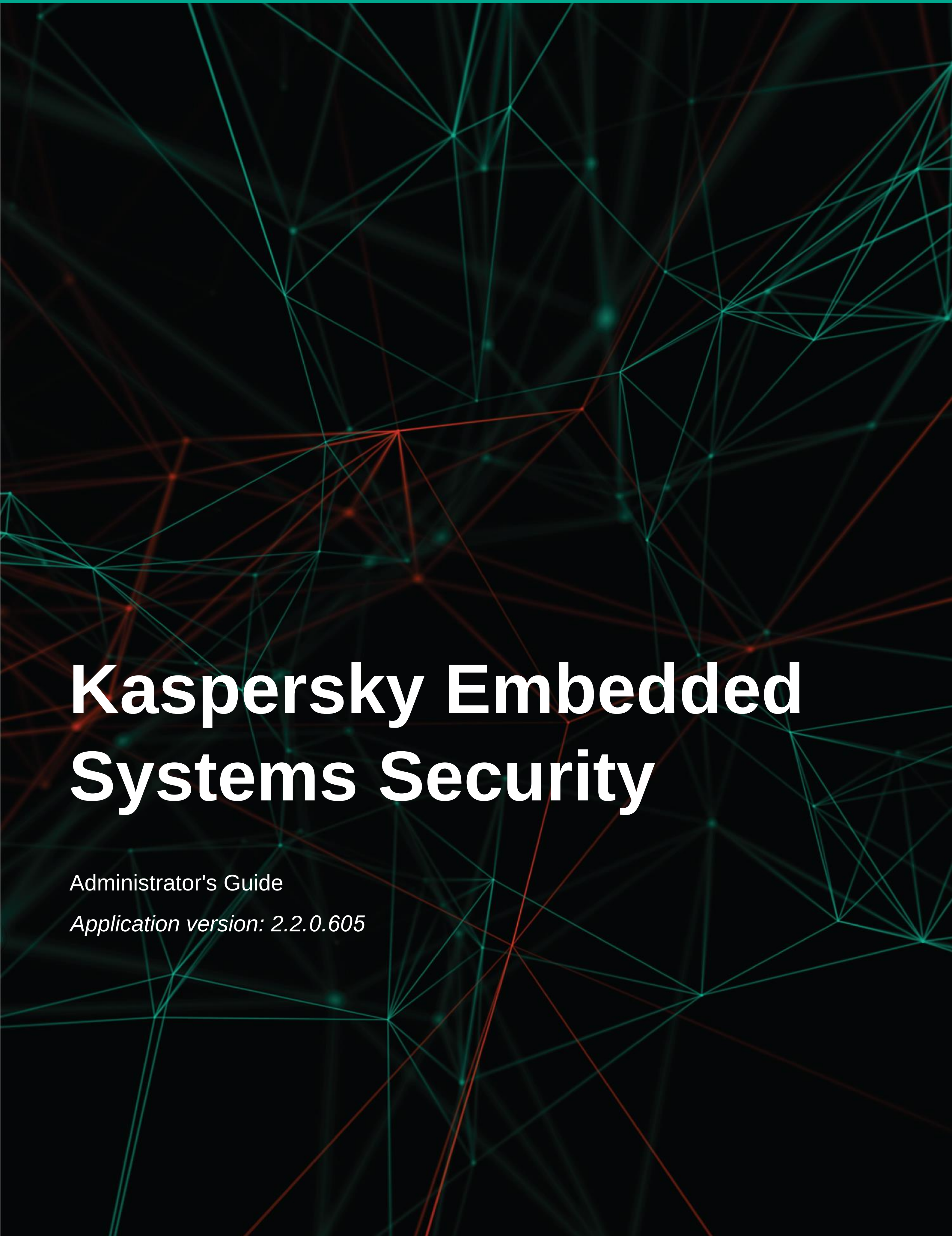

Kaspersky Embedded Systems Security

Administrator's Guide

Application version: 2.2.0.605

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: 29.10.2018

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

Contents

About this Guide

The Kaspersky Embedded Systems Security 2.2.0.605 (hereinafter referred to as "Kaspersky Embedded Systems Security 2.2", "the application") Administrator's Guide is intended for specialists who install and administer Kaspersky Embedded Systems Security 2.2 on all protected devices, and for specialists who provide technical support to organizations using Kaspersky Embedded Systems Security 2.2.

This Guide contains information about configuring and using Kaspersky Embedded Systems Security 2.2.

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 2.2 contains the following sections:

Sources of information about Kaspersky Embedded Systems Security 2.2

This section lists the sources of information about the application.

Kaspersky Embedded Systems Security 2.2

This section describes the functions, components, and distribution kit of Kaspersky Embedded Systems Security 2.2, and provides a list of hardware and software requirements of Kaspersky Embedded Systems Security 2.2.

Installing and removing the application

This section provides step-by-step instructions for installing and removing Kaspersky Embedded Systems Security 2.2.

Application interface

This section contains information about elements of the Kaspersky Embedded Systems Security 2.2 interface.

Application licensing

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

Starting and stopping Kaspersky Embedded Systems Security 2.2

This section contains information about starting and stopping the Kaspersky Embedded Systems Security 2.2 Administration Plug-in (hereinafter referred to as Administration Plug-in) and the Kaspersky Security Service.

About access permissions for Kaspersky Embedded Systems Security 2.2 functions

This section contains information about permissions to manage Kaspersky Embedded Systems Security 2.2 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 2.2 on several computers.

Creating and configuring tasks using Kaspersky Security Center

This section contains information about Kaspersky Embedded Systems Security 2.2 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 2.2 general settings in Kaspersky Security Center.

Real-Time Computer Protection

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

Local Activity Control

This section provides information about Kaspersky Embedded Systems Security 2.2 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 2.2 with third-party features and technologies.

Working with Kaspersky Embedded Systems Security 2.2 from the command line

This section describes working with Kaspersky Embedded Systems Security 2.2 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".
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 the arrow sign.
In the command line, type `help` The following message then appears: Specify the date in `dd:mm:yy` format.	The following types of text content are set off with a special font: • Text in the command line • Text of messages displayed on the screen by the application • Data that must be entered from the keyboard
<User name>	Variables are enclosed in angle brackets. Instead of a variable, the corresponding value should be inserted, omitting the angle brackets.

Sources of information about Kaspersky Embedded Systems Security 2.2

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 2.2:

- Kaspersky Embedded Systems Security 2.2 page on the Kaspersky Lab website.
- Kaspersky Embedded Systems Security 2.2 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 2.2 page on the Kaspersky Lab website

On the Kaspersky Embedded Systems Security 2.2 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 2.2 page contains a link to eStore. There you can purchase the application or renew your license.

Kaspersky Embedded Systems Security 2.2 page in Knowledge Base

Knowledge Base is a section on the Technical Support website.

The Kaspersky Embedded Systems Security 2.2 page in the Knowledge Base (https://support.kaspersky.com/kess/) 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 2.2 but also to other Kaspersky Lab applications. Knowledge Base articles can also include Technical Support news.

Kaspersky Embedded Systems Security 2.2 documentation

Kaspersky Embedded Systems Security 2.2 Administrator's Guide contains information about the application installation, uninstallation, settings configuring and usage.

Discussing Kaspersky Lab applications on the forum

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

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

Kaspersky Embedded Systems Security 2.2

This section describes the functions, components, and distribution kit of Kaspersky Embedded Systems Security 2.2, and provides a list of hardware and software requirements of Kaspersky Embedded Systems Security 2.2.

In this chapter

About Kaspersky Embedded Systems Security 2.2

Kaspersky Embedded Systems Security 2.2 protects computers and other embedded systems under Microsoft® Windows against viruses and other computer threats. Kaspersky Embedded Systems Security 2.2 users are corporate network administrators and specialists responsible for anti-virus protection of the corporate network.

You can install Kaspersky Embedded Systems Security 2.2 on a variety embedded systems under Windows, including the following devices types:

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

Kaspersky Embedded Systems Security 2.2 can be managed in the following ways:

- Via the Application Console installed on the same computer as Kaspersky Embedded Systems Security 2.2, 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 2.2.

It is possible to review Kaspersky Embedded Systems Security 2.2 performance counters for the "System Monitor" application, as well as SNMP counters and traps.

Kaspersky Embedded Systems Security 2.2 components and functions

The application includes the following components:

- **Real-Time File Protection**. Kaspersky Embedded Systems Security 2.2 scans objects when they are accessed. Kaspersky Embedded Systems Security 2.2 scans the following objects:
  - Files
  - Alternate file system streams (NTFS streams)
  - Master boot record and boot sectors on local hard and removable drives

- **On-Demand Scan**. Kaspersky Embedded Systems Security 2.2 runs a single scan of the specified area for viruses and other computer security threats. Application scans files, RAM, and startup objects on a protected 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 2.2 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 2.2 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 2.2 quarantines probably infected objects by moving such objects from their original location to *Quarantine*. For security purposes, objects are stored in Quarantine in encrypted form.
- **Backup**. Kaspersky Embedded Systems Security 2.2 stores encrypted copies of objects classified as *Infected* or *Probably infected* in *Backup* before disinfecting or deleting them.
- **Administrator and user notifications**. You can configure the application to notify the administrator and users who access the protected computer about events in Kaspersky Embedded Systems Security 2.2 operation and the status of Anti-Virus protection on the computer.
- **Importing and exporting settings**. You can export Kaspersky Embedded Systems Security 2.2 settings to an XML configuration file and import settings into Kaspersky Embedded Systems Security 2.2 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 2.2 protection and scan tasks.
- **Managing access permissions for Kaspersky Embedded Systems Security functions**.You can configure the rights to manage Kaspersky Embedded Systems Security 2.2 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 2.2 logs information about software component settings, the current status of tasks, events that occur while tasks run, events associated with Kaspersky Embedded Systems Security 2.2 management, and information required to diagnose errors in Kaspersky Embedded Systems Security 2.2.
- **Trusted Zone**. You can generate the list of exclusions from the protection or scan scope, that Kaspersky Embedded Systems Security 2.2 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 2.2 offers the following new features and improvements::

- Support for new versions of Microsoft Windows operating systems.

  Self-defense mechanisms based on ELAM and PPL technologies: now when the application is installed, it automatically registers an ELAM driver that makes it possible to start the Kaspersky Security service (kavfs.exe) with the Protected Process Light attribute. This makes it possible to bolster the application's self-defense and prevent a broad range of attacks.

  The functionality is available when the application is installed on computers running Microsoft Windows 10 RS2 (build number 15063) and higher.

- Support for checking and processing cloud files stored in Microsoft OneDrive.
- Software distribution control subsystem possibilities are improved.

  Now you can indicate which installation files can pass the trusted installation package attribute for the entire chain of files extracted from them. This makes it possible to increase the stability of the software installation processes on a computer with enabled Applications Launch Control, but it also expands the area for a potential attack by increasing the number of authorized application launches. It is recommended to use this option during complex software deployments, including when the computer must be restarted during the software distribution process.

- Integration with WMI tools.

  Now when the application is installed, a Kaspersky Security namespace is automatically created in the WMI root namespace on the local computer. You can use client solutions that support WMI queries to obtain data about the application and its components.

- The format for displaying information about the application and its components has been expanded with the KAVSHELL OMSINFO command: now you can get information about the status of the Applications Launch Control task as well as information about installed critical updates of application modules.
- Improved possibilities for managing and monitoring application state using the Compact Diagnostic Interface:
  - Now you can review the statistics counters for installed components on the Statistics tab of the Compact Diagnostic Interface.
  - The password is not required upon accessing the Compact Diagnostic Interface, even if the password-protection feature in on: the application limits access to the information and control elements that are available in the Compact Diagnostic Interface based only on the specified user permissions for the application management.
- Starting from version 2.2, the application implements the ability to provide basic computer protection during operating system startup in safe mode.

  By default, the application does not work on a computer running in safe mode. To make the application start when the operating system is started in safe mode, set the LoadInSafeMode parameter equal to 1 in the following Windows Registry key:

  ```
  HKLM\SYSTEM\CurrentControlSet\services\klam\Parameters
  ```

  > When running on a computer started in safe mode, the application's functionality will be limited.

- Kaspersky Security Center reports supported: you can now review reports on the status of application components and two types of reports on prohibited applications.

  This functionality is supported only when using Kaspersky Security Center 11.

- User access permissions for changing the installation folder and modifying critical registry branches of the application components are now limited.

Distribution kit

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

- Start the Kaspersky Embedded Systems Security 2.2 Installation Wizard.
- Start the Kaspersky Embedded Systems Security 2.2 Console Installation Wizard.
- Start the Installation Wizard that will install Kaspersky Embedded Systems Security 2.2 Administration Plug-in for managing the application via the Kaspersky Security Center.
- Read the Administrator's Guide.
- Read the User's Guide.
- Go to Kaspersky Embedded Systems Security 2.2 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 2.2.

The \console folder contains files for the installation of Application Console ("Kaspersky Embedded Systems Security 2.2 Administration Tools" set of components).

The \product folder contains:

- Files for the installation of Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 components and plug-ins 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 2.2 distribution kit files

File	Purpose
autorun.inf	Autorun file for the Kaspersky Embedded Systems Security 2.2 Installation Wizard when installing the application from removable media.
ess_admin_guide_en.pdf	Administrator's Guide.
ess_user_guide_en.pdf	User'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 installation 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.

File	Purpose
\product\bases.cab	Archive of anti-virus databases current at the time of application release.
\product\setup.exe	The file that starts the wizard for installing Kaspersky Embedded Systems Security 2.2 on the protected computer; it starts the installer package file ess.msi with the installation settings specified in the wizard.
\product\ess_x86(x64).msi	Windows Installer installation package; installs Kaspersky Embedded Systems Security 2.2 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 2.2 via Kaspersky Security Center.
\product\klcfginst.exe	Installer for Administration Plug-in for managing Kaspersky Embedded Systems Security 2.2 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 2.2.
\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.

Distribution kit files can be run from the Installation CD. If you have copied the distribution package files onto the local drive beforehand, make sure that the structure of the distribution kit files has been preserved.

Hardware and software requirements

Before installing Kaspersky Embedded Systems Security 2.2, you must uninstall other anti-virus applications from the computer.

Hardware requirements for the protected computer

General requirements:

- x86-compatible systems in single and multiprocessor configurations.
- x64-compatible systems in single and multiprocessor configurations.

Disk volume:

- To install the Applications Launch Control component – 50 MB.
- To install all Kaspersky Embedded Systems Security 2.2 components – 500 MB.

RAM:

- 256 MB to install the Applications Launch Control component only on the computer under Microsoft® Windows operating system.
- 512 MB to perform full installation of all components on the computer under the Microsoft Windows OS.

Minimum processor requirements:

- for 32-bit Microsoft Windows operating systems: Intel® Pentium® III.
- for 64-bit Microsoft Windows operating systems: Intel Pentium IV.

Software requirements for the protected computer

You can install Kaspersky Embedded Systems Security 2.2 on a device 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 2.2 on the devices with embedded operating systems, Filter Manager and Administration Support Tools components are required.

You can install Kaspersky Embedded Systems Security 2.2 on a computer under one of the following 32-bit or 64-bit Microsoft Windows operating systems:

- Windows XP Embedded SP3
- Windows XP Pro SP2 / SP3
- Windows Embedded POSReady 2009
- Windows Embedded Standard 7 SP1
- Windows Embedded Enterprise 7 SP1
- Windows Embedded POSReady 7
- Windows 7 Professional / Enterprise SP1
- Windows Embedded 8.1 Industry Professional / Enterprise
- Windows Embedded 8.1 Professional
- Windows Embedded 8.0 Standard
- Windows 8 Professional / Enterprise
- Windows 8.1 Professional / Enterprise
- Windows 10 Professional / Enterprise
- Windows 10 IoT Enterprise
- Windows 10 Redstone 1 Professional / Enterprise / IoT Enterprise
- Windows 10 Redstone 2 Professional / Enterprise / IoT Enterprise
- Windows 10 Redstone 3 Professional / Enterprise / IoT Enterprise
- Windows 10 Redstone 4 Professional / Enterprise / IoT Enterprise
- Windows 10 Redstone 5 Professional / Enterprise / IoT Enterprise

Installing and removing the application

This section provides step-by-step instructions for installing and removing Kaspersky Embedded Systems Security 2.2.

In this chapter

Kaspersky Embedded Systems Security 2.2 software components and their codes for Windows Installer service

By default, \server\ess_x86(x64).msi files are intended to install all Kaspersky Embedded Systems Security 2.2 components. You can install this component by including it in a custom installation.

The \client\esstools_x86(x64).msi files install all software components from the "Administrative Tools" set.

The following sections list the codes of the Kaspersky Embedded Systems Security 2.2 components 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 2.2 from the command line.

In this section

Kaspersky Embedded Systems Security 2.2 software components

The following table contains codes for and a description of Kaspersky Embedded Systems Security 2.2 software components.

Table 3. Description of Kaspersky Embedded Systems Security 2.2 software components

Component	Code	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 the set 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 ensures 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 2.2 system files and On-demand scan tasks (scanning of objects on the protected computer upon request). If other Kaspersky Embedded Systems Security 2.2 components are specified when installing Kaspersky Embedded Systems Security 2.2 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.
Use of Kaspersky Security Network	Ksn	This component provides protection on the basis of Kaspersky Lab cloud technologies. It implements the KSN Usage task (sending requests to and receiving conclusions from the Kaspersky Security Network service).
File Integrity Monitor	Fim	This component logs operations performed on files in the specified monitoring scope. The component implements the File Integrity Monitor task.

Component	Code	Functions performed
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 2.2 graphical user interface. The component implements the Firewall Management task.
Module for integration with Kaspersky Security Center Network Agent	AKIntegration	Provides a connection between theKaspersky Embedded Systems Security 2.2 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 2.2 performance to be measured and potential bottlenecks to be localized on the computer when Kaspersky Embedded Systems Security 2.2 is used with other programs.
SNMP counters and traps	SnmpSupport	This component publishes Kaspersky Embedded Systems Security 2.2 counters and traps via Simple Network Management Protocol (SNMP) in Microsoft Windows. This component may be installed on the protected computer only if Microsoft SNMP is installed on the same computer.
Kaspersky Embedded Systems Security 2.2 icon in the notification area	TrayApp	This component displays the Kaspersky Embedded Systems Security 2.2 icon in the task tray notification area of the protected computer. The Kaspersky Embedded Systems Security 2.2 icon displays the status of computer protection and can be used open the Kaspersky Embedded Systems Security 2.2 Console in Microsoft Management Console (if installed) and the **About application** window.
Command line utility	Shell	Makes it possible to control Kaspersky Embedded Systems Security 2.2 from the command line of a protected computer.

"Administration tools" set of software components

The following table contains codes for and a description 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 2.2 snap-ins	MmcSnapin	This component installs the Microsoft Management Console snap-in via Kaspersky Embedded Systems Security 2.2 Console. If other components are specified during the installation of "Administration Tools" from the command line, and the MmcSnapin component is not specified, the component will be installed automatically.
Help	Help	.chm help file; saved in the folder with the Kaspersky Embedded Systems Security 2.2 Administration Tools files. You can open Help file using the **Start** menu or by clicking the **F1** key with the Application Console window opened.
Documentation	Help	Kaspersky Embedded Systems Security 2.2 adds a shortcut to the Kaspersky Lab web resource where the Administrator's Guide and User's Guide are available in PDF format. The shortcut is available in the Start menu.

System changes after Kaspersky Embedded Systems Security 2.2 installation

When Kaspersky Embedded Systems Security 2.2 and the Application Console (set of "Administration Tools") are installed together, the Windows Installer service will make the following modifications on the protected computer:

- Creates Kaspersky Embedded Systems Security 2.2 folders on the protected computer and on the computer, where the Application Console is installed.
- Registers Kaspersky Embedded Systems Security 2.2 services.
- Creates a Kaspersky Embedded Systems Security 2.2 group of users.
- Registers Kaspersky Embedded Systems Security 2.2 keys in the system register.

These changes are described in the table below.

Kaspersky Embedded Systems Security 2.2 folders

Table 5. Kaspersky Embedded Systems Security 2.2 folders on a protected computer

Folder	Kaspersky Embedded Systems Security 2.2 files
Kaspersky Embedded Systems Security 2.2 default installation folder: In the Microsoft Windows 32-bit version – %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security\ In the Microsoft Windows 64-bit version – %ProgramFiles(x86)%\Kaspersky Embedded Systems Security\	Executable Kaspersky Embedded Systems Security 2.2 files (destination folder specified during installation).

Folder	Kaspersky Embedded Systems Security 2.2 files
%Kaspersky Embedded Systems Security%\mibs folder	Management Information Base (MIB) files; these files contain a description of the counters and hooks published by Kaspersky Embedded Systems Security 2.2 via the SNMP protocol.
%Kaspersky Embedded Systems Security%\x64 folder	64-bit versions of Kaspersky Embedded Systems Security 2.2 executable files (the folder will be created only during the installation of Kaspersky Embedded Systems Security 2.2 in the 64-bit version of Microsoft Windows).
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Data\ %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Settings\ %ALLUSERSPROFILE%\Application Data\Kaspersky Embedded Systems Security\2.2\Dskm\	Kaspersky Embedded Systems Security 2.2 service files.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Update\	Files with update sources settings.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Update\Distribution\	Updates of databases and software modules downloaded using 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\2.2\Reports\	Task logs and system audit log.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Bases\Current\	Set of databases used at current time.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Bases\Backup\	Backup copy of databases; will be overwritten each time databases are updated.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Bases\Temp\	Temporary files created during execution of update tasks.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Quarantine\	Quarantined objects (default folder).

Folder	Kaspersky Embedded Systems Security 2.2 files
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Backup\	Objects in backup (default folder).
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Restored\	Objects restored from backup and quarantine (default folder for restored objects).

Table 6. Folders created during the installation of the Application Console

Folder	Kaspersky Embedded Systems Security 2.2 Console files
Application Console default installation folder: • In the Microsoft Windows 32-bit version – %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools\ • In the Microsoft Windows 64-bit version – %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools\	"Administration Tools" files (destination folder specified during the installation of Kaspersky Embedded Systems Security 2.2 Console).

Kaspersky Embedded Systems Security 2.2 services

Kaspersky Embedded Systems Security 2.2 services start using the Local system (SYSTEM) account.

Table 7. Kaspersky Embedded Systems Security 2.2 services

Service	Purpose
Kaspersky Security Service (KAVFS)	Essential Kaspersky Embedded Systems Security 2.2 service that manages Kaspersky Embedded Systems Security 2.2 tasks and workflows.
Kaspersky Security Management Service (KAVFSGT)	The service is intended for Kaspersky Embedded Systems Security 2.2 application management through the Application Console.

Kaspersky Embedded Systems Security 2.2 groups

Table 8. Kaspersky Embedded Systems Security 2.2 groups

Group	Purpose
ESS Administrators	A group on the protected computer whose users have full access to the Kaspersky Security Management Service and to all Kaspersky Embedded Systems Security 2.2 functions.

System registry keys

Table 9. System registry keys

Key	Purpose
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFS]	Kaspersky Embedded Systems Security 2.2 service properties.
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Security]	Kaspersky Embedded Systems Security 2.2 event log settings (Kaspersky Event Log).
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]	Kaspersky Embedded Systems Security 2.2 management service properties.
In Microsoft Windows 32-bit version: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security\Performance] In Microsoft Windows 64-bit version: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security x64\Performance].	Performance counters settings.
In Microsoft Windows 32-bit version: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.2\SnmpAgent] In Microsoft Windows 64-bit version: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.2\SnmpAgent]	SNMP Protocol Support component settings.
In Microsoft Windows 32-bit version: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.2\CrashDump] In Microsoft Windows 64-bit version: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.2\CrashDump]	Dump file writing settings.
In Microsoft Windows 32-bit version: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.2\Trace] In Microsoft Windows 64-bit version: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.2\Trace]	Trace file settings.
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.2\Environment]	Configuration of the application's tasks and functions.

Kaspersky Embedded Systems Security 2.2 processes

Kaspersky Embedded Systems Security 2.2 starts processes described in the table below.

