kaspersky

Kaspersky Endpoint Detection and Response Optimum

Contents

Kaspersky Endpoint Detection and Response Optimum 1.0 Help

Kaspersky Endpoint Detection and Response Optimum

This section provides information about Kaspersky Endpoint Detection and Response Optimum solution, its key functions and components.

About Kaspersky Endpoint Detection and Response Optimum

Kaspersky Endpoint Detection and Response Optimum is a solution designed to protect an organization IT infrastructure from complex cyberthreats. The solution functionality combines automatic threat detection with the ability to respond to these threats to resist complex attacks, including new exploits, ransomware, fileless attacks, and methods that use legitimate system tools. The solution is intended for corporate users.

Solution architecture

The solution consists of the following components:

- Kaspersky Endpoint Agent as part of Endpoint Protection Platform (for example, as a part of Kaspersky Endpoint Security) is installed on individual devices in the organization IT infrastructure that are running under Microsoft Windows operating system. The application constantly monitors the processes running on these devices, open network connections and the files being modified.

- Kaspersky Security Center and Kaspersky Security Center Web Console (or Kaspersky Security Center Cloud Console and cloud Administration Console) allow you to centrally manage the solution and its settings by means of a single web interface.

- Kaspersky Sandbox (optional component, distributed separately) is intended for additional inspection of suspicious objects detected by EPP. For detailed information about Kaspersky Sandbox, refer to *Kaspersky Sandbox Help*.

Threat detection

Kaspersky Endpoint Detection and Response Optimum performs review and analysis of the threat development and provides the Security Officer or Administrator with information about a potential attack in order to respond to the threat in a timely manner.

Incident card is a tool for viewing all collected information about a detected threat and for managing response actions. An incident card is displayed in Kaspersky Security Center and may contain, for example, the following information about a detected threat:

- Threat development chain graph.

- Information about the device on which the threat is detected (for example, name, IP address, MAC address, user list, operating system).

- General information about the detection, including detection mode (for example, detection during on-demand scan or during automatic scan).

- Registry changes associated with the detection.

- History of the file presence on the device.

- Response actions performed by the application.

Threat development chain graph is a tool for analyzing the reasons of the threat. The graph provides visual information about the objects involved in the incident, for example, about key processes on the device, network connections, libraries, registry hives.

The solution uses the following Threat Intelligence tools for analyzing threats:

- Kaspersky Security Network (KSN) infrastructure of cloud services that provides access to the online Kaspersky Knowledge Base, which contains information about the reputation of files, web resources, and software. The use of data from Kaspersky Security Network ensures faster responses by Kaspersky applications to threats, improves the performance of some protection components, and reduces the likelihood of false alarms.

- Integration with Kaspersky Private Security Network (hereinafter also referred to as KPSN) that allows the users to access KSN reputation databases, as well as other statistics without submitting data to KSN from their computers.

- Integration with Kaspersky Threat Intelligence Portal information system, which contains and displays information about the reputation of files and URLs.

- Kaspersky Threats database.

Threat response

The threat response functionality provides the following automatic response actions that the application performs when threats are detected:

- Quarantine object.

- Delete file.

- Isolate device from the network.

- Run Critical Areas Scan on the device.

- Start search for indicators of compromise (IOC Scan) for a group of devices.

Additionally, the following actions are available to a Security Officer or an Administrator:

- Place objects to the Execution prevention list.

- Start process on the device.

- Terminate process on the device.

Kaspersky Endpoint Agent functions

As part of Kaspersky Endpoint Detection and Response Optimum solution, Kaspersky Endpoint Agent performs the following actions:

- Collects information about detections from Endpoint Protection Platform (for example, from Kaspersky Endpoint Security).

- Supplements verdict information with data about the detection.
- Submits data to Kaspersky Security Center to create a threat development chain.
- Starts IOC Scan tasks (search for indicators of compromise) on groups of protected devices.
- Performs actions in response to detected indicators of compromise, for example:
  - enables network isolation of the device;
  - starts Critical Areas Scan on the device.
- Submits objects to Kaspersky Sandbox for scan (if integration with Kaspersky Sandbox is configured).

Kaspersky Endpoint Agent

Kaspersky Endpoint Agent is installed on individual devices in the organization IT infrastructure. The application constantly monitors the processes running on these devices, open network connections and the files being modified.

