rule you want to delete.
8. Click the **Remove** button.

   The selected rule is deleted.
9. Click **OK** in the **Firewall rules** window.
10. Click **OK** in the **Firewall Management** window.
11. Click **OK** in the **Properties: <Policy name>** window.

The specified Firewall Management task settings are saved. The new rule parameters will be sent to Windows Firewall.

Managing Firewall rules via the Application Console

In this section, learn how to manage Firewall rules via the Application Console interface.

In this section

Enabling and disabling Firewall rules

► *To enable or disable an existing rule for filtering incoming network traffic, perform the following actions:*

1. In the Application Console tree, expand the **Computer Control** node.
2. Select the **Firewall Management** child node.
3. Click the **Firewall rules** link in the details pane of the **Firewall Management** node.

   The **Firewall rules** window opens.
4. Depending on the type of the rule whose status you want to modify, select **Applications** or **Ports**.
5. In the rule list, select the rule whose status you want to modify and perform one of the following actions:
   - If you want to enable a disabled rule, select the check box to the left of the rule name.

     The selected rule is enabled.
   - If you want to disable an enabled rule, clear the check box to the left of the rule name.

     The selected rule is disabled.
6. Click **Save** in the **Firewall rules** window.

The specified task settings are saved. The new rule parameters will be sent to Windows Firewall.

Adding Firewall rules manually

► *To add a new or edit an existing rule for filtering incoming network traffic, do the following:*

1. In the Application Console tree, expand the **Computer Control** node.
2. Select the **Firewall Management** child node.
3. Click the **Firewall rules** link in the details pane of the **Firewall Management** node.

   The **Firewall rules** window opens.

4. Depending on the type of rule you want to add, select the **Applications** or **Ports** tab and perform one of the following actions:
    - To edit an existing rule, select the rule you want to edit in the rule list and click **Edit**.
    - To add a new rule, click **Add**.

      Depending on the type of rule being configured, the **Port rule** window or **Application rule** window opens.
5. In the window that opens, perform the following operations:
    - If you are working with an application rule, do the following:
        a. Enter the **Rule name** of the edited rule.
        b. Specify the **Application path** to the executable file of the application for which you are allowing a connection by modifying this rule.

           You can set the path manually or by using the **Browse** button.
        c. In the **Rule application scope** field, specify the network addresses for which the modified rule will be applied.

      You can only use IPv4 IP-addresses.
    - If you are working with a port rule, do the following:
        a. Enter the **Rule name** of the edited rule.
        b. Specify the **Port number** for which the application will allow connections.
        c. Select the type of protocol (TCP / UDP) for which the application will allow connections.
        d. In the **Rule application scope** field, specify the network addresses for which the modified rule will be applied.

      You can only use IPv4 IP-addresses.
6. Click **OK** in the **Application rule** or **Port rule** window.
7. Click **Save** in the **Firewall rules** window.

The specified task settings are saved. The new rule parameters will be sent to Windows Firewall.

Deleting Firewall rules

You can only delete application and port rules. You cannot delete existing group rules.

► *To delete an existing rule for filtering incoming network traffic, perform the following actions:*

1. In the Application Console tree, expand the **Computer Control** node.
2. Select the **Firewall Management** child node.
3. Click the **Firewall rules** link in the details pane of the **Firewall Management** node.

The **Firewall rules** window opens.

4. Depending on the type of rule whose status you want to modify, select the **Applications** or **Ports** tab.
5. In the rule list, select the rule you want to delete.
6. Click the **Remove** button.

   The selected rule is deleted.
7. Click **Save** in the **Firewall rules** window.

The specified task settings are saved. The new rule parameters will be sent to Windows Firewall.

File Integrity Monitor

This section contains information about starting and configuring the File Integrity Monitor task.

In this chapter

About the File Integrity Monitor task

The File Integrity Monitor task is designed to track actions performed with the specified files and folders in the monitoring scopes specified in the task settings. You can use the task to detect file changes that may indicate a security breach on the protected computer. You can also configure file changes to be tracked during periods in which monitoring is interrupted.

A *monitoring interruption* occurs when the monitoring scope temporarily falls outside the scope of the task, e.g. if the task is stopped or if a mass storage device is not physically present on a protected computer. Kaspersky Embedded Systems Security reports detected file operations in the monitoring scope as soon as a mass storage device is reconnected.

> If the tasks stops running in the specified monitoring scope due to a reinstallation of the File Integrity Monitor component, this does not constitute a monitoring interruption. In this case, the File Integrity Monitor task is not run.

Requirements on the environment

To start the File Integrity Monitor task, the following conditions must be satisfied:

- A mass storage device that supports the ReFS and NTFS file systems must be installed on the protected computer.
- The Windows USN Journal must be enabled. The component queries this journal to receive information about file operations.

  > If you enable USN Journal after a rule has been created for a volume and the File Integrity Monitor task has been started, the task must be restarted. If not, the rule will not be applied during monitoring.

Excluded monitoring scopes

You can create excluded monitoring scopes (see Section "Configuring monitoring rules" on page 380). Exclusions are specified for each separate rule, and work only for the indicated monitoring scope. You can specify an unlimited number of exclusions for each rule.

> Exclusions have higher priority than the monitoring scope and are not monitored by the task, even if an indicated folder or file is in the monitoring scope. If the settings for one of the rules specify a monitoring scope at a lower level than a folder specified in exclusions, the monitoring scope is not considered when the task is run.

To specify exclusions, you can use the same masks that are used to specify monitoring scopes.

About file operation monitoring rules

The File Integrity Monitor is run based on file operation monitoring rules. You can use rule triggering criteria to configure the conditions that trigger the task, and adjust the importance level of events for detected file operations recorded in the task log.

A file operation monitoring rule is specified for each monitoring scope.

You can configure the following rule triggering criteria:

- Trusted users.
- File operation markers.

Trusted users

By default, the application treats all user actions as potential security breaches. The trusted user list is empty. You can configure the event importance level by creating a list of trusted users in the file operation monitoring rule settings.

Untrusted user – any user not indicated in the trusted user list in the monitoring scope rule settings. If Kaspersky Embedded Systems Security detects a file operation performed by an untrusted user, the File Integrity Monitor task records a Critical event in the task log.

Trusted user – a user or group of users authorized to perform file operations in the specified monitoring scope. If Kaspersky Embedded Systems Security detects file operations performed by a trusted user, the File Integrity Monitor task records an Informational event in the task log.

Kaspersky Embedded Systems Security cannot determine the users that initiate operations during monitoring interruption periods. In this case, the user status is determined to be unknown.

Unknown user – This status is assigned to a user if Kaspersky Embedded Systems Security cannot receive information about a user due to a task interruption or a failure of the data synchronization driver or USN Journal. If Kaspersky Embedded Systems Security detects a file operation performed by an unknown user, the File Integrity Monitor task records a *Warning* event in the task log.

File operation markers

When the File Integrity Monitor task runs, Kaspersky Embedded Systems Security uses file operation markers to determine that an action has been performed on a file.

A file operation marker is a unique descriptor that can characterize a file operation.

Each file operation can be a single action or a chain of actions with files. Each action of this kind is equated to a file operation marker. If the marker you specify as a rule triggering criterion is detected in a file operation chain, the application logs an event indicating that the given file operation was performed.

The importance level of the logged events does not depend on the selected file operation markers or the number of events.

> By default, Kaspersky Embedded Systems Security considers all available file operation marker. You can select file operation markers manually in the task's rule settings.

Table 53. File operation markers

File operation ID	File operation marker	Supported file systems
BASIC_INFO_CHANGE	Attributes or time markers of a file or folder changed	NTFS, ReFS
COMPRESSION_CHANGE	Compression of a file or folder changed	NTFS, ReFS
DATA_EXTEND	Size of file or folder increased	NTFS, ReFS
DATA_OVERWRITE	Data in a file or folder was overwritten	NTFS, ReFS
DATA_TRUNCATION	File or folder truncated	NTFS, ReFS
EA_CHANGE	Extended file or folder attributes changed	Only NTFS
ENCRYPTION_CHANGE	Encryption status of file or folder changed	NTFS, ReFS
FILE_CREATE	File or folder created for the first time	NTFS, ReFS
FILE_DELETE	File or folder permanently deleted using a SHIFT+DEL combination	NTFS, ReFS
HARD_LINK_CHANGE	Hard link created or deleted for file or folder	Only NTFS
INDEXABLE_CHANGE	Index status of file or folder changed	NTFS, ReFS
INTEGRITY_CHANGE	Integrity attribute changed for a named file stream	Only ReFS
NAMED_DATA_EXTEND	Size of a named file stream increased	NTFS, ReFS
NAMED_DATA_OVERWRITE	Named file stream overwritten	NTFS, ReFS
NAMED_DATA_TRUNCATION	Named file stream truncated	NTFS, ReFS
OBJECT_ID_CHANGE	File or folder identifier changed	NTFS, ReFS
RENAME_NEW_NAME	New name assigned to file or folder	NTFS, ReFS
REPARSE_POINT_CHANGE	New reparse point created or existing reparse point changed for a file or folder	NTFS, ReFS
SECURITY_CHANGE	File or folder access rights changed	NTFS, ReFS
STREAM_CHANGE	New named file stream created or existing named file stream changed	NTFS, ReFS
TRANSACTED_CHANGE	Named file stream changed by TxF transaction	Only ReFS

Default File Integrity Monitor task settings

By default, the File Integrity Monitor task has the settings described in the table below. You can change the values of these settings.

Table 54. Default File Integrity Monitor task settings

Setting	Default value	Description
Monitoring scope	Not configured	You can specify the folders and files for which actions will be monitored. Monitoring events will be generated for the folders and files in the specified monitoring scope.
Trusted user list	Not configured	You can specify users and/or groups of users, whose actions in the specified folders will be treated as safe by the component.
Monitor file operations when the task is not running	Used	You can enable or disable logging of file operations performed in the indicated monitoring scopes during periods in which the task in not running.
Exclude the following folders from control	Not applied	You can check the use of exclusions for folders in which file operations do not need to be monitored. When the File Integrity Monitor task runs, Kaspersky Embedded Systems Security will skip monitoring scopes specified as exclusions.
Checksum calculation	Not applied	You can configure file checksum calculation after the changes in the file are made.
Consider file operation markers	All available file operation markers are considered	You can specify the set of file operation markers. If a file operation performed in a monitoring scope is characterized by one or more specified markers, Kaspersky Embedded Systems Security generates an audit event.
Task start schedule	First run is not scheduled	You can configure the settings of scheduled startup of the task.

Managing File Integrity Monitor via the Administration Plug-in

In this section, learn how to configure the File Integrity Monitor task via the Administration Plug-in.

In this section

Configuring the File Integrity Monitor task settings

To configure general File Integrity Monitor task settings, perform the following steps:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.
3. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring a policy" on page 112).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in the Application settings window of the Kaspersky Security Center" on page 117).

   > If an active Kaspersky Security Center policy is applied to a device, and this policy blocks changes to application settings, then these settings cannot be edited in the **Application settings** window.

4. In the **System Inspection** section in the **File Integrity Monitor** block, click the **Settings** button.

   The **File Integrity Monitor** window opens.

5. In the **File operations monitoring settings** tab in the window that opens, configure the monitoring scope settings:

   a. Clear or select the **Log information about file operations that appear during the monitoring interruption period** check box.

      The check box enables or disables monitoring of the file operations specified in the File Integrity Monitor task settings when the task is not running for any reason (removal of a hard disk, task stopped by user, software error).

      If the check box is selected, Kaspersky Embedded Systems Security will record events in all monitoring scopes when the File Integrity Monitor task is not running.

      If the check box is cleared, the application will not log file operations in monitoring scopes when the task is not running.

      The check box is selected by default.

   b. Add the monitoring scopes (see Section "Configuring monitoring rules" on page 380) to be monitored by the task.

6. On the **Task management** tab, configure the task start parameters based on a schedule (see Section "Managing task schedules" on page 129).

7. Click **OK** to save changes.

Configuring monitoring rules

You can change the default settings of the File Integrity Monitor task (see the table below).

Table 55. Default File Integrity Monitor task settings

Setting	Default value	Description
Monitoring scope	Not configured	You can specify the folders and files for which actions will be monitored. Monitoring events will be generated for the folders and files in the specified monitoring scope.
Trusted user list	Not configured	You can specify users and/or groups of users, whose actions in the specified folders will be treated as safe by the component.
Monitor file operations when the task is not running	Used	You can enable or disable logging of file operations performed in the indicated monitoring scopes during periods in which the task in not running.
Exclude the following folders from control	Not applied	You can check the use of exclusions for folders in which file operations do not need to be monitored. When the File Integrity Monitor task runs, Kaspersky Embedded Systems Security will skip monitoring scopes specified as exclusions.
Checksum calculation	Not applied	You can configure file checksum calculation after the changes in the file are made.
Consider file operation markers	All available file operation markers are considered	You can specify the set of file operation markers. If a file operation performed in a monitoring scope is characterized by one or more specified markers, Kaspersky Embedded Systems Security generates an audit event.
Task start schedule	First run is not scheduled	You can configure the settings of scheduled startup of the task.

► *To add a monitoring scope, perform the following steps:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.
3. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring a policy" on page 112).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in the Application settings window of the Kaspersky Security Center" on page 117).

   > If an active Kaspersky Security Center policy is applied to a device, and this policy blocks changes to application settings, then these settings cannot be edited in the **Application settings** window.

4. In the **System Inspection** section in the **File Integrity Monitor** block, click the **Settings** button.

The **Properties: File Integrity Monitor** window opens.

5. In the **Monitoring scope** section, click the **Add** button.

   The **Monitoring scope** window opens.

6. Add a monitoring scope in one of the following ways:

   - If you want to select folders through the standard Microsoft Windows dialog:

     a. Click the **Browse** button.

        The standard Microsoft Windows Browse for Folder window opens.

     b. In the window that opens, select the folder for which you want to monitor operations, and click the **OK** button.

   - If you want to specify a monitoring scope manually, add a path using a supported mask:

     - <*.ext> - all files with the extension <ext>, regardless of their location;
     - <*\name.ext> - all files with name <name> and extension <ext>, regardless of their location;
     - <\dir*> - all files in folder <\dir>;
     - <\dir*\name.ext> - all files with the name <name> and extension <ext> in folder <\dir> and all of its child folders.

   > When specifying a monitoring scope manually, be sure that the path is in the following format: <volume letter>:\<mask>. If the volume letter is missing, Kaspersky Embedded Systems Security will not add the specified monitoring scope.

7. In the **Trusted users** tab, click the **Add** button.

   The standard Microsoft Windows **Select Users or Groups** window opens.

8. Select the users or groups of users for whom file operations are allowed in the selected monitoring scope, and click the **OK** button.

   > By default, Kaspersky Embedded Systems Security treats all users not on the trusted user list as untrusted (see Section "About file operation monitoring rules" on page 375), and generates Critical events for them.

9. Select the **File operation markers** tab.

10. If required, perform the following actions to select a number of markers:

    a. Select the **Detect file operations basing on the following markers** option.

    b. In the list of available file operations (see Section "About file operation monitoring rules" on page 375) select the check boxes next to the operations you want to monitor.

    > By default Kaspersky Embedded Systems Security detects all file operation markers, the **Detect file operations basing on all recognizable markers** option is selected.

11. If you want Kaspersky Embedded Systems Security to calculate files checksum after operation is performed, do the following:

a. Select the **Calculate checksum for the file if possible. The checksum will be available for viewing in the task report** check box.

   If the check box is selected, Kaspersky Embedded Systems Security calculates the checksum of the modified file, where the file operation with at least one selected marker was detected.

   If the file operation is detected by a number of markers, only the final file checksum after all modifications is calculated.

   If the check box is cleared, Kaspersky Embedded Systems Security does not calculate the checksum for the modified files.

   No checksum calculation is performed in the following cases:

   - If the file became unavailable (for example, due to the change of access permissions).
   - If the file operation is detected in the file that has been removed afterwards.

   The check box is cleared by default.

b. In the **Calculate the checksum using the algorithm** drop down list select one of the options:

   - **MD5 hash**
   - **SHA256 hash**

12. If you do not want to monitor all file operations in the list of available file operations (see Section "About file operation monitoring rules" on page 375), and select the check boxes next to the operations you want to monitor.
13. If necessary, add excluded monitoring scopes by performing the following steps:
    a. Select the **Exclusions** tab.
    b. Select the **Exclude the following folders from control** check box.

        The check box disables use of exclusions for folders where file operations do not need to be monitored.

        If the check box is selected, Kaspersky Embedded Systems Security skips the monitoring scopes specified in the exclusions list when the File Integrity Monitor task is run.

        If the check box is cleared, Kaspersky Embedded Systems Security logs events for all specified monitoring scopes.

        By default, the check box is cleared and the exclusion list is empty.
    c. Click the **Add** button.

        The **Select folder to add** window opens.
    d. In the window that opens, specify the folder that you want to exclude from the monitoring scope.
    e. Click **OK**.

        The specified folder is added to the list of excluded scopes.
14. Click **OK** in the **File operations monitoring rule** window.

    The specified rule settings will be applied to the selected monitoring scope of the File Integrity Monitor task.

Managing File Integrity Monitor via the Application Console

In this section, learn how to configure the File Integrity Monitor task via the Application Console.

In this section

Configuring the File Integrity Monitor task settings

► *To configure general File Integrity Monitor task settings, perform the following steps:*

1. In the Application Console tree, expand the **System Inspection** node.
2. Select the **File Integrity Monitor** child node.
3. Click the **Properties** link in the details pane of the **File Integrity Monitor** node.

    The **Task settings** window opens.

4. In the window that opens, on the **General** tab, clear or select the **Log information about file operations that appear during the monitor interruption period** check box.

   The check box enables or disables monitoring of the file operations specified in the File Integrity Monitor task settings when the task is not running for any reason (removal of a hard disk, task stopped by user, software error).

   If the check box is selected, Kaspersky Embedded Systems Security will record events in all monitoring scopes when the File Integrity Monitor task is not running.

   If the check box is cleared, the application will not log file operations in monitoring scopes when the task is not running.

   The check box is selected by default.

5. On the **Schedule** and **Advanced** tabs, configure the task start schedule (see Section "Managing task schedules" on page 129).
6. Click **OK** to save changes.

Configuring monitoring rules

You can change the default settings of the File Integrity Monitor task (see the table below).

Table 56. Default File Integrity Monitor task settings

Setting	Default value	Description
Monitoring scope	Not configured	You can specify the folders and files for which actions will be monitored. Monitoring events will be generated for the folders and files in the specified monitoring scope.
Trusted user list	Not configured	You can specify users and/or groups of users, whose actions in the specified folders will be treated as safe by the component.
Monitor file operations when the task is not running	Used	You can enable or disable logging of file operations performed in the indicated monitoring scopes during periods in which the task in not running.
Exclude the following folders from control	Not applied	You can check the use of exclusions for folders in which file operations do not need to be monitored. When the File Integrity Monitor task runs, Kaspersky Embedded Systems Security will skip monitoring scopes specified as exclusions.
Checksum calculation	Not applied	You can configure file checksum calculation after the changes in the file are made.
Consider file operation markers	All available file operation markers are considered	You can specify the set of file operation markers. If a file operation performed in a monitoring scope is characterized by one or more specified markers, Kaspersky Embedded Systems Security generates an audit event.
Task start schedule	First run is not scheduled	You can configure the settings of scheduled startup of the task.

► *To add a monitoring scope, perform the following steps:*

1. In the Application Console tree, expand the **System Inspection** node.
2. Select the **File Integrity Monitor** child node.
3. Click the **File operations monitoring rules** link in the details pane of the **File Integrity Monitor** node.

   The **File operations monitoring** window opens.
4. Add a monitoring scope in one of the following ways:
   - If you want to select folders through the standard Microsoft Windows dialog:
     a. On the left side of the window, click the **Browse** button.

        The standard Microsoft Windows **Browse For Folder** window opens.

     b. In the window that opens, select the folder for which you want to monitor operations, and click the **OK** button.

     c. Click the **Add** button to have Kaspersky Embedded Systems Security start monitoring file operations in the indicated monitoring scope.

- If you want to specify a monitoring scope manually, add a path using a supported mask:
  - <*.ext> - all files with the extension <ext>, regardless of their location;
  - <*\name.ext> - all files with name <name> and extension <ext>, regardless of their location;
  - <\dir*> - all files in folder <\dir>;
  - <\dir*\name.ext> - all files with the name <name> and extension <ext> in folder <\dir> and all of its child folders.

> When specifying a monitoring scope manually, be sure that the path is in the following format: <volume letter>:\<mask>. If the volume letter is missing, Kaspersky Embedded Systems Security will not add the specified monitoring scope.

On the right side of the window, the **Rule description** tab displays the trusted users and file operation markers selected for this monitoring scope.

5. In the list of added monitoring scopes, select the scope whose settings you want to configure.
6. Select the **Trusted users** tab.
7. Click the **Add** button.

   The standard Microsoft Windows **Select Users or Groups** window opens.
8. Select the users or groups of users that Kaspersky Embedded Systems Security will consider trusted for the selected monitoring scope.
9. Click **OK**.

> By default, Kaspersky Embedded Systems Security treats all users not on the trusted user list as untrusted (see Section "About file operation monitoring rules" on page 375), and generates Critical events for them.

10. Select the **Set file operations markers** tab.
11. If required, perform the following actions to select a number of markers:
    a. Select the **Detect file operations basing on the following markers** option.
    b. In the list of available file operations (see Section "About file operation monitoring rules" on page 375) select the check boxes next to the operations you want to monitor.

> By default Kaspersky Embedded Systems Security detects all file operation markers, the **Detect file operations basing on all recognizable markers** option is selected.

12. If you want Kaspersky Embedded Systems Security to calculate files checksum after operation is performed, do the following:
    a. In the **Checksum calculation** section select the **Calculate checksum for a file final version, after the file was changed, if possible** check box.

       If the check box is selected, Kaspersky Embedded Systems Security calculates the checksum of the modified file, where the file operation with at least one selected marker was detected.

       If the file operation is detected by a number of markers, only the final file checksum after all modifications is calculated.

If the check box is cleared, Kaspersky Embedded Systems Security does not calculate the checksum for the modified files.

No checksum calculation is performed in the following cases:

- If the file became unavailable (for example, due to the change of access permissions).
- If the file operation is detected in the file that has been removed afterwards.

The check box is cleared by default.

b. In the **Calculate the checksum using the algorithm** drop down list select one of the options:

   - **MD5 hash**.
   - **SHA256 hash**.

13. If necessary, add excluded monitoring scopes by performing the following steps:

    a. Select the **Set exclusions** tab.

    b. Select the **Consider excluded monitoring scope** check box.

    The check box disables use of exclusions for folders where file operations do not need to be monitored.

    If the check box is selected, Kaspersky Embedded Systems Security skips the monitoring scopes specified in the exclusions list when the File Integrity Monitor task is run.

If the check box is cleared, Kaspersky Embedded Systems Security logs events for all specified monitoring scopes.

By default, the check box is cleared and the exclusion list is empty.

c. Click the **Browse** button.

   The standard Microsoft Windows **Browse For Folder** window opens.

d. In the window that opens, specify the folder that you want to exclude from the monitoring scope.

e. Click **OK**.

f. Click the **Add** button.

   The specified folder is added to the list of excluded scopes.

> You can also add excluded monitoring scopes manually using the same masks that are used to specify monitoring scopes.

14. Click the **Save** button to apply new rule configuration.

Log Inspection

This section contains information about the Log Inspection task and task settings.

In this chapter

About the Log Inspection task

When the Log Inspection task runs, Kaspersky Embedded Systems Security monitors the integrity of the protected environment based on the results of an inspection of Windows Event Logs. The application notifies the administrator upon detecting abnormal behavior in the system, which may be an indication of attempted cyberattacks.

Kaspersky Embedded Systems Security considers the Window event logs and identifies breaches based on the rules specified by a user or by the settings of the heuristic analyzer, which is used by the task to inspect logs.

Predefined rules and heuristic analysis

You can use the Log Inspection task to monitor the state of the protected system by applying the predefined rules, that are based on existing heuristics. The heuristic analyzer identifies abnormal activity on the protected computer, which may be evidence of an attempted attack. Templates to identify abnormal behavior are included in the available rules in the predefined rules settings.

Seven rules are included in the rule list for the Log Inspection task. You can enable or disable the use of any of the rules. You cannot delete existing or create new rules.

You can configure the triggering criteria for rules that monitor events for the following operations:

- Password brute-force detection
- Network login detection

You can also configure exclusions in the task settings. The heuristic analyzer is not activated when a login is conducted by a trusted user or from a trusted IP address.

Kaspersky Embedded Systems Security does not use heuristics to inspect Windows logs if the heuristic analyzer is not used by the task. By default, the heuristic analyzer is enabled.

When the rules are applied, the application records a *Critical event* in the Log Inspection task log.

Custom rules for the Log Inspection task

You can use the task rule settings to specify and change the criteria for triggering rules upon detecting the selected events in the specified Windows log. By default, the list of Log Inspection task rules contains four rules. You can enable and disable the use these rules, remove rules, and edit rule settings.

You can configure the following rule triggering criteria for each rule:

- List of record identifiers in the Windows Event Log.

  The rule is triggered when a new record is created in the Windows Event Log, if the event properties includes an event identifier specified for the rule. You can also add and remove identifiers for each specified rule.

- Event source.

  For each rule, you can define a sublog of the Windows Event Log. The application will search for records with the specified event identifiers only in this sublog. You can select one of the standard sublogs (Application, Security, or System), or specify a custom sublog by entering the name in the source selection field.

  > The application does not verify that the specified sublog actually exists in the Windows Event Log.

When the rule is triggered, Kaspersky Embedded Systems Security records a Critical event in the Log Inspection task log.

By default Log Inspection task applies custom rules.

> Before starting the Log Inspection task make sure the system audit policy is set up correctly. Refer to Microsoft article https://technet.microsoft.com/en-us/library/cc952128.aspx for details.

Default Log Inspection task settings

By default, the Log Inspection task has the settings described in the table below. You can change the values of these settings.