Table 10. Kaspersky Embedded Systems Security 2.2 processes

File name	Purpose
kavfswp.exe	Kaspersky Embedded Systems Security 2.2 workflow
kavtray.exe	Process for the System Tray Icon
kavshell.exe	Command line utility process
kavfsrcn.exe	Kaspersky Embedded Systems Security 2.2 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 Windows Installer service

The tables provided below contain descriptions of the settings to install and uninstall Kaspersky Embedded Systems Security 2.2, their default values, keys for changing the values of the installation settings, and their possible values. These keys can be used in conjunction with standard keys for the command msiexec of the Windows Installer service when installing Kaspersky Embedded Systems Security 2.2 from the command line.

Table 11. Installation parameters and command line options in Windows Installer

Setting	Windows Installer command line options and their possible values	Default Value	Description
Acceptance of the terms of the End User License Agreement	EULA=<value> 0 – you reject the terms of the End User License Agreement. 1 – you accept the terms of the End User License Agreement.	0	You must accept the terms of the End User License Agreement to install Kaspersky Embedded Systems Security 2.2.
Acceptance of the terms of Privacy Policy	PRIVACYPOLICY=<value> 0 – you reject the terms of Privacy Policy. 1 – you accept the terms of Privacy Policy.	0	You must accept the terms of Privacy Policy to install Kaspersky Embedded Systems Security 2.2.

Setting	Windows Installer command line options and their possible values	Default Value	Description
Destination folder	INSTALLDIR=<full path to the folder>	Kaspersky Embedded Systems Security 2.2: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Administration tools: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools In the x64-bit version of Microsoft Windows: %ProgramFiles(x86)%.	Folder in which Kaspersky Embedded Systems Security 2.2 files will be saved during installation. A different folder can be specified.

Startup of the Real-Time File Protection task when Kaspersky Embedded Systems Security 2.2 starts (**Enable real-time protection after installation of application**)	RUNRTP=<value>
	1 – start;
	0 – do not start.
		1	Turn on this setting to start Real-Time File Protection at the start of Kaspersky Embedded Systems Security 2.2 (recommended).

Exclusions from scan as recommended by Microsoft Corporation (**Add Microsoft recommended files to exclusions list**)	ADDMSEXCLUSION=<value>
	1 – exclude;
	0 – do not exclude.
		1	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 the anti-virus application intercepts or modifies files used by such applications. For example, Microsoft Corporation includes some domain controller applications in the list of such objects.

Setting	Windows Installer command line options and their possible values	Default Value	Description

Objects excluded from the scanning scope according to Kaspersky Lab recommendations (**Add Kaspersky Lab recommended files to exclusions list**)	ADDKLEXCLUSION=<value>
	1 – exclude;
	0 – do not exclude.
		1	In the Real-Time File Protection task exclude from the protection scope objects on the computer that Kaspersky Lab recommends to exclude.

Allow remote connection to the Application Console.	ALLOWREMOTECON=<value>
	1 – allow;
	0 – deny.
		0	By default, remote connection is not allowed to the Application Console installed on the protected computer. During installation, you can allow connection. Kaspersky Embedded Systems Security 2.2 creates allowing rules for the process kavfsgt.exe using the TCP protocol for all ports.

Path to the key file (**Key**)	LICENSEKEYPATH=<key file name>	\product directory in the distribution kit	By default, the 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 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.

Setting	Windows Installer command line options and their possible values	Default Value	Description
			You can add a key after Kaspersky Embedded Systems Security 2.2 is installed using an administration 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 2.2 will not function.
Path to the configuratio n file	CONFIGPATH=<configuration file name>	Not specified	Kaspersky Embedded Systems Security 2.2 imports settings from the specified configuration file created in the application. Kaspersky Embedded Systems Security 2.2 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.

Setting	Windows Installer command line options and their possible values	Default Value	Description

Enabling network connections for the Console	ADDWFEXCLUSION=<value >
	1 – allow;
	0 – deny.
		0	Use this option to install Kaspersky Embedded Systems Security 2.2 on another computer. You can remotely manage a computer protection from another device with the Kaspersky Embedded Systems Security 2.2 Console installed.
			Port 135 (TCP) is opened in the Microsoft Windows firewall, network connections for the executable file kavfsrcn.exe for remote management of Kaspersky Embedded Systems Security 2.2 are allowed, and access is granted to DCOM applications.
			Upon installation completion add users to ESS Administrators group to allow them remote application management, and allow network connections to Kaspersky Security Management Service (kavfsgt.exe file) on the computer.
			You can read more about additional configuration when the Kaspersky Embedded Systems Security 2.2 Console is installed on another computer (see Section "Advanced settings after installation of the Application Console on another computer" on page 39).

Setting	Windows Installer command line options and their possible values	Default Value	Description
Disabling the check for incompatible software	SKIPINCOMPATIBLESW = <value> 0 - The check for incompatible software is performed 1 - The check for incompatible software is not performed	0	Use this setting to enable or disable the check for incompatible software during background installation of the application on the device. Regardless of the value of this setting, during installation of Kaspersky Embedded Systems Security 2.2, the application always warns about other versions of the application installed on the device.

Table 12. Uninstallation settings and command line options in Windows Installer

Setting	Windows Installer command line options and their possible values	Default Value

Restoring quarantined objects	RESTOREQTN =<value>
	0 – remove quarantined content;
	1 – restore quarantined content to the folder specified by the RESTOREPATH parameter into the \Quarantine subfolder.
		0 – Remove

Restoring the content of backup	RESTOREBCK =<value>
	0 – remove backup content;
	1 – restore backup contents to the folder specified by the RESTOREPATH parameter into the \Backup subfolder.
		0 – Remove

Enter of the current password to confirm the deletion (if password protection is enabled)	UNLOCK_PASSWORD=<specified password>	Not specified
Folder for restored objects	RESTOREPATH=<full path to the folder> Restored objects will be saved to the specified folder.	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Restored

Kaspersky Embedded Systems Security 2.2 install and uninstall log

If Kaspersky Embedded Systems Security 2.2 is installed or uninstalled using the Installation (Uninstallation) Wizard, the Windows Installer service creates an install (uninstall) log. Log file ess_install_<uid>.log (where <uid> – unique 8-character log identifier) will be saved into a %temp% folder of the user from whose account the setup.exe file was started.

If you run **Modify or Remove** option for the Application Console or Kaspersky Embedded Systems Security 2.2 from the **Start** menu, the ess_2.2_maintenance.log is automatically created in the %temp% folder.

If Kaspersky Embedded Systems Security 2.2 is installed or uninstalled from the command line, the install file log will not be created by default.

► *To install Kaspersky Embedded Systems Security 2.2 with the log file created 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 contains description of Kaspersky Embedded Systems Security 2.2 administration tools set, and special aspects of Kaspersky Embedded Systems Security 2.2 installation and uninstallation using a wizard (see Section "Installing and uninstalling the application using a wizard" on page 36), command line (see Section "Installing and uninstalling the application from the command line" on page 47), via Kaspersky Security Center (see Section "Installing and uninstalling the application using Kaspersky Security Center" on page 52) and via Active Directory® group policy (see Section "Installing and uninstalling via Active Directory group policies" on page 57).

Before starting to install Kaspersky Embedded Systems Security 2.2, plan its main stages.

1. Determine which administration tools will be used to manage and configure Kaspersky Embedded Systems Security 2.2.
2. Select the necessary application components for installation (see Section "Kaspersky Embedded Systems Security 2.2 software components and their codes for Windows Installer service" on page 20).
3. Select installation method.

In this section

Selecting administration tools

Determine the administration tools that will be used to configure Kaspersky Embedded Systems Security 2.2 settings and to manage it. Kaspersky Embedded Systems Security 2.2 can be managed using the Application Console, command-line utility, and Kaspersky Security Center Administration Console.

Kaspersky Embedded Systems Security 2.2 Console

Kaspersky Embedded Systems Security 2.2 Console is an isolated snap-in added to the Microsoft Management Console. Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 is installed.

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

Command line utility

You can manage Kaspersky Embedded Systems Security 2.2 from the command line of a protected computer.

The command line utility is included in the Kaspersky Embedded Systems Security 2.2 software components group.

Kaspersky Security Center

If the Kaspersky Security Center application is used for centralized management of anti-virus protection of computers at your company, you can manage Kaspersky Embedded Systems Security 2.2 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 2.2 software components group. It ensures Kaspersky Embedded Systems Security 2.2 communication with the Network Agent. Install the module for integration with Kaspersky Security Center Network Agent onto the protected computer.
- **Kaspersky Security Center Network Agent**. Install this component on each protected computer. This component supports interaction between Kaspersky Embedded Systems Security 2.2 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 2.2 Administration Plug-in**. Additionally, install the Administration Plug-in for managing Kaspersky Embedded Systems Security 2.2 via the Administration Console on the computer where the Kaspersky Security Center Administration Server is installed. This ensures the application management interface via the Kaspersky Security Center. The Administration Plug-in installation file, \product\klcfginst.exe, is included in the Kaspersky Embedded Systems Security 2.2 distribution kit.

Selecting the installation type

After specifying the software components for installation of Kaspersky Embedded Systems Security 2.2 (see Section "Kaspersky Embedded Systems Security 2.2 software components and their codes for Windows Installer service" on page 20), you need to select the application installation method.

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

- Whether special Kaspersky Embedded Systems Security 2.2 installation settings will need to be set, or whether the recommended installation settings (see Section "Installation and uninstallation settings and command line options for Windows Installer service" on page 27) will be used.
- Will the installation settings will be the same for all computers or specific to each computer.

Kaspersky Embedded Systems Security 2.2 can be installed interactively using the Setup Wizard or in silent mode without user participation, and invoked by running the installation package file with setup settings from the command line. A centralized remote installation of Kaspersky Embedded Systems Security 2.2 can be performed using Active Directory group policies or using the Kaspersky Security Center remote installation task.

Kaspersky Embedded Systems Security 2.2 can be installed on a single computer, configured for operation and its settings saved to a configuration file; the file created can then be used to install Kaspersky Embedded Systems Security 2.2 on other computer (this possibility does not apply 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 2.2 components (see Section "Kaspersky Embedded Systems Security 2.2 software components" on page 21) on a protected computer out of a \product\setup.exe file included into distribution kit.
- Kaspersky Embedded Systems Security 2.2 Console (see Section "Kaspersky Embedded Systems Security 2.2 Console installation" on page 38) from the \client\setup.exe file of 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 2.2 will be installed with the default settings. Kaspersky Embedded Systems Security 2.2 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 2.2 and the Application Console (see Section "Installing and uninstalling the application from the command line" on page 47).

Centralized installation via the Kaspersky Security Center

If the Kaspersky Security Center is used in your network for managing networked computers' anti-virus protection, Kaspersky Embedded Systems Security 2.2 can be installed on multiple computers by using the Kaspersky Security Center remote installation task.

The computers on which you wish to install Kaspersky Embedded Systems Security 2.2 via Kaspersky Security Center (see Section "Installing and uninstalling the application using Kaspersky Security Center" on page 52) may either be located in the same domain as the Kaspersky Security Center as well as in a different domain, or not belong to any one domain at all.

Centralized installation using Active Directory group policies

Active Directory group policies can be used to install Kaspersky Embedded Systems Security 2.2 on the protected computer. The Application Console can be installed on the protected computer or administrator's workstation.

Kaspersky Embedded Systems Security 2.2 can be installed using just the recommended installation settings.

The computers on which Kaspersky Embedded Systems Security 2.2 is installed using Active Directory group policies (see Section "Installing and uninstalling via Active Directory group policies" on page 57) must be located in the same domain and in 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 contains description of the Kaspersky Embedded Systems Security 2.2 and the Application Console installation and uninstallation processes by means of installation wizard, as well as information about additional Kaspersky Embedded Systems Security 2.2 configuration and actions to be performed upon installation.

In this section

Installing using the Setup Wizard

The following sections contain information about the installation of Kaspersky Embedded Systems Security 2.2 and the Application Console.

► *To install and proceed with using Kaspersky Embedded Systems Security 2.2, take the following steps:*

1. Install Kaspersky Embedded Systems Security 2.2 on a protected computer.
2. Install the Application Console on the computers from which you intend to manage Kaspersky Embedded Systems Security 2.2.
3. If the Application Console has been installed on any computer in the network, other than protected computer, perform the additional adjustment to allow the Application Console users to manage Kaspersky Embedded Systems Security 2.2 remotely.
4. Perform actions after Kaspersky Embedded Systems Security 2.2 installation.

In this section

Kaspersky Embedded Systems Security 2.2 installation

Before installing Kaspersky Embedded Systems Security 2.2, 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 is registered in 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 settings for Kaspersky Embedded Systems Security 2.2 installation. The Kaspersky Embedded Systems Security 2.2 installation process can be stopped at any step of the Setup Wizard. To do so, press 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 Windows Installer service" on page 27).

► *To install Kaspersky Embedded Systems Security 2.2 using an installation wizard:*

1. Start the welcome file setup.exe on the computer.
2. In the window that opens, in the **Installation** section, click the **Install Kaspersky Embedded Systems Security 2.2** link.
3. In the welcome screen of the Kaspersky Embedded Systems Security 2.2 Setup Wizard, click the **Next** button.

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

   > If you do not accept EULA and/or Privacy Policy the installation will be aborted.
6. Click the **Next** button.

   The **Custom installation** window opens.
7. Select the components to be installed.

   By default, all Kaspersky Embedded Systems Security 2.2 components are included in recommended installation set, except the Firewall management component.

   > The SNMP protocol support component of Kaspersky Embedded Systems Security 2.2 will only appear in the list of components suggested for installation if the Microsoft Windows SNMP service is installed on the computer.
8. To cancel all changes, press the **Reset** button in the **Custom installation** window. Click the **Next** button.
9. In the **Select a destination folder** window:
   - If required, specify a folder to which Kaspersky Embedded Systems Security 2.2 files will be copied.
   - If required, review the information about available space on local drives by clicking the **Disk** button.

   Click the **Next** button.
10. 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.
11. In the opened **Import settings from configuration file** window:

    a. Specify the configuration file to import Kaspersky Embedded Systems Security 2.2 settings from an existing configuration file created in any compatible previous version of the application.

    b. Press the **Next** button.

12. 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 2.2 key file for application activation.
    - If you want to activate the application later, press the **Next** button.
    - If a key file has been saved beforehand in the \server folder of the distribution kit, the name of this file will be displayed in the **Key** field.

      > To add the 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 2.2 displays the calculated date of license expiry. The license term runs from the time when you add a key and expires no later than the key file expiration date.

      Click **Next** button to apply the key in the application.
13. In the **Ready to install** window, press the **Install** button. The wizard will start the installation of Kaspersky Embedded Systems Security 2.2 components.
14. The **Installation complete** window opens when installation is completed.
15. Select the **View Release Notes** check box to view information about the release after the Setup Wizard is done.
16. Click **OK**.

The Setup Wizard's window closes. Once installation is completed, Kaspersky Embedded Systems Security 2.2 is ready for use if you have added the activation key.

Kaspersky Embedded Systems Security 2.2 Console installation

Follow the instructions of the Setup Wizard to adjust the 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 from which you are running the Setup Wizard is included in the administrators group on the computer.
2. Run the setup.exe welcome file on the computer.

   The welcome window opens.
3. Click on the **Install Kaspersky Embedded Systems Security 2.2 Console** link.

   The Setup Wizard's welcome window opens. Click the **Next** button.
4. Review the terms of the End User License Agreement and Privacy Policy in the opened window, and select **the terms and conditions of this EULA** and **Privacy Policy describing the handling of data** in order to proceed with the installation. Click the **Next** button.

   The **Advanced installation settings** window opens.
5. In the **Advanced installation settings** window:
   - If you intend to use the Application Console to manage Kaspersky Embedded Systems Security 2.2 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 components of "Administration Tools" set from a list.

     By default, all the components are installed.

  c. Click the **Next** button.

> You can find more detailed information about Kaspersky Embedded Systems Security 2.2 components (see Section "Kaspersky Embedded Systems Security 2.2 software components and their codes for Windows Installer service" on page 20).

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

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

   b. Click the **Next** button.

7. In the **Ready to install** window, press the **Install** button.

   The wizard will begin installing the selected components.

8. Click **OK**.

The Setup Wizard's window closes. The Application Console will be installed on a protected computer.

If the "Administration tools" set has been installed on any computer in the network, other than protected computer, adjust the advanced settings (see Section "Advanced settings after installation of the Application Console on another computer" on page 39).

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 protected computer, perform the actions described below to allow users to manage Kaspersky Embedded Systems Security 2.2 remotely:

- Add Kaspersky Embedded Systems Security 2.2 users to the ESS Administrators group on the protected computer.
- Allow network connections for Kaspersky Security Management Service (kavfsgt.exe) (see Section "About access permissions for the Kaspersky Security Management Service" on page 77), if the protected computer uses Windows Firewall or a third-party firewall.
- If the **Allow remote access** check box is not selected during the Application Console installation on a computer under Microsoft Windows, you should manually allow network connections for the Application Console via computer's firewall.

Allowing network connections for the Application Console

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

The Application Console on the remote computer uses DCOM protocol to receive information about Kaspersky Embedded Systems Security 2.2 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 the Windows Firewall open TCP port 135 and allow network connections for the executable file of the Kaspersky Embedded Systems Security 2.2 remote management process, kavfsrcn.exe.

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

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

Same steps should be applied for configuring any other software or hardware Firewall.

If the Application Console was opened while you were configuring the connection between the protected computer and the computer on which the Application Console is installed, close the Application Console, wait till the Kaspersky Embedded Systems Security 2.2 remote management process kavfsrcn.exe is finished, and restart the the Application Console. The new connection settings are applied.

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

1. On the remote computer with the Kaspersky Embedded Systems Security 2.2 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** group of settings.

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**.

► *To open TCP port 135 in the Windows Firewall and to allow network connections for the Kaspersky Embedded Systems Security 2.2 remote management process executable file:*

1. Close the Kaspersky Embedded Systems Security 2.2 Console on the remote computer.
2. Perform one of the following steps:
   - In Microsoft Windows XP or Microsoft Windows Vista®:
     a. In Microsoft Windows XP SP2 or later, select **Start** > **Windows Firewall**.

        In Microsoft Windows Vista, select **Start** > **Control Panel** > **Windows Firewall** and in the **Windows Firewall** window select the command **Change settings**.

     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 2.2 DCOM, and specify port number (135) in the **Port name** field.
     d. Select **TCP** protocol.
     e. Click **OK**.
     f. Click the **Add** button on the **Exclusions** tab.
   - In 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. This is located in the folder specified as a destination folder during the installation of Kaspersky Embedded Systems Security 2.2 Console using Microsoft Management Console.
4. Click **OK**.
5. Click the **OK** button in the **Windows Firewall (Windows Firewall settings)** window.

► *Add the Windows Firewall outbound rule:*

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 2.2 installation

Kaspersky Embedded Systems Security 2.2 starts the protection and scan tasks immediately after installation if you have activated the application. If **Enable real-time protection after installation of application** (default option) was selected during installation of Kaspersky Embedded Systems Security 2.2, the application scans computer's file system objects when they are accessed. Kaspersky Embedded Systems Security 2.2 will run the Critical Areas Scan task every Friday at 20:00.

We recommend taking the following steps after installing Kaspersky Embedded Systems Security 2.2:

- Start the application databases update task. After installation Kaspersky Embedded Systems Security 2.2 will scan objects using the database included in the application distribution kit.

  > We recommend updating Kaspersky Embedded Systems Security 2.2 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 installing Kaspersky Embedded Systems Security 2.2.
- Configure administrator notifications about Kaspersky Embedded Systems Security 2.2 events.

In this section

Starting and configuring Kaspersky Embedded Systems Security 2.2 databases update task

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

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

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

1. Start the the 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 2.2** > **Administration Tools** > **Kaspersky Embedded Systems Security 2.2 Console**.
   - If the Application Console has been started not on a protected computer, connect to the protected computer:
     a. Open the context menu of the **Kaspersky Embedded Systems Security** node in the 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 77), 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. Do the following:
   a. If Web Proxy Auto-Discovery Protocol (WPAD) is not configured on your network to detect proxy server settings automatically in the LAN, specify the proxy server settings: in the **Proxy server settings** section, select the **Use specified proxy server settings** check box, enter the address in the **Address** field, and enter the port number for the proxy server in the **Port** field.
   b. If your network requires authentication when accessing the proxy server, select the necessary authentication method in the drop-down list of the **Proxy server authentication settings** section:
      - **Use NTLM authentication**, if the proxy server supports the built-in Microsoft Windows NTLM authentication. Kaspersky Embedded Systems Security 2.2 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 2.2 will use the account specified for accessing 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 **Task settings** window.

The settings for connecting with 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 2.2 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 task status **Running** is displayed in the workspace.

► *To view the task log,*

in the details pane of the **Critical areas scan** node, click the **Open log** link.

Modifying set of components and recovering Kaspersky Embedded Systems Security 2.2

Kaspersky Embedded Systems Security 2.2 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 the application management access is password protected, Kaspersky Embedded Systems Security 2.2 requests password when you attempt to delete or modify the set of components on the additional step in Setup Wizard.

► *To modify the set of Kaspersky Embedded Systems Security 2.2 components:*

1. In the **Start** menu, select **All programs > Kaspersky Embedded Systems Security 2.2 > Modify or Remove**.

   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 to Kaspersky Embedded Systems Security 2.2 or that you want to remove. To do this, perform the following actions:

   - To change the set of components, click the button next to the name of the selected component, and 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, and in the context menu select **Component will be unavailable**.

   Click the **Install** 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 2.2 components will be modified based on the specified settings.

If problems occur in the operation of Kaspersky Embedded Systems Security 2.2 (Kaspersky Embedded Systems Security 2.2 crashes; tasks crash or do not start), it is possible to attempt to restore the Kaspersky Embedded Systems Security 2.2. You can perform a restore while saving the current settings of Kaspersky Embedded Systems Security 2.2, or you can select an option to reset all Kaspersky Embedded Systems Security 2.2 settings to their default values.

► *To recover Kaspersky Embedded Systems Security 2.2 after the application or a task crashes, take the following steps:*

1. In the **Start** menu, select **All programs > Kaspersky Embedded Systems Security 2.2 > Modify or Remove**.

   The Setup Wizard's **Modify, repair or remove** window opens.

2. Select **Repair installed components**. Click the **Next** button.

   This opens the **Repair installed components** window.

3. In the **Repair installed components** window, select the **Restore recommended application settings** check box if you want to reset the configured application settings and restore Kaspersky Embedded Systems Security 2.2 with its default settings. Click the **Install** button.

4. In the **Ready to repair** window, confirm the repair operation by clicking the **Install** button.

5. In the window that opens upon completion of the repair operation, click the **OK** button.

Kaspersky Embedded Systems Security 2.2 will be restored based on the specified settings.

Uninstalling using the Setup Wizard

This section contains instructions on removing Kaspersky Embedded Systems Security 2.2 and the the Application Console from a protected computer using the Setup Wizard.

Kaspersky Embedded Systems Security 2.2 uninstallation

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

Kaspersky Embedded Systems Security 2.2 can be uninstalled from the protected computer using the Setup / Uninstallation Wizard.

After Kaspersky Embedded Systems Security 2.2 uninstallation from a protected computer a reboot may be required. Rebooting can be postponed.

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

If the application management access is password protected, Kaspersky Embedded Systems Security 2.2 requests password when you attempt to delete or modify the set of components on the additional step in Setup Wizard.

► *To uninstall Kaspersky Embedded Systems Security 2.2:*

1. In the **Start** menu, select **All programs > Kaspersky Embedded Systems Security 2.2 > Modify or Remove**.

   The Setup Wizard's **Modify, repair or remove installation** window opens.

2. Select **Remove software components**. Click the **Next** button.

   The **Advanced application uninstallation settings** window opens.

