



Kaspersky Embedded Systems Security

User's Guide

Application version: 2.0

Dear User,

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

Warning! This document is the property of Kaspersky Lab AO (hereinafter referred to as Kaspersky Lab). All rights to this document are protected by the copyright laws of the Russian Federation, and by international treaties. Illegal reproduction or distribution of this document or parts thereof will result in civil, administrative, or criminal liability under applicable law.

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

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

This document may be amended without prior notice.

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

All the registered trademarks and service marks in this document are the property of their respective owners.

Revision date: 5/18/2017

© 2017 Kaspersky Lab AO.

<http://www.kaspersky.com>

<http://support.kaspersky.com>

Table of contents

About this Guide	10
In this document	10
Document conventions	13
About Kaspersky Embedded Systems Security	15
Kaspersky Embedded Systems Security interface	18
Kaspersky Embedded Systems Security Console interface	18
Kaspersky Embedded Systems Security icon in task tray notification area	24
Starting and stopping Kaspersky Embedded Systems Security	26
Starting Kaspersky Embedded Systems Security Console from Start menu	26
Starting and stopping Kaspersky Security service	27
Viewing protection status and Kaspersky Embedded Systems Security information	29
About access permissions for Kaspersky Embedded Systems Security functions	38
About permissions to manage Kaspersky Embedded Systems Security	38
About permissions to manage registered services	41
Configuring access permissions for managing Kaspersky Embedded Systems Security and Kaspersky Embedded Systems Security Service	42
Working with Kaspersky Embedded Systems Security	45
About Kaspersky Embedded Systems Security Console	45
Kaspersky Embedded Systems Security settings in Console	46
Managing Kaspersky Embedded Systems Security via Kaspersky Embedded Systems Security Console on another computer	56
Configuring the Trusted Zone	57
About Kaspersky Embedded Systems Security Trusted Zone	57
Enabling and disabling Trusted Zone usage in Kaspersky Embedded Systems Security tasks	60
Adding exclusions to the Trusted Zone	61
Trusting processes	61
Untrusting processes	64
Disabling Real-Time File Protection during backup	64
Adding an exclusion to the Trusted Zone	65

Managing Kaspersky Embedded Systems Security tasks	67
Kaspersky Embedded Systems Security task categories	67
Saving a task after changing its settings.....	68
Starting / pausing / resuming / stopping tasks manually	69
Managing task schedules	69
Configuring the task launch schedule settings	70
Enabling and disabling scheduled tasks.....	72
Using user accounts to start tasks	72
About using accounts to start tasks.....	73
Specifying a user account to start a task.....	74
Importing and exporting settings.....	75
About importing and exporting settings	75
Exporting settings	77
Importing settings	78
Using security settings templates	79
About security settings templates.....	80
Creating a security settings template	80
Viewing security settings in a template.....	81
Applying a security settings template	82
Deleting a security settings template	83
Real-Time Protection	84
Real-Time File Protection	84
About Real-Time File Protection task	85
Real-Time File Protection task statistics.....	85
Configuring Real-Time File Protection task settings.....	88
Selecting protection mode.....	90
Using Heuristic Analyzer	92
Task integration with other Kaspersky Embedded Systems Security components.....	93
List of file extensions scanned by default in Real-Time File Protection task	94
Protection scope in Real-Time File Protection task	99
About protection scope in Real-Time File Protection task.....	99
Predefined protection scopes.....	100
Configuring view mode for network file resources.....	101

Creating protection scope	102
About virtual protection scope	105
Creating virtual protection scope	105
Security settings of selected node in Real-Time File Protection task	107
Selecting predefined security levels	108
Configuring security settings manually	110
KSN Usage	118
About KSN Usage task	118
Starting and stopping KSN Usage task	120
Configuring KSN Usage task	122
KSN Usage task statistics	125
Exploit prevention	127
About Exploit prevention	127
Configuring process memory protection settings	130
Adding a process for protection	132
Impact reduction techniques	134
Computer control	136
Application Launch Control	136
About Applications Launch Control task	137
Configuring Applications Launch Control task settings	139
Selecting operating mode of Applications Launch Control task	141
Generating scope of Applications Launch Control task	143
KSN usage for Applications Launch Control task	145
Software Distribution Control	148
About Applications Launch Control rules	152
Removing Applications Launch Control rules	155
Exporting Applications Launch Control rules	155
Applications launches check	156
About Applications Launch Control rules list filling	157
Adding one Applications Launch Control rule	158
Filling rules list basing on Applications Launch Control task events	162
Importing Applications Launch Control rules from XML file	163
About Rule Generator for Applications Launch Control task	164
Configuring Rule Generator for Application Launch Control task settings	165

Device Control	174
About Device Control task	174
Configuring Device Control task settings	176
About Device Control rules	179
Removing Device Control rules	181
Exporting Device Control rules	182
Activating and deactivating of Device Control rules	182
Expanding Device Control rules usage scope	183
About Device Control rules list filling	184
Adding an allowing rule for one or several external devices	187
Filling rules list basing on Device Control task events	188
Importing Device Control rules from XML file	189
About Rule Generator for Device Control task	190
Configuring Rule Generator for Device Control task	190
Firewall Management	194
About the Firewall Management task	194
About Firewall rules	196
Enabling and disabling Firewall rules	198
Adding Firewall rules manually	199
Deleting Firewall rules	201
System Inspection	202
File Integrity Monitor	202
About the File Integrity Monitor task	203
About file operation monitoring rules	204
Configuring File Integrity Monitor task settings	208
Configuring monitoring rules	210
Log Inspection	214
About the Log Inspection task	214
Configuring the Log inspection rules	216
Heuristic Analyzer configuration	218
On-Demand Scan	220
About On-Demand Scan tasks	221
On-Demand Scan task statistics	222
Configuring On-Demand Scan task settings	224

Using Heuristic Analyzer	228
Running background On-Demand Scan task	229
KSN Usage.....	231
Registering execution of Critical Areas Scan.....	232
Scan scope in On-Demand Scan tasks	233
About scan scope	233
Configuring view mode for network file resources	234
Predefined scan scopes	235
Creating a scan scope.....	237
Including network objects in the scan scope	240
Creating a virtual scan scope	241
Security settings of selected node in On-Demand Scan tasks	243
Selecting predefined security levels for On-Demand Scan tasks	244
Configuring security settings manually	247
Removable Drives Scan	254
Creating an On-Demand Scan task.....	258
Removing tasks	261
Renaming tasks.....	261
Updating Kaspersky Embedded Systems Security bases and software modules	262
About Update tasks	263
About Kaspersky Embedded Systems Security software modules update.....	264
About Kaspersky Embedded Systems Security Database Updates	265
Schemes for updating databases and modules of anti-virus applications used within organization	266
Configuring Update tasks	271
Configuring settings for working with Kaspersky Embedded Systems Security update sources	271
Optimizing use of disk I/O when running Database Update task.....	275
Configuring Copying Updates task settings.....	276
Configuring Software Modules Update task settings	278
Rolling back Kaspersky Embedded Systems Security database updates	280
Rolling back application module updates.....	280
Update task statistics.....	280

Objects isolating and backup copying.....	282
Isolating probably infected objects. Quarantine	283
About quarantining of probably infected objects.....	284
Viewing Quarantine objects.....	284
Sorting quarantined objects	284
Filtering quarantined objects	285
Quarantine Scan	286
Restoring quarantined objects.....	289
Moving objects to Quarantine.....	292
Deleting objects from Quarantine	292
Sending probably infected objects to Kaspersky Lab for analysis	293
Configuring Quarantine settings	294
Quarantine statistics.....	296
Making backup copies of objects. Backup.....	298
About backing up objects before disinfection / deletion.....	298
Viewing objects stored in Backup.....	299
Sorting files in Backup.....	299
Filtering files in Backup	300
Restoring files from Backup.....	301
Deleting files from Backup.....	304
Configuring Backup settings.....	305
Backup statistics.....	307
Event registration. Kaspersky Embedded Systems Security logs.....	308
Ways to register Kaspersky Embedded Systems Security events.....	308
System audit log.....	309
Sorting events in the system audit log.....	310
Filtering events in the system audit log	310
Deleting events from the system audit log.....	311
Task logs	312
About task logs.....	313
Viewing the list of events in task logs	313
Sorting events in task logs.....	313
Filtering events in task logs	314

Viewing statistics and information about a Kaspersky Embedded Systems Security task in task logs	315
Exporting information from a task log	316
Deleting events from task logs	317
Security event log	318
Viewing the event log of Kaspersky Embedded Systems Security in Event Viewer.....	319
Configuring log settings in Kaspersky Embedded Systems Security Console.....	320
About SIEM integration	323
Configuring SIEM integration settings	325
Licensing.....	328
Notification settings.....	329
Administrator and user notification methods.....	329
Configuring administrator and user notifications.....	331
Glossary.....	335
AO Kaspersky Lab	340
Information about third-party code	342
Trademark notices	343
Index.....	344

About this Guide

The Kaspersky Embedded Systems Security User's Guide is intended for specialists who administer Kaspersky Embedded Systems Security Console on a protected device.

This guide contains information about configuring and using Kaspersky Embedded Systems Security Management Console.

In this section

In this document.....	10
Document conventions.....	13

In this document

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

Kaspersky Embedded Systems Security

This section contains information about the purpose, key features, and content of the application.

Kaspersky Embedded Systems Security interface

This section describes the primary elements of the application interface.

Starting and stopping Kaspersky Embedded Systems Security

This section contains information about starting Kaspersky Embedded Systems Security Console, and also about starting and stopping Kaspersky Security Service.

Viewing protection status and Kaspersky Embedded Systems Security information

This section contains information about the computer protection status and information about Kaspersky Embedded Systems Security.

About access permissions for Kaspersky Embedded Systems Security functions

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

Working with Kaspersky Embedded Systems Security

This section provides information about Kaspersky Embedded Systems Security Console and describes how to manage the application using Kaspersky Embedded Systems Security Console installed on the protected computer or another computer.

Configuring the Trusted Zone

This section provides information about the Trusted Zone of Kaspersky Embedded Systems Security, as well as instructions on how to add objects to the Trusted Zone when executing Kaspersky Embedded Systems Security tasks.

Managing Kaspersky Embedded Systems Security tasks

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

Real-Time Protection

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

Computer control

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

System Inspection

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

On-Demand Scan

This section provides information about On-Demand Scan tasks, and instructions on configuring On-Demand Scan task settings and security settings on the protected computer.

Updating Kaspersky Embedded Systems Security bases and software modules

This section provides information about databases and software modules update tasks of Kaspersky Embedded Systems Security, copying updates and rolling back databases updates of Kaspersky Embedded Systems Security, as well as instructions on how to configure databases and software modules update tasks.

Objects isolating and backup copying

This section provides information about backing up of the detected malicious objects before they are disinfected or removed, and information about quarantining of the probably infected objects.

Event registration. Kaspersky Embedded Systems Security logs

This section provides information about working with Kaspersky Embedded Systems Security logs: the system audit log, task execution logs, and the event log.

Notification settings

This section provides information about ways in which users and administrators of Kaspersky Embedded Systems Security can be notified about application events and the computer protection status, as well as instructions on how to configure notifications.

Contacting Technical Support

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

Glossary

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

AO Kaspersky Lab

This section provides information about Kaspersky Lab AO.

Information about third-party code

This section 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.

Sample text	Description of document convention
<p>Example:</p> <p>...</p>	<p>Examples are given in blocks against a blue background under the heading "Example".</p>
<p><i>Update</i> means...</p> <p>The <i>Databases are out of date</i> event occurs.</p>	<p>The following elements are italicized in the text:</p> <ul style="list-style-type: none"> • New terms • Names of application statuses and events
<p>Press ENTER.</p> <p>Press ALT+F4.</p>	<p>Names of keyboard keys appear in bold and are capitalized.</p> <p>Names of keys that are connected by a + (plus) sign indicate the use of a key combination. These keys must be pressed simultaneously.</p>
<p>Click the Enable button.</p>	<p>Names of application interface elements, such as text boxes, menu items, and buttons, are set off in bold.</p>
<p>► <i>To configure a task schedule:</i></p>	<p>Introductory phrases of instructions are italicized and accompanied by the arrow sign.</p>
<p>In the command line, type</p> <p><code>help</code></p> <p>The following message then appears:</p> <p>Specify the date</p> <p>in <code>dd:mm:yy</code> format.</p>	<p>The following types of text content are set off with a special font:</p> <ul style="list-style-type: none"> • Text in the command line • Text of messages displayed on the screen by the application • Data that must be entered from the keyboard
<p><User name></p>	<p>Variables are enclosed in angle brackets. Instead of a variable, the corresponding value should be inserted, omitting the angle brackets.</p>

About Kaspersky Embedded Systems Security

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

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

- ATM (automated teller machines);
- POS (points of sale).

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

- Via Kaspersky Embedded Systems Security Console installed on the same computer, where Kaspersky Embedded Systems Security is installed, or on a different computer
- Using commands in the command line
- Via the Kaspersky Security Center plug-in (for centralized management of protection of a group of computers, where each computer has Kaspersky Embedded Systems Security installed)

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

Kaspersky Embedded Systems Security components and features

The application includes the following components:

- **Real-Time Protection.** Kaspersky Embedded Systems Security scans objects when they are accessed. Kaspersky Embedded Systems Security scans the following objects:
 - Files
 - Alternate file system threads (NTFS threads)
 - Master boot record and boot sectors on local hard and removable drives
- **On-Demand Scan.** Kaspersky Embedded Systems Security runs a single scan of the specified area for viruses and other computer security threats. Application scans files, RAM, and startup objects on a protected computer.
- **Application Launch Control.** The component tracks users' attempts to launch applications and controls applications launches.
- **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 all other ways to configure firewall settings.
- **File Integrity Monitor.** Kaspersky Embedded Systems Security detects changes in files within the monitoring scopes specified in the task settings. These changes may indicate a security breach on the protected computer.
- **Log Inspection.** This component monitors the integrity of the protected environment based on the results of an inspection of Windows event logs.

The following functions are implemented in the application:

- **Databases and software modules update.** Kaspersky Embedded Systems Security downloads updates of application databases and modules from FTP or HTTP update servers of Kaspersky Lab, Kaspersky Security Center Administration Server, or other update sources.

- **Quarantine.** Kaspersky Embedded Systems Security quarantines probably infected objects by moving such objects from their original location to *Quarantine*. For security purposes, objects are stored in Quarantine in encrypted form.
- **Backup.** Kaspersky Embedded Systems Security stores encrypted copies of objects classified as *Infected* or *Probably infected* in *Backup* before disinfecting or deleting them.
- **Administrator and user notifications.** You can configure the application to notify the administrator and users who access the protected computer about events in Kaspersky Embedded Systems Security operation and the status of Anti-Virus protection on the computer.
- **Importing and exporting settings.** You can export Kaspersky Embedded Systems Security settings to an XML configuration file and import settings into Kaspersky Embedded Systems Security from the configuration file. You can save all application settings or only settings for individual components to a configuration file.
- **Applying templates.** You can manually configure a node's security settings in the tree or in a list of the computer's file resources, and save the configured setting values as a template. This template can then be used to configure the security settings of other nodes in Kaspersky Embedded Systems Security protection and scan tasks.
- **Managing access permissions for Kaspersky Embedded Systems Security functions.** You can configure the rights to manage Kaspersky Embedded Systems Security and the Windows services registered by the application, for users and groups of users.
- **Writing events to the application event log.** Kaspersky Embedded Systems Security logs information about software component settings, the current status of tasks, events that occur while tasks run, events associated with Kaspersky Embedded Systems Security management, and information required to diagnose errors in Kaspersky Embedded Systems Security.
- **Trusted Zone.** You can generate the list of exclusions from the protection or scan scope, that Kaspersky Embedded Systems Security will apply in the on-demand and real-time protection tasks.
- **Process Memory Protection.** You can protect process memory from exploits using an Agent injected into the process.

Kaspersky Embedded Systems Security interface

This section describes the primary elements of the application interface.

In this section

Kaspersky Embedded Systems Security Console interface	18
Kaspersky Embedded Systems Security icon in the task tray notification area.....	24

Kaspersky Embedded Systems Security Console interface

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

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

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

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

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

Console tree

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

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

- **Real-Time Protection**: manages Real-Time File Protection and KSN services. The **Real-Time Protection** node allows to configure the following tasks:
 - **Real-Time File Protection**
 - **KSN Usage**
- **Computer Control**: controls launches of applications installed on a protected computer, as well as external devices connections. The **Computer control** node allows to configure the following tasks:
 - **Application Launch Control**
 - **Device Control**
 - **Firewall Management**
- **Automatic rule generation**: configuring automatic generation of group and system rules for the Applications Launch Control task and the Device Control task.
 - **Rule Generator for Applications Launch Control**
 - **Rule Generator for Device Control**
 - Rule generation group tasks **<Task names>** (if any)

Group tasks (see section "Kaspersky Embedded Systems Security task categories" on page [67](#)) are created using Kaspersky Security Center. You cannot manage group tasks through Kaspersky Embedded Systems Security Console.

- **System Inspection:** management of settings for control of file operations and Windows Event Log inspection settings.
 - **File Integrity Monitor**
 - **Log Inspection**
- **On-Demand Scan:** manages On-Demand Scan tasks. There is a separate node for each task:
 - **Scan at Operating System Startup**
 - **Critical Areas Scan**
 - **Quarantine Scan**
 - **Application Integrity Control**
 - Custom tasks <Task names> (if any)

The node displays system tasks (see section "Kaspersky Embedded Systems Security task categories" on page [67](#)) created when the application is installed, custom tasks, and group on-demand scan tasks created and sent to a computer using Kaspersky Security Center.

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

The node displays all custom and group update tasks (see section "Kaspersky Embedded Systems Security task categories" on page [67](#)) created and sent to a computer using Kaspersky Security Center.

- **Storage:** Management of Quarantine and Backup settings.
 - **Quarantine**
 - **Backup**
- **Logs:** manages logs of Real-Time Protection, On-Demand Scan, Computer Control, and Update tasks; manages the security event log and Kaspersky Embedded Systems Security system audit log.
 - **Security event log.**
 - **System audit log.**
 - **Task logs.**
- **Licensing:** add or delete Kaspersky Embedded Systems Security keys and activation codes, view license details.

Details pane

The results pane displays information about the selected node. If the **Kaspersky Embedded Systems Security** node is selected, the results pane displays information about the current computer protection status (see section "View protection status and Kaspersky Embedded Systems Security information" on page [28](#)) and information about Kaspersky Embedded Systems Security, the protection status of its functional components, and the status of the license or key.

Context menu of the Kaspersky Embedded Systems Security node

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

- **Connect to another computer.** Connect to another computer to manage Kaspersky Embedded Systems Security installed on it. You can also perform this operation by clicking the link in the lower right corner of the details pane of the **Kaspersky Embedded Systems Security** node.

- **Start Kaspersky Embedded Systems Security / Stop Kaspersky Embedded Systems Security (Start / Stop).** Start or stop application or a selected task (see section "Start / pause / resume / stop task manually" on page [69](#)). To carry out these operations, you can also use the buttons on the toolbar. You can also perform these operations in context menus of application tasks.
- **Configure removable drives scan settings.** View and configure Removable drives scan on connection (see section "Removable drives scan" on page [291](#)).
- **Exploit Prevention: general settings.** Select exploit prevention mode and actions to reduce exploit impact (see section "Configuring process memory protection settings" on page [148](#)).
- **Exploit Prevention: processes protection settings.** Add processes to the protected processes list and configure protection settings (see section "Adding a process for protection" on page [150](#)).
- **Configure Trusted Zone settings.** View and configure Trusted Zone settings (see section "About Kaspersky Embedded Systems Security Trusted Zone" on page [57](#)).
- **Modify user rights of the application management.** View and configure permissions to access Kaspersky Embedded Systems Security functions (see section "About permissions to manage Kaspersky Embedded Systems Security" on page [38](#)).
- **Modify user rights of Kaspersky Security Service management.** View and configure user rights to manage Kaspersky Security Service.
- **Configure notifications.** View and configure settings of notifications sent to the administrator and users of Kaspersky Embedded Systems Security (see section "Configuring administrator and user notifications" on page [330](#)).
- **Export settings.** Save the application settings in a configuration file in XML format (see section "Exporting settings" on page [77](#)). You can also perform this operations in context menus of application tasks.
- **Import settings.** Import application settings from a configuration file in XML format (see section "Importing settings" on page [78](#)). You can also perform this operations in context menus of application tasks.

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

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

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

Quick access bar and context menu of Kaspersky Embedded Systems Security tasks


You can manage Kaspersky Embedded Systems Security tasks using the items of context menus of each task in the Console tree.

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



- **Resume / Pause** Resume or pause task execution (see section "Start / pause/ resume/ stop task manually" on page [69](#)). To carry out these operations, you can also use the buttons on the toolbar. This operation is available for the Real-Time Protection tasks and the On-Demand Scan tasks.
- **Add task.** Create new custom task (see section "Creating an On-Demand Scan task" on page [257](#)). This operation is available for On-demand scan tasks.
- **Open log.** View and manage a task log. (see section "About task logs" on page [313](#)). This operation is available for all tasks.


- **Save task.** Save and apply modified task settings (see section "Saving task after changing its settings" on page [68](#)). This operation is available for Real-Time File Protection and On-Demand Scan tasks.
- **Remove task.** Delete custom task (see section "Deleting a task" on page [261](#)). This operation is available for On-demand scan tasks.
- **Statistics.** View task statistics. This operation is available for the Application Integrity Control task.
- **Settings templates.** Manage templates. This operation is available for Real-Time File Protection and On-Demand Scan.

Kaspersky Embedded Systems Security icon in task tray notification area

Every time Kaspersky Embedded Systems Security automatically starts after a computer reboot, the Kaspersky Embedded Systems Security Taskbar Icon is displayed in the taskbar notification area . It is displayed by default if the **Kaspersky Embedded Systems Security Taskbar Icon** component was installed during application setup.

The appearance of the Kaspersky Embedded Systems Security Taskbar Icon reflects the current status of computer protection. The Taskbar Icon may have one of the two statuses:

-  active (colored icon) if at least one of the tasks is currently running: Real-Time File Protection, Applications Launch Control, Device Control
-  inactive (black-and-white icon) if none of the tasks are currently running: Real-Time File Protection, Applications Launch Control, Device Control

You can open the context menu of the Kaspersky Embedded Systems Security Taskbar Icon  by right-clicking it.

The context menu offers several commands which can be used to display application windows (see the table below).

Table 2. Context menu commands displayed in the Kaspersky Embedded Systems Security Tray Icon

Command	Description
Open Kaspersky Embedded Systems Security Console	Opens Kaspersky Embedded Systems Security Console (if installed).
About the application	<p>Opens the About the application window containing information about Kaspersky Embedded Systems Security.</p> <p>For registered Kaspersky Embedded Systems Security users, the About the application window contains information about urgent updates that have been installed.</p>
Hide	Hides the Kaspersky Embedded Systems Security Icon in the task tray notification area.

You can display the hidden Kaspersky Embedded Systems Security Taskbar Icon again at any time.

► *To display the application icon again,*

in the **Start** menu Microsoft Windows select **Programs** → **Kaspersky Embedded Systems Security** → **Kaspersky Embedded Systems Security Taskbar Icon**.

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

In the general settings of Kaspersky Embedded Systems Security, you can enable or disable the display of the Kaspersky Embedded Systems Security Taskbar Icon every time the application starts automatically following a computer reboot.

Starting and stopping Kaspersky Embedded Systems Security

This section contains information about starting Kaspersky Embedded Systems Security Console, and also about starting and stopping Kaspersky Security Service.

In this section

Starting Kaspersky Embedded Systems Security Console from the Start menu.....	26
Starting and stopping Kaspersky Security Service	27

Starting Kaspersky Embedded Systems Security Console from Start menu

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

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

in the **Start** menu select **Programs** → **Kaspersky Embedded Systems Security** → **Administration Tools** → **Kaspersky Embedded Systems Security Console**.

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

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

1. In the **Start** menu select **Programs** → **Kaspersky Embedded Systems Security** → **Administration Tools**.
2. In the context menu of **Kaspersky Embedded Systems Security Console**, select the **Author** command.

Kaspersky Embedded Systems Security Console is started in author mode.

If the Console has been started on the protected computer, the Console window opens (see section "Kaspersky Embedded Systems Security Console window interface" on page [18](#)).

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

► *To connect to a protected computer:*

1. In the Console tree, open the context menu of the **Kaspersky Embedded Systems Security** node.

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

The **Select computer** window opens.

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

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

5. Click **OK**.

Kaspersky Embedded Systems Security Console will be connected to a protected computer.

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

Starting and stopping Kaspersky Security service

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

By default when Kaspersky Security Service is started, the Real-Time File Protection, Scan at Operating System Startup, and Application Integrity Control tasks are started, as well as other tasks that are scheduled to start **At application launch**.

If the Kaspersky Security Service is stopped, all running tasks are stopped. After you restart Kaspersky Security Service, the application automatically starts only those tasks whose schedule has the launch frequency set to **At application launch**, while the other tasks have to be started manually.

You can start and stop Kaspersky Security Service using the context menu of the **Kaspersky Embedded Systems Security** node or using the Microsoft Windows **Services** snap-in.

You can start and stop Kaspersky Embedded Systems Security if you are a member of the Administrators group on the protected server.

► *To stop or start application using the Management Console take the following steps:*

1. In the Console tree, open the context menu of the **Kaspersky Embedded Systems Security** node.
2. Select one of the following items:
 - **Stop Kaspersky Embedded Systems Security** to stop Kaspersky Security Service.
 - **Start Kaspersky Embedded Systems Security** to start Kaspersky Security Service.

The Kaspersky Security Service will be started or stopped.

Viewing protection status and Kaspersky Embedded Systems Security information

- ▶ *To view information about the computer protection status Kaspersky Embedded Systems Security,*

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

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

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

You can refresh information manually.

- ▶ *To refresh information in the Kaspersky Embedded Systems Security node manually,* select the **Refresh** command in the context menu of the **Kaspersky Embedded Systems Security** node.

The following application information is displayed in the details pane of Console:

- Computer protection status
- Information about database and application module updates
- License information
- Data about computer control tasks
- Status of integration with Kaspersky Security Center: details of the computer with Kaspersky Security Center installed, to which the application is connected; information about application tasks controlled by the active policy

Color coding is used to display the protection status:

- *Green*. The task is being run in accordance with the configured settings. Protection is active.
- *Yellow*. The task was not started, has been paused, or has been stopped. Security threats may occur. You are advised to configure and start the task.
- *Red*. The task completed with an error or a security threat was detected while the task was running. You are advised to start the task or take measures to eliminate the detected security threat.

Some details in this block (for example, task names or the number of threats detected) are links that, when clicked, take you to the node of the relevant task or open the task log.

The **Protection** block (see the table below) displays information about the computer's current protection status.

Table 3. Information about computer protection status

Protection section	Information
Computer protection status indicator	<p>The color of the panel with the name of the section reflects the status of tasks being performed in the section. The indicator can take the following values:</p> <ul style="list-style-type: none"> • Green color of the panel – displayed by default and signifies that Real-Time Protection tasks are running and the Critical Areas Scan task was performed no more than 30 days ago (by default). • Yellow color of the panel – one or several Real-Time Protection tasks are not running or have been stopped, and the critical areas can task has not been performed for a long time. • Red color of the panel – Real-Time File Protection task could not be started.
Real-Time File Protection	<p>Task status – current task status, for example, <i>Running</i> or <i>Stopped</i>.</p> <p>Detected – the number of objects detected by Kaspersky Embedded Systems Security. For example, if Kaspersky Embedded Systems Security detects one malware in five files, the value in this field increases by one. If the number of detected malwares exceeds 0, the value is highlighted in red.</p>
KSN Usage	<p>Task status – current task status, for example, <i>Running</i> or <i>Stopped</i>.</p> <p>Untrusted conclusions – the number of objects found to be untrusted by KSN services. For example, if the KSN service scanned five files and found one of them to be malicious, the value in this field increases by one. If the number of untrusted conclusions exceeds 0, the row value is highlighted in red.</p>

Protection section	Information
Critical Areas Scan	<p>Last scan date – the date and time of the last Critical Areas Scan for viruses and other computer security threats.</p> <p><i>Not performed</i> – an event that occurs when the Critical Areas Scan task has not been performed in the last 30 days or longer (default value). You can change the threshold for generating this event.</p>
Backed up objects	<p><i>Backup free space threshold exceeded</i> – this event occurs when the threshold of Backup free space is nearing the specified limit. Kaspersky Embedded Systems Security continues to move objects to Backup. In this case, the value in the Space used field is highlighted in yellow.</p> <p><i>Maximum Backup size exceeded</i> – this event occurs when the Backup size has reached the specified limit. Kaspersky Embedded Systems Security continues to move objects to Backup. In this case, the value in the Space used field is highlighted in red.</p> <p>Backed up objects - the number of objects currently in Backup.</p> <p>Space used - amount of Backup space used.</p>
Exploit Prevention	<p>Task status – current task status, for example, <i>Running</i> or <i>Stopped</i>.</p> <p>Mode – one of two available modes, selected during configuration of process memory protection:</p> <ul style="list-style-type: none"> • Prevention of exploits in processes. • Only report suspicious intrusions into processes. <p>Processes in the protection list – The total number of processes being protected and handled in accordance with the selected mode.</p>

The **Update** section (see the table below) displays information about how up-to-date the anti-virus databases and application modules are.

Table 4. Information about the status of Kaspersky Embedded Systems Security databases and modules

Updates section	Information
<p>Status indicator of databases and software modules</p>	<p>The color of the panel with the name of the section reflects the status of application databases and modules. The indicator can take the following values:</p> <ul style="list-style-type: none"> • Green color of the panel – displayed by default and signifies that application database is up to date and that no critical updates of software modules are available to be downloaded. • Yellow color of the panel – one of the following events occurred: <i>Databases are out of date; Critical update for software modules available; Critical update for software modules recalled; Restart the computer to finish updating software modules.</i> • Red color of the panel – the event <i>Application databases are extremely out of date</i> or <i>Application databases are corrupted</i> has occurred.

Updates section	Information
<p>Database and software modules update</p>	<p>Database status – an evaluation of the Database Update status.</p> <p>It can take the following values:</p> <ul style="list-style-type: none"> • Application database is up to date – application databases were updated no more than 7 days ago (default). • Application database is out of date – application databases were updated between 7 and 14 days ago (default). • Application database is extremely out of date – application databases were updated no more than 14 days ago (default). <p>You can change the thresholds for generating the events <i>Application databases are out of date</i> and <i>Application databases are outdated</i>.</p> <p>Database release date – the date and time of release of the latest databases update. The date and time are specified in UTC format.</p> <p>Application database records – the number of threat signatures in the application databases.</p> <p>Status of the latest completed Database Update task – the date and time of the latest database update. The date and time are specified according to the local time of the protected computer. The value in the field is colored red if the <i>Failed</i> event occurred.</p> <p>Number of module updates available – the number of Kaspersky Embedded Systems Security module updates available to be downloaded and installed.</p> <p>Number of module updates installed – the number of installed Kaspersky Embedded Systems Security module updates.</p>

The **Control** section (see table below) displays information about the Applications Launch Control, Device Control, and Firewall Management tasks.

Table 5. Information about Computer Control status

Control section	Information
Computer Control status indicator	<p>The color of the panel with the name of the section reflects the status of tasks being performed in the section. The indicator can take the following values:</p> <ul style="list-style-type: none"> • Green color of the panel – displayed by default and signifies that all Computer Control tasks are running. • Yellow color of the panel – one or several Computer Control tasks are not running; the <i>Not running</i> event occurs. • Red color of the panel – the Applications Launch Control task or the Device Control task could not be started; the <i>Failed</i> event occurs.
Application Launch Control	<p>Task status – current task status, for example, <i>Running</i> or <i>Stopped</i>.</p> <p>Mode – One of the two available modes for the Applications Launch Control task:</p> <ul style="list-style-type: none"> • Apply Rules. • Statistics Only. <p>Applications launches denied – the number of attempts to start applications blocked by Kaspersky Embedded Systems Security during the Applications Launch Control task. If the number of blocked application launches exceeds 0, the field value is colored in red.</p> <p>Average processing time (ms) – the time it took Kaspersky Embedded Systems Security to process an attempt to start applications on the protected computer.</p>

Control section	Information
Device Control	<p>Task status – current task status, for example, <i>Running</i> or <i>Stopped</i>.</p> <p>Mode – One of the two available modes for the Applications Launch Control task:</p> <ul style="list-style-type: none"> • Apply Default Deny. • Statistics Only. <p>Devices blocked – the number of attempts to connect a mass storage device, that were blocked by Kaspersky Embedded Systems Security during the Device Control task. If the number of blocked mass storages exceeds 0, the field value is colored in red.</p>
Firewall Management	<p>Task status – current task status, for example, <i>Running</i> or <i>Stopped</i>.</p> <p>Connections blocked – The number of connections to a protected device, which were blocked by the specified firewall rules.</p>

The **Inspection** section (see the table below) displays information about the File Integrity Monitor and Log Inspection tasks.

Table 6. Information about System Inspection status

Inspection section	Information
Network security status indicator	<p>The color of the panel with the name of the section reflects the status of tasks being performed in the section. The indicator can take the following values:</p> <ul style="list-style-type: none"> • Green – Displayed by default and signifies that all Computer Control tasks are running. • Yellow – One or more Computer Control tasks are not running; the <i>Not running</i> event occurs. • Red – The Applications Launch Control task or the Device Control task could not be started; the <i>Failed</i> event occurs.
File Integrity Monitor	<p>Task status – current task status, for example, <i>Running</i> or <i>Stopped</i>.</p> <p>Potential violations – The number of changes to files within the monitoring scope. These changes may indicate that the security of a protected device has been breached.</p>
Log Inspection	<p>Task status – current task status, for example, <i>Running</i> or <i>Stopped</i>.</p> <p>Potential violations – The number of recorded violations based on data from the Windows Event Log, identified based on the specified task rules or use of the Heuristic Analyzer.</p>

Information about the Kaspersky Embedded Systems Security license status is displayed in the row in the bottom left corner of the details pane of the **Kaspersky Embedded Systems Security** node.

You can configure Kaspersky Embedded Systems Security properties by following the **Application Properties** link (see section "**Kaspersky Embedded Systems Security settings in the Console**" on page [46](#)).

You can connect to a different computer by following the **Connect to another computer** link (see section "**Managing Kaspersky Embedded Systems Security via Kaspersky Security Console on another computer**" on page [55](#)).

About access permissions for Kaspersky Embedded Systems Security functions

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

In this section

About permissions to manage Kaspersky Embedded Systems Security	38
About rights to manage registered services.....	41
Configuring access permissions for managing Kaspersky Embedded Systems Security and Kaspersky Embedded Systems Security Service	42

About permissions to manage Kaspersky Embedded Systems Security

By default, access to all Kaspersky Embedded Systems Security functions is granted to users of the Administrators group on the protected computer, users of the ESS Administrators group created on the protected computer during installation of Kaspersky Embedded Systems Security, as well as the SYSTEM system group.

Users who have access to the **Edit permissions** function of Kaspersky Embedded Systems Security can grant access to Kaspersky Embedded Systems Security functions to other users registered on the protected computer or included in the domain.

Users who are not registered in the list of Kaspersky Embedded Systems Security users cannot open Kaspersky Embedded Systems Security Console.

You can choose one of the following preset levels of Kaspersky Embedded Systems Security 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 settings, component settings, permissions of Kaspersky Embedded Systems Security users, and also view Kaspersky Embedded Systems Security statistics.
- **Edit** – access to all application functions, except editing user permissions: ability to view and edit Kaspersky Embedded Systems Security general settings and Kaspersky Embedded Systems Security component settings.
- **Read** – ability to view Kaspersky Embedded Systems Security general settings, Kaspersky Embedded Systems Security component settings, Kaspersky Embedded Systems Security statistics, and Kaspersky Embedded Systems Security user permissions.

You can also configure advanced access permissions (see section "Configuring access permissions for managing Kaspersky Embedded Systems Security and Kaspersky Embedded Systems Security Service" on page [42](#)): allow or block access to specific Kaspersky Embedded Systems Security functions.

If you have manually configured access permissions for a user or group, the **Special permissions** access level is set for this user or group.

Table 7. About access permissions for Kaspersky Embedded Systems Security functions

User rights	Description
Task management	Ability to start / stop / pause / resume Kaspersky Embedded Systems Security tasks.
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 settings from a configuration file.
Read settings	Ability to: <ul style="list-style-type: none"> • View general Kaspersky Embedded Systems Security settings and task settings. • Export Kaspersky Embedded Systems Security settings to the configuration file. • view settings for task logs, system audit log, and notifications.
Manage storages	Ability to: <ul style="list-style-type: none"> • 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 task.
Application licensing	Kaspersky Embedded Systems Security can be activated or deactivated.
Uninstalling the application	Ability to uninstall Kaspersky Embedded Systems Security

User rights	Description
Read permissions	Ability to view the list of Kaspersky Embedded Systems Security users and access privileges of each user.
Edit permissions	Ability to: <ul style="list-style-type: none"> Edit the list of users with access to application management. Edit user access permissions for Kaspersky Embedded Systems Security functions.

About permissions to manage registered services

Detailed information about registered Windows services and how to configure access to registered services is contained in *Kaspersky Embedded Systems Security Administrator's Guide*.

During installation, Kaspersky Embedded Systems Security registers the Kaspersky Security Service (KAVFS) and the Kaspersky Security Management Service (KAVFSGT) in Windows.

Kaspersky Security Service

By default, access permissions for managing the Kaspersky Security Service are granted to users in the "Administrators" group on the protected computer as well as to the SERVICE and INTERACTIVE groups with read permissions and to the SYSTEM group with read and execute permissions.

Users who have access to functions of the Edit permissions level (see section "About permissions to manage Kaspersky Embedded Systems Security" on page [38](#)) can grant access permissions for managing Kaspersky Embedded Systems Security Service to other users registered on the protected computer or included in the domain.

Kaspersky Security Management Service

To manage the application via Kaspersky Embedded Systems Security Console installed on a different computer, the account whose permissions are used to connect to Kaspersky Embedded Systems Security must have full access to Kaspersky Embedded Systems Security Management Service on the protected computer.

By default, access to the Kaspersky Security Management Service is granted to users of the Administrators group on the protected computer and users of the ESS Administrators group created on the protected computer during Kaspersky Embedded Systems Security installation.

You can only manage the Kaspersky Security Management Service via the Microsoft Windows Services snap-in.

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

You can edit the list of users and user groups allowed to access Kaspersky Embedded Systems Security functions and manage Kaspersky Embedded Systems 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. In the Kaspersky Embedded Systems Security Console tree, open the context menu of the **Kaspersky Embedded Systems Security** node and do one of the following:
 - 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 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.