Table 57. Default File Integrity Monitor task settings

Setting	Default value	Description
Apply custom rules for Log Inspection	Applied.	You can enable, disable, add, or modify the custom rules.
Apply predefined rules for Log Inspection	Applied.	You can enable or disable heuristic analyzer which detects abnormal activity on the protected server.
Brute-force attack detection	10 logon failures per 300 seconds.	You can set the number of attempts and a time frame when these attempts occurred, which will be considered as triggers for heuristic analyzer.
Network logon	12:00:00 AM.	You can indicate the start and end of the time interval during which Kaspersky Embedded Systems Security treats sign-in attempts as abnormal activity.
Exclusions	Not applied.	You can specify users and IP addresses which will not trigger heuristic analyzer.
Task start schedule	First run is not scheduled.	You can configure the settings of scheduled startup of the task.

Managing Log inspection rules via the Administration Plug-in

In this section, learn how to add and configure Log inspection rules via the Administration Plug-in.

In this section

Managing the predefined task rules via the Administration Plug-in

► *Perform the following actions to configure the predefined rules for the Log Inspection task:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.
3. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring a policy" on page 112).

- To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in the Application settings window of the Kaspersky Security Center" on page 117).

  > If an active Kaspersky Security Center policy is applied to a device, and this policy blocks changes to application settings, then these settings cannot be edited in the **Application settings** window.

4. In the **System Inspection** section click the **Settings** button in the **Log Inspection** block.

   The **Log Inspection** window opens.
5. Select the **Predefined rules** tab.
6. Select or clear check box **Apply custom rules for log inspection**.

   If this check box is selected, Kaspersky Embedded Systems Security applies heuristic analyzer to detect abnormal activity on the protected computer.

   If this check box is cleared the heuristic analyzer is not running and Kaspersky Embedded Systems Security applies preset or custom rules to detect abnormal activity.

   The check box is selected by default.

   > For the task to run, at least one Log Inspection rule must be selected.

7. Select the rules which you want to apply from the list of predefined rules:
   - There are patterns of a possible brute-force attack in the system.
   - There are patterns of a possible Windows Event log abuse.
   - Atypical actions detected on behalf of a new service installed.
   - Atypical logon that uses explicit credentials detected.
   - There are patterns of a possible Kerberos forged PAC (MS14-068) attack in the system.
   - Atypical actions detected directed at a privileged built-in group Administrators.
   - There is an atypical activity detected during a network logon session.
8. To configure the selected rules, click the **Advanced settings** button.

   The **Log Inspection** window opens.
9. In the **Brute-force attack detection** section set the number of attempts and a time frame when these attempts occurred, which will be considered as triggers for heuristic analyzer.
10. In the **Network logon detection** section, indicate the start and end of the time interval during which Kaspersky Embedded Systems Security treats sign-in attempts as abnormal activity.
11. Select the **Exclusions** tab.
12. Perform the following actions to add trusted users:

    a. Click the **Browse** button.

    b. Select a user.

    c. Click **OK**.

    A selected user is added to the list of trusted users.

13. Perform the following actions to add trusted IP-addresses:
    a. Enter the IP-address.
    b. Click the **Add** button.
14. An entered IP-address is added to the list of trusted IP-addresses.
15. On the **Task management** tab configure the task start schedule (see Section "Configuring the task start schedule settings" on page 129).
16. Click **OK**.

The Log Inspection task configuration is saved.

Adding Log inspection rules via the Administration Plug-in

► *Perform the following actions to add and configure a new log Inspection custom rule:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.
3. Perform one of the following actions in the details pane of the selected administration group:
    - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring a policy" on page 112).
    - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in the Application settings window of the Kaspersky Security Center" on page 117).

    If an active Kaspersky Security Center policy is applied to a device, and this policy blocks changes to application settings, then these settings cannot be edited in the **Application settings** window.

4. In the **System Inspection** section click the **Settings** button in the **Log Inspection** block.

    The **Log Inspection** window opens.
5. On the **Custom rules** tab select or clear the **Apply custom rules for log inspection** check box.

    If the check box is selected, Kaspersky Embedded Systems Security applies custom rules for Log Inspection according to each rule settings. You can add, remove or configure Log Inspection rules.

    If the check box is cleared, you cannot add or modify the custom rules. Kaspersky Embedded Systems Security applies default rules settings.

    The check box is selected by default. Only the Application popup detection rule is active.

    You can control whether the preset rules are applied for Log Inspection. Select the check boxes corresponding to the rules you want to apply for the Log Inspection.

6. To add a new custom rule, click the **Add** button.

    The **Log inspection rules** window opens.
7. In the **General** section enter the following information about the new rule:

- **Rule name**
- **Source**

  Select a source log to use recorded events for analysis. The following Windows event log types are available:

  - Application
  - Security
  - System

  You can add a new custom log by entering the log name into the **Source** field.

8. In the **Triggered events ID** section specify the item IDs that will trigger the rule on detection:

   a. Enter an ID's numeric value.

   b. Click the **Add** button.

      A selected rule ID is added to the list. You can add an unlimited number of identifiers for each rule.

   c. Click **OK**.

   The Log inspection rule is added to the list of rules.

Managing Log inspection rules via the Application Console

In this section, learn how to add and configure Log inspection rules via the Application Console.

In this section

Managing the predefined task rules via the Application Console

► *Perform the following actions to configure the heuristic analyzer for the Log Inspection task:*

1. In the Application Console tree, expand the **System Inspection** node.
2. Select the **Log Inspection** child node.
3. Click the **Properties** link in the details pane of the **Log Inspection** node.

   The **Task settings** window opens.
4. Select the **Predefined rules** tab.
5. Select or clear check box **Apply custom rules for log inspection**.

   If this check box is selected, Kaspersky Embedded Systems Security applies heuristic analyzer to detect abnormal activity on the protected computer.

   If this check box is cleared the heuristic analyzer is not running and Kaspersky Embedded Systems Security applies preset or custom rules to detect abnormal activity.

   The check box is selected by default.

   > For the task to run, at least one Log Inspection rule must be selected.

6. Select the rules which you want to apply from the list of predefined rules:
   - There are patterns of a possible brute-force attack in the system.
   - There are patterns of a possible Windows Event log abuse.
   - Atypical actions detected on behalf of a new service installed.

- Atypical logon that uses explicit credentials detected.
- There are patterns of a possible Kerberos forged PAC (MS14-068) attack in the system.
- Atypical actions detected directed at a privileged built-in group Administrators.
- There is an atypical activity detected during a network logon session.

7. To configure the selected rules, go to the **Extended** tab.
8. In the **Brute-force attack detection** set the number of attempts and a time frame when these attempts occurred, which will be considered as triggers for heuristic analysis.
9. In the **Network logon** section, indicate the start and end of the time interval during which Kaspersky Embedded Systems Security treats sign-in attempts as abnormal activity.
10. Select the **Exclusions** tab.
11. Perform the following actions to add trusted users:
    a. Click the **Browse** button.
    b. Select a user.
    c. Click **OK**.

       A selected user is added to the list of trusted users.
12. Perform the following actions to add trusted IP-addresses:
    a. Enter the IP-address.
    b. Click the **Add** button.

       An entered IP-address is added to the list of trusted IP-addresses.
13. Select the **Schedule** and **Advanced** tabs to configure the task start schedule.
14. Click **OK**.

    The Log Inspection task configuration is saved.

Configuring the Log inspection rules

Perform the following actions to add and configure a new Log Inspection custom rule:

1. In the Application Console tree, expand the **System Inspection** node.
2. Select the **Log Inspection** child node.
3. In the details pane of the **Log Inspection** node, click the **Log inspection rules** link.

   The **Log inspection rules** window opens.
4. Select or clear the **Apply custom rules for log inspection** check box.

   If the check box is selected, Kaspersky Embedded Systems Security applies custom rules for Log Inspection according to each rule settings. You can add, remove or configure Log Inspection rules.

   If the check box is cleared, you cannot add or modify the custom rules. Kaspersky Embedded Systems Security applies default rules settings.

   The check box is selected by default. Only the Application popup detection rule is active.

You can control whether the predefined rules are applied for the Log Inspection task. Select the check boxes corresponding to the rules you want to apply for the Log Inspection.

5. To create a new custom rule, do the following:
   a. Enter the name of the new rule.
   b. Click the **Add** button.

      The created rule is added to the general rule list.
6. To configure any rule, take the following steps:
   a. Click with the left mouse button to select a rule in the list.

      In the right area of the window, the **Description** tab displays general information about the rule.

      The description for the new rule is blank.
   b. Select the **Rule description** tab.
   c. In the **General** section, edit the rule name, if necessary.
   d. Select the **Source**.
7. In the **Event identifiers** section specify the item IDs that will trigger the rule on detection:
   a. Enter an ID's numeric value.
   b. Click the **Add** button.

      A selected rule ID is added to the list. You can add an unlimited number of identifiers for each rule.
   c. Click the **Save** button.

      The configured log inspection rules will be applied.

On-Demand Scan

This section provides information about On-Demand Scan tasks, and instructions on configuring On-Demand Scan task settings and security settings on the protected computer.

In this chapter

About On-Demand Scan tasks

Kaspersky Embedded Systems Security scans the specified area for viruses and other computer security threats. Kaspersky Embedded Systems Security scans computer files and RAM and also autorun objects.

Kaspersky Embedded Systems Security provides following system tasks of On-Demand Scan:

- The Scan at Operating System Startup task is performed every time Kaspersky Embedded Systems Security starts. Kaspersky Embedded Systems Security scans boot sectors and master boot records of hard and removable drives, system memory, and memory of processes. Every time Kaspersky Embedded Systems Security runs the task, it creates a copy of non-infected boot sectors. If at the next task start it detects a threat in those sectors, it replaces them with the backup copy.
- By default, the Critical Areas Scan task is performed weekly by schedule. Kaspersky Embedded Systems Security scans objects in critical areas of the operating system: autorun objects, boot sectors and master boot records of hard and removable drives, system memory and memory of processes. Application scans files in the system folders, for example, in %windir%\system32. Kaspersky Embedded Systems Security applies security settings the values of which correspond to the Recommended level (see Section "About predefined security levels for On-Demand Scan tasks" on page 404). You can modify the settings of the Critical Areas Scan task.
- Quarantine Scan task is executed by default according to the schedule after every databases update. The Quarantine Scan task scope cannot be modified.

- The Application Integrity Control task is performed daily. It provides the option of checking Kaspersky Embedded Systems Security modules for damage or modification. The application installation folder is checked. The task execution statistics contain information about the number of modules checked and corrupted. The values of the task settings are defined by default and cannot be edited. The task start schedule settings can be edited.

Additionally you can create custom On-Demand Scan tasks, for example, a task for scanning shared folders on the computer.

Kaspersky Embedded Systems Security may run several On-Demand Scan tasks at the same time.

About scan scope

You can configure the scan scope for Scan at Operating System Startup and Critical Areas Scan tasks, and for custom On-Demand Scan tasks.

By default On-Demand Scan tasks scan all objects of the computer file system. If there is no security requirement to scan all objects of the file system, you can limit the scan to the scan scope.

In the Application Console, the scan scope is displayed as a tree or as a list of the computer file resources that Kaspersky Embedded Systems Security can control. By default, the network file resources of the protected computer are displayed in a list-view mode.

► *To display network file resources in the tree-view mode,*

open the drop-down list in the **Scan scope settings** window upper left sector and select **Tree-view**.

The nodes are displayed in a list-view or in a tree-view mode of the computer file resources as follows:

☑ The node is included in the scan scope.

□ The node is excluded from the scan scope.

▣ At least one of the child nodes of this node is excluded from the scan scope, or the security settings of the child node(s) differ from those of this node (only for tree-view mode).

The ▣ icon is displayed if all child nodes are selected, but the parent node is not selected. In this case, changes in the composition of files and folders of the parent node are disregarded automatically when the scan scope for the selected child node is being modified.

The names of virtual nodes in the scan scope are displayed in blue font.

Predefined scan scopes

The tree or list of computer file resources for the selected On-Demand Scan task is displayed on the **Scan scope settings** tab.

> The file resources tree or list displays the nodes to which you have read-access based on the configured security settings of Microsoft Windows.

Kaspersky Embedded Systems Security contains the following predefined scan scopes:

- **My Computer**. Kaspersky Embedded Systems Security scans the entire computer.
- **Local hard drives**. Kaspersky Embedded Systems Security scans objects on a computer hard drives. All hard drives, individual disks, folders or files can be included in or excluded from the scan scope.
- **Removable drives**. Kaspersky Embedded Systems Security scans files on external devices, such as CDs or USB drives. All removable disks, individual disks, folders or files can be included in or excluded from the scan scope.
- **Network**. Network folders or files can be added to the scan scope by specifying their path in UNC (Universal Naming Convention) format. The account used to start the task must have access permissions for the network folders and files added. By default On-Demand Scan tasks run under the system account.

  > Connected network drives will also not be displayed in the computer file resources tree. To include objects on network drives in the scan scope, specify the path to the folder which corresponds to this network drive in UNC format.

- **System memory**. Kaspersky Embedded Systems Security scans the executable files and modules of the processes running in the operating system when the scan is initiated.
- **Startup objects**. Kaspersky Embedded Systems Security scans objects to which registry keys and configuration files refer, for example WIN.INI or SYSTEM.INI, as well as the application's modules that are started automatically at computer startup.
- **Shared folders**. You can include shared folders on the protected computer into the scan scope.
- **Virtual drives**. Dynamic folders and files and drives that are connected to the computer can be included in the scan scope, for example, common cluster drives.

  > Virtual drives created using a SUBST command are not displayed in the computer file resource tree in the Application Console. In order to scan objects on a virtual drive, include the computer folder with which this virtual drive is associated into the scan scope.

By default, you can view and configure predefined scan scopes in the network file resources tree; you can also add predefined scopes to the network file resources list during its formation in the scan scope settings.

By default, On-Demand Scan tasks are run under the following scopes:

- Scan at Operating System Startup task:
  - **Local hard drives**
  - **Removable drives**
  - **System memory**
- Critical Areas Scan:
  - **Local hard drives** (excluding Windows folders)
  - **Removable drives**
  - **System memory**
  - **Startup objects**
- Other tasks:
  - **Local hard drives** (excluding Windows folders)
  - **Removable drives**
  - **System memory**
  - **Startup objects**
  - **Shared folders**

Cloud storage file scanning

About cloud files

Kaspersky Embedded Systems Security can interact with Microsoft OneDrive cloud files. The application supports the new OneDrive Files On-Demand feature.

> Kaspersky Embedded Systems Security does not support other cloud storages.

OneDrive Files On-Demand helps you access all your files in OneDrive without having to download all of them and use storage space on your device. You can download files to your hard drive when you need to.

When the OneDrive Files On-Demand feature is on, you see status icons next to each file in the **Status** column in File Explorer. Each file has one of the following statuses:

☁ This status icon indicates that the file is *only available online*. Online-only files are not physically stored on your hard drive. You can't open online-only files when your device is not connected to the Internet.

✓ This status icon indicates that a file is *locally available*. This happens when you open an online-only file and it downloads to your device. You can open a locally available file anytime, even without Internet access. To clear up space you can change the file back to ☁ online-only.

✅ This status icon indicates that a file is *stored on your hard drive and is always available*.

Cloud file scanning

Kaspersky Embedded Systems Security can only scan cloud files that are stored locally on a protected computer. Such OneDrive files have the ✅ and ✓ statuses. The ☁ files are skipped during scanning, since they are not physically located on the protected computer.

> Kaspersky Embedded Systems Security does not automatically download ☁ files from the cloud during the scanning, even if they are included in the scan scope.

Cloud files are processed by several Kaspersky Embedded Systems Security tasks in various scenarios depending on the task type:

- Real-time cloud files scanning: you can add folders containing cloud files to the Real-Time File Protection task protection scope.The file is scanned when it is accessed by the user. If a ☁ file is accessed by the user, it is downloaded, becomes locally available, and its status changes to ✓ . This allows the file to be processed by the Real-Time File Protection task.
- On-demand cloud file scanning: you can add folders containing cloud files to the On-Demand Scan task's scan scope. The task scans files with the ✅ and ✓ statuses. If any ☁ files are found in the scope, they will be skipped during scanning and an informational event will be recorded in the task log, indicating that the scanned file is only a placeholder for a cloud file and does not exist on a local drive.
- Application Control rule generation and usage: you can create allowing and denying rules for ✅ and ✓ files using the Rule Generator for Applications Launch Control task. The Applications Launch Control task applies the Default Deny principle and created rules to process and block cloud files.

  > The Applications Launch Control task blocks the start of all cloud files, irrespective of their status. The ☁ files are not included in the rule generation scope by the application, as they are not physically stored on a hard drive. Since no allowing rules cannot be created for such files, they are subject to the Default Deny principle.

When a threat is detected in a OneDrive cloud file, the application applies the action specified in the settings of the task performing the scanning. In this way, the file can be removed, disinfected, moved to quarantine, or backed up.

> Changes to local files are synchronized with the copies stored on OneDrive in accordance with to the principles outlined in the relevant Microsoft OneDrive documentation.

Security settings of selected node in On-Demand Scan tasks

In the selected On-Demand Scan task, the default values of security settings can be modified by configuring them as common settings for the entire protection or scan scope, or as different settings for different nodes or items in the computer file resource tree or list.

Security settings configured for the selected parent node are automatically applied to all child nodes. The security settings of the parent node are not applied to child nodes that are configured separately.

The settings for a selected scan scope or protection scope can be configured using one of the following methods:

- Select one of three predefined security levels (**Maximum performance**, **Recommended**, or **Maximum protection**).
- Manually change the security settings for the selected nodes or items in the tree or in the list of the computer's file resources (the security level changes to **Custom**).

A set of node settings can be saved in a template in order to be applied later to other nodes.

About predefined security levels for On-Demand Scan tasks

The security settings **Use iChecker technology**, **Use iSwift technology**, **Use heuristic analyzer**, and **Check Microsoft signature in files** are not included in the settings of preset security levels. If the status of such settings as **Use iChecker technology**, **Use iSwift technology**, **Use heuristic analyzer**, and **Check Microsoft signature in files** is changed, the preset security level that you have selected will not change.

One of three predefined security levels for a node selected in the computer file resources tree can be applied: **Maximum performance**, **Recommended**, and **Maximum protection**. Each of these levels contains its own predefined set of security settings (see the table below).

Maximum performance

The **Maximum performance** security level is recommended if, beyond using Kaspersky Embedded Systems Security on computers, there are additional computer security measures inside your network, for example, firewalls and existing security policies.

Recommended

The **Recommended** security level ensures an optimum combination of protection and performance impact on protected computers. This level is recommended by Kaspersky Lab experts as sufficient to protect computers on most corporate networks. The **Recommended** security level is set by default.

Maximum protection

The **Maximum protection** security level is recommended if your organization’s network has elevated computer security requirements.

Table 58. Predefined security levels and corresponding security setting values

Options	Security level		
	Maximum performance	Recommended	Maximum protection
Scan objects	By format	All objects	All objects
Scan only new and modified files	Enabled	Disabled	Disabled
Action to perform on infected and other objects	Disinfect. Remove if disinfection fails	Perform recommended action (Disinfect. Remove if disinfection fails)	Disinfect. Remove if disinfection fails
Action to perform on probably infected objects	Quarantine	Perform recommended action (Quarantine)	Quarantine
Exclude files	No	No	No
Do not detect	No	No	No
Stop scanning if it takes longer than (sec.)	60 sec.	No	No
Do not scan compound objects larger than (MB)	8 MB	No	No
Scan alternate NTFS streams	Yes	Yes	Yes
Scan disk boot sectors and MBR	Yes	Yes	Yes
Scan of compound objects	• SFX archives* • Packed objects* • Embedded OLE objects* * New and modified objects only	• Archives* • SFX archives* • Packed objects* • Embedded OLE objects* * All objects	• Archives* • SFX archives* • Email databases* • Plain mail* • Packed objects* • Embedded OLE objects* * All objects

About the Removable Drives Scan

You can configure scanning of removable drives connected to the protected computer via the USB port.

Kaspersky Embedded Systems Security scans a removable drive using the On-Demand Scan task. The application automatically creates a new On-Demand Scan task when the removable drive is connected and deletes the task after the scanning is completed. The created task is performed with the predefined security level defined for removable drive scanning. You cannot configure the settings of the temporary On-Demand Scan task.

If you installed Kaspersky Embedded Systems Security without anti-virus databases, the removable drives scan will be unavailable.

Kaspersky Embedded Systems Security scans a removable drive using the On-Demand Scan task. The application automatically creates a new On-Demand Scan task when the removable drive is connected and deletes the task after the scanning is completed. The created task is performed with the predefined security level defined for removable drive scanning. You cannot configure the settings of the temporary On-Demand Scan task.

> Kaspersky Embedded Systems Security scans connected removable USB drives when they are registered as USB mass storage devices in the operating system. The application does not scan a removable drive if the connection is blocked by the Device Control task. The application does not scan MTP-connected mobile devices.

Kaspersky Embedded Systems Security allows access to removable drives during scanning.

Scan results for each removable drive are available in the log for the On-Demand Scan task created upon connection of the removable drive.

You can change the settings of the Removable Drives Scan component (see the table below).

Table 59. Removable Drives Scan settings

Setting	Default Value	Description
Scan removable drives on connection via USB	Check box is cleared	You can turn on or turn off scanning of removable drive upon connection to the protected computer via USB.
Scan removable drives if its stored data volume does not exceed (MB)	1024 MB	You can reduce the component's scope by setting the maximum volume of data on the scanned drive. Kaspersky Embedded Systems Security does not perform removable drive scanning if the volume of stored data exceeds the specified value.
Scan with security level	Maximum protection	You can configure the created On-Demand Scan tasks by selecting one of three security levels: • **Maximum protection** • **Recommended** • **Maximum performance** The algorithm used when infected, probably infected, and other objects are detected, as well as the other scan settings for each security level, correspond to the predefined security levels in the On-Demand Scan tasks.

Default On-Demand Scan tasks settings

By default On-Demand Scan tasks have the settings described in the table below. You can configure system and user On-Demand Scan tasks.

Table 60. Default On-Demand Scan tasks settings

Setting	Value	Description
Scan scope	Applied in system and custom tasks: • **Scan at Operating System Startup**: the entire server, excluding shared folders and autorun objects. • **Critical Areas Scan**: the entire server, excluding shared folders and certain operating system files. • Custom **On-Demand Scan** tasks: the entire server.	You can change the scan scope. The scan scope cannot be configured for the **Quarantine Scan** and **Application Integrity Control** system tasks.
Security settings	Common settings for the entire scan scope correspond to the security level **Recommended**.	For nodes selected in the computer file resources list or tree, you can: • Select a different predefined security level • Manually change security settings You can save a set security settings for a selected node as a template to use later for a different node.
Use heuristic analyzer	It is used with the **Medium** analysis level for Critical Areas Scan, Scan at Operating System Startup, and custom tasks. It is used with the **Deep** analysis level for the Quarantine Scan task.	The heuristic analyzer can be enabled or disabled and the analysis level configured. The Quarantine Scan task analysis level cannot be configured. The heuristic analyzer is not used in the Application Integrity Control task.
Apply Trusted Zone	Applied (Not applied for Quarantine Scan task)	General list of exclusions which can be used in selected tasks.
Use KSN for scanning	Applied	You can improve your server's protection using the Kaspersky Security Network infrastructure of cloud services.
Task start settings with permissions	The task is started under a system account.	You can edit start settings with account permissions for all system and user On-Demand Scan tasks, except Quarantine Scan and Application Integrity Control tasks.
Perform task in background mode (low priority)	Not applied	You can configure the priority level of On-Demand Scan tasks.

Setting	Value	Description
Task start schedule	Applied in system tasks: • Scan at Operating System Startup - **At application launch** • Critical Areas Scan - **Weekly** • Quarantine Scan - **After application database update** • Application Integrity Control - **Daily** Not used in newly created custom tasks.	You can configure the settings of scheduled startup of the task.
Registering scan execution and updating server protection status	The server protection status is updated weekly after the Critical Areas Scan is performed.	You can configure settings for registering the execution of the Critical Areas Scan in the following ways: • Edit the settings of the Critical Areas Scan task start schedule. • Edit the scan scope of the Critical Areas Scan task. • Create user On-Demand Scan tasks.

Managing On-Demand Scan tasks via the Administration Plug-in

In this section, learn how to navigate the Administration Plug-In interface and configure task settings for one or all computers on the network.

In this section

Navigation

Learn how to navigate to the required task settings via the interface.

In this section

Opening the On-Demand Scan task Wizard

► *To start creating a new custom On-Demand Scan task:*

1. To create a local task:
   a. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console.
   b. Select the administration group that the computer belongs to.
   c. In the details pane, on the **Devices** tab open the context menu for the protected server.
   d. Select the **Properties** menu option.
   e. In the window that opens, click the **Add** button in the **Tasks** section.

   The **New Task Wizard** window opens.
2. To create a group task:
   a. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
   b. Select the administration group for which you want to create a task.
   c. Open the **Tasks** tab.
   d. Click the **Create a task** button.

   The **New Task Wizard** window opens.
3. To create a task for a custom set of computers:
   a. In the **Device selections** node in the Kaspersky Security Center Administration Console tree, click **Run selection** button to perform a device selection.
   b. Open the **Selection results "selection name"** tab.
   c. In the **Perform selection** drop-down list, select the **Create a task for a selection result** option.

   The **New Task Wizard** window opens.
4. Select the **On-Demand Scan** task in the list of available tasks for Kaspersky Embedded Systems Security .
5. Click **Next**.

   The **Settings** window opens.

Configure the task settings as required.

► *To configure an existing On-Demand Scan task,*

double-click the task name in the list of Kaspersky Security Center tasks.

The **Properties: On-Demand Scan** window opens.

Opening the On-Demand Scan task properties

► *To open the application properties for the On-Demand Scan task for a single computer:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group that the protected computer belongs to.
3. Select the **Devices** tab.
4. Double-click the name of the computer for which you want to configure the scan scope.

   The **Properties: <computer name>** window opens.
5. Select the **Tasks** section.
6. In the list of tasks created for the device select the On-Demand Scan task that you created.
7. Click the **Properties** button.

   The **Properties: On-Demand Scan** window opens.

Configure the task settings as required.