3. If necessary, in the **Advanced application uninstallation settings** window:

   a. Select the **Export quarantine objects** check box in order for Kaspersky Embedded Systems Security 2.2 to export objects that have been quarantined. The check box is cleared by default.

   b. Check the **Export Backup objects** check box, in order to export objects from Kaspersky Embedded Systems Security 2.2 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 being restored. By default, the objects will be exported to %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security 2.2\Uninstall.

      Click the **Next** button.

4. In the **Ready to uninstall** window, confirm the uninstallation by clicking the **Uninstall** button.

5. In the window that opens upon completion of uninstallation, click the **OK** button.

Kaspersky Embedded Systems Security 2.2 will be uninstalled from a protected computer.

Kaspersky Embedded Systems Security 2.2 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 you have uninstalled the Application Console, you do not need to restart the computer.

► *To uninstall the Application Console:*

1. In the **Start** menu, select **All programs > Kaspersky Embedded Systems Security > Administration tools > Modify or Remove**.
2. The wizard's **Modify, repair or remove** window opens.

   Select **Remove software components** and click the **Next** button.
3. The **Ready to uninstall** window opens. Click the **Remove** button.

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

Removal 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 2.2 from the command line and contains examples of commands to install and uninstall Kaspersky Embedded Systems Security 2.2 from the command line, and examples of commands to add and remove Kaspersky Embedded Systems Security 2.2 components from the command line.

In this section

About installing and uninstalling Kaspersky Embedded Systems Security 2.2 from command line

Kaspersky Embedded Systems Security 2.2 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 \client\esstools.msi installation package.

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

If one of the \product\ess_x86(x64).msi files is run on the protected computer without additional keys, Kaspersky Embedded Systems Security 2.2 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 2.2

This section provides examples of commands used to install Kaspersky Embedded Systems Security 2.2.

> 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 for Kaspersky Embedded Systems Security 2.2 installation from file setup.exe

► *To install Kaspersky Embedded Systems Security 2.2 with the recommended installation settings without interaction with the user, run the following command:*

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

► *To install Kaspersky Embedded Systems Security 2.2 with the following settings:*

- install Real-Time File Protection and On-Demand Scan components only;
- do not run Real-Time Protection when starting Kaspersky Embedded Systems Security 2.2;
- do not exclude from the scan files that Microsoft Corporation recommends to exclude;

perform the following command:

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

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

- *To install Kaspersky Embedded Systems Security 2.2 with the recommended installation settings without interaction with the user, run the following command:*

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

- *To install Kaspersky Embedded Systems Security 2.2 with the recommended installation settings; display the installation interface, run the following command:*

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

- *In order to install Kaspersky Embedded Systems Security 2.2 with activation 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 2.2 with a preliminary scan of active processes and boot sectors of the local disks, run the following command:*

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

- *To install Kaspersky Embedded Systems Security 2.2 while saving its files in the destination folder C:\ESS, execute the following command:*

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

- *To install Kaspersky Embedded Systems Security 2.2: save the installation log file with name ess.log in the folder in which the msi file of the Kaspersky Embedded Systems Security 2.2 installation package is stored, and execute the following command:*

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

- *To install Kaspersky Embedded Systems Security 2.2 Console, run the following command:*

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

- *To install Kaspersky Embedded Systems Security 2.2 with activation using the key file C:\0000000A.key; configure Kaspersky Embedded Systems Security 2.2 according to the settings described in the configuration file C:\settings.xml, and execute the following command:*

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

- *To install the application patch when Kaspersky Embedded Systems Security 2.2 is password-protected execute the following command:*

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

Actions to perform after Kaspersky Embedded Systems Security 2.2 installation

Kaspersky Embedded Systems Security 2.2 starts the protection and scan tasks immediately after installation if you have activated the application. If you selected **Enable real-time protection after installation of application** during installation of Kaspersky Embedded Systems Security 2.2, the application scans computer file system objects when they are accessed. Kaspersky Embedded Systems Security 2.2 will run the Critical Areas Scan task every Friday at 8 p.m.

We recommend taking the following steps after installing Kaspersky Embedded Systems Security 2.2:

- Start Kaspersky Embedded Systems Security 2.2 databases update task. After installation Kaspersky Embedded Systems Security 2.2 will scan objects using the database included in its distribution kit. We recommend updating Kaspersky Embedded Systems Security 2.2 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, updates of Kaspersky Embedded Systems Security 2.2 databases 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 installing Kaspersky Embedded Systems Security 2.2.

  ► *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 2.2 events.

Adding / removing components. Sample commands

The Applications Launch Control 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 2.2 components.

► *To add the On-demand scan component to already installed components, run the following command:*

```
msiexec /i ess.msi ADDLOCAL=Oas,Ods /qn EULA=1 PRIVACYPOLICY=1
```

or

```
\server\setup.exe /s /p "ADDLOCAL=Oas,Ods" /p EULA=1 /p PRIVACYPOLICY=1
```

If you enumerate the components you want to install along with the already installed components, Kaspersky Embedded Systems Security 2.2 will reinstall the existing components.

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

```
msiexec /i ess.msi "ADDLOCAL=Oas,AppCntrl,Ksn,AntiExploit,DevCtrl,Firewall,
LogInspector,AKIntegration,PerfMonCounters,SnmpSupport,Shell,TrayApp,AVPro
tection,RamDisk REMOVE=Ods,Fim" /qn
```

Kaspersky Embedded Systems Security 2.2 uninstallation. Sample commands

► *To uninstall Kaspersky Embedded Systems Security 2.2 from the protected computer, run the following command:*

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

or

- For 32-bit operating systems:

```
msiexec /x {D8279E25-E44F-4164-8651-10123E2E30EA} /qn
```

- For 64-bit operating systems:

```
msiexec /x {E8584EDC-0675-4784-96E5-FD10C26A613E} /qn
```

► *To uninstall Kaspersky Embedded Systems Security 2.2 Console, run the following command:*

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

or

- For 32-bit operating systems:

```
msiexec /x {A727008F-F8CC-4B35-848A-1AECEEF22178} /qn
```

- For 64-bit operating systems:

```
msiexec /x {D978C311-2D2D-41A3-8158-BDF97149CCD4} /qn
```

► *To uninstall Kaspersky Embedded Systems Security 2.2 from a protected computer on which password protection is enabled, perform the following command:*

- For 32-bit operating systems:

```
msiexec /x {D8279E25-E44F-4164-8651-10123E2E30EA} UNLOCK_PASSWORD=*** /qn
```

- For 64-bit operating systems:

```
msiexec /x {E8584EDC-0675-4784-96E5-FD10C26A613E} UNLOCK_PASSWORD=*** /qn
```

Return codes

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

Table 13. Return codes

Code	Description
1324	The destination folder name contains invalid characters.
25001	Insufficient rights to install Kaspersky Embedded Systems Security 2.2. To install the application, start the installation wizard with local administrator rights.
25003	Kaspersky Embedded Systems Security 2.2 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 2.2 via Kaspersky Security Center. It also describes how to install and uninstall Kaspersky Embedded Systems Security 2.2 via Kaspersky Security Center and actions after installing Kaspersky Embedded Systems Security 2.2.

In this section

General information about installing via Kaspersky Security Center

You can install Kaspersky Embedded Systems Security 2.2 via Kaspersky Security Center using the remote installation task.

After the remote installation task is complete, Kaspersky Embedded Systems Security 2.2 will be installed with identical settings on several computers.

All computers can be combined in a single administration group and a group task created to perform Kaspersky Embedded Systems Security 2.2 installation on the computers of this group.

You can create a task to remotely install Kaspersky Embedded Systems Security 2.2 on a set of computers that are not in the same administration group. When creating this task you must generate a list of the individual computers on which Kaspersky Embedded Systems Security 2.2 should be installed.

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

Rights to install or uninstall Kaspersky Embedded Systems Security 2.2

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 computers on which Kaspersky Embedded Systems Security 2.2 is to be installed (no matter in which domain the computers are located and 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 2.2 using a remote installation task. Before installing the Network Agent, make sure that the account that 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 2.2 are in the same domain as the Administration Server, and the Administration Server is registered under 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 from which the Administration Server runs.

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

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

Kaspersky Embedded Systems Security 2.2 installation procedure 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 2.2 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 2.2 distribution kit).
- Kaspersky Security Center Network Agent is installed on protected computers. If Kaspersky Security Center Network Agent is not installed on the protected computers, you can install it together with Kaspersky Embedded Systems Security 2.2 using a remote installation task.

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

► *To install Kaspersky Embedded Systems Security 2.2 with the help of remote installation task:*

1. Start the Kaspersky Security Center Administration Console.
2. In Kaspersky Security Center, expand the **Remote installation** node and in the **Installation packages** child node select the **Create installation package for a Kaspersky Lab application** option.
3. Enter the installation package name.
4. Specify the ess.kud file from the Kaspersky Embedded Systems Security 2.2 distribution kit as the installation package file.

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

   You must accept the License Agreement and the Privacy Policy to proceed.
6. To change the set of Kaspersky Embedded Systems Security 2.2 components to be installed (see Section "Modifying set of components and recovering Kaspersky Embedded Systems Security 2.2" on page 44) and the default installation settings (see Section "Installation and uninstallation settings and command line options for Windows Installer service" on page 27) in the installation package:
   a. In Kaspersky Security Center, expand the **Remote installation** node.
   b. In the **Installation packages** child node workspace open the context menu of the created Kaspersky Embedded Systems Security 2.2 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** group of settings select check boxes next to the names of the Kaspersky Embedded Systems Security 2.2 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**.

7. In the **Installation packages** node create a task to remotely install Kaspersky Embedded Systems Security 2.2 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*.

8. Run the remote installation task for Kaspersky Embedded Systems Security 2.2.

Kaspersky Embedded Systems Security 2.2 will be installed on the computers specified in the task.

Actions to perform after Kaspersky Embedded Systems Security 2.2 installation

After Kaspersky Embedded Systems Security 2.2 is installed we recommend that Kaspersky Embedded Systems Security 2.2 databases on the computers are updated, and that a Critical Areas Scan of the computers is performed, if no anti-virus applications with enabled Real-Time Protection function were installed on the computers before the installation of Kaspersky Embedded Systems Security 2.2.

If the computers on which Kaspersky Embedded Systems Security 2.2 was installed are unified in a single 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 2.2 was installed. Set Kaspersky Security Center Administration Server as the update source.
2. Create an On-Demand Scan group task with the Critical Areas Scan task status. Kaspersky Security Center evaluates the security status of each computer in the group based on the results of the execution 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 created policy's properties on the **System tasks** tab, deactivate the scheduled start of system scan tasks as required and the database update tasks on the administration group's computers.

You can also configure administrator notifications about Kaspersky Embedded Systems Security 2.2 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 **Remote installation** node, and in the **Installation Packages** child node create a new installation package on the basis of the client\setup.exe file. While creating a new installation package:
   - In the **Selecting the distribution package for installation** window select client\setup.exe file from the Kaspersky Embedded Systems Security 2.2 distribution kit folder and select the **Copy updates from repository to installation package** check box.
   - 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, proceed as follows:

     ```
     /s /p "ADDLOCAL=MmcSnapin INSTALLDIR=C:\KasperskyConsole EULA=1
     PRIVACYPOLICY=1"
     ```
2. In the **Installation packages** 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*.
3. Run the created remote installation task.

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

Uninstalling Kaspersky Embedded Systems Security 2.2 via Kaspersky Security Center

If the Kaspersky Embedded Systems Security 2.2 management access on network computers is password protected, enter the password when creating a multiple applications uninstallation task. If the password protection is not managed centrally by the application will be successfully uninstalled from the access protected computers, on which the entered password matched the set value. Kaspersky Embedded Systems Security 2.2 will not be uninstalled from the rest computers.

► *In order to uninstall Kaspersky Embedded Systems Security 2.2, take the following steps in the Kaspersky Security Center Administration Console:*

1. In the Kaspersky Security Center Administration Console, create and start the application removal task.
2. In the task, select the uninstallation method (similar to selecting the installation method; see the previous section) and specify an account whose rights the Administration Server will use to address the computers. You can uninstall Kaspersky Embedded Systems Security 2.2 only with default uninstallation settings (see Section "Installation and uninstallation settings and command line options for Windows Installer service" on page 27).

Installing and uninstalling via Active Directory group policies

This section describes installing and uninstalling Kaspersky Embedded Systems Security 2.2 via Active Directory group polices. It also contains information about actions after installing Kaspersky Embedded Systems Security 2.2 through group policies.

In this section

Installing Kaspersky Embedded Systems Security 2.2 via Active Directory group policies

You can install Kaspersky Embedded Systems Security 2.2 on several computers via the Active Directory group policy. You can install the Application Console the same way.

Computers on which you wish to install Kaspersky Embedded Systems Security 2.2 or the Application Console must be in a single domain and a single organized unit.

The operating systems on the computers on which you wish to install Kaspersky Embedded Systems Security 2.2 with the help of the policy must be of the same version (32-bit or 64-bit).

You must have domain administrator rights.

To install Kaspersky Embedded Systems Security 2.2, 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 2.2 (or the Application Console):*

1. Save the msi file of the installation package that corresponds to the word size (32- or 64-bit) of the installed version of the Microsoft Windows operating system, in the public folder on the domain controller.
2. On the domain controller create a new policy for the group that the computers belong to.
3. Using the **Group Policy Object Editor** create a new installation package in the **Computer Configuration** node. Specify the path to the msi file of the installation package of Kaspersky Embedded Systems Security 2.2 (or the Application Console) in the UNC format (Universal Naming Convention).
4. 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.
5. Apply the changes with the `gpupdate / force` command.

Kaspersky Embedded Systems Security 2.2 will be installed on the computers of the group after they have been restarted, and before logging into Microsoft Windows.

Actions to perform after Kaspersky Embedded Systems Security 2.2 installation

After installing Kaspersky Embedded Systems Security 2.2 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 2.2 installation" on page 42) from the Application Console.

You can also configure administrator notifications about Kaspersky Embedded Systems Security 2.2 events.

Uninstalling Kaspersky Embedded Systems Security 2.2 via Active Directory group policies

If you installed Kaspersky Embedded Systems Security 2.2 (or the Application Console) on the group computers using the Active Directory group policy, you may use this policy to uninstall the Kaspersky Embedded Systems Security 2.2 (or the Application Console).

You can uninstall the application only with default uninstallation parameters.

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

If the application management access is password protected, Kaspersky Embedded Systems Security 2.2 uninstallation using Active Directory group policies is not available.

► *To uninstall Kaspersky Embedded Systems Security 2.2 (or the Application Console):*

1. Select the organizational unit on the domain controller from whose computers you wish to delete Kaspersky Embedded Systems Security 2.2 or the Application Console.
2. Select the policy created for the installation of Kaspersky Embedded Systems Security 2.2 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 2.2 (or the Application Console) installation package and select the **All tasks > Remove** command.
3. Select the removal method **Immediately uninstall the software from users and computers**.
4. Apply the changes with the `gpupdate / force` command.

Kaspersky Embedded Systems Security 2.2 is removed from the computers after they are restarted and before logging in to Microsoft Windows.

Kaspersky Embedded Systems Security 2.2 functions check. Using the EICAR test virus

This section describes the EICAR test virus and how to use the EICAR test virus to verify Kaspersky Embedded Systems Security 2.2's Real-Time Protection and On-Demand Scan features.

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 virus and does not contain program code to 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 on that drive is disabled.

The eicar.com file contains a line of text. When scanning the file Kaspersky Embedded Systems Security 2.2 detects a test threat in this text line, assigns the **Infected** status to this 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 in order to check how Kaspersky Embedded Systems Security 2.2 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.

> In order to make sure that Kaspersky Embedded Systems Security 2.2 processes the eicar.com file with a prefix, in the **Objects protection** security settings section, set the **All objects** value for the Kaspersky Embedded Systems Security 2.2 Real-Time File Protection tasks and Default On-Demand Scan tasks.

Table 14. Prefixes in EICAR files

Prefix	File status after the scan and Kaspersky Embedded Systems Security 2.2 action
No prefix	Kaspersky Embedded Systems Security 2.2 assigns the **Infected** status to the object and deletes it.
SUSP–	Kaspersky Embedded Systems Security 2.2 assigns **Probably infected** status to the object (detected by the heuristic analyzer) and deletes it (probably infected objects are not disinfected).
WARN–	Kaspersky Embedded Systems Security 2.2 assigns **Probably infected** status to the object (the object's code partly matches the code of a known threat) and deletes it (probably infected objects are not disinfected).
CURE–	Kaspersky Embedded Systems Security 2.2 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".

Real-Time Protection and On-Demand Scan test

After installing Kaspersky Embedded Systems Security 2.2, you can confirm that Kaspersky Embedded Systems Security 2.2 finds objects containing malicious code. To check, you can use a test virus from EICAR (see Section "About the EICAR test virus" on page 59).

► *In order to check the Real-Time Protection feature, take the following steps:*

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

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

2. If you wish to check the functioning of network user notifications, 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 the 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 works correctly if the following conditions are met:

- The eicar.com file has been deleted from the protected computer.
- In the the Application Console, the task log was given the status **Critical**. A line has appeared in the log with information about a threat in the eicar.com file. (To view the task log, in the 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 log** link).

- A Microsoft Windows Messenger Service message will have appeared on the computer from which you copied the file, as follows: `Kaspersky Embedded Systems Security 2.2 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 Microsoft Windows Messenger Service is functioning on the computer from which you have copied the eicar.com file.

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

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

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

2. Open the Application Console.
3. Do the following:
   a. Expand the **On-Demand Scan** node in the 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 format (Universal Naming Convention).
   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 works as it should if the following conditions are met:

- The eicar.com file has been deleted from the computer's hard drive.
- In the the Application Console, the task log was given the status **Critical**; in the execution log of the task Critical Areas Scan a line appeared with information on a threat in the eicar.com file. (To view the task log, in the 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 log** link).

Application interface

You can control Kaspersky Embedded Systems Security 2.2 through the local Application Console and the Administration Plug-in. Actions with the local Application Console are described in the *Kaspersky Embedded Systems Security 2.2 User's Guide*. The Kaspersky Security Center Administration Console interface is used to take 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 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 2.2 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 term of application use depend on the type of license under which the application has been activated.

The application is activated using a key file for a purchased commercial license.

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

Kaspersky Embedded Systems Security 2.2 offers two types of 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 2.2 databases cannot be updated). To continue using all the features of Kaspersky Embedded Systems Security 2.2, 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 the 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 2.2. You receive the activation code at the email address that you provided when you bought Kaspersky Embedded Systems Security 2.2.

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 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 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 key file

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

You receive a key file at the email address that you provided when you bought Kaspersky Embedded Systems Security 2.2.

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

You can recover a key file if it is accidentally deleted. You may need a key file to register with Kaspersky CompanyAccount.

To recover a key file, you should perform any of the following actions:

- Contact Technical Support https://support.kaspersky.com/.
- Obtain a key file on the Kaspersky Lab website based on your existing activation code.

About data provision

The License Agreement for Kaspersky Embedded Systems Security 2.2, 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, unique 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 2.2 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 2.2 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 2.2 locally processes and stores a sequence of data types on the protected computer:

- Information about scanned files and detected objects, for example, names and attributes of processed files and full paths to them on the scanned media, 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.
- 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 2.2 processes and stores data as part of the application's basic functionality, particularly for logging application events and receiving diagnostic data. Locally processed data is protected in accordance with the configured and applied application settings.

Kaspersky Embedded Systems Security 2.2 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 on the media where 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 stored on a local computer is removed after Kaspersky Embedded Systems Security 2.2 uninstallation, except files with diagnostics information (trace and dump files), and also the Windows Event Log records of the application activity. You need to manually remove these files. You can find detailed information about configuring diagnostics processes in the corresponding sections of this Guide.

When uninstalling the application you can save the contents of backup and quarantine storages.

Activate application with key

You can activate Kaspersky Embedded Systems Security 2.2 by applying a key.

If an active key has already been added for Kaspersky Embedded Systems Security 2.2 and you add another key as the active key, the new key replaces the key added previously. The active key installed earlier is removed.

If an additional key has already been added for Kaspersky Embedded Systems Security 2.2 and you add another key as an additional one, the new key replaces the key added previously. The additional key installed earlier is removed.

If an active key and an additional key have already been added for Kaspersky Embedded Systems Security 2.2 and you add a new key as the active key, the new key replaces the active key added previously; the additional key is not deleted.

► *To activate Kaspersky Embedded Systems Security 2.2:*

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. To add a key as an additional select the **Use as additional key** check box.

4. Click **OK**.

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

Viewing information about current license

Viewing the licensing information

Information about the current license is displayed in the details pane of the **Kaspersky Embedded Systems Security** node of the Application Console. Key status can take the following values:

- **Checking the key status** – Kaspersky Embedded Systems Security 2.2 is checking the added key file or activation code applied and waiting for a response about the current key status.
- **License expiration date** – Kaspersky Embedded Systems Security 2.2 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 or activation code have been added.
  - The added key has been black-listed and is about to be blocked.

- **Application not activated** – Kaspersky Embedded Systems Security 2.2 is not activated because the key has not been added or the activation code has not been applied. The status is highlighted in red.
- **License has expired** – Kaspersky Embedded Systems Security 2.2 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 2.2 is not activated because the terms of the End User License Agreement (see Section "About End User License Agreement" on page 63) have been violated. The status is highlighted in red.
- **Key is blacklisted** – the added key file has been blocked and blacklisted by Kaspersky Lab, for example, if the key was used by third parties to activate the application illegally. The status is highlighted in red.

Viewing information about the current license

► *To view the 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 15. General information about the license in the Licensing node

Field	Description
Activation code	Number of 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. Information in the Activation status column in the control panel of the Licensing node may have the following values: • **Applied** – if you have activated the application using an activation code or key. • **Activation** – if you have applied an activation code to activate the application, but the activation process has not been finalized yet. The status value changes to Applied after application activation has been completed and the contents of the details pane of the node have been refreshed. • **Activation error** – if application activation failed. You can view the cause of unsuccessful activation in the task log.
Key	The number of the key that you used to activate the application.
License type	License type: commercial.
Expiration date	Expiry date and time of the license associated with an active key.
Activation code status or key status	Activation code status or key status: Active or Additional.

► *To view the detailed information about license,*

select the **Licensing** node and open the context menu on the string 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 2.2 (see the table below).

Table 16. Detailed license information in the Properties: <Activation code status or key status> window

Field	Description
General tab	
Key	The number of the key that you used to activate the application.
Key addition date	Date when the key was added to the application.
License type	License type: commercial.
Days till expiration	Number of days remaining until the expiry of the license associated with the active key.
Expiration date	Expiry date and time of the license associated with an active key. If you activate the application under unlimited subscription, the field value is *Unlimited*. If Kaspersky Embedded Systems Security 2.2 is unable to determine the license expiry date, the field value is set to *Unknown*.
Application	The name of the application that was activated with the key or an activation code added.
Key usage restriction	Restriction on key usage (if any).
Eligible for technical support	Information on whether Kaspersky Lab or one of its partners will provide technical support for customers according to the license terms.
Additional tab	
Information about the license	Number and type of current license.
Support information	Contact details of Kaspersky Lab or of its partner providing technical support. This field may be empty if technical support is not provided.
Owner information	Information about the license customer: a customer name and the name of an organization for which the license was acquired.

Functional limitations upon license expiration

When the current license expires the following limitations in the work of functional components are applied:

- All tasks are stopped, except the Real-Time File Protection, On-Demand Scan and Application Integrity Control tasks.
- Start of any tasks except the Real-Time Protection, On-Demand Scan and Application Integrity Control tasks is denied. 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 (storage, logs, diagnostic information) will still be available.

Renewing license

By default, when the license has 14 days remaining before expiration, Kaspersky Embedded Systems Security 2.2 notifies you about this. In this case the status **License expiration date** in the details pane of the **Kaspersky Embedded Systems Security** node is highlighted in yellow.

You can renew the license expiration date before it comes to an end using an additional key or an activation code. This ensures that your server remains protected after expiration of the existing license and before you activate the application with a new license.

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

1. Purchase 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 or activation code will be added and automatically applied upon expiration of the current Kaspersky Embedded Systems Security 2.2 license.

Deleting key

You can remove the added key.