2. 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.
3. 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 or Kaspersky Embedded Systems Security Service:*

1. In the Kaspersky Embedded Systems Security Console tree, open the context menu of the **Kaspersky Embedded Systems Security** node and do one of the following:
 - Select **Modify user rights of application management** if you want to configure access permissions for Kaspersky Embedded Systems Security functions.
 - Select **Modify user rights of Kaspersky Security Service management** if you want to configure access permissions for the Kaspersky Security Service.

The **Permissions for Kaspersky Embedded Systems Security group** window opens.

2. 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.
3. 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 or Kaspersky Security Service.
 - **Read:**
 - the following permissions to manage Kaspersky Embedded Systems Security: **Retrieve statistics, Read settings, Read logs** and **Read permissions**;

- the following permissions to manage Kaspersky Security Service: **Read service settings, Request service status from Service Manager, Request status from service, List dependent services, Read permissions.**
 - **Modification:**
 - all permissions to manage Kaspersky Embedded Systems Security, except **Edit permissions;**
 - the following permissions to manage Kaspersky Security Service: **Edit 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.**
4. 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** window that opens, select the user or group that you need.
 - b. Click the **Edit** button.
 - c. In the window that opens, click the **Show special permissions** link.
 - d. In the drop down list in the top part of the window, select the type of access control (**Allow** or **Block**).
 - e. Select the check boxes opposite the functions that you want to allow or block for the selected user or group.
 - f. Click **OK**.
 - g. In the **Additional security settings for Kaspersky Embedded Systems Security** window, click **OK**.
5. In the **Permissions for Kaspersky Embedded Systems Security group** window, click the **Apply** button.

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

Working with Kaspersky Embedded Systems Security

This section provides information about Kaspersky Embedded Systems Security Console (hereinafter "Console") and describes how to manage the application using Kaspersky Embedded Systems Security Console installed on the protected computer or another computer.

In this section

About Kaspersky Embedded Systems Security Console.....	45
Kaspersky Embedded Systems Security settings in the Console	46
Managing Kaspersky Embedded Systems Security via Kaspersky Security Console on another computer	55

About Kaspersky Embedded Systems Security Console

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

You can managed the application via the Kaspersky Security Console installed on the protected computer or on another computer in the corporate network. After Kaspersky Embedded Systems Security Console has been installed on another computer, advanced configuration must be run (see section "Managing Kaspersky Embedded Systems Security via Kaspersky Embedded Systems Security Console on another computer" on page [55](#)).

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

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

You can start Kaspersky Embedded Systems Security Console from the **Start** menu. You can also start Kaspersky Embedded Systems Security Console on the protected computer by clicking the Kaspersky Embedded Systems Security Taskbar Icon in the taskbar notification area.

The Kaspersky Embedded Systems Security snap-in msc-file can be run or added to the existing Microsoft Management Console as a new element in the tree (see section "Kaspersky Embedded Systems Security Console window interface" on page [18](#)).

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

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

Kaspersky Embedded Systems Security settings in Console

General settings and malfunction diagnostics settings of Kaspersky Embedded Systems Security settings establish the general conditions on which the application operates. These settings allow you to control the number of working processes used by Kaspersky Embedded Systems Security, enable Kaspersky Embedded Systems Security task recovery after an abnormal termination,

maintain the tracking log, enable creating dump file of Kaspersky Embedded Systems Security processes in case of an abnormal termination, and configure other general settings.

Application settings cannot be configured in Kaspersky Embedded Systems Security Console if the Kaspersky Security Center active policy blocks changes to these settings.

► *To configure Kaspersky Embedded Systems Security settings:*

1. In the Kaspersky Embedded Systems Security Console tree, select the **Kaspersky Embedded Systems Security** node and do one of the following:

- Click the **Application properties** link in the details pane of the node.
- Select **Properties** in the node's context menu.

The **Application settings** window opens.

2. In the window that opens, configure general Kaspersky Embedded Systems Security settings according to your preferences:

- The following settings can be configured on the **Scalability and interface** tab:
 - In the **Scalability settings** section:
 - Maximum number of working processes that Kaspersky Embedded Systems Security can run;

Table 8. Maximum number of active processes

Setting	Maximum number of active processes									
Description	<p>This setting belongs to the Scalability settings group in Kaspersky Embedded Systems Security. It sets the maximum number of active processes that application can run simultaneously.</p> <p>Increasing the number of processes running in parallel increases the speed of file scanning and improves the fail-safety of Kaspersky Embedded Systems Security. However, if the value of this setting is too high, it may reduce the general computer performance and increase RAM usage.</p> <p>In the Administration Console of the Kaspersky Security Center application you can change the Maximum number of active processes setting only for Kaspersky Embedded Systems Security installed on a stand-alone computer (using the Application settings dialog box); however, you cannot modify this setting in the policy settings for group of computers.</p>									
Possible values	1 – 8									
Default Value	<p>Kaspersky Embedded Systems Security handles scalability automatically depending on the number of processors on the computer:</p> <table border="1"> <thead> <tr> <th>Number of processors</th> <th>Maximum number of active processes</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>1</td> </tr> <tr> <td>1 < number of processors < 4</td> <td>2</td> </tr> <tr> <td>4 or more</td> <td>4</td> </tr> </tbody> </table>		Number of processors	Maximum number of active processes	1	1	1 < number of processors < 4	2	4 or more	4
Number of processors	Maximum number of active processes									
1	1									
1 < number of processors < 4	2									
4 or more	4									

- Number of processes for Real-Time Protection;

Table 9. Number of processes for Real-Time Protection

Setting	Number of processes for Real-Time Protection
Description	<p>This setting belongs to the Scalability settings group in Kaspersky Embedded Systems Security.</p> <p>Using this setting you can specify the fixed number of processes in which Kaspersky Embedded Systems Security will execute Real-Time Protection tasks.</p> <p>A higher value of this setting will increase the scan speed in the Real-Time Protection tasks. However, the more processes Kaspersky Embedded Systems Security uses, the greater its influence will be on the general performance of the protected computer and usage of RAM resources.</p> <p>In the Administration Console of the Kaspersky Security Center application you can change the Number of processes for Real-Time Protection setting only for Kaspersky Embedded Systems Security installed on a stand-alone computer (using the Application settings window); however, you cannot modify this setting in the policy settings for group of computers.</p>
Possible values	<p>Possible values: 1-N where N is the value specified using the Maximum number of active processes setting.</p> <p>If you set the value of the Number of processes for Real-Time Protection setting as equal to the maximum number of active processes, you will reduce the impact of Kaspersky Embedded Systems Security on the rate of the file exchange between the computers and the computer, thus further improving its performance during Real-Time Protection. However, update tasks and On-Demand Scan tasks with the Medium (Normal) basic priority will be executed in Kaspersky Embedded Systems Security processes which are already running. On-Demand Scan tasks will be executed with less speed. If the execution of a task causes an abnormal termination of a process, it will take more time to restart it.</p> <p>On-Demand Scan tasks with the Low basic priority are always executed in a separate process or processes.</p>

Default Value	Kaspersky Embedded Systems Security handles scalability automatically depending on the number of processors on the computer:	
	Number of processors	Number of processes for Real-Time Protection
	=1	1
	>1	2

- Number of working processes for background On-Demand Scan tasks;

Table 10. Number of processes for background On-Demand Scan tasks

Setting	Number of processes for background On-Demand Scan tasks
Description	<p>This setting belongs to the Scalability settings group in Kaspersky Embedded Systems Security.</p> <p>You can use this setting to specify the maximum number of processes which Kaspersky Embedded Systems Security will use to run On-Demand Scan tasks in the background mode.</p> <p>The number of processes specified by this setting is not included in the total number of Kaspersky Embedded Systems Security processes specified by the Maximum number of active processes setting.</p> <p>For example, if you specify the following values of settings:</p> <ul style="list-style-type: none"> • Maximum number of active processes – 3; • Number of processes for Real-Time Protection tasks – 3; • Number of processes for background On-Demand Scan tasks – 1; <p>and then start Real-Time Protection tasks and one On-Demand Scan task in background mode, the total number of kavfswp.exe processes of Kaspersky Embedded Systems Security will be 4.</p> <p>Several On-Demand Scan tasks can be running in one process with low priority.</p> <p>You can increase the number of processes, for example, if you run several tasks in background mode in order to allocate a separate process for each task. Allocating separate processes for tasks increases the reliability and speed of task execution.</p>

Possible values	1-4
Default Value	1

- In the **Interaction with user** section select if the Kaspersky Embedded Systems Security icon will be displayed in the taskbar after each application start (see "Kaspersky Embedded Systems Security icon in the notification area" on page [24](#)).
- The following settings can be configured on the **Security and reliability** tab:
 - In the **Reliability settings** section, specify the number of attempts to recover an On-Demand Scan task after it crashed.

Table 11. Task recovery

Setting	Task recovery (Perform task recovery)
Description	<p>This setting belongs to the Reliability settings group in Kaspersky Embedded Systems Security. It enables recovery of tasks in case of their emergency termination and defines the number of attempts used to recover On-Demand Scan tasks.</p> <p>When a task crashes, the kavfs.exe process of Kaspersky Embedded Systems Security attempts to restart the process in which that task was running at the time of the crash.</p> <p>If task recovery is disabled, Kaspersky Embedded Systems Security does not restore the Real-Time Protection and On-Demand Scan tasks.</p> <p>If task recovery is enabled, Kaspersky Embedded Systems Security attempts to restore the Real-Time Protection tasks until they are started successfully and tries to restore On-Demand Scan tasks using the number of attempts specified in the setting.</p>

Possible values	Enabled / disabled. The number of On-Demand Scan tasks recovery attempts: 1 - 10.
Default Value	Task recovery is enabled. The number of On-Demand Scan tasks recovery attempts: 2.

- In the **Actions when switching to UPS backup power** section, specify actions that Kaspersky Embedded Systems Security performs after switching to UPS power:

Table 12. Use of uninterruptible power supply

Setting	Actions when switching to UPS backup power.
Description	This setting determines the actions that Kaspersky Embedded Systems Security performs when the computer switches to an uninterruptible power supply source.
Possible values	Run or do not run On-Demand Scan tasks to be started according to schedule. Perform or stop all active On-Demand Scan tasks.
Default Value	By default, if uninterruptible power supply is used to power the computer, Kaspersky Embedded Systems Security: <ul style="list-style-type: none"> • does not run On-Demand Scan tasks that run according to schedule; • automatically stops all active On-Demand Scan tasks.

- In the **Password settings** section, configure the settings for password-protection of the application's functions.
- On the **Connection settings** tab:
 - In the **Proxy server settings** section, specify the proxy server usage settings.
 - In the **Proxy server authentication settings** section specify authentication type and details required for authentication on the proxy server.
 - In the **Licensing** section, indicate whether Kaspersky Security Center will be used as a proxy-server for application activation.
- On the **Malfunction diagnosis** tab:

- If you want the application to write debug information to file, select the **Write debug information to trace file** check box.

- In the field below specify the folder in which Kaspersky Embedded Systems Security will save trace files.
- Configure the level of detail of debug information.

This drop-down list lets you select the level of detail of debug information that Kaspersky Embedded Systems Security saves to the trace file.

You can select one of the following detail levels:

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

A Technical Support representative determines the detail level that needs to be set in order to resolve the issue that arose.

The default level of detail is set to **All debug information**.

The drop-down list is available if the **Write debug information to trace file** check box is selected.

- Specify the maximum size of trace files.
- Specify the components to be debugged.

A list of codes of Kaspersky Embedded Systems Security components for which application saves debug information in the trace file.

Component codes must be separated with a semicolon. The codes are case sensitive (see table below).

Table 13. Kaspersky Embedded Systems Security subsystem codes

Component Code	Name of component
*	All components.
gui	User interface subsystem, Kaspersky Embedded Systems Security snap-in in Microsoft Management Console.
ak_conn	Subsystem for integrating Network Agent and Kaspersky Security Center.
bl	Control process, implements Kaspersky Embedded Systems Security control tasks.
wp	Work process, handles anti-virus protection tasks.
blgate	Kaspersky Embedded Systems Security remote management process.
ods	On-Demand Scan subsystem.
oas	Real-Time File Protection subsystem.
qb	Quarantine and Backup subsystem.
scandll	Auxiliary module for anti-virus scans.
core	Subsystem for basic anti-virus functionality.
avscan	Anti-virus processing subsystem.
avserv	Subsystem for controlling the anti-virus kernel.
prague	Subsystem for basic functionality.
updater	Subsystem for updating databases and software modules.
snmp	SNMP protocol support subsystem.
perfcoun	Performance counter subsystem.

The trace settings of the Kaspersky Embedded Systems Security snap-in (gui) and the Kaspersky Embedded Systems Security 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 (perfcoun) are applied after all processes that use performance counters are restarted. Trace settings for other Kaspersky Embedded Systems Security subsystems are applied as soon as the crash diagnostics settings are saved.

By default, Kaspersky Embedded Systems Security logs debug information for all Kaspersky Embedded Systems Security components.

The entry field is available if the **Write debug information to trace file** check box is selected.

- If you want the application to create a dump file, select the **Create dump file** check box.
 - In the field below specify the folder in which Kaspersky Embedded Systems Security will save the memory dump file.

Kaspersky Embedded Systems Security writes information to trace files and the dump file in unencrypted form.

1. Click **OK**.

Kaspersky Embedded Systems Security settings are saved.

Managing Kaspersky Embedded Systems Security via Kaspersky Embedded Systems Security Console on another computer

You can manage Kaspersky Embedded Systems Security via the Console installed on a remote computer.

To manage the application using Kaspersky Embedded Systems Security Console on a remote computer, make sure that:

- Kaspersky Embedded Systems Security Console users on the remote computer are added to the ESS Administrators group on the protected computer.
- Network connections are allowed for the Kaspersky Security Management Service process (kavfsgt.exe) if Windows Firewall is enabled on the protected computer.
- During installation of Kaspersky Embedded Systems Security, the **Allow remote access** check box was selected in the Installation Wizard window.

If Kaspersky Embedded Systems Security on the remote computer is password protected, enter the password to get access for application management via the Console.

Configuring the Trusted Zone

This section provides information about the Trusted Zone of Kaspersky Embedded Systems Security, as well as instructions on how to add objects to the Trusted Zone when executing Kaspersky Embedded Systems Security tasks.

In this section

About Kaspersky Embedded Systems Security Trusted Zone.....	57
Enabling and disabling the use of the Trusted Zone in Kaspersky Embedded Systems Security tasks.....	60
Adding exclusions to the Trusted Zone	61

About Kaspersky Embedded Systems Security Trusted Zone

The Trusted Zone is a list of exclusions from the protection or scan scope that you can generate and apply to On-Demand Scan and Real-Time File Protection tasks.

If you selected the **Add Microsoft recommended files to exclusions list** and **Add files recommended by Kaspersky Lab to exclusions** check boxes when installing Kaspersky Embedded Systems Security, Kaspersky Embedded Systems Security adds to the Trusted Zone files recommended by Microsoft and Kaspersky Lab for Real-Time Protection tasks.

You can create a Trusted Zone in Kaspersky Embedded Systems Security according to the following rules:

- **Trusted processes.** Objects accessed by application processes that are sensitive to file intercepts are placed in the Trusted Zone.

- **Backup operations.** Objects accessed by systems to backup hard drives to external devices are placed in the Trusted Zone.
- **Exclusions.** Objects specified by their location and / or an object detected inside them are placed in the Trusted Zone.

You can apply the Trusted Zone in Real-Time File Protection tasks, newly created custom On-Demand Scan tasks, and all system On-Demand Scan tasks, except for the Quarantine Scan task.

The Trusted Zone is applied in Real-Time File Protection and On-Demand Scan tasks by default.

The list of rules for generating the Trusted Zone can be exported to a configuration file in XML format for it then to be imported into Kaspersky Embedded Systems Security running on another computer.

Trusted processes

Applies to the Real-Time File Protection task.

Some applications on the computer may be instable if the files that they access are intercepted by Kaspersky Embedded Systems Security. Such applications include, for example, system domain controller applications.

To avoid disrupting the operation of such applications, you can disable Real-Time Protection of files accessed by the running processes of these applications (thereby creating a list of trusted processes within the Trusted Zone).

Microsoft Corporation recommends excluding some Microsoft Windows operating system files and Microsoft application files from Real-Time File Protection as programs that cannot be infected. The names of some of these are listed on the Microsoft website <https://www.microsoft.com/en-us/> (article code: KB822158).

You can enable or disable the use of trusted processes in the Trusted Zone.

If the executable process file is modified, for example, if it is updated, Kaspersky Embedded Systems Security will exclude it from the list of trusted processes.

Kaspersky Embedded Systems Security does not apply path to file value on a protected computer to trust the process. The path to the file on the protected computer is used only to search for the file, calculate a checksum, and provide the user with the information about the source of the executable file.

Backup operations

Applies to Real-Time Protection tasks.

While data stored on hard drives is backed up to external devices you can disable Real-Time Protection of objects that are accessed during the backup operations. Kaspersky Embedded Systems Security will scan objects which the backup copying application opens for reading with the FILE_FLAG_BACKUP_SEMANTICS attribute.

Exclusions

Applies to Real-Time File Protection and On-Demand Scan tasks.

You can select tasks for which you want to use every exclusion added to the Trusted Zone. Also, you can exclude objects from scans in the security level settings of every single Kaspersky Embedded Systems Security task.

You can add objects to the Trusted Zone by their location on the computer, by name or name mask of the object detected in those objects, or by using both criteria.

Based on the exclusion, Kaspersky Embedded Systems Security can skip objects while performing the specified tasks according to the following settings:

- Specified objects detected by name or name mask in the specified areas of the computer
- All detected objects in the specified areas of the computer
- Specified detectable objects by name or name mask within the entire protection or scan scope

Enabling and disabling Trusted Zone usage in Kaspersky Embedded Systems Security tasks

By default, the Trusted Zone is applied in the Real-Time File Protection task, newly created custom On-Demand Scan tasks, and all system On-Demand Scan tasks, except the Quarantine Scan task.

After the Trusted Zone is enabled or disabled, the specified exclusions are immediately applied or cease to be applied in running tasks.

► *To enable or disable the use of the Trusted Zone in Kaspersky Embedded Systems Security tasks, take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, open the context menu for which you want to configure how the Trusted Zone is applied.
2. Select **Properties**.

The **Task settings** window opens.

3. In the window that opens, go to the **General** tab and do one of the following actions in the appropriate section:
 - To apply the Trusted Zone in the task, select the **Apply Trusted Zone** check box.
 - To disable the Trusted Zone in the task, clear the **Apply Trusted Zone** check box.
4. If you want to configure Trusted Zone settings, click the link set in the name of the **Apply Trusted Zone** check box (see section «**Adding exclusions to the Trusted Zone**» on page [61](#)).
5. Click **OK**.

Any changes are saved.

Adding exclusions to the Trusted Zone

This section provides instructions on how to add common exclusions to the Trusted Zone of Kaspersky Embedded Systems Security.

In this section

Trusting processes	61
Untrusting processes	64
Disabling Real-Time File Protection during backup	64
Adding an exclusion to the Trusted Zone	65

Trusting processes

You can add a process to the list of trusted processes using one of the following methods:

- Select the process from the list of processes running on the protected computer;
- Select the executable file of a process regardless of whether the process is currently running.

If the executable file of a process has been modified, Kaspersky Embedded Systems Security excludes this process from the list of trusted processes.

► *To add a process to the list of trusted processes, take the following steps:*

1. In the Console tree, open the context menu of the **Kaspersky Embedded Systems Security** node.
2. Select **Configure Trusted Zone settings**.

The **Trusted Zone** window opens.

3. In the **Trusted Zone** window, on the **Trusted processes** tab, select the **Do not check file activity of the specified processes** check box.

4. Click the **Add** button.

The **Add trusted process** window opens.

5. Add a trusted process in one of the following ways:

- To add a process from the list of running processes:
 - a. In the **Add trusted process** window, click the **Processes** button.

The **Active processes** window opens.

- b. In the **Active processes** window, select the desired process in the list of running processes and click the **OK** button.

The **Trust Criteria** section is automatically populated with data for this process.

It is required that the account under which the Real-Time File Protection task is run has the administrator rights on the computer with Kaspersky Embedded Systems Security installed in order to allow viewing the list of active processes. You can sort processes in the list of active processes by file name, PID, or path to the executable file of the process on the local computer.

- To specify the executable file of the process:
 - a. In the **Add trusted process** window, click the **Browse** button.

The standard Microsoft Windows Open File window opens.

- b. Select the process's executable file and click **Browse**.

The **Trust Criteria** section is automatically populated with data for this file.

Kaspersky Embedded Systems Security does not apply path to file value on a protected computer to trust the process. The path to the file on the protected computer is used only to search for the file, calculate a checksum, and provide the user with the information about the source of the executable file.

6. Choose the trust criteria you want to consider for the selected executable file or process:

- Use the full path to determine whether the process is trusted.

If the check box is selected, Kaspersky Embedded Systems Security uses the full path to the file to determine the process's trust status.

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

The check box is selected by default.

- Use the file's hash to determine whether the process is trusted.

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

If the check box is cleared, the file's hash will not be considered as a criterion for determining the process's trust status.

The check box is selected by default.

To add an executable file or 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.

Untrusting processes

► To disable the use of a trusted process in the Trusted Zone, take the following steps:

1. In the Console tree, open the context menu of the **Kaspersky Embedded Systems Security** node.
2. Select **Configure Trusted Zone settings**.

The **Trusted Zone** window opens.

3. In the **Trusted Zone** window, on the **Trusted processes** tab. In the list of trusted processes, clear the check box next to the name of the executable file of the process that you want to not be applied temporarily in the Trusted Zone.
4. Click **OK**.

The **Trusted Zone** window closes, and the selected processes are removed from the list of trusted processes.

Disabling Real-Time File Protection during backup

► To disable Real-Time File Protection while backing up data from hard drives, take the following steps:

1. In the Console tree, open the context menu of the **Kaspersky Embedded Systems Security** node.
2. Select **Configure Trusted Zone settings**.

The **Trusted Zone** window opens.

3. On the **Trusted processes** tab in the **Trusted Zone** window, select the **Do not check file backup operations** check box.
4. Click **OK**.

The **Trusted Zone** window closes, and Real-Time File Protection is paused during backup.

Adding an exclusion to the Trusted Zone

► To add an exclusion to the Trusted Zone, take the following steps:

1. In the Console tree, open the context menu of the **Kaspersky Embedded Systems Security** node.
2. Select **Configure Trusted Zone settings**.

The **Trusted Zone** window opens.

3. In the **Trusted Zone** window, on the **Exclusions** tab, click the **Add** button.

The **Exclusion** window opens.

4. In the **Object will not be scanned if the following conditions are met** section, specify the objects that you want to exclude from the protection / scan scope and objects that you want to exclude from among detectable objects (such as remote administration utilities):

- If you want to exclude an object from the protection / scan scope:

- a. Select the **Object to scan** check box.

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

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

The check box is selected by default.

- b. Click the **Edit** button.

The **Select object** window opens.

- c. In the window that opens, specify the object that you want to exclude from the scan scope.

You can use the special characters ? and * to specify objects.

- If you want to specify the name of a detectable object:

- a. Select the **Objects to detect** check box.

Objects are excluded from scanning by the name or name mask of the detectable object. The list of names of detectable objects is available on the Virus Encyclopedia website (<http://www.securelist.com>).

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

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

The check box is cleared by default.

- b. Click the **Edit** button.

The **List of objects to detect** window opens.

- c. In the window that opens, specify the name or the mask of the name of the detectable object according to the Virus Encyclopedia classification (<http://www.securelist.com>).

- In the **Exclusion scope** section, select the check boxes next to the names of the tasks to which the exclusion should be applied.

5. Click **OK**.

The exclusion is displayed in the list on the **Exclusions** tab of the **Trusted Zone** window.

Managing Kaspersky Embedded Systems Security tasks

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

In this section

Kaspersky Embedded Systems Security task categories	67
Saving a task after changing its settings	68
Starting / pausing / resuming / stopping tasks manually	69
Managing task schedules.....	69
Using user accounts to launch tasks	72
Importing and exporting settings	74
Using security settings templates	79

Kaspersky Embedded Systems Security task categories

Real-Time Protection, Computer Control, On-Demand Scan, and Update functions in Kaspersky Embedded Systems Security are implemented as tasks.

You can manage tasks using the task's context menu in the Console tree, the toolbar, and the quick access bar. You can view task status information in the details pane. Task management operations are recorded in the system audit log.

There are two types of Kaspersky Embedded Systems Security tasks: *local* and *group*.

Local tasks

Local tasks are executed only on the protected computer for which they are created.

Depending on the start method, the following types of local tasks exist:

- **Local system tasks.** Created automatically during installation of Kaspersky Embedded Systems Security. You can edit the settings of all system tasks, except for the Quarantine Scan and Rollback of Database Update tasks. System tasks cannot be renamed or deleted. You can run system and custom On-Demand Scan tasks simultaneously.
- **Local custom tasks.** In the Kaspersky Embedded Systems Security Console, you can create On-Demand Scan tasks. In Kaspersky Security Center you can create On-Demand Scan, Database Update, Rollback of Database Update, and Copying Updates tasks. Such tasks are called custom tasks. Custom tasks can be renamed, configured, and deleted. You can run several custom tasks simultaneously.

Group tasks

Group tasks and tasks for sets of computers created using Kaspersky Security Center are displayed in Kaspersky Embedded Systems Security Console. Such tasks are called group tasks. Group tasks can be managed and configured from the Kaspersky Security Center. In Kaspersky Embedded Systems Security Console, you can only view the status of group tasks.

Saving a task after changing its settings

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

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

► *To save modified task settings,*

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

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

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

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

Starting / pausing / resuming / stopping tasks manually

You can pause and resume only Real-Time Protection and On-Demand Scan tasks.

► *To start / pause / resume / stop a task, take the following steps:*

1. Open the context menu of the task name in Kaspersky Embedded Systems Security Console.
2. Select one of the following: **Start**, **Pause**, **Resume** or **Stop**.

The operation is executed and registered in the system audit log (see section "System audit log" on page [309](#)).

When an On-Demand Scan task is resumed, Kaspersky Embedded Systems Security continues with the object that was being scanned when the task was paused.

Managing task schedules

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

In this section

Configuring the task launch schedule settings.....	70
Enabling and disabling scheduled tasks.....	72

Configuring the task launch schedule settings

You can configure the launch schedule for local system and custom tasks in the Kaspersky Embedded Systems Security Console (see page [67](#)). You cannot configure the launch schedule for group tasks.

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

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

The **Task settings** window opens.

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

Fields with task schedule settings for the On-Demand Scan and Update tasks are not available if starting the tasks on a schedule is blocked by a Kaspersky Security Center policy.

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

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

- **Hourly**, if you want the task to run at intervals of a specified number of hours; specify the number of hours in the **Every <number> hours** 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> days** 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> weeks** field. Specify the days of the week on which the task will be started (by default the task runs on Mondays).
- **At application launch**, if you want the task to run every time Kaspersky Embedded Systems Security starts.

- **After application database update**, if you want the task to run after every update of the application databases.
- b. Specify the time for the first task start in the **Start time** field.
 - c. In the **Start date** field, specify the date from which the schedule applies.

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

Blocked by policy is displayed in the **Next start** field if starting system tasks on a schedule is blocked by the settings of a Kaspersky Security Center policy.

5. Use the **Advanced** tab to configure the following schedule settings in accordance with your requirements.
 - In the **Task stop settings** section:
 - a. Select the **Duration** check box and enter the required number of hours and minutes in the fields to the right to specify the maximum duration of the task execution.
 - b. Select the **Pause from ... until** 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 launch of skipped tasks.
 - c. Select the **Randomize the task start within interval of** check box and specify a value in minutes.
6. Click the **Apply** button.

The configured task launch settings will be saved.

Enabling and disabling scheduled tasks

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

► *To enable or disable the task launch schedule, take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree open the context menu on the task name for which you wish to configure the launch schedule.

2. Select **Properties**.

The **Task settings** window opens.

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

- Select the **Run by schedule** check box if you want to enable scheduled task start.
- Clear the **Run by schedule** check box if you want to disable scheduled task start.

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

4. Click the **Apply** button.

The configured task launch schedule settings are saved.

Using user accounts to start tasks

You can start tasks under the system account or specify a different account.

In this section

About using accounts to launch tasks	73
Specifying a user account to launch a task.....	73

About using accounts to start tasks

You can specify the account under which you want to run the selected task for the following functional components of Kaspersky Embedded Systems Security:

- Rule Generator for Applications Launch Control and Rule Generator for Device Control tasks;
- On-Demand Scan task
- Update tasks.

By default, these tasks are run using system account permissions.

A different account with proper access permissions is recommended in the following cases:

- in the Update task, if you specified a public folder on a different computer on the network as the update source;
- in the Update task, if a proxy server with built-in Windows NTLM authentication is used to access the update source;
- in On-Demand Scan tasks, if the system account does not possess permissions to access any of the scanned objects (for example, to files in shared network folders on the computer);
- in the Rule Generator for Applications Launch Control task, if after completion of the task the generated rules are exported to a configuration file located at a path that the system account cannot access (for example, in one of the shared network folders on the computer).

You can run Update, On-Demand Scan, and Rule Generator tasks with system account permissions. During execution of these tasks, Kaspersky Embedded Systems Security accesses shared folders on another computer in the network if this computer is registered in the same domain as the protected computer. In this case, the system account must possess access permissions for these folders. Kaspersky Embedded Systems Security will access the computer using permissions of the account **<domain name \ computer_name>**.

Specifying a user account to start a task

► *To specify an account to start a task, take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, open the context menu of the name of the task for which you want to configure start with account permissions.
2. Select **Properties**.

The **Task settings** window opens.

3. In the window that opens, do the following on the **Run as** tab:
 - a. Select **User name**.
 - b. Enter the user name and password for the account you want to use.

The selected user must be registered on the protected computer or in the same domain as this computer.

- c. Confirm the password that has been entered.
4. Click the **Apply** button.

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

Importing and exporting settings

This section provides information about how to export the settings of Kaspersky Embedded Systems Security or the settings of specific software components to a configuration file in XML format and how to import those settings from that configuration file back to the application.

In this section

About importing and exporting settings	75
Exporting settings.....	77
Importing settings.....	78

About importing and exporting settings

You can export Kaspersky Embedded Systems Security settings to an XML configuration file and import settings into Kaspersky Embedded Systems Security from the configuration file.

You can save all application settings or only settings for individual components to a configuration file.

When you export all settings of Kaspersky Embedded Systems Security to a file, the general application settings and settings of the following Kaspersky Embedded Systems Security components and functions are saved:

- Real-Time File Protection
- KSN Usage
- Device Control
- Applications Launch Control
- Rule Generator for Device Control
- Rule Generator for Applications Launch Control

- On-Demand Scan
- Kaspersky Embedded Systems Security database and software modules update
- Quarantine
- Backup
- Logs
- Administrator and user notifications
- Trusted Zone

Also, you can save the general settings of Kaspersky Embedded Systems Security in the file, as well as the rights of user accounts.

You cannot export group task settings.

Kaspersky Embedded Systems Security exports all passwords used by the application, for example, account data for running tasks or connecting to a proxy server. Exported passwords are saved in encrypted form in the configuration file. You can import passwords only using Kaspersky Embedded Systems Security installed on this computer if it has not been reinstalled or updated.

You cannot import previously saved passwords using Kaspersky Embedded Systems Security installed on a different computer. After settings have been imported on another, all passwords must be entered manually.

If a Kaspersky Security Center policy is active at the time of export, the application exports the specified values used by that policy.

Settings from a configuration file containing parameters for individual components of Kaspersky Embedded Systems Security (e.g., from a file created in Kaspersky Embedded Systems Security installed with incomplete set of components) can be imported. After the settings are imported, only those Kaspersky Embedded Systems Security settings that were contained in the configuration file are changed. All other settings remain the same.

Imported task settings are not applied during task execution. To apply imported settings, you must restart the task.

Settings of an active Kaspersky Security Center policy that have been blocked do not change when importing the settings.

Exporting settings

► *To export settings to a configuration file, take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, do one of the following:

- In the context menu of the **Kaspersky Embedded Systems Security** node, select **Export settings** to export all Kaspersky Embedded Systems Security settings.
- In the context menu for the task whose settings you want to export, select **Export settings** to export the settings of an individual functional component of the application.

• To export the settings of the Trusted Zone component:

a. In the Console tree, open the context menu of the **Kaspersky Embedded Systems Security** node.

b. Select **Configure Trusted Zone settings**.

The **Trusted Zone** window opens.

c. Click the **Export** button.

The welcome window of the settings export wizard opens.

2. Follow the instructions in the Wizard: specify the name of the configuration file for saving settings and the path to it.

System environment variables can be used when specifying the path; user environment variables are not allowed.

If a Kaspersky Security Center policy is active at the time of export, the application exports the settings' values used by that policy.

3. Click **OK** in the **Export of application settings complete** window.

The export settings are saved when the wizard closes.

Importing settings

► *To import settings from a saved configuration file, take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, do one of the following:

- In the context menu of the **Kaspersky Embedded Systems Security** node, select **Import settings** to import all Kaspersky Embedded Systems Security settings.
- In the context menu for the task whose settings you want to import, select **Import settings** to import the settings of an individual functional component of the application.
- To import the settings of the Trusted Zone component:
 - a. In the Console tree, open the context menu of the **Kaspersky Embedded Systems Security** node.
 - b. Select **Configure Trusted Zone settings**.
The **Trusted Zone** window opens.
 - c. Click the **Import** button.

The welcome window of the settings import wizard opens.

2. Follow the instructions in the Wizard: specify the configuration file from which you want to import settings.

After you have imported the general settings of Kaspersky Embedded Systems Security or its functional components on the computer, you will not be able return to the previous setting values.

3. Click **OK** in the **Application settings import completed** window.

The imported settings are saved when the wizard closes.

4. In the toolbar of the Kaspersky Embedded Systems Security Console, click the **Refresh** button.

The imported settings are displayed in the Console window.

Kaspersky Embedded Systems Security does not import passwords (account data to launch tasks or connect to the proxy server) from the file created on another computer or on the same computer, after Kaspersky Embedded Systems Security has been re-installed or updated on it. After the importing operation is completed, passwords must be entered manually.

Using security settings templates

This section contains information about using security settings templates in Kaspersky Embedded Systems Security protection and scan tasks.

In this section

About security settings templates.....	79
Creating a security settings template.....	80
Viewing security settings in a template.....	81
Applying a security settings template	82
Deleting a security settings template	83

About security settings templates

You can manually configure a node's security settings in the tree or in a list of the computer's file resources, and save the configured setting values as a template. This template can then be used to configure the security settings of other nodes in Kaspersky Embedded Systems Security protection and scan tasks.

Templates can be used to configure the security settings of the following Kaspersky Embedded Systems Security tasks:

- Real-Time File Protection
- Scan at Operating System Startup
- Critical Areas Scan
- On-Demand Scan tasks

Security settings from a template applied to a parent node in the computer's file resource tree are applied to all subnodes. A parent node's template is not applied to subnodes in the following cases:

- If the security settings of the subnodes were configured separately (see section "Applying a security settings template" on page [82](#)).
- If the subnodes are virtual. You must apply the template to each virtual node separately.

Creating a security settings template

► *To manually save a node's security settings to a template:*

1. In the Kaspersky Embedded Systems Security Console tree, select the task for which you want to save the security settings to a template.
2. In the details pane of the selected task, click the **Configure protection scope** or **Configure scan scope** link.
3. In the tree or list of the computer's file resources, choose the node whose settings you want to save as a template.

4. In the lower part of the window click the **Save as template** button.

The **Template properties** window opens.

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

The template with the set of security settings is saved.

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

Viewing security settings in a template

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

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

The **Templates** window opens.

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

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

Applying a security settings template

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

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

The security settings template is applied to the selected node in the tree of the computer's file resources. The **Security level** tab of the selected node now has the value **Custom**.

Security settings from a template applied to a parent node in the computer's file resource tree are applied to all subnodes.

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

► *To apply security settings from a template to all selected nodes, take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, select the task for which you want to save the security settings to a template.
2. In the details pane of the selected task, click the **Configure protection scope** or **Configure scan scope** link.
3. In the tree or list of the computer's file resources, select a parent node in order to apply the template to the selected node and to all of its subnodes.

4. Select **Apply template** → <Template name>.
5. In the Console tree, open the context menu of the task being configured.
6. Select **Save task**.

The security settings template is applied to the parent and all subnodes in the computer's file resource tree. The **Security level** tab of the selected node now has the value **Custom**.

Deleting a security settings template

► To delete a security settings template, take the following steps:

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

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

The **Templates** window opens.

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

A window opens to confirm the deletion.

5. In the window that opens, click **Yes**.

The selected template is deleted.

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

Real-Time Protection

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

In this section

Real-Time File Protection	84
KSN Usage	117
Exploit Prevention	126

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	84
Real-Time File Protection task statistics	85
Configuring Real-Time File Protection task settings	88
Protection scope in Real-Time File Protection task	98

About Real-Time File Protection task

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

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

When any application writes a file to a computer or reads a file from it, Kaspersky Embedded Systems Security intercepts this file, scans it for threats, and, if a threat is detected, performs a default action or an action you have specified: tries to disinfect it, places it in Quarantine, or deletes it. Kaspersky Embedded Systems Security returns the file to the application if it is not infected or if it has been successfully disinfecting.

Real-Time File Protection task statistics

While the Real-Time File Protection task is being executed, you can view detailed real-time information about the number of objects processed by Kaspersky Embedded Systems Security since the task was started until the current moment.

► *To view the statistics of a Real-Time File Protection task, take the following steps:*

1. In the Console tree, expand the **Real-Time Protection** node.
2. Select the **Real-Time File Protection** subnode.

Task statistics are displayed in the **Statistics** section of the details pane of the selected node.

The following information can be viewed about objects processed by Kaspersky Embedded Systems Security since it was started until the current moment (see the table below).

Table 14. Real-Time File Protection task statistics

Field	Description
Detected	Number of objects detected by Kaspersky Embedded Systems Security. For example, if Kaspersky Embedded Systems Security detects one malware in five files, the value in this field increases by one.
Infected and other objects detected	Number of objects that Kaspersky Embedded Systems Security found and classified as infected or number of found legitimate software files, which were not excluded from the real-time protection and on-demand tasks scope and were classified as riskware.
Probably infected objects	Number of objects found by Kaspersky Embedded Systems Security to be probably infected
Objects not disinfected	<p>Number of objects which Kaspersky Embedded Systems Security did not disinfect for the following reasons:</p> <ul style="list-style-type: none"> • the type of detected object cannot be disinfected; • an error occurred during disinfection.
Objects not moved to quarantine	The number of objects that Kaspersky Embedded Systems Security attempted to quarantine but was unable to do so, for example, due to insufficient disk space.
Objects not removed	The number of objects that Kaspersky Embedded Systems Security attempted but was unable to delete, because, for example, access to the object was blocked by another application.
Objects not scanned	The number of objects in the protection scope that Kaspersky Embedded Systems Security failed to scan because, for example, access to the object was blocked by another application.