Creating an On-Demand Scan task

► *To create a custom On-Demand Scan task:*

1. Open the **Settings** (see Section "**Opening the On-Demand Scan task Wizard**" on page 410) window in the **New Task Wizard**.
2. Select the required **Task creation method**.
3. Click **Next**.
4. Create a scan scope in the **Scan scope** window:

   > By default, scan scope includes critical areas of the computer. Scan scopes are marked in the table with the icon ☑. Excluded scan scopes are marked with the □ icon in the table.
   > You can change the scan scope: add specific preset scan scopes, disks, folders, network objects and files and assign specific security settings for each scope added.

   - To exclude all critical areas from the scan, open the context menu on each of the lines and select the **Remove scope** option.
   - To include a predefined scan scope, disk, folder, network object, or file in the scan scope:

     a. Right-click the **Scan scope** table and select **Add scope** or click the **Add** button.

b. In the **Add objects to the scan scope** window, select the predefined scope in the **Predefined scope** list, specify the computer drive, folder, network object, or file on the computer or on another network computer, and click the **OK** button.

- To exclude subfolders or files from the scan, select the added folder (disk) in the **Scan scope** window of the wizard:

  a. Open the context menu and select the **Configure** option.

  b. Click the **Settings** button in the **Security level** window.

  c. On the **General** tab in the **On-demand scan settings** window clear the **Subfolders** and **Subfiles** check boxes.

- To change scan scope security settings:

  a. Open the context menu on the scope whose settings you wish to configure, and select **Configure**.

  b. In the **On-demand scan settings** window, select one of the predefined security levels, or click the **Settings** button to configure security settings manually.

  > Security settings are configured the same way as for the Real-Time File Protection task (see Section "Configuring security settings manually" on page 251).

- To skip embedded objects in the added scan scope:

  a. Open the context menu on the **Scan scope** table, select **Add exclusion**.

  b. Specify the objects to exclude: select predefined scope in the **Predefined scope** list, specify the computer disk, folder, network object, or file on the computer or on another network computer.

  c. Click the **OK** button.

5. In the **Options** window, configure the heuristic analyzer and integration with other components:

- Configure the usage of heuristic analyzer (see Section "Configuring Heuristic Analyzer and integration with other application components" on page 246).

- Select the **Apply Trusted Zone** check box, if you want to exclude objects added to the Trusted Zone list from the scan scope of the task.

  This check box enables / disables use of the Trusted Zone for a task.

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

  If the check box is cleared, Kaspersky Embedded Systems Security disregards the file operations of trusted processes when forming the protection scope for the task.

  The check box is selected by default.

- Select the **Use KSN for scanning** check box, if you want to use Kaspersky Security Network cloud services for the task.

  This check box enables / disables the use of Kaspersky Security Network (KSN) cloud services in the task.

  If the check box is selected, the application uses data received from KSN services to ensure a faster response time by the application to new threats and reduce the likelihood of false positives.

If the check box is cleared, the On-Demand Scan task does not use KSN services.

The check box is selected by default.

- To assign the base priority *Low* to the working process in which the task will be executed, select the **Perform task in background mode** check box in the **Options** window.

  The check box modifies the priority of the task.

  If the check box is selected, the task priority in the operating system is reduced. The operating system provides resources for performing the task depending on the load on the CPU and the computer file system from other Kaspersky Embedded Systems Security tasks and other applications. As a result, task performance will slow down during increased loads and will speed up at lower loads.

  If the check box is cleared, the task will start and run with the same priority as the other Kaspersky Embedded Systems Security tasks and other applications. In this case, the speed of task execution increases.

  The check box is cleared by default.

  > By default, the working processes in which Kaspersky Embedded Systems Security tasks are run have the *Medium* (Normal) priority.

- To use the created task as a Critical Areas Scan task, select the **Consider task as critical areas scan** check box in the **Options** window.

  The check box changes the task priority: enables or disables logging of the *Critical Areas Scan* event and refreshing of the computer protection status. Kaspersky Security Center evaluates the security rating of the computer (computers) by the performance results of tasks with the *Critical Areas Scan* status. The check box is not available in the properties of local system and custom tasks of Kaspersky Embedded Systems Security. You can edit this setting only on the side of Kaspersky Security Center.

  If this check box is selected, Administration Server logs the Critical Areas Scan completion and refreshes the computer protection status based on the task execution results. The scan task has a high priority.

  If the check box is cleared, the task is run with a low priority.

  The check box is cleared by default for custom On-demand tasks.

6. Click **Next**.
7. In the **Schedule** window, set the scheduled task start settings.
8. Click **Next**.
9. In the **Selecting an account to run the task** window, specify the account you want to use.
10. Click **Next**.
11. Define a task name.

12. Click **Next**.

> The task name should be no longer than 100 characters and cannot contain the following symbols: " * < > & \ : |

The **Finish task creation** window opens.

13. You can optionally run the task after the Wizard finishes by selecting the **Run task after Wizard finishes** check box.
14. Click **Finish** to finish creating the task.

The new On-Demand Scan task will be created for a selected computer or a group of computers.

In this section

Assigning the Critical Areas Scan task status to an On-Demand Scan task

By default, Kaspersky Security Center assigns the *Warning* status to the computer if the Critical Areas Scan task is performed less often than specified by the *Critical areas scan has not been performed for a long time* event generation threshold setting of Kaspersky Embedded Systems Security.

► *To configure scanning of all computers in a single administration group, take the following steps:*

1. Create a group On-Demand Scan task (see Section "Creating an On-Demand Scan task" on page 411).
2. In the **Options** window of the task wizard, select the **Consider task as critical areas scan** check box. The task settings specified (the scan scope and security settings) will be applied to all computers in the group. Configure the task schedule.

> You can select the **Consider task as critical areas scan** check box when creating the On-Demand Scan task for a group of computers or later in the **Properties: <Task name>** window (see Section "Opening the On-Demand Scan task properties" on page 411).

3. Using a new or existing policy disable the scheduled start of system on-demand scan tasks (see Section "Configuring scheduled start of local system tasks" on page 95) on the group computers.

Kaspersky Security Center Administration Server will then evaluate the security status of the protected computer and will notify you about it based on the results of the last run of the task with the *Critical Areas Scan* status, rather than based on the results of the Critical Areas Scan system task.

You can assign the *Critical Areas Scan* task status both to group On-Demand Scan tasks and to tasks for sets of computers.

The Application Console can be used to view whether the On-Demand Scan task is a Critical Areas Scan task.

> In the Application Console, the **Consider task as critical areas scan** check box is displayed in task properties but cannot be edited.

Running background On-Demand Scan task

By default the processes in which Kaspersky Embedded Systems Security tasks are executed are assigned the base priority *Medium* (Normal).

The process that will run an On-Demand Scan task can be assigned *Low* priority. Demoting the process priority increases the time required to execute the task, but may have a beneficial effect on the execution speed of the processes of other active programs.

Multiple background tasks can be running in a single working process with low priority. You can specify the maximum number of processes to background On-Demand Scan tasks.

► *To change the priority of an existing On-Demand Scan task:*

1. Open the **Properties: On-Demand Scan** window (see Section "Opening the On-Demand Scan task Wizard" on page 410).
2. Select or clear the **Perform task in background mode** check box.

   The check box modifies the priority of the task.

   If the check box is selected, the task priority in the operating system is reduced. The operating system provides resources for performing the task depending on the load on the CPU and the computer file system from other Kaspersky Embedded Systems Security tasks and other applications. As a result, task performance will slow down during increased loads and will speed up at lower loads.

   If the check box is cleared, the task will start and run with the same priority as the other Kaspersky Embedded Systems Security tasks and other applications. In this case, the speed of task execution increases.

   The check box is cleared by default.
3. Click **OK**.

Configured task settings are saved and applied immediately to the running task. If the task is not running, the modified settings are applied at next start.

Registering execution of Critical Areas Scan

By default, the computer protection status is displayed in the details pane of the **Kaspersky Embedded Systems Security** node and is updated weekly after the Critical Areas Scan task is performed.

The time of the computer protection status update is linked to the schedule of the On-Demand task in whose settings the **Consider task as critical areas scan** check box is selected. By default, the check box is selected only for the Critical Areas Scan task and cannot be modified for this task.

> You can select the On-Demand Scan task linked to the computer's protection status only from Kaspersky Security Center.

Configuring the task scan scope

If you modify the scan scope in the Scan at Operating System Startup and Critical Areas Scan tasks, you can restore the default scan scope in these tasks by restoring Kaspersky Embedded Systems Security itself (**Start** > **Programs** > **Kaspersky Embedded Systems Security** > **Modify or Remove Kaspersky Embedded Systems Security**). In the setup wizard, select **Repair installed components** and click **Next**, and then select the **Restore recommended application settings** check box.

► *To configure a scan scope for an existing On-Demand Scan task:*

1. Open the **Properties: On-Demand Scan** window (see Section "Opening the On-Demand Scan task properties" on page 411).
2. Select the **Scan scope** tab.
3. To include items in the scan scope:
   a. Open the context menu in the empty space of the scan scope list.
   b. Select the **Add scope** context menu option.
   c. In the opened **Add objects to the scan scope** window select an object type that you want to add:
      - **Predefined scope** to add one of the predefined scopes on a protected server. Then in the drop down list select a necessary scan scope.
      - **Disk, folder or network location** to include individual drive, folder or a network object into a scan scope. Then select a necessary scope by clicking the **Browse** button.
      - **File** to include an individual file into scan scope. Then select a necessary scope by clicking the **Browse** button.

   > You cannot add an object into a scan scope if it has already been added as an exclusion out of the scan scope.

4. To exclude individual nodes from the scan scope, clear the check boxes next to the names of these nodes or take the following steps:
   a. Open the context menu on the scan scope by right-clicking it.
   b. In the context menu select **Add exclusion** option.

c. In the **Add exclusion** window select an object type that you want to add as an exclusion out of the scan scope following the logic of the adding object to a scan scope procedure.

5. To modify the scan scope or an exclusion added, select the **Edit scope** option in the context menu for the necessary scan scope.
6. To hide the previously added scan scope or an exclusion in the list of network file resources, select the **Remove scope** option in the context menu for the necessary scan scope.

   > The scan scope is excluded out of the On-demand scan task scope on its removal from the network file resources list.

7. Click the **OK** button.

Scan scope settings window will be closed. Your newly configured settings have been saved.

Selecting predefined security levels for On-Demand Scan tasks

One of three predefined security levels for an item selected in the list of the computer network file resources can be applied: **Maximum performance**, **Recommended**, and **Maximum protection**.

► *To select one of the predefined security levels:*

1. Open the **Properties: On-Demand Scan** (see Section "**Opening the On-Demand Scan task properties**" on page 411) window.
2. Select the **Scan scope** tab.
3. In the list of the computer select an item included in the scan scope to set the predefined security level.
4. Click the **Configure** button.

   The **On-demand scan settings** window opens.
5. On the **Security level** tab select the security level to be applied.

   The window displays the list of security settings corresponding to the security level selected.
6. Click the **OK** button.
7. Click the **OK** button in the **Properties: On-Demand Scan** window.

   Configured task settings are saved and applied immediately to the running task. If the task is not running, the modified settings are applied at next start.

Configuring security settings manually

By default On-Demand Scan tasks use common security settings for the entire scan scope. These settings correspond to the **Recommended** predefined security level (see Section "Predefined security levels" on page 238).

The default values of security settings can be modified by configuring them as common settings for the entire protection scope or as different settings for different items in the computer file resource list or nodes in the tree.

► *To configure security settings manually:*

1. Open the **Properties: On-Demand Scan** window (see Section "Opening the On-Demand Scan task properties" on page 411).
2. Select the **Scan scope** tab.
3. Select the items in the scan scope list for which you want to configure security settings.

   > A predefined template containing security settings (see Section "About security settings templates" on page 156) can be applied for a selected node or item in the scan scope.

4. Click the **Configure** button.

   The **On-demand scan settings** window opens.

5. Configure the required security settings of the selected node or item in accordance with your requirements:
   - **General** settings (see Section "Configuring general task settings" on page 418)
   - **Actions** (see Section "**Configuring actions**" on page 421)
   - **Performance** (see Section "**Configuring performance**" on page 423)
6. Click **OK** in the **On-demand scan settings** window.
7. Click **OK** in the **Scan scope** window.

New scan scope settings are saved.

In this section

Configuring general task settings

► *To configure general On-Demand Scan task settings:*

1. Open the **Properties: On-Demand Scan** (see Section "**Opening the On-Demand Scan task properties**" on page 411) window.
2. Select the **Scan scope** tab.
3. Click the **Configure** button.

   The **On-demand scan settings** window opens.

4. Click the **Settings** button.
5. On the **General** tab, in the **Scan objects** section, specify the object types that you want to include in the scan scope:
   - **Objects to scan**
     - **All objects**

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

       Kaspersky Embedded Systems Security scans only infectable objects based on file format.

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

       Kaspersky Embedded Systems Security scans only infectable objects based on file extension.

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

       Kaspersky Embedded Systems Security scans files based on file extension. List of file extensions can be manually customized in the **List of extensions** window, which can be opened by clicking the **Edit** button.
   - **Subfolders**
   - **Subfiles**
   - **Scan disk boot sectors and MBR**

     Enables protection of boot sectors and master boot records.

     If the check box is selected, Kaspersky Embedded Systems Security scans boot sectors and master boot records on hard drives and removable drives of the computer.

     The check box is selected by default.
   - **Scan alternate NTFS streams**

     Scanning of alternative file and folder streams on the NTFS file system drives.

     If the check box is selected, the application scans a probably infected object and all NTFS streams associated with that object.

     If the check box is cleared, the application scans only the object that was detected and considered as probably infected.

     The check box is selected by default.

6. In the **Performance** section, select or clear the **Scan only new and modified files** check box.

   This check box enables / disables scanning and protection of files that have been recognized by Kaspersky Embedded Systems Security as new or modified since the last scan.

   If the check box is selected, Kaspersky Embedded Systems Security scans and protects only the files that it has recognized as new or modified since the last scan.

   If the check box is cleared, you can select if you want to scan and protect only new files or all files disregarding their modification status.

   By default, the check box is selected for the **Maximum performance** security level. If the **Maximum protection** or **Recommended** security levels are set, the check box is cleared.

> To switch between available options when the check box is cleared, click on the **All** / **Only new** link for each of the compound object types.

7. In the **Scan of compound objects** section, specify the compound objects that you want to include in the scan scope:

   - **All / Only new archives**

     Scanning of ZIP, CAB, RAR, ARJ archives and other archive formats.

     If this check box is selected, Kaspersky Embedded Systems Security scans archives.

     If this check box is cleared, Kaspersky Embedded Systems Security skips archives during scanning.

     The default value depends on the selected protection level.

   - **All / Only new SFX archives**

     Scanning of self-extracting archives.

     If this check box is selected, Kaspersky Embedded Systems Security scans SFX archives.

     If this check box is cleared, Kaspersky Embedded Systems Security skips SFX archives during scanning.

     The default value depends on the selected protection level.

     This option is active when the **Archives** check box is cleared.

   - **All / Only new email databases**

     Scanning of Microsoft Outlook and Microsoft Outlook Express mail database files.

     If this check box is selected, Kaspersky Embedded Systems Security scans mail database files.

     If this check box is cleared, Kaspersky Embedded Systems Security skips mail database files during scanning.

     The default value depends on the selected security level.

   - **All / Only new packed objects**

     Scanning of executable files packed by binary code packers, such as UPX or ASPack.

     If this check box is selected, Kaspersky Embedded Systems Security scans executable files packed by packers.

If this check box is cleared, Kaspersky Embedded Systems Security skips executable files packed by packers during scanning.

The default value depends on the selected protection level.

- **All / Only new plain email**

  Scanning of files of mail formats, such as Microsoft Outlook and Microsoft Outlook Express messages.

  If this check box is selected, Kaspersky Embedded Systems Security scans files of mail formats.

  If this check box is cleared, Kaspersky Embedded Systems Security skips files of mail formats during scanning.

  The default value depends on the selected security level.

- **All / Only new embedded OLE objects**

  Scanning of objects embedded into files (such as Microsoft Word macros, or email message attachments).

  If this check box is selected, Kaspersky Embedded Systems Security scans objects embedded into files.

  If this check box is cleared, Kaspersky Embedded Systems Security skips objects embedded into files during scanning.

  The default value depends on the selected protection level.

8. Click **OK**.

New task configuration will be saved.

Configuring actions

► *To configure actions on infected and other detected objects during the On-Demand Scan task execution:*

1. Open the **Properties: On-Demand Scan** (see Section "**Opening the On-Demand Scan task properties**" on page 411) window.
2. Select the **Scan scope** tab.
3. Click the **Configure** button.

   The **On-demand scan settings** window opens.
4. Click the **Settings** button.
5. Select the **Actions** tab.
6. Select the action to be performed on infected and other detected objects:

   - **Notify only**.

     When this mode is selected, Kaspersky Embedded Systems Security does not block access to detected or other detected objects, or perform any actions on them. The following event is registered in the task log: *Object not disinfected. Reason: no action was* *taken to neutralize detected object due to user-defined settings.* The event specifies all available information about the detected object.

The **Notify only** mode should be separately configured for each protection or scan area. This mode is not used by default on any of the security levels. If you select this mode, Kaspersky Embedded Systems Security automatically changes the security level to **Custom**.

- **Disinfect**.
- **Disinfect. Remove if disinfection fails**.
- **Remove**.
- **Perform recommended action**.

7. Select the action to be performed on probably infected objects:

   - **Notify only**.

     When this mode is selected, Kaspersky Embedded Systems Security does not block access to detected or other detected objects, or perform any actions on them. The following event is registered in the task log: *Object not disinfected. Reason: no action was taken to neutralize detected object due to user-defined settings.* The event specifies all available information about the detected object.

     The **Notify only** mode should be separately configured for each protection or scan area. This mode is not used by default on any of the security levels. If you select this mode, Kaspersky Embedded Systems Security automatically changes the security level to **Custom**.

   - **Quarantine**.
   - **Remove**.
   - **Perform recommended action**.

8. Configure actions to be performed on objects depending on the type of object detected:

   a. Clear or select the **Perform actions depending on the type of object detected** check box.

      If the check box is selected, you can independently set primary and secondary action for each detected object type by clicking the **Settings** button next to the check box. At that, Kaspersky Embedded Systems Security will not allow to open or execute an infected object regardless of your choice.

      If the check box is cleared, Kaspersky Embedded Systems Security performs actions that are selected in the **Action to perform on infected and other objects** and **Action to perform on probably infected objects** sections for named object types respectively.

      The check box is cleared by default.

   b. Click the **Settings** button.

   c. In the window that opens select primary and secondary action (if the first action fails) for each type of the detected object.

   d. Click **OK**.

9. Select the action to perform on incurable compound objects: select or clear the **Entirely remove compound file that cannot be modified by the application in case of embedded object detect** 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 Embedded Systems Security 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 Embedded Systems Security does not perform the selected action, if the parent object is unmodifiable.

10. Click **OK**.

New task configuration will be saved.

Configuring performance

► *To configure the performance for the On-Demand Scan task:*

1. Open the **Properties: On-Demand Scan (see Section "Opening the On-Demand Scan task properties" on page** 411**)** window.
2. Select the **Scan scope** tab.
3. Click the **Configure** button.

    The **On-demand scan settings** window opens.

4. Click the **Settings** button.
5. Select the **Performance** tab.
6. In the **Exclusions** section:

    - Clear or select the **Exclude files** check box.

        Excluding files from scanning by file name or file name mask.

        If this check box is selected, Kaspersky Embedded Systems Security skips specified objects during scanning.

        If this check box is cleared, Kaspersky Embedded Systems Security scans all objects.

        The check box is cleared by default.

    - Clear or select the **Do not detect** check box.

        Objects are excluded from scanning by the name or name mask of the detectable object. The list of names of detectable objects is available on the Virus Encyclopedia https://encyclopedia.kaspersky.com/knowledge/classification/ website.

        If this check box is selected, Kaspersky Embedded Systems Security skips specified detectable objects during scanning.

        If the check box is cleared, Kaspersky Embedded Systems Security detects all objects specified in the application by default.

The check box is cleared by default.

- Click the **Edit** button for each setting to add exclusions.

7. In the **Advanced settings** section:

- **Stop scanning if it takes longer than (sec.)**

  Limits the duration of object scanning. The default value is 60 seconds.

  If the check box is cleared, scan duration is limited to the specified value.

  If the check box is cleared, scan duration is unlimited.

  By default, the check box is selected for the **Maximum performance** security level.

- **Do not scan compound objects larger than (MB)**

  Excludes objects larger than the specified size from the scanning.

  If the check box is selected, Kaspersky Embedded Systems Security skips compound objects whose size exceeds the specified limit during virus scan.

  If this check box is cleared, Kaspersky Embedded Systems Security scans compound objects of any size.

  By default, the check box is selected for the **Maximum performance** security level.

- **Use iSwift technology**

  iSwift compares file NTFS identifier, that is stored in a database, with a current identifier. The scanning is performed only for files, whose identifiers has changed (new files and files modified since the last scan of NTFS system objects).

  If the check box is selected, Kaspersky Embedded Systems Security scans only new files or those modified since the last scan of NTFS system objects.

  If the check box is cleared, Kaspersky Embedded Systems Security scans objects of NTFS file system disregarding the date of file creation or modification except for files from network folders.

  The check box is selected by default.

- **Use iChecker technology**

  iChecker calculates and remembers checksums of scanned files. If an object is modified the checksum changes. The application compares all checksums during the scan task and scans only new and modified since the last scan files.

  If the check box is selected, Kaspersky Embedded Systems Security scans only new and modified files.

  If the check box is cleared, Kaspersky Embedded Systems Security scans files disregarding the date of file creation or modification.

  The check box is selected by default.

8. Click **OK**.

New task configuration will be saved.

Configuring the Removable Drives Scan

► *To configure scanning of the removable drives upon connection to the protected computer:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure the task.
3. Select the **Policies** tab.
4. Double-click the policy name you want to configure.

   In the **Properties: <Policy name>** window that opens, select the **Supplementary** section.
5. Click the **Settings** button in the **Removable Drives Scan** subsection.

   The **Removable Drives Scan** window opens.
6. In the **Scan on connection** section do the following:
   - Select the **Scan removable drives on connection via USB** check box, if you want Kaspersky Embedded Systems Security to automatically scan removable drives when they are connected.
   - If required, select the **Scan removable drives if its stored data volume does not exceed (MB)** and specify the maximum value in the field on the right.
   - In the **Scan with security level** drop-down list specify the security level with the settings that are required for removable drives scanning.
7. Click **OK**.

The specified settings are saved and applied.

Managing On-Demand Scan tasks via the Application Console

In this section, learn how to navigate the Application Console interface and configure task settings on a local computer.

In this section

Navigation

Learn how to navigate to the required task settings via the interface.

In this section

Opening the On-Demand Scan task settings

► *To open the general settings of the On-Demand Scan task via the Application Console:*

1. Expand the **On-Demand Scan** node in the Application Console tree.
2. Select the child node that corresponds to the task that you want to configure.
3. In the child node details pane click the **Properties** link.

   The **Task settings** window opens.

► *To open the scan scope settings window via the Application Console:*

1. Expand the **On-Demand Scan** node in the Application Console tree.
2. Select the child node corresponding to an On-Demand Scan task that you want to configure.
3. In the details pane of the selected node click the **Configure scan scope** link.

   Scan scope settings window opens.

Creating and configuring an On-Demand Scan task

Custom tasks for a single computer can be created in the **On-Demand Scan** node. In the other functional components of Kaspersky Embedded Systems Security creation of custom tasks is not available.

► *To create and configure a new On-Demand Scan task:*

1. In the Application Console tree, open the context menu of the **On-Demand Scan** node.
2. Select **Add task**.

   The **Add task** window opens.
3. Configure the following task settings:
   - **Name** – task name of no more than 100 characters, may contain any symbols apart from **" * < > & \ : |**.

     > You cannot save a task or configure a new task on the **Schedule**, **Advanced** and **Run as** tabs if the task name is not specified.

   - **Description** – any additional information about the task, no more than 2000 characters. This information will be displayed in the task properties window.

- **Use heuristic analyzer**.

  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.

- **Perform task in background mode**.

  The check box modifies the priority of the task.

  If the check box is selected, the task priority in the operating system is reduced. The operating system provides resources for performing the task depending on the load on the CPU and the computer file system from other Kaspersky Embedded Systems Security tasks and other applications. As a result, task performance will slow down during increased loads and will speed up at lower loads.

  If the check box is cleared, the task will start and run with the same priority as the other Kaspersky Embedded Systems Security tasks and other applications. In this case, the speed of task execution increases.

  The check box is cleared by default.

- **Apply Trusted Zone**.

  This check box enables / disables use of the Trusted Zone for a task.

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

  If the check box is cleared, Kaspersky Embedded Systems Security disregards the file operations of trusted processes when forming the protection scope for the task.

  The check box is selected by default.

- **Consider task as critical areas scan**.

  The check box changes the task priority: enables or disables logging of the *Critical Areas Scan* event and refreshing of the computer protection status. Kaspersky Security Center evaluates the security rating of the computer (computers) by the performance results of tasks with the *Critical Areas Scan* status. The check box is not available in the properties of local system and custom tasks of Kaspersky Embedded Systems Security. You can edit this setting only on the side of Kaspersky Security Center.

  If this check box is selected, Administration Server logs the Critical Areas Scan completion and refreshes the computer protection status based on the task execution results. The scan task has a high priority.

  If the check box is cleared, the task is run with a low priority.

  The check box is cleared by default for custom On-demand tasks.

- **Use KSN for scanning**.

  This check box enables / disables the use of Kaspersky Security Network (KSN) cloud services in the task.

  If the check box is selected, the application uses data received from KSN services to ensure a faster response time by the application to new threats and reduce the likelihood of false positives.

  If the check box is cleared, the On-Demand Scan task does not use KSN services.

  The check box is selected by default.

4. Configure the task start schedule settings (see Section "Configuring the task start schedule settings" on page 149) on the **Schedule** and **Advanced** tabs.
5. On the **Run as** tab, configure the task start settings with account permissions (see Section "Specifying a user account to start a task" on page 152).
6. Click **OK** in the **Add task** window.

   A new custom On-Demand Scan task is created. A node with the name of the new task is displayed in the Application Console tree. The operation is registered in the system audit log (on page 201).
7. If required, in the details pane of the selected node, select **Configure scan scope**.