If an additional key has been added to Kaspersky Embedded Systems Security 2.2 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.

Starting and stopping Kaspersky Embedded Systems Security 2.2 Plug-in

This section contains information about starting and stopping the Kaspersky Embedded Systems Security 2.2 Administration Plug-in and the Kaspersky Security Service.

In this chapter

Starting the Kaspersky Embedded Systems Security 2.2 Administration Plug-in

No additional actions are required to start the Kaspersky Embedded Systems Security 2.2 Administration Plug-in in Kaspersky Security Center. After the Pug-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 and stopping Kaspersky Security Service

By default, Kaspersky Security Service starts automatically at the startup of the operating system. Kaspersky Security Service manages working processes in which Real-Time Computer Protection, Local activity control, On-Demand Scan and update tasks are executed.

By default when Kaspersky Embedded Systems Security 2.2 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 start 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 the application 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.

Access permissions for Kaspersky Embedded Systems Security 2.2 functions

This section contains information about permissions to manage Kaspersky Embedded Systems Security 2.2 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 2.2

By default, access to all Kaspersky Embedded Systems Security 2.2 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 2.2, as well as the SYSTEM group.

Users who have access to the **Edit** permissions function of Kaspersky Embedded Systems Security 2.2 can grant access to Kaspersky Embedded Systems Security 2.2 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 2.2 users cannot open the Application Console.

You can choose one of the following preset levels of Kaspersky Embedded Systems Security 2.2 access levels for a user or group of users:

- **Full control** – access to all application functions: ability to view and edit general Kaspersky Embedded Systems Security 2.2 settings, component settings, permissions of Kaspersky Embedded Systems Security 2.2 users, and also view Kaspersky Embedded Systems Security 2.2 statistics.
- **Edit** – access to all application functions except editing user permissions: ability to view and edit general settings of Kaspersky Embedded Systems Security 2.2 and Kaspersky Embedded Systems Security 2.2 component settings.
- **Read** – ability to view Kaspersky Embedded Systems Security 2.2 general settings, Kaspersky Embedded Systems Security 2.2 component settings, Kaspersky Embedded Systems Security 2.2 statistics, and Kaspersky Embedded Systems Security 2.2 user permissions.

You can also configure advanced access permissions (see Section "Configuring access permissions for Kaspersky Embedded Systems Security 2.2 and Kaspersky Security Service" on page 77): allow or block access to specific functions of Kaspersky Embedded Systems Security 2.2.

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 17. About access permissions for Kaspersky Embedded Systems Security 2.2 functions

User rights	Description
Task management	Ability to start / stop / pause / resume Kaspersky Embedded Systems Security 2.2 tasks.
Creating and deleting On-Demand Scan tasks	Ability to create and delete On-Demand Scan tasks.
Edit settings	Ability to: • Import Kaspersky Embedded Systems Security 2.2 settings from a configuration file. • Edit the application settings.
Read settings	Ability to: • View general Kaspersky Embedded Systems Security 2.2 settings and task settings. • Export Kaspersky Embedded Systems Security 2.2 settings to the configuration file. • View settings for task logs, system audit log, and notifications.
Manage storages	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 of each Kaspersky Embedded Systems Security 2.2 task.
Application licensing	Kaspersky Embedded Systems Security 2.2 can be activated or deactivated.
Uninstalling the application	Ability to uninstall Kaspersky Embedded Systems Security 2.2.
Read permissions	Ability to view the list of Kaspersky Embedded Systems Security 2.2 users and access privileges of each user.
Edit permissions	Ability to: • Edit the list of users with access to application management. • Edit user access permissions for Kaspersky Embedded Systems Security 2.2 functions.

About permissions to manage the Kaspersky Security Service

During installation, Kaspersky Embedded Systems Security 2.2 registers Kaspersky Security Service (KAVFS) in Windows, and internally enables functional components started at operating system startup. To reduce the risk of third-party access to application functions and security settings on the 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 as well as to the SERVICE and INTERACTIVE groups with read permissions and to the SYSTEM group with read and execute permissions.

> You cannot delete the SYSTEM user account or edit permissions for this account. If the SYSTEM user account permissions were edited, the maximum privileges are restored for this this account when you save the changes.

Users who have access to functions (see Section "About permissions to manage Kaspersky Embedded Systems Security 2.2" on page 73) of the Edit permissions level can grant access permissions for managing Kaspersky Security Service to other users registered on the protected computer or included in the domain.

You can choose one of the following preset levels of access permissions for a user or group of users of Kaspersky Embedded Systems Security 2.2 for managing 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 2.2 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 18. Delimitation of access permissions for Kaspersky Embedded Systems Security 2.2 functions

Feature	Description
Viewing service configurations	Viewing: ability to view Kaspersky Security Service general settings and user permissions.
Request service status from Service 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.
List dependent services	Ability to view a list of services on which the Kaspersky Security Service depends and which depend on the Kaspersky Security Service.

Feature	Description
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 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.

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 2.2 installation and is used for registering the Kaspersky Security Service as a PPL when the operating system starts. When the Kaspersky Security Service (kavfs.exe) 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 a 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 2.2 on a computer running PPL-supporting operating system, the permission management for Kaspersky Security Service (KAVFS) will not be available.

The Kaspersky Security Service starts all child processes as PPLs.

► *To install Kaspersky Embedded Systems Security 2.2 as PPL run the following command:*

```
msiexec /i ks4ws_x64.msi NOPPL=0 EULA=1 PRIVACYPOLICY=1 /qn
```

You can use the command line to configure the PPL usage.

About access permissions for the Kaspersky Security Management Service

You can review the list of Kaspersky Embedded Systems Security 2.2 services.

During installation, Kaspersky Embedded Systems Security 2.2 registers Kaspersky Security Management Service (KAVFSGT). 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 2.2 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 2.2 installation.

You can manage 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 2.2.

You can connect to Kaspersky Embedded Systems Security 2.2 from a local account if an account with the same name and password is registered on the protected computer.

Configuring access permissions for Kaspersky Embedded Systems Security 2.2 and Kaspersky Security Service

You can edit the list of users and user groups allowed to access Kaspersky Embedded Systems Security 2.2 functions and manage Kaspersky Security Service, and 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 and select the administration group for which you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring policy" on page 84).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in Application settings window of Kaspersky Security Center" on page 96).

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

3. In the **Supplementary** section, perform one of the following steps:
   - Select **User access permissions for application management** if you want to edit the list of users who have access permissions for managing Kaspersky Embedded Systems Security 2.2 functions.
   - Select **User access permissions for Security Service management** if you want to edit the list of users who have access permissions for managing Kaspersky Security Service.

     The **Permissions for Kaspersky Embedded Systems Security 2.2** group window opens.
4. 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 to whom you want to grant privileges.
   - 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.
5. Click the **Apply** button.

The selected users (groups) are added or removed.

► *To edit permissions of a user or group to manage Kaspersky Embedded Systems Security 2.2 or Kaspersky Security Service:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree and select the administration group for which you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring policy" on page 84).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in Application settings window of Kaspersky Security Center" on page 96).

     If a device is being managed by an active Kaspersky Security Center policy and this policy blocks changes to the application settings, these settings cannot be edited in the **Application settings** window.
3. In the **Supplementary** section, perform one of the following steps:
   - Select **Modify user rights of application management** if you want to edit the list of users who have access permissions for managing Kaspersky Embedded Systems Security 2.2 functions.
   - Select **Modify user rights of Kaspersky Security Service management** 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.
4. In the window that opens, in the **Groups** or users list select the user or group of users for whom you want to change permissions.

5. In the **Permissions for group "<User (Group)>"** section, select the **Allow** or **Block** check boxes for the following access levels:
   - **Full control**: full set of permissions to manage Kaspersky Embedded Systems Security 2.2 or Kaspersky Security Service.
   - **Read**:
     - The following permissions to manage Kaspersky Embedded Systems Security 2.2: **Retrieve statistics**, **Read settings**, **Read logs** and **Read permissions**.
     - The following permissions to manage 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 2.2, except **Edit permissions**.
     - The following permissions to manage Kaspersky Security Service: **Modify service settings**, **Read permissions**.
   - **Execution**: the following permissions to manage Kaspersky Security Service: **Starting service**, **Stopping service**, **Pause / Resume service**, **Read permissions**, **User defined requests to service**.
6. To configure advanced settings of permissions for a user or group (**Special permissions**), click the **Advanced** button.
   a. In the **Advanced security settings for Kaspersky Embedded Systems Security 2.2** window that opens, select the user or group that you need.
   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 opposite 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 2.2** window, click **OK**.
7. In the **Permissions for Kaspersky Embedded Systems Security** group window, click the **Apply** button.

The configured permissions for managing Kaspersky Embedded Systems Security 2.2 or Kaspersky Security Service are saved.

Password-protected access to Kaspersky Embedded Systems Security 2.2 functions

You can restrict access to application management and registered services by configuring user permissions (see Section "Access permissions for Kaspersky Embedded Systems Security 2.2 functions" on page 73). You can also set password protection in the Kaspersky Embedded Systems Security 2.2 settings for additional protection of the execution of critical operations.

Kaspersky Embedded Systems Security 2.2 requests a password when you attempt to access the following application functions:

- connection to the Application Console;
- uninstallation of Kaspersky Embedded Systems Security 2.2;
- modification of Kaspersky Embedded Systems Security 2.2 components;
- executing the command line commands.

The Kaspersky Embedded Systems Security 2.2 interface disguises the specified password on screen. Kaspersky Embedded Systems Security 2.2 stores the password as a checksum calculated when the password is specified.

You can export and import a password-protected application configuration. The configuration file, created as a result of exporting the protected application configuration, contains the password checksum and the value of the modifier used to pad the password string.

Do not change the checksum or modifier in the configuration file. Importing a password-protected configuration that has been changed manually may cause access to the application to be entirely blocked.

► *To protect access to Kaspersky Embedded Systems Security 2.2 functions, take the following steps:*

1. In the tree of the Administration Console of Kaspersky Security Center, expand the **Managed devices** node. Expand the administration group with the computers whose application settings you want to configure.
2. Perform one of the following actions in the details pane of the selected administration group:
   - To configure policy settings for a group of computers select the **Policies** tab and open **<Policy name> > Properties**.
   - If you want to configure application settings for a single computer, open the required settings in the **Application settings** (see Section "**Configuring local tasks in Application settings window of Kaspersky Security Center**" on page 96) window in Kaspersky Security Center.
3. In the **Security** section, click the **Settings** button.

   The **Security settings** window opens.
4. In the **Password protection settings** section, select the **Apply password protection** check box.

   The **Password** and **Confirm password** fields become active.
5. In the **Password** field, enter the value you want to use to protect access to Kaspersky Embedded Systems Security 2.2 functions.
6. In the **Confirm password** field, enter your password again.
7. Click **OK**.

The specified settings are saved. Kaspersky Embedded Systems Security 2.2 will request the specified password for accessing the protected functions.

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 change or reset the password specified in the application settings at any time.

► *To reset the password,*

clear the **Apply password protection** check box in the policy or application settings.

Password protection will be disabled. Kaspersky Embedded Systems Security 2.2 deletes the old password checksum from the application settings.

Enabling network connections for the Kaspersky Security Management Service

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

► *To allow network connections for the Kaspersky Security Management Service on the protected computer, take the following steps:*

1. On a protected computer running Microsoft Windows , select **Start > Control panel > Security > Windows Firewall**.
2. In the **Windows firewall settings** window, select **Change** settings.
3. In the list of predefined exclusions on the **Exclusions** tab select the following check boxes: **COM + Network access**, **Windows Management Instrumentation (WMI)** and **Remote Administration**.
4. Click the **Add Program** button.
5. Select the kavfsgt.exe file in the **Add program** window. This file is stored in the folder that you specified as the destination folder during installation of the Application Console.
6. Click **OK**.
7. Click **OK** in the **Windows Firewall settings** window.

Network connections for the Kaspersky Security Management Service on the protected computer will be allowed.

Creating and configuring policies

This section provides information on using Kaspersky Security Center policies for managing Kaspersky Embedded Systems Security 2.2 on several computers.

In this chapter

About policies

Global Kaspersky Security Center policies can be created for managing protection on several computers where Kaspersky Embedded Systems Security 2.2 is installed.

A policy enforces the Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 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 2.2 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 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.

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 2.2, the Quarantine and Backup settings, the level of detail for task logs, as well as user and administrator notifications about Kaspersky Embedded Systems Security 2.2 events.

► *In order to create a policy for a group of computers running the installed Kaspersky Embedded Systems Security 2.2, 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 2.2 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 **Browse** button and select the policy you want to apply.

   c. 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** section. 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** section. 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 Processing" on page 156).

- To edit the default settings of the Exploit Prevention component, click the **Settings** button in the **Exploit Prevention** section. 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 in the **Completing the Wizard** window of the Wizard.

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 2.2.

Configuring policy

In the **Properties: <Policy name>** window of an existing policy, you can configure general Kaspersky Embedded Systems Security 2.2 settings, quarantine and backup settings, Trusted Zone settings, Real-Time 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 2.2 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** child node 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 do not want the policy to be applied on all computers within the selected group.

   > The **Out-of-office policy** setting is not available when you manage Kaspersky Embedded Systems Security 2.2.

5. In the **Event notification**, **Application settings**, **Logs and Notifications**, **Supplementary**, **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.

> Detailed instructions on how to configure task settings and application functions via the Application Console are provided in the relevant sections of the *Kaspersky Embedded Systems Security 2.2 User's Guide*.

Sections with Kaspersky Embedded Systems Security 2.2 policy settings

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 notifications

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

- *Critical events*
- *Failure*
- *Warning*
- *Informational event*

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 19. Settings of the Application Settings section

Section	Options
Scalability and interface	In the **Scalability and interface** section, 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 and reliability** section, 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** section, 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 20. Settings of the Supplementary section

Section	Options
Trusted Zone	Click the **Settings** button on the **Trusted Zone** section 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	Click the **Settings** button to configure scan settings for removable USB drives.
User access permissions for application management	In this section, you can configure user rights and user group rights to manage Kaspersky Embedded Systems Security 2.2.
User access permissions for Security Service management	In this section, you can configure user rights and user group rights to manage the Kaspersky Security Service.

Section	Options
Storages	In the **Storages** subsection, click the **Settings** button to configure the following Quarantine and Backup 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 transmission of information about Quarantine and Backup objects to Administration Server.

Real-Time Computer Protection

Table 21. Settings of the Real-Time Computer Protection section

Section	Options
Real-Time File Protection	In the **Real-Time File Protection** section, 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 launch 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 configure dependable data exchange settings.
Exploit Prevention	In the **Exploit Prevention** section, 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 22. Settings of the Local activity control section

Section	Options
Applications Launch Control	In the **Applications Launch Control** section, 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 launch settings.
Device Control	In the **Device Control** section, 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 23. Settings of the Network activity control section

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

System Inspection

Table 24. Settings of the System Inspection section

Section	Options
File Integrity Monitor	In the **File Integrity Monitor** section 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 25. Settings of the Logs and Notifications section

Section	Options
Task logs	In the **Task logs** section, 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.

Section	Options
Event notifications	In the **Event notifications** section, you can click the **Settings** button to configure the following settings: • Specify the user notification settings for the *Object detected* event. • Specify the administrator notification settings for any event selected in the event list in the **Notification settings** section.
Interaction with the Administration Server	In the **Interaction with the Administration Server** section, you can click the **Settings** button to select the types of objects that Kaspersky Embedded Systems Security 2.2 will report to Administration Server.

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 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 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 2.2 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, Software Modules Integrity Check.
- 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 2.2 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 2.2 system tasks on the group of computers, select the **Properties** command.
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 (see Section "About policies" on page 82) 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.

Creating and configuring tasks using Kaspersky Security Center

This section contains information about Kaspersky Embedded Systems Security 2.2 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 89) 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

> The process of configuring the settings of Kaspersky Embedded Systems Security 2.2 functional components in Kaspersky Security Center is similar to local configuration of the settings of these components in the Application Console. Detailed instructions on how to configure task settings and application functions are provided in the relevant sections of the *Kaspersky Embedded Systems Security 2.2 User's Guide*.

► *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 and select the group for which you want to create a task.
     b. In the details pane, open the **Tasks** tab and select **Create a task**.
   - To create a task for a custom set of computers, in the **Device selections** node in the Kaspersky Security Center Administration Console tree select **Create a task**.

   The task wizard window opens.
2. In the **Select the task type** window under the heading **Kaspersky Embedded Systems Security 2.2**, select the type of the task to be created.

3. If you selected any task type except Rollback of Database Update or Activation of Application, **Settings** window opens. Depending on the type of task created, do one of the following actions:

   - *To create an On-Demand Scan task*:

     a. 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 ☑.

        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, right-click the **Scan scope** table and select Add scope. 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, open the context menu and select the **Configure** option, then click the **Settings** button in the Security level window, and in the **On-demand scan settings** window on the **General** tab, clear the **Subfolders** and **Subfiles** check boxes.
        - To change scan scope security settings, open the context menu on the scope whose settings you wish to configure, and select **Configure**. 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 configuration is performed in the same way as in Kaspersky Embedded Systems Security 2.2 Console.
        - To skip embedded objects in the added scan scope, open the context menu on the **Scan scope** table, select **Add exclusion** and specify the objects to exclude: select predefined scope in the Predefined scope list, specify the computer disk, folder, network object, or file on a protected computer or on another network computer, and click the **OK** button.
        - Excluded scan scopes are marked with the ☐ icon in the table.

     b. Do the following in the **Options** window.

        Select the **Apply Trusted Zone** check box if you wish to exclude objects described in the Kaspersky Embedded Systems Security 2.2 Trusted Zone from the scan scope of the task.

        If you plan to use the task created as a Critical Areas Scan task, select the **Perform task in background mode** check box in the **Options** window. Kaspersky Security Center evaluates the security rating of the computer (computers) by the performance results of tasks with the *Critical Areas Scan* status, and not only by the performance results of the **Critical Areas Scan** system task. When creating a local On-Demand Scan task, this check box is not available.

        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. By default, the working processes in which Kaspersky Embedded Systems Security 2.2 tasks are run have the **Medium** (Normal) priority. Demoting the process priority increases the time required to execute the task, but it may have a beneficial effect on the execution speed of the processes of other active programs.

- *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 2.2 to restart the computer automatically upon task completion, select the **Allow operating system restart** check box. To disable automatic computer restart upon task completion, clear the **Allow operating system restart** check box.

  c. To obtain information about Kaspersky Embedded Systems Security 2.2 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*, in the **Activation Settings** window 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 create a task for renewing the license.

- *To create the Rule Generator for Applications Launch Control task or the Rule Generator for Device Control task*, in the **Settings** window specify the settings based on which the list of allowing rules will be created:

  a. Specify a prefix for the rule names (only for the Rule Generator for Applications Launch Control task).

  b. Configure the usage scope of the allowing rules (only for the Rule Generator for Applications Launch Control task). Click the **Next** button.

  c. Specify the actions that the allowing task will perform while generating allowing rules (only for the Rule Generator for Applications Launch Control task) and after the task completion.

4. Configure the task schedule (you can configure a schedule for all task types except Rollback of Database Update task). Do the following in the **Schedule** window:

   a. Select the **Run by schedule** check box to enable the schedule;

   b. Specify the task start frequency: select one of the following values from the **Frequency** list: **Hourly**, **Daily**, **Weekly**, **At application launch**, **After application database update** (the start frequency

After Administration Server has retrieved updates can also be specified in the following group tasks: Database Update and Software Modules Update):

- If **Hourly** is selected, specify the number of hours in the **Every <number> hour(s)** in the **Task start settings** configuration group.
- If **Daily** is selected, specify the number of days in the **Every <number> day(s)** in the **Task start settings** configuration group.
- If **Weekly** is selected, specify the number of weeks in the **Every <number> week(s)** in the **Task start settings** configuration group. Specify on which days of the week the task will be started (on Mondays, by default).

c. In the **Start time** field, specify the time when the task will be started; in the **Start date** field specify the date when the schedule will become effective.

d. Specify the remaining schedule settings if required: click the **Advanced** button and do the following in the **Advanced schedule settings** window:

- Specify the maximum duration of task execution: enter the number of hours and minutes in the **Duration** field in the **Task stop settings** configuration group.
- Specify the time interval within a 24-hour period in which a task execution is be paused: in the **Task stop settings** configuration group, enter the start and end values of the interval in the **Pause from** and **to** fields.
- Specify the date at which the schedule will be disabled: select the **Cancel schedule from** check box and select the date when schedule will be disabled using the **Calendar** window.
- Enable start of missed tasks: select the **Run skipped tasks** check box.
- Enable the start time distribution setting: select the **Randomize the task start time within the interval of** check box and specify the value in minutes.

e. Click **OK**.

5. If the task created is for sets of computers, select the network (group) of computers on which this task will be executed.
6. In the **Selecting an account to run the task** window, specify the account under which you want to run the task.
7. 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").
8. 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 Application settings window of Kaspersky Security Center

► *To configure local tasks or general application settings in the Application settings window for a single network computer, perform the following tasks:*

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.
      - Choose **Properties** in the context menu of the selected task.
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.

      > 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 settings** window.

> The process of configuring the settings of Kaspersky Embedded Systems Security 2.2 functional components in Kaspersky Security Center is similar to local configuration of the settings of these components in the Application Console. Detailed instructions on how to configure task settings and application functions are provided in the relevant sections of the *Kaspersky Embedded Systems Security 2.2 User's Guide*.

Configuring group tasks in Kaspersky Security Center

The process of configuring the settings of Kaspersky Embedded Systems Security 2.2 functional components in Kaspersky Security Center is similar to local configuration of the settings of these components in the Application Console. Detailed instructions on how to configure task settings and application functions are provided in the relevant sections of the *Kaspersky Embedded Systems Security 2.2 User's Guide*.

► *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 activation code or key** check box if you want to add an activation code or key 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 26. Kaspersky Embedded Systems Security 2.2 group tasks settings

Kaspersky Embedded Systems Security 2.2 task types	Section in the Properties: <Task name> window	Task settings
Automatic rule generation (see Section "Rule Generator for Applications Launch Control and Rule Generator for Device Control tasks" on page 101)	**Settings**	While configuring the Rule Generator for Applications Launch Control task settings you can: • Change the protection scope by adding or removing the paths to folders and specifying file types for which start is allowed by automatically generated rules. • Take into account currently running applications.
	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 2.2 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 103)	**Activation Settings**	To activate the application or to renew expiration date you can add a key.
	Schedule	You can configure the settings of scheduled startup of the task.

Kaspersky Embedded Systems Security 2.2 task types	Section in the Properties: <Task name> window	Task settings
Copying Updates (see Section "Update tasks" on page 103)	**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.
	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 2.2 to store copied updates.
	Schedule	You can configure the settings of scheduled startup of the task.
Database Update (see Section "Update tasks" on page 103)	**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 **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.
	Schedule	You can configure the settings of scheduled start of the task.

Kaspersky Embedded Systems Security 2.2 task types	Section in the Properties: <Task name> window	Task settings
Software Modules Update (see Section "Update tasks" on page 103)	**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 2.2 perform when critical software module updates are available or have already been installed, and also if Kaspersky Embedded Systems Security 2.2 should receive information regarding scheduled updates.
	Schedule	You can configure the settings of scheduled startup of the task.
On-Demand Scan (see Section "Creating an On-Demand Scan task" on page 106)	**Scan scope**	You can specify a Scan scope for On-Demand Scan task and configure security level settings.
	On-demand scan settings window	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.
	Schedule	You can configure the settings of scheduled startup of the task.
Software Modules Integrity Check (on page 105)	**Schedule**	You can configure the settings of scheduled startup of the task.

For the tasks, such as Rollback of Database Update, 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

Rule Generator for Applications Launch Control and Rule Generator for Device Control tasks

► *To configure the Rule Generator for Device Control task or the Rule Generator for Applications Launch Control task, 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.
5. For detailed information regarding configuring settings in this section, see the *Kaspersky Security Center Help*.
6. In the **Settings** section, you can configure the following settings:
   - Change the protection scope by adding or removing the paths to folders and specifying file types for which launch is allowed by automatically generated rules.
   - Take into account currently running applications.
7. In the **Settings** 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 the 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. This option is recommended 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 the 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 the criterion for triggering the allowing rules for Applications Launch Control. Kaspersky Embedded Systems Security 2.2 will allow applications that are launched using files with a thumbprint and a digital certificate specified.