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

You can view the Real-Time File Protection task statistics in the task log by clicking the **Open task log** in the **Management** section in the detail pane.

If the value of the **Events in total** field in the Real-Time Protection task log window exceeds 0, it is recommended to process the events appeared in the task log on the **Events** tab manually.

Configuring Real-Time File Protection task settings

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 15. 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: <ul style="list-style-type: none"> • Apply another predefined security level. • Edit the security level manually. • Save security settings of the selected node as a template for later application to a different node.
Protection mode	On access and modification.	You can select protection mode, i.e. define type of access at which Kaspersky Embedded Systems Security will scan objects.
Heuristic Analyzer	The Medium security level is applied.	The Heuristic Analyzer can be enabled or disabled and the analysis level configured.
Trusted Zone	Applied. If you selected the Add Microsoft recommended files to exclusions list when installing Kaspersky Embedded Systems Security, the files recommended by Microsoft are excluded.	General list of exclusions which can be used in selected tasks.

Setting	Default Value	Description
KSN Usage services	Used	You can improve your computer's protection using the Kaspersky Security Network infrastructure of cloud services.
Task start schedule	At application start	You can configure the settings of scheduled startup of the task.

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

1. Depending on the application interface, perform the following steps:

- If you want to modify the configuration locally, in the Kaspersky Embedded Systems Security Console select **Real-Time Protection** → **Real-Time File Protection**. Then click the **Properties** link in the details pane of the **Real-Time File Protection** node.
- If you want to modify the configuration locally in the Administration Console of Kaspersky Security Center in the computer group select **Policies** → **<Policy name>** → **Real-Time Protection** → **Settings (Real-Time File Protection section)**.
- If you want to configure the task settings for a single computer through Kaspersky Security Center, open the **Task settings** window in Kaspersky Security Center.

The **Task settings** window opens.

2. Configure the following task settings:

- On the **General** tab:
 - Protection mode (see section "Selecting protection mode" on page [90](#))
 - Using the Heuristic Analyzer (see page [92](#))
 - Settings of integration with other Kaspersky Embedded Systems Security components (see section "Task integration with other components of Kaspersky Embedded Systems Security" on page [93](#))

- On the **Schedule** and **Advanced** tabs:
 - Scheduled task launch settings (see section "Configuring the task launch schedule settings" on page [70](#)).
3. Click **OK** in the **Task settings** window.

The modified settings are saved.

4. In the details pane of the **Real-Time File Protection** node click the **Configure protection scope** link.
5. Do the following:
 - In the tree or in the list of file resources of the computer, select the nodes that you want to be included in the task protection scope (see section "About the protection scope in the Real-Time File Protection task" on page [99](#)).
 - Select one of the predefined security levels (see section "Selecting predefined security levels" on page [108](#)) or configure the object protection settings manually (see section "Configuring security settings manually" on page [110](#)).
6. In the context menu of the task name, select **Save task**.

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

Selecting protection mode

In the Real-Time File Protection task, the protection mode can be selected. The **Objects protection mode** section lets you specify the type of access to objects upon which Kaspersky Embedded Systems Security should scan the objects.

The **Objects protection mode** setting has the common value for the entire protection scope specified in the task. You cannot specify different values for the setting for individual nodes within the protection scope.

► *To select protection mode, take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Real-Time Protection** node.
2. Select the **Real-Time File Protection** subnode.
3. Click the **Properties** link in the details pane.

The **Task settings** 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 selects objects to be scanned on its own. The object is scanned on being opened and then again after being saved if the object has been modified. If multiple calls to the object were made by the process while it was running and if the process modified it, Kaspersky Embedded Systems Security rescans the object only after the object was saved by the process for the last time.

- **On access and modification**

Kaspersky Embedded Systems Security scans the object when it is opened and rescans after it is saved if the object was modified.

This option is selected by default.

- **On access**

Kaspersky Embedded Systems Security scans all objects when they are opened for reading or for execution or modification.

- **When run**

Kaspersky Embedded Systems Security scans the file only when it is accessed to be executed.

5. Click **OK**.

The selected protection mode will take effect.

Using Heuristic Analyzer

In the Real-Time File Protection task, you can use the Heuristic Analyzer and configure the level of analysis.

► *To configure the Heuristic Analyzer, take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Real-Time Protection** node.
2. Select the **Real-Time File Protection** subnode.
3. Click the **Properties** link in the details pane.

The **Task settings** window opens on the **General** tab.

4. Clear or select the **Use Heuristic Analyzer** check box.
5. 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.

6. Click **OK**.

The newly configured settings will be applied.

Task integration with other Kaspersky Embedded Systems Security components

In the Real-Time File Protection task, you can configure the settings of task integration with other functional components of Kaspersky Embedded Systems Security.

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

If you accepted the KSN Statement when the application is installed, the KSN Usage task will be started automatically when Kaspersky Embedded Systems Security is started. You can also run the task manually (see section "Starting and stopping the KSN Usage task" on page [119](#)) or schedule its launch (see section "Configuring the KSN Usage task" on page [121](#)).

► *To configure interaction between the Real-Time File Protection task and other software components, take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Real-Time Protection** node.
2. Select the **Real-Time File Protection** subnode.
3. Click the **Properties** link in the details pane.

The **Task settings** window opens on the **General** tab.

4. In the **Integration with other Kaspersky Security components** section, configure the following settings:

- Select or clear the **Apply Trusted Zone** check box.

This check box enables / disables use of the Trusted Zone for a task.

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

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

The check box is selected by default.

- Select or clear the **Use KSN for protection** check box.

This check box enables / 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 Real-Time File Protection task does not use KSN service.

The check box is selected by default.

5. Click **OK**.

The newly configured settings will be applied.

List of file extensions scanned by default in Real-Time File Protection task

Kaspersky Embedded Systems Security scans files with the following extensions by default:

- *386*;
- *acm*;
- *ade, adp*;
- *asp*;
- *asx*;
- *ax*;
- *bas*;
- *bat*;
- *bin*;
- *chm*;

- *cla, clas**;
- *cmd*;
- *com*;
- *cpl*;
- *crt*;
- *dll*;
- *dpl*;
- *drv*;
- *dvb*;
- *dwg*;
- *efi*;
- *emf*;
- *eml*;
- *exe*;
- *fon*;
- *fpm*;
- *hlp*;
- *hta*;
- *htm, html**;
- *htt*;
- *ico*;
- *inf*;

- *ini*;
- *ins*;
- *isp*;
- *jpg, jpe*;
- *js, jse*;
- *lnk*;
- *mbx*;
- *msc*;
- *msg*;
- *msi*;
- *msp*;
- *mst*;
- *nws*;
- *ocx*;
- *oft*;
- *otm*;
- *pcd*;
- *pdf*;
- *php*;
- *pht*;
- *phm**;
- *pif*;

- *plg*;
- *png*;
- *pot*;
- *prf*;
- *prg*;
- *reg*;
- *rsc*;
- *rtf*;
- *scf*;
- *scr*;
- *sct*;
- *shb*;
- *shs*;
- *sht*;
- *shtm**;
- *swf*;
- *sys*;
- *the*;
- *them**;
- *tsp*;
- *url*;
- *vb*;

- *vbe*;
- *vbs*;
- *vxd*;
- *wma*;
- *wmf*;
- *wmv*;
- *wsc*;
- *wsf*;
- *wsh*;
- *do?*;
- *md?*;
- *mp?*;
- *ov?*;
- *pp?*;
- *vs?*;
- *xl?*.

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

About the protection scope in the Real-Time File Protection task.....	99
Predefined protection scopes.....	100
Configuring view mode for network file resources	101
Creating the protection scope	102
Virtual protection scope.....	105
Creating a virtual protection scope	105
Security settings of the selected node in the Real-time file protection task.....	107
Selecting predefined security levels	108
Configuring security settings manually	110

About protection scope in Real-Time File Protection task

By default, the Real-Time File Protection task protects all objects of the computer file system. If there is no security requirement to protect all objects of the file system or you want to exclude any objects from the task scope, you can limit the protection scope.

In Kaspersky Embedded Systems Security Console, the protection scope is displayed as a tree or in the list of the computer file resources that Kaspersky Embedded Systems Security can control. By default, the network file resources of the protected computer are displayed in a list-view mode.

► *To display network file resources in the tree-view mode,*

open the drop down list in the **Protection scope settings** window upper left sector and select **Tree-view**.

The nodes are displayed in a list-view or in a tree-view mode of the Computer file resources as follows:

The node is included in the protection scope.

The node is excluded from the protection scope.

At least one of the subnodes of this node is excluded from the protection scope, or the security settings of the subnode(s) differ(s) from the setting of a parental node (for a tree-view mode only).

The icon is displayed if all subnodes are selected, but the parent node is not selected. In this case, changes in the composition of files and folders of the parent node are disregarded automatically when the protection scope for the selected subnode is being created.

The names of the virtual nodes in the protection scope are displayed in blue font.

Predefined protection scopes

To view the computer file resources click **Protection scope settings** link in the details pane of the **Real-Time File Protection** node. You can configure a tree-view or a list-view modes of network file resources displaying.

The file resources tree or list displays the nodes to which you have read-access based on the configured security settings of Microsoft Windows.

Kaspersky Embedded Systems Security covers the following predefined protection scopes:

- **Local hard drives.** Kaspersky Embedded Systems Security protects files on the computer hard drives.
- **Removable drives.** Kaspersky Embedded Systems Security protects files on external devices, such as CDs or USB drives. All removable disks, individual disks, folders or files can be included in or excluded from the protection scope.

- **Network** Kaspersky Embedded Systems Security protects files that are written to network folders or read from them by applications running on the computer. Kaspersky Embedded Systems Security does not protect files when such files are accessed by applications from other computers.
- **Virtual drives** Dynamic folders and files and drives that are temporarily connected to the computer can be included in the protection scope, for example, common cluster drives.

By default, you can view and configure predefined protection scopes in the network file resources tree; you can also add predefined scopes to the network file resources 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 Kaspersky Embedded Systems Security 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 tree. 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.

Configuring view mode for network file resources

► *To select view-mode for the network file resources during configuring the protection scope settings, take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Real-Time Protection** node.
2. Select the **Real-Time File Protection** subnode.
3. In the details pane of the **Real-Time File Protection** node click the **Configure protection scope** link.

The **Protection scope settings** window opens.

4. Open the drop down list in the upper left section of the window. Perform one of the following steps:
 - Select the **Tree-view** option to display the network file resources in a tree-view mode.
 - Select the **List-view** option to display the network file resources in a list-view mode.

By default, the network file resources of the protected computer are displayed in a list-view mode.

5. Click the **Save** button.

Scan scope settings window will be closed. The newly configured settings will be applied.

Creating protection scope

The procedure of creating the Real-Time File Protection task scope depends on the network file resources view mode (see section «Configuring view mode for network file resources» on page [101](#)). You can configure network file resources view mode as a tree or as a list (set as default).

To apply the new protection scope settings to the task, the Real-Time File Protection task must be restarted.

- *To create a protection scope using the network file resources tree, take the following steps:*
 1. In the Kaspersky Embedded Systems Security Console tree, expand the **Real-Time Protection** node.
 2. Select the **Real-Time File Protection** subnode.
 3. In the details pane of the selected node click the **Configure protection scope** link.

The **Protection scope settings** window opens.

4. In the left section of the window open the network file resources tree to display all the nodes and subnodes.

5. Do the following:

- To exclude individual nodes from the protection scope, clear check boxes next to the names of these nodes.
- To include individual nodes in the protection scope, clear the **My computer** check box and do the following:
 - if all drives of one type are to be included in the protection scope, select the check box opposite the name of the required disk type (for example, to add all removable drives on the computer, select the **Removable drives** check box);
 - if an individual disk of a certain type is to be included in the protection scope, expand the node that contains the list of drives of this type and check the box next to the name of the required drive. For example, in order to select removable drive **F:**, expand node **Removable drives** and check the box for drive **F:**;
 - if you would like to include only a single folder or file on the drive, select the check box next to the name of that folder or file.

6. Click the **Save** button.

Scan scope settings window will be closed. Your newly configured settings have been saved.

► *To create a scan scope using the network file resources list, take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Real-Time Protection** node.
2. Select the **Real-Time File Protection** subnode.
3. In the details pane of the selected node click the **Configure protection scope** link.

The **Protection scope settings** window opens.

4. To include individual nodes in the protection scope, clear the **My computer** check box and do the following:
 - a. Open the context menu on the scan scope by right-clicking it.
 - b. In the context menu of the button, select **Add protection scope**.

c. In the **Add protection scope** window select an object type to add it to a protection scope:

- **Predefined scope** to include one of the predefined scopes into protection scope on the computer. Then in the drop down list select a necessary scan scope.
- **Disk, folder or network location** to include individual drive, folder or a network object into a protection scope. Then select a necessary scope by clicking the **Browse** button.
- **File** to include an individual file into protection scope. Then select a necessary scope by clicking the **Browse** button.

You cannot add an object into protection scope if it has already been added as an exclusion out of a protection scope.

5. To exclude individual nodes from the protection scope, clear check boxes next to the names of these nodes or take the following steps:
 - a. Open the context menu on the scan scope by right-clicking it.
 - b. In the context menu select **Add exclusion** option.
 - c. In the **Add exclusion** window select an object type that you want to add as an exclusion out of the protection scope following the logic of the adding object to a protection scope procedure.
6. To modify the protection scope or an exclusion added, select the **Edit scope** option in the context menu for the necessary scope.
7. To hide the previously added protection scope or an exclusion in the list of network file resources, select the **Remove from the list** option in the context menu for the necessary scope.

The protection scope is excluded out of the Real-Time File Protection task scope on its removal from the network file resources list.

8. Click the **Save** button.

Scan scope settings window will be closed. Your newly configured settings have been saved.

The **Real-Time File Protection** task can be started if at least one of the computer file resource nodes is included into a protection scope.

If a complex protection scope is specified, for example, if different security values for settings for multiple nodes in the computer file resource tree are specified, this may slow the scanning of objects when they are accessed.

About virtual protection scope

Kaspersky Embedded Systems Security can scan not only existing folders and files on hard and removable drives, but also drives that are connected to the computer temporarily.

If all computer objects are included in the protection scope, these dynamic nodes will automatically be included in the protection scope. However, if you want to specify special values for the security settings of these dynamic nodes or if you have selected not the entire computer for Real-Time Protection, but discrete areas of it, then in order to include dynamic drives, files or folders in the protection scope, you will first have to create them in Kaspersky Embedded Systems Security Console: that is, specify the virtual protection scope. The drives, files and folders created will exist only in Kaspersky Embedded Systems Security Console, but not in the file structure of the protected computer.

If, while creating a protection scope, all subfolders or files are selected without the parent folder being selected, then all dynamic folders or files which will appear in it will not automatically be included in the protected scope. "Virtual copies" of these should be created in Kaspersky Embedded Systems Security Console and added to the protection scope.

Creating virtual protection scope

You can expand the protection / scan scope by adding individual virtual drives, folders, or files only if the protection / scan scope is presented as a tree of file resources (see section "Configuring view mode for network file resources" on page [101](#)).

► *To add a virtual drive to the protection scope, take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Real-Time Protection** node.
2. Select the **Real-Time File Protection** subnode.
3. In the details pane of the **Real-Time File Protection** node click the **Configure protection scope** link.

The **Protection scope settings** window opens.

4. Open the drop-down list in the window upper left sector and select **Tree-view**.
5. Open the context menu of the **Virtual drives** and in the list of names available select the name for the virtual drive that is being created.
6. Check box next to the drive added to include the drive in the protection scope.
7. In the context menu of the task name, select **Save task**.

Your newly configured settings have been saved.

► *To add a virtual folder or virtual file to the protection scope, take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Real-Time Protection** node.
2. Select the **Real-Time File Protection** subnode.
3. In the details pane of the **Real-Time File Protection** node click the **Configure protection scope** link.

The **Protection scope settings** window opens.

4. Open the drop-down list in the window upper left sector and select **Tree-view**.

5. Open the context menu for the virtual drive to which you want to add a folder or a file, and select one of the following options:
 - **Add virtual folder** if you want to add a virtual folder to the protection scope.
 - **Add virtual file** if you want to add a virtual file to the protection scope.
6. In the entry field specify the name of the folder or file.
7. In the line containing the name of the created folder or file, select the check box to include the folder or file in the protection scope.
8. In the context menu of the task name, select **Save task**.

The modified task settings are saved.

Security settings of selected node in Real-Time File Protection task

In the Real-Time File Protection task, the default values of security settings can be modified by configuring them as common settings for the entire protection or scan scope, or as different settings for different nodes in the computer file resource tree or list.

Security settings configured for the selected parent node are automatically applied to all subnodes. The security settings of the parent node are not applied to subnodes that are configured separately.

The settings for a selected scan scope or protection scope can be configured using one of the following methods:

- Select one of three predefined security levels (**Maximum performance**, **Recommended** or **Maximum protection**).
- Manually change the security settings for the selected nodes in the tree or in the list of the computer's file resources (the security level changes to **Custom**).

A set of node settings can be saved in a template in order to be applied later to other nodes.

Selecting predefined security levels

One of the following predefined security levels for the nodes selected either in the computer file resources tree or file resources list can be applied: **Maximum performance**, **Recommended**, and **Maximum protection**. Each of these levels contains its own predefined set of security settings (see the table below).

Maximum performance.

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

Recommended;

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

Maximum protection

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

Table 16. Preset security levels and corresponding setting values

Options	Security level		
	Maximum performance.	Recommended;	Maximum protection
Objects protection	By extension	By format	By format
Optimization	Enabled	Enabled	Disabled
Action to be performed with infected and other detected objects	Disinfect, delete if disinfection is impossible	Disinfect, delete if disinfection is impossible	Disinfect, delete if disinfection is impossible
Action to be performed on infected objects	Quarantine	Quarantine	Quarantine
Exclude objects	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
Boot sectors of drives and MBR	Yes	Yes	Yes
Compound objects protection	<ul style="list-style-type: none"> • Packed objects* • New and modified objects only 	<ul style="list-style-type: none"> • SFX archives* • Packed objects* • Embedded OLE-objects* • New and modified objects only 	<ul style="list-style-type: none"> • SFX archives* • Packed objects* • Embedded OLE-objects* <p>*All objects</p>

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. In the Kaspersky Embedded Systems Security Console tree, expand the **Real-Time Protection** node.
2. Select the **Real-Time File Protection** subnode.
3. In the details pane of the **Real-Time File Protection** node click the **Configure protection scope** link.

The **Protection scope settings** window opens.

4. Select the node to set the predefined security level.
5. Make sure that this node is included in the protection scope.
6. In the **Security level** tab select the security level to be applied in the list.

The window displays the list of security values for settings which correspond to the security level selected.

7. In the context menu of the task name, select **Save task**.

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

Configuring security settings manually

By default, the Real-Time File Protection task uses common security settings for the entire protection scope. Their values correspond to those of the **Recommended** predefined security level (see section "**Selecting predefined security levels**" on page [108](#)).

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.

On working with the computer file resources tree, security settings configured for the selected parental node are automatically applied to all subnodes when working with the network file resources tree. The security settings of the parent node are not applied to subnodes that are configured separately.

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

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Real-Time Protection** node.
2. Select the **Real-Time File Protection** subnode.
3. In the details pane of the **Real-Time File Protection** node click the **Configure protection scope** link.

The **Protection scope settings** window opens.

4. In the left window section select the node to configure security settings.

A predefined template containing security settings can be applied for a selected protection scope (see section "About templates of security settings" on page [79](#)).

5. Configure the required security settings of the selected node in accordance with your requirements. To do this, perform the following actions:

- On the **General** tab, configure the following settings, if necessary:

In the **Objects protection** section, specify the objects that you want to include in the protection scope:

- **All objects**

Kaspersky Embedded Systems Security scans all objects:

- **Objects scanned by format**

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

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

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

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

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

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

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

- **Boot sectors of drives and MBR**

Enables protection of boot sectors and master boot records.

If the check box is selected, Kaspersky Embedded Systems Security scans boot sectors and master boot records on hard drives and removable drives of the computer.

The check box is selected by default.

- **Alternative NTFS streams**

Scanning of alternative file and folder threads on the NTFS file system drives.

If the check box is selected, Kaspersky Embedded Systems Security scans additional file and folder threads.

The check box is selected by default.

In the **Performance** section, select or clear the check box:

- **Scan only new and modified files**

This check box enables / disables scanning and protection of files that have been recognized by Kaspersky Embedded Systems Security as new or modified since the last scan.

If the check box is selected, Kaspersky Embedded Systems Security scans and protects only the files that it has recognized as new or modified since the last scan.

If the check box is cleared, Kaspersky Embedded Systems Security scans and protects all files.

By default, the check box is selected for the **Maximum performance** security level. If the **Recommended** or **Maximum protection** security level is set, the check box is cleared.

In the **Compound objects protection** section, specify the compound objects that you want to include in the protection scope:

- **All / Only new archives**

Scanning of ZIP, CAB, RAR, ARJ archives and other archive formats.

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

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

The default value depends on the selected security level.

- **All / Only new SFX archives**

Scanning of archives that contain an extraction module.

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

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

The default value depends on the selected security level.

This option is active when the **Archives** check box is cleared.

- **All / Only new mail databases**

Scanning of Microsoft Outlook and Microsoft Outlook® Express mail database files.

If this check box is selected, Kaspersky Embedded Systems Security scans mail database files.

If this check box is cleared, Kaspersky Embedded Systems Security skips mail database files during scanning.

The default value depends on the selected security level.

- **All / Only new packed objects**

Scanning of executable files packed by binary code packers, such as UPX or ASPack.

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

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

The default value depends on the selected 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 scans files of mail formats.

If this check box is cleared, Kaspersky Embedded Systems Security skips files of mail formats during scanning.

The default value depends on the selected security level.

- **All / Only new embedded OLE objects**

Scanning of objects embedded into files (such as Microsoft Word macros, or email message attachments).

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

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

The default value depends on the selected security level.

You can choose to protect all or only new compound objects if the **Protect only new and modified files** check box is selected. If the **Protect only new and modified files** check box is cleared, Kaspersky Embedded Systems Security protects all of the specified compound objects.

- On the **Actions** tab, configure the following settings, if necessary:
 - Select the action to be performed on infected and other detected objects.
 - Select the action to be performed on probably infected objects.
 - Configure actions to be performed on objects depending on the type of object detected.
 - Select the actions to perform on immutable containers: select or clear the **Enforce entire parent container deletion in case of infected embedded or other object detection if the container modification is not possible** check box.

This check box enables or disables forced deletion of the parent file container when a malicious child or other object is detected.

If the check box is selected and the action selected to perform on infected and probably infected objects is **Delete**, Kaspersky Embedded Systems Security forcibly deletes the entire parent container when a malicious child or other object is detected. Forceful deletion of a parent container along with all of its contents happens if the application cannot delete only the detected child object (for example, if the parent container is immutable).

If this check box is cleared and the action selected to perform on infected and probably infected objects is **Delete**, Kaspersky Embedded Systems Security does not perform the selected action for the parent container when a malicious child or other object is detected if the parent container is immutable.

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

- On the **Performance** tab, configure the following settings, if necessary:

In the **Exclusions** section:

- **Exclude files**

Excluding files from scanning by file name or file name mask.

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

If this check box is cleared, Kaspersky Embedded Systems Security scans all objects.

The check box is cleared by default.

- **Do not 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 (<http://www.securelist.com>).

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

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

The check box is cleared by default.

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.

The default value is 8 MB.

If the check box is selected, Kaspersky Embedded Systems Security skips compound objects whose size exceeds the specified limit during virus scan.

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

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

- **Use iChecker technology**

Scanning of only new files and those modified since the last scan.

If the check box is selected, Kaspersky Embedded Systems Security scans only new files or those modified since the last scan.

If the check box is cleared, Kaspersky Embedded Systems Security scans files without regard for the date of file creation or modification.

The check box is selected by default.

- **Use iSwift technology**

Scanning of only new files and those modified since the last scan of NTFS system objects.

If the check box is selected, Kaspersky Embedded Systems Security scans only new files or those modified since the last scan of NTFS system objects.

If the check box is cleared, Kaspersky Embedded Systems Security scans NTFS system files without regard for the date of file creation or modification.

The check box is selected by default.

6. Click **OK**.

Your newly configured settings have been saved.

KSN Usage

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

In this section

About KSN Usage task	118
Starting and stopping KSN Usage task	119
Configuring KSN Usage task.....	121
KSN Usage task statistics	125

About KSN Usage task

Kaspersky Security Network (KSN) is an infrastructure of online services providing access to Kaspersky Lab's operative knowledge base on the reputation of files, web resources and programs. Kaspersky Security Network allows Kaspersky Embedded Systems Security to react very promptly to new threats, improves the performance of several protection components, and reduces the likelihood of false positives.

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

If you accepted the KSN Statement when the application is installed, the KSN Usage task will be started automatically when Kaspersky Embedded Systems Security is started. You can also run the task manually (see section "Starting and stopping the KSN Usage task" on page [119](#)) or schedule its launch (see section "Configuring the KSN Usage task" on page [121](#)).

Information received by Kaspersky Embedded Systems Security from Kaspersky Security Network pertains only to the reputation of programs.

Participation in KSN allows Kaspersky Lab to receive real-time information about types and sources of new threats, develop ways to neutralize them, and reduce the number of false positives in application components.

Personal data is not collected, processed, or stored. More detailed information about the collection, processing, storage, and destruction of information about application usage is available in the KSN Statement on the **KSN Statement** tab in the properties window of the KSN Usage task, and on Kaspersky Lab's website <http://www.kaspersky.com/privacy>.

Participation in Kaspersky Security Network is voluntary. The decision regarding participation in Kaspersky Security Network is made during or after installation of Kaspersky Embedded Systems Security. You can change your decision regarding participation in Kaspersky Security Network at any time (see section "Starting and stopping KSN Usage task" on page [119](#)).

Kaspersky Security Network can be used in the following Kaspersky Embedded Systems Security tasks:

- Real-Time File Protection (see section "Configuring the Real-Time File Protection task settings" on page [88](#)).
- On-Demand Scan (see section "Configuring the On-Demand Scan task settings" on page [224](#)).
- Applications Launch Control (see section "Configuring Applications Launch Control task settings" on page [138](#)).

Starting and stopping KSN Usage task

If you accepted the KSN Statement when the application is installed, the KSN Usage task will be started automatically when Kaspersky Embedded Systems Security is started.

You can also start the task manually.

► *To start the KSN Usage task:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Real-Time Protection** node.
2. Select the **KSN Usage** subnode.
3. Click the **Properties** link in the details pane.

The **Task settings** window opens on the **General** tab.

4. Select the **KSN Statement** tab.
5. Select the **I accept KSN Statement** check box if you agree with the terms and conditions of the Kaspersky Security Network Statement and want to enable KSN.

If you clear the **I accept KSN Statement** check box when running the KSN Usage task, the latter will be stopped.

6. Select the **Send event-triggered statistics** check box if you want to allow the application to send additional statistics to KSN.

The check box enables and disables the delivery of additional statistics to KSN. If the check box is selected, then the application sends information about malware, including fraudulent software, detected during execution of the Real-Time and On-Demand tasks, as well as debugging information about errors during scanning. If the check box is cleared, then the application sends only the checksums of the scanned files in order to receive verdicts from the KSN service, as well as general information about the application and operating system.

The check box is selected by default.

The application sends the statistics if all of the following conditions are satisfied:

- 1) KSN Usage task has been started.
- 2) The KSN Statement has been accepted.
- 3) In the Real-Time File Protection task properties, the **Use KSN for protection** check box is selected; in the On-Demand Scan task properties the **Use KSN for scanning** check box is selected.

7. Click **OK**.

The modified settings are saved.

8. In the **Management** section of the details pane of the **KSN Usage** node, click the **Start** link.

The KSN Usage task starts.

The KSN Usage task cannot be started if you do not accept the KSN Statement.
Before starting the task, make sure that the **I accept KSN Statement** check box is selected.

► *To stop the KSN Usage task:*

1. In the Console tree, expand the **Real-Time Protection** node.
2. Select the **KSN Usage** subnode.
3. In the **Management** section of the details pane of the **KSN Usage** node, click the **Stop** link.

The KSN Usage task is stopped.

Configuring KSN Usage task

The KSN Usage task has the following default settings described in the table below.

You can change the values of these settings.

Table 17. Default KSN Usage task settings

Setting	Default Value	Description
Actions to perform on KSN untrusted objects	Delete	You can specify actions that Kaspersky Embedded Systems Security will take on objects identified by KSN as infected.
Data transmission	The file checksum (MD5 hash) is calculated for files that do not exceed 2 MB in size.	You can specify the maximum size of files for which a checksum is calculated using the MD5 algorithm for delivery to KSN. If the check box is cleared, Kaspersky Embedded Systems Security calculates the MD5 hash for files of any size.
	The Send event-triggered statistics check box is selected.	You can allow or prohibit the application to send additional statistics about Kaspersky Embedded Systems Security functioning to KSN.
KSN Statement	The I accept KSN Statement check box is cleared or selected.	You can accept the KSN Statement during installation of the application. You can change your decision about whether to use KSN at any moment.
Task start schedule	First run is not scheduled.	The KSN Usage task starts automatically when Kaspersky Embedded Systems Security starts, if the KSN Statement was accepted during installation of the application. You can also start the task manually or configure a scheduled start.

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

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Real-Time Protection** node.
2. Select the **KSN Usage** subnode.
3. Click the **Properties** link in the details pane.

The **Task settings** window opens on the **General** tab.

4. Configure the task:
 - In the **Action to perform on KSN untrusted objects** section, specify the action that Kaspersky Embedded Systems Security is to perform if it detects an object identified by KSN as infected:
 - **Remove**

Kaspersky Embedded Systems Security deletes the object with KSN infected status and places a copy of it in Backup.

This option is selected by default.
 - **Log information**

Kaspersky Embedded Systems Security records information about the object with KSN infected status in the task log. Kaspersky Embedded Systems Security does not delete the infected object.
 - In the **Data transfer** section, restrict the size of files for which the checksum is calculated:
 - a. Clear or select the **Do not calculate checksum for sending to KSN if the file size exceeds (MB)** check box.

This check box enables or disables calculation of the checksum for files of the specified size for delivery of this information to the KSN service.

The duration of the checksum calculation depends on the file size.

If this check box is selected, Kaspersky Embedded Systems Security does not calculate the checksum for files that exceed the specified size (in MB).

If the check box is cleared, Kaspersky Embedded Systems Security calculates the checksum for files of any size.

The check box is selected by default.

- b. If required, in the field to the right, specify the maximum size of files for which Kaspersky Embedded Systems Security calculates the checksum.
- c. Clear or select the **Send event-triggered statistics** check box if you want to allow the application to send additional statistics to KSN.

The check box enables and disables the delivery of additional statistics to KSN. If the check box is selected, then the application sends information about malware, including fraudulent software, detected during execution of the Real-Time and On-Demand tasks, as well as debugging information about errors during scanning. If the check box is cleared, then the application sends only the checksums of the scanned files in order to receive verdicts from the KSN service, as well as general information about the application and operating system.

The check box is selected by default.

5. If required, configure a task launch schedule on the **Schedule** and **Advanced** tabs. For example, you can enable task launch by schedule and specify the launch frequency of the **At application launch** task if you want the task to run automatically when the computer is restarted.

The application will automatically start the KSN Usage task by schedule.

The KSN Usage task cannot be started if you do not accept the KSN Statement. Before starting the task, make sure that the **I accept KSN Statement** check box is selected on the **KSN Statement** tab.

6. 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.

KSN Usage task statistics

While the KSN Usage task is being executed, detailed information can be viewed in real time about the number of objects processed by Kaspersky Embedded Systems Security since it was started up till now. Information about all events that occur during the task performing is recorded in the task log (see section "About task logs" on page [313](#)).

► *To view KSN Usage task statistics take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Real-Time Protection** node.
2. Select the **KSN Usage** subnode.

Task statistics are displayed in the **Statistics** section of the details pane of the selected node.

You can view information about objects processed by Kaspersky Embedded Systems Security since the task was started (see the table below).

Table 18. KSN Usage task statistics

Field	Description
File requests sent	Number of file reputation queries sent by Kaspersky Embedded Systems Security to KSN.
Untrusted conclusions received	Number of objects classed as untrusted by KSN.
Request sending errors	Number of KSN requests whose processing resulted in a task error.
Objects removed	Number of objects that Kaspersky Embedded Systems Security deleted when running the KSN Usage task.
Moved to Backup	The number of object copies that Kaspersky Embedded Systems Security saved to Backup.
Objects not removed	The number of objects that Kaspersky Embedded Systems Security attempted but was unable to delete, because, for example, access to the object was blocked by another application. Information about such objects is recorded in the task log.
Objects not backed up	The number of objects the copies of which Kaspersky Embedded Systems Security attempted to save in Backup but was unable to do so, for example, due to insufficient disk space. The application does not disinfect or delete files that it could not move to Backup. Information about such objects is recorded in the task log.

Exploit prevention

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

In this section

About Exploit prevention	127
Configuring process memory protection settings	129
Adding a process for protection.....	132
Impact reduction techniques	134

About Exploit prevention

Kaspersky Embedded Systems Security provides the ability to protect process memory from exploits. This feature is implemented in the Process Memory Protection component.

You can change the component's activity status and configure process memory protection settings.

The component protects process memory from exploits by inserting an external Process Protection Agent ("Agent") in the protected process.

A Process Protection Agent is a dynamically loaded Kaspersky Embedded Systems Security module that is inserted in protected processes to monitor their integrity and reduce the risk of being exploited.

The Agent's operation within the protected process requires starting and stopping the process: the initial loading of the Agent into a process added to the protected process list is only possible if the process is restarted. Additionally, after a process has been removed from the protected process list, the Agent can be unloaded only after the process has been restarted.

The Agent must be stopped to unload it from protected processes: if the Exploit prevention component is uninstalled, the application freezes the environment and forces the Agent to be unloaded from protected processes. A restart of the protected computer may be required to uninstall the component if there are protected processes on the system.

If evidence of an exploit attack in a protected process is detected, Kaspersky Embedded Systems Security performs one of the following actions:

- it terminates the process if an exploit attempt is made;
- it 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.

During uninstallation, if the Agent has been inserted into one or more protected processes, the protected computer must be restarted.

Kaspersky Security Broker Host Service

Kaspersky Security Broker Host Service is required on the protected computer in order for the Exploit prevention component to be most effective. This service and the exploit protection component are part of the recommended installation. During installation of the service on the protected computer, the kavfsw process is created and started. This communicates information about protected processes from the component to the Security Agent.

After the Kaspersky Security Broker Host Service is stopped, Kaspersky Embedded Systems Security continues to protect processes added to the protected process list, is also loaded in newly-added processes, and applies all available impact reduction techniques to protect process memory.

If the Kaspersky Security Broker Host 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 protection mode

You can select one of the following modes to configure actions to reduce risks that vulnerabilities will be exploited in protected processes:

- Terminate on exploit: apply this mode to terminate a process when an exploit attempt is made.

Upon detecting an attempt to exploit a vulnerability in a protected critical operating system process, Kaspersky Embedded Systems Security does not terminate the process, regardless of the mode indicated in the exploit protection component settings.

- Only inform about abused processes: 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 logs all attempts to exploit vulnerabilities by creating events.

Configuring process memory protection settings

► To add a process to the list of protected processes:

1. Select the **Kaspersky Embedded Systems Security** main node in the console tree.
2. In the node results pane click the **Only inform about** link in the **Protection** section.

The **Exploit prevention settings** window opens.

3. Configure the process memory protection settings:

- **Protect processes memory from exploitation of vulnerabilities in the mode.**

If this check box is selected, Kaspersky Embedded Systems Security reduces the risks that vulnerabilities will be exploited in processes for the list of protected processes.

If this check box is cleared, Kaspersky Embedded Systems Security does not protect computer processes from exploits.

The check box is cleared by default.

- **Terminate compromised processes.**

If this mode is selected, Kaspersky Embedded Systems Security terminates a protected process upon detecting an exploit attempt if an active impact reduction technique has been applied to the process.

- **Only inform about abused processes.**

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

If Kaspersky Embedded Systems Security detects an exploit in a critical process while the application is running in *Terminate on exploit* mode, the component forcibly switches to *Only inform about abused processes* mode.

4. In the **Actions to reduce impact** section, configure the following settings:

- **Inform about abused processes via Terminal Service**

If this check box is selected, Kaspersky Embedded Systems Security displays a terminal window with a description explaining why protection was activated and an indication of the process in which an exploit attempt was detected.

If the check box is cleared, Kaspersky Embedded Systems Security displays a terminal window when an exploit attempt or termination of a compromised process is detected.

A terminal window is displayed regardless of the status of the Kaspersky Security Broker Host Service.

The check box is selected by default.

- **Reduce impact of exploits even if Kaspersky Security Service is disabled.**

If this check box is selected, Kaspersky Embedded Systems Security will reduce risk of vulnerabilities being exploited in processes that have already been started, regardless of whether the Kaspersky Security service is running. Kaspersky Embedded Systems Security will not protect processes added after the Kaspersky Security service is stopped. After the service is started, exploit impact reduction will be stopped for all processes.

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

The check box is selected by default.

5. In the **Exploit prevention settings** window click **OK**.

Kaspersky Embedded Systems Security saves and applies the configured process protection settings.

Adding a process for protection

► To add a process to the list of protected processes:

1. Select the **Kaspersky Embedded Systems Security** main node in the console tree.
2. In the node results pane click the **Exploit prevention** link in the **Protection** section.

The **Protection scope** window opens.

3. To add a process to the list of protected processes perform the following actions:
 - a. Click the **Browse** button.

The standard Microsoft Windows **Open** window opens.

- b. In the window that opens select a process you want to add to the list.
- c. Click the **Open** button.
- d. Click the **Add** button.

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

4. Select a process in the list.
5. On the **Process memory protection settings** a current configuration displays:

- **Status**
- **Path to executable file**
- **Impact reduction techniques**

6. To modify the impact reduction techniques that are applied to the process, select the **Impact reduction techniques** tab.

7. Select one of the impact reduction techniques usage modes:

- **Apply all available impact reduction techniques.**

If this option is selected, you cannot edit the list, all techniques are applied by default.

- **Apply listed impact reduction techniques for the process.**

If this option is selected, you can edit the list of applied impact reduction techniques by selecting the corresponding check boxes.

8. In the **Modules launched from the process** section you can configure the **Attack Surface Reduction** technique:

- Add the names of modules, whose launch from the protected process is blocked in the **Disallow modules** field.
- In the **Do not prohibit modules if launched in the Internet Zone** field select the area options, where you want to allow launching modules.
 - Internet
 - Intranet
 - Trusted sites
 - Limited access sites
 - Computer

These options are available for Internet Explorer only.