   The **Scan scope settings** window opens.
8. In the computer file resources tree or list, select the nodes or items that you want to include in the scan scope.
9. Select one of the predefined security levels (see Section "About predefined security levels for On-Demand Scan tasks" on page 404) or configure the scan settings manually (see Section "Configuring security settings manually" on page 432).
10. Click **Save** in the **Scan scope settings** window.

The configured settings are applied at the next task start.

Scan scope in On-Demand Scan tasks

This section contains information on creating and using a scan scope in On-Demand Scan tasks.

In this section

Configuring view mode for network file resources

► *To select a view mode for the network file resources during configuring the scan scope settings:*

1. Open the **Scan scope settings** (on page 426) window.
2. Open the drop down list in the upper left section of the window. Perform one of the following steps:
   - Select the **Tree-view** option to display the network file resources in a tree-view mode.
   - Select the **List-view** option to display the network file resources in a list-view mode.

   By default, the network file resources of the protected computer are displayed in a list-view mode.

3. Click the **Save** button.

Scan scope settings window will close. The newly configured settings will be applied.

Creating scan scope

If you are remotely managing Kaspersky Embedded Systems Security on the protected computer using the Application Console installed on administrator's workstation, you must be a member of administrators group on the protected computer to be able to view folders on it.

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

If you modify the scan scope in the Scan at Operating System Startup and Critical Areas Scan tasks, you can restore the default scan scope in these tasks by restoring Kaspersky Embedded Systems Security itself (**Start** > **Programs** > **Kaspersky Embedded Systems Security** > **Modify or Remove Kaspersky Embedded Systems Security**). In the setup wizard, select **Repair installed components** and click **Next**, and then select the **Restore recommended application settings** check box.

The procedure of creating an On-Demand Scan task scope depends on the network file resources view mode (see Section "Configuring view mode for network file resources" on page 429). You can configure network file resources view mode as a tree or as a list (set as default).

► *To create a scan scope working with a network file resources tree:*

1. Open the **Scan scope settings** window (on page 426).
2. In the left section of the window open the network file resources tree to display all the nodes and child nodes.
3. Do the following:
   - To exclude individual nodes from the scan scope, clear the check boxes next to the names of these nodes.
   - To include individual nodes in the scan scope, clear the **My Computer** check box and do the following:
     - If all drives of one type are to be included in the scan scope, select the check box opposite the name of the required drive type (for example, to add all removable drives on the computer, select the **Removable drives** check box).

- If an individual drive of a certain type is to be included in the scan scope, expand the node that contains the list of drives of this type and check the box next to the name of the required drive. For example, in order to select the removable drive **F:**, expand node **Removable drives** and select the check box for the drive **F:**.
- If you would like to include only a single folder or file on the drive, select the check box next to the name of that folder or file.

4. Click the **Save** button.

Scan scope settings window will be closed. Your newly configured settings will be saved.

► *To create a scan scope using the network file resources list:*

1. Open the **Scan scope settings** window (on page 426).
2. To include individual nodes in the scan scope, clear the **My Computer** check box and do the following:
   a. Open the context menu on the scan scope by right-clicking it.
   b. In the context menu of the button, select **Add scan scope**.
   c. In the opened **Add scan scope** window select an object type that you want to add:
      - **Predefined scope** to add one of the predefined scopes on a protected computer. Then in the drop-down list select a necessary scan scope.
      - **Disk, folder or network location** to include individual drive, folder or a network object into a scan scope. Then select a necessary scope by clicking the **Browse** button.
      - **File** to include an individual file into scan scope. Then select a necessary scope by clicking the **Browse** button.

      > You cannot add an object into a scan scope if it has already been added as an exclusion out of the scan scope.

3. To exclude individual nodes from the scan scope, clear the check boxes next to the names of these nodes or take the following steps:
   a. Open the context menu on the scan scope by right-clicking it.
   b. In the context menu select **Add exclusion** option.
   c. In the **Add exclusion** window select an object type that you want to add as an exclusion out of the scan scope following the logic of the adding object to a scan scope procedure.
4. To modify the scan scope or an exclusion added, select the **Edit scope** option in the context menu for the necessary scan scope.
5. To hide the previously added scan scope or an exclusion in the list of network file resources, select the **Remove from the list** option in the context menu for the necessary scan scope.

   > The scan scope is excluded out of the On-Demand Scan task scope on its removal from the network file resources list.

6. Click the **Save** button.

Scan scope settings window will be closed. Your newly configured settings will be saved.

Including network objects in the scan scope

Network drives, folders or files can be added to the scan scope by specifying their path in UNC (Universal Naming Convention) format.

> You can scan network folders under the system account.

► *To add a network place to the scan scope:*

1. Open the **Scan scope settings** (on page 426) window.
2. Open the drop-down list in the window upper left sector and select **Tree-view**.
3. In the context menu of the **Network** node:
   - Select **Add network folder**, if you want to add a network folder to the scan scope.
   - Select **Add network file**, if you want to add a network file to the scan scope.
4. Enter the path to network folder or file in UNC format and press the **ENTER** key.
5. Select the check box next to the newly added network object to include it in the scan scope.
6. If necessary, change the security settings for the network object added.
7. Click the **Save** button.

The modified task settings are saved.

Creating a virtual scan scope

Dynamic drives, folders, and files can be included in the scan scope in order to create a virtual scan scope.

> You can expand the protection / scan scope by adding individual virtual drives, folders, or files only if the protection / scan scope is presented as a tree of file resources (see Section "Configuring view mode for network file resources" on page 429).

► *To add a virtual drive to the scan scope:*

1. Open the **Scan scope settings** (on page 426) window.
2. Open the drop-down list in the window upper left sector and select **Tree-view**.
3. In the computer file resource tree open the context menu on the **Virtual drives** node, click **Add virtual drive** and select the virtual drive name from the list of available names.
4. Select the check box next to the added drive in order to include the drive in the scan scope.
5. Click the **Save** button.

The modified task settings are saved.

► *To add a virtual folder or virtual file to the scan scope:*

1. Open the **Scan scope settings** window (on page 426).
2. Open the drop-down list in the window upper left sector and select **Tree-view**.
3. In the computer file resources tree open the context menu of the node to add a folder or file, and select one of the following options:
   - **Add virtual folder** if you want to add a virtual folder to the scan scope.
   - **Add virtual file** if you want to add a virtual file to the scan scope.
4. In the entry field specify the name of the folder or file.
5. In the line with the name of the folder or file created, select the check box to include this folder or file in the scan scope.
6. Click the **Save** button.

The modified task settings are saved.

Selecting predefined security levels for On-Demand Scan tasks

One of three predefined security levels for a node or an item selected in the tree or in the list of the computer network file resources can be applied: **Maximum performance**, **Recommended**, and **Maximum protection**.

► *To select one of the predefined security levels:*

1. Open the **Scan scope settings** (on page 426) window.
2. In the tree or in the list of the computer network file resources select a node or item to set the predefined security level.
3. Make sure that the selected node or item is included in the scan scope.
4. In the right sector of the window, on the **Security level** tab select the security level to be applied.

   The window displays the list of security settings corresponding to the security level selected.
5. Click the **Save** button.

   Configured task settings are saved and applied immediately to the running task. If the task is not running, the modified settings are applied at next start.

Configuring security settings manually

By default On-Demand Scan tasks use common security settings for the entire scan scope. These settings correspond to the **Recommended** predefined security level (see Section "Predefined security levels" on page 238).

The default values of security settings can be modified by configuring them as common settings for the entire protection scope or as different settings for different items in the computer file resource list or nodes in the tree.

When working with the network file resources tree, security settings that are configured for the selected parent node are automatically applied to all child nodes. The security settings of the parent node are not applied to child nodes that are configured separately.

► *To configure security settings manually:*

1. Open the **Scan scope settings** (on page 426) window.
2. In the left window section select the node or item to configure security settings.

   A predefined template containing security settings (see Section "About security settings templates" on page 156) can be applied for a selected node or item in the scan scope.
3. Configure the required security settings of the selected node or item in accordance with your requirements in the following tabs:
   - General settings (see Section "Configuring general task settings" on page 433)
   - Actions (see Section "Configuring actions" on page 436)
   - Performance (see Section "Configuring performance" on page 437)
   - Hierarchical storage
4. Click **Save** in the **Scan scope settings** window.

New scan scope settings are saved.

In this section

Configuring general task settings

► *To configure the general security settings of the On-Demand Scan task:*

1. Open the **Scan scope settings** (on page 426) window.
2. Select the **General** tab.
3. In the **Scan objects** section, specify the object types that you want to include in the scan scope:
   - **Objects to scan**
     - **All objects**

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

       Kaspersky Embedded Systems Security scans only infectable objects based on file format.

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

       Kaspersky Embedded Systems Security scans only infectable objects based on file extension.

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

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

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

- **Scan disk boot sectors and MBR**

  Enables protection of boot sectors and master boot records.

  If the check box is selected, Kaspersky Embedded Systems Security scans boot sectors and master boot records on hard drives and removable drives of the computer.

  The check box is selected by default.

- **Scan alternate NTFS streams**

  Scanning of alternative file and folder streams on the NTFS file system drives.

  If the check box is selected, the application scans a probably infected object and all NTFS streams associated with that object.

  If the check box is cleared, the application scans only the object that was detected and considered as probably infected.

  The check box is selected by default.

4. In the **Performance** section, select or clear the **Scan only new and modified files** check box.

   This check box enables / disables scanning and protection of files that have been recognized by Kaspersky Embedded Systems Security as new or modified since the last scan.

   If the check box is selected, Kaspersky Embedded Systems Security scans and protects only the files that it has recognized as new or modified since the last scan.

   If the check box is cleared, you can select if you want to scan and protect only new files or all files disregarding their modification status.

   By default, the check box is selected for the **Maximum performance** security level. If the **Maximum protection** or **Recommended** security levels are set, the check box is cleared.

> To switch between available options when the check box is cleared, click on the **All** / **Only new** link for each of the compound object types.

5. In the **Scan of compound objects** section, specify the compound objects that you want to include in the scan scope:

   - **All / Only new archives**

     Scanning of ZIP, CAB, RAR, ARJ archives and other archive formats.

     If this check box is selected, Kaspersky Embedded Systems Security scans archives.

     If this check box is cleared, Kaspersky Embedded Systems Security skips archives during scanning.

     The default value depends on the selected protection level.

- **All / Only new SFX archives**

  Scanning of self-extracting archives.

  If this check box is selected, Kaspersky Embedded Systems Security scans SFX archives.

  If this check box is cleared, Kaspersky Embedded Systems Security skips SFX archives during scanning.

  The default value depends on the selected protection level.

  This option is active when the **Archives** check box is cleared.

- **All / Only new email databases**

  Scanning of Microsoft Outlook and Microsoft Outlook Express mail database files.

  If this check box is selected, Kaspersky Embedded Systems Security scans mail database files.

  If this check box is cleared, Kaspersky Embedded Systems Security skips mail database files during scanning.

  The default value depends on the selected security level.

- **All / Only new packed objects**

  Scanning of executable files packed by binary code packers, such as UPX or ASPack.

  If this check box is selected, Kaspersky Embedded Systems Security scans executable files packed by packers.

  If this check box is cleared, Kaspersky Embedded Systems Security skips executable files packed by packers during scanning.

  The default value depends on the selected protection level.

- **All / Only new plain email**

  Scanning of files of mail formats, such as Microsoft Outlook and Microsoft Outlook Express messages.

  If this check box is selected, Kaspersky Embedded Systems Security scans files of mail formats.

  If this check box is cleared, Kaspersky Embedded Systems Security skips files of mail formats during scanning.

  The default value depends on the selected security level.

- **All / Only new embedded OLE objects**

  Scanning of objects embedded into files (such as Microsoft Word macros, or email message attachments).

  If this check box is selected, Kaspersky Embedded Systems Security scans objects embedded into files.

  If this check box is cleared, Kaspersky Embedded Systems Security skips objects embedded into files during scanning.

  The default value depends on the selected protection level.

6. Click **Save**.

New task configuration will be saved.

Configuring actions

► *To configure the actions on infected and other detected objects for the On-Demand Scan task:*

1. Open the **Scan scope settings** (on page 426) window.
2. Select the **Actions** tab.
3. Select the action to be performed on infected and other detected objects:
   - **Notify only**.

     When this mode is selected, Kaspersky Embedded Systems Security does not block access to detected or other detected objects, or perform any actions on them. The following event is registered in the task log: *Object not disinfected. Reason: no action was taken to neutralize detected object due to user-defined settings.* The event specifies all available information about the detected object.

     The **Notify only** mode should be separately configured for each protection or scan area. This mode is not used by default on any of the security levels. If you select this mode, Kaspersky Embedded Systems Security automatically changes the security level to **Custom**.
   - **Disinfect**.
   - **Disinfect. Remove if disinfection fails**.
   - **Remove**.
   - **Perform recommended action**.
4. Select the action to be performed on probably infected objects:
   - **Notify only**.

     When this mode is selected, Kaspersky Embedded Systems Security does not block access to detected or other detected objects, or perform any actions on them. The following event is registered in the task log: *Object not disinfected. Reason: no action was taken to neutralize detected object due to user-defined settings.* The event specifies all available information about the detected object.

     The **Notify only** mode should be separately configured for each protection or scan area. This mode is not used by default on any of the security levels. If you select this mode, Kaspersky Embedded Systems Security automatically changes the security level to **Custom**.
   - **Quarantine**.
   - **Remove**.
   - **Perform recommended action**.

5. Configure actions to be performed on objects depending on the type of object detected:

   a. Clear or select the **Perform actions depending on the type of object detected** check box.

      If the check box is selected, you can independently set primary and secondary action for each detected object type by clicking the **Settings** button next to the check box. At that, Kaspersky Embedded Systems Security will not allow to open or execute an infected object regardless of your choice.

      If the check box is cleared, Kaspersky Embedded Systems Security performs actions that are selected in the **Action to perform on infected and other objects** and **Action to perform on probably infected objects** sections for named object types respectively.

      The check box is cleared by default.

   b. Click the **Settings** button.

   c. In the window that opens select primary and secondary action (if the first action fails) for each type of the detected object.

   d. Click **OK**.

6. Select the action to perform on incurable compound objects: select or clear the **Entirely remove compound file that cannot be modified by the application in case of embedded object detect** 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 Embedded Systems Security 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 Embedded Systems Security does not perform the selected action, if the parent object is unmodifiable.

7. Click **Save**.

New task configuration will be saved.

Configuring performance

► *To configure the performance for the On-Demand Scan task:*

1. Open the **Scan scope settings** (on page 426) window.
2. Select the **Performance** tab.
3. In the **Exclusions** section:

   - Clear or select the **Exclude files** check box.

     Excluding files from scanning by file name or file name mask.

     If this check box is selected, Kaspersky Embedded Systems Security skips specified objects during scanning.

If this check box is cleared, Kaspersky Embedded Systems Security scans all objects.

The check box is cleared by default.

- Clear or select the **Do not detect** check box.

  Objects are excluded from scanning by the name or name mask of the detectable object. The list of names of detectable objects is available on the Virus Encyclopedia https://encyclopedia.kaspersky.com/knowledge/classification/ website.

  If this check box is selected, Kaspersky Embedded Systems Security skips specified detectable objects during scanning.

  If the check box is cleared, Kaspersky Embedded Systems Security detects all objects specified in the application by default.

  The check box is cleared by default.

- Click the **Edit** button for each setting to add exclusions.

4. In the **Advanced settings** section:

- **Stop scanning if it takes longer than (sec.)**

  Limits the duration of object scanning. The default value is 60 seconds.

  If the check box is cleared, scan duration is limited to the specified value.

  If the check box is cleared, scan duration is unlimited.

  By default, the check box is selected for the **Maximum performance** security level.

- **Do not scan compound objects larger than (MB)**

  Excludes objects larger than the specified size from the scanning.

  If the check box is selected, Kaspersky Embedded Systems Security skips compound objects whose size exceeds the specified limit during virus scan.

  If this check box is cleared, Kaspersky Embedded Systems Security scans compound objects of any size.

  By default, the check box is selected for the **Maximum performance** security level.

- **Use iSwift technology**

  iSwift compares file NTFS identifier, that is stored in a database, with a current identifier. The scanning is performed only for files, whose identifiers has changed (new files and files modified since the last scan of NTFS system objects).

  If the check box is selected, Kaspersky Embedded Systems Security scans only new files or those modified since the last scan of NTFS system objects.

  If the check box is cleared, Kaspersky Embedded Systems Security scans objects of NTFS file system disregarding the date of file creation or modification except for files from network folders.

  The check box is selected by default.

- **Use iChecker technology**

  iChecker calculates and remembers checksums of scanned files. If an object is modified the checksum changes. The application compares all checksums during the scan task and scans only new and modified since the last scan files.

If the check box is selected, Kaspersky Embedded Systems Security scans only new and modified files.

If the check box is cleared, Kaspersky Embedded Systems Security scans files disregarding the date of file creation or modification.

The check box is selected by default.

5. Click **Save**.

New task configuration will be saved.

Configuring hierarchical storage

► *To configure the actions on infected and other detected objects for the On-Demand Scan task:*

1. Open the **Scan scope settings** (on page 426) window.
2. Select the **Hierarchical storage** tab.
3. Select the action to be performed on the offline files:
   - **Do not scan**.
   - **Scan resident part of file only**.
   - **Scan entire file**.

     If this action is selected, you can specify the following options:

     - Select or clear the **Only if the file has been accessed within the specified period (days)** check box and specify the number of days.
     - Select or clear the **Do not copy file to a local hard drive, if possible** check box.
4. Click **Save**.

New task configuration will be saved.

Scanning removable drives

► *To configure scanning of the removable drives upon connection to the protected computer in the Application Console:*

1. In the Application Console tree, open the context menu of the **Kaspersky Embedded Systems Security** node and select the **Configure removable drives scan settings** option.

   The **Removable Drives Scan** window opens.
2. In the **Scan on connection** section do the following:
   - Select the **Scan removable drives on connection via USB** check box, if you want Kaspersky Embedded Systems Security to automatically scan removable drives when they are connected.
   - If required, select the **Scan removable drives if its stored data volume does not exceed (MB)** and specify the maximum value in the field on the right.
   - In the **Scan with security level** drop-down list specify the security level with the settings that are required for removable drives scanning.

3. Click **OK**.

The specified settings are saved and applied.

On-Demand Scan task statistics

While the On-Demand Scan task is being executed, you can view information about the number of objects processed by Kaspersky Embedded Systems Security since it was started until the current moment.

This information remains available even if the task is paused. You can view the task statistics in the task log (see Section "Viewing statistics and information about a Kaspersky Embedded Systems Security task in task logs" on page 205).

► *To view the statistics of an On-Demand Scan task, take the following steps:*

1. Expand the **On-Demand Scan** node in the Application Console tree.
2. Select the On-Demand Scan task whose statistics you want to view.

Task statistics are displayed in the **Statistics** section of the details pane of the selected node.

The information about objects processed by Kaspersky Embedded Systems Security since it was started until the current moment is presented in the table below.

Table 61. On-Demand Scan task statistics

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

You can also view the On-Demand Scan task statistics in the selected task log by clicking the **Open task log** link in the **Management** section of the details pane.

It is recommended to manually process events registered in the task log on the **Events** tab upon the task completion.

Trusted Zone

This section provides information about the Trusted Zone of Kaspersky Embedded Systems Security, as well as instructions on how to add objects to the Trusted Zone when executing the tasks.

In this chapter

About the Trusted Zone

The Trusted Zone is a list of exclusions from the protection or scan scope that you can generate and apply to On-Demand Scan and Real-Time File Protection tasks.

If you selected the **Add Microsoft recommended files to exclusions list** and **Add Kaspersky Lab recommended files to exclusions list** check boxes when installing Kaspersky Embedded Systems Security, Kaspersky Embedded Systems Security adds to the Trusted Zone files recommended by Microsoft and Kaspersky Lab for Real-Time Computer Protection tasks.

You can create a Trusted Zone in Kaspersky Embedded Systems Security according to the following rules:

- Trusted processes. Objects accessed by application processes that are sensitive to file intercepts are placed in the Trusted Zone.
- Backup operations. Objects accessed by systems to backup hard drives to external devices are placed in the Trusted Zone.
- Exclusions. Objects specified by their location and / or an object detected inside them are placed in the Trusted Zone.

You can apply the Trusted Zone in the Real-Time File Protection task, newly created custom On-Demand Scan tasks, and all system On-Demand Scan tasks, except for the Quarantine Scan task.

The Trusted Zone is applied in Real-Time File Protection and On-Demand Scan tasks by default.

The list of rules for generating the Trusted Zone can be exported to a configuration file in XML format for it then to be imported into Kaspersky Embedded Systems Security running on another computer.

Trusted processes

Applies to the Real-Time File Protection and Traffic Security tasks.

Some applications on the computer may be instable if the files that they access are intercepted by Kaspersky Embedded Systems Security. Such applications include, for example, system domain controller applications.

To avoid disrupting the operation of such applications, you can disable protection of files accessed by the running processes of these applications (thereby creating a list of trusted processes within the Trusted Zone).

Microsoft Corporation recommends excluding some Microsoft Windows operating system files and Microsoft application files from Real-Time File Protection as programs that cannot be infected. The names of some of these are listed on the Microsoft website https://www.microsoft.com/en-us/ (article code: KB822158).

You can enable or disable the use of trusted processes in the Trusted Zone.

> If the executable process file is modified, for example, if it is updated, Kaspersky Embedded Systems Security will exclude it from the list of trusted processes.

The application does not apply path to file value on a protected computer to trust the process. The path to the file on the protected computer is used only to search for the file, calculate a checksum, and provide the user with the information about the source of the executable file.

Backup operations

Applies to Real-Time Computer Protection tasks.

While data stored on hard drives is backed up to external devices, you can disable protection of objects that are accessed during the backup operations. Kaspersky Embedded Systems Security will scan objects which the backup copying application opens for reading with the FILE_FLAG_BACKUP_SEMANTICS attribute.

Exclusions

Applies to Real-Time File Protection and On-Demand Scan tasks.

You can select tasks for which you want to use every exclusion added to the Trusted Zone. Also, you can exclude objects from scans in the security level settings of every single Kaspersky Embedded Systems Security task.

You can add objects to the Trusted Zone by their location on the computer, by name or name mask of the object detected in those objects, or by using both criteria.

Based on the exclusion, Kaspersky Embedded Systems Security can skip objects while performing the specified tasks according to the following settings:

- Specified objects detectable by name or name mask in the specified areas of the computer.
- All detectable objects in the specified areas of the computer.
- Specified detectable objects by name or name mask within the entire protection or scan scope.

Managing Trusted Zone via the Administration Plug-in

In this section, learn how to navigate through the Administration Plug-in interface and configure the Trusted Zone for one or for all computers of the network.

In this section

Navigation

Learn how to navigate to the required task settings via the interface.

In this section

Managing the application via the Kaspersky Security Center

► *To open the Trusted Zone via the Kaspersky Security Center policy:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure the task.
3. Select the **Policies** tab.
4. Double-click the policy name you want to configure.
5. In the **Properties: <Policy name>** window that opens, select the **Supplementary** section.
6. Click the **Settings** button in the **Trusted Zone** subsection.

   The **Trusted Zone** window opens.

Configure the policy as required.

If a computer is being managed by an active Kaspersky Security Center policy and this policy blocks changes to the application settings, these settings cannot be edited via the Application Console.

Opening the Trusted Zone properties window

► *To configure the Trusted Zone in the Application properties window:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure the task.
3. Select the **Devices** tab.
4. Open the **Properties: <Computer name>** window in one of the following ways:
   - Double-click the name of the protected computer.
   - Select the **Properties** item in the context menu of the protected computer.

   The **Properties: <Computer name>** window opens.
5. In the **Applications** section, select the **Kaspersky Embedded Systems Security**.
6. Click the **Properties** button.

   The **Kaspersky Embedded Systems Security settings** window opens.

7. Select the **Supplementary** section.
8. Click the **Settings** button in the **Trusted Zone** subsection.

   The **Trusted Zone** window opens.

Configure the Trusted Zone as required.

Configuring Trusted Zone settings via the Administration Plug-in

By default, Trusted Zone is applied for all newly created policies and tasks.

To configure Trusted Zone settings, do the following:

1. Specify the objects to be skipped (see Section "Adding an exclusion" on page 446) by Kaspersky Embedded Systems Security during task execution on the **Exclusions** tab.
2. Specify the processes to be skipped (see Section "Adding trusted processes" on page 448) by Kaspersky Embedded Systems Security during task execution on the **Trusted processes** tab.
3. Apply the not-a-virus mask (see Section "Applying the not-a-virus mask" on page 450).

In this section

Adding an exclusion

► *To add an exclusion to the Trusted Zone via the Kaspersky Security Center policy:*

1. Open the **Trusted Zone (see Section "Managing the application via the Kaspersky Security Center" on page** 445**)** window.
2. On the **Exclusions** tab, specify the objects to be skipped by Kaspersky Embedded Systems Security during scanning:
   - To create recommended exclusions, click the **Add recommended exclusions** button.

     Clicking this button allows you to extend the list of exclusions by adding exclusions recommended by Microsoft, exclusions recommended by Kaspersky Lab.
   - To import exclusions, click the **Import** button and in the window that opens select the files that Kaspersky Embedded Systems Security will consider trusted.
   - To manually specify the conditions under which a file will be considered trusted click the **Add** button.

     The **Exclusion** window opens.

3. In the **Object will not be scanned if the following conditions are met** section, specify the objects that you want to exclude from the protection / scan scope and objects that you want to exclude among detectable objects:

    - If you want to exclude an object from the protection or scan scope:

        a. Select the **Object to scan** check box.

            Adds a file, folder, drive, or script file to an exclusion.

            If the check box is selected, Kaspersky Embedded Systems Security skips the specified predefined scope, file, folder, drive or script file while running the scan with the use of the Kaspersky Embedded Systems Security component selected in the **Rule usage scope** section.

            The check box is cleared by default.

        b. Click the **Edit** button.

            The **Select an object** window opens.

        c. Specify the object that you want to exclude from the scan scope.

            > You can use the special symbols ? and * when specifying the objects.

        d. Click **OK**.

        e. Select the **Apply also to subfolders** check box, if you want to exclude all child files and folders of the specified object from the protection or scan scope.

    - If you want to specify the name of a detectable object:

        a. Select the **Objects to detect** check box.