Selecting this check box strongly 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 the 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**

  Drop down list that allows you to select the criterion for triggering the allowing rules for Applications Launch Control if the file, which is used to generate the rule, has no digital certificate.

  - **SHA256 hash**. The checksum value of the file, which is used to generate the rule, is set as the 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, which is used to generate the rule, is set as the 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 tab in the Create allowing rules for applications from the folders table.

- **Use SHA256 hash**

  If this option is selected, the checksum value of the file, which is used to generate the rule, is specified as the 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 value.

  This option is recommended for cases when the generated rules are required to meet ultimate security level: SHA256 checksum may be applied as a unique file ID. The usage of SHA256 checksum as a rule triggering criterion constricts the rule usage scope up to one file.

- **Generate rules for user or group of users**.

  Field that displays a user and / or group of users. The application will monitor any applications run by the specified user and / 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 2.2 creates upon the task completion.

8. Configure the task schedule in the **Schedule** section (you can configure a schedule for all task types except Rollback of Database Update).
9. In the **Account** section specify the account which rights will be used for the task execution.
10. 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*.

11. In the **Properties: <Task name>** window, click **OK**.

    The newly configured group tasks settings are saved.

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.
5. For detailed information regarding configuring settings in this section, see the *Kaspersky Security Center Help*.
6. 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 a key to extend the license.
7. Configure the task schedule in the **Schedule** section (you can configure a schedule for all task types except Rollback of Database Update).
8. In the **Account** section specify the account which rights will be used for the task execution.
9. 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*.

10. 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 2.2 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 2.2 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*.

Software Modules Integrity Check

► *To configure the Software Modules Update 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 Software Modules Integrity Check 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.

Creating an On-Demand Scan task

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

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 Server of Kaspersky Security Center and select the group that the protected computer belongs to.
     b. In the details pane, on the **Devices** tab open the context menu on the line with information about 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 and select the group for which you want to create a policy.
     b. In the details pane, open the context menu on the **Tasks** tab and select **New > Task**.
   - To create a task for a custom set of computers, in the **Device selections** node in the Kaspersky Security Center Administration Console tree select **New task**.

   The task wizard window opens.
2. In the **Specify task name** window, enter the task name (no longer than 100 characters) not containing the symbols **I * < > ? \ / | :)**. It is recommended that the task type is added to its name (for example, "On-demand scan of shared folders").
3. In the **Task type** window under the heading **Kaspersky Embedded Systems Security 2.2**, select the **On-Demand Scan** task and 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 145).

- 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 "Using Heuristic Analyzer" on page 140).

- Select the **Apply Trusted Zone** check box, if you want to exclude objects described in the Kaspersky Embedded Systems Security 2.2 Trusted Zone 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 2.2 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 2.2 disregards the file operations of trusted processes when forming the protection scope for the Real-Time File Protection task.

  The check box is selected by default.

- Select 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 service.

  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 2.2 tasks and 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 2.2 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 2.2 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 2.2. 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 completed event and refreshes the computer protection status on the basis of 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 selected by default for the Critical Areas Scan task.

6. Click **Next**.
7. In the **Schedule** window, setup a schedule (see Section "Configuring the task start schedule settings" on page 114) for the task.
8. Specify a user account under which you want to run the task and define the task name.
9. Click **Finish**.

The new On-Demand Scan task will be created for a selected computer or a group of computers.

Configuring the On-Demand Scan task

► *To configure an existing On-Demand Scan 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 **Settings** section, you can perform the following actions:

   a. In the **Scan scope** section, select the check boxes next to those file resources that you want to included in the scan scope.

   b. Click the **Configure** button and select the security level.

      You can select one of predefined security levels, or customize security level manually.

   c. To configure the security level manually, in the **On-demand scan settings** window click the **Settings** button.

6. In the **Options** section, you can perform the following actions:

   a. Enable or disable use of the **Heuristic Analyzer** and set the analysis level using the slider in the **Heuristic analyzer** block.

   b. Configure the advanced settings (see Section "Creating an On-Demand Scan task" on page 106).

7. Configure the task schedule in the **Schedule** section (you can configure a schedule for all task types except Rollback of Database Update).

8. In the **Account** section specify the account which rights will be used for the task execution.

9. 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*.

10. In the **Properties: <Task name>** window, click **OK**.

    The newly configured group tasks settings are saved.

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 2.2.

► *To configure scanning of all computers in a single administration group, take the following steps:*

1. Create a group On-Demand Scan task.

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 both when creating the On-Demand Scan task for a group of computers or a set of computers and later in the **Properties: <Task name>** window.

3. Using a new or existing policy disable the scheduled start of system scan tasks (see Section "Configuring scheduled start of local system tasks" on page 89) 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 task 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.

Cloud storage file scanning

About cloud files

Kaspersky Embedded Systems Security 2.2 can interact with Microsoft OneDrive cloud files. The application supports the new OneDrive Files On-Demand feature.

Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 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 2.2 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.

Configuring crash diagnostics settings in Kaspersky Security Center

If a problem occurs during Kaspersky Embedded Systems Security 2.2 operation (for example, Kaspersky Embedded Systems Security 2.2 crashes) and you want to diagnose it, you can enable the creation of trace files and the dump file of Kaspersky Embedded Systems Security 2.2 process and send these files for analysis to Kaspersky Lab Technical Support.

> Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 settings. You can configure access permissions (see Section "Access permissions for Kaspersky Embedded Systems Security 2.2 functions" on page 73) 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 Application settings window of Kaspersky Security Center**" on page 96) 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 2.2 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 2.2 saves to the trace file.

       You can select one of the following detail levels:

       - **Critical events** – Kaspersky Embedded Systems Security 2.2 saves information only about critical events to the trace file.
       - **Errors** – Kaspersky Embedded Systems Security 2.2 saves information about critical events and errors to the trace file.
       - **Important events** – Kaspersky Embedded Systems Security 2.2 saves information about critical events, errors, and important events to the trace file.
       - **Informational events** – Kaspersky Embedded Systems Security 2.2 saves information about critical events, errors, important events, and informational events to the trace file.
       - **All debug information** – Kaspersky Embedded Systems Security 2.2 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 27. Kaspersky Embedded Systems Security 2.2 subsystem codes

Component Code	Name of component
*	All components.
gui	User interface subsystem, Kaspersky Embedded Systems Security 2.2 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 2.2 control tasks.
wp	Work process, handles anti-virus protection tasks.
blgate	Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 subsystems are applied as soon as the crash diagnostics settings are saved.

By default, Kaspersky Embedded Systems Security 2.2 logs debug information for all Kaspersky Embedded Systems Security 2.2 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 2.2 will save the memory 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 2.2 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, do the following:*

1. In the Kaspersky Security Center Administration Console tree, expand the **Managed devices** node and do the following:

   - If you want to configure policy settings, in the computer group select **Policy > <Policy name> > <Section> > Configure > Task Management**.
   - If you want to configure application settings for a single computer using Kaspersky Security Center, open the **Task Settings** (see Section "**Configuring local tasks in Application settings window of Kaspersky Security Center**" on page 96) window in Kaspersky Security Center.

   The **Settings** window opens.

2. In the window that opens, on the **Schedule** tab, 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.

3. 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 2.2 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 89).

4. 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.

5. Click the **Apply** button to save the task start settings.

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 the **Apply** button.

The configured task start schedule settings are saved.

Managing application settings

This section contains information about configuring Kaspersky Embedded Systems Security 2.2 general settings in Kaspersky Security Center.

In this chapter

Managing Kaspersky Embedded Systems Security 2.2 from Kaspersky Security Center

You can centrally manage several computers with Kaspersky Embedded Systems Security 2.2 installed and included in an administration group by means of the Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 on that computer is controlled by an active Kaspersky Security Center policy.

Kaspersky Embedded Systems Security 2.2 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 2.2 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.

Configuring general application settings in Kaspersky Security Center

You can configure general Kaspersky Embedded Systems Security 2.2 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

> The process of configuring the settings of Kaspersky Embedded Systems Security 2.2 functional components in Kaspersky Security Center is similar to local configuration of the settings of these components in the Application Console. Detailed instructions on how to configure task settings and application functions are provided in the relevant sections of the *Kaspersky Embedded Systems Security 2.2 User's Guide*.

► *To configure scalability settings and the application interface, take the following steps:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree and select the administration group for which you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring policy" on page 84).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in Application settings window of Kaspersky Security Center" on page 96).

     > If a device is being managed by an active Kaspersky Security Center policy and this policy blocks changes to the application settings, these settings cannot be edited in the **Application settings** window.
3. In the **Application settings** section, in the **Scalability and interface** block, click **Settings**.

4. In the **Scalability and interface** 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 2.2:

     - **Automatically detect scalability settings**.

       Kaspersky Embedded Systems Security 2.2 automatically regulates the number of processes used.

     - **Set the number of working processes manually**.

       Kaspersky Embedded Systems Security 2.2 regulates the number of active working processes according to the values specified.

       This is the default value.

       - **Maximum number of active processes.**

       Maximum number of processes that Kaspersky Embedded Systems Security 2.2 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.

5. Click **OK**.

The configured application settings are saved.

Configuring security settings in Kaspersky Security Center

The process of configuring the settings of Kaspersky Embedded Systems Security 2.2 functional components in Kaspersky Security Center is similar to local configuration of the settings of these components in the Application Console. Detailed instructions on how to configure task settings and application functions are provided in the relevant sections of the *Kaspersky Embedded Systems Security 2.2 User's Guide*.

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

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree and select the administration group for which you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:

   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring policy" on page 84).

- To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in Application settings window of Kaspersky Security Center" on page 96).

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

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

- In the **Reliability settings** section, configure the settings for recovery of Kaspersky Embedded Systems Security 2.2 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 2.2 tasks when the application returns an error or terminates.

    If the check box is selected, Kaspersky Embedded Systems Security 2.2 automatically recovers Kaspersky Embedded Systems Security 2.2 tasks when the application returns an error or terminates.

    If the check box is cleared, Kaspersky Embedded Systems Security 2.2 does not recover Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 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 2.2 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 2.2 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 2.2 pauses running scan tasks after the computer switches to a UPS source.

If the check box is cleared, Kaspersky Embedded Systems Security 2.2 continues running scan tasks after the computer switches to a UPS source.

The check box is selected by default.

> Computer switches to UPS power only if the battery charge level drops below 90%.

- In the **Password protection settings** section, set a password to protect access to Kaspersky Embedded Systems Security 2.2 functions.

5. Click **OK**.

The scalability and reliability settings are saved.

Configuring connection settings using Kaspersky Security Center

> The process of configuring the settings of Kaspersky Embedded Systems Security 2.2 functional components in Kaspersky Security Center is similar to local configuration of the settings of these components in the Application Console. Detailed instructions on how to configure task settings and application functions are provided in the relevant sections of the *Kaspersky Embedded Systems Security 2.2 User's Guide*.

The configured connection settings are used to connect Kaspersky Embedded Systems Security 2.2 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 and select the administration group for which you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring policy" on page 84).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in Application settings window of Kaspersky Security Center" on page 96).

   > If a device is being managed by an active Kaspersky Security Center policy and this policy blocks changes to the application settings, these settings cannot be edited in the **Application settings** window.
3. In the **Application settings** section click the **Settings** button in the **Proxy server** block.

   The **Connection settings** window opens.
4. 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 2.2 connects to KSN services directly, without using any proxy server.

  - **Automatically detect proxy server settings**.

    If this option is selected, Kaspersky Embedded Systems Security 2.2 automatically defines the settings for connection to KSN services using Web Proxy Auto-Discovery Protocol (WPAD).

    This option is selected by default.

  - **Use specified proxy server settings**.

    If this option is selected, Kaspersky Embedded Systems Security 2.2 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 2.2 installed.

    If this check box is selected, computers are accessed directly from the network, which hosts the computer with Kaspersky Embedded Systems Security 2.2 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**.

5. Click **OK**.

The configured connection settings are saved.

Configuring advanced features

You can configure Kaspersky Embedded Systems Security 2.2 advanced features from Kaspersky Security Center for a group of computers or for a single computer.

In this section

Configuring Trusted Zone settings in Kaspersky Security Center

By default, Trusted Zone is applied in newly created policies and tasks.

► *To configure the Trusted Zone 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. 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 policy" on page 84).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in Application settings window of Kaspersky Security Center" on page 96).

     > If a device is being managed by an active Kaspersky Security Center policy and this policy blocks changes to the application settings, these settings cannot be edited in the **Application settings** window.
3. In the **Supplementary** section, click the **Settings** button in the **Trusted zone** block.

   The **Trusted Zone** window opens.
4. On the **Exclusions** tab, specify the objects to be skipped by Kaspersky Embedded Systems Security 2.2 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 2.2 will consider trusted.

- To manually specify the conditions under which a file will be considered trusted, click the **Add** button. In the window that opens, specify the following settings:
  - **Object to scan**

    Adds a file, folder, drive, or script file to an exclusion.

    If the check box is selected, Kaspersky Embedded Systems Security 2.2 skips the specified predefined scope, file, folder, drive or script file while running the scan with the use of the Kaspersky Embedded Systems Security 2.2 component selected in the **Exclusion usage scope** section.

    The check box is selected by default.
  - **Objects to detect**

    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 2.2 skips specified detectable objects during scanning.

    If the check box is cleared, Kaspersky Embedded Systems Security 2.2 detects all objects specified in the application by default.

    The check box is cleared by default.
  - **Exclusion usage scope**

    Name of the Kaspersky Embedded Systems Security 2.2 task in which the rule is used.
  - If necessary, specify additional information explaining the exclusion in the **Comment** field.

5. In the **Trusted Zone** window on the **Trusted processes** tab specify the processes to be skipped by Kaspersky Embedded Systems Security 2.2 during scanning:
   - **Do not check file backup 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 2.2 skips file read operations performed by Backup tools installed on the computer.

     If the check box is cleared, Kaspersky Embedded Systems Security 2.2 scans file read operations performed by Backup tools installed on the computer.

     The check box is selected by default.
   - **Do not check file activity of the specified 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 2.2 skips operations of trusted processes during scanning.

     If the check box is cleared, Kaspersky Embedded Systems Security 2.2 scans file operations of trusted processes.

     The check box is cleared by default.
6. If necessary, add processes whose file activity you do not want to scan (see Section "Adding trusted processes" on page 124) by clicking the **Add** button.
7. Click **OK** in the **Trusted Zone** window to save changes.

Adding trusted processes

► *To add one or a number of processes to the list of trusted processes:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree and select the administration group for which you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
    - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring policy" on page 84).
    - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in Application settings window of Kaspersky Security Center" on page 96).

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

3. In the **Supplementary** section, click the **Settings** button in the **Trusted zone** block.

    The **Trusted Zone** window opens.

4. On the **Trusted processes** tab, select the **Do not check file activity of the specified processes** check box.
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 2.2 will use the full path to the file to determine the process trust status.

         If the check box is cleared, the path to the file is not considered as a criterion for determining the process trust status.

         The check box is selected by default.

      b. **Use process file hash to consider it trusted**.

         If the check box is selected, Kaspersky Embedded Systems Security 2.2 uses the selected file hash to determine the process trust status.

         If the check box is cleared, the file hash will not be considered as a criterion for determining 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 2.2 installed in order to allow viewing the list of active processes. You can sort processes in the list of active processes by file name, 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 the name and path.**

  In the **Add trusted process manually** window that opens, configure the following:

  a. Enter a path to executable file (including the file name).

  b. Click **OK**.

- **One process based on the properties of the object.**

  In the **Add trusted process** 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 2.2 will use the full path to the file to determine the process trust status.

  If the check box is cleared, the path to the file is not considered as a criterion for determining the process trust status.

  The check box is selected by default.

  c. **Use process file hash to consider it trusted**.

  If the check box is selected, Kaspersky Embedded Systems Security 2.2 uses the selected file hash to determine the process trust status.

  If the check box is cleared, the file hash will not be considered as a criterion for determining 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 **Add trusted process** 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 2.2 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. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree and select the administration group for which you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring policy" on page 84).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in Application settings window of Kaspersky Security Center" on page 96).

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

3. In the **Supplementary** section, click the **Settings** button in the **Trusted zone** block.

   The **Trusted Zone** window opens.
4. On the **Exclusions** tab, 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.

Removable Drives Scan

You can configure scanning of removable drives connected to the protected computer via the USB port.

Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 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 28. 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 2.2 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.

► *To configure scanning of removable drives on connection, perform the following actions:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree and select the administration group for which you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring policy" on page 84).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in Application settings window of Kaspersky Security Center" on page 96).

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

3. In the **Supplementary** section click **Settings** in the **Removable Drives Scan** block.

   The **Removable Drives Scan** window opens.

4. 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 2.2 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.

5. Click **OK**.

   The specified settings are saved and applied.

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.

> The process of configuring the settings of Kaspersky Embedded Systems Security 2.2 functional components in Kaspersky Security Center is similar to local configuration of the settings of these components in the Application Console. Detailed instructions on how to configure task settings and application functions are provided in the relevant sections of the *Kaspersky Embedded Systems Security 2.2 User's Guide*.

► *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 and select the administration group for which you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:

   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring policy" on page 84).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in Application settings window of Kaspersky Security Center" on page 96).

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

3. Open the **Supplementary** section and do the following:

   - To configure access permissions for managing Kaspersky Embedded Systems Security 2.2 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.

4. In the window that opens, configure the access privileges (see Section "Access permissions for Kaspersky Embedded Systems Security 2.2 functions" on page 73) according to your needs.

The specified settings are saved.

Configuring Quarantine and Backup settings in Kaspersky Security Center

The process of configuring the settings of Kaspersky Embedded Systems Security 2.2 functional components in Kaspersky Security Center is similar to local configuration of the settings of these components in the Application Console. Detailed instructions on how to configure task settings and application functions are provided in the relevant sections of the *Kaspersky Embedded Systems Security 2.2 User's Guide*.

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

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree and select the administration group for which you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring policy" on page 84).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in Application settings window of Kaspersky Security Center" on page 96).

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

3. In the **Supplementary** section, click the **Settings** button in the **Storages** block.
4. 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.

5. 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.
6. 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 2.2 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 2.2 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 **Events** 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 **Events** 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.

> The process of configuring the settings of Kaspersky Embedded Systems Security 2.2 functional components in Kaspersky Security Center is similar to local configuration of the settings of these components in the Application Console. Detailed instructions on how to configure task settings and application functions are provided in the relevant sections of the *Kaspersky Embedded Systems Security 2.2 User's Guide*.

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 **Events** 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

> The process of configuring the settings of Kaspersky Embedded Systems Security 2.2 functional components in Kaspersky Security Center is similar to local configuration of the settings of these components in the Application Console. Detailed instructions on how to configure task settings and application functions are provided in the relevant sections of the *Kaspersky Embedded Systems Security 2.2 User's Guide*.

► *To configure Kaspersky Embedded Systems Security 2.2 logs, perform the following steps:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree and select the administration group for which you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring policy" on page 84).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in Application settings window of Kaspersky Security Center" on page 96).

     > If a device is being managed by an active Kaspersky Security Center policy and this policy blocks changes to the application settings, these settings cannot be edited in the **Application settings** window.
3. In the **Logs and notifications** section, click the **Settings** button in the **Task logs** block.
4. In the **Logs settings** window define the following settings of Kaspersky Embedded Systems Security 2.2 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 2.2 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.
5. Click **OK**.

The configured log settings are saved.

Security log

Kaspersky Embedded Systems Security 2.2 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. Moreover, Kaspersky Embedded Systems Security 2.2 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 2.2 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 29. 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 main 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 and select the administration group for which you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring policy" on page 84).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in Application settings window of Kaspersky Security Center" on page 96).

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

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

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

4. Select the **SIEM integration** tab.

5. 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.

6. 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.

7. 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.

8. 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.
   - If necessary, 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.

9. Click **OK**.

The configured SIEM integration settings will be applied.

Configuring notification settings

► *To configure Kaspersky Embedded Systems Security 2.2 notifications, perform the following steps:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree and select the administration group for which you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring policy" on page 84).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in Application settings window of Kaspersky Security Center" on page 96).

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

3. In the **Logs and notifications** section, click the **Settings** button in the **Event notifications** block.
4. In the **Notification settings** window, define the following settings of Kaspersky Embedded Systems Security 2.2 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 2.2 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.
5. 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 2.2 sends information to the Kaspersky Security Center Administration Server:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree and select the administration group for which you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring policy" on page 84).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in Application settings window of Kaspersky Security Center" on page 96).

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

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

   The **Administration Server Network** lists window opens.
4. In the **Administration Server Network lists** window, select the types of objects about which Kaspersky Embedded Systems Security 2.2 will send information to the Kaspersky Security Center Administration Server:
   - Quarantined objects.
   - Backed up objects.
5. Click **OK**.

   Kaspersky Embedded Systems Security 2.2 will send information about the selected object types to the Administration Server.

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 Protection tasks and manage the security settings of a protected computer.

In this chapter

Real-Time File Protection

This section contains information about the Real-Time File Protection task and how to configure it.

In this section

About Real-Time File Protection task

When the Real-Time File Protection task is running, Kaspersky Embedded Systems Security 2.2 scans the following protected computer objects when they are accessed:

- Files.
- Alternate file system streams (NTFS streams).
- Master boot record and boot sectors on the local hard drives and external devices.
- Windows Server® 2016 and Windows Server 2019 container files.

When any application writes a file to a computer or reads a file from it, Kaspersky Embedded Systems Security 2.2 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, places it in Quarantine, or deletes it. Kaspersky Embedded Systems Security 2.2 returns the file to the application if it is not infected or if it has been successfully disinfected.

Kaspersky Embedded Systems Security 2.2 intercepts file operations, executed in Windows Server 2016 and Windows Server 2019 containers.

A container is an isolated environment, which allows applications to run without direct interaction with the operating system. If container is located in task the task protection scope, Kaspersky Embedded Systems Security 2.2 scans container files, which are being accessed by users, for computer threats. When a threat is detected, the application attempts to disinfect the container. If the attempt is successful, the container continues to work; if disinfection fails, the container is shut down.

Kaspersky Embedded Systems Security 2.2 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.

Configuring the Real-Time File Protection task

By default, the Real-Time File Protection system task uses the settings described in the table below. You can change the values of these settings.

Table 30. 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.
Security level	Common settings for the entire protection scope; corresponds to the **Recommended** security level.	For nodes selected in the computer file resources tree, you can: • Apply another predefined security level. • Edit the security level manually. • Save security settings of the selected node as a template for later usage.
Objects protection mode	On access and modification.	You can select protection mode, i.e. define type of access at which Kaspersky Embedded Systems Security 2.2 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 computer 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.

► *To configure the Real-Time File Protection task settings, take the following steps:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree and select the administration group for which you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring policy" on page 84).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in Application settings window of Kaspersky Security Center" on page 96).

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

3. In the **Real-Time File Protection** section click the **Settings** button in the **Real-Time File Protection** block.

   The **Real-Time File Protection** window opens.
4. Configure the following task settings:
   - On the **General** tab:
     - Protection mode (see Section "Selecting protection mode" on page 140)
     - Using Heuristic Analyzer (on page 140)
     - Settings of integration with other Kaspersky Embedded Systems Security 2.2 components.
   - On the **Task Management** tab:
     - Scheduled task start settings (see Section "Configuring the task start schedule settings" on page 114).
5. Select the **Protection scope** tab and do the following:
   - Click the **Add** or **Edit** button to edit the protection scope (see Section "Protection scope in Real-Time File Protection task" on page 142).
     - In the window that opens, choose what you want to include in the task's protection scope:
       - **Predefined scope**
       - **Disk, folder, or network location**
       - **File**
     - Select one of the predefined security levels (see Section "Selecting predefined security levels" on page 143) or manually configure the protection (see Section "Configuring security settings manually" on page 145) settings.
6. Click **OK** in the **Real-Time File Protection** window.