9. Click **OK**.

Impact reduction techniques

Table 19. Impact reduction techniques

Impact reduction techniques	Description
Data Execution Prevention (DEP)	Data execution prevention blocks execution of arbitrary code in protected areas of memory.
Address Space Layout Randomization (ASLR)	Changes to the layout of data structures in the address space of the process.
Structured Exception Handler Overwrite Protection (SEHOP)	Replacement of exception records or replacement of the exception handler.
Null Page Allocation	Prevention of redirecting the null pointer.
LoadLibrary Network Call Check (Anti ROP)	Protection against loading DLLs from network paths.
Executable Stack (Anti ROP)	Blocking of unauthorized execution of areas of the stack.
Anti RET Check (Anti ROP)	Check that the CALL instruction is invoked safely.
Anti Stack Pivoting (Anti ROP)	Protection against relocation of the ESP stack pointer to an executable address.
Export Address Table Access Moitor (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
Heapspray Allocation	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.

Impact reduction techniques	Description
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	Blocking the start of vulnerable add-ins via the protected process.

Computer control

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

In this section

Applications Launch Control.....	136
Device Control	174
Firewall Management.....	194

Application Launch Control

This section contains information about the Applications Launch Control task and how to configure it.

In this section

About Applications Launch Control task.....	137
Configuring Applications Launch Control task settings	138
About Applications Launch Control rules.....	152
About Applications Launch Control rules list filling.....	157
About Rule Generator for Applications Launch Control task.....	164

About Applications Launch Control task

During the ongoing Applications Launch Control task, Kaspersky Embedded Systems Security monitors application starts attempted by users and allows or denies starting. Applications Launch Control task is based on the Default Deny technology, which implies automatic start block for any applications that are not allowed in the task settings.

You can allow application start using one of the following methods:

- set allowing rules for trusted applications;
- consider the trusted applications reputation in KSN on launch.

Application start block has a full priority: if application start is blocked by one of the Applications Launch Control task components, the application start will be denied regardless of the conclusions of other task components. For example, if the application considered untrusted by the KSN services, but included into the allowing rule scope, this application launch will be denied.

All attempts to start applications are recorded in the task log (see section "About task logs" on page [313](#)).

The Applications Launch Control task can operate in one out of two modes:

- **Apply Rules.** Kaspersky Embedded Systems Security uses a set of rules to control the start of programs that fall under the scope of the applications launch control task rules. The scope of the Applications Launch Control task rules is specified in the settings of this task. If an application falls under the rule usage scope of the Applications Launch Control task, and its settings do not satisfy any rule specified, such application launch will be denied.

The launches of the applications that do not fall under the usage scope of any rule specified in the Applications Launch Control task settings is allowed, regardless of the Applications Launch Control task settings.

The Applications Launch Control task cannot be started in **Apply Rules** mode if not a single rule has been created or if the number of rules for one computer exceeds the threshold of 65,535 rules.

- **Statistics Only.** Kaspersky Embedded Systems Security does not use Applications Launch Control rules to allow or deny application start, but only records information about application start, about the rules that satisfy running applications and actions that would have been performed if the task run in Apply Rules mode. Start of all programs is allowed. This mode is set by default.

You can apply this mode to create the applications launch control rules basing on information fixed in the task log (see section «Filling the rules list basing on the Applications Launch Control task events» on page [162](#)).

You can configure the Application Launch Control task operation according to one of the following scenarios:

- Advanced rules configuration and their usage for application launch control.
- Basic rules configuration and KSN usage for application launch control (see section "KSN usage for Applications Launch Control task" on page [144](#)).

If the operating system files fall under the scope of the Applications Launch Control task, we recommend that you make sure that running such applications is allowed by the newly created rules, when creating Applications Launch Control rules. Otherwise, the operating system may fail to start.

Configuring Applications Launch Control task settings

By default, the Applications Launch Control task has the settings described in the table below. You can change the values of these settings.

Table 20. Applications Launch Control task settings by default

Setting	Default Value	Description
Task operating mode	Statistics Only. The task logs application blocking and startup events based on the set rules. Application start blocking is not actually executed.	You can select Apply Rules mode for computer protection after the final list of rules is generated.
Rules usage scope in the task	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 KSN are not used.	You can use KSN application reputation conclusions when running the Applications Launch Control task.

Setting	Default Value	Description
Allowing distribution of applications for the specified distribution packages	Not applied.	You can allow automatic software installation or update via the specified distribution packages.
Allowing software distribution via Windows Installer	Applied.	You can allow any software installation or update, if the operations are performed via Windows Installer.
Task start schedule	First run is not scheduled.	The Applications Launch Control task does not start automatically at startup of Kaspersky Embedded Systems Security. You can start the task manually or configure a scheduled start.

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

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Computer Control** node.
2. Select the **Applications Launch Control** subnode.
3. Click the **Properties** link in the details pane of the **Applications Launch Control** node.

The **Task settings** window opens.

4. Configure the following task settings:

- On the **General** tab:
 - Operating mode of the Applications Launch Control task (see section "Selecting the operating mode of the Applications Launch Control task" on page [141](#)).

- Rules usage scope in the task (see section "Generating the scope of the Applications Launch Control task" on page [143](#)).
 - KSN Usage (see section "KSN Usage for Application Launch Control task" on page [144](#)).
 - On the **Software Distribution Control** tab:
 - Software Distribution Control settings (see section "Software Distribution Control" on page [148](#)).
 - On the **Schedule** and **Advanced** tabs:
 - Scheduled task launch settings (see section "Configuring the task launch schedule settings" on page [70](#)).
5. Click **OK** in the **Task settings** window.

The modified settings are saved.

6. In the lower part of the details pane of the **Applications Launch Control** node, click the **Applications Launch Control rules** link.
7. If required, edit the list of Applications Launch Control rules.

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

Selecting operating mode of Applications Launch Control task

► *To configure the operating mode of the Applications Launch Control task:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Computer Control** node.
2. Select the **Applications Launch Control** subnode.
3. Click the **Properties** link in the details pane of the **Applications Launch Control** node.

The **Task settings** window opens on the **General** tab.

4. In the **Applications Launch Control task mode** list, specify the task execution mode.

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

- **Apply Rules.** Kaspersky Embedded Systems Security uses the specified rules to monitor any applications being run.
- **Statistics Only.** Kaspersky Embedded Systems Security 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 **Statistics Only** mode.

5. Clear or select the **Handle second launches of controlled applications using the same procedure as for the first launch.**

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 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 analyses an application on its every launch attempt.

The check box is selected by default.

Kaspersky Embedded Systems Security creates a new list of cached incidents for every alteration of the Application Launch Control task settings. Thus, application launch is controlled according to the actual security settings.

6. Click **OK**.

The specified settings are saved.

All attempts to start programs are recorded in the task log.

Generating scope of Applications Launch Control task

► To generate the scope of the Applications Launch Control task take the following steps:

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Computer Control** node.
2. Select the **Applications Launch Control** subnode.
3. Click the **Properties** link in the details pane of the **Applications Launch Control** node.

The **Task settings** window opens on the **General** tab.

4. 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 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 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 DLL modules loading**

The check box enables / disables monitoring of DLL modules loading

If this check box is selected, Kaspersky Embedded Systems Security 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 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 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 does not control launch of scripts and MSI packages using specified rules. Startup of scripts and MSI packages is allowed.

The check box is selected by default.

5. Click **OK**.

The specified settings are saved.

KSN usage for Applications Launch Control task

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

If you accepted the KSN Statement when the application is installed, the KSN Usage task will be started automatically when Kaspersky Embedded Systems Security is started. You can also run the task manually (see section "Starting and stopping the KSN Usage task" on page [119](#)) or schedule its launch (see section "Configuring the KSN Usage task" on page [121](#)).

If the stored in KSN data about the applications reputation is used by Application Launch Control task, the application reputation in KSN is considered a criterion for allowing or denying that application launch. If Kaspersky Embedded Systems Security receives an untrusted conclusion from KSN when attempting to launch an application, the application launch is denied. If Kaspersky Embedded Systems Security receives a trusted conclusion from KSN when attempting to launch an application, the application launch is allowed. KSN can be used along with the application launch control rules or as an independent criterion for application launch block.

Using KSN conclusions as independent criterion for denying application launch

This scenario allows to securely control applications launches on the protected computer without the necessity for advanced configuration of the rule list.

You can apply KSN conclusions to Kaspersky Embedded Systems Security together with the only specified rule. The application will only allow the applications to start that are trusted in KSN or are allowed by a specified rule.

For such a scenario, it is recommended to set a rule allowing application start based on a digital certificate.

All the other applications are denied in accordance with the Default Deny policy. Using KSN when no rules are applied protects a computer from applications that KSN considers to be a threat.

Using KSN conclusions simultaneously with application launch control rules

When using KSN conclusions simultaneously with application launch control rules the following scenarios are applied:

- Kaspersky Embedded Systems Security always denies application launch, if this application is included in at least one denying rule scope. If the application considered trusted by KSN, this conclusion has a lower priority and is not considered; the application launch will still be denied. This allows you to extend the list of unwanted applications.
- Kaspersky Embedded Systems Security always blocks the launch of applications if application launch is prohibited for applications not trusted in KSN and the application is not trusted in KSN. If an allowing rule is set for this application, it has a lower priority and is not considered; the application launch will still be denied. This protects the computer from applications that KSN considers to be a threat but were not considered during the initial configuration of rules.

► *To configure the KSN Usage services in the Applications Launch Control task:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Computer Control** node.
2. Select the **Applications Launch Control** subnode.
3. Click the **Properties** link in the details pane of the **Applications Launch Control** node.

The **Task settings** window opens on the **General** tab.

4. In the **KSN Usage** section, specify the settings for KSN services usage:
 - If necessary, select the **Block start of applications not trusted in KSN** check box.

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 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

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.

- If necessary, select the **Allow start of applications trusted in KSN** check box.

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 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 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.

- If the **Allow start of applications trusted in KSN** check box is selected, indicate the users and/or groups of users allowed to start applications trusted in KSN. To do this, perform the following actions:
 - a. Click the **Edit** button.
The standard Microsoft Windows **Select users or groups** window opens.
 - b. Specify the list of users and/or user groups.
 - c. Click **OK**.

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

The specified settings are saved.

Software Distribution Control

Software installation and updates may be simplified by using Software Distribution Control. Software Distribution Control allows automatic start of applications, if they are started by the trusted application or trusted distribution package. After the trusted distribution package is started, Kaspersky Embedded Systems Security automatically calculates a checksum for each child file and thereafter does not apply Default Deny policies to such files. Kaspersky Embedded Systems Security allows the trusted distribution package to be decompressed and all child files to start, unless these objects are blocked by the Device Control task rules or listed as untrusted in KSN.

The editing or moving of a child file may prevent the file from starting.

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

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Computer Control** node.
2. Select the **Applications Launch Control** subnode.
3. Click the **Properties** link in the details pane of the **Applications Launch Control** node.

The **Task settings** window opens.

4. On the selected tab, select the **Automatically allow software distribution for 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 packages listed**, if the **Apply rules to executable files** check box is selected in the Application 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 distribution package child files 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 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.

1. To edit the list of trusted distribution packages, click the **Change package list** button and in the menu that opens select one of the available options:

- **Add one manually.**

- a. Click the **Browse** button and select the startup file or distribution package.

The **Trust Criteria** section is automatically populated with data about the selected file.

- b. Select one of the two available criteria used 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.

This option is selected by default.

- **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 variant 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.

- **Add several using a hash.**

You can select an unlimited number of startup files and distribution packages and add them to the list all at the same time. Kaspersky Embedded Systems Security examines the hash and allows the operating system to launch the specified files.

- **Edit selected.**

Use this option to choose a different startup file or distribution package, or to change the trust criteria.

- **Import from a text file.**

You can import the list of trusted distribution packages from the configuration file. The file recognized by Kaspersky Embedded Systems Security 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 the list of trusted distribution packages.

2. If you want to remove a previously added application or distribution package, click the **Remove distribution package** button. Child files will be allowed to run.

To prevent child files from starting, uninstall the application on the protected computer or create a denying rule in the Application Launch Control task settings.

3. Click **OK**.

Your newly configured settings have been saved.

About Applications Launch Control rules

Work principles of applications launch control rules

The operation of Applications Launch Control rules is based on the following components:

- Type of rule.

Applications Launch Control rules can allow or deny application start, and are named *allowing* or *denying* rules, accordingly. To create a list of allowing rules for Applications Launch Control, you can use the task for generating allowing rules (see section "About Rule Generator for Applications Launch Control task" on page [164](#)). Or the **Statistics Only** mode in the Applications Launch Control task (see section "Generating the rules list based on Device Control task events" on page [162](#)) You can also add allowing rules manually (see section "Adding one Applications Launch Control rule" on page [158](#)) by ones.

- User and / or user group.

Applications Launch Control rules control the start of programs specified in the rule by a user and / or user group.

- Rule usage scope.

Applications Launch Control rules can be applied to start of *program executable files* or *scripts* and *MSI packages*.

- Rule triggering criterion.

Applications Launch Control rules control the launch of files that satisfy one of the criteria specified in the rule settings: signed by the specified *digital certificate*, match the specified *SHA256 hash*, or are located at the specified *path*.

If **Digital certificate** is set as the rule triggering criterion, the created rule controls the start of all programs trusted in the operating system. You can set stricter conditions for this criterion by selecting the check boxes:

- **Use subject**

The check box enables / disables the use of the subject of the digital certificate as a rule-triggering criterion.

If the check box is selected, the specified subject of the digital certificate is used as a rule-triggering criterion. The created rule will control the start of applications only for the supplier specified in the subject.

If the check box is cleared, the application will not use the subject of the digital certificate as the rule triggering criterion. If the **Digital certificate** criterion is selected, the created rule will control the start of applications signed with a digital certificate containing any subject.

The subject of the digital certificate with which the file is signed can be specified only from the properties of the selected file using the **Set rule triggering criterion from file properties** button located above the **Rule triggering criterion** section.

The check box is cleared by default.

- **Use thumb**

The check box enables / disables the use of the thumb of the digital certificate as a rule-triggering criterion.

If the check box is selected, the specified thumb of the digital certificate is used as a rule-triggering criterion. The created rule will control the start of applications signed with a digital certificate with the specified thumb.

If the check box is cleared, the application will not use the thumb of the digital certificate as the rule triggering criterion. If the **Digital certificate** criterion is selected, the application will control the start of applications signed with a digital certificate containing any thumb.

The thumb of the digital certificate with which the file is signed can be specified only from the properties of the selected file using

the **Set rule triggering criterion from file properties** button located above the **Rule triggering criterion** section.

The check box is cleared by default.

Use of a thumb most strictly restricts the triggering of application start rules based on a digital certificate because a thumb is a unique identifier of a digital certificate and cannot be forged, unlike the subject of a digital certificate.

You can specify exclusions for Applications Launch Control rules. Exclusions to Applications Launch Control rules are based on the same criteria that trigger the rules: digital certificate; SHA256 hash; file path. Exclusions to Applications Launch Control rules can be required to specify allowing rules: for example, if you want to allow users to start programs from the C:\Windows path, while blocking launch of the file Regedit.exe.

If the operating system files fall under the scope of the Applications Launch Control task, we recommend that you make sure that running such applications is allowed by the newly created rules, when creating Applications Launch Control rules. Otherwise, the operating system may fail to start.

Managing Applications Launch Control rules

You can perform the following actions with the Applications Launch Control rules:

- Add rules manually.
- Generate and add rules automatically.
- Remove rules.
- Export rules to file.
- Check selected files for rules, which allow execution of these files.
- Filter the rules in the list according to specified criterion.

Removing Applications Launch Control rules

► *To remove the Applications Launch Control rules, take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Computer Control** node.
2. Select the **Applications Launch Control** subnode.
3. In the lower part of the details pane of the **Applications Launch Control** node, click the **Applications Launch Control rules** link.

The **Applications Launch Control rules** window opens.

4. In the list, select one or several rules that you want to delete.
5. Click the **Remove selected** button.
6. Click the **Save** button.

The selected Applications Launch Control rules are deleted.

Exporting Applications Launch Control rules

► *To export the Applications Launch Control rules to a configuration file, take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Computer Control** node.
2. Select the **Applications Launch Control** subnode.
3. In the lower part of the details pane of the **Applications Launch Control** node, click the **Applications Launch Control rules** link.

The **Applications Launch Control rules** window opens.

4. Click the **Export to a file** button.

The standard Microsoft Windows window opens.

5. In the window that opens, specify the file to which you want to export the rules. If no such file exists, it will be created. If a file with the specified name already exists, its contents will be rewritten after the rules are exported.
6. Click the **Save** button.

The rule settings will be exported in the specified file.

Applications launches check

Before applying the configured Applications Launch Control rules, you can test any application for rules triggering to determine the rules that control launch of the selected application.

Kaspersky Embedded Systems Security denies applications whose launch is not controlled by a single rule by default. To avoid launch denying of important applications you need to create allowing rules for them.

If the application launch is controlled by several rules of different types, denying rules are given priority for such application: the application launch is to be denied if comes under one denying rule at least.

► *To test Applications Launch Control rules take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Computer Control** node.
2. Select the **Applications Launch Control** subnode.
3. In the lower part of the details pane of the **Applications Launch Control** node, click the **Applications Launch Control rules** link.

The **Applications Launch Control rules** window opens.

4. In the window that opens, click the **Show rules for the file** button.

The standard Microsoft Windows window opens.

5. Select the file whose start control you want to test.

The path to the specified file displays in the search field. The list contains all found rules that will be triggered at the start of the selected file.

About Applications Launch Control rules list filling

You can import lists of Applications Launch Control rules from XML files that are automatically generated during performing of the Applications Launch Control task or the Rule Generator for Applications Launch Control task. Lists contained in XML files can only be used to create Applications Launch Control allowing rules.

Applications Launch Control denying rules are created manually. An application launch is also denied, if there is no rule for the application.

The Rule Generator for Applications Launch Control task usage

The XML file generated upon completion of the Rule Generator for Applications Launch Control task contains the application start allowing rules that were specified when configuring the settings for the task when it is started. No rules will be created for applications that are not allowed to start in the specified task settings, and their start will be blocked by default.

You can configure automatic import of the generated rules into the list of rules for the Applications Launch Control task.

Statistics Only mode of the Applications Launch Control task usage

XML-file that is created upon the Applications Launch Control task completion in the **Statistics Only** mode and is based on the task log.

During the task running Kaspersky Embedded Systems Security registers information about all the applications launches on a protected computer in the task log. You can generate allowing rules based on task events and export them to an XML file. Before starting the task in the **Statistics Only** mode, you need to configure the task execution period so that all possible operating scenarios of the protected computer are executed and at least one restart of the computer occurs during the specified time interval.

XML files containing lists of allowing rules are created based on an analysis of tasks started on the protected computer. In order to account for all utilized applications on the network when generating lists of rules, you are advised to start up the Rule Generator for Applications Launch Control task and the Applications Launch Control task in the **Statistics Only** mode on a template machine.

Before starting the generation of the allowing rules basing on the applications launched on a template machine, make sure that the template machine is secure and there is no malware on it.

When configuring a policy in Kaspersky Security Center and applying allowing rules for the entire network, you can use lists of rules obtained based on an analysis of application launches on a reference machine.

In this section

Adding one Applications Launch Control rule	158
Filling the rules list basing on the Applications Launch Control task events.....	162
Importing the Applications Launch Control rules from a file	163

Adding one Applications Launch Control rule

► *To add an Applications Launch Control rule, take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Computer Control** node.
2. Select the **Applications Launch Control** subnode.
3. In the lower part of the details pane of the **Applications Launch Control** node, click the **Applications Launch Control rules** link.

The **Applications Launch Control rules** window opens.

4. Click the **Add** button.
5. In the context menu of the button, select **Add one rule**.

The **Rule settings** context window opens.

6. Define the following settings:
 - a. In the **Name** field, enter the name of the rule.
 - b. In the **Type** drop down list, select the rule type:
 - **Allowing** if you want the rule to allow launch of the applications in accordance with the criteria specified in the rule settings.
 - **Denying** if you want the rule to block launch of the applications in accordance with the criteria specified in the rule settings.
 - c. In the **Scope** drop down list, select the type of files whose execution will be controlled by the rule:
 - **Executable files** if you want the rule to control launch of applications executable files.
 - **Scripts and MSI packages** if you want the rule to control launch of scripts and MSI packages.
 - d. In the **User and/or user group** field, specify the users who will be allowed or not allowed to start programs based on the type of rule. To do this, perform the following actions:
 - i. Click the **Browse** button.
 - ii. The standard Microsoft Windows **Select user or groups** window opens.
 - iii. Specify the list of users and/or user groups.
 - iv. Click **OK**.

e. If you want to take the values of the rule-triggering criteria listed in the **Rule triggering criterion** section from a specific file:

i. Click the **Set rule triggering criterion from file properties** button.

The standard Microsoft Windows **Open** window opens.

ii. Select the file and click **OK**.

The values of criteria from the file are displayed in fields of the **Rule triggering criterion** section. The criterion for which data are available in the file properties is selected by default.

f. In the **Rule triggering criterion** section, select one of the following options:

- **Digital certificate** if you want the rule to control start of programs launched using files signed with a digital certificate:
 - Select the **Use subject** check box if you want the rule to control launch of files signed with a digital certificate only with the specified header.
 - Select the **Use thumb** check box if you want the rule to control launch of files signed with a digital certificate only with the specified thumb.
- **SHA256 hash** if you want the rule to control start of programs launched using files whose checksum matches the one specified.
- **Path to file** if you want the rule to control start of programs launched using files located at the specified path.

g. If you want to add rule exclusions:

i. In the **Exclusions from rule** section, click the **Add** button.

The **Exclusion from rule** window opens.

ii. In the **Name** field, enter the name of the rule exception.

iii. Specify the settings for exclusion of application run files from the Applications Launch Control rule. You can complete the settings fields from the file properties by clicking the **Set exclusion based on file properties** button.

- **Digital certificate**

If this criterion is selected, the application excludes from the rule programs launched using files signed by a digital certificate.

This criterion is the default option.

- **Use subject**

The check box enables or disables the use of the subject of the digital certificate as a criterion for excluding files from the rule.

If the check box is selected, the specified subject of the digital certificate is used as a criterion for excluding files from the rule. The application excludes from the rule files signed with a digital certificate only with this subject.

If the check box is cleared, the specified subject of the digital certificate is not used as a criterion for excluding files from the rule. If the **Digital certificate** criterion is selected, the application excludes from the rule files signed with a digital certificate with any subject.

The subject of the digital certificate with which the file is signed can be specified only from the properties of the selected file using the **Create exclusion based on file properties** button.

The check box is cleared by default.

- **Use thumb**

The check box enables or disables the use of the thumb of the digital certificate as a criterion for excluding files from the rule.

If the check box is selected, the specified thumb of the digital certificate is used as a criterion for excluding files from the rule. The application excludes from the rule files signed with a digital certificate only with this thumb.

If the check box is cleared, the specified thumb of the digital certificate is not used as a criterion for excluding files from the rule. If the **Digital certificate** criterion is selected, the application excludes from the rule files signed with a digital certificate with any thumb.

The thumb of the digital certificate with which the file is signed can be specified only from the properties of the selected file using the **Create exclusion based on file properties** button.

The check box is cleared by default.

- **SHA256 hash.**

If this criterion is selected, the application excludes from the rule programs launched using a file with the specified checksum.

The checksum can be specified only from the properties of the selected file using the **Create exclusion based on file properties** button.

- **Path to file.**

If this criterion is selected, the application excludes programs launched using files located at the specified path.

- i. Click **OK**.

- ii. If necessary, repeat items (i)-(iv) to add additional exclusions.

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

The created rule is displayed in the list in the **Applications Launch Control rules** window.

Filling rules list basing on Applications Launch Control task events

► *To create a configuration file that contains applications launches control rules and is generated basing on the Applications Launch Control task events, take the following steps:*

1. Start the Applications Launch Control task in the **Statistics Only** mode (see section "**Selecting the operating mode of the Applications Launch Control task**" on page [141](#)) to register the information about all the applications launches on a protected computer in the task log.
2. After the task in the **Statistics Only** mode is finished, open the task log by clicking the **Open task log** button in the **Management** section of the **Applications Launch Control** node detail pane.

3. In the **Logs** window click the **Generate rules based on events**.

Kaspersky Embedded Systems Security will generate an XML configuration file that will contain rules list based on events of the Applications Launch Control task in the **Statistics Only** mode. You can apply this rule list in the Applications Launch Control task (see section "Importing the Applications Launch Control rules from a file" on page [163](#)).

Before applying the rule list that is generated out of the task events logged, it is recommended to review and manually process the list to make certain that the critical files execution (for example, system files) is allowed by the rules specified.

All the task events are registered in the task log regardless of the task mode. You can generate a configuration file with the rule list basing on the log created for the task running in the **Apply Rules** mode. This scenario is not recommended except urgent cases, as far as the task efficiency requires to generate a final rule list version before the task is run under the mode of rule applying.

Importing Applications Launch Control rules from XML file

► *To import the Applications Launch Control rules, take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Computer Control** node.
2. Select the **Applications Launch Control** subnode.
3. In the details pane of the **Applications Launch Control** node, click the **Applications Launch Control rules** link.

The **Applications Launch Control rules** window opens.

4. Click the **Add** button.
5. In the context menu of the button, select **Import rules from file**.

6. Specify the method for adding the imported rules. To do so, select one of the options from the context menu of the **Import rules from file** button:
 - **Add to existing rules** if you want to add the imported rules to the list of existing ones. Rules with identical settings are duplicated.
 - **Replace existing rules** if you want to replace the existing rules with the imported ones.
 - **Merge with existing rules** if you want to add the imported rules to the list of existing ones. Rules with identical settings are not added; the rule is added if at least one rule parameter is unique.

The standard Microsoft Windows **Open** window opens.

7. In the **Open** window, select the XML file that contains the settings of the Applications Launch Control rules.
8. Click the **Open** button.

The imported rules will be displayed in the list of the **Applications Launch Control rules** window.

About Rule Generator for Applications Launch Control task

The Rule Generator for Applications Launch Control task can automatically create a list of allowing Applications Launch Control rules based on the specified file types from the specified folders. For example, if you specify executable files from the folder C:\Program Files (x86) as the task settings, the application automatically generates rules to allow launch of these files. The application will subsequently allow start of programs for which allowing rules were automatically generated.

The generated rules are displayed in the window via the **Applications Launch Control rules** link in the **Applications Launch Control** node.

Configuring Rule Generator for Application Launch Control task settings

By default, the Rule Generator for Application Launch Control task has the settings described in the table below. You can change the values of these settings.

Table 21. Rule Generator for Applications Launch Control task default settings default

Setting	Default Value	Description
Prefix for allowing rules names	Identical to the name of the computer on which Kaspersky Embedded Systems Security is installed.	You can change the prefix for names of allowing rules.
Allowing rules usage scope	<p>The scope of allowing rules includes the following file categories by default:</p> <ul style="list-style-type: none"> Files with the EXE extension located in the folders C:\Windows, C:\Program Files (x86) and C:\Program Files MSI packages stored in the C:\Windows folder Scripts stored in the C:\Windows folder <p>The task also creates rules for all running applications, regardless of their location and format.</p>	You can 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. Also, you can ignore running applications when creating allowing rules.
Criteria for generation of allowing rules	A digital certificate subject and thumb are used; rules are generated for all users and groups of users.	<p>You can use the SHA256 hash when generating allowing rules.</p> <p>You can select a user and group of users for which allowing rules need to be automatically generated.</p>

Setting	Default Value	Description
Actions upon task completion	Allowing rules are added to the list of the Applications Launch Control task rules; new rules are merged with existing ones; duplicated rules are removed.	You can add rules to existing ones without merging them and without deleting duplicated rules, or replace existing rules with new allowing rules, or configure export of allowing rules to a file.
Task launch settings with permissions	The task is started under a system account.	You can allow start of the Rule Generator for Applications Launch Control task through a system account or through the permissions of a specified user.
Task start schedule	First run is not scheduled.	The Rule Generator for Applications Launch Control task does not start automatically at the start of Kaspersky Embedded Systems Security. You can start the task manually or configure a scheduled start.

► *To configure the Rule Generator for Applications Launch Control task settings, take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Automated rule generators** node.
2. Select the **Rule Generator for Applications Launch Control** subnode.
3. In the details pane of the **Rule Generator for Applications Launch Control** subnode click the **Properties** link.

The **Task settings** window opens. Configure the following settings:

- On the **General** tab:

- Specify a prefix for rule names.

First part of a rule name. The second part of the name of the rule is formed from the name of the object for which start is allowed.

The default prefix is the name of the computer on which Kaspersky Embedded Systems Security is installed. You can change the prefix for names of allowing rules.

- Configure allowing rules usage scope (see section "Task usage scope restriction" on page [168](#)).
- On the **Actions** tab, specify the actions that must be performed by Kaspersky Embedded Systems Security:
 - When generating rules (see section "Actions to perform during an automatic rules generation process" on page [169](#)).
 - Upon task completion (see section "Actions to perform upon completion of an automatic rules generation process" on page [171](#)).
- On the **Schedule** and **Advanced** tabs:
 - Scheduled task launch settings (see section "Configuring the task launch schedule settings" on page [70](#)).
- On the **Run as** tab:
 - Task launch settings with account permissions (see section "Specifying a user account for running a task" on page [73](#)).

4. Click **OK**.

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

Task usage scope restriction

► *To restrict the scope of the Rule Generator for Applications Launch Control task, take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Automated rule generators** node.
2. Select the **Rule Generator for Applications Launch Control** subnode.
3. In the details pane of the **Rule Generator for Applications Launch Control** subnode click the **Properties** link.

The **Task settings** window opens on the **General** tab.

4. Configure the following task settings:

- **Create allowing rules based on running applications**

This check box enables / disables Rule Generator for Applications Launch Control of Applications Launch Control for applications that are already running. This option is recommended if the computer has a template set of applications based on which you want to create allowing rules.

If this check box is selected, allowing rules for Applications Launch Control are generated in accordance with running applications.

If this check box is cleared, the running applications are not taken into account when generating allowing rules.

The check box is selected by default.

This check box cannot be cleared if none of the folders are selected in the **Create allowing rules for applications from the folders** table.

- **Create allowing rules for applications from the folders**

You can use the table to select or specify scan areas for the task and the types of executable files to be taken into account when creating Applications Launch Control rules. The task will generate allowing rules for files of selected types that are located in the specified folders.

5. Click **OK**.

The specified settings are saved.

Actions to perform during automatic rules generation process

► *To configure actions that Kaspersky Embedded Systems Security is to perform during the Rule Generator for Applications Launch Control task is running, take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Automated rule generators** node.
2. Select the **Rule Generator for Applications Launch Control** subnode.
3. In the details pane of the **Rule Generator for Applications Launch Control** subnode click the **Properties** link.

The **Task settings** window opens on the **General** tab.

4. Open the **Actions** tab.
5. In the **While generating allowing rules** section, configure the following settings:

- **Use digital certificate**

If this option is selected, the presence of a digital certificate is specified as 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.

The application 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 applications 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 variant 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 a user and / 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 **All**.

6. Click **OK**.

The specified settings are saved.

Actions to perform upon completion of automatic rules generation process

► *To configure the actions to be taken by Kaspersky Embedded Systems Security after execution of the Rule Generator for Applications Launch Control task:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Automated rule generators** node.
2. Select the **Rule Generator for Applications Launch Control** subnode.
3. In the details pane of the **Rule Generator for Applications Launch Control** subnode click the **Properties** link.

The **Task settings** window opens on the **General** tab.

4. Open the **Actions** tab.
5. In the **After task completes** section, configure the following settings:

- **Add allowing rules to list of Application Control rules**

The check box enables or disables adding newly generated allowing rules to the list of Application Control rules. The list of Applications Launch Control rules is displayed when you click the **Applications Launch Control rules** link in the details pane of the **Applications Launch Control** node.

If this check box is selected, Kaspersky Embedded Systems Security adds the rules that were generated by the Rule Generator for Applications Launch Control task to the list of applications launch control rules according to the adding principle that has been set.

If this check box is cleared, Kaspersky Embedded Systems Security does not add the newly generated allowing rules to the list of Applications Launch Control rules. The generated rules are only exported to file.

The check box is selected by default.

The check box cannot be selected if the **Export allowing rules to file** check box has not been selected.

- **Principle of adding**

Drop down list is used to specify the method of adding newly generated allowing rules to the list of applications launch control rules.

- **Add to existing rules.** The rules are added to the list of existing rules. Rules with identical settings are duplicated.
- **Replace existing rules.** The rules replace the existing rules in the list.
- **Merge with existing rules.** The rules are added to the list of existing rules. Rules with identical settings are not added; the rule is added if at least one rule parameter is unique.

By default, the **Merge with existing rules** method is selected.

- **Export allowing rules to file**

The check box enables or disables export of allowing rules for Applications Launch Control to a file.

If the check box is selected, Kaspersky Embedded Systems Security exports the allowing rules to the file specified in the field below on completion of the Rule Generator for Applications Launch Control task.

If this check box is cleared, Kaspersky Embedded Systems Security does not export the generated allowing rules to file when the Rule Generator for Applications Launch Control task is completed, but only adds them to the list of Applications Launch Control rules.

The check box is cleared by default.

The check box cannot be selected if the **Add allowing rules to the list of Applications Launch Control rules** check box has not been selected.

- **Add computer details to file name**

The check box enables or disables adding information about the protected computer to the name of the destination file for export of allowing rules of Applications Launch Control.

If this check box is selected, the application adds the protected computer name and the file creation date and time to the name of the export file.

If the check box is cleared, the application does not add information about the protected computer to the name of the export file.

The check box is active if the **Export allowing rules to file** check box is selected.

The check box is selected by default.

6. Click **OK**.

The specified settings are saved.

Device Control

This section contains information about the Device Control task, as well as instruction to configure the task settings.

In this section

About Device Control task.....	174
Configuring Device Control task settings.....	176
About Device Control rules.....	178
About Device Control rules list filling	184
About Rule Generator for device Control task	190

About Device Control task

Kaspersky Embedded Systems Security 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 controls the following USB external devices connections:

- USB-connected flash-drives
- CD ROM drives
- USB-connected floppy disk drives
- USB-connected MTP-mobile devices

The Device Control task monitors all the attempts of external devices connections to a protected computer via USB and blocks their usage as mass storages if there are no allowing rules for such devices. After the connection is restricted, the device content is no longer available for reading or changing.

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 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 during rule generation.

The Device Control task can operate in two modes:

- **Apply Default Deny**. Kaspersky Embedded Systems Security applies rules to control the connection of flash-drives and other external devices, and allows or blocks the use of all devices according to the *Default Deny* principle and specified allowing rules. The use of trusted external devices is allowed. The use of untrusted external devices is blocked by default.

If an external device you consider to be untrusted is connected to a protected computer when the Device Control task is run in the **Apply Default Deny** mode, the device is not blocked by the application. We recommend that you disconnect the untrusted device manually or restart the computer. Otherwise, the Default Deny principle will not be applied to the device.

- **Statistics Only.** Kaspersky Embedded Systems Security does not control the connection of flash-drives and other external devices, but only logs information about the connection and registration of external devices on a protected computer, and about the Device Control allowing rules triggered by the connected devices. The use of all external devices is allowed. This mode is set by default.

You can apply this mode for rules generation basing on the information logged during the task running (see section "Filling rules list basing on Device Control task events" on page [188](#)).

Configuring Device Control task settings

By default, the Device Control task has the settings described in the table below. You can change the values of these settings.

Table 22. Device Control default task settings

Setting	Default Value	Description
Task operating mode	Statistics Only	The task logs information about external devices that were blocked or allowed according to the specified rules. External devices are not actually blocked. You can select the Apply Default Deny mode for computer protection to actually block the use of external devices.
Allow using all external devices when the Device Control task is not running	Not applied	Kaspersky Embedded Systems Security blocks use of external devices, regardless of the Device Control task state. This provides maximum protection level against computer security threats arising when exchanging files with external devices. You can adjust the setting so that Kaspersky Embedded Systems Security allows use of all external devices when the Device Control task is not running.
Task start schedule	At application start	The Device Control task does not start automatically at the start of Kaspersky Embedded Systems Security. You can configure the task start schedule.

► To configure the Device Control task settings, take the following steps:

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Computer Control** node.
2. Select the **Device Control** subnode.
3. Click the **Properties** link in the details pane of the **Device Control** node.

The **Task settings** window opens.

4. On the **General** tab, configure the following task settings:

- In the **Task mode** section, select one of the task modes:

- **Apply Default Deny.**

Kaspersky Embedded Systems Security applies rules to control the connection of flash-drives and other external devices, and allows or blocks the use of all devices according to the *Default Deny* principle and specified allowing rules. The use of trusted external devices is allowed. The use of untrusted external devices is blocked by default.

If an external device you consider to be untrusted is connected to a protected computer when the Device Control task is run in the **Apply Default Deny** mode, the device is not blocked by the application. We recommend that you disconnect the untrusted device manually or restart the computer. Otherwise, the Default Deny principle will not be applied to the device.

- **Statistics Only.**

Kaspersky Embedded Systems Security does not control the connection of flash-drives and other external devices, but only logs information about the connection and registration of external devices on a protected computer, and about the Device Control allowing rules triggered by the connected devices. The use of all external devices is allowed. This mode is set by default.

- Select or clear the **Allow using all mass storages when the Device Control task is not running** check box.

The check box allows or blocks the use of mass storages when the Device Control task is not running.

If the check box is selected and Device Control task is not running, Kaspersky Embedded Systems Security allows using any mass storage devices on a protected computer.

If the check box is cleared, Kaspersky Embedded Systems Security blocks the use of untrusted mass storages on a protected computer when the Device Control task is not running or if the Kaspersky Security Service is turned off. This option is recommended to maximize the level of protection against computer security threats arising when exchanging files with external devices.

The check box is cleared by default.

5. If necessary, on the **Schedule** and **Advanced** tabs, configure the scheduled task launch settings (see section "Configuring the task launch schedule settings" on page [70](#)).
6. Click **OK** in the **Task settings** window.

The modified settings are saved.

7. In the lower part of the details pane of the **Device Control** node, click the **Device Control rules** link.
8. If required, edit the list of device control rules.

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

About Device Control rules

The rules are generated uniquely for each device that is currently connected or has ever been connected to a protected computer if the information about this device is stored in the system registry.

To generate allowing rules for device control you can:

- Apply the Rule Generator for Device Control task (see section "About Rule Generator for Device Control task" on page [190](#))
- Run the Device Control task in the **Statistics Only** mode (see section "Filling rules list basing on Device Control task events" on page [188](#))
- Apply system information about previously connected devices (see section "Adding rule for one or several external devices" on page [187](#))
- Expand the usage scope for already specified rules (see section "Expanding Device Control rules usage scope" on page [183](#))

The maximum number of the Device Control rules supported by Kaspersky Embedded Systems Security - 3072.

Device Control rules are based on the following parameters:

- Rule type
- Rule usage scope
- Initial device values
- Description

Rule type

Rule type is always *allowing*. By default, the Device Control task blocks all flash-drives and other external devices connections if these devices are not included into any allowing rule usage scope.