            Objects are excluded from scanning by the name or name mask of the detectable object. The list of names of detectable objects is available on the Virus Encyclopedia website.

            If this check box is selected, Kaspersky Embedded Systems Security skips specified detectable objects during scanning.

            If the check box is cleared, Kaspersky Embedded Systems Security detects all objects specified in the application by default.

            The check box is cleared by default.

        b. Click the **Edit** button.

            The **List of objects to detect** window opens.

        c. Specify the name or the mask of the name of the detectable object according to the Virus Encyclopedia classification.

        d. Click the **Add** button.

        e. Click **OK**.

4. In the **Rule usage scope** section, select the check boxes next to the names of the tasks to which the exclusion should be applied.

    Name of the Kaspersky Embedded Systems Security task in which the rule is used.

5. Click **OK**.

The exclusion is displayed in the list on the **Exclusions** tab of the **Trusted Zone** window.

Adding trusted processes

► *To add one or a number of processes to the list of trusted processes:*

1. Open the **Trusted Zone** window (see Section "Managing the application via the Kaspersky Security Center" on page 445).
2. Select the **Trusted processes** tab.
3. Select the **Do not check file backup operations** check box to skip scanning of file read operations.

   The check box enables or disables the scanning of file read operations if such operations are performed by backup tools installed on the computer.

   If the check box is selected, Kaspersky Embedded Systems Security skips file read operations performed by backup tools installed on the computer.

   If the check box is cleared, Kaspersky Embedded Systems Security scans file read operations performed by backup tools installed on the computer.

   The check box is selected by default.
4. Select the **Do not check file activity of the specified processes** check box to skip file operations scanning for trusted processes.

   The check box enables or disables the scanning of file activity of trusted processes.

   If the check box is selected, Kaspersky Embedded Systems Security skips operations of trusted processes during scanning.

   If the check box is cleared, Kaspersky Embedded Systems Security scans file operations of trusted processes.

   The check box is cleared by default.
5. Click the **Add** button.
6. From the button context menu select one of the options:

   - **Multiple processes**.

     In the **Trusted processes adding** window that opens, configure the following:

     a. **Use full process path on disk to consider it trusted**.

        If the check box is selected, Kaspersky Embedded Systems Security uses the full path to the file to determine whether the process is trusted.

        If the check box is cleared, the path to the file is not used to determine whether the process is trusted.

        The check box is cleared by default.

     b. **Use process file hash to consider it trusted**.

        If the check box is selected, Kaspersky Embedded Systems Security uses the selected file hash to determine the process trust status.

        If the check box is cleared, the file hash is not used to determine the process trust status.

        The check box is selected by default.

     c. Click the **Browse** button to add data based on executable processes.

     d. Select an executable file in the window that opens.

> You can only add one executable file at a time. Repeat steps c-d to add other executable files.

e. Click the **Processes** button to add data based on running processes.

f. Select processes in the window that opens. To select multiple processes, press and hold **CTRL** button while selecting.

g. Click **OK**.

> It is required that the account under which the Real-Time File Protection task is run has the administrator rights on the computer with Kaspersky Embedded Systems Security installed in order to allow viewing the list of active processes. You can sort processes in the list of active processes by file name, process identifier (PID), or path to the executable file of the process on the local computer. Note, that you can select running processes by clicking the **Processes** button only using the Application Console on a local computer or in the specified host settings via the Kaspersky Security Center.

- **One process based on file name and path.**

  In the **Adding a process** window that opens, do the following:

  a. Enter a path to executable file (including the file name).

  b. Click **OK**.

- **One process based on object properties.**

  In the **Trusted process adding** window that opens, configure the following:

  a. Click the **Browse** button and select a process.

  b. **Use full process path on disk to consider it trusted**.

  If the check box is selected, Kaspersky Embedded Systems Security uses the full path to the file to determine whether the process is trusted.

  If the check box is cleared, the path to the file is not used to determine whether the process is trusted.

  The check box is cleared by default.

  c. **Use process file hash to consider it trusted**.

  If the check box is selected, Kaspersky Embedded Systems Security uses the selected file hash to determine the process trust status.

  If the check box is cleared, the file hash is not used to determine the process trust status.

  The check box is selected by default.

  d. Click **OK**.

> To add the selected process to the list of trusted processes, at least one trust criterion must be selected.

7. In the **Adding trusted processes** window, click the **OK** button.

The selected file or process will be added to the list of trusted processes in the **Trusted Zone** window.

Applying the not-a-virus mask

The not-a-virus mask allows to skip legitimate software files and web resources, which can be considered harmful, during the scanning. The mask affects the following tasks:

- Real-Time File Protection.
- On-Demand scan.

If the mask is not added to exclusions list, Kaspersky Embedded Systems Security will apply the actions specified in the task settings for the software which fall under this category.

► *To apply the not-a-virus mask:*

1. Open the **Trusted Zone** window (see Section "Managing the application via the Kaspersky Security Center" on page 445).
2. On the **Exclusions** tab, in the **Objects to detect** column, scroll the list and select the line with **not-a-virus:*** value, if the check box is cleared.
3. Click **OK**.

New configuration is applied.

Managing Trusted Zone via the Application Console

In this section, learn how to navigate through the Application Console interface and configure the Trusted Zone on a local computer.

In this section

Applying Trusted Zone for tasks in the Application Console

By default, the Trusted Zone is applied in the Real-Time File Protection task, newly created custom On-Demand Scan tasks, and all system On-Demand Scan tasks, except the Quarantine Scan task.

After the Trusted Zone is enabled or disabled, the specified exclusions are immediately applied or cease to be applied in running tasks.

► *To enable or disable the use of the Trusted Zone in Kaspersky Embedded Systems Security tasks:*

1. In the Application Console tree, open the context menu of the task, for which you want to configure the Trusted Zone usage.
2. Select **Properties**.

   The **Task settings** window opens.
3. In the window that opens, select the **General** tab and do one of the following actions:
   - To apply the Trusted Zone in the task, select the **Apply Trusted Zone** check box.
   - To disable the Trusted Zone in the task, clear the **Apply Trusted Zone** check box.
4. If you want to configure Trusted Zone settings, click the link in the name of the **Apply Trusted Zone** check box.

   The **Trusted Zone** window opens.
5. Click **OK** in the **Task settings** window to save changes.

Configuring Trusted Zone settings in the Application Console

To configure Trusted Zone settings, do the following:

1. Specify the objects to be skipped (see Section "Adding an exclusion to the Trusted Zone" on page 452) by Kaspersky Embedded Systems Security during task execution on the **Exclusions** tab.
2. Specify the processes to be skipped (see Section "Trusted processes" on page 453) by Kaspersky Embedded Systems Security during task execution on the **Trusted processes** tab.
3. Apply the Trusted Zone for the application tasks (see Section "Applying Trusted Zone for tasks in the Application Console" on page 451).
4. Apply the not-a-virus mask (see Section "Applying the not-a-virus mask" on page 455).

In this section

Adding an exclusion to the Trusted Zone

► *To manually add an exclusion to the Trusted Zone via the Application Console:*

1. In the Application Console tree, open the context menu of the **Kaspersky Embedded Systems Security** node.
2. Select **Configure Trusted Zone settings** menu option.

   The **Trusted Zone** window opens.
3. Select the **Exclusions** tab.
4. Click the **Add** button.

   The **Exclusion** window opens.
5. In the **Object will not be scanned if the following conditions are met** section, specify the objects that you want to exclude from the protection / scan scope and objects that you want to exclude among detectable objects:
   - If you want to exclude an object from the protection or scan scope:

     a. Select the **Object to scan** check box.

        Adds a file, folder, drive, or script file to an exclusion.

        If the check box is selected, Kaspersky Embedded Systems Security skips the specified predefined scope, file, folder, drive or script file while running the scan with the use of the Kaspersky Embedded Systems Security component selected in the **Rule usage scope** section.

        The check box is cleared by default.

     b. Click the **Edit** button.

        The **Select an object** window opens.

     c. Specify the object that you want to exclude from the scan scope.

        > You can use the special symbols ? and * when specifying the objects.

     d. Click **OK**.

     e. Select the **Apply also to subfolders** check box, if you want to exclude all child files and folders of the specified object from the protection or scan scope.
   - If you want to specify the name of a detectable object:

     a. Select the **Objects to detect** check box.

        Objects are excluded from scanning by the name or name mask of the detectable object. The list of names of detectable objects is available on the Virus Encyclopedia website.

        If this check box is selected, Kaspersky Embedded Systems Security skips specified detectable objects during scanning.

        If the check box is cleared, Kaspersky Embedded Systems Security detects all objects specified in the application by default.

        The check box is cleared by default.

b. Click the **Edit** button.

   The **List of objects to detect** window opens.

c. Specify the name or the mask of the name of the detectable object according to the Virus Encyclopedia classification.

d. Click the **Add** button.

e. Click **OK**.

6. In the **Rule usage scope** section, select the check boxes next to the names of the tasks to which the exclusion should be applied.

   Name of the Kaspersky Embedded Systems Security task in which the rule is used.

7. Click **OK**.

The exclusion is displayed in the list on the **Exclusions** tab of the **Trusted Zone** window.

Trusted processes

You can add a process to the list of trusted processes using one of the following methods:

- Select the process from the list of processes running on the protected computer.
- Select the executable file of a process regardless of whether the process is currently running.

If the executable file of a process has been modified, Kaspersky Embedded Systems Security excludes this process from the list of trusted processes.

► *To add one or a number of processes to the list of trusted processes:*

1. In the Application Console tree, open the context menu of the **Kaspersky Embedded Systems Security** node.
2. Select **Configure Trusted Zone settings** menu option.

   The **Trusted Zone** window opens.

3. Select the **Trusted processes** tab.
4. Select the **Do not check file backup operations** check box to skip scanning of file read operations.

   The check box enables or disables the scanning of file read operations if such operations are performed by backup tools installed on the computer.

   If the check box is selected, Kaspersky Embedded Systems Security skips file read operations performed by backup tools installed on the computer.

   If the check box is cleared, Kaspersky Embedded Systems Security scans file read operations performed by backup tools installed on the computer.

   The check box is selected by default.

5. Select the **Do not check file activity of the specified processes** check box to skip file operations scanning for trusted processes.

   The check box enables or disables the scanning of file activity of trusted processes.

   If the check box is selected, Kaspersky Embedded Systems Security skips operations of trusted processes during scanning.

   If the check box is cleared, Kaspersky Embedded Systems Security scans file operations of trusted processes.

   The check box is cleared by default.

6. Click the **Add** button.

7. From the button context menu select one of the options:

   - **Multiple processes**.

     In the **Trusted processes adding** window that opens, configure the following:

     a. **Use full process path on disk to consider it trusted**.

        If the check box is selected, Kaspersky Embedded Systems Security uses the full path to the file to determine whether the process is trusted.

        If the check box is cleared, the path to the file is not used to determine whether the process is trusted.

        The check box is cleared by default.

     b. **Use process file hash to consider it trusted**.

        If the check box is selected, Kaspersky Embedded Systems Security uses the selected file hash to determine the process trust status.

        If the check box is cleared, the file hash is not used to determine the process trust status.

        The check box is selected by default.

     c. Click the **Browse** button to add data based on executable processes.

     d. Select an executable file in the window that opens.

     > You can only add one executable file at a time. Repeat steps c-d to add other executable files.

     e. Click the **Processes** button to add data based on running processes.

     f. Select processes in the window that opens. To select multiple processes, press and hold **CTRL** button while selecting.

     g. Click **OK**.

     > It is required that the account under which the Real-Time File Protection task is run has the administrator rights on the computer with Kaspersky Embedded Systems Security installed in order to allow viewing the list of active processes. You can sort processes in the list of active processes by file name, process identifier (PID), or path to the executable file of the process on the local computer. Note, that you can select running processes by clicking the **Processes** button only using the Application Console on a local computer or in the specified host settings via the Kaspersky Security Center.

- **One process based on file name and path.**

  In the **Adding a process** window that opens, do the following:

  a. Enter a path to executable file (including the file name).

  b. Click **OK**.

- **One process based on object properties.**

  In the **Trusted process adding** window that opens, configure the following:

  a. Click the **Browse** button and select a process.

  b. **Use full process path on disk to consider it trusted**.

  If the check box is selected, Kaspersky Embedded Systems Security uses the full path to the file to determine whether the process is trusted.

  If the check box is cleared, the path to the file is not used to determine whether the process is trusted.

  The check box is cleared by default.

  c. **Use process file hash to consider it trusted**.

  If the check box is selected, Kaspersky Embedded Systems Security uses the selected file hash to determine the process trust status.

  If the check box is cleared, the file hash is not used to determine the process trust status.

  The check box is selected by default.

  d. Click **OK**.

  > To add the selected process to the list of trusted processes, at least one trust criterion must be selected.

8. In the **Adding trusted processes** window, click the **OK** button.

The selected file or process will be added to the list of trusted processes in the **Trusted Zone** window.

Applying the not-a-virus mask

The not-a-virus mask allows to skip legitimate software files and web resources, which can be considered harmful, during the scanning. The mask affects the following tasks:

- Real-Time File Protection.
- On-Demand scan.

If the mask is not added to exclusions list, Kaspersky Embedded Systems Security will apply the actions specified in the task settings for the software or web resources which fall under this category.

► *To apply the not-a-virus mask:*

1. In the Application Console tree, open the context menu of the **Kaspersky Embedded Systems Security** node.
2. Select **Configure Trusted Zone settings** menu option.

   The **Trusted Zone** window opens.

3. Select the **Exclusions** tab.
4. Scroll the list and select the line with **not-a-virus:*** value, if the check box is cleared.
5. Click **OK**.

New configuration is applied.

Exploit Prevention

This section contains instructions on how to configure process memory protection settings.

In this chapter

About the Exploit Prevention

Kaspersky Embedded Systems Security provides the ability to protect process memory from exploits. This feature is implemented in the Exploit Prevention component. You can change the component's activity status and configure process memory protection settings.

The component protects process memory from exploits by inserting an external Process Protection Agent (“Agent”) in the protected process.

A Process Protection Agent is a dynamically loaded Kaspersky Embedded Systems Security module that is inserted in protected processes to monitor their integrity and reduce the risk of being exploited.

The Agent's operation within the protected process requires starting and stopping the process: the initial loading of the Agent into a process added to the protected process list is only possible if the process is restarted. Additionally, after a process has been removed from the protected process list, the Agent can be unloaded only after the process has been restarted.

The Agent must be stopped to unload it from protected processes: if the Exploit Prevention component is uninstalled, the application freezes the environment and forces the Agent to be unloaded from protected processes. If during the component uninstallation the Agent is inserted in any of the protected processes, you must terminate the affected process. Computer restart may be required (for example, if system process is being protected).

If evidence of an exploit attack in a protected process is detected, Kaspersky Embedded Systems Security performs one of the following actions:

- Terminates the process if an exploit attempt is made.
- Reports the fact that the process has been compromised.

You can stop process protection using one of the following methods:

- Uninstalling the component.
- Removing the process from the list of protected processes and restarting the process.

Kaspersky Security Exploit Prevention Service

Kaspersky Security Exploit Prevention Service is required on the protected computer in order for the Exploit Prevention component to be most effective. This service and the Exploit Prevention component are part of the recommended installation. During installation of the service on the protected computer, the kavfswh process is created and started. This communicates information about protected processes from the component to the Security Agent.

After the Kaspersky Security Exploit Prevention Service is stopped, Kaspersky Embedded Systems Security continues to protect processes added to the protected process list, is also loaded in newly-added processes, and applies all available exploit prevention techniques to protect process memory.

> If your computer runs Windows 10 operating system or later, the application will not continue to protect processes and process memory after the Kaspersky Security Exploit Prevention Service is stopped.

If the Kaspersky Security Exploit Prevention Service is stopped, the application will not receive information about events occurring with protected processes (including information about exploit attacks and the termination of processes). Furthermore, the Agent will not be able to receive information about new protection settings and the addition of new processes to the protected process list.

Exploit Prevention mode

You can select one of the following modes to configure actions to reduce risks that vulnerabilities will be exploited in protected processes:

- **Terminate on exploit**: apply this mode to terminate a process when an exploit attempt is made.

  > Upon detecting an attempt to exploit a vulnerability in a protected critical operating system process, Kaspersky Embedded Systems Security does not terminate the process, regardless of the mode indicated in the Exploit Prevention component settings.

- **Notify only**: apply this mode to receive information about instances of exploits in protected processes using events in the Security log.

  If this mode is selected, Kaspersky Embedded Systems Security logs all attempts to exploit vulnerabilities by creating events.

Managing Exploit Prevention via the Administration Plug-in

In this section, learn how to navigate the Administration Plug-In interface and configure the component settings for one or all computers on the network.

In this section

Navigation

Learn how to navigate to the required task settings via the interface.

In this section

Opening policy settings for the Exploit Prevention

► *To open the Exploit Prevention settings via the Kaspersky Security Center policy:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure the task.
3. Select the **Policies** tab.
4. Double-click the policy name you want to configure.
5. In the **Properties: <Policy name>** window that opens, select the **Real-time computer protection** section.
6. Click the **Settings** button in the **Exploit Prevention** subsection.

   The **Exploit Prevention** window opens.

Configure the Exploit Prevention as required.

Opening the Exploit Prevention properties window

► *To open the **Properties: <Server name>** window for the Exploit Prevention:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure the task.
3. Select the **Devices** tab.
4. Open the **Properties: <Computer name>** window in one of the following ways:
   - Double-click the name of the protected computer.
   - Select the **Properties** item in the context menu of the protected computer.

   The **Properties: <Computer name>** window opens.
5. In the **Applications** section, select the **Kaspersky Embedded Systems Security**.
6. Click the **Properties** button.

   The **Kaspersky Embedded Systems Security settings** window opens.

7. Select the **Real-time computer protection** section.
8. Click the **Settings** button in the **Exploit Prevention** subsection.

   The **Exploit Prevention** window opens.

Configure the Exploit Prevention as required.

Configuring process memory protection settings

► *To configure settings to protect the memory of processes added to the list of protected processes, perform the following actions:*

1. Open the **Exploit Prevention** (see Section "**Opening policy settings for the Exploit Prevention**" on page 459) window.
2. In the **Exploit prevention mode** block, configure the following settings:
   - **Prevent vulnerable processes exploit**.

     If this check box is selected, Kaspersky Embedded Systems Security reduces the risks of exploitation of vulnerabilities in processes in the list of protected processes.

     If this check box is cleared, Kaspersky Embedded Systems Security does not protect computer processes from exploits.

     The check box is cleared by default.

     - **Terminate on exploit**.

       If this mode is selected, Kaspersky Embedded Systems Security terminates a protected process upon detecting an exploit attempt if an active impact reduction technique has been applied to the process.

     - **Notify only**.

       If this mode is selected, Kaspersky Embedded Systems Security reports exploits by displaying a terminal window. The compromised process continues to run.

       If Kaspersky Embedded Systems Security detects an exploit in a critical process while the application is running in **Terminate on exploit** mode, the component forcibly switches to **Notify only** mode.
3. In the **Preventing actions** block, configure the following settings:
   - **Notify about abused processes via Terminal Service.**

     If this check box is selected, Kaspersky Embedded Systems Security displays a terminal window with a description explaining why protection was activated and an indication of the process in which an exploit attempt was detected.

     If the check box is cleared, Kaspersky Embedded Systems Security displays a terminal window when an exploit attempt or termination of a compromised process is detected. A terminal window is displayed regardless of the status of the Kaspersky Security Exploit Prevention Service. The check box is selected by default.

- **Prevent vulnerable processes exploit even if Kaspersky Security Service is disabled**.

  If this check box is selected, Kaspersky Embedded Systems Security will reduce risk of vulnerabilities being exploited in processes that have already been started, regardless of whether the Kaspersky Security Service is running. Kaspersky Embedded Systems Security will not protect processes added after the Kaspersky Security Service is stopped. After the service is started, exploit impact reduction will be stopped for all processes.

  If this check box is cleared, Kaspersky Embedded Systems Security does not protect processes from exploits when the Kaspersky Security Service is stopped.

  The check box is selected by default.

4. Click **OK**.

Kaspersky Embedded Systems Security saves and applies the configured process memory protection settings.

Adding a process for protection

Exploit Prevention component protects a number of processes by default. You can exclude the processes from the protection scope by clearing the corresponding check boxes in the list.

► *To add a process to the list of protected processes:*

1. Open the **Exploit Prevention** (see Section "**Opening policy settings for the Exploit Prevention**" on page 459) window.
2. On the **Protected processes** tab, click the **Browse** button.

   The Microsoft Windows Explorer window opens.
3. Select the process you want to add to the list.
4. Click the **Open** button.

   The process name is displayed in the line.
5. Click the **Add** button.

   The process will be added to the list of protected processes.
6. Select the added process.
7. Click **Set exploit prevention techniques**.

   The **Exploit prevention techniques** window opens.
8. Select one of the options for applying impact reduction techniques:
   - **Apply all available exploit prevention techniques**.

     If this option is selected, the list cannot be edited. All techniques available for a process are applied by default.
   - **Apply selected exploit prevention techniques**.

     If this option is selected, you can edit the list of impact reduction techniques applied:

     a. Select the check boxes next to the techniques that you want to apply to protect the selected process.

     b. Select or clear the **Apply Attack Surface Reduction technique** check box.

9. Configure settings for the Attack Surface Reduction technique:
   - Enter the names of the modules whose launch will be blocked from the protected process in the **Deny modules** field.
   - In the **Do not deny modules if launched in the Internet Zone** field, select the check boxes next to the options under which you want to allow modules to be launched:
     - Internet
     - Local intranet
     - Trusted sites
     - Restricted sites
     - Computer

     > These settings are only applicable to Internet Explorer®.
10. Click **OK**.

The process is added to the task protection scope.

Managing Exploit Prevention via the Application Console

In this section, learn how to navigate the Application Console interface and configure the component settings on a local computer.

In this section

Navigation

Learn how to navigate to the required task settings via the interface.

In this section

Opening the Exploit Prevention general settings

► *To open the **Exploit Prevention settings** window:*

1. In the Application Console tree, select the **Kaspersky Embedded Systems Security** node.
2. Open the context menu and select the **Exploit Prevention: general settings** menu option.

   The **Exploit Prevention settings** window opens.

Configure general settings for the Exploit Prevention as required.

Opening the Exploit Prevention process protection settings

► *To open the **Processes protection settings** window:*

1. In the Application Console tree, select the **Kaspersky Embedded Systems Security** node.
2. Open the context menu and select the **Exploit Prevention: processes protection settings** menu option.

   The **Processes protection settings** window opens.

Configure process protection settings for the Exploit Prevention as required.

Configuring process memory protection settings

► *To add a process to the list of protected processes:*

1. Open the Exploit Prevention settings window.
2. In the **Exploit prevention mode** block, configure the following settings:
   - **Prevent vulnerable processes exploit**.

     If this check box is selected, Kaspersky Embedded Systems Security reduces the risks of exploitation of vulnerabilities in processes in the list of protected processes.

     If this check box is cleared, Kaspersky Embedded Systems Security does not protect computer processes from exploits.

     The check box is cleared by default.

     - **Terminate on exploit**.

       If this mode is selected, Kaspersky Embedded Systems Security terminates a protected process upon detecting an exploit attempt if an active impact reduction technique has been applied to the process.

     - **Notify only**.

       If this mode is selected, Kaspersky Embedded Systems Security reports exploits by displaying a terminal window. The compromised process continues to run.

       If Kaspersky Embedded Systems Security detects an exploit in a critical process while the application is running in **Terminate on exploit** mode, the component forcibly switches to **Notify only** mode.

3. In the **Preventing actions** block, configure the following settings:

   - **Notify about abused processes via Terminal Service.**

     If this check box is selected, Kaspersky Embedded Systems Security displays a terminal window with a description explaining why protection was activated and an indication of the process in which an exploit attempt was detected.

     If the check box is cleared, Kaspersky Embedded Systems Security displays a terminal window when an exploit attempt or termination of a compromised process is detected. A terminal window is displayed regardless of the status of the Kaspersky Security Exploit Prevention Service. The check box is selected by default.

   - **Prevent vulnerable processes exploit even if Kaspersky Security Service is disabled**.

     If this check box is selected, Kaspersky Embedded Systems Security will reduce risk of vulnerabilities being exploited in processes that have already been started, regardless of whether the Kaspersky Security Service is running. Kaspersky Embedded Systems Security will not protect processes added after the Kaspersky Security Service is stopped. After the service is started, exploit impact reduction will be stopped for all processes.

     If this check box is cleared, Kaspersky Embedded Systems Security does not protect processes from exploits when the Kaspersky Security Service is stopped.

     The check box is selected by default.

4. In the **Exploit Prevention settings** window click **OK**.

Kaspersky Embedded Systems Security saves and applies the configured process memory protection settings.

Adding a process for protection

Exploit Prevention component protects a number of processes by default. You can uncheck the processes, that you don't want to protect in the list of protected processes.

► *To add a process to the list of protected processes:*

1. Open the Processes protection settings window.
2. To add a process to protect them from abuse and to reduce possible exploit impact, perform the following actions:
   a. Click the **Browse** button.

      The standard Microsoft Windows **Open** window opens.

   b. In the window that opens select a process you want to add to the list.
   c. Click the **Open** button.
   d. Click the **Add** button.

      The process will be added to the list of protected processes.
3. Select a process in the list.
4. On the **Process protection settings**, current configuration is displayed:
   - **Process name**.
   - **Is being executed**.
   - **Exploit prevention techniques applied**.

- **Attack Surface Reduction settings**.

5. To modify the exploit prevention techniques that are applied to the process, select the **Exploit prevention techniques** tab.
6. Select one of the options for applying impact reduction techniques:
   - **Apply all available exploit prevention techniques**.

     If this option is selected, the list cannot be edited. All techniques available for a process are applied by default.
   - **Apply listed exploit prevention techniques for the process**.

     If this option is selected, you can edit the list of impact reduction techniques applied:

     a. Select the check boxes next to the techniques that you want to apply to protect the selected process.
7. Configure settings for the Attack Surface Reduction technique:
   - Enter the names of the modules whose launch will be blocked from the protected process in the **Deny modules** field.
   - In the **Do not deny modules if launched in the Internet Zone** field, select the check boxes next to the options under which you want to allow modules to be launched:
     - Internet
     - Local intranet
     - Trusted sites
     - Restricted sites
     - Computer

   > These settings are only applicable to Internet Explorer®.
8. Click **OK**.