Kaspersky Embedded Systems Security 2.2 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.

Using Heuristic Analyzer

You can use the Heuristic Analyzer and configure the level of analysis for Kaspersky Embedded Systems Security 2.2 tasks.

► *To configure the Heuristic Analyzer:*

1. Open the application settings (see Section "Managing Kaspersky Embedded Systems Security 2.2 from Kaspersky Security Center" on page 116) or policy settings (see Section "Configuring policy" on page 84), for which you want to configure the Heuristic Analyzer.
2. 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. 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.

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 2.2 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. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree and select the administration group for which you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring policy" on page 84).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in Application settings window of Kaspersky Security Center" on page 96).

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

3. In the **Real-Time Computer Protection** section click the **Settings** button in the **Real-Time File Protection** block.

   The **Real-Time File Protection** window opens.
4. 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 2.2 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 2.2 rescans the object only after the object was saved by the process for the last time.
   - **On access and modification**

     Kaspersky Embedded Systems Security 2.2 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 2.2 scans all objects when they are opened for reading or for execution or modification.
   - **When run**

     Kaspersky Embedded Systems Security 2.2 scans the file only when it is accessed to be executed.
5. Click **OK**.

The selected protection mode will take effect.

Protection scope in Real-Time File Protection task

This section provides instructions on creating and managing a protection scope in the Real-Time File Protection task.

In this section

Predefined protection scopes

The protected computer's file resources are displayed in the **Real-Time File Protection** task settings on the **Protection scope** 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 2.2 covers the following predefined protection scopes:

- **Local hard drives**. Kaspersky Embedded Systems Security 2.2 protects files on the computer hard drives.
- **Removable drives**. Kaspersky Embedded Systems Security 2.2 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 2.2 protects files that are written to network folders or read from them by applications running on the computer. Kaspersky Embedded Systems Security 2.2 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.

Selecting predefined security levels

One of the following predefined security levels for the nodes selected in the computer 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 2.2 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 31. 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

Options	Security level		
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.

► *To select one of the predefined security levels, take the following steps:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree and select the administration group for which you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring policy" on page 84).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in Application settings window of Kaspersky Security Center" on page 96).

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

3. In the **Real-Time Computer Protection** section click the **Settings** button in the **Real-Time File Protection** block.

   The **Real-Time File Protection** window opens.

4. On the **Protection scope** tab, select the node whose securities settings you want to configure, and click **Configure**.

   The **Real-Time File Protection settings** window opens.

5. Select the desired security level in the drop-down list:
   - **Maximum protection**
   - **Recommended**
   - **Maximum performance**
6. Click **OK**.

Your newly configured settings have been saved.

Kaspersky Embedded Systems Security 2.2 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.

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 "Selecting predefined security levels" on page 143).

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 nodes in the computer file resource list or tree.

When working with the computer 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 the security settings of the selected node manually:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree and select the administration group for which you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring policy" on page 84).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in Application settings window of Kaspersky Security Center" on page 96).

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

3. In the **Real-Time Computer Protection** section click the **Settings** button in the **Real-Time File Protection** block.

   The **Real-Time File Protection** window opens.
4. 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.

5. On the **Security level** tab you can select any existing level or click the **Settings** button to set custom configuration.
6. 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 146)
    - Actions (see Section "Configuring actions" on page 148)
    - Performance (see Section "Configuring performance" on page 150)
7. Click **Save** in the **Protection scope settings** window.

New protection scope settings are saved.

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 "Configuring security settings manually" on page 145).
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 2.2 scans all objects.
    - **Objects scanned by format**

      Kaspersky Embedded Systems Security 2.2 scans only infectable objects based on file format.

      Kaspersky Lab compiles the list of formats. It is included in the Kaspersky Embedded Systems Security 2.2 databases.
    - **Objects scanned according to list of extensions specified in anti-virus database**

      Kaspersky Embedded Systems Security 2.2 scans only infectable objects based on file extension.

      Kaspersky Lab compiles the list of extensions. It is included in the Kaspersky Embedded Systems Security 2.2 databases.
    - **Objects scanned by specified list of extensions**

      Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 as new or modified since the last scan.

   If the check box is selected, Kaspersky Embedded Systems Security 2.2 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** and **Recommended** security levels. If the **Maximum protection** security level is 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 2.2 scans archives.

     If this check box is cleared, Kaspersky Embedded Systems Security 2.2 skips archives during scanning.

     The default value depends on the selected security level.

   - **All / Only new SFX archives**

     Scanning of self-extracting archives.

     If this check box is selected, Kaspersky Embedded Systems Security 2.2 scans SFX archives.

     If this check box is cleared, Kaspersky Embedded Systems Security 2.2 skips SFX archives during scanning.

     The default value depends on the selected security 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 2.2 scans mail database files.

If this check box is cleared, Kaspersky Embedded Systems Security 2.2 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 2.2 scans executable files packed by packers.

  If this check box is cleared, Kaspersky Embedded Systems Security 2.2 skips executable files packed by packers during scanning.

  The default value depends on the selected security level.

- **All / Only new plain mail**

  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 2.2 scans files of mail formats.

  If this check box is cleared, Kaspersky Embedded Systems Security 2.2 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 2.2 scans objects embedded into files.

  If this check box is cleared, Kaspersky Embedded Systems Security 2.2 skips objects embedded into files during scanning.

  The default value depends on the selected security 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** window (see Section "Configuring security settings manually" on page 145).
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 2.2 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 area. This mode is not used by default on any of the security levels. If you select this mode, Kaspersky Embedded Systems Security 2.2 automatically changes the security level to **Custom**.

- **Block access**.

  When this option is selected Kaspersky Embedded Systems Security 2.2 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 2.2 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 area. This mode is not used by default on any of the security levels. If you select this mode, Kaspersky Embedded Systems Security 2.2 automatically changes the security level to **Custom**.

   - **Block access**.

     When this option is selected Kaspersky Embedded Systems Security 2.2 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 set primary and secondary action for each detected object type by clicking the **Settings** button next to the check box.

      If the check box is cleared, Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 does not perform the selected action, if the parent object is unmodifiable.

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

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** window (see Section "Configuring security settings manually" on page 145).
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 2.2 skips specified objects during scanning.

    If this check box is cleared, Kaspersky Embedded Systems Security 2.2 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 website http://www.securelist.com.

    If this check box is selected, Kaspersky Embedded Systems Security 2.2 skips specified detectable objects during scanning.

If the check box is cleared, Kaspersky Embedded Systems Security 2.2 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.

  The check box is selected by default.

- **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 2.2 skips compound objects whose size exceeds the specified limit during virus scan.

  If this check box is cleared, Kaspersky Embedded Systems Security 2.2 scans compound objects of any size.

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

- **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 2.2 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 2.2 scans NTFS system files disregarding the date of file creation or modification.

  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 2.2 scans only new and modified files.

  If the check box is cleared, Kaspersky Embedded Systems Security 2.2 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.

KSN Usage

This section contains information about the KSN Usage task and how to configure it.

In this section

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 2.2 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 2.2 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 2.2. 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 2.2 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 Processing" on page 156) of the KSN Usage task you can read the KSN Statement and enable the task by selecting the **I accept the terms of 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 2.2: all KSN-related data processing stops.

Configuring the KSN Usage task

You can change the default settings of the KSN Usage task (see the table below).

Table 32. The KSN Usage task default settings

Setting	Default Value	Description
Actions to perform on KSN untrusted objects	Remove	You can specify actions that Kaspersky Embedded Systems Security 2.2 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 2.2 calculates the MD5 hash for files of any size.
KSN Statement	The **I accept the terms of the Kaspersky Security Network Statement** check box is cleared.	Decide whether you want to participate in KSN after the installation. You can change your decision at any moment.

Setting	Default Value	Description
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.
I 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.
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.

► *To configure the KSN Usage task, take the following steps:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree and select the administration group for which you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring policy" on page 84).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in Application settings window of Kaspersky Security Center" on page 96).

     > If a device is being managed by an active Kaspersky Security Center policy and this policy blocks changes to the application settings, these settings cannot be edited in the **Application settings** window.
3. In the **Real-Time Computer Protection** section, click the **Settings** button in the **KSN Usage** block.

   The **KSN Usage** window opens.
4. 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 2.2 is to perform if it detects an object identified by KSN as untrusted:
     - **Remove**

       Kaspersky Embedded Systems Security 2.2 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 2.2 records information about the object with KSN-untrusted status in the task log. Kaspersky Embedded Systems Security 2.2 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 2.2 does not calculate the checksum for files that exceed the specified size (in MB).

    If the check box is cleared, Kaspersky Embedded Systems Security 2.2 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 2.2 calculates the checksum.
- 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.

5. 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 computer is restarted.

   The application will automatically start the KSN Usage task by schedule.
6. Configure the data handling (see Section "Configuring Data Processing" on page 156) 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 task log.

Configuring Data Processing

► *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 and select the administration group for which you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring policy" on page 84).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in Application settings window of Kaspersky Security Center" on page 96).

   > If a device is being managed by an active Kaspersky Security Center policy and this policy blocks changes to the application settings, these settings cannot be edited in the **Application settings** window.
3. In the **Real-Time Computer Protection** section click the **Data handling** button in the **KSN Usage** block.

   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 2.2 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 2.2 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 2.2 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 2.2 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 2.2.

   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 2.2 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 only if the **I accept the terms of the Kaspersky Security Network Statement** check box is selected.

By default Kaspersky Embedded Systems Security 2.2 sends checksums of files and additional statistics after you accept the KSN Statement.

Table 33. 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
☑	• reputation requests are sent • check box is editable	• additional statistics is sent • check box is editable
☑	• reputation requests are not sent • check box is not editable	• additional statistics is not sent • check box is not editable

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
□	• reputation requests are not sent • check box is editable	• additional statistics is not sent • check box is editable
□	• reputation requests are not sent • check box is not editable	• additional statistics is not sent • check box is not editable

Exploit Prevention

This section contains instructions on how to configure process memory protection settings.

In this chapter

About Exploit Prevention

Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 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 2.2 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 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 2.2 does not terminate the process, regardless of the mode indicated in the Exploit Prevention component settings.

- **Only notify about abused process**: apply this mode to receive information about instances of exploits in protected processes using events in the Filtered Security Audit.

  If this mode is selected, Kaspersky Embedded Systems Security 2.2 logs all attempts to exploit vulnerabilities by creating events.

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. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree and select the administration group for which you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring policy" on page 84).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in Application settings window of Kaspersky Security Center" on page 96).

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

3. In the **Real-Time Computer Protection** section click the **Settings** button in the **Exploit Prevention** block.

   The **Exploit Prevention** window opens.
4. In the **Exploit prevention mode** section, configure the following settings:
   - **Prevent vulnerable processes exploit**.

     If this check box is selected, Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 terminates a protected process upon detecting an exploit attempt if an active impact reduction technique has been applied to the process.
     - **Only notify about abused process**.

       If this mode is selected, Kaspersky Embedded Systems Security 2.2 reports exploits by displaying a terminal window. The compromised process continues to run.

       If Kaspersky Embedded Systems Security 2.2 detects an exploit in a critical process while the application is running in **Terminate on exploit** mode, the component forcibly switches to **Only notify about abused processes** mode.
5. In the **Preventing actions** section, configure the following settings:
   - **Notify about abused processes via Terminal Service.**

     If this check box is selected, Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 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 2.2 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 2.2 does not protect processes from exploits when the Kaspersky Security Service is stopped.

  The check box is selected by default.

6. Click **OK**.

Kaspersky Embedded Systems Security 2.2 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. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree and select the administration group for which you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring policy" on page 84).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in Application settings window of Kaspersky Security Center" on page 96).

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

3. In **Real-Time Computer Protection** section, click the **Settings** button in the **Exploit Prevention** block.

   The **Exploit Prevention** window opens.

4. On the **Protected processes** tab, click the **Browse** button.

   The Microsoft Windows Explorer window opens.

5. Select the process you want to add to the list.
6. Click the **Open** button.

   The process name is displayed in the line.

7. Click the **Add** button.

   The process will be added to the list of protected processes.

8. Select the added process and click **Set exploit prevention techniques**.

   The **Exploit prevention techniques** window opens.

9. 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.

     b. Select or clear the **Apply Attack Surface Reduction technique** check box.

10. 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 websites
      - Restricted sites
      - Computer

      > These settings are only applicable to Internet Explorer®.

11. Click **OK**.

The process is added to the task protection scope.

Exploit prevention techniques

Table 34. 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.

Exploit prevention technique	Description
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.

Local activity control

This section provides information about Kaspersky Embedded Systems Security 2.2 functionality that controls applications launches, connections by external devices via USB, and the Windows Firewall.

In this chapter

Managing applications launch from Kaspersky Security Center

You can allow or deny launch of applications on all computers within the corporate network by creating common lists of Applications Launch Control rules on the side of Kaspersky Security Center for groups of computers.

In this section

About using profile to configure Applications Launch Control tasks in Kaspersky Security Center policy

Applications Launch Control rules configured in the policy are applied to all computers within the administration group. If one administration group includes computers of various types, custom lists of rules may be required for Applications Launch Control on each computer. You can use *policy profiles* to apply different policies to computers within a single administration group.

It is recommended to apply policy profiles to set Applications Launch Control rules for different computer types within a single administration group governed by a unified policy. This allows to optimize a computer protection as far as specified rules cover only those applications launches that are typical for this exact computer type.

Policy profiles are applied to computers of the administration group according to the *tags* assigned to them. You can configure a policy profile for all group computers, which have single tag.

Detailed information on tags and policy profiles as well as instructions on using them are provided in the *Kaspersky Security Center Help*.

► *To apply a policy profile in the Applications Launch Control task:*

1. In the Kaspersky Security Center Administration Console tree, expand the **Managed devices** node. Expand the administration group for which you want to configure the application of policy profiles.
2. Assign tags to each computer within the administration group according to the computer type. To do this, perform the following actions:
   - In the details pane of the selected administration group, open the **Devices** tab and select the computer for which you want to assign tags. In the **Properties: <Computer name>** window of the selected computer, select the **Tags** section and create a list of tags. Click **OK**.
3. Create a policy profile and configure its application for protecting computers within the administration group. To do this, perform the following actions:
   - In the details pane of the selected administration group, open the **Policies** tab and select the policy for which you want to configure the application of profiles. In the **Properties: <Policy name>** window of the selected policy, open the **Policy profiles** section and click the **Add** button to create a new profile. The **Properties: <Profile name>** window opens. Do the following:
     a. In the **Activation rules** section, configure the scope of application of the profile and specify the conditions under which the profile will be activated.
     b. In the **Applications Launch Control** section, configure the lists of Applications Launch Control rules for the profile you are editing.
     c. Click **OK**.
4. In the **Properties: <Policy name>** window, click **OK**.

Configured profile will be applied in the policy related to Applications Launch Control task.

Configuring Applications Launch Control task settings

You can change the default Applications Launch Control task settings (see the table below).

Table 35. Applications Launch Control task settings by default

Setting	Default Value	Description
Task mode	**Statistics only**. The task logs application blocking and startup events based on the set rules. Application launch is not actually denied.	You can select **Active** mode for computer protection after the final list of rules is generated.
Rules managing	**Replace local rules with policy rules**	You can select a mode in which rules specified in a policy are applied jointly with the rules on the local computer.
Rules usage scope	The task controls the launch of executable files, scripts, and MSI packages.	You can specify types of files for which launch is controlled by rules.
KSN Usage	Data on application reputation in the KSN are not used.	You can use KSN application reputation data when running the Applications Launch Control task.

Setting	Default Value	Description
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.	You can allow any software installation or update, if the operations are performed via Windows Installer.
Deny the command interpreters launch with no command to execute	Not applied.	You can deny launch of command interpreters with no command for execution.
Task start	First run is not scheduled.	The Applications Launch Control task does not start automatically at start of Kaspersky Embedded Systems Security 2.2. You can start the task manually or configure a scheduled start.

► *To configure general Applications Launch Control task settings take the following steps:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree and select the administration group for which you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring policy" on page 84).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in Application settings window of Kaspersky Security Center" on page 96).

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

3. In the **Local activity control** section, click the **Settings** button in the **Applications Launch Control** section.

   The **Applications Launch Control** window opens.

4. On the **General** tab, select the following settings in the **Mode** section:

   In the **Task mode** drop-down list, specify the task operation mode.

In this drop-down list you can select an Applications Launch Control task mode:

  - **Active**. Kaspersky Embedded Systems Security 2.2 uses the specified rules to monitor any applications being run.
  - **Statistics Only**. Kaspersky Embedded Systems Security 2.2 does not use the specified rules to monitor applications launches, but just records information about those launches in the task log instead. Start of all programs is allowed. You can use this mode to generate a list of Applications Launch Control rules on the basis of information recorded in the task log.

  By default, the Applications Launch Control task runs in the **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 basing on the incident information stored in the cache.

  If the check box is selected, Kaspersky Embedded Systems Security 2.2 allows or denies an application restart basing on the conclusion that the task had submitted on the first start of this application. For example, if the first application launch was allowed by the rules, the information about this action will be stored in the cache, and the second and all subsequent restarts will also be allowed, without any additional recheck.

  If the check box is cleared, Kaspersky Embedded Systems Security 2.2 analyzes an application on its every launch attempt.

  The check box is selected by default.

- Clear or select the **Deny the command interpreters launch with no command to execute** check box.

  If the check box is selected Kaspersky Embedded Systems Security 2.2 denies the launch of the command line interpreter even if the interpreter launch is allowed. The command line with no command can only be launched if both conditions are met:

  - The command line interpreter launch is allowed.
  - The executed command is allowed.

  If the check box is cleared, Kaspersky Embedded Systems Security 2.2 only considers the allowing rules for the command line launch. The launch is denied if no allowing rule is applied or the executable process does not have KSN-trusted status. If the allowing rule is applied or the process has KSN-trusted status, the command line can be launched with or without command for execution.

  Kaspersky Embedded Systems Security 2.2 recognizes the following command line interpreters:

  - cmd.exe
  - powershell.exe
  - python.exe
  - perl.exe

5. In the **Rules** section, configure the settings for applying rules:

   a. Click the **Rules list** button to add allowing rules for task launch control.

   > Kaspersky Embedded Systems Security 2.2 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 applications 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 2.2 applies two preset rules that allow a list of scripts, MSI packages, and startup files based on a certificate.

6. In the **Rules usage scope** section, specify the following settings:

   - **Apply rules to executable files**.

     The check box enables / disables control over start of program executable files.

     If this check box is selected, Kaspersky Embedded Systems Security 2.2 allows or blocks start of program executable files using the specified rules whose settings specify Executable files as the scope.

     If the check box is cleared, Kaspersky Embedded Systems Security 2.2 does not control start of program executable files using specified rules. Startup of program executable files is allowed.

     The check box is selected by default.

   - **Monitor loading of DLL modules**.

     The check box enables / disables monitoring of DLL modules loading

     If this check box is selected, Kaspersky Embedded Systems Security 2.2 allows or blocks downloads 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 2.2 does not monitor downloads of DLL modules using the specified rules. Download of DLL modules is allowed.

     The check box is active if the check box Apply rules to executable files is selected.

     The check box is cleared by default.

   > Monitoring download of DLL modules may affect the operating system performance.

- **Apply rules to scripts and MSI packages**.

  The check box enables / disables launch of scripts and MSI packages.

  If this check box is selected, Kaspersky Embedded Systems Security 2.2 allows or blocks runs 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 2.2 does not control launch of scripts and MSI packages using specified rules. Start of scripts and MSI packages is allowed.

  The check box is selected by default.

7. In the **KSN Usage** section, configure the following application launch settings:

   - **Deny applications untrusted by KSN**.

     The check box either enables or disables Applications Launch Control according to their reputation in KSN.

     If this check box is selected, Kaspersky Embedded Systems Security 2.2 blocks any applications from running if they have the untrusted status in KSN. Applications Launch Control allowing rules that apply to KSN-untrusted applications will not trigger. Selecting the check box provides additional protection from malware.

     If the check box is cleared, Kaspersky Embedded Systems Security 2.2 does not take into account the reputation of KSN-untrusted programs and allows or blocks start in accordance with the rules that apply to such programs.

     The check box is cleared by default.

   - **Allow applications trusted by KSN**.

     The check box either enables or disables Applications Launch Control according to their reputation in KSN.

     If this check box is selected, Kaspersky Embedded Systems Security 2.2 allows applications to run if they have KSN-trusted status. Denying application launch control rules that are applied to the KSN-trusted applications have a higher priority: if the application is considered trusted by the KSN services, this application launch will be denied.

     If the check box is cleared, Kaspersky Embedded Systems Security 2.2 does not take into account the reputation of KSN-trusted programs and allows or blocks start in accordance with the rules that apply to such programs.

     The check box is cleared by default.

   - Users and / or user groups allowed to launch applications trusted in KSN.

8. On the **Software Distribution Control** tab, configure the settings for software distribution control (see Section "Configuring Software Distribution Control" on page 172).

9. On the **Task management** tab, configure the scheduled task start settings (see Section "Configuring the task start schedule settings" on page 114).

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

Kaspersky Embedded Systems Security 2.2 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.

About Software Distribution Control

The applications launch control rules generation may be complicated, if you need to also consider software distribution control on a protected computer. For example, for those computers where periodic automatic updates of installed software occur. In this case it is required to update the list of allowing rules after each software update in order for newly created files to be considered in the Applications Launch Control task settings. To simplify launch control in the software distribution scenarios you can use Applications Launch Control subsystem.

A *software distribution package* (also “a 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 the 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 will allow decompression of these trusted packages and automatic start of software, that is created or modified by a trusted package. The extracted files can inherit the trusted attribute of a primary distribution package. A *primary distribution package* is a package, that was added to the list of Software Distribution Control exclusions by user and became a trusted package.

Kaspersky Embedded Systems Security 2.2 controls only full cycles of software distribution. The application cannot correctly process start of files, that are 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 2.2 establishes connection between trusted packages and files created during software distribution procedure with the help of dynamically generated *software distribution cache* (also “distribution cache”). At the first package start Kaspersky Embedded Systems Security 2.2 detects all files created during the software distribution process from this package and stores files’ checksums and paths in the distribution cache. Afterwards the start of all files, that are stored in the distribution cache are allowed by default.

You cannot review, clear or manually modify distribution cache via user interface. The cache is populated and controlled by Kaspersky Embedded Systems Security 2.2.

You can export distribution cache in the configuration file (in XML format) and also clear the cache using command line options.

► *To export distribution cache to a configuration file execute the following command:*

```
kavshell appcontrol /config /savetofile:<full path> /sdc
```

► *To clear distribution cache execute the following command:*

```
kavshell appcontrol /config /clearsdc
```

Kaspersky Embedded Systems Security 2.2 updates distribution cache every 24 hours. If full path or checksum of a file that was previously allowed is changed, the application deletes this file record from the distribution cache. If the Applications Launch Control task is started in an active mode, further starts of this file will be blocked.

Extracted files processing

The trusted attribute for all extracted files of the trusted package is inherited upon the first start of the package. If you clear the check box after the first start the inheritance for all extracted files of this package will still be maintained. To reset the firstly applied inheritance for 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, that are created by a trusted primary distribution package, acquire the trusted attribute as their checksums are added to the distribution cache when the software distribution package from the exclusion list is opened for the first time. Hence, a distribution package itself and all extracted files of this package will also be trusted. By default the number of levels for the trusted attribute inheritance is unlimited.

The trusted attribute will be maintained by extracted files after the operating system restart.

The files processing is configured in the Software Distribution Control settings (see Section "Configuring Software Distribution Control" on page 172) by selecting or clearing the **Allow launching to all files from this distribution package extraction chain** check box.

For example, you add a test.msi package containing a number of other packages and applications to the exclusions list and select the check box. In this case, all packages and applications that are contained in the test.msi package, are allowed to be run or 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 from a primary trusted package directly (nested on the first level). The checksums of such files are stored in the distribution cache. All files nested on the second level and further will be blocked by the Default Deny principle.