Triggering criterion and rule usage scope

Device Control rules identify flash-drives and other external devices basing on *Device Instance Path*. Device instance path is a unique criterion that is assigned to a device by the system when the device is connected and is registered as a Mass Storage or CD/DVD drive (for example, IDE or SCSI).

Kaspersky Embedded Systems Security controls connection of the CD/DVD drives regardless of the bus used for connection. When mounting such device via USB, operating system registers two path values to the device instance: for the mass storage and for CD/DVD drive (for example, IDE or SCSI). To connect such devices correctly, allowing rules for each path value to the instance must be set.

Kaspersky Embedded Systems Security automatically defines the device instance path and parses the value obtained into the following elements:

- Device manufacturer (VID)
- Device controller type (PID)
- Device serial number

You cannot set the device instance path manually. Allowing rule triggering criteria define the rule usage scope. By default, newly created rule usage scope includes one initial device, basing on whose properties Kaspersky Embedded Systems Security had generated the rule.

You can configure the values in the created rule settings by using a mask to expand the rule usage scope (see section "Expanding Device Control rules usage scope" on page [183](#)).

Initial device values

Device properties that Kaspersky Embedded Systems Security used for allowing rule generation and that are displayed in Windows Device Manager for each device connected.

Initial device values contain the following information:

- **Device Instance Path.** Basing on this property Kaspersky Embedded Systems Security defines rule triggering criteria and fills the following fields: **Manufacturer (VID)**, **Controller type (PID)**, **Serial number** in the **Rule usage scope** section of the **Rule properties** window.
- **Friendly name.** Device clear name that is set in the device properties by its manufacturer.

Kaspersky Embedded Systems Security automatically defines initial device values when the rule is generating. Later on you can use these values to recognize the device that was used as a base for the rule generating. Initial device values are not available for editing.

Description

You can add additional information for each created device control rule in the **Description** field, for example, you can note name of the connected flash driver or define its owner. The description is displayed in a corresponding graph in the **Device Control rules** window.

Description and initial device values are not allowed for rule triggering and are prescribed only to simplify device identification by user.

Removing Device Control rules

► *To remove the Device Control rules, take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Computer Control** node.
2. Select the **Device Control** subnode.
3. In the lower part of the details pane of the **Device Control** node, click the **Device Control rules** link.

The **Device Control rules** window opens.

4. In the list, select one or several rules that you want to delete.
5. Click the **Remove selected** button.
6. Click the **Save** button.

The selected Device Control rules will be removed.

Exporting Device Control rules

► *To export Device Control rules to a configuration file, take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Computer Control** node.
2. Select the **Device Control** subnode.
3. In the lower part of the details pane of the **Device Control** node, click the **Device Control rules** link.

The **Device Control rules** window opens.

4. Click the **Export to a file** button.

The standard Microsoft Windows window opens.

5. In the window that opens, specify the file to which you want to export the rules. If no such file exists, it will be created. If a file with the specified name already exists, its contents will be rewritten after the rules are exported.

6. Click the **Save** button.

The rules and its settings will be exported in the specified file.

Activating and deactivating of Device Control rules

You can activate and deactivate created device control rules without removing them.

► *To activate or deactivate a created device control rule, take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Computer Control** node.
2. Select the **Device Control** subnode.
3. In the lower part of the details pane of the Device Control node, click the **Device Control rules** link.

The **Device Control rules** window opens.

4. In the list of specified rules open the **Rule properties** window by double clicking on the rule whose properties you want to configure.
5. In the window that opens, select or clear the **Apply rule** check box.

The check box enables or disables a device control rule.

If the check box is selected for a rule, the rule is activated. Connection for the external devices that are included into the rule usage scope is allowed.

If the check box is cleared in the rule properties, the rule is inactive.

Connection for the external devices that are included into the rule usage scope is blocked.

By default the check box is selected in the settings for each created rule.

6. Click **OK**.

Rule apply status will be saved and displayed for a specified rule.

Expanding Device Control rules usage scope

Each automatically generated device control rule covers only one external device.

You can manually expand a rule usage scope by setting the device instance path mask in properties of any specified rule.

Device instance path application reduces the total number of rules specified and simplifies rules processing. But expanding of a rule usage scope can lead to decreasing of mass storage devices control efficiency.

- *To apply a device instance path mask in a device control rule properties, take the following steps:*
 1. In the Kaspersky Embedded Systems Security Console tree, expand the **Computer Control** node.
 2. Select the **Device Control** subnode.
 3. In the lower part of the details pane of the **Device Control** node, click the **Device Control rules** link.

4. In the **Device Control rules** window, select a rule to use its properties for mask application.
5. Open the **Rule properties** window by double clicking on a selected device control rule.
6. In the window that opens, perform the following operations:
 - Select the **Use mask** check box next to the **Controller type (PID)** field if you want a rule selected to allow connections for those all mass storages that fit the specified information about device manufacturer and device serial number.
 - Select the **Use mask** check box next to the **Serial number** field if you want a rule selected to allow connections for those all mass storages that fit the specified information about device manufacturer and controller type.
 - Select the **Use mask** check boxes next to the **Controller type (PID)** field and the **Serial number** field if you want a rule selected to allow connections for those all mass storages that fit the specified information about device manufacturer.

If the **Use mask** check box is selected in at least one of the fields, the data from the fields with the cleared check box is replaced with the * sign and is not considered when the rule is applied.

7. If necessary, specify additional information about rule in the **Description** field.
For example, specify the devices affected by the rule.
8. Click **OK**.

The newly configured rule properties will be saved. The rule usage scope will be expanded according to a device instance path mask specified.

About Device Control rules list filling

You can import device control allowing rules from the XML files that were automatically generated during the Device Control or the Rule Generator for Device Control tasks running.

By default, Kaspersky Embedded Systems Security restricts connections of any flash-drives and other external devices, if they are not included into the usage scope of specified device control rules.

Table 23. Targets and scenarios for list generation of device control rules

Rule generation scenario	Target
The Rule Generator for Device Control task	<ul style="list-style-type: none"> • Add allowing rules for previously connected trusted devices before the first start of the Device Control task. • Generate rules list for devices trusted in the protected computers network.
Generate rules basing on system data	Add allowing rules for one or several newly connected devices.
The Device Control task in the Statistics Only mode	Generate allowing rules for a large number of trusted devices or for trusted MTP mobile devices.

The rule Generator for Device Control task usage

XML file, generated upon the Rule Generator for Device Control task completion, contains allowing rules for those flash-drives and other external devices whose data have been stored in a system registry.

During the task running, Kaspersky Embedded Systems Security receives system data about all mass storages that have ever been connected or are currently connected to a protected computer and generates allowing rules list basing on system data for detected devices. Upon task completion the application creates XML file in folder that is situated by path specified in the task settings. You can configure automatic import of the generated rules into the list of rules for the Device Control task.

This scenario is recommended to generate allowing rules list before the first start of the Device Control task, so that allowing rules generated cover all trusted external devices that are used on a protected computer.

Usage of system data about all connected devices

During the task running, Kaspersky Embedded Systems Security receives system data about all external devices that have ever been connected or that are currently connected to a protected computer, and displays detected devices in the list of the **Generate rules based on the system information** window.

For each detected device Kaspersky Embedded Systems Security parses the values of manufacturer (VID), controller type (PID), friendly name, serial number and device instance path. You can generate allowing rules for any mass storage, whose data have been stored in the system, and straightly add newly created rules to the list of the device control rules.

This scenario is recommended to renew an already specified rules list when it is necessary to trust a little amount of new mass storages.

Kaspersky Embedded Systems Security does not get access to system data about mobile devices connected via MTP. You cannot generate allowing rules for trusted MTP-connected mobile devices using scenarios for rules list filling on the base of system data about all connected devices.

Usage of the Device Control task in the Statistics Only mode

XML file received upon the Device Control task completion in the **Statistics Only** mode is generated basing on the task log.

During the task running Kaspersky Embedded Systems Security logs information about all connections of flash-drives and other mass storages to a protected computer. You can generate allowing rules based on task events and export them to an XML file. Before starting the task in the **Statistics Only** mode, it is recommended to configure the task running period so that during the term specified all the possible external devices connections to a protected computer would be performed.

This scenario is recommended to renew an already generated rules list if it is required to allow a large number of new external devices, as well as to generate allowing rules for MTP-connected mobile devices.

If the rule list generation according to this scenario is performed on a template machine, you can apply a generated allowing rules list while configuring the Device Control policy via the Kaspersky Security Center. This way you will be able to allow to use the external devices that are connected to a template machine on all the computers included into a protected network.

Adding an allowing rule for one or several external devices

The function of manual adding rules by ones is not supported in the Device Control task. However, in cases when you need to add rules for one or several new external devices you can use the **Generate rules basing on system data** option. If this scenario is applied, the application uses Windows data about all ever connected external devices and also allows for currently connected devices for filling an allowing rules list.

Kaspersky Embedded Systems Security does not get access to system data about mobile devices connected via MTP. You cannot generate allowing rules for trusted MTP-connected mobile devices using scenarios for rules list filling on the base of system data about all connected devices.

► *To add an allowing rule for one or several external devices that are currently connected, take the following steps:*

1. Connect a new external device, for which you want to create an allowing rule, to a protected computer.
2. In the Kaspersky Embedded Systems Security Console tree, expand the **Computer Control** node.
3. Select the **Device Control** subnode.
4. In the details pane of the **Device Control** node, click the **Device Control rules** link.

The **Device Control rules** window opens.

5. Click the **Add** button.
6. In the context menu that opens select the **Generate rules basing on system data** option.
7. In the window that opens, review the detected devices list and select a single device or several devices that you want to trust on a protected computer.
8. Click the **Add rules for devices selected** button.

New rules will be generated and added to the device control rules list.

Filling rules list basing on Device Control task events

► To create a configuration file that contains device control rules list basing on the Device Control task events, take the following steps:

1. Start the Device Control task in the **Statistics Only** mode (see section "**Configuring Device Control task settings**" on page [176](#)), to log all events of flash-drives and other external devices connections to a protected computer.
2. Upon the task in the **Statistics Only** mode task completion, open the task log by clicking the **Open task log** button in the **Management** section of the **Device Control** node details pain.
3. In the **Logs** window click the **Generate rules based on events**.

Kaspersky Embedded Systems Security will create an XML configuration file that contains a rules list generated basing on events of the Device Control task in the **Statistics Only** mode. You can apply this list in the Device Control task (see section "Importing rules from an XML file" on page [189](#)).

Before applying a rules list generated basing on the task events, it is recommended to review and then manually process the rules list to make certain that there are no untrusted devices allowed by the specified rules.

During the conversion of an XML file with the task events to a rules list, the application generates allowing rules for all registered events, including the devices restrictions.

All the task events are registered in the task log regardless of the task mode. You can create a configuration file with a rules list basing on the events of the task in the **Apply Default Deny** mode. This scenario is not recommended except urgent cases, as far as the task efficiency requires to generate a final rule list version before the task is run under the mode of default deny applying.

Importing Device Control rules from XML file

► To import the Device Control rules, take the following steps:

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Computer Control** node.
2. Select the **Device Control** subnode.
3. In the details pane of the **Device Control** node, click the **Device Control rules** link.

The **Device Control rules** window opens.

4. Click the **Add** button.
5. In the context menu of the button, select **Import rules from XML file**.
6. Specify the method for adding the imported rules. To do so, select one of the options from the context menu of the **Import rules from XML file** button:

- **Add to existing rules** if you want to add the imported rules to the list of existing ones. Rules with identical settings are duplicated.
- **Replace existing rules** if you want to replace the existing rules with the imported ones.
- **Merge with existing rules** if you want to add the imported rules to the list of existing ones. Rules with identical settings are not added; the rule is added if at least one rule parameter is unique.

The standard Microsoft Windows **Open** window opens.

7. In the **Open** window, select the XML file that contains the settings of the Device Control rules.
8. Click the **Open** button.

The imported rules will be displayed in the list of the **Device Control rules** window.

About Rule Generator for Device Control task

The task Rule Generator for Device Control task can automatically create a list of allowing rules for connected flash-drives and other mass storages basing on the system data about all external devices that have ever been connected to a protected computer.

Kaspersky Embedded Systems Security does not get access to system data about mobile devices connected via MTP. You cannot generate allowing rules for trusted MTP-connected mobile devices using scenarios for rules list filling on the base of system data about all connected devices.

Upon the task completion Kaspersky Embedded Systems Security creates an XML configuration file that contains allowing rules list for all detected external devices or straightly adds generated rules in the Device Control task depending on the Rule Generator for Device Control settings. The application will subsequently allow start of applications for which allowing rules were automatically generated.

Generated and added in the task rules are displayed in the window via the **Device Control rules** link in the **Device Control** node.

Configuring Rule Generator for Device Control task

By default, the Rule Generator for Device Control task has the settings described in the table below. You can change the values of these settings.

Table 24. Rule Generator for Device Control task default settings

Setting	Default Value	Description
Actions upon task completion	Allowing rules are added to the list of Device Control rules; new rules are merged with existing ones; duplicated rules are removed.	You can add rules to existing ones without merging them and without deleting duplicated rules, or replace existing rules with new allowing rules, or configure export of allowing rules to a file.
Task start schedule	First run is not scheduled.	The Rule Generator for Device Control task does not start automatically at startup of Kaspersky Embedded Systems Security. You can start the task manually or configure a scheduled start.

► To configure the Rule Generator for Device Control task, take the following steps:

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Automated rule generators** node.
2. Select the **Rule Generator for Device Control** subnode.
3. Click the **Properties** link in the details pane of the **Rule Generator for Device Control** node.

The **Task settings** window opens.

4. On the **General** tab, specify the actions that must be performed by Kaspersky Embedded Systems Security upon task completion:

- **Add allowing rules to the list of Device Control rules**

The check box enables or disables adding newly generated allowing rules to the list of Device Control rules. The list of Device Control rules is displayed by clicking the **Device Control rules** link in the details pane of the **Device Control** node.

If the check box is selected Kaspersky Embedded Systems Security adds

the rules that were generated by the Rule Generator for Device Control task to the list of Device Control rules according to the adding principle that has been set.

If this check box is cleared, Kaspersky Embedded Systems Security does not add the newly generated allowing rules to the list of Device Control rules. The generated rules are only exported to file.

The check box is selected by default.

The check box cannot be selected if the **Export allowing rules to file** check box has not been selected.

- **Principle of adding**

Drop down list used to specify the method of adding newly generated allowing rules to the list of Device Control rules.

- **Add to existing rules.** The rules are added to the list of existing rules. Rules with identical settings are duplicated.
- **Replace existing rules.** The rules replace the existing rules in the list.
- **Merge with existing rules.** The rules are added to the list of existing rules. Rules with identical settings are not added; the rule is added if at least one rule parameter is unique.

By default, the **Merge with existing rules** method is selected.

- **Export allowing rules to file**

The check box enables or disables export of allowing rules for Device Control to a file.

If the check box is selected, Kaspersky Embedded Systems Security exports the allowing rules to the file specified in the field below on completion of the Rule Generator for Applications Launch Control task.

If this check box is cleared, Kaspersky Embedded Systems Security does not export the generated allowing rules to file when the Rule Generator for Device Control task is completed, but only adds them to the list of Device Control rules.

The check box is cleared by default.

The check box cannot be selected if the **Add allowing rules to the list of Device Control rules** check box has not been selected.

- **Add computer details to file name**

The check box enables or disables adding information about the protected computer to the name of the destination file for export of allowing Device Control rules.

If this check box is selected, the application adds the protected computer name and the file creation date and time to the name of the export file.

If the check box is cleared, the application does not add information about the protected computer to the name of the export file.

The check box is active if the **Export allowing rules to file** check box is selected.

The check box is selected by default.

5. On the **Schedule** and **Advanced** tabs, configure the scheduled task launch settings (see section "Configuring the task launch schedule settings" on page [70](#)).
6. Click **OK**.

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

Firewall Management

This section contains information about the Applications Launch Control task and how to configure it.

In this section

About the Firewall Management task.....	194
About Firewall rules.....	196
Enabling and disabling Firewall rules.....	198
Adding Firewall rules manually.....	199
Deleting Firewall rules.....	201

About the Firewall Management task

Kaspersky Embedded Systems Security provides a reliable and ergonomic solution for protecting network connections using the Firewall Management task.

The Firewall Management task does not perform independent network traffic filtering, but it allows you to manage Windows Firewall through the Kaspersky Embedded Systems Security graphical interface. During the Firewall Management task Kaspersky Embedded Systems Security takes over management of the settings and policies of the operation system's firewall and blocks any possibility of external firewall configuration.

During installation of the application, the Firewall Management component reads and copies the Windows Firewall status and all specified rules. After that, the set of rules and the rule parameters may only be changed, and the firewall may only be turned on or off in Kaspersky Embedded Systems Security.

If Windows Firewall is turned off during installation of Kaspersky Embedded Systems Security, the Firewall Management task will not be executed after the installation completes. If Windows Firewall is turned on during installation of the application, the Firewall Management task is executed after the installation completes, blocking all network connections that are not allowed by the specified rules.

The Firewall Management component is not installed by default, as it is not included in the set of components for the Recommended Installation.

The Firewall Management task enforces blocking of all incoming and outgoing connections not allowed by the task's specified rules.

The task polls the Windows Firewall regularly and monitors its status. By default, the polling interval is set to 1 minute and cannot be changed. If during polling Kaspersky Embedded Systems Security detects a mismatch between the Windows Firewall settings and the Firewall Management task settings, the application forcibly applies the task settings on the operating system firewall.

With minute-by-minute polling of the Windows Firewall, Kaspersky Embedded Systems Security monitors the following:

- Operating status of the Windows Firewall.
- Status of rules added after installation of Kaspersky Embedded Systems Security by other applications or tools (for example, the addition of a new application rule for a port/application using wf.msc).

When applying the new rules to Windows Firewall, Kaspersky Embedded Systems Security creates a Kaspersky Security Group rule set in the **Windows Firewall** snap-in. This rule set unites all the rules created by Kaspersky Embedded Systems Security using the Firewall Management task. The rules in the Kaspersky Security Group are not monitored by the application during the polling each minute and are not automatically synchronized with the list of rules specified in the Firewall Management task settings.

► *To update the Kaspersky Security Group rules manually,*

restart the Kaspersky Embedded Systems Security Firewall Management task.

You can also edit the Kaspersky Security Group rules manually using the **Windows Firewall** snap-in.

If Windows Firewall is managed by the Kaspersky Security Center group policy, the Firewall Management task cannot be started.

About Firewall rules

The Firewall Management task controls filtration of incoming and outgoing network traffic using allowing rules forcibly applied to the Windows Firewall during task execution.

The first time the task is started Kaspersky Embedded Systems Security reads and copies all the incoming network traffic rules specified in the Windows Firewall settings to the Firewall Management task settings. Then the application operates according to the following rules:

- If a new rule is created in the Windows Firewall settings (manually or automatically during a new application installation), Kaspersky Embedded Systems Security deletes the rule.
- If an existing rule is deleted from the Windows Firewall settings, Kaspersky Embedded Systems Security restores the rule.
- If the parameters of an existing rule are changed in the Windows Firewall settings, Kaspersky Embedded Systems Security rolls back the changes.
- If a new rule is created in the Firewall Management settings, Kaspersky Embedded Systems Security forcibly applies the rule to Windows Firewall.
- If an existing rule is deleted from the Firewall Management settings, Kaspersky Embedded Systems Security forcibly deletes the rule from the Windows Firewall settings.
- If an existing rule is deleted from the Firewall Management settings, Kaspersky Embedded Systems Security forcibly deletes the rule from the Windows Firewall settings.

Kaspersky Embedded Systems Security does not work with blocking rules or rules controlling outgoing network traffic. Upon start of the Firewall Management task, Kaspersky Embedded Systems Security deletes all such rules from the Windows Firewall settings.

You can set, delete and edit filtration rules for incoming network traffic.

You cannot specify a new rule to control outgoing network traffic in the Firewall Management task settings. All Firewall rules specified in Kaspersky Embedded Systems Security control only incoming network traffic.

You can manage the following types of Firewall rules:

- Application rules
- Port rules

Application rules

This type of rule allows targeted network connections for specified applications. The triggering criterion for these rules is based on a path to an executable file.

You can manage application rules:

- Add new rules.
- Remove existing rules.
- Enable or disable specified rules.
- Edit the parameters of the specified rules: specify the rule name, path to the executable file, and the rule usage scope.

Port rules

This type of rule allows network connections for specified ports and protocols (TCP / UDP). The triggering criteria for these rules are based on the port number and protocol type.

You can manage port rules:

- Add new rules.
- Remove existing rules.
- Enable or disable specified rules.
- Edit the parameters of the specified rules: set the rule name, port number, protocol type, and scope for application of the rule.

Port rules imply a broader scope than application rules. By allowing connections based on port rules, you lower the security level of the protected computer.

Enabling and disabling Firewall rules

► *To enable or disable an existing rule for filtering incoming network traffic, perform the following actions:*

1. Depending on the application interface, perform the following steps:
 - If you want to configure the task locally, in the Kaspersky Embedded Systems Security Console tree, select **Computer Control** → **Firewall Management**. Then go to the **Firewall** node and click the **Firewall rules** link.
 - If you want to configure policies in the Administration Console of Kaspersky Security Center, in the computer group select **Policies** → **<Policy name>** → **Network Control** → **Settings (Firewall Management section)** → **Rule list**.
 - If you want to configure application settings for a single computer using Kaspersky Security Center, open the **Firewall rules** window from the **Task settings** window in Kaspersky Security Center.

The **Rules list** window opens.

2. Depending on the type of the rule whose status you want to modify, select **Applications** or **Ports**.

3. 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.

4. Click **Save** in the **Firewall rules** window.

The specified task settings are saved. The new rule parameters will be sent to Windows Firewall.

Adding Firewall rules manually

► *To add a new or edit an existing rule for filtering incoming network traffic, do the following:*

1. Depending on the application interface, perform the following steps:

- If you want to configure the task locally, in the Kaspersky Embedded Systems Security Console tree, select **Computer Control** → **Firewall Management**. Then go to the **Firewall** node and click the **Firewall rules** link.
- If you want to configure policies in the Administration Console of Kaspersky Security Center, in the computer group select **Policies** → **<Policy name>** → **Network Control** → **Settings (Firewall Management section)** → **Rule list**.
- If you want to configure application settings for a single computer using Kaspersky Security Center, open the **Firewall rules** window from the **Task settings** window in Kaspersky Security Center.

The **Rules list** window opens.

2. 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.

3. 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 usage 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 usage scope** field, specify the network addresses for which the modified rule will be applied.

You can only use IPv4 IP-addresses.

4. Click **OK** in the **Application rule** or **Port rule** window.

5. 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. Depending on the application interface, perform the following steps:
 - If you want to configure the task locally, in the Kaspersky Embedded Systems Security Console tree, select **Computer Control** → **Firewall Management**. Then go to the **Firewall** node and click the **Firewall rules** link.
 - If you want to configure policies in the Administration Console of Kaspersky Security Center, in the computer group select **Policies** → **<Policy name>** → **Network Control** → **Settings (Firewall Management section)** → **Rule list**.
 - If you want to configure application settings for a single computer using Kaspersky Security Center, open the **Firewall rules** window from the **Task settings** window in Kaspersky Security Center.

The **Rules list** window opens.

2. Depending on the type of rule whose status you want to modify, select the **Applications** or **Ports** tab.
3. In the rule list, select the rule you want to delete.
4. Click the **Remove** button.

The selected rule is deleted.

5. Click **Save** in the **Firewall rules** window.

The specified 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 section

File Integrity Monitor.....	202
Log Inspection.....	214

File Integrity Monitor

This section contains information about starting the File Integrity Monitor task and how to configure it.

In this section

About the File Integrity Monitor task	202
About file operation monitoring rules	204
Configuring File Integrity Monitor task settings	207
Configuring monitoring rules	210

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 reports detected files operations within the monitoring scope as soon as the 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 enabled the USN Journal after a rule was created for a volume and the File Integrity Monitor task has been launched, the task must be restarted. If not, the rule is not considered during monitoring.

Excluded monitoring scopes

You can specify monitoring scope exclusions (see section "Configuring monitoring rules" on page [210](#)). 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 (see section "Configuring monitoring rules" on page [210](#)).

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 listed in the trusted user list in the settings for the monitoring scope rules. If Kaspersky Embedded Systems Security detects a file operation performed by an untrusted user, the File Integrity Monitor task records a *Critical event* in the task log.

Trusted user – a user or group of users authorized to perform file operations in the specified monitoring scope. If Kaspersky Embedded Systems Security detects file operations performed by a trusted user, the File Integrity Monitor task records an *Informational event* in the task log.

Kaspersky Embedded Systems Security cannot determine the users that initiate operations during monitoring interruption periods. In this case, the user status is determined to be unknown.

Unknown user – This status is assigned to a user if Kaspersky Embedded Systems Security cannot receive information about a user due to a task interruption or a failure of the data synchronization driver or USN Journal. If Kaspersky Embedded Systems Security detects a file operation performed by an unknown user, the File Integrity Monitor task records a *Warning* event in the task log.

File operation markers

When the File Integrity Monitor task runs, Kaspersky Embedded Systems Security uses file operation markers to determine that an action has been performed on a file.

A *file operation marker* is a unique descriptor that can characterize a file operation.

Each file operation can be a single action or a chain of actions with files. Each action of this kind is equated to a file operation marker. If the marker you specify as a rule triggering criterion is detected in a file operation chain, the application logs an event indicating that the given file operation was performed.

The importance level of the logged events does not depend on the selected file operation markers or the number of events.

By default, Kaspersky Embedded Systems Security considers all available file operation marker. You can select file operation markers manually in the task's rule settings (see the table below).

Table 25. 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

File operation ID	File operation marker	Supported file systems
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 deleted	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

File operation ID	File operation marker	Supported file systems
RENAME_NEW_NAME	New name assigned to file or folder	NTFS, ReFS
REPARSE_POINT_CHANGE	New reparse point created or existing reparse point changed for a file or folder	NTFS, ReFS
SECURITY_CHANGE	File or folder access rights changed	NTFS, ReFS
STREAM_CHANGE	New named file stream created or existing named file stream changed	NTFS, ReFS
TRANSACTIONED_CHANGE	Named file stream changed by TxF transaction	Only ReFS

Configuring File Integrity Monitor task settings

You can change the default settings of the File Integrity Monitor task (see the table below).

Table 26. Default File Integrity Monitor task settings

Setting	Value	How to set
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 is not running.
Consider excluded monitoring scopes	Not applied	You can check the use of exclusions for folders in which file operations do not need to be monitored. When the File Integrity Monitor task runs, Kaspersky Embedded Systems Security will skip monitoring scopes specified as exclusions.

Setting	Value	How to set
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 of the specified markers, Kaspersky Embedded Systems Security generates a monitoring event.
Checksum calculation	Not applied	You can configure file checksum calculation after the changes in the file are made.
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, implement the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **System Inspection** node.
2. Select the **File Integrity Monitor** subnode.
3. Click the **Properties** link in the details pane of the **File Integrity Monitor** node.

The **Task settings** window opens.

4. In the window that opens, on the **General** tab, clear or select the **Monitor file operations when the task is not running** check box.

The check box enables or disables monitoring of the file operations specified in the File Integrity Monitor task settings when the task is not running for any reason (removal of a hard disk, task stopped by user, software error).

If the check box is selected, Kaspersky Embedded Systems Security will record events in all monitoring scopes when the File Integrity Monitor task is not running.

If the check box is cleared, the application will not log file operations in monitoring scopes when the task is not running.

The check box is selected by default.

5. On the **Schedule** and **Advanced** tabs, configure the task launch schedule (see section "Configuring the task launch schedule settings" on page [70](#)).
6. Click **OK**.

The specified settings are saved.

Configuring monitoring rules

By default, a monitoring scope is not specified and the task does not monitor file operations in any folder.

► *To add a monitoring scope, perform the following steps:*

1. In the Kaspersky Embedded Systems Security console tree, expand the **System Inspection** node.
2. Select the **File Integrity Monitor** subnode.
3. Click the **Monitoring rules** link in the details pane of the **File Integrity Monitor** node.

The **Monitoring rules** window opens.

4. Add a monitoring scope in one of the following ways:

- If you want to select folders through the standard Microsoft Windows dialog:
 - a. On the left side of the window, click the **Browse** button.

The standard Microsoft Windows **Browse for Folder** window opens.

- b. In the window that opens, select the folder for which you want to monitor operations, and click the **OK** button.
- c. Click the **Add** button to have Kaspersky Embedded Systems Security start monitoring file operations in the indicated monitoring scope.

- If you want to specify a monitoring scope manually, add a path using a supported mask:
 - `<*.ext>` - all files with the extension `<ext>`, regardless of their location.
 - `<*\name.ext>` - all files with name `<name>` and extension `<ext>`, regardless of their location.
 - `<\dir*>` - all files in 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 will not add the specified monitoring scope.

On the right side of the window, the **Rule settings** tab displays the trusted users and file operation markers selected for this monitoring scope.

5. In the list of added monitoring scopes, select the scope whose settings you want to configure.
6. Select the **Users** tab.
7. Click the **Add** button.

The standard Microsoft Windows **Select Users or Groups** window opens.

8. Select the users or groups of users that Kaspersky Embedded Systems Security will consider trusted for the selected monitoring scope.
9. Click **OK**.

By default, Kaspersky Embedded Systems Security treats all users not on the trusted user list as untrusted, and generates (see section "About file operation monitoring rule" on page [204](#)) *Critical events* for them.

10. Select the **Set file operations markers** tab.

11. If required, perform the following actions to select a number of markers:

- a. Select the **Detect file operations basing on the following markers** option.
- b. In the list of available file operations (see the section "About file operation monitoring rules" on page [204](#)), select the check boxes next to the operations you want to monitor.

By default Kaspersky Embedded Systems Security detects all file operation markers, the **Detect file operations basing on all recognizable markers** option is selected.

12. If you want Kaspersky Embedded Systems Security to calculate files checksum after operation is performed, do the following:

- a. In the **Checksum calculation** section select the **Calculate checksum for a file final version, after the file was changed, if possible** check box.

If the check box is selected, Kaspersky Embedded Systems Security calculates the checksum of the modified file, where the file operation with at least one selected marker was detected.

If the file operation is detected by a number of markers, only the final file checksum after all modifications is calculated.

If the check box is cleared, Kaspersky Embedded Systems Security does not calculate the checksum for the modified files.

No checksum calculation is performed in the following cases:

- If the file became unavailable (for example, due to the change of access permissions).
- If the file operation is detected in the file that has been removed afterwards.

The check box is cleared by default.

b. In the drop down list **Calculate the checksum using the algorithm** select one of the options:

- **MD5 hash**
- **SHA256 hash**

13. 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 skips the monitoring scopes specified in the exclusions list when the File Integrity Monitor task is run.

If the check box is cleared, Kaspersky Embedded Systems Security logs events for all specified monitoring scopes.

By default, the check box is cleared and the exclusion list is empty.

c. Click the **Browse** button.

The standard Microsoft Windows **Browse for Folder** window opens.

d. In the window that opens, specify the folder that you want to exclude from the monitoring scope.

e. Click the **Add** button.

The specified folder is added to the list of excluded scopes.

You can also add excluded monitoring scopes manually using the same masks that are used to specify monitoring scopes.

14. Click the **Save** button.

The specified monitoring rules will be applied to File Integrity Monitor task.

Log Inspection

This section contains information about the Log Inspection task and configuring task settings.

In this section

About the Log Inspection task	214
Configuring Log analysis rules	216
Configuring heuristic analyzer	218

About the Log Inspection task

When the Log Inspection task runs, Kaspersky Embedded Systems Security monitors the integrity of the protected environment based on the results of an inspection of Windows Event Logs.

The application notifies the administrator upon detecting abnormal behavior in the system, which may be an indication of attempted cyberattacks.

Kaspersky Embedded Systems Security considers the Window event logs and identifies breaches based on the rules specified by a user or by the settings of the Heuristic Analyzer, which is used by the task to inspect logs.

Heuristic Analyzer

You can use the Log Inspection task to monitor the state of the protected system based on preset 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 heuristics in the Heuristic Analyzer settings.

Seven heuristics are included in the heuristic list for the Log Inspection task. You can enable or disable the use of any of the heuristics. You cannot delete existing heuristics or create new heuristics.

You can configure the following triggering criteria for each heuristic:

- Password brute-force detection
- Network login detection

You can also configure exclusions in the task settings. The Heuristic Analyzer is not activated when a login is conducted by a trusted user or from a trusted IP address.

Kaspersky Embedded Systems Security does not use heuristics to inspect Windows logs if the Heuristic Analyzer is not used by the task. By default, the Heuristic Analyzer is enabled.

When the Heuristic Analyzer is activated, 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.

The application does not verify that the specified sublog actually exists in the Windows Event Log.

When the rule is triggered, Kaspersky Embedded Systems Security records a *Critical event* in the Log Inspection task log.

By default, the Log Inspection task does not consider custom rules.

Configuring the Log inspection rules

Perform the following actions to add and configure a new log analysis custom rule:

1. In the Kaspersky Embedded Systems Security Console tree, expand the **System Inspection** node.
2. Select the **Log Inspection** subnode.
3. In the details pane of the **Log Inspection** node, click the **Log Inspection Rules** link.
The **Log Inspection Rules** window opens.
4. Select or clear the **Apply custom rules for log inspection** check box.

If the check box is selected, Kaspersky Embedded Systems Security applies custom rules for log analysis according to each rule settings. You can add and configure log analysis rules.

If the check box is cleared, you cannot add or modify the custom rules. Kaspersky Embedded Systems Security applies default rules settings.

You cannot delete or modify the preset rules.

The check box is cleared by default.

You can control whether the preset rules are applied for log analysis. Select the check boxes corresponding to the rules you want to apply for the log analysis.

5. To create a new custom rule, do the following:
 - a. Enter the name of the new rule.
 - b. Click the **Add** button.

The created rule is added to the general rule list.

6. To configure any rule, take the following steps:

- a. Click with the left mouse button to select a rule in the list.

In the right area of the window, the **Comments** tab displays general information about the rule.

The comments for the new rule are blank.

- b. Select the **Description** tab.

- c. In the **General** section, edit the rule name, if necessary.

- d. Select the **Data analysis source**.

Select a source log to use recorded events for analysis. The following Windows event log types are available:

- Application
- Security
- System

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 the **Save** button.

The configured log inspection rules will be applied.

Heuristic Analyzer configuration

► Perform the following actions to configure the heuristic analyzer for the Log Inspection task:

1. In the Kaspersky Embedded Systems Security Console tree, expand the **System Inspection** node.
2. Select the **Log Inspection** subnode.
3. Click the **Properties** link in the details pane of the **Log Inspection** node.

The **Task settings** window opens.

4. Select the **Heuristic analyzer** tab.
5. Select or clear check box **Apply heuristic analyzer for log inspection**.

If this check box is selected, Kaspersky Embedded Systems Security applies heuristic analyzer to detect abnormal activity on the protected computer.

If this check box is cleared the heuristic analyzer is not running and Kaspersky Embedded Systems Security applies preset or custom rules to detect abnormal activity.

For the task to run, at least one log inspection mode must be selected.

The check box is selected by default.

6. Select the heuristics which you want to apply from the list of heuristics available:
 - Password Crack Attempt.
 - Windows EventLogs Compromise.
 - A service was installed in the system.
 - Logon Attempt with Explicit Credentials.
 - Network Logon with NTLM v 1 (MS14-068 Kerberos forged PAC).
 - Security Group was Compromised.

7. To configure the selected heuristics, go to the **Triggering criteria** tab.
8. In the **Brute-force attack detection** set the number of attempts and a time frame when these attempts occurred, which will be considered as triggers for heuristic analyzer.
9. In the **Network login detection** section, indicate the start and end of the time interval during which Kaspersky Embedded Systems Security treats sign-in attempts as abnormal activity.
10. Select the **Exclusions** tab.
11. Perform the following actions to add trusted users:
 - a. Click the **Browse** button.
 - b. Select a user.
 - c. Click **OK**.

A selected user is added to the list of trusted users.

12. Perform the following actions to add trusted IP-addresses:
 - a. Enter the IP-address.
 - b. Click the **Add** button.

13. An entered IP-address is added to the list of trusted IP-addresses.

14. Select the **Task Management** tab to configure the task launch schedule.

15. Click **OK**.

The Log Inspection task configuration is saved.

On-Demand Scan

This section provides information about On-Demand Scan tasks, and instructions on configuring On-Demand Scan task settings and security settings on the protected computer.

In this section

About On-Demand Scan tasks	220
On-Demand Scan task statistics	222
Configuring On-Demand Scan task settings.....	224
Scan scope in On-Demand Scan tasks	232
Removable Drives Scan.....	254
Creating an On-Demand Scan task.....	257
Removing tasks	261
Renaming tasks	261

About On-Demand Scan tasks

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

Kaspersky Embedded Systems Security provides four system tasks of On-Demand Scan:

- The Scan at Operating System Startup task is performed every time Kaspersky Embedded Systems Security starts. Kaspersky Embedded Systems Security scans boot sectors and master boot records of hard and removable drives, system memory, and memory of processes. Every time Kaspersky Embedded Systems Security runs the task, it creates a copy of non-infected boot sectors. If at the next task launch it detects a threat in those sectors, it replaces them with the backup copy.
- By default, the Critical Areas scan task is performed weekly by schedule. Kaspersky Embedded Systems Security scans objects in critical areas of the operating system: startup objects, boot sectors and master boot records of hard and removable drives, system memory and memory of processes. Application scans files in the system folders, for example, in %windir%\system32. Kaspersky Embedded Systems Security applies security settings the values of which correspond to the **Recommended** level (see section "**Selecting predefined security levels for On-Demand Scan tasks**" on page [243](#)). You can modify the settings of the Critical Areas scan task.
- Quarantine Scan task is executed by default according to the schedule after every databases update. The Quarantine Scan task settings cannot be modified.
- The Application Integrity Control task is performed every time Kaspersky Embedded Systems Security starts running. It provides the option of checking Kaspersky Embedded Systems Security modules for damage or modification. The application installation folder is checked. The task execution statistics contain information about the number of modules checked and corrupted. The values of the task settings are defined by default and cannot be edited. The values of the task launch schedule settings can be edited.

Additionally custom On-Demand Scan tasks can be created. For example you can create a task for scanning public access folders on the computer.

Kaspersky Embedded Systems Security may run several On-Demand Scan tasks at the same time.

On-Demand Scan task statistics

While the On-Demand Scan task is being executed, you can view information about the number of objects processed by Kaspersky Embedded Systems Security since it was started until the current moment.

This information remains available even if the task is paused. You can view the task statistics in the task log (see the section "Viewing statistics and information of a Kaspersky Embedded Systems Security task using logs" on page [315](#)).

► *To view the statistics of an On-Demand Scan task, take the following steps:*

1. Expand the **On-Demand Scan** node in the Kaspersky Embedded Systems Security Console tree.
2. Select the On-Demand Scan task whose statistics you want to view.