The process is added to the task protection scope.

Exploit prevention techniques

Table 62. Exploit prevention techniques

Exploit prevention technique	Description
Data Execution Prevention (DEP)	Data execution prevention blocks execution of arbitrary code in protected areas of memory.
Address Space Layout Randomization (ASLR)	Changes to the layout of data structures in the address space of the process.
Structured Exception Handler Overwrite Protection (SEHOP)	Replacement of exception records or replacement of the exception handler.
Null Page Allocation	Prevention of redirecting the null pointer.
LoadLibrary Network Call Check (Anti ROP)	Protection against loading DLLs from network paths.
Executable Stack (Anti ROP)	Blocking of unauthorized execution of areas of the stack.
Anti RET Check (Anti ROP)	Check that the CALL instruction is invoked safely.
Anti Stack Pivoting (Anti ROP)	Protection against relocation of the ESP stack pointer to an executable address.
Simple Export Address Table Access Monitor (EAT Access Monitor & EAT Access Monitor via Debug Register)	Protection of read access to the export address table for kernel32.dll, kernelbase.dll, and ntdll.dll
Heap Spray Allocation (Heapspray)	Protection against allocating memory to execute malicious code.
Execution Flow Simulation (Anti Return Oriented Programming)	Detection of suspicious chains of instructions (potential ROP gadget) in the Windows API component.
IntervalProfile Calling Monitor (Ancillary Function Driver Protection (AFDP))	Protection against escalation of privileges through a vulnerability in the AFD driver (execution of arbitrary code in ring 0 through a QueryIntervalProfile call).
Attack Surface Reduction (ASR)	Blocking the start of vulnerable add-ins via the protected process.
Anti Process Hollowing (Hollowing)	Protection against creating and executing the malicious copies of trusted processes.
Anti AtomBombing (APC)	Global atom table exploit via Asynchronous Procedure Calls (APC).
Anti CreateRemoteThread (RThreadLocal)	Another process has created a thread in protected process.
Anti CreateRemoteThread (RThreadRemote)	Protected process has created a thread in another process.

Integrating with third-party systems

This section describes integration of Kaspersky Embedded Systems Security with third-party features and technologies.

In this chapter

Monitoring performance. Kaspersky Embedded Systems Security counters

This section provides information about Kaspersky Embedded Systems Security counters: System Monitor performance counters, and SNMP counters and traps.

In this section

Performance counters for System Monitor

This section contains information about performance counters for the Microsoft Windows System Monitor that are registered by Kaspersky Embedded Systems Security during installation.

In this section

About Kaspersky Embedded Systems Security performance counters

The **Performance Counters** component is included in the installed components of Kaspersky Embedded Systems Security by default. Kaspersky Embedded Systems Security registers its own performance counters for the Microsoft Windows System Monitor during installation.

Using Kaspersky Embedded Systems Security counters, you can monitor the application's performance while Real-Time Protection tasks are running. You can uncover tight places when it is running with other applications and resource shortages. You can diagnose undesirable Kaspersky Embedded Systems Security settings and crashes in its operation.

You can view Kaspersky Embedded Systems Security performance counters by opening the **Performance** console in the **Administration** item of Windows Control Panel.

The following sections list definitions of counters, recommended intervals for taking readings, threshold values, and recommendations for Kaspersky Embedded Systems Security settings if the counter values exceed them.

Total number of denied requests

Table 63. Total number of denied requests

Name	Total number of requests denied
Definition	Total number of requests from the file interception driver to process objects that were not accepted by the application processes; counted from the time Kaspersky Embedded Systems Security was last started. The application skips objects for which requests for processing are denied by Kaspersky Embedded Systems Security processes.
Purpose	This counter can help you detect: • Lower quality of Real-Time Protection from bogging down the working processes of Kaspersky Embedded Systems Security. • Interruption of Real-Time Protection because of file interception dispatcher failures.
Normal / threshold value	0 / 1.
Recommended reading interval	1 hour.
Recommendations for configuration if value exceeds the threshold	The number of requests for processed denied corresponds to the number of skipped objects. The following situations are possible depending on counter behavior: • the counter shows several requests denied over extended period of time: all Kaspersky Embedded Systems Security processes are fully loaded so Kaspersky Embedded Systems Security could not scan objects. To avoid skipping objects, increase the number of application processes for Real-Time Protection tasks. You can use such settings of Kaspersky Embedded Systems Security as **Maximum number of active processes** and **Number of processes for real-time protection**. • The number of request denied significantly exceeds the critical threshold and is growing quickly: the file interception dispatcher has crashed. Kaspersky Embedded Systems Security is not scanning objects on access. Restart Kaspersky Embedded Systems Security.

Total number of skipped requests

Table 64. Total number of skipped requests

Name	Total number of requests skipped
Definition	The total number of requests from the file interception driver to process objects that have been received by Kaspersky Embedded Systems Security but have not generated events of processing completion; this number is counted starting from the moment application was last started. If a request for processing of such object accepted by one of the work processes did not send an event for completion of the processing, the driver will transfer such request to another process and the value of counter **Total Number of Skipped Requests** will increment by 1. If the driver has gone through all of the working processes and none of them has received the request for processing (was busy) or has sent events of processing completion, Kaspersky Embedded Systems Security will skip such object, so the value of counter **Total Number of Skipped Requests** will increment by 1.
Purpose	This counter enables you to detect drops in performance because of file interception dispatcher failures.
Normal / threshold value	0 / 1
Recommended reading interval	1 hour
Recommendations for configuration if value exceeds the threshold	If the counter value is anything other than zero, this means that one or several file interception dispatcher streams have frozen and are down. The counter value corresponds to the number of streams currently down. If the scan speed is not satisfactory, restart Kaspersky Embedded Systems Security to restore the off-line streams.

Number of requests not processed because of lack of system resources

Table 65. Number of requests not processed because of lack of system resources

Name	Number of requests not processed due to lack of resources.
Definition	Total number of requests from the file interception driver which were not processed because of a lack of system resources (for example, RAM); counted from the time Kaspersky Embedded Systems Security was last started. Kaspersky Embedded Systems Security skips objects requests to process which are not processed by the file interception driver.
Purpose	This counter can be used to detect and eliminate potentially lower quality in Real-Time Protection that occurs because of low system resources.
Normal / threshold value	0 / 1.
Recommended reading interval	1 hour.
Recommendations for configuration if value exceeds the threshold	If the counter value is anything other than zero, Kaspersky Embedded Systems Security working processes need more RAM to process requests. Active processes of other applications may be using all available RAM.

Number of requests sent to be processed

Table 66. Number of requests sent to be processed

Name	Number of requests sent to be processed.
Definition	The number of objects that wait for processing by working processes.
Purpose	This counter can be used to track the load on Kaspersky Embedded Systems Security working processes and the overall level of file activity on the computer.
Normal / threshold value	The counter value may vary depending on the level of file activity on the computer.
Recommended reading interval	1 minute
Recommendations for configuration if value exceeds the threshold	No

Average number of file interception dispatcher streams

Table 67. Average number of file interception dispatcher streams

Name	Average number of file interception dispatcher streams.
Definition	The number of file interception dispatcher streams in one process and the average for all processes currently involved in Real-Time Protection tasks.
Purpose	This counter can be used to detect and eliminate potentially lower quality in Real-Time Protection that occurs because of full load on Kaspersky Embedded Systems Security processes.
Normal / threshold value	Varies / 40
Recommended reading interval	1 minute
Recommendations for configuration if value exceeds the threshold	Up to 60 file interception dispatcher streams can be created in each working process. If the counter value approaches 60, there is a risk that none of the working processes will be able to process the next request in queue from the file interception driver and Kaspersky Embedded Systems Security will skip the object. Increase the number of Kaspersky Embedded Systems Security processes for Real-Time Protection tasks. You can use such Kaspersky Embedded Systems Security settings as **Maximum number of active processes** and **Number of processes for real-time protection**.

Maximum number of file interception dispatcher streams

Table 68. Maximum number of file interception dispatcher streams

Name	Maximum number of file interception dispatcher streams.
Definition	The number of file interception dispatcher streams in one process and the maximum for all processes currently involved in Real-Time Protection tasks.
Purpose	This counter enables you to detect and eliminate drops in performance because of uneven distribution of loads in running processes.
Normal / threshold value	Varies / 40
Recommended reading interval	1 minute
Recommendations for configuration if value exceeds the threshold	If the value of this counter significantly and continuously exceeds the following of the **Average number of file interception dispatcher streams** counter, Kaspersky Embedded Systems Security is distributing the load to running processes unevenly. Restart Kaspersky Embedded Systems Security.

Number of elements in infected objects queue

Table 69. Number of elements in infected objects queue

Name	Number of items in the infected objects queue.
Definition	Number of infected objects currently waiting to be processed (disinfected or deleted).
Purpose	This counter can help you detect: • Interruption of Real-Time Protection because of possible file interception dispatcher failures. • Overload of processes because of uneven distribution of processor time between different working processes and Kaspersky Embedded Systems Security. • Virus outbreaks.
Normal / threshold value	This value may be something other than zero while Kaspersky Embedded Systems Security is processing infected or probably infected objects but will return to zero after processing is finished / The value remains non-zero for an extended period of time.
Recommended reading interval	1 minute
Recommendations for configuration if value exceeds the threshold	If the value of the counter does not return to zero for an extended period of time: • Kaspersky Embedded Systems Security is not processing objects (the file interception dispatcher may have crashed). Restart Kaspersky Embedded Systems Security. • Not enough processor time to process the objects. Make sure Kaspersky Embedded Systems Security receives additional processor time (by lowering other applications' load on the computer, for example). • There has been a virus outbreak. A large number of infected or probably infected objects in the Real-Time File Protection task also is a sign of a virus outbreak. You can view information about the number of detected objects in the task statistics or task logs.

Number of objects processed per second

Table 70. Number of objects processed per second

Name	Number of objects processed per second.
Definition	Number of objects processed divided by the amount of time that it took to process those objects (calculated over equal time intervals).
Purpose	This counter reflects the speed of object processing; it can be used to detect and eliminate low points in computer performance that occur because of insufficient processor time being allotted to Kaspersky Embedded Systems Security processes or errors in Kaspersky Embedded Systems Security operation.
Normal / threshold value	Varies / No.
Recommended reading interval	1 minute.
Recommendations for configuration if value exceeds the threshold	The values of this counter depend on the values set in Kaspersky Embedded Systems Security settings and the load on the computer from other applications' processes. Observe the average level of counter numbers over an extended period of time. If the general level of the counter values becomes lower, one of the following situations is possible: • Kaspersky Embedded Systems Security processes do not have enough processor time to process the objects. Make sure Kaspersky Embedded Systems Security receives additional processor time (by lowering other applications' load on the computer, for example). • Kaspersky Embedded Systems Security has experienced an error (several streams are idle). Restart Kaspersky Embedded Systems Security.

Kaspersky Embedded Systems Security SNMP counters and traps

This section contains information about Kaspersky Embedded Systems Security counters and traps.

In this section

About Kaspersky Embedded Systems Security SNMP counters and traps

If you have included SNMP Counters and Traps in the set of Anti-Virus components to be installed, you can view Kaspersky Embedded Systems Security counters and traps using Simple Network Management Protocol (SNMP).

To view Kaspersky Embedded Systems Security counters and traps from the administrator's workstation, start SNMP Service on the protected computer and start SNMP and SNMP Trap Services on the administrator's workstation.

Kaspersky Embedded Systems Security SNMP counters

This section contains tables with a description of the settings for Kaspersky Embedded Systems Security SNMP counters.

In this section

Performance counters

Table 71. Performance counters

Counter	Definition
currentRequestsAmount	Number of requests sent to be processed (on page 471)
currentInfectedQueueLength	Number of elements in the infected objects queue (see Section "Number of elements in infected objects queue" on page 473)
currentObjectProcessingRate	Number of objects processed per second (on page 474)
currentWorkProcessesNumber	Current number of working processes used by Kaspersky Embedded Systems Security

Quarantine counters

Table 72. Quarantine counters

Counter	Definition
totalObjects	Number of objects currently in Quarantine
totalSuspiciousObjects	Number of probably infected objects currently in Quarantine
currentStorageSize	Total size of data in Quarantine (MB)

Backup counter

Table 73. Backup counter

Counter	Definition
currentBackupStorageSize	Total size of data in Backup (MB)

General counters

Table 74. General counters

Counter	Definition
lastCriticalAreasScanAge	The period since the last complete scan of the computer's critical areas (time elapsed in seconds since the last *Critical Areas Scan task* was completed).
licenseExpirationDate	License expiration date If an active and additional keys have been added, the date of expiry of the license associated with the additional key is displayed.
currentApplicationUptime	The amount of time that Kaspersky Embedded Systems Security has been running since it was last started, in hundredths of seconds.
currentFileMonitorTaskStatus	Real-Time File Protection task status: **On** – running; **Off** – stopped or paused.

Update counter

Table 75. Update counter

Counter	Definition
avBasesAge	"Age" of databases (time elapsed in hundredths of seconds since the creation date of the latest updated databases installed).

Real-Time Protection counters

Table 76. Real-Time Protection counters

Counter	Definition
totalObjectsProcessed	Total number of objects scanned since the time the last Real-Time File Protection task was run
totalInfectedObjectsFound	Total number of infected and other objects detected since the time the last Real-Time File Protection task was run
totalSuspiciousObjectsFound	Total number of probably infected objects detected since the time the last Real-Time File Protection task was run
totalVirusesFound	Total number of objects detected since the time the Real-Time File Protection task was last run
totalObjectsQuarantined	Total number of infected, probably infected and other objects which were placed into Quarantine by Kaspersky Embedded Systems Security; calculated from the time the Real-Time File Protection task was last started
totalObjectsNotQuarantined	Total number of infected or probably infected objects Kaspersky Embedded Systems Security attempted to quarantine but was unable to do so; calculated from the time the Real-Time File Protection task was last started
totalObjectsDisinfected	Total number of infected objects which were disinfected by Kaspersky Embedded Systems Security; calculated from the time the Real-Time File Protection task was last started
totalObjectsNotDisinfected	Total number of infected and other objects which Kaspersky Embedded Systems Security attempted to disinfect but was unable to do so; calculated from the time Real-Time File Protection task was last started
totalObjectsDeleted	Total number of infected, probably infected and other objects which were disinfected by Kaspersky Embedded Systems Security; calculated from the time the Real-Time File Protection task was last started
totalObjectsNotDeleted	Total number of infected, probably infected and other objects which Kaspersky Embedded Systems Security attempted to disinfect but was unable to do so; calculated from the time Real-Time File Protection task was last started
totalObjectsBackedUp	Total number of infected objects and other which were placed into Backup by Kaspersky Embedded Systems Security; calculated from the time the Real-Time File Protection task was last started
totalObjectsNotBackedUp	Total number of infected objects and other which Kaspersky Embedded Systems Security attempted to place into Backup but was unable to do so; calculated from the time Real-Time File Protection task was last started

Kaspersky Embedded Systems Security SNMP traps

The options of SNMP traps in Kaspersky Embedded Systems Security are summarized as follows:

- eventThreatDetected: an object has been detected.

  The options of the trap are as follows:

  - eventDateAndTime
  - eventSeverity
  - computerName
  - userName
  - objectName
  - threatName
  - detectType
  - detectCertainty

- eventBackupStorageSizeExceeds: maximum Backup size exceeded.The total size of data in Backup has exceeded the value specified by the **Maximum Backup size (MB)**. Kaspersky Embedded Systems Security continues to back up infected objects.

  The options of the trap are as follows:

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventThresholdBackupStorageSizeExceeds: Backup free space threshold reached. The amount of free size in Backup assigned by the **Threshold value for space available (MB)** is equal to or less than the specified value. Kaspersky Embedded Systems Security continues to back up infected objects.

  The options of the trap are as follows:

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventQuarantineStorageSizeExceeds: maximum Quarantine size exceeded. The total size of data in Quarantine has exceeded the value specified by the **Maximum Quarantine size (MB)**. Kaspersky Embedded Systems Security continues to quarantine probably infected objects.

  The options of the trap are as follows:

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventObjectNotQuarantined: Quarantine error.

  The options of the trap are as follows:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - userName

    - computerName
    - objectName
    - storageObjectNotAddedEventReason
- eventObjectNotBackuped: Error of saving an object copy in the Backup.

  The options of the trap are as follows:

    - eventSeverity
    - eventDateAndTime
    - eventSource
    - objectName
    - userName
    - computerName
    - storageObjectNotAddedEventReason

- eventQuarantineInternalError: Quarantine internal error.

  The options of the trap are as follows:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - eventReason
- eventBackupInternalError: Backup error.

  The options of the trap are as follows:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - eventReason
- eventAVBasesOutdated: Anti-virus database is out of date. Number of days since the last execution of database update task (local task, or group task, or task for sets of computers) is being calculated.

  The options of the trap are as follows:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days
- eventAVBasesTotallyOutdated: Anti-virus database is obsolete. Number of days since the last execution of database update task (local task, or group task, or task for sets of computers) is being calculated.

  The options of the trap are as follows:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days
- eventApplicationStarted: Kaspersky Embedded Systems Security is running.

  The options of the trap are as follows:

  - eventSeverity
  - eventDateAndTime
  - eventSource

- eventApplicationShutdown: Kaspersky Embedded Systems Security is stopped.

  The options of the trap are as follows:

  - eventSeverity
  - eventDateAndTime
  - eventSource
- eventCriticalAreasScanWasntPerformForALongTime: Critical areas have not been scanned for a long time. Calculated as the number of days since the last completion of the Critical Areas Scan task.

  The options of the trap are as follows:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days
- eventLicenseHasExpired: License has expired.

  The options of the trap are as follows:

  - eventSeverity
  - eventDateAndTime
  - eventSource
- eventLicenseExpiresSoon: License expires soon. Calculated as the number of days until the expiration date for the license.

  The options of the trap are as follows:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days
- eventTaskInternalError: Task completion error.

  The options of the trap are as follows:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - errorCode
  - knowledgeBaseId
  - taskName

- eventUpdateError: Error of update task performance.

  The options of the trap are as follows:

  - eventSeverity
  - eventDateAndTime
  - taskName
  - updaterErrorEventReason

Descriptions of the traps options and their possible parameter values are as follows:

- eventDateAndTime: event date and time.
- eventSeverity: importance level.

  The option can take the following values:

  - critical (1) – critical
  - warning (2) – warning
  - info (3) – informational
- userName: a user name (for example, name of the user that attempted to gain access to an infected file).
- computerName: computer name (for example, name of the computer from which a user attempted to gain access to an infected file).
- eventSource: functional component where the event was generated.

  The option can take the following values:

  - unknown (0) – functional component not known
  - quarantine (1) – Quarantine
  - backup (2) – Backup
  - reporting (3) – task logs
  - updates (4) – Update
  - realTimeProtection (5) – Real-Time File Protection
  - onDemandScanning (6) – On-Demand Scan
  - product (7) – event related to operation of Kaspersky Embedded Systems Security as a whole rather than operation of individual components
  - systemAudit (8) – system audit log
- eventReason: event trigger: what provoked the event.

  The option can take the following values:

  - reasonUnknown(0) – reason is unknown
  - reasonInvalidSettings (1) – only for a Backup and Quarantine events, displayed if Quarantine or Backup is unavailable (insufficient access permissions or the folder is specified incorrectly in the Quarantine settings -- for example, a network path is specified). In this case, Kaspersky Embedded Systems Security will use the default Backup or Quarantine folder.
- objectName: an object name (for example, name of the file where the virus was detected).

- threatName: The name of the object according to the Virus Encyclopedia https://encyclopedia.kaspersky.com/knowledge/classification/ classification. This name is included in the full name of the detected object that Kaspersky Embedded Systems Security returns on detecting an object. You can view the full name of a detected object in the task log (see Section "Configuring log settings" on page 98).
- detectType: type of object detected.

  The option can take the following values:

  - undefined (0) – undefined
  - virware – classic viruses and network worms
  - trojware – Trojans
  - malware – other malicious programs
  - adware – advertising software
  - pornware – pornographic software
  - riskware – legitimate applications that may be used by intruders to damage the user's computer or personal data
- detectCertainty: certainty level for threat detection.

  The option can take the following values:

  - Suspicion (probably infected) – Kaspersky Embedded Systems Security has detected a partial match between a section of the object code and the known malicious code section.
  - Sure (infected) – Kaspersky Embedded Systems Security has detected a complete match between a section of the object code and the known malicious code section.
- days: number of days (for example, the number of days until the license expiration date).
- errorCode: an error code.
- knowledgeBaseId: address of a knowledge base article (for example, address of an article that explains a particular error).
- taskName: a task name.
- updaterErrorEventReason: a reason of the update error.

  The option can take the following values:

  - reasonUnknown(0) – reason is unknown
  - reasonAccessDenied – access denied
  - reasonUrlsExhausted – the list of update sources is exhausted
  - reasonInvalidConfig – invalid configuration file
  - reasonInvalidSignature – invalid signature
  - reasonCantCreateFolder – folder cannot be created
  - reasonFileOperError – file error
  - reasonDataCorrupted – object is corrupted
  - reasonConnectionReset – connection reset
  - reasonTimeOut – connection timeout exceeded

- reasonProxyAuthError – proxy authentication error
- reasonServerAuthError – server authentication error
- reasonHostNotFound – computer not found
- reasonServerBusy – server unavailable
- reasonConnectionError – connection error
- reasonModuleNotFound – object not found
- reasonBlstCheckFailed(16) – error checking the black list of keys. It is possible that databases updates were being published at the moment of update; please repeat the update in a few minutes.

- storageObjectNotAddedEventReason: the reason why the object was not backed up or quarantined.

  The option can take the following values:

  - reasonUnknown(0) – reason is unknown
  - reasonStorageInternalError – database error; Kaspersky Embedded Systems Security must be restored.
  - reasonStorageReadOnly – database is read-only; Kaspersky Embedded Systems Security must be restored.
  - reasonStorageIOError – input-output error: a) Kaspersky Embedded Systems Security is corrupted, Kaspersky Embedded Systems Security must be restored; b) disk with Kaspersky Embedded Systems Security files is corrupted.
  - reasonStorageCorrupted – storage is corrupted; Kaspersky Embedded Systems Security must be restored.
  - reasonStorageFull – database is full; free disk space is required.
  - reasonStorageOpenError – database file could not be opened; Kaspersky Embedded Systems Security must be restored.
  - reasonStorageOSFeatureError – some operating system features do not correspond to Kaspersky Embedded Systems Security requirements.
  - reasonObjectNotFound – object being placed to Quarantine does not exist on the disk.
  - reasonObjectAccessError – insufficient permissions to use Backup API: the account being used to perform the operation does not have Backup Operator permissions.
  - reasonDiskOutOfSpace – not enough space on the disk.

Integrating with WMI

Kaspersky Embedded Systems Security supports integration with Windows Management Instrumentation (WMI): you can use client systems that use WMI to receive data via the Web-Based Enterprise Management (WBEM) standard in order to gather information about the status of Kaspersky Embedded Systems Security and its components.

When Kaspersky Embedded Systems Security is installed, it registers proprietary module on the system, which facilitates the creation of a Kaspersky Embedded Systems Security namespace the WMI root namespace on the local computer. A Kaspersky Embedded Systems Security namespace lets you work with Kaspersky Embedded Systems Security classes and instances and their properties.

The values of some instance properties depend on task types.

Non-periodic task is an application task that is not limited in time and can either be constantly running or stopped. No execution progress exists for such tasks. The results of task execution are logged non-stop while the task is running as a single events (for example, detection of an infected object by any of Real-Time Computer Protection tasks). This type of tasks is managed via the Kaspersky Security Center policies.

Periodic task is an application task that is limited in time and has an execution progress displayed in percentage. The task results are generated upon the task completion and are represented as a single item or changed application state (for example, completed application database update, generated configuration files for the rule generation tasks). A number of periodic tasks of the same type can be running on a single computer simultaneously (three On-Demand scan tasks with different scan scopes). Periodic tasks can be managed via Kaspersky Security Center as group tasks.

If you use tools for generating WMI namespace queries and receiving dynamic data from WMI namespaces on your corporate network, you will be able to receive the information about the current application state (see the table below).

Table 77. Information about the application state

Instance property	Description	Values
ProductName	The name of the application installed.	Full name of application without version number.
ProductVersion	The full version of the application installed	Full application version number, including the build number.
InstalledPatches	The array of patch display names that are deployed for the application.	List of critical fixes installed for the application.
IsLicenseInstalled	The application activation state.	Status of the key used to activate the application. Possible values: • False - A key or activation code has not been set in the application. • True - A key or activation code has been added to the application.

Instance property	Description	Values
LicenseDaysLeft	Shows how many days are left before a current license expiration.	Number of days remaining before expiration of the current license. Possible non-positive values: • 0 - License has expired • -1 - Unable to get information on the current key or the specified key cannot be used to activate the application (for example, it is blocked based on a blacklist of keys).
AVBasesDatetime	The timestamp for a current anti-virus database version.	Date and time of the creation of the anti-virus databases currently in use. If the installed application does not use anti-virus databases, then the field has the value “Not installed”.
IsExploitPreventionEnabled	The Exploit Prevention component state.	Status of the Exploit Prevention component. Possible values: • True - The Exploit Prevention component is enabled and providing protection. • False - The Exploit Prevention component is not providing protection. For example: disabled, not installed, the License Agreement has been violated.
ProtectionTasksRunning	The array of protection tasks that are currently running.	List of protection, control, and monitoring tasks currently running. This field should account for all running non-periodic tasks. If not one non-periodic task is running, the field has the value “No”.
IsAppControlRunning	The Applications Launch Control task state.	Status of the Applications Launch Control task. • True - The Applications Launch Control task is currently running. • False - The Applications Launch Control is not currently running or the Applications Launch Control component is not installed.