Interaction with the applications launch control rules 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 the KSN conclusions

Untrusted KSN conclusions have a higher priority than the software distribution control exclusions: decompression of a trusted package or start of files created and modified by this package will be blocked, if untrusted conclusion for these files is received form KSN.

Configuring Software Distribution Control

► *To add a trusted distribution package, do the following:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree and select the administration group for which you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring policy" on page 84).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in Application settings window of Kaspersky Security Center" on page 96).

     If a device is being managed by an active Kaspersky Security Center policy and this policy blocks changes to the application settings, these settings cannot be edited in the **Application settings** window.
3. In the **Local activity control** section, click the **Settings** button in the **Applications Launch Control** section.

   The **Applications Launch Control** window opens.
4. On the selected 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 for 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 is selected in the **Applications Launch Control** task settings.
5. 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 the Windows Installer.

   If the check box is selected, the application will always allow files installed via the Windows Installer to start.

   If the check box is cleared, the application will not be unconditionally allowed, even if it is started via the Windows Installer.

   The check box is selected by default.

   The check box is not editable if **Automatically allow software distribution for 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 updating operating system files and also prevent files extracted from a distribution package from starting.

6. 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 2.2 automatically allows Microsoft Windows deployment using the System Center Configuration Manager.
   The application allows software distribution only via Background Intelligent Transfer Service.

   The application controls start of the objects with the following extensions:

   - .exe
   - .msi

   The check box is cleared by default.

> The application controls software distribution cycle on the computer from the package delivery to the installation/update. The application does not control processes if any of the distribution stages was performed before the installation of the application on the computer.

7. To edit the list of trusted distribution packages, click the **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**

          If this option is selected, the presence of a digital certificate is specified as the 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. This option is recommended if you want to allow the start of any applications that are trusted in the operating system.

        - **Use SHA256 hash**

          If this option is selected, the checksum value of the file, which is used to generate the rule, is specified as the 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 value.

          This option is recommended for cases when the generated rules are required to meet ultimate security level: SHA256 checksum may be applied as a unique file ID. The usage of SHA256 checksum as a rule triggering criterion constricts the rule usage scope up to one file.

          This option is selected by default.

   - **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 2.2 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 he list of trusted distribution packages from the configuration file. The file recognized by Kaspersky Embedded Systems Security 2.2 must satisfy the following parameters:

  - The file has a text extension.
  - 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>:<hash SHA256>.
    - <hash SHA256>*<file name>.

  In the **Open** window, specify the configuration file containing a list of trusted distribution packages.

8. 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.

9. Click **OK**.

Your newly configured settings have been saved.

Enabling the Default Allow mode

The Default Allow mode allows all applications to start, if they are not blocked by rules or by KSN untrusted conclusion. Default Allow mode can be enabled by adding specific allowing rules. You can enable Default Allow only for scripts or for all executable files.

► *To add a Default Allow rule:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree and select the administration group for which you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring policy" on page 84).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in Application settings window of Kaspersky Security Center" on page 96).

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

3. In the **Local Activity Control** section, click the **Settings** button in the **Applications Launch Control** block.
4. On the **General** tab, click the **Rules list** button.

   The **Applications Launch Control rules** window opens.
5. Click the **Add** button and in the context menu of the button select **Add one rule** option.

   The **Rule settings** window opens.
6. In the **Name** field, enter the name of the rule.
7. In the **Type** drop down list, select the **Allowing** rule type.
8. 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 applications executable files.
   - **Scripts and MSI packages** if you want the rule to control launch of scripts and MSI packages.
9. In the **Rule triggering criterion** section, select a **Path to file** option.
10. Enter the following mask: **?:**
11. Click **OK** in the **Rule settings** window.

Kaspersky Embedded Systems Security 2.2 applies the Default Allow mode.

About generating Applications Launch Control rules for all computers in Kaspersky Security Center

You can create lists of Applications Launch Control rules using Kaspersky Security Center tasks and policies for all computers and groups of computers on the corporate network at once. This scenario is recommended if the corporate network does not have a reference machine and you are unable to create a common list of rules using a task to automatically generate allowing rules based on applications installed on the reference machine.

The Applications Launch Control component is installed with two predefined allowing rules:

- Allowing rule for scripts and MSI with operating system trusted certificate.
- Allowing rule for executable files with operating system trusted certificate.

You can create lists of Applications Launch Control rules on the side of Kaspersky Security Center in two ways:

- Using a Rule Generator for Applications Launch Control group task for Applications Launch Control.

  When this scenario is used, 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 network folder. You can then manually import the created list of rules into the Applications Launch Control task of 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 completed.

  This scenario is recommended when you need to create lists of Applications Launch Control rule on short notice. It is recommended to configure the scheduled launch of the Rule Generator for Applications Launch Control task only if the scope of application of the allowing rules includes folders, containing files you know to be safe.

Before using the Applications Launch Control policy in the network, make sure 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 Automatic Rules Generators 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 operation of the Applications Launch Control task in **Statistics only** mode.

  When this scenario is used, Kaspersky Embedded Systems Security 2.2 does not deny applications launches, but while Applications Launch Control run in **Statistics only** mode, it reports all allowed and denied applications launches across all network computers in the Kaspersky Security Center **Events** section. Kaspersky Security Center generates unified list of denied application launch events, based on the task log.

  You need to configure the task execution period so that all possible operation scenarios of protected computers and groups of computers and at least one restart would be performed during the specified time period. Then as rules are added to the Applications Launch Control task you can import data on application launches from the saved Kaspersky Security Center event report file (in 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 quantity of differently typed computers (see Section "About using profile to configure Applications Launch Control tasks in Kaspersky Security Center policy" on page 164) (with a different set of 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.

It is recommended to 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). It is recommended to use the Rule Generator for Applications Launch Control task or the Applications Launch Control policy in **Statistics only** mode, run on computers in the test administration group, in order to generate an updated list of rules. The test administration group includes computers required for the test launch of new applications before they are installed on network computers.

Before adding allowing rules, select one of the available rule application modes (see Section "Configuring Applications Launch Control task settings" on page 165). The list of Kaspersky Security Center policy rules displays only those rules that are specified by the policy, regardless of the rule application mode. The list of local rules displays all applied rules - both local rules and rules added through a policy.

In this section

Creating allowing rules from Kaspersky Security Center events

► *To generate allowing rules using the 'Create allowing rules for applications from Kaspersky Security Center events' option in the Applications Launch Control, do the following:*

1. In the Kaspersky Security Center Administration Console, expand the **Managed devices** node.
2. Expand the administration group whose policy settings you want to configure and select the **Policies** tab in the details pane.
3. Select **Properties** in the context menu of the policy that you want to configure.

   The **Properties: <Policy name>** window opens.
4. In the **Local Activity Control** section, click the **Settings** button in the **Applications Launch Control** block.
5. On the **General** tab, click the **Rules list** button.

   The **Applications Launch Control rules** window opens.
6. Click the **Add** button and in the context menu of the button select **Create allowing rules for applications from Kaspersky Security Center events**.
7. 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 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 **Applications launch control rules generation** window opens.
8. Configure the following request settings:
   - **Administration Server address**
   - **Port**
   - **User**
   - **Password**
9. Select the types of events that you want to base the generation task on:
   - **Statistics Only mode: application launch denied**.
   - **Application launch denied**.
10. Select the time period from the **Request events generated within the period** drop-down list.
11. Click the **Generate rules** button.
12. Click the **Save** button in the **Applications Launch Control rules** window.

    Rules list in the Applications Launch Control policy will be filled up with new rules generated basing on a system data of 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 2.2 adds the selected rules from the blocking events to the already specified rules. The rules with same hash are not added, as all rules in a list must be unique.

Importing Applications Launch Control rules from XML file

You can import reports generated upon the Rule Generator for Applications Launch Control group task completion 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 network folder. Each file with the list of rules is created based on analysis of files executed and applications launched on each separate computer on the corporate network. Lists contain allowing rules for files and applications whose type matches the type specified in the Rule Generator for Applications Launch Control group task.

> The process of configuring the settings of Kaspersky Embedded Systems Security 2.2 functional components in Kaspersky Security Center is similar to local configuration of the settings of these components in the Application Console. Detailed instructions on how to configure task settings and application functions are provided in the relevant sections of the *Kaspersky Embedded Systems Security 2.2 User's Guide*.

► *To specify allowing rules for application launch for a group of computers based on an automatically generated list of allowing rules, take the following steps.*

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.
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 content of the folders containing allowed applications: exclude default folders from the task scope or add new folders manually.
   - In the **Options** section, specify the task operations while it is running and after it is completed. Specify the criterion based on which the rules will be generated and the name of the file to which these 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 2.2 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 that you have created, and click the **Start** button to start the task.

   When the task is completed, automatically generated lists of allowing rules are saved in a shared network folder in XML files.

   > Before using the Applications Launch Control policy in the network, make sure 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 Automatic Rules Generators task for computer control rules on the test computer group or on a template machine.

4. Add the generated lists of allowing rules to the Applications Launch Control task. To do so, in the properties of the policy being configured, 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 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 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.

   d. In the standard window of Microsoft Windows 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 application launch, in the policy in the properties of the Applications Launch Control task select the **Active** task run mode.

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 launching only those applications for which allowing rules have been created.

Importing rules from file of Kaspersky Security Center report on blocked applications

You can import data on blocked application launches from the report generated in Kaspersky Security Center after completion of the Applications Launch Control task 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 the report on events occurring during an Applications Launch Control task, you can keep track of the applications whose launch is blocked.

> When importing data from the 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 allowing rules for application start for a group of computers based on the blocked applications report from Kaspersky Security Center, take the following steps:*

1. In the policy properties in the settings of the Applications Launch Control task, select the **Statistics only** operation mode.
2. In the policy properties in the **Events** section, make sure that:
   - The **Critical Events** tab of the application launch denied event shows an event storage time that exceeds the planned time of task operation in **Statistics only** mode (the default value is 30 days).
   - The **Warning** tab of the *Statistics only: application launch denied event* shows an event storage time that exceeds the planned time of task operation in **Statistics only** mode (the default value is 30 days).

   When the period specified in the **Storage time** column elapses, information about 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 storage time for the specified events.

3. When the task has been completed, export the logged events into a TXT file:

   a. To do so, in the properties of the Applications Launch Control task, expand the **Logs and notifications** node.

   b. In the **Events** child node 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 the **Export events** to file list to save the report on blocked application starts to a TXT file.

   Before importing and applying the generated report in a policy, make sure that the report contains data only on those applications whose start you want to allow.

4. 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 context menu of the button select **Import data of blocked applications 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 Applications Launch Control rules:
   - **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.

   d. In the standard window of Microsoft Windows that opens, select the TXT file to which events from the blocked application launches report have been exported.

   e. Click **OK** in the Applications Launch Control rules and in the **Task settings** window.

Rules created on the basis of the Kaspersky Security Center report on blocked applications are added to the list of Applications Launch Control rules.

Managing devices connections via Kaspersky Security Center

You can allow or restrict connections of flash drives and other mass storages to all computers on the network by generating unified computer control lists via the Kaspersky Security Center for the groups of computers.

In this section

About Device Control task

Kaspersky Embedded Systems Security 2.2 controls registration and usage of the mass storages 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 is an external device that may be connected to a computer in order to copy or store files.

Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 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:

- *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 2.2 identifies mass storages 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 2.2 during rule generation.

The Device Control task can operate in two modes:

- **Active**. Kaspersky Embedded Systems Security 2.2 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 2.2 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 basing on the information logged during the task running.

About 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 two 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 2.2 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 policy 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 Applications Launch Control group task is completed.

  This scenario is recommended to generate allowing rules list before the first Device Control policy 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 Automatic Rules Generators 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 2.2 does not restrict mass storage devices connections but logs information about all devices connections and mass storages registration on all network computers during the Device Control task running in the **Statistics only** mode; information logged may be found in the Kaspersky Security Center **Events** section. Kaspersky Security Center generates unified list of mass storages 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 storages, 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 policy settings).

  According to this scenario Kaspersky Embedded Systems Security 2.2 generates allowing rules for mass storages 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 2.2 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 2.2 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 rues list filling on the base of system data about all connected devices.

Rules generation based on system data about external devices connected to network computers

You can generate rules (see Section "About generating Device Control rules for all computers via Kaspersky Security Center" on page 182) basing on Windows data about all mass storages 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 storages that are registered by the systems on all network computers.
- Using the **Generate rules based on system data** option in the Device Control policy settings. Use this scenario during the rule generation process to take into account all ever connected mass storages 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 policy settings 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 2.2 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 rues list filling on the base of system data about all connected devices.

In this section

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, take the following steps.*

1. On the **Tasks** tab in the control panel of the group of computers you are configuring, create a Rule Generator for Device Control group task or select an existing task.
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 **Notifications** section, configure the settings for saving the task execution report.
   - In the **Settings** section, specify the task operations after it is completed. Specify the file name where rules generated will be exported.
   - In the **Schedule** section, configure the task launch schedule settings.
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 Device Control you have created and click the **Start** button to start the task.

   When the task is completed, automatically generated lists of allowing rules are saved in a shared network 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 Automatic Rules Generators task for computer control rules on the test computer group or on a template machine.
4. Add the generated lists of allowing rules to the Device Control task. To do so, in the properties of the policy being configured, in the Device Control task settings:

   a. On the **General** tab, click the **Rules list** button.

      The **Device Control rules** window opens.

   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 Device Control rules:

      - **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.

d. In the standard window of Microsoft Windows that opens, select XML files created after completion of the Rule Generator for Device Control group task.

e. Click **OK** in the Device Control rules and in the **Task settings** window.

5. 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.

Creating allowing rules on the basis of 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 policy, take the following steps:*

1. If necessary, connect a new mass storage that you want to trust to a computer with the Kaspersky Security Center Administration Console installed.
2. In the Kaspersky Security Center Administration Console, expand the **Managed devices** node.
3. Expand the administration group whose policy settings you want to configure and select the **Policies** tab in the details pane.
4. Select **Properties** in the context menu of the policy that you want to configure.
5. The **Properties: <Policy name>** window opens.
6. In the policy settings open the Device Control task settings and take the following steps:

   a. On the **General** tab, click the **Rules list** button.

   The **Device Control rules** window opens.

   b. Click the **Add** button and in the context menu that opens select the **Generate rules based on system data** option.

   c. Select the principle for adding the 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 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.
7. Click **OK** in the **Device Control rules** and in the **Task settings** window.

Rules list in the Device Control policy 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 system data** option in the Device Control policy, take the following steps:*

1. In the Kaspersky Security Center Administration Console, expand the **Managed devices** node.
2. Expand the administration group whose policy settings you want to configure and select the **Policies** tab in the details pane.
3. Select **Properties** in the context menu of the policy that you want to configure.
4. The **Properties: <Policy name>** window opens.
5. In the **Local activity control** section, click the **Settings** button in the **Device Control** section.
6. On the **General** tab, click the **Rules list** button.

   The **Device Control rules** window opens.
7. Click the **Add** button and in the context menu, select **Generate rules based on connected devices**.

   The **Generate rules based on system data** window opens.
8. In the list of detected devices connected to the protected computer, select the devices you want to generate allowing rules for.
9. Click the **Add** rules for devices selected button.
10. Click the **Save** button in the **Device Control** window.

Rules list in the Device Control policy 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 file of Kaspersky Security Center report on restricted devices

You can import data on restricted devices connections from the report generated in Kaspersky Security Center after completion of the Device Control task in **Statistics only** mode 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.

When importing data from the report on restricted devices into policy settings, make certain that the list you are using contains only devices which connection you want to allow.

► *To specify allowing rules for devices connection for a group of computers based on the Kaspersky Security Center report about restricted devices, take the following steps:*

1. In the policy properties in the settings of the Device Control task, select the **Statistics only** mode.
2. In the policy properties in the **Events** section, make sure that:
   - The **Critical Events** tab of the *Mass storage restricted* event shows an event storage time that exceeds the planned time of task operation in **Statistics only** mode (the default value is 30 days).
   - The **Warning** tab of the *Statistics only: untrusted mass storage detected* event shows an event storage time that exceeds the planned time of task operation in **Statistics only** mode (the default value is 30 days).

   When the period specified in the **Storage time** column 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.

3. When the task has been completed, export the logged events into a TXT file. To do so, expand the **Logs and notifications** node and in the **Events** child node create a selection of events based on the *Denied* 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 list to save the report on blocked application starts 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.

4. Import data about restricted devices connections into the Device Control policy. To do so, in the properties of the policy being configured, in the Device Control task settings, take the following steps:
   a. On the **General** tab, click the **Rules list** button.

      The **Device Control rules** window opens.

   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 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.

   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 **OK** in the **Device Control rules** and in the **Task settings** window.

Rules created on the basis of the Kaspersky Security Center report on restricted devices are added to the list of Device Control rules.

Network activity control

This section contains information about the Firewall Management task.

Firewall Management

This section contains information about the Firewall Management task and how to configure it.

In this section

About the Firewall Management task

Kaspersky Embedded Systems Security 2.2 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 2.2 graphical interface. During the Firewall Management task Kaspersky Embedded Systems Security 2.2 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 2.2.

> If Windows Firewall is turned off during installation of Kaspersky Embedded Systems Security 2.2, 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 2.2 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 2.2 monitors the following:

- Operating status of the Windows Firewall.
- Status of rules added after installation of Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 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 2.2 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 2.2 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 2.2 deletes the rule.
- If an existing rule is deleted from the Windows Firewall settings, Kaspersky Embedded Systems Security 2.2 restores the rule.
- If the parameters of an existing rule are changed in the Windows Firewall settings, Kaspersky Embedded Systems Security 2.2 rolls back the changes.
- If a new rule is created in the Firewall Management settings, Kaspersky Embedded Systems Security 2.2 forcibly applies the rule to Windows Firewall.
- If an existing rule is deleted from the Firewall Management settings, Kaspersky Embedded Systems Security 2.2 forcibly deletes the rule from the Windows Firewall settings.

Kaspersky Embedded Systems Security 2.2 does not work with blocking rules or rules controlling outgoing network traffic. Upon start of the Firewall Management task, Kaspersky Embedded Systems Security 2.2 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 2.2 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.

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 and select the administration group for which you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring policy" on page 84).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in Application settings window of Kaspersky Security Center" on page 96).

     If a device is being managed by an active Kaspersky Security Center policy and this policy blocks changes to the application settings, these settings cannot be edited in the **Application settings** window.
3. In the **Network activity control** section click the **Settings** button in the **Firewall Management** block**.**
4. Click the **Rules list** button in the window that opens.

   The **Rules list** window opens.
5. Depending on the type of the rule whose status you want to modify, select **Applications** or **Ports**.
6. 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.
7. Click **Save** in the **Rules list** 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 and select the administration group for which you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring policy" on page 84).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application**

settings window (see Section "Configuring local tasks in Application settings window of Kaspersky Security Center" on page 96).

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

3. In the **Network activity control** section click the **Settings** button in the **Firewall Management** block.
4. Click the **Rules list** button in the window that opens.

   The **Rules list** window opens.
5. 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.
6. 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.
7. Click **OK** in the **Application rule** or **Port rule** window.
8. 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. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree and select the administration group for which you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
    - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring policy" on page 84).
    - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in Application settings window of Kaspersky Security Center" on page 96).

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

3. In the **Network activity control** section click the **Settings** button in the **Firewall Management** block**.**
4. Click the **Rules list** button in the window that opens.

    The **Rules list** window opens.

5. Depending on the type of rule whose status you want to modify, select the **Applications** or **Ports** tab.
6. In the rule list, select the rule you want to delete.
7. Click the **Remove** button.

    The selected rule is deleted.

8. Click **Save** in the **Firewall rules** window.

The specified Firewall Management task settings are saved. The new rule parameters will be sent to Windows Firewall.

System Inspection

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

In this chapter

File Integrity Monitor

This section contains information about starting and configuring the File Integrity Monitor task.

In this section

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 protected device is not physically present on a protected computer. Kaspersky Embedded Systems Security 2.2 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 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 exclusions for the monitoring scope (see Section "Configuring monitoring rules" on page 198). 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 2.2 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 2.2 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 2.2 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 2.2 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 2.2 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 2.2 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 2.2 considers all available file operation marker. You can select file operation markers manually in the task's rule settings.

Table 36. 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

File operation ID	File operation marker	Supported file systems
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

Configuring the File Integrity Monitor task

You can change the default settings of the File Integrity Monitor task (see the table below).

Table 37. 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 directories 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.
Consider excluded monitoring scope	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 2.2 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 2.2 generates an audit event.
Task start schedule	First run is not scheduled	You can configure the settings of scheduled startup of the task.

► *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 and select the administration group for which you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring policy" on page 84).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in Application settings window of Kaspersky Security Center" on page 96).

   > If a device is being managed by an active Kaspersky Security Center policy and this policy blocks changes to the application settings, these settings cannot be edited in the **Application settings** window.
3. In the **System Inspection** section in the **File Integrity Monitor** block, click the **Settings** button.

   The **File Integrity Monitor** window opens.
4. 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 2.2 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 198) to be monitored by the task.
5. On the **Task Management** tab, start the task based on a schedule (see Section "Managing task schedules" on page 114).
6. Click **OK** to save changes.

Configuring monitoring rules

By default, a monitoring scope is not specified and the task does not monitor file operations in any directory.

► *To add a monitoring scope, perform the following steps:*

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree and select the administration group for which you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring policy" on page 84).

- To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in Application settings window of Kaspersky Security Center" on page 96).

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

3. In the **System Inspection** section in the **File Integrity Monitor** block, click the **Settings** button.

   The **Properties: File Integrity Monitor** window opens.
4. In the **Monitoring scope** section, click the **Add** button.

   The **Monitoring scope** window opens.
5. 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 directory <\dir>;
     - <\dir*\name.ext> - all files with the name <name> and extension <ext> in directory <\dir> and all of its subdirectories.

   > 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 2.2 will not add the specified monitoring scope.
6. In the **Trusted users** tab, click the **Add** button.

   The standard Microsoft Windows **Select Users or Groups** window opens.
7. 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 2.2 treats all users not on the trusted user list as untrusted (see Section "About file operation monitoring rules" on page 195), and generates Critical events for them.
8. Select the **File operation markers** tab.

9. 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 195) select the check boxes next to the operations you want to monitor.

> By default Kaspersky Embedded Systems Security 2.2 detects all file operation markers, the **Detect file operations basing on all recognizable markers** option is selected.

10. If you want Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 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**

11. 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 195), and select the check boxes next to the operations you want to monitor.

12. If necessary, add excluded monitoring scopes by performing the following steps:

    a. Select the **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 2.2 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 2.2 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.

13. Click **OK** in the **Monitoring Scope** window.

    The specified rule settings will be applied to the selected monitoring scope of the File Integrity Monitor task.

Log Inspection

This section contains information about the Log Inspection task and task settings.

In this section

About the Log Inspection task

When the Log Inspection task runs, Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 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 2.2 records a Critical event in the Log Inspection task log.

By default Log Inspection task does not apply 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.

Configuring predefined task rules

► *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 and select the administration group for which you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring policy" on page 84).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in Application settings window of Kaspersky Security Center" on page 96).

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

3. In the **System Inspection** section click the **Settings** button in the **Log Inspection** block.

   The **Log Inspection settings** window opens.
4. Select the **Predefined rules** tab.
5. Select or clear check box **Apply predefined rules for Log Inspection**.

   If this check box is selected, Kaspersky Embedded Systems Security 2.2 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 2.2 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, click the **Advanced settings** button.

   The **Log Inspection** window opens.
8. 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.
9. In the **Network logon detection** section, indicate the start and end of the time interval during which Kaspersky Embedded Systems Security 2.2 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.
13. An entered IP-address is added to the list of trusted IP-addresses.
14. On the **Task management** tab configure the task start schedule (see Section "Configuring the task start schedule settings" on page 114).
15. 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. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree and select the administration group for which you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of computers, select the **Policies** tab and open the **Properties: <Policy name>** window (see Section "Configuring policy" on page 84).
   - To configure the application for a single computer, select the **Devices** tab and open the **Application settings** window (see Section "Configuring local tasks in Application settings window of Kaspersky Security Center" on page 96).