Task statistics are displayed in the **Statistics** section of the details pane of the selected node.

The following information can be viewed about objects processed by Kaspersky Embedded Systems Security since it was started until the current moment (see the table below).

Table 27. On-Demand Scan task statistics

Field	Description
Detected	Number of objects detected by Kaspersky Embedded Systems Security. For example, if Kaspersky Embedded Systems Security detects one malware in five files, the value in this field increases by one.
Infected and other objects detected	Number of objects that Kaspersky Embedded Systems Security found and classified as infected or number of found legitimate software files, which were not excluded from the real-time protection and on-demand tasks scope and were classified as riskware.
Probably infected objects	Number of objects found by Kaspersky Embedded Systems Security to be probably infected
Objects not disinfected	<p>Number of objects which Kaspersky Embedded Systems Security did not disinfect for the following reasons:</p> <ul style="list-style-type: none"> • the type of detected object cannot be disinfected • an error occurred during disinfection
Objects not quarantined	The number of objects that Kaspersky Embedded Systems Security attempted to quarantine but was unable to do so, for example, due to insufficient disk space.
Objects not removed	The number of objects that Kaspersky Embedded Systems Security attempted but was unable to delete, because, for example, access to the object was blocked by another application.
Objects not scanned	The number of objects in the protection scope that Kaspersky Embedded Systems Security failed to scan because, for example, access to the object was blocked by another application.
Objects not backed up	The number of objects the copies of which Kaspersky Embedded Systems Security attempted to save in Backup but was unable to do so, for example, due to insufficient disk space.
Processing errors	Number of objects whose processing resulted in an error.

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

You can also view the On-Demand Scan task statistics in the selected task log by clicking the **Open task log** link in the **Management** section of the details pane.

It is recommended to manually proceed events registered in the task log on the **Events** tab upon the task completion.

Configuring On-Demand Scan task settings

By default On-Demand Scan tasks have the settings described in the table below. You can configure system and user On-Demand Scan tasks.

Table 28. On-Demand Scan task settings

Setting	Value	How to set
Scan scope	<p>Applied in system and custom tasks:</p> <ul style="list-style-type: none"> • Scan at Operating System Startup: the entire computer, excluding shared folders and autorun objects • Critical Areas Scan: the entire computer, excluding shared folders and certain operating system files • Custom On-Demand Scan tasks: the entire computer 	<p>You can change the scan scope. The protection scope cannot be configured for the Quarantine Scan and Application Integrity Control system tasks.</p>
Security settings	<p>Common settings for the entire scan scope correspond to the security level Recommended.</p>	<p>For nodes selected in the computer file resources list or tree, you can:</p> <ul style="list-style-type: none"> • Select a different predefined security level. • Manually change security settings <p>You can save a set security settings for a selected node as a template to use later for a different node.</p>
Heuristic Analyzer	<p>It is used with the Medium analysis level for Critical Areas Scan, Scan at Operating System Startup, and custom tasks.</p> <p>It is used with the Deep analysis level for the Quarantine Scan task.</p>	<p>The Heuristic Analyzer can be enabled or disabled and the analysis level configured. The Quarantine Scan task analysis level cannot be configured.</p> <p>The Heuristic Analyzer is not used in the Application Integrity Control task.</p>

Setting	Value	How to set
Trusted Zone	Used	General list of exclusions which can be used in selected tasks.
KSN Usage	Used	You can improve your computer's protection using the Kaspersky Security Network infrastructure of cloud services.
Task launch settings with permissions	The task is started under a system account.	You can edit launch settings with account permissions for all system and user On-Demand Scan tasks, except Quarantine Scan and Application Integrity Control tasks.
Run in background mode (low priority)	Not applied	You can configure the priority level of On-Demand Scan tasks.
Task start schedule	<p>Applied in system tasks:</p> <ul style="list-style-type: none"> • Scan at Operating System Startup - At application launch • Critical Areas Scan - Weekly • Quarantine Scan - After application database update • Application Integrity Control - At application launch <p>Not used in newly created custom tasks.</p>	You can configure the settings of scheduled startup of the task.
Registering scan execution and	The computer protection status is updated weekly after the Critical Areas Scan is performed.	You can configure settings for registering the execution of the Critical Areas Scan

Setting	Value	How to set
updating computer protection status		<p>in the following ways:</p> <ul style="list-style-type: none"> • Edit the settings of the Critical Areas Scan task launch schedule • Edit the protection scope of the Critical Areas Scan task • Create user On-Demand Scan tasks

► *To configure an On-Demand Scan task, take the following steps:*

1. Expand the **On-Demand Scan** node in the Kaspersky Embedded Systems Security Console tree.
2. Select the subnode that corresponds to the task that you want to configure.
3. In the details pane of the node on the **Overview and management** tab, click the **Properties** link.

The **Task settings** window opens. Configure the following task settings:

- On the **General** tab:
 - Using the Heuristic Analyzer (see page [228](#))
 - Running the task in the background mode (see section "Running background On-Demand Scan task" on page [229](#))
 - KSN Usage (on page [230](#))
 - Applying a Trusted Zone (see section "Enabling and disabling the use of the Trusted Zone in Kaspersky Embedded Systems Security tasks" on page [60](#))
 - Registering the execution of the Critical Areas Scan (see page [232](#))
- On the **Schedule** and **Advanced** tabs:
 - Scheduled task launch settings (see section "Configuring the task launch schedule settings" on page [70](#)).

- On the **Run as** tab:
 - Task launch settings with account permissions (see section "Specifying a user account for running a task" on page [73](#)).
4. Click **OK** in the **Task settings** window.

The modified settings are saved.

5. If required, in the details pane of the selected node, open the **Configure scan scope** tab.

Do the following:

- In the computer file resources tree, select the nodes that you want to include in the scan scope.
 - Select one of the predefined security levels (see section "Selecting predefined security levels for On-Demand Scan tasks" on page [243](#)) or configure the scan settings manually (see section "Configuring security settings manually" on page [247](#)).
6. In the context menu of the name of the selected task, select **Save task**.

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

Using Heuristic Analyzer

► *To configure the Heuristic Analyzer, take the following steps:*

1. Expand the **On-Demand Scan** node in the Kaspersky Embedded Systems Security Console tree.
2. Select the subnode that corresponds to the task that you want to configure.
3. Click the **Properties** link in the details pane.

The **Task settings** window opens on the **General** tab.

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

5. 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.

6. 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.

Running background On-Demand Scan task

By default the processes in which Kaspersky Embedded Systems Security tasks are executed are assigned the base priority **Medium (Normal)**.

The process that will run an On-Demand Scan task can be assigned **Low** priority.

Demoting the process priority increases the time required to execute the task, but may have a beneficial effect on the execution speed of the processes of other active programs.

Multiple background tasks can be running in a single working process with low priority.

You can specify the maximum number of processes to background On-Demand Scan tasks.

► *To change the priority of an On-Demand Scan task, take the following steps:*

1. Expand the **On-Demand Scan** node in the Kaspersky Embedded Systems Security Console tree.
2. Select the subnode that corresponds to the task whose priority you want to modify.
3. Click the **Properties** link in the details pane of the selected node.

The **Task settings** window opens on the **General** tab.

4. Select or clear the **Perform task in background mode** check box.

The check box modifies the priority of the task.

If the check box is selected, the task priority in the operating system is reduced. The operating system provides resources for performing the task depending on the load on the CPU and the computer file system from other Kaspersky Embedded Systems Security tasks and applications. As a result, task performance will slow down during increased loads and will speed up at lower loads.

If the check box is cleared, the task will start and run with the same priority as the other Kaspersky Embedded Systems Security tasks and other applications. In this case, the speed of task execution increases.

The check box is cleared by default.

5. Click **OK**.

Configured task settings are saved and applied immediately to the running task. If the task is not running, the modified settings are applied at next start.

KSN Usage

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

If you accepted the KSN Statement when the application is installed, the KSN Usage task will be started automatically when Kaspersky Embedded Systems Security is started. You can run the task manually (see section "Starting and stopping the KSN Usage task" on page [119](#)) or schedule its launch (see section "Configuring the KSN Usage task" on page [121](#)).

► *To configure the KSN Usage in On-Demand Scan tasks, take the following steps:*

1. Expand the **On-Demand Scan** node in the Kaspersky Embedded Systems Security Console tree.
2. Select the subnode that corresponds to the task that you want to configure.
3. Click the **Properties** link in the details pane of the selected node.

The **Task settings** window opens on the **General** tab.

4. Select or clear the **Use KSN for scan** check box.

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 Real-Time File Protection task does not use KSN service.

The check box is selected by default.

5. Click **OK**.

Configured task settings are saved and applied immediately to the running task. If the task is not running, the modified settings are applied at next start.

Registering execution of Critical Areas Scan

By default, the computer protection status is displayed in the details pane of the **Kaspersky Embedded Systems Security** node and is updated weekly after the Critical Areas Scan task is performed.

The time of the computer protection status update is linked to the On-demand task schedule in whose settings the **Consider task as critical areas scan** check box is selected. The check box is selected only for the Critical Areas Scan task and cannot be modified.

You can relink the On-Demand Scan task to the computer's protection status only from Kaspersky Security Center.

Scan scope in On-Demand Scan tasks

This section contains information on generating and using a scan scope in On-Demand Scan tasks.

In this section

About a scan scope.....	233
Configuring view mode for network file resources	234
Predefined scan scopes	235
Creating a scan scope	237
Including network objects in the scan scope.....	240
Creating a virtual scan scope	241
Security settings of the selected node in On-Demand Scan tasks.....	243
Selecting predefined security levels for On-Demand Scan tasks.....	243
Configuring security settings manually	247

About scan scope

You can configure the scan scope for Scan at Operating System Startup and Critical Areas Scan tasks, and for custom On-Demand Scan tasks.

By default On-Demand Scan tasks scan all objects of the computer file system. If there is no security requirement to scan all objects of the file system, you can limit the scan to the scan scope.

In Kaspersky Embedded Systems Security Console, the scan scope is displayed as a tree or as a list of the computer file resources that Kaspersky Embedded Systems Security can control. By default, the network file resources of the protected computer are displayed in a list-view mode.

► *To display network file resources in the tree-view mode,*

open the drop down list in the **Protection scope settings** window upper left sector and select **Tree-view**.

The nodes are displayed in a list-view or in a tree-view mode of the Computer file resources as follows:

The node is included in the scan scope.

The node is excluded from the scan scope.

At least one of the subnodes of this node is excluded from the scan scope, or the security settings of the subnode(s) differ from those of this node (only for tree-view mode).

The icon is displayed if all subnodes are selected, but the parent node is not selected. In this case, changes in the composition of files and folders of the parent node are disregarded automatically when the scan scope for the selected subnode is being created.

The names of virtual nodes in the scan scope are displayed in blue font.

Configuring view mode for network file resources

► *To select view-mode for the network file resources during configuring the scan scope settings, take the following steps:*

1. Expand the **On-Demand Scan** node in the Kaspersky Embedded Systems Security Console tree.
2. Select the subnode corresponding to an On-Demand Scan task that you want to configure.
3. In the details pane of the selected node click the **Configure scan scope** link.

Scan scope settings window opens.

4. Open the drop down list in the upper left section of the window. Perform one of the following steps:

- Select the **Tree-view** option to display the network file resources in a tree-view mode.

- Select the **List-view** option to display the network file resources in a list-view mode.

By default, the network file resources of the protected computer are displayed in a list-view mode.

5. Click the **Save** button.

Scan scope settings window will be closed. The newly configured settings will be applied.

Predefined scan scopes

The tree or list of computer file resources is displayed in the details pane of the node of the selected On-Demand Scan task on the **Scan scope settings** tab.

The file resources tree or list displays the nodes to which you have read-access based on the configured security settings of Microsoft Windows.

Kaspersky Embedded Systems Security contains the following predefined scan scopes:

- **My Computer.** Kaspersky Embedded Systems Security scans all computer:
- **Local hard drives.** Kaspersky Embedded Systems Security scans objects on a computer hard drives. All hard drives, individual disks, folders or files can be included in or excluded from the scan scope.
- **Removable drives.** Kaspersky Embedded Systems Security scans files on external devices, such as CDs or USB drives. All removable disks, individual disks, folders or files can be included in or excluded from the scan scope.
- **Network.** Network folders or files can be added to the scan scope by specifying their path in UNC (Universal Naming Convention) format. The account used to launch the task must have access permissions for the network folders and files added. By default On-Demand Scan tasks run under the system account.
- **System memory.** Kaspersky Embedded Systems Security scans the executable files and modules of the processes running in the operating system when the check is initiated.

- **Startup objects.** Kaspersky Embedded Systems Security scans objects to which register keys and configuration files refer, for example WIN.INI or SYSTEM. INI, as well as the application's modules that are started automatically at computer startup.
- **Shared folders.** You can include shared folders on the protected computer into the scan scope.
- **Virtual drives.** Dynamic folders and files and drives that are connected to the computer can be included in the scan scope, for example, common cluster drives.

By default, you can view and configure predefined scan scopes in the network file resources tree; you can also add predefined scopes to the network file resources list during its formation in the scan scope settings.

By default, On-Demand Scan tasks are run under the following scopes:

- Scan at Operating System Startup task:
 - **Local hard drives**
 - **Removable drives**
 - **System memory**
- Critical Areas Scan:
 - **Local hard drives** (excluding Windows folders)
 - **Removable drives**
 - **System memory**
 - **Startup objects**
- On-Demand Scan tasks:
 - **Local hard drives** (excluding Windows folders)
 - **Removable drives**
 - **System memory**

- **Startup objects**
- **Shared folders**

Virtual drives created using a SUBST command are not displayed in the computer file resource tree in the Kaspersky Embedded Systems Security Console. In order to scan objects on a virtual drive, include the computer folder with which this virtual drive is associated into the scan scope.

Connected network drives will also not be displayed in the computer file resources tree. To include objects on network drives in the scan scope, specify the path to the folder which corresponds to this network drive in UNC format.

Creating a scan scope

If you are remotely managing Kaspersky Embedded Systems Security on the protected computer using Kaspersky Embedded Systems Security Console installed on administrator's workstation, you must be a member of administrators group on the protected computer to be able to view folders on it.

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

If you modify the scan scope in the Scan at system startup and Critical Areas Scan tasks, you can restore the default scan scope in these tasks by restoring Kaspersky Embedded Systems Security itself (**Start** → **Programs** → **Kaspersky Embedded Systems Security** → **Modify or Remove**). In the setup wizard, select the **Restore recommended application settings** check box.

The procedure of creating an On-Demand Scan task scope depends on the network file resources view mode (see section "Configuring view mode for network file resources" on page [101](#)). You can configure network file resources view mode as a tree or as a list (set as default).

► *To create a scan scope working with a network file resources tree, take the following steps:*

1. Expand the **On-Demand Scan** node in the Kaspersky Embedded Systems Security Console tree.
2. Select the subnode corresponding to an On-Demand Scan task that you want to configure.
3. In the details pane of the selected node click the **Configure scan scope** link.

Scan scope settings window opens.

4. In the left section of the window open the network file resources tree to display all the nodes and subnodes.
5. Do the following:
 - To exclude individual nodes from the scan scope, clear the check boxes next to the names of these nodes.
 - To include individual nodes in the scan scope, clear the **My computer** check box and do the following:
 - if all drives of one type are to be included in the protection scope, select the check box opposite the name of the required disk type (for example, to add all removable drives on the computer, select the **Removable drives** check box);
 - if an individual disk of a certain type is to be included in the protection scope, expand the node that contains the list of drives of this type and check the box next to the name of the required drive. For example, in order to select removable drive **F:**, expand node **Removable drives** and check the box for drive **F:**;
 - if you would like to include only a single folder or file on the drive, select the check box next to the name of that folder or file.
6. Click the **Save** button.

Scan scope settings window will be closed. Your newly configured settings have been saved.

► *To create a scan scope using the network file resources list, take the following steps:*

1. Expand the **On-Demand Scan** node in the Kaspersky Embedded Systems Security Console tree.
2. Select the subnode corresponding to an On-Demand Scan task that you want to configure.
3. In the details pane of the selected node click the **Configure scan scope** link.

Scan scope settings window opens.

4. To include individual nodes in the protection scope, clear the **My computer** check box and do the following:

- a. Open the context menu on the scan scope by right-clicking it.
- b. In the context menu of the button, select **Add scan scope**.
- c. In the opened **Add scan scope** window select an object type that you want to add to a scan scope:
 - **Predefined scope** to add one of the predefined scopes on a protected computer. Then in the drop down list select a necessary scan scope.
 - **Disk, folder or network location** to include individual drive, folder or a network object into a scan scope. Then select a necessary scope by clicking the **Browse** button.
 - **File** to include an individual file into scan scope. Then select a necessary scope by clicking the **Browse** button.

You cannot add an object into a scan scope if it has already been added as an exclusion out of the scan scope.

5. To exclude individual nodes from the scan scope, clear the check boxes next to the names of these nodes or take the following steps:
 - a. Open the context menu on the scan scope by right-clicking it.
 - b. In the context menu select **Add exclusion** option.

- c. In the **Add exclusion** window select an object type that you want to add as an exclusion out of the scan scope following the logic of the adding object to a protection scope procedure.
6. To modify the scan scope or an exclusion added, select the **Edit scope** option in the context menu for the necessary scope.
7. To hide the previously added scan scope or an exclusion in the list of network file resources, select the **Remove from the list** option in the context menu for the necessary scope.

The scan scope is excluded out of the Real-Time File Protection task scope on its removal from the network file resources list.

8. Click the **Save** button.

Scan scope settings window will be closed. Your newly configured settings have been saved.

Including network objects in the scan scope

Network drives, folders or files can be added to the scan scope by specifying their path in UNC (Universal Naming Convention) format.

You can scan network folders under the system account.

► *To add a network place to the scan scope, take the following steps:*

1. Expand the **On-Demand Scan** node in the Kaspersky Embedded Systems Security Console tree.
2. Select the On-Demand Scan, the scan scope of which a network path is to be added to.
3. In the details pane of the selected node click the **Configure scan scope** link.

Scan scope settings window opens.

4. Open the drop-down list in the window upper left sector and select **Tree-view**.

5. In the context menu of the name of the **Network** node:
 - Select **Add network folder**, if you want to add a network folder to the scan scope.
 - Select **Add network file**, if you want to add a network file to the scan scope.
6. Enter the path to network folder or file in UNC format and click the **ENTER** key.
7. Select the check box next to the newly added network object to include it in the scan scope.
8. If necessary, change the security settings for the network object added.
9. Click the **Save** button.

The modified task settings are saved.

Creating a virtual scan scope

Dynamic drives, folders, and files can be included in the scan scope in order to create a virtual scan scope.

You can expand the protection / scan scope by adding individual virtual drives, folders, or files only if the protection / scan scope is presented as a tree of file resources (see section "Configuring view mode for network file resources" on page [101](#)).

► *To add a virtual drive to the scan scope, take the following steps:*

1. Expand the **On-Demand Scan** node in the Kaspersky Embedded Systems Security Console tree.
2. Select On-Demand Scan task to create a scan scope for.
3. In the details pane of the selected node click the **Configure scan scope** link.

Scan scope settings window opens.

4. Open the drop-down list in the window upper left sector and select **Tree-view**.
5. In the computer file resource tree open the context menu on the **Virtual drives** node and select the virtual drive name from the list of available names.

6. Check the box next to the drive added in order to include the drive in the scan scope.
7. Click the **Save** button.

The modified task settings are saved.

► *To add a virtual folder or virtual file to the scan scope, and take the following steps:*

1. Expand the **On-Demand Scan** node in the Kaspersky Embedded Systems Security Console tree.
2. Select the On-Demand Scan task in which you wish to create a virtual scan scope.
3. In the details pane of the selected node click the **Configure scan scope** link.

Scan scope settings window opens.

4. Open the drop-down list in the window upper left sector and select **Tree-view**.
5. In the computer file resources tree open the context menu of the node to add a folder or file, and select one of the following options:
 - **Add virtual folder** if you want to add a virtual folder to the protection scope.
 - **Add virtual file** if you want to add a virtual file to the protection scope.
6. In the entry field specify the name of the folder or file.

When specifying the file name, a mask can be used with the special symbols * and ?.

7. In the line with the name of the folder or file created, select the check box to include this folder or file in the scan scope.
8. Click the **Save** button.

The modified task settings are saved.

Security settings of selected node in On-Demand Scan tasks

In the selected On-Demand Scan task, the default values of security settings can be modified by configuring them as common settings for the entire protection or scan scope, or as different settings for different nodes in the computer file resources tree or list.

Security settings configured for the selected parent node are automatically applied to all subnodes. The security settings of the parent node are not applied to subnodes that are configured separately.

The settings for a selected scan scope or protection scope can be configured using one of the following methods:

- Select one of three predefined security levels (**Maximum performance**, **Recommended** or **Maximum protection**).
- Manually change the security settings for the selected nodes in the tree or in the list of the computer's file resources (the security level changes to **Custom**).

A set of node settings can be saved in a template in order to be applied later to other nodes.

Selecting predefined security levels for On-Demand Scan tasks

One of three predefined security levels for a node selected in the computer file resources tree can be applied: **Maximum performance**, **Recommended**, and **Maximum protection**.

Each of these levels contains its own predefined set of security settings (see the table below).

Maximum performance

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

Recommended

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

Maximum protection

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

Table 29. Predefined security levels and corresponding security setting values

Options	Security level		
	Maximum performance.	Recommended	Maximum protection
Scan objects	By format	All objects	All objects
Optimization	Enabled	Disabled	Disabled
Action to be performed on infected and other detected objects	Disinfect, delete if disinfection is impossible	Disinfect, delete if disinfection is impossible (Perform recommended action)	Disinfect, delete if disinfection is impossible
Action to be performed on infected objects	Quarantine	Quarantine (Perform recommended action)	Quarantine
Exclude files	No	No	No
Do not detect	No	No	No
Stop scanning if it takes longer than (sec.)	60 sec.	No	No
Do not scan compound objects larger than (MB)	8 MB	No	No
Scan alternate NTFS streams	Yes	Yes	Yes
Boot sectors of drives and MBR	Yes	Yes	Yes

Options	Security level		
	Maximum performance.	Recommended	Maximum protection
Scan composite objects	<ul style="list-style-type: none"> • SFX archives* • Packed objects* • Embedded OLE-objects* <p>* New and modified objects only</p>	<ul style="list-style-type: none"> • Archives* • SFX archives* • Packed objects* • Embedded OLE-objects* <p>* All objects</p>	<ul style="list-style-type: none"> • Archives* • SFX archives* • Email databases* • Plain mail* • Packed objects* • Embedded OLE-objects* <p>* All objects</p>

The security settings **Use iChecker technology**, **Use iSwift technology**, and **Use Heuristic Analyzer** and **Check Microsoft signature in files** are not included in the settings of preset security levels. If the status of such settings as **Use iChecker technology**, **Use iSwift technology**, **Use heuristic analyzer** is changed, the preset security level that you have selected will not change.

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

1. Expand the **On-Demand Scan** node in the Kaspersky Embedded Systems Security Console tree.
2. Select the subnode that corresponds to the task for which you want to configure security settings.
3. In the details pane of the selected node click the **Configure scan scope** link.

Scan scope settings window opens.

4. In the tree or in the list of the computer network file resources select a node to set the predefined security level.
5. Make sure that the selected node is included in the scan scope.

6. In the right sector of the window, on the **Security level** tab select the security level to be applied.

The window displays the list of security settings corresponding to the security level selected.

7. Click the **Save** button.

Configured task settings are saved and applied immediately to the running task. If the task is not running, the modified settings are applied at next start.

Configuring security settings manually

By default On-Demand Scan tasks use common security settings for the entire scan scope. Their values correspond to those of the **Recommended** predefined security level (see section "**Selecting predefined security levels for On-Demand Scan tasks**" on page [243](#)).

The default values of security settings can be modified by configuring them as common settings for the entire scan scope, or as different settings for different nodes in the computer file resource tree or list.

On working with the computer file resources tree, security settings configured for the selected parental node are automatically applied to all subnodes when working with the network file resources tree. The security settings of the parent node are not applied to subnodes that are configured separately.

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

1. Expand the **On-Demand Scan** node in the Kaspersky Embedded Systems Security Console tree.
2. Select the subnode that corresponds to the task for which you want to configure security settings.
3. In the details pane of the selected node click the **Configure scan scope** link.

Scan scope settings window opens.

4. In the left window section select the node to configure security settings.

A predefined template containing security settings can be applied for a selected node in the scan scope (see section "About templates of security settings" on page [79](#)).

5. Configure the required security settings of the selected node in accordance with your requirements. To do this, perform the following actions:

- On the **General** tab, configure the following settings, if necessary:

In the **Scan objects** section, specify the objects that you want to include in the scan scope:

- **All objects**

Kaspersky Embedded Systems Security scans all objects:

- **Objects scanned by format**

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

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

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

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

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

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

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

- **Boot sectors of drives and MBR**

Enables protection of boot sectors and master boot records.

If the check box is selected, Kaspersky Embedded Systems Security scans boot sectors and master boot records on hard drives and removable drives of the computer.

The check box is selected by default.

- **Alternative NTFS streams**

Scanning of alternative file and folder threads on the NTFS file system drives.

If the check box is selected, Kaspersky Embedded Systems Security scans additional file and folder threads.

The check box is selected by default.

In the **Performance** section, select or clear the check box:

- **Scan only new and modified files**

This check box enables / disables scanning and protection of files that have been recognized by Kaspersky Embedded Systems Security as new or modified since the last scan.

If the check box is selected, Kaspersky Embedded Systems Security scans and protects only the files that it has recognized as new or modified since the last scan.

If the check box is cleared, Kaspersky Embedded Systems Security scans and protects all files.

By default, the check box is selected for the **Maximum performance** security level. If the **Recommended** or **Maximum protection** security level is set, the check box is cleared.

In the **Scan of compound objects** section, specify the compound objects that you want to include in the scan scope:

- **All / Only new archives**

Scanning of ZIP, CAB, RAR, ARJ archives and other archive formats.

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

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

The default value depends on the selected security level.

- **All / Only new SFX archives**

Scanning of archives that contain an extraction module.

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

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

The default value depends on the selected security level.

This option is active when the **Archives** check box is cleared.

- **All / Only new mail databases**

Scanning of Microsoft Outlook and Microsoft Outlook® Express mail database files.

If this check box is selected, Kaspersky Embedded Systems Security scans mail database files.

If this check box is cleared, Kaspersky Embedded Systems Security skips mail database files during scanning.

The default value depends on the selected security level.

- **All / Only new packed objects**

Scanning of executable files packed by binary code packers, such as UPX or ASPack.

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

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

The default value depends on the selected 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 scans files of mail formats.

If this check box is cleared, Kaspersky Embedded Systems Security skips files of mail formats during scanning.

The default value depends on the selected security level.

- **All / Only new embedded OLE objects**

Scanning of objects embedded into files (such as Microsoft Word macros, or email message attachments).

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

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

The default value depends on the selected security level.

You can choose to scan all or only new compound objects if the **Scan only new and modified files** check box is selected. If the **Scan only new and modified files** check box is cleared, Kaspersky Embedded Systems Security scans all of the specified compound objects.

- On the **Actions** tab take the following actions:
 - Select the action to be performed on infected and other detected objects.
 - Select the action to be performed on probably infected objects.
 - If necessary, select actions to be performed depending on the type of detected object.

- Select the actions to perform on immutable containers: select or clear the **Enforce entire parent container deletion in case of infected embedded or other object detection if the container modification is not possible** check box.

This check box enables or disables forced deletion of the parent file container when a malicious child or other object is detected.

If the check box is selected and the action selected to perform on infected and probably infected objects is **Delete**, Kaspersky Embedded Systems Security forcibly deletes the entire parent container when a malicious child or other object is detected. Forceful deletion of a parent container along with all of its contents happens if the application cannot delete only the detected child object (for example, if the parent container is immutable).

If this check box is cleared and the action selected to perform on infected and probably infected objects is **Delete**, Kaspersky Embedded Systems Security does not perform the selected action for the parent container when a malicious child or other object is detected if the parent container is immutable.

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

- On the **Performance** tab, configure the following settings, if necessary:

In the **Exclusions** section:

- **Exclude files**

Excluding files from scanning by file name or file name mask.

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

If this check box is cleared, Kaspersky Embedded Systems Security scans all objects.

The check box is cleared by default.

- **Do not 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 (<http://www.securelist.com>).

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

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

The check box is cleared by default.

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 selected, 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.

The default value is 8 MB.

If the check box is selected, Kaspersky Embedded Systems Security skips compound objects whose size exceeds the specified limit during virus scan.

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

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

- **Using iChecker technology**

Scanning of only new files and those modified since the last scan.

If the check box is selected, Kaspersky Embedded Systems Security scans only new files or those modified since the last scan.

If the check box is cleared, Kaspersky Embedded Systems Security scans files without regard for the date of file creation or modification.

The check box is selected by default.

- **Use iSwift technology**

Scanning of only new files and those modified since the last scan of NTFS system objects.

If the check box is selected, Kaspersky Embedded Systems Security scans only new files or those modified since the last scan of NTFS system objects.

If the check box is cleared, Kaspersky Embedded Systems Security scans NTFS system files without regard for the date of file creation or modification.

The check box is selected by default.

6. Click the **Save** button.

Your newly configured settings have been saved.

Removable Drives Scan

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

Kaspersky Embedded Systems Security scans USB removable drives using the On-Demand Scan task (see section "About On-Demand Scan tasks" on page [220](#)). The application automatically creates a new On-Demand Scan task when the removable drive is connected and deletes the task after the scanning is completed. The created task is performed with the predefined security level defined for removable drive scanning. You cannot configure the settings of the temporary On-Demand Scan task.

If you installed Kaspersky Embedded Systems Security without anti-virus databases, the removable drives scan will be unavailable.

Kaspersky Embedded Systems Security scans connected removable USB drives when they are registered as USB mass storage devices in the operating system. The application does not scan a removable drive if the connection is blocked by the Device Control task. The application does not scan MTP-connected mobile devices.

Kaspersky Embedded Systems Security allows access to removable drives during scanning.

Scan results for each removable drive are available in the log for the On-Demand Scan task created upon connection of the removable drive.

You can change the settings of the Removable Drives Scan component (see the table below).

Table 30. 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	<p>You can reduce the component's scope by setting the maximum volume of data on the scanned drive.</p> <p>Kaspersky Embedded Systems Security does not perform removable drive scanning if the volume of stored data exceeds the specified value.</p>
Scan with security level	Maximum protection	<p>You can configure the created On-Demand Scan tasks by selecting one of three security levels:</p> <ul style="list-style-type: none"> • Maximum protection • Recommended • Maximum performance <p>The actions taken for infected, probably infected and other objects, as well as the other scan settings for each security level correspond to the preset security levels for On-Demand Scan tasks (see section "Selecting preset security levels for On-Demand Scan tasks" on page 243).</p>

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

1. In the Kaspersky Embedded Systems Security Console tree, open the context menu of the **Kaspersky Embedded Systems Security** node and select the **Removable Drives Scan** item:

The **Removable Drives Scan** window opens.

2. In the **Scan on connection** section do the following:
 - Select the **Scan removable drives on connection via USB** check box, if you want Kaspersky Embedded Systems Security to automatically scan removable drives when they are connected.
 - If required, select the **Scan removable drive if its stored data volume does not exceed (MB)** and specify the maximum value in the field on the right.
 - In the **Scan with security level** drop-down list specify the security level with the settings that are required for removable drives scanning.
3. Click **OK**.

The specified settings are saved and applied.

Creating an On-Demand Scan task

Custom tasks can be created in the **On-Demand Scan** node. In the other functional components of Kaspersky Embedded Systems Security creation of custom tasks is not provided for.

► *To create a new On-Demand Scan task, take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, open the context menu of the **On-Demand Scan** node.

2. Select **Add task**.

The **Add task** window opens.

3. Enter the following information about the task:

- **Name** – task name of no more than 100 characters, may contain any symbols apart from % ? | \ | / : * < >.

You cannot save a task or configure a new task on the **Schedule**, **Advanced** and **Run as** if the task name is not specified.

- **Description** - any additional information about the task, no more than 2000 characters. This information will be displayed in the task properties window.

4. Configure the following task settings, if necessary:

5. On the **General** tab:

- **Use heuristic analyzer**

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

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

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

The check box is selected by default.

- **Perform task in background mode**

The check box modifies the priority of the task.

If the check box is selected, the task priority in the operating system is reduced. The operating system provides resources for performing the task depending on the load on the CPU and the computer file system from other Kaspersky Embedded Systems Security tasks and applications. As a result, task performance will slow down during increased loads and will speed up at lower loads.

If the check box is cleared, the task will start and run with the same priority as the other Kaspersky Embedded Systems Security tasks and other applications. In this case, the speed of task execution increases.

The check box is cleared by default.

- **Apply Trusted Zone**

This check box enables / disables use of the Trusted Zone for a task.

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

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

The check box is selected by default.

- **Consider task as critical areas scan**

The check box changes the task priority: enables or disables logging of the *Critical Areas Scan* event and refreshing of the protection computer status. The check box is not available in the properties of local system and custom tasks of Kaspersky Embedded Systems Security. You can edit this setting 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.

- **Use KSN for protection**

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 Real-Time File Protection task does not use KSN service.

The check box is selected by default.

- On the **Schedule** and **Advanced** tabs:
 - Scheduled task launch settings (see section "Configuring the task launch schedule settings" on page [70](#)).
- On the **Run as** tab:
 - Task launch settings with account permissions (see section "Specifying a user account for running a task" on page [73](#)).

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

A new custom On-Demand Scan task is created. A node with the name of the new task is displayed in the Console tree. The operation is registered in the system audit log (see section "System audit log" on page [309](#)).

7. If required, in the details pane of the selected node, open the **Configure scan scope** tab.

Do the following:

- In the computer file resources tree, select the nodes that you want to include in the scan scope.
- Select one of the predefined security levels (see section "Selecting predefined security levels for On-Demand Scan tasks" on page [243](#)) or configure the scan settings manually (see section "Configuring security settings manually" on page [247](#)).

8. In the context menu of the name of the selected task, select **Save task**.

A custom On-Demand Scan task is created. The configured settings are applied at the next task start.

Removing tasks

In the Kaspersky Embedded Systems Security Console, you can remove only custom On-Demand Scan tasks. You cannot delete system or group tasks.

► *To delete a task, take the following steps:*

1. Expand the **On-Demand Scan** node in the Kaspersky Embedded Systems Security Console tree.
2. Open the context menu of the name of the custom task that you want to delete.
3. Select **Remove task**.
A window opens to confirm the operation.
4. Click **Yes** to confirm the deletion.

The task status will be deleted, and the operation will be registered into the system audit log.

Renaming tasks

In Kaspersky Embedded Systems Security Console, you can rename only custom On-Demand Scan tasks. System or group tasks cannot be renamed.

► *To rename a task, take the following steps:*

1. Expand the **On-Demand Scan** node in the Kaspersky Embedded Systems Security Console tree.
2. Open the context menu of the name of the custom task that you want to rename.
3. Select **Properties**.
The **Task settings** window opens.
4. In the window that opens, enter the new task name in the **Name** field.
5. Click **OK**.

The task will be renamed. The operation will be logged in the system audit log.

Updating Kaspersky Embedded Systems Security bases and software modules

This section provides information about databases and software modules update tasks of Kaspersky Embedded Systems Security, copying updates and rolling back databases updates of Kaspersky Embedded Systems Security, as well as instructions on how to configure databases and software modules update tasks.

In this section

About Update tasks.....	262
About Kaspersky Embedded Systems Security software modules update	264
About Kaspersky Embedded Systems Security database update	265
Schemes for updating databases and modules of anti-virus applications used within an organization	266
Configuring Update tasks	271
Rolling back Kaspersky Embedded Systems Security database updates.....	280
Rolling back application module updates	280
Update task statistics	280

About Update tasks

Kaspersky Embedded Systems Security provides four system update tasks: Database Update, Software Modules Update, Copying Updates, and Rollback of Database Update.

By default Kaspersky Embedded Systems Security connects to the updates source (one of Kaspersky Lab's update computers) every hour, by automatically detecting proxy computer settings in the network, and by not authenticating on access to the proxy computer.

You can configure all Update tasks (see section "Configuring Update tasks" on page [271](#)), except for the Rollback of Database Update task. When task settings are modified, Kaspersky Embedded Systems Security will apply the new values at the next task launch.

You are not allowed to pause and resume Update tasks.

Database Update

By default, Kaspersky Embedded Systems Security copies databases from the update source to the protected computer and immediately starts using them in the running Real-Time Protection task. The On-Demand Scan tasks start using the updated database at the next launch.

By default, Kaspersky Embedded Systems Security runs the Database Update task every hour.

Software Modules Update

By default, Kaspersky Embedded Systems Security copies updates of its software modules from the updates source to the protected computer and installs them. In order to start using installed software modules, a computer restart and / or a restart of Kaspersky Embedded Systems Security may be required.

By default, Kaspersky Embedded Systems Security runs the Software Modules Update task on a weekly basis on Fridays at 04:00 PM (time according to the regional settings of the protected computer). During task execution, the application checks for availability of important and scheduled updates of Kaspersky Embedded Systems Security modules without distributing them.

Copying Updates

By default, during task execution, Kaspersky Embedded Systems Security downloads Database Update and Software Modules Update files and saves them to the specified network or local folder without applying them.

The Copying Updates task is disabled by default.

Rollback of Database Update

During task execution, Kaspersky Embedded Systems Security returns to using databases with previously installed updates.

The Rollback of Database Update task is disabled by default.

About Kaspersky Embedded Systems Security software modules update

Kaspersky Lab can issue update packages for Kaspersky Embedded Systems Security modules. The update packages can be *urgent* (or *critical*) and *planned*. Critical update packages repair vulnerabilities and errors; planned packages add new features or enhance existing features.

Urgent (critical) update packages are uploaded to Kaspersky Lab's update servers.

Their automatic installation can be configured using the Software Modules Update task. By default, Kaspersky Embedded Systems Security runs the Software Modules Update task on a weekly basis on Fridays at 04:00 PM (time according to the regional settings of the protected computer).

Kaspersky Lab does not publish planned update packages on its update servers for automatic update; these can be downloaded from the Kaspersky Lab website. The Software Modules Update task can be used to receive information about the release of scheduled Kaspersky Embedded Systems Security updates.

Critical updates can be updated from the Internet to each protected computer, or one computer can be used as intermediary by copying all updates onto it and then distributing them to the network computers. In order to copy and save updates without installing them use the Copying Updates task.

Before updates of modules are installed Kaspersky Embedded Systems Security creates backup copies of the previously installed modules. If the software modules updating process is interrupted or results in an error, Kaspersky Embedded Systems Security will automatically return to using the previously installed software modules. Software modules can be rolled back manually to the previously installed updates.

During the installation of downloaded updates the Kaspersky Security Service service automatically stops and then restarts.