Instance property	Description	Values
AppControlMode	The Applications Launch Control task mode.	Description of the current status of the Applications Launch Control component, and describes the selected mode for the corresponding task. Possible values: • Active - The **Active** mode is selected in the task settings. • Statistics Only - The **Statistics Only** mode is selected in the task settings. • Not installed - The Applications Launch Control component is not installed
AppControlRulesNumber	Total number of the applications launch control rules.	The number of rules currently specified in the Applications Launch Control task settings.
AppControlLastBlocking	The timestamp for the last application launch blocking by the Applications Launch Control task in any mode.	Date and time when the Applications Launch Control component last blocked the launch of an application. This field includes all blocked applications, regardless of the task mode. If no instances of blocked application launch are registered at the time the WMI query is processed, the field is assigned the value “No”.
PeriodicTasksRunning	The array of periodic tasks that are currently running.	List of On-Demand Scan, Update, and inventory-taking tasks currently running. This field should include all running periodic tasks. If no periodic tasks are currently running, then the field has the value “No”.
ConnectionState	The state of the connection between WMI Provider component and the Kaspersky Security Service (KAVFS).	Information about the status of the connection between the WMI Provider module and the Kaspersky Security Service. Possible values: • Success - The connection was successfully established: the WMI client can receive information about application status. • Failed. Error Code: <code> - The connection could not be established due to an error with the specified code.

This data represents instance properties KasperskySecurity_ProductInfo.ProductName=Kaspersky Embedded Systems Security, where:

- KasperskySecurity_ProductInfo is the name of the Kaspersky Embedded Systems Security class
- .ProductName=Kaspersky Embedded Systems Security is the Kaspersky Embedded Systems Security key parameter

The instance is created in the ROOT\Kaspersky\Security namespace.

Working with Kaspersky Embedded Systems Security from the command line

This section describes working with Kaspersky Embedded Systems Security from the command line.

In this chapter

Command line commands

You can perform basic Kaspersky Embedded Systems Security management commands from the command line of the protected computer if you included the Command line utility component into the list of installed features during installation of Kaspersky Embedded Systems Security.

Using command line commands you can manage only those functions which are accessible to you based on the permissions assigned to you in Kaspersky Embedded Systems Security.

Certain Kaspersky Embedded Systems Security commands are executed in the following modes:

- Synchronous mode: management returns to the Console only after command execution is complete.
- Asynchronous mode: management returns to the Console immediately after the command is run.

► *To interrupt command execution in synchronous mode*

press the **Ctrl+C** keyboard shortcut.

Follow the following rules when entering Kaspersky Embedded Systems Security commands:

- Enter modifiers and commands using upper and lower case.
- Delimit modifiers with the space character.
- if the file/folder name whose path you specify as the key value contains a space, specify the file/folder path in quotes, for example: `"C:\TEST\test cpp.exe"`
- if necessary, use placeholders in the filename or path masks, for example: “`C:\Temp\Temp*\`”, “`C:\Temp\Temp???.doc`”, “`C:\Temp\Temp*.doc`”

You can use the command line for the entire range of operations required for management and administration of Kaspersky Embedded Systems Security (see the table below).

Table 78. Kaspersky Embedded Systems Security commands

Command	Description
KAVSHELL APPCONTROL (see Section "Filling list of Applications Launch Control rules KAVSHELL APPCONTROL" on page 503)	Renews the specified rules list according to selected adding principle.
KAVSHELL APPCONTROL /CONFIG (see Section "Managing the Applications Launch Control task KAVSHELL APPCONTROL /CONFIG" on page 500)	Controls the operating mode of the Applications Launch Control task
KAVSHELL APPCONTROL /GENERATE (see Section "Rule Generator for Applications Launch Control KAVSHELL APPCONTROL /GENERATE" on page 501)	Starts the Rule Generator for Applications Launch Control task.
KAVSHELL VACUUM (see Section "Kaspersky Embedded Systems Security log files defragmentation. KAVSHELL VACUUM" on page 510)	Defragments Kaspersky Embedded Systems Security log files.
KAVSHELL PASSWORD	Manages password protection settings.
KAVSHELL HELP (see Section "Displaying Kaspersky Embedded Systems Security command help. KAVSHELL HELP" on page 491)	Displays Kaspersky Embedded Systems Security command help.
KAVSHELL START (see Section "Starting and stopping Kaspersky Security service KAVSHELL START, KAVSHELL STOP" on page 491)	Starts Kaspersky Embedded Systems Security service.
KAVSHELL STOP (see Section "Starting and stopping Kaspersky Security service KAVSHELL START, KAVSHELL STOP" on page 491)	Stops Kaspersky Embedded Systems Security service.
KAVSHELL SCAN (see Section "Scanning selected area.	Creates and starts a temporary On-Demand Scan task with the scan scope and security settings set by the command modifiers.

Command	Description
KAVSHELL SCAN" on page 492)	
KAVSHELL SCANCRITICAL (see Section "Starting the Critical Areas Scan task. KAVSHELL SCANCRITICAL" on page 495)	Starts the Critical Areas Scan system task.
KAVSHELL TASK (see Section "Managing specified task asynchronously. KAVSHELL TASK" on page 496)	Starts, pauses / resumes, stops the selected task asynchronously, returns the current task status / statistics.
KAVSHELL RTP (see Section "Starting and stopping Real-Time Protection tasks. KAVSHELL RTP" on page 499)	Starts or stops all Real-Time Protection tasks.
KAVSHELL UPDATE (see Section "Starting Kaspersky Embedded Systems Security databases update task. KAVSHELL UPDATE" on page 505)	Starts Kaspersky Embedded Systems Security bases update task with the settings specified using command modifiers.
KAVSHELL ROLLBACK (see Section "Rolling back Kaspersky Embedded Systems Security database updates. KAVSHELL ROLLBACK" on page 508)	Rolls back bases to the previous version.
KAVSHELL LICENSE	Adds or deletes the keys. Displays information about the added keys.
KAVSHELL TRACE (see Section "Enabling, configuring and disabling trace log. KAVSHELL TRACE" on page 509)	Enables or disables the trace log, manages settings of the trace log.
KAVSHELL DUMP (see Section "Enabling and disabling dump file creation. KAVSHELL DUMP" on page 512)	Enables or disables Kaspersky Embedded Systems Security process dump files in case of abnormal termination of processes.
KAVSHELL IMPORT (see Section "Importing settings. KAVSHELL IMPORT" on page 513)	Imports general Kaspersky Embedded Systems Security settings, functions, and tasks from a configuration file created beforehand.
KAVSHELL EXPORT (see Section "Exporting settings. KAVSHELL EXPORT" on page 514)	Exports all Kaspersky Embedded Systems Security settings and existing tasks to a configuration file.

Command	Description
KAVSHELL DEVCONTROL (see Section "Filling the list of Device Control rules. KAVSHELL DEVCONTROL" on page 504)	Adds to the list of generated device control rules according to selected method.

Displaying Kaspersky Embedded Systems Security command help. KAVSHELL HELP

To obtain the list of all Kaspersky Embedded Systems Security commands, run one of the following commands:

```
KAVSHELL
```

```
KAVSHELL HELP
```

```
KAVSHELL /?
```

To obtain a description of a command and its syntax, run one of the following commands:

```
KAVSHELL HELP <command>
```

```
KAVSHELL <command> /?
```

KAVSHELL HELP command examples

To view detailed information about the KAVSHELL SCAN command, execute the following command:

```
KAVSHELL HELP SCAN
```

Starting and stopping Kaspersky Security service KAVSHELL START, KAVSHELL STOP

To run the Kaspersky Security Service, execute the command

```
KAVSHELL START
```

By default when Kaspersky Security Service is started, tasks Real-Time File Protection and Scan at system startup as well as other tasks that are scheduled to start **At application launch** will be started.

To stop the Kaspersky Security Service, execute command

```
KAVSHELL STOP
```

Password might be required to execute the command. To enter the current password use `[/pwd:<password>]` key.

Scanning selected area. KAVSHELL SCAN

In order to start a task for scanning specific areas of the protected computer use command `KAVSHELL SCAN`. The command modifiers specify the scan scope and security settings of the selected node.

The On-Demand Scan task started using `KAVSHELL SCAN` command is a temporary task. It is displayed in the Application Console only while being executed (you cannot view task settings in the Application Console). The task performance log is generated at the same time. It is displayed in the **Task logs** of the Application Console.

When specifying paths in scan tasks for specific areas, you can use environmental variables. If you use environmental variable specified for user, execute `KAVSHELL SCAN` command with the permissions for this user.

Command `KAVSHELL SCAN` is executed in the synchronous mode.

To start an existing On-Demand Scan task from the command line, use the KAVSHELL TASK (see Section "Managing specified task asynchronously. KAVSHELL TASK" on page 496) command.

KAVSHELL SCAN command syntax

```
KAVSHELL SCAN <scan scope>
[/MEMORY|/SHARED|/STARTUP|/REMDRIVES|/FIXDRIVES|/MYCOMP] [/L:< path to file
with the list of scan scopes >] [/F<A|C|E>] [/NEWONLY]
[/AI:<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>]
[/AS:<QUARANTINE|DELETE|REPORT|AUTO>] [/DISINFECT|/DELETE] [/E:<ABMSPO>]
[/EM:<”masks”>] [/ES:<size>] [/ET:<number of seconds>] [/TZOFF]
[/OF:<SKIP|RESIDENT|SCAN[=<days>] [NORECALL]>]
[/NOICHECKER][/NOISWIFT][/ANALYZERLEVEL][/NOCHECKMSSIGN][/W:<path to task log
file>] [/ANSI] [/ALIAS:<task alias>]
```

The KAVSHELL SCAN command has both mandatory and optional keys (see table below).

KAVSHELL SCAN command examples

```
KAVSHELL SCAN Folder56 D:\Folder1\Folder2\Folder3\ C:\Folder1\
C:\Folder2\3.exe “\\another server\Shared\” F:\123\*.fgb /SHARED
/AI:DISINFDEL /AS:QUARANTINE /FA /E:ABM /EM:”*.xtx;*.fff;*.ggg;*.bbb;*.info”
/NOICHECKER /ANALYZERLEVEL:1 /NOISWIFT /W:log.log
```

```
KAVSHELL SCAN /L:scan_objects.lst /W:c:\log.log
```

Table 79. KAVSHELL SCAN command modifiers

Key	Description
Scan scope. Mandatory modifier.	
<files>	Specifies the scan scope - list of files, folders, network paths and predefined areas. Specify network paths to the UNC format (Universal Naming Convention). In the following example folder Folder4 is specified without a path - it is located in the folder from which you run KAVSHELL command: KAVSHELL SCAN Folder4 If the name of the object to be checked contains spaces, it must be placed in quotation marks.
<folders>	
<network path>	

Key	Description
	When a folder is selected, Kaspersky Embedded Systems Security will also check all subfolders for the folder in question. The symbols * or ? can be used to scan a group of files.
/MEMORY	Scan objects in RAM
/SHARED	Scan shared folders on the computer
/STARTUP	Scan autorun objects
/REMDRIVES	Scan removable drives
/FIXDRIVES	Scan hard drives
/MYCOMP	Scan all areas of protected computer
/L:<path to file with the list of scan scopes>	File name with the list of scan scopes including full path to the file. Delimit scan scopes in the files using line breaks. You can specify predefined scan areas as shown as follows in this example of a file with a scan scope list: C:\ D:\Docs\*.doc E:\My Documents /STARTUP /SHARED
Scanned objects (File types). If you do not specify values for this modifier, Kaspersky Embedded Systems Security will scan objects by their format.	
/FA	Scan all objects
/FC	Scan objects by format (by default). Kaspersky Embedded Systems Security scans only objects format of which are included into the list of formats of infectable objects.
/FE	Scan objects by extension. Kaspersky Embedded Systems Security scans only objects with extensions included into the list of extensions of infectable objects.
/NEWONLY	Scan only new and modified files. If you do not provide this modifier, Kaspersky Embedded Systems Security will scan all objects.
Action to perform on infected and other objects. If you do not specify values for this modifier, Kaspersky Embedded Systems Security will perform the **Skip** action.	
DISINFECT	Disinfect, skip if disinfection is not possible The settings DISINFECT and DELETE are saved in the current version of Kaspersky Embedded Systems Security in order to ensure compatibility with previous versions. These settings can be used instead of the key commands /AI: and /AS: In this case, Kaspersky Embedded Systems Security will not process probably infected objects.
DISINFDEL	Disinfect, delete if disinfection is not possible
DELETE	Delete The settings DISINFECT and DELETE are saved in the current version of Kaspersky Embedded Systems Security in order to ensure compatibility with

Key	Description
	previous versions. These settings can be used instead of the key commands /AI: and /AS: In this case, Kaspersky Embedded Systems Security will not process probably infected objects.
REPORT	Send report (by default)
AUTO	Perform recommended action
/AS: **Action to perform on probably infected objects**/ If you do not specify values for this modifier, Kaspersky Embedded Systems Security will perform the **Skip** action.	
QUARANTINE	Quarantine
DELETE	Delete
REPORT	Send report (by default)
AUTO	Perform recommended action
Exclusions	
/E:ABMSPO	Excludes compound objects of the following types: A – archives (scan SFX archives only) B – email databases M – plain mail S – archives and SFX-archives P – packed objects O – embedded OLE objects
/EM:<″masks″>	Exclude files by mask You can specify several masks, for example: EM:″*.txt; *.png; C\Videos\*.avi″.
/ET:<number of seconds>	Stop processing object if it continues longer than the number of seconds specified by value <number of seconds>. There is no time restriction by default.
/ES:<size>	Do not scan compound objects larger than the size (in MB) specified by value <size>. Kaspersky Embedded Systems Security scans all sizes of objects by default.
/TZOFF	Disable Trusted Zone exclusions
Advanced settings (Options)	
/NOICHECKER	Disable the use of iChecker (enabled by default)
/NOISWIFT	Disable the use of iSwift (enabled by default)
/ANALYZERLEVEL:<analysis intensity>	Enable Heuristic Analyzer, configure analysis level. The following heuristic analysis levels are available: 1 – light 2 – medium 3 – deep If you omit the modifier, Kaspersky Embedded Systems Security will not use heuristic analyzer.

Key	Description
/ALIAS:<task alias>	Enables you to assign an On-Demand Scan task a temporary name by which the task can be accessed during its execution, for example in order to view its statistics using TASK command. The task alias must be unique among the task aliases of all functional components of Kaspersky Embedded Systems Security. If this modifier is not specified, temporary name scan_<kavshell_pid> is used, for example scan_1234. In the Application Console, the task is assigned the name Scan objects (<date and time>), for example, Scan objects 8/16/2007 5:13:14 PM.
Settings of task logs (Report settings)	
/W:<path to task log file>	If this key is specified, Kaspersky Embedded Systems Security will save the task log file with the name defined by the key's value. The log file contains task execution statistics, the time when it was started and completed (stopped), and information about events in this task. The log is used to register events defined by the settings of task logs and the Kaspersky Embedded Systems Security event log in the Event Viewer. Either the absolute or relative path to the log file can be specified. If you specify only the name of a file without specifying the respective path, the log file will be created in the current folder. Restarting the command with the same log settings will overwrite the existing log file. The log file can be viewed while a task is running. The log appears in the Task logs node of the Application Console. If Kaspersky Embedded Systems Security fails to create the log file, it will not stop the command from executing but it will display an error message.
/ANSI	The option enables recording of events to task log in the ANSI encoding. The ANSI option will not be applied, if the W option is not defined. If the ANSI option is not specified, task log is generated using the UNICODE encoding.

Starting the Critical Areas Scan task. KAVSHELL SCANCRITICAL

Use the `KAVSHELL SCANCRITICAL` command to start the system On-Demand Scan task Critical Areas Scan with the settings defined in the Application Console.

KAVSHELL SCANCRITICAL command syntax

```
KAVSHELL SCANCRITICAL [/W:<path to task log file>]
```

KAVSHELL SCANCRITICAL command examples

To run the Critical Areas Scan On-Demand Scan task, and save the task log scancritical.log in the current folder, execute the following command:

```
KAVSHELL SCANCRITICAL /W:scancritical.log
```

Depending upon the syntax of the /W modifier, you can configure the location of the task log (see the table below).

Table 80. Syntax of the /W modifier for the KAVSHELL SCANCRITICAL command

Key	Description
/W:<path to task log file>	If this key is specified, Kaspersky Embedded Systems Security will save the task log file with the name defined by the key's value. The log file contains task execution statistics, the time when it was started and completed (stopped), and information about events in this task. The log is used to register events defined by the settings of task logs and the Application Event Log in the Event Viewer. Either the absolute or relative path to the log file can be specified. If you specify only the name of a file without specifying the respective path, the log file will be created in the current folder. Restarting the command with the same log settings will overwrite the existing log file. The log file can be viewed while a task is running. The log appears in the **Task logs** node of the Application Console. If Kaspersky Embedded Systems Security fails to create the log file, it will not stop the command from executing but it will display an error message.

Managing specified task asynchronously. KAVSHELL TASK

Using `KAVSHELL TASK` command you can manage the specified task: run, pause, resume and stop the specified task and view the current task status and statistics. The command is performed in asynchronous mode.

Password might be required to execute the command. To enter the current password use `[/pwd:<password>]` key.

KAVSHELL TASK command syntax

```
KAVSHELL TASK [<task name alias> </START | /STOP | /PAUSE | /RESUME | /STATE
| /STATISTICS >]
```

KAVSHELL TASK command examples

```
KAVSHELL TASK
```

```
KAVSHELL TASK on-access /START
```

```
KAVSHELL TASK user-task_1 /STOP
```

```
KAVSHELL TASK scan-computer /STATE
```

`KAVSHELL TASK` command can run without modifiers or with one/several modifiers (see the table below).

Table 81. KAVSHELL TASK command modifiers

Key	Description
Without keys	Returns the list of all existing Kaspersky Embedded Systems Security tasks The list contains the fields: alternative task name, task category (system or custom) and current task status.
<task alias>	Instead of the task name, in the SCAN TASK command, use its Task alias, an additional short-form name that Kaspersky Embedded Systems Security assigns to tasks. To view Kaspersky Embedded Systems Security task aliases enter the command KAVSHELL TASK without any modifiers
/START	Starts the specified task in asynchronous mode.
/STOP	Stops the specified task.
/PAUSE	Pauses the specified task.
/RESUME	Resumes the specified task in asynchronous mode.
/STATE	Returns the current task status (for example, *Running*, *Completed*, *Paused*, *Stopped*, *Failed*, *Starting*, *Recovering*).
/STATISTICS	Retrieve task statistics - information on the number of objects processed from the time the task started until now.

Note that not all Kaspersky Embedded Systems Security tasks fully support these keys.

Return codes for the KAVSHELL TASK command (see Section "Return codes for KAVSHELL TASK command" on page 517).

Registering KAVFS as a system protected process. KAVSHELL CONFIG

The `KAVSHELL CONFIG` command allows you to control the registration of the Kaspersky Security Service as a system protected process (Protected Process Light) using the ELAM driver, installed in the operating system during the application installation.

KAVSHELL CONFIG command syntax

```
KAVSHELL CONFIG /PPL:<ON|OFF>
```

Table 82. KAVSHELL CONFIG command keys

Key	Description
/PPL:ON	Register Kaspersky Security Service as PPL.
/PPL:OFF	Remove PPL attribute for Kaspersky Security Service.

The application performs the service unregistration automatically when any of the following actions are taken:

- application uninstallation
- application upgrade
- patch installation
- application components repair

Return codes for KAVSHELL CONFIG command.

Starting and stopping Real-Time Protection tasks. KAVSHELL RTP

Using the `KAVSHELL RTP` command you can start or stop all Real-Time Protection tasks.

> Password might be required to execute the command. To enter the current password use `[/pwd:<password>]` key.

KAVSHELL RTP command syntax

```
KAVSHELL RTP {/START | /STOP}
```

KAVSHELL RTP command examples

To start all Real-Time Protection tasks, execute the following command:

```
KAVSHELL RTP /START
```

The KAVSHELL RTP command can include any of two mandatory modifiers (see the table below).

Table 83. KAVSHELL RTP command modifiers

Key	Description
/START	Starts all Real-Time Protection tasks: Real-Time File Protection, and KSN Usage.
/STOP	Stops all Real-Time Protection tasks.

Managing the Applications Launch Control task KAVSHELL APPCONTROL /CONFIG

You can use the KAVSHELL APPCONTROL /CONFIG command to configure the mode in which the Applications Launch Control task runs and monitors the loading of DLL modules.

KAVSHELL APPCONTROL /CONFIG command syntax

```
 /config /mode:<applyrules|statistics> [/dll:<no|yes>] | /config
/savetofile:<full path to XML file>
```

KAVSHELL APPCONTROL /CONFIG command examples

► *To run the Applications Launch Control task in* ***Active*** *mode without loading a DLL and save the task settings upon completion, run the following command:*

```
KAVSHELL APPCONTROL /CONFIG /mode:applyrules /dll:<no>
/savetofile:c:\appcontrol\config.xml
```

You can configure Applications Launch Control task settings using the command-line parameters (see the table below).

Table 84. KAVSHELL APPCONTROL /GENERATE command switches

Key	Description
/mode:<applyrules|statistics>	Operating mode of the Applications Launch Control task. You can select one of the following modes: • active - Apply Applications Launch Control rules; • statistics - Only statistics.
/dll:<no|yes>	Enable or disable monitoring of DLL loading.
/savetofile: <path to XML file>	Export specified rules in the indicated file in XML format.
/savetofile: <the fullname to xml file>	Save the list of rules to file.
/savetofile: <the fullname to xml file> /sdc	Save the list of Software Distribution Control rules to file.
/clearsdc	Delete all Software Distribution Control rules from the list.

Rule Generator for Applications Launch Control KAVSHELL APPCONTROL /GENERATE

Using the `KAVSHELL APPCONTROL /GENERATE` command you can generate the Applications Launch Control rules lists.

> Password might be required to execute the command. To enter the current password use `[/pwd:<password>]` key.

KAVSHELL APPCONTROL /GENERATE command syntax

```
KAVSHELL APPCONTROL /GENERATE <path to folder> | /source:<path to file with
folders list> [/masks:<edsms>] [/runapp] [/rules:<ch|cp|h>] [/strong]
[/user:<user or group of users>] [/export:<path to XML file>]
[/import:<a|r|m>] [/prefix:<prefix for rules names>] [/unique]
```

KAVSHELL APPCONTROL /GENERATE command examples

► *To generate rules for files from specified folders, execute the following command:*

```
KAVSHELL APPCONTROL /GENERATE /source:c\folderslist.txt
/export:c:\rules\appctrlrules.xml
```

► *To generate rules for executable files of all extensions available in the specified folder and, upon the task completion, save generated rules in the specified file XML file, execute the following command:*

```
KAVSHELL APPCONTROL /GENERATE c:\folder /masks:edms
/export:c\rules\appctrlrules.xml
```

Depending on keys syntax you can configure automatic rules generation settings for the Applications Launch Control task (see table below).

Table 85. KAVSHELL APPCONTROL /GENERATE command keys

Key	Description
Allowing rules usage scope	
<path to folder>	Specifies path to folder with executable files that require automatically generated allowing rules.
/source: <path to file with folders list>	Specifies path to TXT file with list of folders containing executable files that require automatically generated allowing rules.

Key	Description
/masks: <edms>	Specifies extensions of executable files that require automatically generated allowing rules. You can include into rules usage scope files of following extensions: • e - EXE files • d - DLL files • m - MSI files • s - scripts
/runapp	When generation allowing rules, takes into account applications running on a protected computer at the moment of the task performing.
Actions when automatically generating allowing rules	
/rules: <ch|cp|h>	Specifies actions to perform during the Applications Launch Control allowing rules generation: • ch - use digital certificate. If the certificate is missing, use SHA256 hash. • cp - use digital certificate. If the certificate is missing, use the path to executable file. • h - use SHA256 hash.
/strong	Use digital certificate subject and thumbprint while automatically generating the Applications Launch Control allowing rules. The command is executed if the /rules: <ch|cp> key is specified.
/user: <user or group of users>	Specifies user name or a group of users for which the rules will be applied. The application will monitor any applications run by the specified user and / or group of users.
Actions on completion of Rule Generator for Applications Launch Control	
/export: <path to XML file>	Saves generated rules into XML file.
/unique	Add information about the computer with applications installed that are the base for the Applications Launch Control allowing rules generation.
/prefix: <prefix for rules names>	Specifies name prefix for the generating applications launches control allowing rules.
/import: <a|r|m>	Imports generated rules to the list of specified applications launch control rules according to the selected adding principle: • a - **Add to existing rules** (rules with identical settings are duplicated) • r - **Replace existing rules** (rules with identical parameters are not added; the rule is added if at least one rule parameter is unique) • m - **Merge with existing rules** (rules with identical parameters are not added; the rule is added if at least one rule parameter is unique)

Filling list of Applications Launch Control rules KAVSHELL APPCONTROL

Using the `KAVSHELL APPCONTROL` you can add rules from the XML file to the Applications Launch Control task rules list according to the selected principle and also delete all set rules from the list.

> Password might be required to execute the command. To enter the current password use `[/pwd:<password>]` key.

KAVSHELL APPCONTROL command syntax

```
KAVSHELL APPCONTROL /append <path to XML file> | /replace <path to XML file>
| /merge <path to XML file> | /clear
```

KAVSHELL APPCONTROL command examples

► *To add rules from an XML file to already specified rules for the Applications Launch Control task according to Add to existing rules principle, execute the following command:*

```
KAVSHELL APPCONTROL /append c:\rules\appctrlrules.xml
```

Depending on the keys syntax, you can select principle to add new rules an XML file specified to a list of the Applications Launch Control defined rules (see table below).

Table 86. KAVSHELL APPCONTROL command keys

Key	Description
/append <path to XML file>	Renew list of applications launches control rules based on a specified XML file. Adding principle - **Add to existing rules** (rules with identical settings are duplicated).
/replace <path to XML file>	Renew list of applications launches control rules based on a specified XML file. Adding principle - **Replace existing rules** (rules with identical parameters are not added; the rule is added if at least one rule parameter is unique).
/merge <path to XML file>	Renew list of applications launches control rules based on a specified XML file. Adding principle - **Merge with existing rules** (new rules do not duplicate already set rules).
/clear	Clear the list of Applications Launch Control rules.

Filling the list of Device Control rules. KAVSHELL DEVCONTROL

Using `KAVSHELL DEVCONTROL` you can add rules from the XML file to the Device Control task rules list according to the selected principle and also delete all set rules from the list.

> Password might be required to execute the command. To enter the current password use `[/pwd:<password>]` key.