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

3. In the **System Inspection** section click the **Settings** button in the **Log Inspection** block.

   The **Log Inspection** window opens.
4. On the **Log Inspection rules** tab select or clear the **Apply custom rules for Log Inspection** check box.

   If the check box is selected, Kaspersky Embedded Systems Security 2.2 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 2.2 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.

5. To add a new custom rule, click the **Add** button.

   The **Log inspection rules** window opens.

6. In the **General** section enter the following information about the new 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.
7. 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.

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 2.2:

- 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 Application settings window of Kaspersky Security Center" on page 96).
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 (see Section "Managing applications launch from Kaspersky Security Center" on page 164) 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 servers 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 165).
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 165),
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 Kaspersky Embedded Systems Security 2.2 from the command line

This section describes working with Kaspersky Embedded Systems Security 2.2 from the command line.

In this chapter

Command line commands

You can perform basic Kaspersky Embedded Systems Security 2.2 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 2.2.

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 2.2.

Certain Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 (see the table below).

Table 38. Kaspersky Embedded Systems Security 2.2 commands

Command	Description
KAVSHELL APPCONTROL (see Section "Filling list of Applications Launch Control rules KAVSHELL APPCONTROL" on page 220)	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 217)	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 218)	Starts the Rule Generator for Applications Launch Control task.
KAVSHELL VACUUM (see Section "Kaspersky Embedded Systems Security 2.2 log files defragmentation. KAVSHELL VACUUM" on page 228)	Defragments Kaspersky Embedded Systems Security 2.2 log files.
KAVSHELL PASSWORD	Manages password protection settings.
KAVSHELL HELP (see Section "Displaying Kaspersky Embedded Systems Security 2.2 command help. KAVSHELL HELP" on page 210)	Displays Kaspersky Embedded Systems Security 2.2 command help.
KAVSHELL START (see Section "Starting and stopping Kaspersky Security service KAVSHELL START, KAVSHELL STOP" on page 211)	Starts Kaspersky Embedded Systems Security 2.2 service.
KAVSHELL STOP (see Section "Starting and stopping Kaspersky Security service KAVSHELL START, KAVSHELL STOP" on page 211)	Stops Kaspersky Embedded Systems Security 2.2 service.
KAVSHELL SCAN (see Section "Scanning selected area. KAVSHELL SCAN" on page 211)	Creates and starts a temporary On-Demand Scan task with the scan scope and security settings set by the command modifiers.
KAVSHELL SCANCRITICAL (see Section "Starting the Critical Areas Scan task. KAVSHELL SCANCRITICAL" on page 215)	Starts the Critical Areas Scan system task.
KAVSHELL TASK (see Section "Managing specified task asynchronously. KAVSHELL TASK" on page 215)	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 216)	Starts or stops all Real-Time Protection tasks.
KAVSHELL UPDATE (see Section "Starting Kaspersky Embedded Systems Security 2.2 databases update task. KAVSHELL UPDATE" on page 221)	Starts Kaspersky Embedded Systems Security 2.2 bases update task with the settings specified using command modifiers.
KAVSHELL ROLLBACK (see Section "Rolling back Kaspersky Embedded Systems Security 2.2 database updates. KAVSHELL ROLLBACK" on page 224)	Rolls back bases to the previous version.
KAVSHELL LICENSE (see Section "Activating application KAVSHELL LICENSE" on page 225)	Manages keys.

Command	Description
KAVSHELL TRACE (see Section "Enabling, configuring and disabling trace log. KAVSHELL TRACE" on page 226)	Enables or disables the tracing log, manages settings of the tracing log.
KAVSHELL DUMP (see Section "Enabling and disabling dump file creation. KAVSHELL DUMP" on page 229)	Enables or disables Kaspersky Embedded Systems Security 2.2 process dump files in case of abnormal termination of processes.
KAVSHELL IMPORT (see Section "Importing settings. KAVSHELL IMPORT" on page 230)	Imports general Kaspersky Embedded Systems Security 2.2 settings, functions, and tasks from a configuration file created beforehand.
KAVSHELL EXPORT (see Section "Exporting settings. KAVSHELL EXPORT" on page 231)	Exports all Kaspersky Embedded Systems Security 2.2 settings and existing tasks to a configuration file.
KAVSHELL DEVCONTROL (see Section "Filling the list of Device Control rules. KAVSHELL DEVCONTROL" on page 220)	Adds to the list of generated device control rules according to selected method.

Displaying Kaspersky Embedded Systems Security 2.2 command help. KAVSHELL HELP

To obtain the list of all Kaspersky Embedded Systems Security 2.2 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 215) 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 39. 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. When a folder is selected, Kaspersky Embedded Systems Security 2.2 will also check all subfolders for the folder in question. The symbols * or ? can be used to scan a group of files.
<folders>	
<network path>	
/MEMORY	Scan objects in RAM
/SHARED	Scan shared folders on the computer
/STARTUP	Scan startup 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 2.2 will scan objects by their format.	
/FA	Scan all objects
/FC	Scan objects by format (by default). Kaspersky Embedded Systems Security 2.2 scans only objects format of which are included into the list of formats of infectable objects.

Key	Description
/FE	Scan objects by extension. Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 will perform the **Skip** action.	
DISINFECT	Disinfect, skip if disinfection is not possible
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 2.2 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 2.2 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 2.2 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 2.2 scans all sizes of objects by default.

Key	Description
/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 2.2 will not use heuristic analyzer.
/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 2.2. 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 2.2 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 2.2 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 2.2 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 40. 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 2.2 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 2.2 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 41. KAVSHELL TASK command modifiers

Key	Description
Without keys	Returns the list of all existing Kaspersky Embedded Systems Security 2.2 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 2.2 assigns to tasks. To view Kaspersky Embedded Systems Security 2.2 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.

Return codes for the KAVSHELL TASK command (see Section "Return codes for KAVSHELL TASK command" on page 233).

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 42. 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>
```

Examples of the KAVSHELL APPCONTROL /CONFIG command

► *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 43. `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 - Statistics only.
`/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:<edms>] [/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 44. 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 launches 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 45. `KAVSHELL SCAN` 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 46. 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 2.2 databases update task. KAVSHELL UPDATE

The `KAVSHELL UPDATE` command can be used to start the Kaspersky Embedded Systems Security 2.2 databases update command in the synchronous mode.

The Kaspersky Embedded Systems Security 2.2 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 2.2 on computers using Kaspersky Security Center, refer to the section "Managing Kaspersky Embedded Systems Security 2.2 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.

Command syntax for KAVSHELL UPDATE

```
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).

Examples of the KAVSHELL UPDATE command

- ► *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
```

- ► *In order to download Kaspersky Embedded Systems Security 2.2 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 47. KAVSHELL UPDATE command keys

Key	Description
Updates source (mandatory key). Specify one or multiple sources. Kaspersky Embedded Systems Security 2.2 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 2.2 will automatically detect the settings of the proxy server used in the local area network.

Key	Description
/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 2.2 will contact the proxy server under the **Local system** (**SYSTEM**) account **1** – in-built Microsoft Windows NTLM-authentication; Kaspersky Embedded Systems Security 2.2 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	
/NOFTPPASSIVE	If this key is specified, Kaspersky Embedded Systems Security 2.2 will use the active FTP server mode to connect to the protected computer. If this key is not specified, Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 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 2.2 will detect the location of the protected computer based on the regional settings on the computer where the Application Console is installed.

Key	Description
/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 2.2. If this key is not specified, update_<kavshell_pid>, for example, update_1234 will be used. In the Application Console the task will be automatically assigned 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 2.2 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 2.2 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 2.2 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 234).

Rolling back Kaspersky Embedded Systems Security 2.2 database updates. KAVSHELL ROLLBACK

The `KAVSHELL ROLLBACK` command can be used to perform a Kaspersky Embedded Systems Security 2.2 database rollback system task (roll back Kaspersky Embedded Systems Security 2.2 databases to the previously installed version). The command is performed synchronously.

Command syntax:

```
KAVSHELL ROLLBACK
```

Return codes for the KAVSHELL ROLLBACK command (on page 235).

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 48. 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 233).

Activating application KAVSHELL LICENSE

Kaspersky Embedded Systems Security 2.2 keys and activation codes can be managed using the `KAVSHELL LICENSE` command.

> Password might be required to execute the command. To enter the current password use `[/pwd:<password>]` key.

Command syntax for KAVSHELL FULLSCAN

```
KAVSHELL LICENSE [/ADD:<key file | activation code> [/R] | /DEL:<key | activation code number>]
```

Examples of the KAVSHELL SCAN command

► *To activate the application, execute the command:*

```
KAVSHELL.EXE LICENSE / ADD: <activation code or key>
```

► *To view information on added keys, execute the command:*

```
KAVSHELL LICENSE
```

► *To remove an added key with number 0000-000000-00000001, execute the command:*

```
KAVSHELL LICENSE /DEL:0000-000000-00000001
```

`The KAVSHELL LICENSE` command can run with keys or without them (see table below).

Table 49. KAVSHELL LICENSE command keys

Key	Description
Without keys	The command returns the following information about added keys: • Key. • License type (commercial). • Duration of the license associated with the key. • Key status (active or additional). If the value specified is *, the key has been added as an additional key.
/ADD:<key file name or activation code>	Adds key via the specified file or activation code. System environment variables can be used when specifying the path to a key file; user environment variables are not allowed.
/R	The /R activation code or key is an addition to the /ADD activation code or key and indicates that the activation code or key being added is an additional activation code or key.
/DEL:<key or activation code>	Deletes the key with the specified number or the selected activation code.

Return codes for KAVSHELL LICENSE command (see Section "Return codes for the KAVSHELL LICENSE command" on page 235).

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 2.2 subsystems and to set the log detail level.

> Kaspersky Embedded Systems Security 2.2 writes information to trace files and the dump file in unencrypted form.

Command syntax for KAVSHELL TRACE

```
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 log settings with values of /S and /LVL keys (see table below).

Table 50. 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. Network paths in UNC (Universal Naming Convention) format can be used, but paths to folders on the network drives of the protected computer 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 2.2 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.

Examples of the KAVSHELL TRACE command

- ► *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 236).

Kaspersky Embedded Systems Security 2.2 log files defragmentation. KAVSHELL VACUUM

Using the `KAVSHELL VACUUM` command you can defragment the application log files. It allows to avoid system errors or errors during the Kaspersky Embedded Systems Security 2.2 work that are connected to a hard log storage.

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 2.2 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 2.2\2.2\Reports. If you have manually specified another path for the log storage, the `KAVSHELL VACUUM` command executes defragmentation for files in folder that is specified in the Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 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 2.2 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 2.2 creates in the %SYSTEMDRIVE%\System Volume Information directory 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 2.2. The file only contains current information about files existing in the system: if a file is removed, Kaspersky Embedded Systems Security 2.2 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 2.2 does not pause the protection (unlike in cases of manual deletion of klamfb.dat).
- Kaspersky Embedded Systems Security 2.2 may increase the computer workload after the data is cleared in klamfb.dat. In this case, Anti-Virus scans all files accessed for the first time after the clearing of klamfb.dat. After the scan, Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 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).

Command syntax for KAVSHELL DUMP

```
KAVSHELL DUMP </ON /F:<folder with the dump file>|/SNAPSHOT /F:< folder
with the dump file> / P:<pid> | /OFF>
```

Examples of the KAVSHELL DUMP command

► *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 /P:1234
```

► *To disable generation of the dump file, execute the command:*

```
KAVSHELL DUMP /OFF
```

Table 51. 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. If a path to a non-existent folder is specified, no dump file will be created. Network paths can be used in UNC (Universal Naming Convention) format, but paths to folders on network drives of the protected computer 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 specified Kaspersky Embedded Systems Security 2.2 process in progress 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 236).

Importing settings. KAVSHELL IMPORT

The `KAVSHELL IMPORT` command allows you to import the settings of Kaspersky Embedded Systems Security 2.2, its features and tasks from a configuration file to a copy of Kaspersky Embedded Systems Security 2.2 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.

Command syntax for KAVSHELL IMPORT

```
KAVSHELL IMPORT <name of configuration file and path to file>
```

Examples of KAVSHELL IMPORT command

```
KAVSHELL IMPORT Host1.xml
```

Table 52. 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 237).

Exporting settings. KAVSHELL EXPORT

The `KAVSHELL EXPORT` command allows you to export all of the settings of Kaspersky Embedded Systems Security 2.2 and its current tasks to a configuration file in order to import them later into copies of Kaspersky Embedded Systems Security 2.2 installed on other computer.

Command syntax for KAVSHELL EXPORT

```
KAVSHELL EXPORT <name of configuration file and path to file>
```

Examples of KAVSHELL EXPORT command

```
KAVSHELL EXPORT Host1.xml
```

Table 53. 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 237).

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>
```

Examples of KAVSHELL OMSINFO command

```
KAVSHELL OMSINFO C:\Users\Admin\Desktop\omsinfo.json
```

Table 54. 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 55. 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 2.2 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 2.2 service runs under the Local system user account)
-99	Unknown error

Return code for KAVSHELL SCAN and KAVSHELL SCANCRITICAL commands

Table 56. 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 57. Return code for KAVSHELL TASK LOG-INSPECTOR command

Return code	Description
0	Operation completed successfully
-6	Invalid operation (for example, Kaspersky Embedded Systems Security 2.2 service is already running or already stopped)
402	Task is already running (for modifier /STATE)

Return codes for KAVSHELL TASK command

Table 58. Return codes for KAVSHELL TASK command

Return code	Description
0	Operation completed successfully
-2	Service not running
-3	Permissions error

Return code	Description
-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 59. 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 60. 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

Return code	Description
-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 2.2 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 61. 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 62. 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 63. 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 64. 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 65. 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 66. 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 2.2 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 2.2)

Return codes for the KAVSHELL EXPORT command

Table 67. 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 2.2 did not export parameters of some functional component

Integrating with third-party systems

This section describes integration of Kaspersky Embedded Systems Security 2.2 with third-party features and technologies.

In this chapter

Monitoring performance. Kaspersky Embedded Systems Security 2.2 counters

This section provides information about Kaspersky Embedded Systems Security 2.2 counters: System Monitor performance counters, and SNMP counters and traps.

In this chapter

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 2.2 during installation.

In this section

About Kaspersky Embedded Systems Security 2.2 SNMP counters

The **Performance counters** component is included in the installed components of Kaspersky Embedded Systems Security 2.2 by default. Kaspersky Embedded Systems Security 2.2 registers its own performance counters for the Microsoft Windows System Monitor during installation.

Using Kaspersky Embedded Systems Security 2.2 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 2.2 settings and crashes in its operation.

You can view Kaspersky Embedded Systems Security 2.2 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 2.2 settings if the counter values exceed them.

Total number of denied requests

Table 68. 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 2.2 was last started. The application skips objects for which requests for processing are denied by Kaspersky Embedded Systems Security 2.2 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 2.2. • 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 2.2 processes are fully loaded so Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 is not scanning objects on access. Restart Kaspersky Embedded Systems Security 2.2.

Total number of skipped requests

Table 69. 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 2.2 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 2.2 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 2.2 to restore the off-line streams.

Number of requests not processed because of lack of system resources

Table 70. 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 2.2 was last started. Kaspersky Embedded Systems Security 2.2 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 2.2 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 71. 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 2.2 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 72. 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 2.2 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 2.2 will skip the object. Increase the number of Kaspersky Embedded Systems Security 2.2 processes for Real-Time Protection tasks. You can use such Kaspersky Embedded Systems Security 2.2 settings as **Maximum number of active processes** and **Number of processes for Real-Time Protection**.

Maximum number of file interception dispatcher streams

Table 73. 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 2.2 is distributing the load to running processes unevenly. Restart Kaspersky Embedded Systems Security 2.2.

Number of elements in infected objects queue

Table 74. 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 2.2. • Virus outbreaks.
Normal / threshold value	This value may be something other than zero while Kaspersky Embedded Systems Security 2.2 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 2.2 is not processing objects (the file interception dispatcher may have crashed). Restart Kaspersky Embedded Systems Security 2.2. • Not enough processor time to process the objects. Make sure Kaspersky Embedded Systems Security 2.2 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 75. 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 2.2 processes or errors in Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 processes do not have enough processor time to process the objects. Make sure Kaspersky Embedded Systems Security 2.2 receives additional processor time (by lowering other applications' load on the computer, for example). • Kaspersky Embedded Systems Security 2.2 has experienced an error (several streams are idle). Restart Kaspersky Embedded Systems Security 2.2.

Kaspersky Embedded Systems Security 2.2 SNMP counters and traps

This section contains information about Kaspersky Embedded Systems Security 2.2 counters and traps.

In this section

About Kaspersky Embedded Systems Security 2.2 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 2.2 counters and traps using Simple Network Management Protocol (SNMP).

To view Kaspersky Embedded Systems Security 2.2 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 2.2 SNMP counters

This section contains tables with a description of the settings for Kaspersky Embedded Systems Security 2.2 SNMP counters.

In this section

Performance counters

Table 76. Performance counters

Counter	Definition
currentRequestsAmount	Number of requests sent to be processed (on page 241)
currentInfectedQueueLength	Number of elements in the infected objects queue (see Section "Number of elements in infected objects queue" on page 242)
currentObjectProcessingRate	Number of objects processed per second (on page 243)
currentWorkProcessesNumber	Current number of working processes used by Kaspersky Embedded Systems Security 2.2

Quarantine counters

Table 77. 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 counters

Table 78. Backup counters

Counter	Definition
currentBackupStorageSize	Total size of data in Backup (MB)

General counters

Table 79. 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 2.2 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 80. Updates 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 81. 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 2.2; 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 2.2 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 2.2; 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 2.2 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 2.2; 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 2.2 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 2.2; 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 2.2 attempted to place into Backup but was unable to do so; calculated from the time Real-Time File Protection task was last started

SNMP traps

The settings of SNMP traps in Kaspersky Embedded Systems Security 2.2 are summarized in the table below.

Table 82. Kaspersky Embedded Systems Security 2.2 SNMP traps

Trap	Description	Options
eventThreatDetected	An object has been detected.	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 2.2 continues to back up infected objects.	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 2.2 continues to back up infected objects.	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 2.2 continues to quarantine probably infected objects.	eventDateAndTime eventSeverity eventSource

Trap	Description	Options
eventThresholdQuarantineStorageSizeExceeds	Quarantine free space threshold reached. The amount of free size in Quarantine assigned by the **Threshold value for space available (MB)** is less than the specified value. Kaspersky Embedded Systems Security 2.2 continues to quarantine probably infected objects.	eventDateAndTime eventSeverity eventSource
eventObjectNotQuarantined	Quarantine error.	eventSeverity eventDateAndTime eventSource userName computerName objectName storageObjectNotAddedEventReason
eventObjectNotBackuped	Error of saving an object copy in the Backup.	eventSeverity eventDateAndTime eventSource objectName userName computerName storageObjectNotAddedEventReason
eventQuarantineInternalError	Quarantine error.	eventSeverity eventDateAndTime eventSource eventReason
eventBackupInternalError	Backup error.	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.	eventSeverity eventDateAndTime eventSource days

Trap	Description	Options
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.	eventSeverity eventDateAndTime eventSource days
eventApplicationStarted	Kaspersky Embedded Systems Security 2.2 is running.	eventSeverity eventDateAndTime eventSource
eventApplicationShutdown	Kaspersky Embedded Systems Security 2.2 is stopped.	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*.	eventSeverity eventDateAndTime eventSource days
eventLicenseHasExpired	License has expired.	eventSeverity eventDateAndTime eventSource
eventLicenseExpiresSoon	License expires soon. Calculated as the number of days until the expiration date for the license.	eventSeverity eventDateAndTime eventSource days
eventTaskInternalError	Task completion error.	eventSeverity eventDateAndTime eventSource errorCode knowledgeBaseId taskName
eventUpdateError	Error performance an update task.	eventSeverity eventDateAndTime taskName updaterErrorEventReason

The table below describes the settings of traps and possible parameter values.

Table 83. SNMP traps: values of the settings

Setting	Description and possible values
eventDateAndTime	Event time.
eventSeverity	Importance level. The setting can take the following values: • critical (1) – critical • warning (2) – warning • info (3) – informational
userName	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	Event source: functional component where the event was generated. The setting 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 2.2 as a whole rather than operation of individual components • systemAudit (8) – system audit log
eventReason	Event trigger: what provoked the event. The setting 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 2.2 will use the default Backup or Quarantine folder.
objectName	Object name (for example, name of the file where the virus was detected).
threatName	The name of the object according to the Virus Encyclopedia classification. This name is included in the full name of the detected object that Kaspersky Embedded Systems Security 2.2 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 131).

Setting	Description and possible values
detectType	Type of object detected. The setting 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 harm the user's computer or data
detectCertainty	Certainty level for threat detection. The setting can take the following values: • Suspicion (probably infected) – Kaspersky Embedded Systems Security 2.2 has detected a partial match between a section of the object code and the known malicious code section. • Sure (infected) – Kaspersky Embedded Systems Security 2.2 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	Error code.
knowledgeBaseId	Address of a knowledge base article (for example, address of an article that explains a particular error).
taskName	Task name.

Setting	Description and possible values
updaterErrorEventReason	Reason of the update error. The setting 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 setting can take the following values: • reasonUnknown(0) – reason is unknown • reasonStorageInternalError – database error; please restore Kaspersky Embedded Systems Security 2.2. • reasonStorageReadOnly – database is read-only; please restore Kaspersky Embedded Systems Security 2.2. • reasonStorageIOError – input-output error: a) Kaspersky Embedded Systems Security 2.2 is corrupted, please restore Kaspersky Embedded Systems Security 2.2; b) disk with Kaspersky Embedded Systems Security 2.2 files is corrupted. • reasonStorageCorrupted – storage is corrupted; please restore Kaspersky Embedded Systems Security 2.2. • reasonStorageFull – database is full, free up disk space. • reasonStorageOpenError – database file could not be opened; please restore Kaspersky Embedded Systems Security 2.2. • reasonStorageOSFeatureError – some operating system features do not correspond to Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 and its components.

When Kaspersky Embedded Systems Security 2.2 is installed, it registers proprietary module on the system, which facilitates the creation of a Kaspersky Embedded Systems Security 2.2 namespace the WMI root namespace on the local computer. A Kaspersky Embedded Systems Security 2.2 namespace lets you work with Kaspersky Embedded Systems Security 2.2 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 a Real-Time Computer Protection task). 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 84. 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 name of the Kaspersky Embedded Systems Security 2.2 class
- .ProductName=Kaspersky Embedded Systems Security is the Kaspersky Embedded Systems Security 2.2 key parameter

The instance is created in the ROOT\Kaspersky\Security namespace.

Contacting Technical Support

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

In this chapter

How to get technical support

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

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

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

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

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

Technical Support via Kaspersky CompanyAccount

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

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

Kaspersky CompanyAccount is available in the following languages:

- English
- Spanish
- Italian

- German
- Polish
- Portuguese
- Russian
- French
- Japanese

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

Using trace files and AVZ scripts

After you report a problem to Kaspersky Lab Technical Support specialists, they may ask you to generate a report with information about the operation of Kaspersky Embedded Systems Security 2.2 and to send it to Kaspersky Lab Technical Support. Kaspersky Lab Technical Support specialists may also ask you to create a trace file. The trace file allows following the process of how application commands are performed, step by step, in order to determine the stage of application operation at which an error occurs.

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

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

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

AO Kaspersky Lab

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

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

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

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

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

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

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

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

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

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

Information about third-party code

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

Trademark notices

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

Intel and Pentium are trademarks of Intel Corporation in the U.S. and/or other countries.

Microsoft, Active Directory, Excel, Internet Explorer, Outlook, Windows, Windows Server and Windows Vista are registered trademarks of Microsoft Corporation in the United States and other countries.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

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

Protection status

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

Q

Quarantine

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

R

Real-time protection

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

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

S

Security level

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

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.

Index