About Kaspersky Embedded Systems Security Database Updates

Kaspersky Embedded Systems Security databases stored on the protected computer quickly become outdated. Kaspersky Lab's virus analysts detect hundreds of new threats daily, create identifying records for them, and include them in application database updates. Database updates are a file or set of files containing records that identify threats discovered during the time since the last update was created. To maintain the required level of computer protection, we recommend that database updates are received regularly.

By default, if the Kaspersky Embedded Systems Security databases are not updated within a week from the time at which the installed database updates were last created, the *Databases out of date* event occurs. If the databases are not updated for a period of two weeks, the *Databases are obsolete* event occurs. Information about the up-to-date status of the databases is displayed in the **Kaspersky Embedded Systems Security** node of the Console tree (see section "Viewing protection status and Kaspersky Embedded Systems Security information" on page [28](#)). You can use Kaspersky Embedded Systems Security general settings to indicate a different number of days before these events occur. You can also configure administrator notifications about these events (see section "Configuring administrator and user notifications" on page [330](#)).

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

Updates can be downloaded to every protected computer, or one computer can be used as intermediary by copying all updates onto it and then distributing them to the computers. If you use Kaspersky Security Center for centralized administration of protection of computers

in an organization, you can use Kaspersky Security Center Administration Server as an intermediary for downloading updates.

Database Update tasks can be started manually or based on a schedule (see section "Configuring the task launch schedule settings" on page [70](#)). By default, Kaspersky Embedded Systems Security runs the Database Update task every hour.

If the update downloading process is interrupted or results in an error Kaspersky Embedded Systems Security will automatically switch back to using the databases with the last installed updates. If the Kaspersky Embedded Systems Security databases become corrupted, they can be manually rolled back to previously installed updates (see section "Rolling back Kaspersky Embedded Systems Security Database Updates" on page [280](#)).

Schemes for updating databases and modules of anti-virus applications used within organization

Selection of updates source in the update tasks depends on the databases and program modules update scheme used in the organization.

Kaspersky Embedded Systems Security databases and modules can be updated on the protected computers using the following schemes:

- Download updates directly from the Internet to each protected computer (Scheme 1).
- Download updates from the Internet to an intermediary computer and distribute updates to computers from the computer.

Any computer with the software listed below installed can serve as an intermediary computer:

- Kaspersky Embedded Systems Security (one of the protected computers) (Scheme 2).
- Kaspersky Security Center Administration Server (Scheme 3).

Updating using an intermediary computer will not only allow Internet traffic to be decreased, but will also ensure additional network computers security.

Description of update schemes listed is provided below.

Scheme 1. Updating directly from the Internet

- ▶ *To configure Kaspersky Embedded Systems Security updates directly from the Internet:*

on each protected computer in the settings of the Database Update task and the Software Modules Update task, specify Kaspersky Lab's update computers as the source of updates.

Other HTTP or FTP servers which have an update folder can be configured as the updates source.

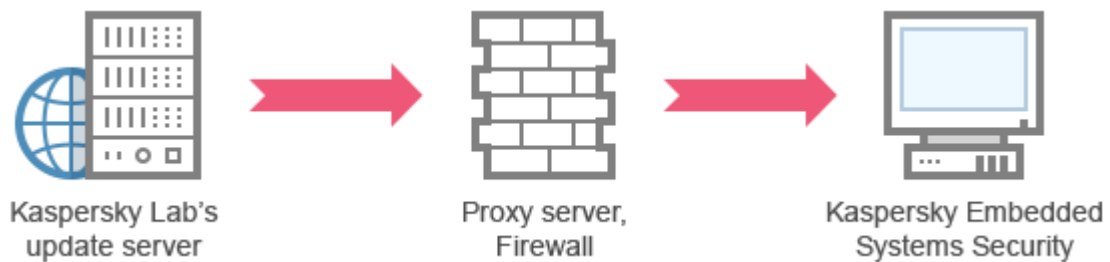


Figure 1. Schemes for updating databases and application modules

Scheme 2. Updating via one of the protected computers

- ▶ *To configure Kaspersky Embedded Systems Security updates via one of the protected computers:*

1. Copy updates to the selected protected computer. To do this, perform the following actions:
 - Configure the Copying Updates task settings on the selected computer:
 - a. Specify Kaspersky Lab's update computers as the updates source.
 - b. Specify a shared folder to be used as the folder where updates are saved.

2. Distribute updates to other protected computers. To do this, perform the following actions:

- On each protected computer, configure the settings for the Database Update task and the Software Modules Update task (see the figure below).
 - a. For the update source, specify a folder on the intermediary computer's drive to which updates will be downloaded.

Kaspersky Embedded Systems Security will obtain updates via one of the protected computers.

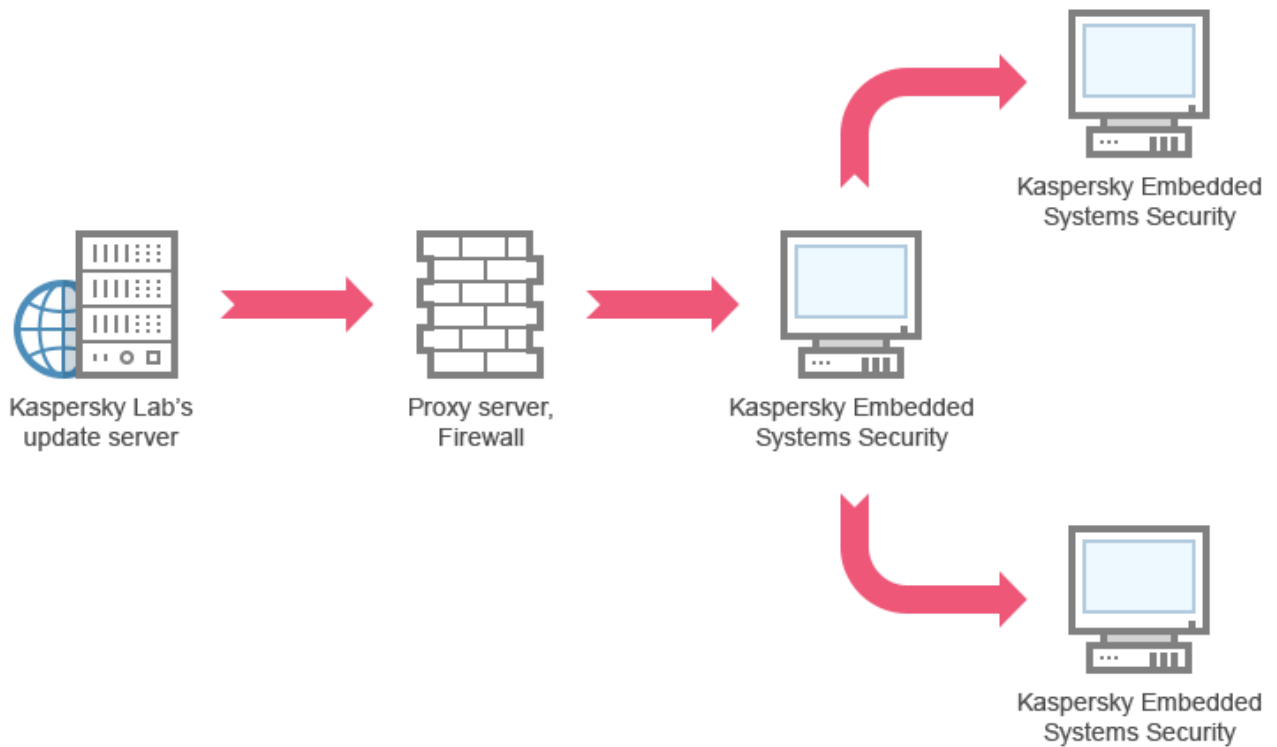


Figure 2. Updating via one of the protected servers

Scheme 3. Updating via Kaspersky Security Center Administration Server

If the Kaspersky Security Center application is used for the centralized administration of Anti-Virus computer protection, updates can be downloaded via the Kaspersky Security Center Administration Server installed in the local area network (see figure below).

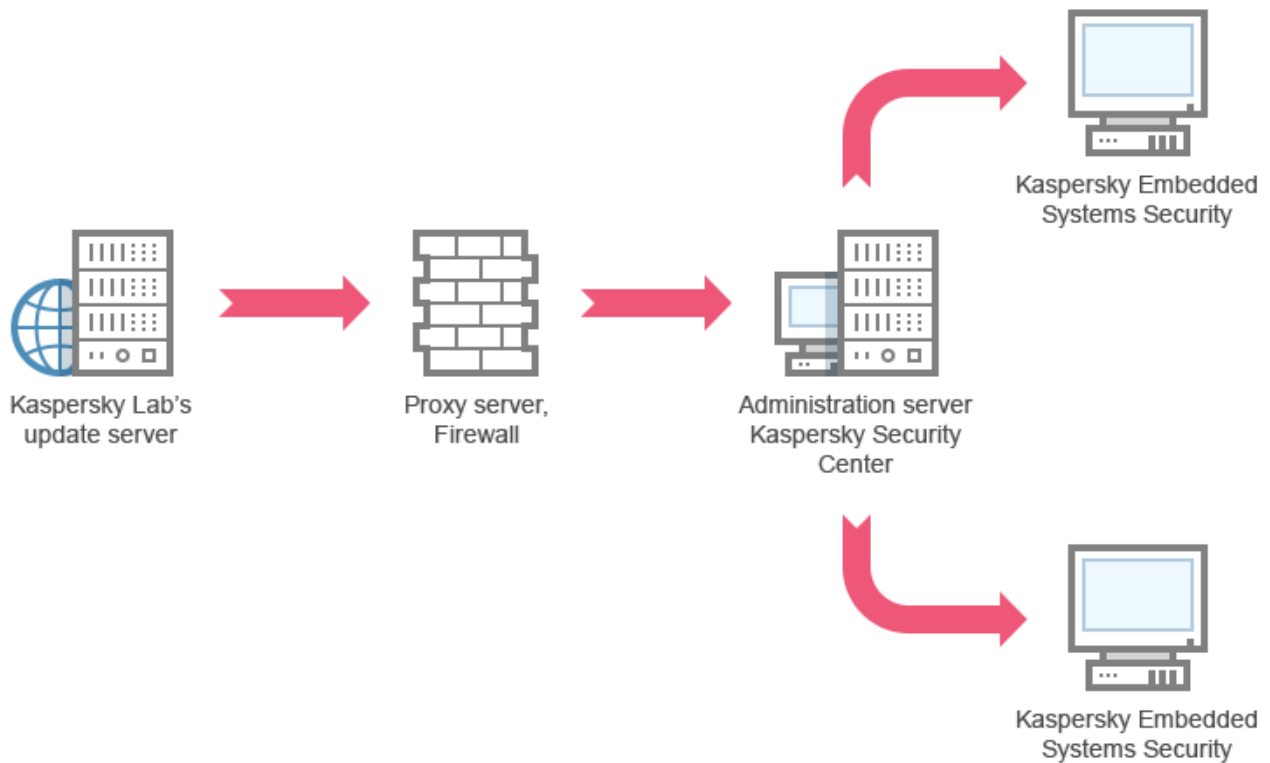


Figure 3. Updating via Kaspersky Security Center Administration Server

► *To configure Kaspersky Embedded Systems Security updates via the Kaspersky Security Center Administration Server:*

1. Download updates from Kaspersky Lab's update servers to Kaspersky Security Center Administration Server. To do this, perform the following actions:
 - Configure the Retrieve updates by Administration Server task for the specified set of computers:
 - a. Specify Kaspersky Lab's update servers as the updates source.

2. Distribute updates to protected computers. To do so, perform one of the following actions:

- On the Kaspersky Security Center configure an Anti-Virus database (application module) update group task to distribute updates to protected computers:
 - a. In the task schedule specify **After Administration Server has retrieved updates** as start frequency.

Administration Server will start the task each time it receives updates (recommended method).

The start frequency of **After Administration Server has retrieved updates** cannot be specified in the Kaspersky Embedded Systems Security Console.

- On each protected computer, configure the Database Update task and the Software Modules Update task:
 - a. Specify the Kaspersky Security Center Administration Server as the update source.
 - b. Configure the task schedule if necessary.

If Kaspersky Embedded Systems Security anti-virus databases are rarely updated (from once a month to once a year), the likelihood of detecting threats decreases and the frequency of false alarms raised by application components increases.

Kaspersky Embedded Systems Security will obtain updates via the Kaspersky Security Center Administration Server.

If you plan to use Kaspersky Security Center administration server for updates distribution, install Network Agent, an application component included in the Kaspersky Security Center distribution kit, onto each of the protected computers. This ensures interaction between the Administration Server and Kaspersky Embedded Systems Security on the protected computer.

Detailed information about the Network Agent and its configuration using

Kaspersky Security Center is provided in the *Administrator's Guide for Kaspersky Security Center*.

Configuring Update tasks

This section provides instructions on how to configure Kaspersky Embedded Systems Security update tasks.

In this section

Configuring the settings for working with Kaspersky Embedded Systems Security update sources	271
Optimizing the use of the disk I/O when running the Database Update task.....	275
Configuring Copying updates task settings.....	276
Configuring Software Modules Update task settings	278

Configuring settings for working with Kaspersky Embedded Systems Security update sources

For each update task except the Rollback of Database Update task, you can specify one or several update sources, add user-defined update sources, and configure the settings for connection with the specified sources.

After update task settings are modified, the new settings will not be immediately applied in the running update tasks. The configured settings will be applied only when the task is restarted.

► *To specify the type of update source take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Update** node.
2. Select the subnode corresponding to the update task that you want to configure.
3. Click the **Properties** link in the details pane of the selected node.

The **Task settings** window opens on the **General** tab.

4. In the **Update source** section, select the type of Kaspersky Embedded Systems Security update source:

- **Kaspersky Security Center Administration Server**

Kaspersky Embedded Systems Security uses Kaspersky Security Center Administration Server as the update source.

You can only select this option if Kaspersky Lab applications on your network are administered using the Kaspersky Security Center remote access system and if Network Agent – the Kaspersky Security Center component that provides the connection between computers and Administrator Server – is installed on the protected computer.

- **Kaspersky Lab update servers**

Kaspersky Embedded Systems Security uses Kaspersky Lab websites as update sources, hosting updates for the databases and software modules of all of the company's products.

This option is selected by default.

- **Custom HTTP or FTP servers, or network folders**

Kaspersky Embedded Systems Security uses the administrator-specified HTTP or FTP computers or folders on local network computers as the update source.

You can create a list of sources with the current updates by clicking the **Custom HTTP or FTP servers, or network folders** link.

5. If required, configure the advanced settings for user-defined update sources:

- a. Click on the **Custom HTTP or FTP servers, or network folders** link.

- i. In the **Update servers** window that opens, select or clear the check boxes next to the user-defined update sources in order to begin or terminate their use.
- ii. Click **OK**.

- b. In the **Update source** section on the **General** tab, select or clear the **Use Kaspersky Lab update servers if specified servers are not available**.

This check box enables or disables the option of using Kaspersky Lab update computers as the update source if the user-defined update sources are unavailable.

If the check box is selected, this function is enabled.

The check box is selected by default.

You can select the **Use Kaspersky Lab update servers if specified servers are not available** check box when the **Custom HTTP or FTP servers, or network folders** option is enabled.

6. In the **Task settings** window, select the **Connection settings** tab to configure the settings for connecting to update sources:

Do the following:

- Clear or select the **Use passive FTP mode if possible** check box.

The check box enables or disables the option that lets you download updates from FTP servers in passive connection mode.

If the check box is selected, the connection is established in passive mode.

If the check box is cleared, the connection is established in standard mode.

The check box is selected by default.

- If necessary, specify the timeout period (seconds).

In the **Update source connection settings**:

- Clear or select the **Use proxy server settings for connecting to Kaspersky Lab update servers** check box.

The check box enables / disables the use of proxy server settings if updates are received from Kaspersky Lab servers or if the **Use Kaspersky Lab update servers if specified servers are not available** check box is selected.

If the check box is selected, the proxy server settings are used.

If the check box is cleared, the proxy server settings are not used.

The check box is cleared by default.

- Clear or select the **Use proxy server settings to connect to other servers** check box.

The check box enables or disables the use of proxy computer settings if the option **Custom HTTP or FTP servers, or network folders** is selected as the update source.

If the check box is selected, the proxy server settings are used.

The check box is cleared by default.

7. Click **OK**.

The configured settings for the Kaspersky Embedded Systems Security update source will be saved and applied at the next task start.

You can manage the list of user-defined Kaspersky Embedded Systems Security update sources.

► *To edit the list of user-defined application update sources:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Update** node.
2. Select the subnode corresponding to the update task that you want to configure.
3. Click the **Properties** link in the details pane of the selected node.

The **Task settings** window opens on the **General** tab.

4. Click on the **Custom HTTP or FTP servers, or network folders** link.

The **Update servers** window opens.

5. Do the following:

- To add a new user-defined update source, in the entry field specify the address of the folder containing update files on the FTP or HTTP server; specify a local or network folder in the UNC (Universal Naming Convention) format. Press **ENTER**.

By default, the added folder is used as the source of updates.

- To disable use of a user-defined source, clear the check box next to the source in the list.
- To enable use of a user-defined source, select the check box next to the source in the list.
- In order to change the order in which Kaspersky Embedded Systems Security accesses user-defined files, use the **Move Up** and **Move Down** buttons to move the selected source to the beginning or to the end of the list, depending on whether it is to be used before or after other sources.
- To change the path to the user-defined source, select the source in the list and click the **Edit** button, make the required changes in the entry field and press the **ENTER** key.
- To remove a user-defined source, select it in the list and press the **Remove** button.

You cannot delete the only remaining user-defined source from the list.

6. Click **OK**.

The changes in the list of user-defined application update sources will be saved.

Optimizing use of disk I/O when running Database Update task

When running the Database Update task, Kaspersky Embedded Systems Security stores update files on the local disk of the computer. You can lower the workload on the disk I/O subsystem of the computer through storing update files on a virtual drive in the RAM when running the update task.

► *To lower the workload on your computer's disk I/O subsystem during Database Update task, take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Update** node.
2. Select the **Database Update** subnode.
3. Click the **Properties** link in the details pane of the **Database Update** node.
4. The **Task settings** window opens on the **General** tab.
5. In the **Disk I/O usage optimization** section, define the following settings:

- Clear or select the **Lower the load on the disk I/O** check box.

This check box enables or disables the feature of the disk subsystem optimization through storing update files on a virtual drive in the RAM.

If the check box is selected, this function is enabled.

The check box is cleared by default.

- In the **RAM used for optimization** field, specify the RAM volume (in MB).
The operating system temporarily allocates the specified RAM volume to store update files while running the task. The default RAM size is 512 MB.

6. Click **OK**.

The configured settings will be saved and applied at the next task start.

Configuring Copying Updates task settings

► *To configure the Copying Updates task:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Update** node.
2. Select the **Copying Updates** subnode.
3. Click the **Properties** link in the details pane of the **Copying Updates** node.

The **Task settings** window opens.

4. On the **General** and **Connection settings** tabs, configure the settings for working with update sources (see section "Configuring the settings for working with Kaspersky Embedded Systems Security update sources" on page [271](#)).
5. On the **General** tab in the **Copying Updates settings** section:
 - Specify the conditions for Copying Updates:
 - **Copy database updates.**

Kaspersky Embedded Systems Security downloads only software database updates.

This option is selected by default.
 - **Copy critical software modules updates.**

Kaspersky Embedded Systems Security downloads only urgent Kaspersky Embedded Systems Security software module updates.
 - **Copy database updates and critical software modules updates.**

Kaspersky Embedded Systems Security downloads software database updates and critical software module updates of Kaspersky Embedded Systems Security.
 - Specify the local or network folder to which Kaspersky Embedded Systems Security will be distributing downloaded updates.
6. On the **Schedule** and **Advanced** tabs configure the task launch schedule (see section "Configuring the task launch schedule settings" on page [70](#)).
7. On the **Run as** tab, configure the task to launch using account permissions (see section "Specifying a user account for running a task" on page [73](#)).
8. Click **OK**.

The configured settings will be saved and applied at the next task start.

Configuring Software Modules Update task settings

► To configure the Software Modules Update task:

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Update** node.
2. Select the **Software Modules Update** subnode.
3. Click the **Properties** link in the details pane of the **Software Modules Update** node.

The **Task settings** window opens.

4. On the **General** and **Connection settings** tabs, configure the settings for working with update sources (see section "Configuring the settings for working with Kaspersky Embedded Systems Security update sources" on page [271](#)).
5. On the **General** tab in the **Application update settings** section, configure the settings for updating application modules:

- **Only check for critical software updates available**

Kaspersky Embedded Systems Security displays a notification about urgent updates to software modules available in the update source without downloading the updates. The notification is displayed if notifications about events of this type are enabled.

This option is selected by default.

- **Copy and install critical software modules updates**

Kaspersky Embedded Systems Security downloads and installs critical updates to software modules.

- **Allow operating system restart**

The operating system is restarted after installing updates that require a restart.

If the check box is selected, Kaspersky Embedded Systems Security reboots the operating system after installing updates that require a reboot.

This check box is active if the **Copy and install critical software modules updates** option is selected.

The check box is cleared by default.

- **Receive information about available updates to software modules**

Notifications about all scheduled updates to Kaspersky Embedded Systems Security software modules available in the update source are displayed. Kaspersky Embedded Systems Security displays a notification if notifications are enabled for events of this type.

If the check box is selected, Kaspersky Embedded Systems Security displays a notification about all scheduled updates to software modules available in the update source.

The check box is selected by default.

6. On the **Schedule** and **Advanced** tabs configure the task launch schedule (see section "Configuring the task launch schedule settings" on page [70](#)). By default, Kaspersky Embedded Systems Security runs the Software Modules Update task on a weekly basis on Fridays at 04:00 PM (time according to the regional settings of the protected computer).
7. On the **Run as** tab, configure the task to launch using account permissions (see section "Specifying a user account for running a task" on page [73](#)).
8. Click **OK**.

The configured settings will be saved and applied at the next task start.

Kaspersky Lab does not publish planned update packages on the update servers for automatic installation; these can be downloaded manually from the Kaspersky Lab website.

Administrator notification about the *New scheduled update of application software modules is available* event can be configured; this will contain the URL of the page on the website from which scheduled updates can be downloaded.

Rolling back Kaspersky Embedded Systems Security database updates

Before database updates are applied, Kaspersky Embedded Systems Security creates backup copies of the previously used databases. If the update has been interrupted or has resulted in an error, Kaspersky Embedded Systems Security will automatically return to using the previously installed databases.

If any problems arise after you have updated the databases, they can be rolled back to the previously installed updates through the Rollback of Database Update task.

► *To start the Rollback of Database Update task:*

click the **Start** link in the details pane of the **Rollback of Database Update** node.

Rolling back application module updates

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

Before applying updates of software modules, Kaspersky Embedded Systems Security creates backup copies of the modules currently in use. If the modules updating process has been interrupted or has resulted in an error, Kaspersky Embedded Systems Security will automatically return to using modules with the latest installed updates.

In order to roll back the software modules use the Microsoft Windows component **Install and delete applications**.

Update task statistics

While the update task is running, real-time information can be viewed about the amount of data downloaded since the task has been launched until the present moment, and also other task execution statistics.

When the task is completed or stopped, you can view this information in the task log (see section "Viewing statistics and information about a Kaspersky Embedded Systems Security task using logs" on page [315](#)).

► *To view update task statistics take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Update** node.
2. Select the subnode that corresponds to the task whose statistics you want to view.

Task statistics are displayed in the **Statistics** section of the details pane of the selected node.

If you are viewing the Database Update task or the Copying Updates task the **Statistics** block shows the volume of data downloaded by Kaspersky Embedded Systems Security on the present moment (**Received data**).

If you are viewing the Software Modules Update task, you will see the information described in the following table.

Table 31. Information about the Software Modules Update task

Field	Description
Received data	Total amount of downloaded data
Available critical updates	Number of critical updates available for installation
Available scheduled updates	Number of planned updates available for installation
Errors applying updates	If the value of this field is non-zero, the update was not applied. The name of the update, which caused an error during its application, can be viewed in the task log (see section "Viewing statistics and information about a Kaspersky Embedded Systems Security task using logs" on page 315).

Objects isolating and backup copying

This section provides information about backing up of the detected malicious objects before they are disinfected or removed, and information about quarantining of the probably infected objects.

In this section

Isolating probably infected objects. Quarantine	282
Making backup copies of objects. Backup	297

Isolating probably infected objects. Quarantine

This section describes how to isolate probably infected objects by quarantining them and how to configure Quarantine settings.

In this section

About quarantining of probably infected objects	283
Viewing Quarantine objects.....	284
Quarantine Scan	286
Restoring objects from quarantine.....	288
Moving objects to Quarantine.....	292
Deleting objects from quarantine.....	292
Sending probably infected objects to Kaspersky Lab for analysis.....	293
Configuring Quarantine settings	294
Quarantine statistics.....	296

About quarantining of probably infected objects

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

Viewing Quarantine objects

Quarantined objects can be viewed in the **Quarantine** node of the Kaspersky Embedded Systems Security Console.

► *To view quarantined objects, take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Storages** node.
2. Select the **Quarantine** subnode.

Information about quarantined objects is displayed in the details pane of the selected node.

► *To find the required object in the list of Quarantined objects,*

sort the objects (see section "Sorting quarantined objects" on page [284](#)) or filter the objects (see section "Filtering quarantined objects" on page [285](#)).

Sorting quarantined objects

By default, objects in the list of quarantined objects are sorted by date of quarantining in reverse chronological order. To find the desired object you may sort objects by columns with information about the objects. Sorted results will be saved if you close and then re-open the **Quarantine** node, or if you close Kaspersky Embedded Systems Security Console, save the msc file and then re-open it from this file.

► *To sort objects, take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Storages** node.
2. Select the **Quarantine** subnode.

3. In the details pane of the **Quarantine** node, select the column heading that you wish to use to sort objects in the list.

Objects in the list will be sorted based on the selected setting.

Filtering quarantined objects

To find the required quarantined object you can filter objects in the list - display only those objects that satisfy the filtering criteria (filters) that you specify. Filtered results are saved if you leave and then reopen the Quarantine node or if you close Kaspersky Embedded Systems Security Console, save the msc file and then reopen it from this file.

► *To specify one or multiple filters, take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Storages** node.
2. Select the **Quarantine** subnode.
3. Select **Filter** in the context menu of the node's name.

The **Filter settings** window opens.

4. To add a filter, perform the following steps:
 - a. In the **Field name** select a file to which the filter value will be compared.
 - b. In the **Operator** list select the filtering condition. The values of the filtering conditions in the list may differ depending on the value you have selected in the **Field name** list.
 - c. Enter the filter value in the **Field value** field or select it from the list.
 - d. Click the **Add** button.

The filter you have added will appear in the list of filters in the **Filter settings** window.

Repeat steps a-d for each filter you add. Use the following guidelines while working with filters:

- To combine multiple filters using the logical operator "AND", select **If all conditions are met**.

- To combine multiple filters using the logical operator "OR", select **If any condition is met**.
- In order to delete a filter, select the filter you wish to delete in the filter list, and click the **Remove** button.
- In order to edit a filter, select the filter in the list in the **Filter settings** window. Then change the required values in the **Field name**, **Operator** or **Field value** fields and click the **Replace** button.

5. After all filters have been added, click the **Apply** button.

The created filters will be saved.

- ▶ *In order to re-display all objects in the list of quarantined objects,*
select **Remove filter** in the context menu of the name of the **Quarantine** node.

Quarantine Scan

By default, after each database update, Kaspersky Embedded Systems Security performs the Quarantine Scan system task. Task settings are described in the table below. The Quarantine Scan task settings cannot be modified.

You can configure the task launch schedule (see section "Configuring the task launch schedule settings" on page [70](#)), start it manually, and modify the permissions of the account (see section "Specifying a user account for running a task" on page [73](#)) used to start the task.

Having scanned Quarantine objects after updating the databases, Kaspersky Embedded Systems Security can reclassify some of them as not infected: the status of such objects is changed to **False alarm**. Other objects can be reclassified as infected, in which case Kaspersky Embedded Systems Security handles such objects as specified by the Quarantine Scan: disinfect, or delete if disinfection failed On-Demand Scan task settings.

Table 32. Quarantine Scan task settings

Quarantine Scan task setting	Value
Scan scope	Quarantine folder
Security settings	Common for the entire scan area; their values are provided in the next table

Table 33. Scan settings in the Quarantine Scan task

Security setting	Value
Scan objects	All objects included into scan scope
Optimization	Disabled
Action to be performed with infected and other detected objects	Disinfect, delete if disinfection is impossible
Action to be performed on infected objects	Skip
Exclude objects	No
Do not detect	No
Stop scan if takes longer than (sec)	Not configured
Do not scan compound objects larger than (MB)	Not configured
Scan alternate NTFS streams	Enabled
Boot sectors of drives and MBR	Disabled
Using iChecker technology	Disabled
Using iSwift technology	Disabled

Security setting	Value
Scan composite objects	<ul style="list-style-type: none"> • Archives* • SFX archives* • Packed objects* • Embedded OLE-objects* <p>* Scan only new and modified files is disabled.</p>
Checking files for Microsoft signatures	Not performed
Use heuristic analyzer	Enabled with Deep analysis level
Trusted zone (see page 57)	Not applied

Restoring quarantined objects

Kaspersky Embedded Systems Security places probably infected objects into the quarantine folder in encrypted form to shield the protected computer against their possible harmful effect.

You can restore any object from the quarantine. This may be required in the following cases:

- If after the quarantine scan using the updated database the status of the object changed to **False alarm** or **Disinfected**.
- If you consider the object harmless for the computer and wish to use it. If you do not wish Kaspersky Embedded Systems Security to isolate this object during the subsequent scans you can exclude this object from the processing in the Real-Time File Protection task and in the On-Demand Scan tasks. To do this, specify the object as the value of the **Exclude objects** (by filename) or **Do not detect** security setting in those tasks, or add it to the trusted zone (see section "Configuring the Trusted Zone" on page [57](#)).

When you restore objects you can select where the object being restored will be saved to: original location (by default), special folder for restored objects on the protected computer or custom folder on computer where Kaspersky Embedded Systems Security console is installed or on another computer in the network.

The Restore to folder is used for storing restored objects on the protected computer.

You can configure special security settings for it to be scanned. The path to this folder is set by the Quarantine settings.

Restoring objects from the quarantine may lead to computer infection.

You can restore the object and save its copy in the quarantine folder to use it later, for example in order to rescan the object after the database has been updated.

If a quarantined object was contained in a composite object (for example in an archive), Kaspersky Embedded Systems Security will not include into this composite object during the restoration, rather it will save separately into a selected folder.

You can restore one or several objects.

► *To restore quarantined objects, perform the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Storages** node.
2. Select the **Quarantine** subnode.
3. Perform one of the following actions in the details pane of the **Quarantine** node:
 - To restore one object, select **Restore** from the context menu of the object that you want to restore.
 - To restore multiple objects select the objects you wish to restore using the **CTRL** or **SHIFT** key, right-click one of the selected objects and select **Restore** from the context menu.

The **Restore object** window opens.

4. In the **Restore object** window, specify folder into which the object being restored will be saved for each of the selected object. (The name of the object is displayed in the **Object** field in the upper part of the window. If you selected several objects, the name of the first object in the list of selected objects will be displayed).

Perform one of the following steps:

- To restore an object to its original location, select **Restore to the source folder**.
 - To restore an object to the folder specified as the location for restored objects in the Quarantine settings, select **Restore to the default folder for restoration**.
 - To save an object to a different folder on computer where Kaspersky Embedded Systems Security console is installed or to a network folder, select **Restore to folder on your local computer or on network resource** and then select required folder or specify path to it.
5. If you wish to save a copy of the object in the quarantine folder after this objects is restored, clear the **Remove objects from storage after they are restored** check box.
 6. In order to apply the specified restoration conditions to the rest of the selected objects, check the **Apply to all selected objects** box.

All selected objects are restored and saved in the specified location: if you selected **Restore to the source folder**, each of the objects will be saved into its original location if you selected **Restore to the default folder for restoration** or **Restore to folder on your local computer or on network resource** - all objects will then be saved into one specified folder.

7. Click **OK**.

Kaspersky Embedded Systems Security will start restoring the first of the selected objects.

8. If an object with this name already exists in the specified location, the **Object with this name already exists** window opens.

a. Select one of the following Kaspersky Embedded Systems Security actions:

- **Replace**, in order to restore an object instead of the existing one.
- **Rename**, to save the restored object under a different name. In the entry field enter a new object's filename and full path to it.
- **Rename by adding suffix**, to rename the object by adding a suffix to its filename. Enter suffix in the entry field.

b. If you have selected several objects to be restored, then in order to apply the selected action, such as **Replace** or **Rename**, by adding suffix to the rest of the selected objects, select the **Apply to all selected objects** check box. (If you have selected the **Rename** value, the **Apply to all selected objects** check box will be unavailable).

c. Click **OK**.

The object will be restored; information about the restoration operation will be entered into the system audit log.

If you did not select option **Apply to all selected objects** in the **Restore object** window, the **Restore object** window will open again. Using this window you can specify the location into which next selected object will be saved (see Step 4 of this procedure).

Moving objects to Quarantine

You can quarantine files manually.

► *To quarantine a file take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, open the context menu of the name of the **Quarantine** node.
2. Select **Add**.
3. In the **Open** window, select the file on the disk that you wish to quarantine.
4. Click **OK**.

Kaspersky Embedded Systems Security will quarantine the selected file.

Deleting objects from Quarantine

According to the settings of the **Quarantine Scan** task (see page [286](#)), Kaspersky Embedded Systems Security automatically deletes objects from the Quarantine folder if their status has changed to *Infected* during the scan of Quarantine with the updated databases and if Kaspersky Embedded Systems Security has failed to disinfect them. Kaspersky Embedded Systems Security does not remove other objects from Quarantine.

One or multiple objects can be deleted from Quarantine.

► *To delete one or multiple objects from the Quarantine take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Storages** node.
2. Select the **Quarantine** subnode.
3. Perform one of the following steps:
 - To remove one object, select **Remove** in the context menu of the name of the object.
 - To delete multiple objects, select the objects that you want to delete using the **Ctrl** or **Shift** key, open the context menu on any one of the selected objects and select **Remove**.
4. In the confirmation window, click the **Yes** button to confirm operation.

The selected objects will be removed from quarantine.

Sending probably infected objects to Kaspersky Lab for analysis

If the behavior of a file gives you a reason to suspect that it contains a threat, and Kaspersky Embedded Systems Security considers this file to be clean, you may have encountered a new unknown threat whose signature has not yet been added to the databases. You may send this file to Kaspersky Lab for analysis. Kaspersky Lab's Anti-Virus analysts will analyze it and, if they detect a new threat in it, will add a record identifying it in the databases. It is likely that when you rescan the object after the database has been updated Kaspersky Embedded Systems Security will find this object to be infected and will be able to disinfect it. You will not only be able to keep the object, but will prevent a virus outbreak.

Only quarantined files can be sent for analysis. Quarantined files are stored in encrypted form and are not deleted by the Anti-Virus application installed on the mail server during transfer.

Quarantined object cannot be sent for analysis to Kaspersky Lab after the license expires.

► *To send a file for analysis to Kaspersky Lab take the following steps:*

1. If the file was not quarantined, first move it into Quarantine (see page [292](#)).
2. In the **Quarantine** node, open the context menu on the file which you wish to send for analysis and select **Send object for analysis** in the context menu.
3. In the confirmation window that opens, click **Yes** if you are sure you want to send the selected object for analysis.
4. If a mail client is configured on the computer on which Kaspersky Embedded Systems Security Console is installed, a new email message is created. Review it and click the **Send** button.

The **Receiver** field contains the Kaspersky Lab email address `newvirus@kaspersky.com`. The **Subject** field will contain the text "Quarantined object".

The body of the message will contain the following text: "This file will be sent to Kaspersky Lab for analysis". Any additional information about the file, why you considered it probably infected or dangerous, how it behaves, or how it affects the system, can be included in the body of the message.

Archive <object name>.cab will be attached to the message. This archive will contain file <uuid>.klq with the object in encrypted form, file <uuid>.txt with information about the object collected by Kaspersky Embedded Systems Security, as well as the file Sysinfo.txt, which contains the following information about Kaspersky Embedded Systems Security and the operation system installed on the computer:

- name and version of the operating system
- name and version of Kaspersky Embedded Systems Security
- release date of the latest database update installed
- active key number

This information is required by Kaspersky Lab's anti-virus analysts in order analyze your file faster and more efficiently. If, however, you do not wish to transfer this information you can delete Sysinfo.txt file from the archive.

If a mail client is not installed on the computer with Kaspersky Embedded Systems Security Console, the application prompts you to save the selected encrypted object to file. This file can be sent to Kaspersky Lab manually.

► *To save an encrypted object to a file, take the following steps:*

1. In the window that opens with a prompt to save the object click the **Yes** button.
2. Select a folder on the drive of the protected computer or a network folder where the file containing the object will be saved.

The object will be saved to a CAB file.

Configuring Quarantine settings

You can configure quarantine settings. New Quarantine values for settings apply immediately after they are saved.

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

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Storages** node.
2. Open the context menu of the name of the **Quarantine** subnode.

3. Select **Properties**.
4. In the **Storage settings** window, configure the necessary quarantine settings in accordance with your requirements:

In the **Quarantine settings** section:

- **Quarantine folder**

Path to the Quarantine folder in UNC (Universal Naming Convention) format.

The default path is C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\2.0\Quarantine\.

- **Maximum quarantine size**

This check box enables or disables the function that monitors the total size of objects stored in the Quarantine folder. If the specified value is exceeded (the default value being 200 MB), Kaspersky Embedded Systems Security logs the *Maximum Quarantine size exceeded* event and issues a notification according to the settings for notifications about events of this type.

If the check box is selected, Kaspersky Embedded Systems Security monitors the total size of objects placed in Quarantine.

If the check box is cleared, Kaspersky Embedded Systems Security does not monitor the total size of objects placed in Quarantine.

The check box is cleared by default.

- **Threshold value for space available**

The check box enables or disables the function that monitors the minimum amount of free space in Backup (the default value being 50 MB).

If the amount of free space decreases below the specified threshold, Kaspersky Embedded Systems Security logs the *Backup free space threshold exceeded* event and issues a notification according to the settings for notifications about events of this type.

If the check box is selected, Kaspersky Embedded Systems Security monitors the amount of free space in Backup.

The **Threshold value for space available (MB)** check box is active if the **Maximum Backup size (MB)** check box is selected.

The check box is selected by default.

If the size of objects in Quarantine exceeds the maximum quarantine size or exceeds the available space threshold, Kaspersky Embedded Systems Security will notify you about this while continuing to place objects in Quarantine.

In the **Restoration settings** section:

- **Target folder for restoring objects**

Path to the folder for restoring objects, in UNC (Universal Naming Convention) format.

Default path: C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.0\Restored\.

5. Click **OK**.

The newly configured settings for Quarantine will be saved.