KAVSHELL DEVCONTROL command syntax

```
KAVSHELL DEVCONTROL /append <path to XML file> | /replace <path to XML file>
| /merge <path to XML file> | /clear
```

KAVSHELL DEVCONTROL command examples

► *To add rules from an XML file to already specified rules for the Device Control task according to **Add to existing rules** principle, execute the following command:*

```
KAVSHELL DEVCONTROL /append :c:\rules\devctrlrules.xml
```

Depending on the keys syntax, you can select principle to add new rules an XML file specified to a list of the Device Control defined rules (see table below).

Table 87. KAVSHELL DEVCONTROL command keys

Key	Description
/append <path to XML file>	Renew list of device control rules based on a specified XML file. Adding principle - **Add to existing rules** (rules with identical settings are duplicated).
/replace <path to XML file>	Renew list of device control rules based on a specified XML file. Adding principle - **Replace existing rules** (rules with identical parameters are not added; the rule is added if at least one rule parameter is unique).
/merge <path to XML file>	Renew list of device control rules based on a specified XML file. Adding principle - **Merge with existing rules** (new rules do not duplicate already set rules).
/clear	Clear the list of Device Control rules.

Starting Kaspersky Embedded Systems Security databases update task. KAVSHELL UPDATE

The `KAVSHELL UPDATE` command can be used to start the Kaspersky Embedded Systems Security databases update command in the synchronous mode.

The Kaspersky Embedded Systems Security databases update task, run using a `KAVSHELL UPDATE` command, is a temporary task. It is only displayed in the Application Console while being executed. The task log is generated at the same time. It is displayed in the **Task logs** of the Application Console. Kaspersky Security Center policies may apply to update tasks created and started using the `KAVSHELL UPDATE` command and update tasks created in the Application Console. For information about managing Kaspersky Embedded Systems Security on computers using Kaspersky Security Center, refer to the section "Managing Kaspersky Embedded Systems Security using Kaspersky Security Center".

Environment variables can be used when specifying the path to updates source in this task. If a user's environment variables are used, execute the `KAVSHELL UPDATE` command with the permissions for this user.

KAVSHELL UPDATE command syntax

```
KAVSHELL UPDATE < Path to updates source | /AK | /KL> [/NOUSEKL]
[/PROXY:<address>:<port>] [/AUTHTYPE:<0-2>] [/PROXYUSER:<user name>]
[/PROXYPWD:<password>] [/NOPROXYFORKL] [/USEPROXYFORCUSTOM] [/NOFTPPASSIVE]
[/TIMEOUT:<seconds>] [/REG:<iso3166 code>] [/W:<path to task log file>]
[/ALIAS:<task alias>]
```

The KAVSHELL UPDATE command has both mandatory and optional keys (see the following table).

KAVSHELL UPDATE command examples

► *To start a custom database update task, execute the following command:*

```
KAVSHELL UPDATE
```

► *To run the database update task using the update files in the \\server\databases network folder, run the following command:*

```
KAVSHELL UPDATE \\server\databases
```

► *To start an update task from the FTP server ftp://dnl-ru1.kaspersky-labs.com/ and write all task events to the c:\update_report.log file, execute the command:*

```
KAVSHELL UPDATE ftp://dnl-ru1.kaspersky-labs.com /W:c:\update_report.log
```

► *To download Kaspersky Embedded Systems Security database updates from Kaspersky Lab's update server, connect to the updates source through a proxy server (proxy server address: proxy.company.com, port: 8080). To access the computer using the in-built Microsoft Windows NTLM authentication with user name: inetuser, password: 123456, execute the following command:*

```
KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1
/PROXYUSER:inetuser /PROXYPWD:123456
```

Table 88. KAVSHELL UPDATE command keys

Key	Description
Updates source (mandatory key). Specify one or multiple sources. Kaspersky Embedded Systems Security will access the sources in the order in which they are listed. Delimit sources with a space.	
<path in UNC format>	User-defined update source. Path to network update folder in the UNC format.
<URL>	User-defined updates source. HTTP or FTP server address where update folder is located.
<Local folder>	User-defined updates source. Folder on the protected computer.
/AK	Kaspersky Security Center Administration server as the updates source.
/KL	Kaspersky Lab's update servers as the updates sources.
/NOUSEKL	Do not use Kaspersky Lab's update servers if other updates sources are not available (used by default).
Proxy server settings	
/PROXY:<address>:<port>	Network name or IP address of the proxy server and its port. If this key is not specified, Kaspersky Embedded Systems Security will automatically detect the settings of the proxy server used in the local area network.
/AUTHTYPE:<0-2>	This key specifies the authentication method to access proxy server. It can have the following values: **0** – in-built Microsoft Windows NTLM-authentication; Kaspersky Embedded Systems Security will contact the proxy server under the **Local system** (**SYSTEM**) account **1** – in-built Microsoft Windows NTLM-authentication; Kaspersky Embedded Systems Security will contact the proxy server under account with login name and password specified by the keys /PROXYUSER and /PROXYPWD **2** – authentication by login name and password specified by keys /PROXYUSER and /PROXYPWD (basic authentication) If authentication is not required for accessing the proxy server, there is no requirement to specify a key.
/PROXYUSER:<user name>	User name which will be used for accessing proxy server. If the value of key /AUTHTYPE:0 is specified, then /PROXYUSER:<user name> and /PROXYPWD:<password> keys will be ignored.
/PROXYPWD:<password>	User password which will be used for accessing proxy server. If the value of key /AUTHTYPE:0 is specified, then /PROXYUSER:<user name> and /PROXYPWD:<password> keys will be ignored. If /PROXYUSER key is specified and /PROXYPWD omitted, the password will be considered blank.
/NOPROXYFORKL	Do not use proxy server settings for connecting with Kaspersky Lab's update servers (used by default).
/USEPROXYFORCUSTOM	Use proxy server settings for connecting to user-defined updates sources (not used by default).
/USEPROXYFORLOCAL	Use proxy server settings for connecting to local updates sources. If not specified, the value **Do not use proxy server for local addresses** will apply.
General FTP and HTTP server settings	

Key	Description
/NOFTPPASSIVE	If this key is specified, Kaspersky Embedded Systems Security will use the active FTP server mode to connect to the protected computer. If this key is not specified, Kaspersky Embedded Systems Security will use the passive FTP server mode, if possible.
/TIMEOUT:<number of seconds>	FTP or HTTP server connection timeout. If you do not specify this key,Kaspersky Embedded Systems Security will use the default value: 10 sec. The key value must be a whole number.
/REG:<iso3166 code>	Regional settings. This key is used when receiving updates from Kaspersky Lab's update servers. Kaspersky Embedded Systems Security optimizes the update load on the protected computer by selecting the update server nearest to it. As the value of this key, specify the letter code of the location country for the protected computer in accordance with ISO 3166-1, for example /REG: gr or /REG:RU. If this key is omitted or a non-existent country code is specified, Kaspersky Embedded Systems Security will detect the location of the protected computer based on the regional settings on the computer where the Application Console is installed.
/ALIAS:<task alias>	This key will allow you to assign a temporary name to the task, to be used to access the task during its execution. For example, task statistics can be viewed using the TASK command. The task alias must be unique among the task aliases of all functional components of Kaspersky Embedded Systems Security. If this key is not specified, temporary name update_<kavshell_pid> is used; for example, update_1234. In the Application Console, the task is assigned the name Update-databases (<date time>); for example, Update-databases 8/16/2007 5:41:02 PM.
/W:<path to task log file>	If this key is specified, Kaspersky Embedded Systems Security will save the task log file with the name defined by the key's value. The log file contains task execution statistics, the time when it was started and completed (stopped), and information about events in this task. The log is used to register events defined by the settings of task logs and the Kaspersky Embedded Systems Security event log in the "Event Viewer". Either the absolute or relative path to the log file can be specified. If only the file name is specified without its path, then the log file will be created in the current folder. Restarting the command with the same log settings will overwrite the existing log file. The log file can be viewed while a task is running. The log appears in the **Task logs** node of the Application Console. If Kaspersky Embedded Systems Security fails to create the log file, it does not stop the command from executing or display an error message.

Return codes for KAVSHELL UPDATE command (on page 518).

Rolling back Kaspersky Embedded Systems Security database updates. KAVSHELL ROLLBACK

The `KAVSHELL ROLLBACK` command can be used to perform a Kaspersky Embedded Systems Security database rollback system task (roll back Kaspersky Embedded Systems Security databases to the previously installed version). The command is performed synchronously.

Command syntax:

```
KAVSHELL ROLLBACK
```

Return codes for the KAVSHELL ROLLBACK command (on page 518).

Managing log inspection. KAVSHELL TASK LOG-INSPECTOR

The `KAVSHELL TASK LOG-INSPECTOR` command can be used to monitor the environment integrity based on the Windows Event Log analysis.

Command syntax

```
KAVSHELL TASK LOG-INSPECTOR
```

Command examples

```
KAVSHELL TASK LOG-INSPECTOR /stop
```

Table 89. KAVSHELL TASK LOG-INSPECTOR command modifiers

Key	Description
/START	Starts the specified task in asynchronous mode.
/STOP	Stops the specified task.
/STATE	Returns the current task status (for example, *Running*, *Completed*, *Paused*, *Stopped*, *Failed*, *Starting*, *Recovering*).
/STATISTICS	Retrieve task statistics - information on the number of objects processed from the time the task started until now.

Return codes for the KAVSHELL TASK LOG-INSPECTOR command (see Section "Return codes for KAVSHELL TASK LOG-INSPECTOR command" on page 516).

Enabling, configuring and disabling trace log. KAVSHELL TRACE

The `KAVSHELL TRACE` command can be used to enable and disable the trace log for all Kaspersky Embedded Systems Security subsystems and to set the log detail level.

Kaspersky Embedded Systems Security writes information to trace files and the dump file in unencrypted form.

KAVSHELL TRACE command syntax

```
KAVSHELL TRACE </ON /F:<path to trace log file folder> [/S:<maximum log size
in megabytes>] [/LVL:debug|info|warning|error|critical] | /OFF>
```

If the trace log is maintained and you wish to change its settings, enter `KAVSHELL TRACE` command with /ON key and specify trace log settings with values of /S and /LVL keys (see table below).

Table 90. KAVSHELL TRACE command keys

Key	Description
/ON	Enables the trace log.
/F:<folder with trace log files>	This key specifies the full path to the folder to which the trace log files will be saved (required). If a path to a non-existent folder is specified, no trace log will be created. Paths to folders on the network drives of other computers cannot be specified. If a space character is contained in the name of the folder to which you specify the path as the value of the key, put the path to this folder into quotes, for example: /F:"C\Trace Folder". System environment variables can be used when specifying the path to the trace log files; user environment variables are not allowed.
/S: <maximum log file size in megabytes>	This key sets the maximum size of a single trace log file. As soon as the log file reaches the maximum level, Kaspersky Embedded Systems Security will start recording information into a new file; the previous log file will be saved. If the value of this key is not specified, the maximum size of one log file will be 50 MB.
/LVL:debug|info|warning|error|critical	This key sets the log detail level from maximum (**All debug information**) in which all events are recorded into the log, to minimum (**Critical events**) in which only critical events are recorded. If this key is not specified, events with the **All debug information** level of detail will be recorded in the trace log.
/OFF	This key disables the trace log.

KAVSHELL TRACE command examples

► *To enable the trace log using the* ***All debug information*** *level of detail and maximum log size of 200MB, and to save the log file to folder C:\Trace Folder, execute the command:*

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /S:200
```

► *To enable the trace log using the* ***Important events*** *level of detail, and to save the log file to folder C:\Trace Folder, execute the command:*

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:warning
```

► *To disable the trace log, execute the command:*

```
KAVSHELL TRACE /OFF
```

Return codes for KAVSHELL TRACE command (see Section "Return codes for the KAVSHELL TRACE command" on page 519).

Kaspersky Embedded Systems Security log files defragmentation. KAVSHELL VACUUM

Using the `KAVSHELL VACUUM` command you can defragment the application log files. It allows to avoid system and the application errors due to the storage of large number of log files generated based on the application events.

> Password might be required to execute the command. To enter the current password use `[/pwd:<password>]` key.

It is recommended to apply the `KAVSHELL VACUUM` command to optimize log files storage in case of frequent On-Demand Scan scans and update tasks starts. While executing the command, Kaspersky Embedded Systems Security renews a logical structure for the application log files that are stored on a protected computer by specified path.

By default, the application log files are stored at C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Reports. If you have manually specified another path for storing logs, the `KAVSHELL VACUUM` command executes defragmentation for files in folder that is specified in the Kaspersky Embedded Systems Security logs settings.

> Big size of files defragmenting increases the `KAVSHELL VACUUM` command execution period.

The Real-Time Protection and the Computer Control tasks are not available to perform during the KAVSHELL VACUUM command execution. On-going defragmentation process restricts access to Kaspersky Embedded Systems Security log and rejects events logging. To avoid security level decrease, it is recommended to plan the KAVSHELL VACUUM command execution at the downtime in advance.

► *To defragment the Kaspersky Embedded Systems Security log files, execute the following command:*

```
KAVSHELL VACUUM
```

Command execution is possible if started with local administrator account rights.

Cleaning iSwift base. KAVSHELL FBRESET

Kaspersky Embedded Systems Security uses the iSwift technology, which allows the application to avoid rescanning files that have not been modified since the last scan (**Use iSwift technology**).

Kaspersky Embedded Systems Security creates in the %SYSTEMDRIVE%\System Volume Information folder files klamfb.dat and klamfb2.dat, which contains information about clean objects that have already been scanned. The file klamfb.dat (klamfb2.dat) grows with the number of files scanned by Kaspersky Embedded Systems Security. The file only contains current information about files existing in the system: if a file is removed, Kaspersky Embedded Systems Security purges information about it from klamfb.dat.

To clean up a file, use the command KAVSHELL FBRESET.

Please keep in mind the following specifics for operating the KAVSHELL FBRESET command:

- While cleaning the file klamfb.dat by means of the KAVSHELL FBRESET command, Kaspersky Embedded Systems Security does not pause the protection (unlike in cases of manual deletion of klamfb.dat).
- Kaspersky Embedded Systems Security may increase the computer workload after the data is cleared in klamfb.dat. In this case, Kaspersky Embedded Systems Security scans all files accessed for the first time after the clearing of klamfb.dat. After the scan, Kaspersky Embedded Systems Security adds back to klamfb.dat the information about each scanned object. In the case of new attempts to access the object, the iSwift technology will prevent rescanning of the file provided it remains unchanged.

The KAVSHELL FBRESET command execution is available only if the command line is started under the SYSTEM account.

Enabling and disabling dump file creation. KAVSHELL DUMP

Creation of snapshots (dump file) for Kaspersky Embedded Systems Security processes in cases of abnormal termination can be enabled or disabled using the `KAVSHELL DUMP` command (see the following table). Additionally memory snapshots of Kaspersky Embedded Systems Security processes in progress can be taken at any time.

> For the dump file to be successfully created the `KAVSHELL DUMP` command must be executed under the local system account (SYSTEM).

KAVSHELL DUMP command syntax

```
KAVSHELL DUMP </ON /F:<folder with the dump file>|/SNAPSHOT /F:< folder with
the dump file> / P:<pid> | /OFF>
```

Table 91. KAVSHELL DUMP command keys

Key	Description
/ON	Enables creation of the process memory dump file in cases of abnormal termination.
/F:<path to folder with dump files>	This is a mandatory key. It specifies the path to the folder to which the dump file will be saved. Paths to folders on the network drives of other unprotected computers cannot be specified. System environment variables can be used when specifying the path to the folder with the memory dump file; user environment variables are not allowed.
/SNAPSHOT	Takes a snapshot of the memory of the process in progress with a specified PID and saves the dump file into the folder the path to which is specified by key /F.
/P	PID process identifier is displayed in the Microsoft Windows Task Manager.
/OFF	Disables the creation of the memory dump file in cases of abnormal termination.

Return codes for KAVSHELL DUMP command (see Section "Return codes for the KAVSHELL DUMP command" on page 520).

KAVSHELL DUMP command examples

► *To enable creation of the dump file; to save the dump file to folder C:\Dump Folder, execute the command:*

```
KAVSHELL DUMP /ON /F:”C:\Dump Folder”
```

► *To make a dump for the process with ID 1234 to folder C:/Dumps, execute the command:*

```
KAVSHELL DUMP /SNAPSHOT /F:C:\dumps /F:1234
```

► *To disable generation of the dump file, execute the command:*

```
KAVSHELL DUMP /OFF
```

Importing settings. KAVSHELL IMPORT

The `KAVSHELL IMPORT` command allows you to import the settings of Kaspersky Embedded Systems Security, its features and tasks from a configuration file to a copy of Kaspersky Embedded Systems Security on the protected computer. A configuration file can be created using the `KAVSHELL EXPORT` command.

> Password might be required to execute the command. To enter the current password use `[/pwd:<password>]` key.

KAVSHELL IMPORT command syntax

```
KAVSHELL IMPORT <name of configuration file and path to file>
```

KAVSHELL IMPORT command examples

```
KAVSHELL IMPORT Host1.xml
```

Table 92. KAVSHELL IMPORT command keys

Key	Description
<name of configuration file and path to file>	Name of configuration file used as the import source for settings. System environment variables can be used when specifying the path to the file; user environment variables are not allowed.

Return codes for KAVSHELL IMPORT command (see Section "Return codes for the KAVSHELL IMPORT command" on page 521).

Exporting settings. KAVSHELL EXPORT

The `KAVSHELL EXPORT` command allows you to export all of the settings of Kaspersky Embedded Systems Security and its current tasks to a configuration file in order to import them later into copies of Kaspersky Embedded Systems Security installed on other computer.

KAVSHELL EXPORT command syntax

```
KAVSHELL EXPORT <name of configuration file and path to file>
```

KAVSHELL EXPORT command examples

```
KAVSHELL EXPORT Host1.xml
```

Table 93. KAVSHELL EXPORT command keys

Key	Description
<name of configuration file and path to file>	Name of configuration file which will contain settings. Any extension can be assigned to the configuration file. System environment variables can be used when specifying the path to the file; user environment variables are not allowed.

Return codes for KAVSHELL EXPORT command (see Section "Return codes for the KAVSHELL EXPORT command" on page 521).

Integration with Microsoft Operations Management Suite. KAVSHELL OMSINFO

Using the KAVSHELL OMSINFO command you can review status of the application and information about threats detected by anti-virus databases and KSN service. The data about threats is taken from the available event logs.

KAVSHELL OMSINFO command syntax

```
KAVSHELL OMSINFO <full path to generated file with file name>
```

KAVSHELL OMSINFO command examples

```
KAVSHELL OMSINFO C:\Users\Admin\Desktop\omsinfo.json
```

Table 94. KAVSHELL OMSINFO command keys

Key	Description
<path to generated file with file name>	Name of the generated file which will contain information about application status and detected threats.

Command line return codes

In this section

Return code for the commands KAVSHELL START and KAVSHELL STOP

Table 95. Return code for the commands KAVSHELL START and KAVSHELL STOP

Return code	Description
0	Operation completed successfully
-3	Permissions error
-5	Invalid command syntax
-6	Invalid operation (for example, Kaspersky Embedded Systems Security service is already running or already stopped)
-7	Service not registered
-8	Automatic Service startup is disabled.
-9	Attempt to start computer under another user account failed (by default Kaspersky Embedded Systems Security service runs under the Local system user account)
-99	Unknown error

Return code for KAVSHELL SCAN and KAVSHELL SCANCRITICAL commands

Table 96. Return code for KAVSHELL SCAN and KAVSHELL SCANCRITICAL commands

Return code	Description
0	Operation completed successfully (no threats detected)
1	Operation canceled
-2	Service not running
-3	Permissions error
-4	Object not found (file with the list of scan scopes not found)
-5	Invalid command syntax or scan scope not defined
-80	Infected and other objects detected
-81	Probably infected objects detected
-82	Processing errors detected
-83	Unchecked objects found
-84	Corrupted objects detected
-85	Task log file creation failed
-99	Unknown error
-301	Invalid key

Return codes for KAVSHELL TASK LOG-INSPECTOR command

Table 97. Return code for KAVSHELL TASK LOG-INSPECTOR command

Return code	Description
0	Operation completed successfully
-6	Invalid operation (for example, Kaspersky Embedded Systems Security service is already running or already stopped)
402	Task is already running (for modifier /STATE)

Return codes for KAVSHELL TASK command

Table 98. Return codes for KAVSHELL TASK command

Return code	Description
0	Operation completed successfully
-2	Service not running
-3	Permissions error
-4	Object not found (task not found)
-5	Invalid command syntax
-6	Invalid operation (for example, task not running, already running, or cannot be paused)
-99	Unknown error
-301	Invalid key
401	Task not running (for modifier /STATE)
402	Task already running (for modifier /STATE)
403	Task already paused (for modifier /STATE)
-404	Error executing operation (change in task status led to it crashing)

Return codes for the KAVSHELL RTP command

Table 99. Return codes for the KAVSHELL RTP command

Return code	Description
0	Operation completed successfully
-2	Service not running
-3	Permissions error
-4	Object not found (one of the Real-Time Protection tasks or all Real-Time Protection tasks not found)
-5	Invalid command syntax
-6	Invalid operation (for example, the task is already running or already stopped)
-99	Unknown error
-301	Invalid key

Return codes for KAVSHELL UPDATE command

Table 100. Return codes for KAVSHELL UPDATE command

Return code	Description
0	Operation completed successfully
200	All objects are up-to-date (database or program components are current)
-2	Service not running
-3	Permissions error
-5	Invalid command syntax
-99	Unknown error
-206	Extension files are missing in the specified source or have unknown format
-209	Error connecting to the update source
-232	Authentication error while connecting to proxy server
-234	Error connecting to Kaspersky Security Center
-235	Kaspersky Embedded Systems Security was not authenticated when connecting to the update source
-236	Application database is corrupted
-301	Invalid key

Return codes for the KAVSHELL ROLLBACK command

Table 101. Return codes for the KAVSHELL ROLLBACK command

Return code	Description
0	Operation completed successfully
-2	Service not running
-3	Permissions error
-99	Unknown error
-221	Backup copy of database not found or corrupted
-222	Backup copy of database corrupted

Return codes for the KAVSHELL LICENSE command

Table 102. Return codes for the KAVSHELL LICENSE command

Return code	Description
0	Operation completed successfully
-2	Service not running
-3	Insufficient privileges to manage keys
-4	Key with specified number not found
-5	Invalid command syntax
-6	Invalid operation (key already added)
-99	Unknown error
-301	Invalid key
-303	License applies to a different application

Return codes for the KAVSHELL TRACE command

Table 103. Return codes for the KAVSHELL TRACE command

Return code	Description
0	Operation completed successfully
-2	Service not running
-3	Permissions error
-4	Object not found (path specified as path to the Tracking logs folder not found)
-5	Invalid command syntax
-6	Invalid operation (attempt of KAVSHELL TRACE /OFF command execution if trace log creation is already disabled)
-99	Unknown error

Return codes for the KAVSHELL FBRESET command

Table 104. Return codes for the KAVSHELL FBRESET command

Return code	Description
0	Operation completed successfully
-99	Unknown error

Return codes for the KAVSHELL DUMP command

Table 105. Return codes for the KAVSHELL DUMP command

Return code	Description
0	Operation completed successfully
-2	Service not running
-3	Permissions error
-4	Object not found (path specified as path to the dump file folder not found; process with specified PID not found)
-5	Invalid command syntax
-6	Invalid operation (attempt of KAVSHELL DUMP/OFF command execution if dump file creation is already disabled)
-99	Unknown error

Return codes for the KAVSHELL IMPORT command

Table 106. Return codes for the KAVSHELL IMPORT command

Return code	Description
0	Operation completed successfully
-2	Service not running
-3	Permissions error
-4	Object not found (importable configuration file not found)
-5	Invalid syntax
-99	Unknown error
501	Operation completed successfully, however an error/comment occurred during the command execution, for example, Kaspersky Embedded Systems Security did not import parameters of some functional component
-502	File being imported is missing or has an unrecognized format
-503	Incompatible settings (configuration file exported from a different program or a later and incompatible version of Kaspersky Embedded Systems Security)

Return codes for the KAVSHELL EXPORT command

Table 107. Return codes for the KAVSHELL EXPORT command

Return code	Description
0	Operation completed successfully
-2	Service not running
-3	Permissions error
-5	Invalid syntax
-10	Unable to create a configuration file (for example no access to the folder specified in the path to the file)
-99	Unknown error
501	Operation completed successfully, however an error/comment occurred during the command execution, for example, Kaspersky Embedded Systems Security did not export parameters of some functional component

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).

Get technical support by phone

You can call Technical Support specialists from most regions worldwide. You can find information about how to obtain technical support in your region and contact information for Technical Support on the Kaspersky Lab Technical Support website (https://support.kaspersky.com/b2b).

> Before contacting Technical Support, please read the support rules (https://support.kaspersky.com/support/rules#en_us).

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 Embedded Systems Security 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.

Glossary

A

Active key

A key that is currently used by the application.

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.

D

Disinfection

A method of processing infected objects that results in full or partial recovery of data. Not all infected objects can be disinfected.

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.

F

False positive

A situation when a Kaspersky Lab application considers a non-infected object to be infected because the object's code is similar to that of a virus.

File mask

Representation of a file name using wildcards. The standard wildcards used in file masks are * and ?, where * represents any number of any characters and ? stands for any single character.

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.

L

License term

A time period during which you have access to the application features and rights to use additional services. The services you can use depend on the type of the license.

Local task

A task defined and running on a single client computer.

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 an application’s settings and manages the ability to configure that application on computers within an administration group. An individual policy must be created for each application. You can create an unlimited number of different policies for applications installed on computers in each administration group, but only one policy can be applied at a time to each application 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.

SIEM

A technology that analyzes security events originating from various network devices and applications.

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.

T

Task

Functions performed by the Kaspersky Lab application are implemented as tasks, such as: Real-time file protection, Full computer scan, and Database update.

Task settings

Application settings that are specific for each task type.

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.

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
Kaspersky VirusDesk:	https://virusdesk.kaspersky.com (for analyzing suspicious files and websites)
Kaspersky Lab's web community:	https://community.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.

Intel and Pentium are trademarks of Intel Corporation in the U.S. and/or other countries.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Microsoft, Active Directory, Excel, Internet Explorer, and Windows are registered trademarks of Microsoft Corporation in the United States and other countries.

UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Limited.

Index