Quarantine statistics

You can view information about the number of quarantined objects - quarantine statistics.

► *In order to view quarantine statistics,*

in the context menu of the name of the **Quarantine** node in the Kaspersky Embedded Systems Security Console tree, select **Statistics**.

The **Statistics** window displays information about the number of objects currently stored in Quarantine (see the following table):

Table 34. Information about quarantined objects in the Statistics window

Field	Description
Probably infected objects	Number of objects found by Kaspersky Embedded Systems Security to be probably infected
Used quarantine space	Total size of data in the quarantine folder
False alarms	The number of objects that received <i>False alarm</i> status because they were classified as non-infected during the quarantine scan using updated databases
Objects disinfected	The number of objects that received <i>Disinfected</i> status after the quarantine scan
Total number of objects	Total number of objects in Quarantine

Making backup copies of objects.

Backup

This section provides information about backup of detected malicious objects before disinfection or deletion, as well as instructions for configuring Backup.

In this section

About backing up objects before disinfection / deletion	298
Viewing objects stored in Backup.....	299
Restoring files from Backup	301
Deleting files from Backup.....	304
Configuring Backup settings.....	305
Backup statistics	306

About backing up objects before disinfection / deletion

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

If the object is a part of a composite object (for example, part of an archive), Kaspersky Embedded Systems Security will save such a composite object in its entirety in Backup. For example, if Kaspersky Embedded Systems Security has detected that one of the objects from a mail database is infected, it will back up the entire mail database.

Large objects placed in Backup by Kaspersky Embedded Systems Security can slow down the system and reduce disc space on the hard drive.

Files can be restored from Backup either to their original folder or to a different folder on the protected computer or on another computer in the local area network. A file can be restored from Backup, for example, if an infected file contained important information, but during the disinfection of this file Kaspersky Security was unable to maintain its integrity and therefore the information became unavailable.

Restoring files from Backup may lead to computer infection.

Viewing objects stored in Backup

Objects can be stored in the Backup folder only by using Kaspersky Embedded Systems Security Console in **Backup** node. They cannot be viewed using Microsoft Windows file managers.

► *In order to view the objects in Backup,*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Storages** node.
2. Select the **Backup** subnode.

Information about objects placed into Backup is displayed in the details pane of the selected node.

► *To find the necessary object in the list of objects in Backup,*
sort the objects or filter the objects.

In this section

Sorting files in Backup.....	299
Filtering files in Backup	300

Sorting files in Backup

By default, files in Backup are sorted by the date of saving in reverse chronological order. To find the required file, you can sort files according to the content of any column in the details pane.

Sorted results are saved if you leave and then reopen the **Backup** node or if you close Kaspersky Embedded Systems Security Console, save the msc file and then reopen it from this file.

► *To sort files in Backup, take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Storages** node.
2. Select the **Backup** subnode.
3. In the list of files in Backup select the column heading which you wish to use to sorting the objects.

Files in Backup will be sorted based on the selected criterion.

Filtering files in Backup

To find the required file in Backup you can filter files: display in the **Backup** node only those files which satisfy the filtering criteria you have specified (filters).

The sorting result will be saved if you leave and then re-open the **Backup** node or if you close the Kaspersky Embedded Systems Security Console, save the msc file and then re-open it from this file.

► *To filter files in Backup, take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, open the context menu of the **Backup** node and select **Filter**.

The **Filter settings** window opens.

2. To add a filter, perform the following steps:
 - a. From the **Field name** list select the field against whose values the filter values will be compared during selection.
 - b. In the **Operator** list select the filtering condition. The values of the filtering conditions in the list may differ depending on the value you have selected in the **Field name** field.

- c. Enter the filter value in the **Field value** field or select filter value.
- d. Click the **Add** button.

The filter you have added will appear in the list of filters in the **Filter settings** window. Repeat these steps for each filter you add. The following guidelines can be used while working with the filters:

- To combine multiple filters using the logical operator "AND", select **If all conditions are met**.
- To combine multiple filters using the logical operator "OR", select **If any condition is met**.
- In order to delete a filter, select the filter you wish to delete in the filter list, and click the **Remove** button.
- To edit the filter, select it from the filter list in the **Filter settings** window, modify the required values in the **Field name**, **Operator** or **Field value** fields and click the **Replace** button.

When all filters have been added, click the **Apply** button. Only files selected by the filters you have specified will then be displayed in the list.

- ▶ *In order to display all files included in the list of objects stored in Backup,*
select **Remove filter** in the context menu of the **Backup** node.

Restoring files from Backup

Kaspersky Embedded Systems Security stores files in the Backup folder in encrypted form in order to protect the protected computer against their possible harmful effect.

Any file can be restored from Backup.

A file may need to be restored in the following cases:

- If the original file, which appeared to be infected, had been containing important information and Kaspersky Embedded Systems Security failed to keep its integrity so, as a result, the information in the file became unavailable.

- If you consider the file harmless to the computer and wish to use it. If you do not wish Kaspersky Embedded Systems Security to consider this file infected or probably infected, during subsequent scans you can exclude it from processing in the Real-Time File Protection task and in the On-Demand Scan tasks. To do this, specify the file as the **Exclude objects** setting or as the **Do not detect** setting in the corresponding tasks.

Restoring files from Backup may lead to computer infection.

When you restore a file you can select where it will be saved: in the original location (by default), the special folder for restored objects on the protected computer, or a custom folder on the computer where Kaspersky Embedded Systems Security console is installed or another computer in the network.

The Restore to folder is used for storing restored objects on the protected computer. You can configure special security settings for it to be scanned. The path to this folder is specified by Backup settings (see section "Configuring Backup settings" on page [305](#)).

By default when Kaspersky Embedded Systems Security is restoring a file it makes a copy of it in Backup. The file copy can be deleted from Backup after it is restored.

► *To restore files from Backup take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Storages** node.
2. Select the **Backup** subnode.
3. Perform one of the following steps:
 - In order to restore one file, open the context menu on the file you wish to restore in the list of files in Backup and select **Restore**.
 - To restore multiple files, select the files you want to restore in the list using the **Ctrl** or **Shift** key, open the context menu on one of the selected files and select **Restore**.
4. In the **Restore object** window, specify the folder to which the restored file will be saved.

The name of the file is displayed in the **Object** field in the upper part of the window. If multiple files are selected, this field will contain the name of the file displayed first in the list.

Perform one of the following steps:

- To save the file being restored on the protected computer, select one of the following options:
 - **Restore to the source folder**, if you do not want to restore the file to its original folder.
 - **Restore to the default folder for restoration**, if you wish to restore the file to the folder specified as the folder for restored objects in the Backup settings.
 - To save the restored file to a different folder select **Restore to folder on your local computer or on network resource** and select the required folder (on the computer where Kaspersky Embedded Systems Security Console is installed or network folder), or specify the path to it.
5. If you do not want to save a copy of the file in the Backup folder after it is restored, select the **Delete objects from storage after they are restored** check box (by default, this check box is cleared).
 6. If several files are selected to be restored, then in order to apply the selected saving conditions to the rest of the selected objects, check the box **Apply to all selected objects**.

All selected files are restored and saved in the specified location: if you selected **Restore to the source folder**, each of the files will be saved in its original location; if you selected **Restore to the default folder for restoration** or **Restore to folder on your local computer or on network resource**, all files will then be saved to one specified folder.

7. Click **OK**.

Kaspersky Embedded Systems Security starts restoring the first of the selected files.

If a file with this name already exists in the specified location, the **Object with this name already exists** window opens.

8. Do the following:

a. Select the condition for saving the restored file:

- **Replace**, to restore a file instead of the existing one.
- **Rename**, to save a restored file with a different name. In the entry field enter the new filename and a full path to the file.
- **Rename by adding suffix**, to rename the file by adding a suffix to its filename. Enter suffix in the entry field.

b. If you wish to apply the action **Replace** or **Rename** by adding a suffix to other selected files, select the **Apply to all objects** check box.

If you have specified **Rename**, then the **Apply to all objects** box will not be available.

c. Click **OK**.

The file will be restored. Information about the restore operation will be registered in the system audit log.

If you have selected several files to be restored and did not select the option **Apply to all selected objects** in the **Restore object** window, the **Restore object** window opens again. This window can be used to specify the folder in which the next selected object will be saved (see Step 4 of this procedure).

Deleting files from Backup

► *To delete one or multiple files from Backup, take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Storages** node.
2. Select the **Backup** subnode.
3. Perform one of the following steps:
 - To delete one file, open the context menu on the file you wish to delete in the object list, and select **Remove**;

- To delete multiple files, select the files you wish to delete using the **Ctrl** or **Shift** key, open the context menu on the one of the selected files, and select **Remove** in the context menu.

4. In the **Confirm** window, click the **Yes** button to confirm the operation.

The selected files will be deleted from Backup.

Configuring Backup settings

► To configure Backup settings, take the following steps:

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Storages** node.
2. Open the context menu of the name of the **Backup** subnode.
3. Select **Properties**.
4. In the **Storage settings** window, configure the necessary Backup settings in accordance with your requirements:

In the **Backup settings** section:

- **Backup folder**

Path to the Backup folder in UNC (Universal Naming Convention) format.

Default path: C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\Backup\.

- **Maximum Backup size (MB)**

The check box enables / disables the function that monitors the total size of objects stored in Backup. If the specified value is exceeded (the default value being 200 MB), Kaspersky Embedded Systems Security logs the *Maximum Backup size exceeded* event and issues a notification according to the settings for notifications about events of this type.

If the check box is selected, Kaspersky Embedded Systems Security monitors the total size of objects placed in Backup.

The check box is cleared by default.

- **Threshold value for space available (MB)**

The check box enables or disables the function that monitors the minimum amount of free space in Backup (the default value being 50 MB).

If the amount of free space decreases below the specified threshold, Kaspersky Embedded Systems Security logs the *Backup free space threshold exceeded* event and issues a notification according to the settings for notifications about events of this type.

If the check box is selected, Kaspersky Embedded Systems Security monitors the amount of free space in Backup.

The **Threshold value for space available (MB)** check box is active if the **Maximum Backup size (MB)** check box is selected.

The check box is selected by default.

If the size of objects in Backup exceeds the maximum Backup size or exceeds the available space threshold, Kaspersky Embedded Systems Security will notify you about this while continuing to place objects in Backup.

In the **Restoration settings** section:

- **Target folder for restoring objects**

Path to the folder for restoring objects, in UNC (Universal Naming Convention) format.

Default path: C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.0\Restored\.

5. Click **OK**.

The configured Backup settings will be saved.

Backup statistics

You can view information about the current status of Backup: Backup statistics.

► *To view Backup statistics,*

open the context menu on the **Backup** node in the Console tree and select **Statistics**.

The **Backup statistics** window opens.

The **Backup statistics** window displays information about the current Backup status (see table below).

Table 35. Information about current Backup status

Field	Description
Current Backup size	Data size in the Backup folder; application calculates the file size in encrypted form
Total number of objects	Current total number of objects in Backup

Event registration.

Kaspersky Embedded Systems Security logs

This section provides information about working with Kaspersky Embedded Systems Security logs: the system audit log, task execution logs, and the event log.

In this section

Ways to log Kaspersky Embedded Systems Security events	308
System audit log	309
Task logs	312
Security event log.....	318
Viewing the event log of Kaspersky Embedded Systems Security in Event Viewer	319
Configuring log settings in Kaspersky Embedded Systems Security Console	320

Ways to register Kaspersky Embedded Systems Security events

Events of Kaspersky Embedded Systems Security are divided into two groups:

- Events related to the processing of objects in Kaspersky Embedded Systems Security tasks
- Events related to the administration of Kaspersky Embedded Systems Security, such as start of application, creation or deletion of tasks, or edition of task settings

Kaspersky Embedded Systems Security uses the following methods of logging events:

- **Task logs.** A task log contains information about current task status and events that occurred during its execution.
- **System audit log.** The system audit log contains information about events that are related to the administration of Kaspersky Embedded Systems Security.
- **Event Log.** The Event Log contains information about events that are required for diagnostics of failures in the operation of Kaspersky Embedded Systems Security. The Event Log is available in Microsoft Windows Event Viewer.
- **Security event log.** The Security Event Log contains information about events that associated with security breaches or attempted security breaches on the protected computer.

If a problem occurs during Kaspersky Embedded Systems Security operation (for example, Kaspersky Embedded Systems Security or an individual task terminates abnormally or does not start), you can create a trace file and memory dump of Kaspersky Embedded Systems Security processes and send files with this information for analysis to Kaspersky Lab Technical Support in order to diagnose the problem encountered.

Kaspersky Embedded Systems Security writes information to trace files and the dump file in unencrypted form.

System audit log

Kaspersky Embedded Systems Security performs the system audit of events related to the administration of Kaspersky Embedded Systems Security. The application logs information about, for example, start of the application, starts and stops of Kaspersky Embedded Systems Security tasks, changes in task settings, creation and deletion of On-Demand Scan tasks. Records of all those events are displayed in the results pane when you select the **System audit log** node in Kaspersky Embedded Systems Security Console.

By default Kaspersky Embedded Systems Security stores records in the system audit log for an unlimited period of time. You specify the storage period for records in the system audit log.

You can specify a folder which Kaspersky Embedded Systems Security will use to store files containing system audit log other than the default one.

In this section

Sorting events in the system audit log	310
Filtering events in the system audit log	310
Deleting events from the system audit log	311

Sorting events in the system audit log

By default, events in the system audit log node are displayed in reverse chronological order.

Events can be sorted by the contents of any column except the **Event** column.

► *To sort events in the system audit log:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Logs** node.
2. Select the **System audit log** subnode.
3. In the results pane, select the header of the column that you want to use to sort the events in the list.

The sorted results will be saved until your next viewing session in the system audit log.

Filtering events in the system audit log

You can configure the system audit log to display only the records of events that meet the filtering conditions (filters) that you have specified.

► *To filter events in the system audit log, take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Logs** node.
2. Open the context menu of the **System audit log** subnode and select **Filter**.

The **Filter settings** window opens.

3. To add a filter, perform the following steps:

- a. In the **Field name** list, select a column by which events will be filtered.
- b. In the **Operator** list select the filtering condition. Filtering conditions vary depending on the item selected in the **Field name** list.
- c. In the **Field value** list, select a value for the filter.
- d. Click the **Add** button.

The filter you have added will appear in the list of filters in the **Filter settings** window.

4. If necessary, perform one of the following actions:

- If you want to combine multiple filters using the logical operator "AND", select **If all conditions are met**.
- If you want to combine multiple filters using the logical operator "OR", select **If any condition is met**.

5. Click the **Apply** button to save the filtering conditions in the system audit log.

The list of events of the system audit log displays only events that meet the filtering conditions. The filtering results will be saved until your next viewing session in the system audit log.

► *To disable the filter:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Logs** node.
2. Open the context menu of the **System audit log** subnode and select **Remove filter**.

The list of events of the system audit log will then display all events.

Deleting events from the system audit log

By default Kaspersky Embedded Systems Security stores records in the system audit log for an unlimited period of time. You specify the storage period for records in the system audit log.

You can manually delete all events from system audit log.

► *To delete events from the system audit log:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Logs** node.
2. Open the context menu of the **System audit log** subnode and select **Clear**.
3. Perform one of the following steps:
 - If you want to save the log contents as a file in CSV or TXT format before deleting events from the system audit log, click the **Yes** button in the deletion confirmation window. In the window that opens, specify the name and location of the file.
 - If you do not want to save the log contents as a file, click the **No** button in the deletion confirmation window.

The system audit log will be cleared.

Task logs

This section provides information about task logs of Kaspersky Embedded Systems Security and instructions on how to manage them.

In this section

About task logs	313
Viewing the list of events in task logs	313
Sorting events in task logs	313
Filtering events in task logs	314
Viewing statistics and information about a Kaspersky Embedded Systems Security task in task logs	315
Exporting information from a task log	316
Deleting events from task logs	317

About task logs

Information about the execution of Kaspersky Embedded Systems Security tasks is displayed in the results pane when you select the **Task logs** node in Kaspersky Embedded Systems Security Console.

In the log of each task, you can view the statistics of the task execution, details of each of the objects that have been processed by the application since the start of the task until the present moment, and the task settings.

By default, Kaspersky Embedded Systems Security stores records in task logs during 30 days since the task completion. You can change the storage period for records in task logs.

You can specify a folder that Kaspersky Embedded Systems Security will use to store files containing task logs other than the default one. You can also select events that Kaspersky Embedded Systems Security will record into task logs.

Viewing the list of events in task logs

► *To view the list of events in task logs:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Logs** node.
2. Select the **Task logs** subnode.

The list of events saved in task logs of Kaspersky Embedded Systems Security will be displayed in the results pane.

Events can be sorted by any column or filtered.

Sorting events in task logs

By default, events in task logs are displayed in reverse chronological order. They can be sorted by any column.

► *To sort events in task logs:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Logs** node.
2. Select the **Task logs** subnode.
3. In the results pane, select the header of the column that you want to use to sort events in task logs of Kaspersky Embedded Systems Security.

The sorted results will be saved until your next viewing session in the task logs.

Filtering events in task logs

You can configure the list of task logs to display only the records of events that meet the filtering conditions (filters) that you have specified.

► *To filter events in the task logs:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Logs** node.
2. Open the context menu of the **Task logs** subnode and select **Filter**.

The **Filter settings** window opens.

3. To add a filter, perform the following steps:
 - a. In the **Field name** list, select a column by which events will be filtered.
 - b. In the **Operator** list select the filtering condition. Filtering conditions vary depending on the item selected in the **Field name** list.
 - c. In the **Field value** list, select a value for the filter.
 - d. Click the **Add** button.

The filter you have added will appear in the list of filters in the **Filter settings** window.

4. If necessary, perform one of the following actions:
 - If you want to combine multiple filters using the logical operator "AND", select **If all conditions are met**.
 - If you want to combine multiple filters using the logical operator "OR", select **If any condition is met**.
5. Click the **Apply** button to save the filtering conditions in the list of task logs.

The list of events of task logs displays only events that meet the filtering conditions. The filtered results will be saved until your next viewing session in the task logs.

► *To disable the filter:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Logs** node.
2. Open the context menu of the **Task logs** subnode and select **Remove filter**.

The list of events of the task logs will then display all events.

Viewing statistics and information about a Kaspersky Embedded Systems Security task in task logs

In task logs, you can view detailed information about all events that have occurred in tasks since they had been started until the present moment, as well as task execution statistics and task settings.

► *To view statistics and information about a Kaspersky Embedded Systems Security task:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Logs** node.
2. Select the **Task logs** subnode.

3. In the results pane, open the **Logs** window using one of the following methods:
 - By double-clicking the event that has occurred in the task for which you want to view the log.
 - Open the context menu of the event that has occurred in the task for which you want to view the log, and select **View log**.
4. In the window that opens, the following details are displayed:
 - The **Statistics** tab displays the time of the task start and completion, as well as the task statistics.
 - The **Events** tab displays a list of events that have been logged during the task run.
 - The **Options** tab displays the task settings.
5. If necessary, click the **Filter** button to filter the events in the task log.
6. If necessary, click the **Export** button to export data from the task log into a file in CSV or TXT format.
7. Press the **Close** button.

The **Logs** window will be closed.

Exporting information from a task log

You can export data from a task log into a file in CSV or TXT format.

► *To export data from a task log:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Logs** node.
2. Select the **Task logs** subnode.

3. In the results pane, open the **Logs** window using one of the following methods:
 - By double-clicking the event that has occurred in the task for which you want to view the log.
 - Open the context menu of the event that has occurred in the task for which you want to view the log, and select **View log**.
4. In the lower part of the **Logs** window, click the **Export** button.

The **Save as** window opens.

5. Specify the name, location, type, and coding of the file into which you want to export data from the task log.
6. Click the **Save** button.

The specified settings are saved.

Deleting events from task logs

By default, Kaspersky Embedded Systems Security stores records in task logs during 30 days since the task completion. You can change the storage period for records in task logs.

You can manually delete all events from logs of tasks that have been already completed for the present moment.

Events from logs of tasks that are currently running and tasks being used by other users will not be deleted.

► *To delete the events from task logs:*

1. In the Kaspersky Embedded Systems Security Console tree, expand the **Logs** node.
2. Select the **Task logs** subnode.

3. Perform one of the following steps:

- If you want to delete the events from the logs of all tasks that have been already completed for the present moment, open the context menu of the **Task logs** subnode and select **Clear**.
- If you want to clear the log of an individual task, in the results pane, open the context menu of an event that has occurred in the task for which you want to clear the log, and select **Remove**.
- If you want to clear the logs for several tasks:
 - a. In the results pane, use the **Ctrl** or **Shift** keys to select events that have occurred in the tasks for which you want to clear the logs.
 - b. Open the context menu of any selected event and select **Remove**.

4. Click the **Yes** button in the deletion confirmation window to confirm that you want to delete the logs.

The task logs that you have selected will be cleared. The deletion of events from the task logs will be registered with the system audit log.

Security event log

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

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

You can clear the Security Event Log as well as the System Audit Log (see section "Deleting events from the system audit log" on page [311](#)). Moreover, Kaspersky Embedded Systems Security records system audit events regarding clearing the Security Event Log.

Viewing the event log of Kaspersky Embedded Systems Security in Event Viewer

You can view the event log of Kaspersky Embedded Systems Security using Microsoft Windows **Event Viewer** snap-in for Microsoft Management Console. The log contains events registered by Kaspersky Embedded Systems Security and required for diagnostics of failures in its operation.

Events that will be registered in the events log can be selected based on the following criteria:

- **by event types**
- **by level of detail.** The level of detail corresponds to the importance level of the events registered in the log (informational, important, or critical events). The most detailed is the **Informational events** level, which registers all events, and the least detailed is the **Critical events** level, which registers critical events only. By default, all components except for the **Update** component have the level of detail **Important events** selected (only important and critical events are logged); for the **Update** component the level **Informational events** is selected.

► *To view the Kaspersky Embedded Systems Security event log:*

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

The window of Microsoft Management Console opens.

2. Select **File** → **Add or remove snap-in**.

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

3. In the list of available snap-ins, select the **Event Viewer** snap-in and click the **Add** button.

The **Select computer** window opens.

4. In the **Select computer** window, specify the computer on which Kaspersky Embedded Systems Security is installed, and click **OK**.

5. In the **Add and remove snap-ins** window, click **OK**.

In the Console tree, the **Event Viewer** node appears.

6. In the Console tree, expand the **Event Viewer** node and select the **Logs of applications and services** → **Kaspersky Embedded Systems Security** subnode.

The Kaspersky Embedded Systems Security event log opens.

Configuring log settings in Kaspersky Embedded Systems Security Console

You can edit the following settings of logs of Kaspersky Embedded Systems Security:

- Length of the storage period for events in task logs and the system audit log
 - Location of the folder in which Kaspersky Embedded Systems Security stores files of task logs and the system audit log
 - Events generation thresholds for *Application database is out of date*, *Application database is extremely out of date* and *Critical Areas Scan has not been performed for a long time*
 - Events that Kaspersky Embedded Systems Security saves in task logs, the system audit log, and the event log of Kaspersky Embedded Systems Security in Event Viewer
 - Settings for publishing audit events and task performance events to the syslog server via the Syslog protocol
- *To configure Kaspersky Embedded Systems Security logs, perform the following steps:*
1. In the Kaspersky Embedded Systems Security Console tree, open the context menu of the **Logs and Notifications** node and select **Properties**.

The **Logs settings** window opens.

2. In the **Logs settings** window, configure the logs in accordance with your requirements.

To do this, perform the following actions:

- On the **General** tab, if necessary, select events that Kaspersky Embedded Systems Security will save in task logs, the system audit log, and the event log of Kaspersky Embedded Systems Security in Event Viewer. To do this, perform the following actions:
 - In the **Component** list, select the component of Kaspersky Embedded Systems Security for which you want to set the detail level.

For the Real-Time File Protection, On-Demand Scan, and Update components, registration of events with task logs and the event log is provided. For these components, the table of event list contains the **Logs** and **Event Log** columns. Events for the Quarantine and Backup components are registered in the system audit log and the event log. For these components, the table of event list contains the **Audit** and **Event Log** columns.

- In the **Importance level** list, select a detail level for events in task logs, the system audit log, and the event log for the selected component.

In the following table with a list of events, the check boxes are selected next to events that are registered with task logs, the system audit log, and the event log, according to the current detail level.

- If you want to manually enable registration of specific events for a selected component, perform the following actions:
 - a. In the **Importance level** list, select **Custom**.
 - b. In the table with the list of events, select the check boxes next to events that you want to be registered in task logs, the system audit log, and the event log.
- On the **Advanced** tab, configure the log storage settings and event generation thresholds for computer protection status:

- In the **Log storage** section:

- **Logs folder**

Path to the log folder in UNC (Universal Naming Convention) format.

Default path: C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\Reports\.

- **Delete task logs and event logs older than (days)**

The check box enables / disables a function that deletes logs with the results of execution of completed tasks and events published in logs of running tasks after the specified period of time (default value: 30 days).

If the check box is selected, Kaspersky Embedded Systems Security deletes logs with the results of execution of completed tasks and events published in logs of running tasks after the specified period of time.

The check box is selected by default.

- **Delete from the audit log events older than (days)**

The check box enables / disables a function that deletes events recorded in the audit log after the specified period of time (default value: 60 days).

If the check box is selected, Kaspersky Embedded Systems Security deletes events recorded in the audit log after the specified period of time.

The check box is selected by default.

- In the **Event generation thresholds** section:

- Specify the number of days after which the events *Application database is out of date*, *Application database is extremely out of date* and *Critical Areas Scan has not been performed for a long time* will occur

Table 36. Event generation thresholds

Setting	Event generation thresholds.
Description	<p>You can specify thresholds for generation of the following three event types:</p> <ul style="list-style-type: none"> • <i>Application database is out of date and Application database is extremely out of date.</i> This event occurs if Kaspersky Embedded Systems Security database has not been updated during the period (in days) specified by the setting since the release date of the most recently installed database updates. You can configure administrator notifications about this event. • <i>Critical Areas Scan has not been performed for a long time.</i> This event occurs if none of the tasks marked with the Consider task as Critical Areas Scan check box are performed during the specified number of days.
Possible values	Number of days from 1 to 365.
Default Value	<p>Application databases are obsolete – 7 days;</p> <p>Application databases are extremely out of date – 14 days;</p> <p>Critical Areas Scan has not been performed for a long time – 30 days.</p>

- On the **SIEM integration** tab, configure the settings for publishing audit events and task performance events to the syslog server (see section "Configuring SIEM integration settings" on page [325](#)).

3. Click **OK**.

Any changes are saved.

About SIEM integration

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

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

You can use SIEM integration in two modes:

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

It is recommended to use this mode to maximally reduce the load on the protected computer.

- Delete local copies of events: this mode prescribes that all events that are registered during application operation and published to SIEM will be deleted from the local computer.

The application never deletes local versions of the security log.

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

It is recommended to select the format of events based on the configuration of the utilized SIEM.

Reliability settings

You can reduce the risk of unsuccessful relay of events to SIEM by defining the settings for connecting to the mirror syslog server.

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

Kaspersky Embedded Systems Security also notifies you about unsuccessful attempts to connect to SIEM and about errors sending events to SIEM using system audit events.

Configuring SIEM integration settings

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

Table 37. SIEM integration settings

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

► *To configure SIEM integration settings:*

1. In the Kaspersky Embedded Systems Security Console tree, open the context menu of the **Logs and Notifications** node.

2. Select **Settings**.

The **Logs settings** window opens.

3. Select the **SIEM integration** tab.

4. In the **Integration settings** section, select the **Send events to a remote syslog server via syslog protocol** check box.

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

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

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

The check box is cleared by default.

5. If necessary, in the **Integration settings** section, select the **Remove local copies for events that have been sent to a remote syslog server** check box.

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

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

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

The check box is cleared by default.

The status of the **Remove local copies for events that have been sent to a remote syslog server** check box does not affect the settings for storing events of the security log: the application never automatically deletes security log events.

6. In the **Events format** section, specify the format to which you want to convert application operation events so that they can be sent to SIEM.

By default, the application converts them into structured data format.

7. In the **Connection settings** section:

- Specify the SIEM connection protocol.
- Specify the settings for connecting to the main syslog server.

You can specify an IP address in IPv4 format only.

- 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 settings for connecting to the mirror syslog server.

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

You can specify an IP address in IPv4 format only.

8. Click **OK**.

The configured SIEM integration settings will be applied.

Licensing

Please refer to the *Kaspersky Embedded Systems Security 2.0 Administrator's Guide*, Application licensing section for the detailed information about the Kaspersky Embedded Systems Security licensing procedures.

Notification settings

This section provides information about ways in which users and administrators of Kaspersky Embedded Systems Security can be notified about application events and the computer protection status, as well as instructions on how to configure notifications.

In this section

Administrator and user notification methods.....	329
Configuring administrator and user notifications	330

Administrator and user notification methods

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

The application ensures performance of the following tasks:

- The administrator can receive information about events of selected types;
- LAN users who access a protected computer and terminal computer users can receive information about events of the type *Object detected* in the Real-Time File Protection task.

In Kaspersky Embedded Systems Security Console, administrator or user notifications can be activated using several methods:

- User notification methods:

- a. Terminal service tools.

You can apply this method for notifying terminal users if the protected computer is used as terminal.

- b. Message service tools.

You can apply this method for notification via Microsoft Windows message services.

- Administrator notification methods:

- a. Message service tools.

You can apply this method for notification via Microsoft Windows message services.

- b. Running an executable file.

This method runs an executable file stored on the local drive of the protected computer, when the event occurs.

- c. Sending by email.

This method uses email to transmit messages.

You can create a message text for individual event types. It can include an information field to describe an event. By default, the application uses a predefined text to notify users.

Configuring administrator and user notifications

Event notification settings give you a choice of methods for configuring and composing a message text.

► *To configure event notification settings, take the following steps:*

1. In the Kaspersky Embedded Systems Security Console tree, open the context menu of the **Logs** node and select **Properties**.

The **Logs settings** window opens.

2. On the **Notifications** tab select the notification mode:
 - a. Select the event for which you wish to select a notification method from the **Event type** list.
 - b. In the **Notify administrators** or **Notify users** group settings, select the check box next to the notification methods that you wish to configure.

You can configure user notifications for the **Object detected** event only.

3. To add the text of a message:
 - a. Click the **Message text** button. Enter in the **Message text** window the text to be displayed in the corresponding event message.

You can create one message text for several event types: after you have selected a notification method for one event type, select the other event types for which you want to use the same message text by using the **CTRL** or **SHIFT** key, and then click the **Message text** button.

- b. To add fields with information about an event, click the **Macro** button and select the relevant fields from the drop-down list. Fields with event information are described in the table in this section.
 - c. To restore the default event message text, click the **By default** button.
 4. To configure the selected methods of administrator notification of selected event, click the **Settings** button in the **Notifications** window and configure the selected methods in the **Advanced settings** window. To do this, perform the following actions:
 - a. For email notifications, open the **Email** tab and specify the email addresses of recipients (delimit addresses with semicolon), name or network address of SMTP server, and port number in the appropriate fields. If necessary, specify the text that will be displayed in the **Subject** and **From** fields. The text in the **Subject** field can also include variables with information about the event (see table below).

If you want to apply user account authentication when connecting to the SMTP server, select **Use SMTP authentication** in the **Authentication settings** group and specify the name and password of the user whose user account will be authenticated.

- b. For notifications using **Windows Messenger Service** create a list of recipient computers for notifications on the Windows Messenger Service tab: for each computer that you wish to add, press the **Add** button and enter its network name in the input field.
 - c. To run an executable file, select the file on a local drive of the protected computer that will be executed on the computer triggered by the event or enter the full path to it on the **Executable file** tab. Enter the user name and password which will be used to execute the file.

System environment variables can be used when the path to the executable file is specified; user environment variables are not allowed.

If you wish to limit the number of messages for one event type over a period of time, on the **Advanced** tab select **Do not send the same notification more than** and specify the number of times and time unit.

5. Click **OK**.

The configured notification settings are saved.

Table 38. Fields with event information

Variable	Description
%EVENT_TYPE%	Event type.
%EVENT_TIME%	Event time.
%EVENT_SEVERITY%	Importance level.
%OBJECT%	Object name (in Real-Time Protection and On-Demand Scan tasks). The Software Modules Update task includes the name of the update and the address of the web page with information on the update.
%VIRUS_NAME%	The name of the object according to the Virus Encyclopedia classification (http://www.securelist.com). This name is included in the full name of the detected object that Kaspersky Embedded Systems Security returns on detecting an object. You can view the full name of the detected object in the task log (see the section "Viewing statistics and information of a Kaspersky Embedded Systems Security task using task logs" on page 315).
%VIRUS_TYPE%	The type of detected object according to the Kaspersky Lab classification, such as "virus" or "trojan". It is included in the full name of the detected object, which is returned by Kaspersky Embedded Systems Security when it finds an object to be infected or probably infected. You can view the full name of the detected object in the task log (see the section "Viewing statistics and information of a Kaspersky Embedded Systems Security task using task logs" on page 315).
%USER_COMPUTER%	In the Real-time file protection task, the computer name for the user who accessed the object on the computer.
%USER_NAME%	In the Real-Time File Protection task, the name of the user who accessed the object on the computer.
%FROM_COMPUTER%	Name of the protected computer where the notification originated.

Variable	Description
%EVENT_REASON%	Reason event occurred (some events do not have this field).
%ERROR_CODE%	Error code (used only for the "internal task error" event).
%TASK_NAME%	Task name (only for events related to task performance).

Glossary

A

Active key

The key that the application currently uses in its operation.

Additional key

The additional key is a key that confirms the right to use the application but is not currently in use.

Administration group

A set of computers associated in accordance with their functions and the pool of Kaspersky Lab applications installed on them. Computers are grouped for the ease of management, which allows administering them as a single unit. A group may include other groups. Group policies and group tasks can be created for each of the applications installed within one group.

Administration server

A component of Kaspersky Security Center that performs centralized storage of information about Kaspersky Lab applications installed on the corporate network and ways of managing them.

Anti-virus databases

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

Application settings

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

Archive

One or more files packed into a single file in a compressed form. A special archiver application is required to archive and unarchive data.

B

Backup

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

D

Disinfection of objects

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

F

False alarm

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

File mask

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

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

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

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

H

Heuristic analysis

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

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

Heuristic Analyzer

A module of Kaspersky Embedded Systems Security that performs heuristic analysis.

I

Infected file

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

O

OLE object

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

P

Potentially infectable file

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

Probably infected file

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

Q

Quarantine

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.

S

Startup objects

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

T

Task

The functions of the Kaspersky Lab application are implemented in the form of tasks, such as: Real-Time File Protection, Full scan, and Database Update.

Task settings

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

U

Update

A procedure that consists in replacing / adding new files (databases or application modules) retrieved from Kaspersky Lab update servers.

V

Vulnerability

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

AO Kaspersky Lab

Kaspersky Lab is a world-renowned vendor of systems for protection of computers against various threats, including viruses and other malware, spam, network and hacking attacks.

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

Kaspersky Lab was founded in Russia in 1997. Today, Kaspersky Lab is an international group of companies running 38 offices in 33 countries. The company is now employing more than 3,000 skilled professionals.

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

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

The company offers solutions and technologies for protection and control of workstations and mobile devices, virtual machines, file servers and web servers, mail gateways, and firewalls. The company's portfolio also includes dedicated products for protection against DDoS attacks, protection of environments managed with industrial control systems, and fraud prevention. Used in conjunction with centralized management tools, these solutions ensure effective automated protection against computer threats for companies and organizations of any scale. Kaspersky Lab products are certified by major testing laboratories, compatible with the applications of most software vendors, and optimized for work on most hardware platforms.

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

Technologies. Many technologies that are now part and parcel of modern anti-virus tools were originally developed by Kaspersky Lab. It is no coincidence that the program kernel of Kaspersky Anti-Virus is integrated in products of many software vendors, including

Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, and ZyXEL. Many of the company's innovative technologies are patented.

Achievements. Over the years, Kaspersky Lab has won hundreds of awards for its services in combating computer threats. 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 eventually 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: <http://www.kaspersky.com>

Virus Encyclopedia <https://securelist.com/>

Virus Lab: <https://virusdesk.kaspersky.com> (for scanning suspicious files and websites)

Kaspersky Lab web forum: <http://forum.kaspersky.com>

Information about third-party code

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

Trademark notices

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

Excel, Microsoft, Outlook, and Windows are trademarks of Microsoft Corporation, registered in the United States and other countries.

Index

A

Action

infected objects 110, 247

suspicious objects 110, 247

Actions on objects 110, 122, 244

Administration groups 335

Administration server 335

Application interface 18, 45

icon in taskbar notification area 24

Archives 110, 247

B

Backup 298

configuring settings 305

deleting objects 304

restoring objects 301

Backup storage folder 305

C

Configuration

security settings 107, 108, 110, 243, 244, 247

Configuring

task 67, 88, 122, 139, 165, 176, 190, 224, 271

Console 18, 45, 46, 56

connection.....56

start.....26

D

Databases.....262, 265

automatic update..... 70, 265, 271

date created29

manual update271

Default Deny 174, 176

Disinfection of objects 110, 247

E

Event Log 308, 319

Executable file57, 61, 139, 143, 152, 158, 168, 247

F

Folder for restoration

Quarantine294

Folder to save updates in.....276

FTP server 271, 276, 278

H

HTTP server 266, 271, 276, 278

I

Icon in notification area of the task tray24

iSwift files..... 108, 110, 244, 247, 286

K

Kaspersky Embedded Systems Security

 running at system startup27

L

Launching missed tasks.....70

Logs folder320

M

Main window 18

Maximum size

 Quarantine294

 scanned object 110, 247

P

Protection mode.....90

Proxy server.....271

Purging system audit log.....311

Q

Quarantine

deleting objects	292
free space threshold	294
object restoration	289
viewing objects	284, 285

Quarantine and Backup	282
-----------------------------	-----

R

Real-Time Protection	84, 85
----------------------------	--------

Restore object	289, 301
----------------------	----------

Restoring the default settings	108, 244
--------------------------------------	----------

Rules	152, 157, 164, 179, 184, 190
-------------	------------------------------

applications launch control	152, 155, 156, 157, 158, 162, 163, 164, 165, 168, 169, 171
-----------------------------------	------------------------------------------------------------

device control	179, 181, 182, 183, 184, 187, 188, 189, 190
----------------------	---------------------------------------------

S

Scan alternate NTFS streams	110, 247
Scan scope exclusions	57, 110, 247
Scanning	
maximum object scan time	110, 247
only new and modified objects.....	110, 247
security level	108, 244
Statistics	29

T

Task.....	67
Tasks schedule	70, 72
Threat type	
action	110, 247
Trusted devices	174
Trusted Zone	
exclusion rules.....	57
trusted applications	57

U

Update

by schedule	70, 271
rolling back to the previous update	280
software modules	262
Update source	271, 276, 278
Updates content.....	276

V

Virus scan of storages	286
------------------------------	-----