Kaspersky Endpoint Agent interacts with other Kaspersky solutions to detect comprehensive threats (such as targeted attacks).

Kaspersky Endpoint Agent distribution kit

Kaspersky Endpoint Agent distribution kit includes the following files:

Kaspersky Endpoint Agent distribution kit

File	Purpose
`agent\endpointagent.msi`	Kaspersky Endpoint Agent installation package.
`agent\endpointagent.kud`	File for creating Kaspersky Endpoint Agent installation package using Kaspersky Security Center.
`agent\klcfginst.msi`	Installation package for Kaspersky Endpoint Agent Management plug-in for Kaspersky Security Center.
`agent\kpd.loc\en-us.ini`	Configuration file required for creating installation package for English version of Kaspersky Endpoint Agent using Kaspersky Security Center.
`agent\kpd.loc\ru-ru.ini`	Configuration file required for creating installation package for Russian version of Kaspersky Endpoint Agent using Kaspersky Security Center.
`agent\en-us\ksn.txt`	File with the text of the terms of participation in Kaspersky Security Network in English.
`agent\en-us\license.txt`	File with the text of the End User License Agreement and the Privacy Policy in English.
`agent\en-us\release_notes.txt`	File with the text of the Release Notes for Kaspersky Endpoint Agent in English.
`agent\ru-ru\ksn.txt`	File with the text of the terms of participation in Kaspersky Security Network in Russian.
`agent\ru-ru\license.txt`	File with the text of the End User License Agreement and the Privacy Policy

	in Russian.
`agent\ru-ru\release_notes.txt`	File with the text of the Release Notes for Kaspersky Endpoint Agent in Russian.

If Kaspersky Endpoint Agent is installed by means of Kaspersky Security Center using the application installation package from Kaspersky web server, the distribution package also includes the install_props.json configuration file.

Hardware and software requirements

Kaspersky Endpoint Agent has the following hardware and software requirements:

Minimum hardware requirements:

- Processor: 1.4 GHz (single core) or higher.
- RAM: 256 MB (512 MB if a 64-bit operating system is used).
- Free disk space: 500 MB.

Supported operating systems:

- Windows 7 SP1 Home / Professional / Enterprise 32-bit / 64-bit
- Windows 8.1.1 Professional / Enterprise 32-bit / 64-bit
- Windows 10 RS3 (version 1703) Home / Professional / Education / Enterprise 32-bit / 64-bit
- Windows 10 RS4 (version 1803) Home / Professional / Education / Enterprise 32-bit / 64-bit
- Windows 10 RS5 (version 1809) Home / Professional / Education / Enterprise 32-bit / 64-bit
- Windows 10 19H1 (version 1903) Home / Professional / Education / Enterprise 32-bit / 64-bit
- Windows 10 19H2 (version 1909) Home / Professional / Education / Enterprise 32-bit / 64-bit
- Windows 10 20H1 (version 2004) Home / Professional / Education / Enterprise 32-bit / 64-bit
- Windows 10 20H2 (version 2009) Home / Professional / Education / Enterprise 32-bit / 64-bit
- Windows Server 2008 R2 Foundation / Standard / Enterprise 32-bit / 64-bit
- Windows Server 2012 Foundation / Standard / Enterprise 32-bit / 64-bit
- Windows Server 2012 R2 Foundation / Standard / Enterprise 32-bit / 64-bit
- Windows Server 2016 Essentials / Standard / Datacenter 32-bit / 64-bit
- Windows Server 2019 Essentials / Standard / Datacenter 32-bit / 64-bit

Google Chrome for Windows is required to manage Kaspersky Endpoint Agent using Kaspersky Security Center Web Console.

Kaspersky Endpoint Agent 3.10 compatibility with the previous versions of Kaspersky Endpoint Agent

If Endpoint Sensor version 3.6.X is installed and used on the device as part of Kaspersky Endpoint Security, Endpoint Sensor must be disabled before installing Kaspersky Endpoint Agent in order to avoid possible conflicts between the applications.

Kaspersky Endpoint Agent 3.10 can be installed on a device with Endpoint Sensor version 3.5 or lower installed as part of Kaspersky Endpoint Security. The applications work independently without conflicts.

Only Kaspersky Endpoint Agent versions 3.7, 3.8, and 3.9 can be updated to Kaspersky Endpoint Agent version 3.10. Update is possible for the previous application versions installed either as part of the Endpoint Protection Platform application, or separately.

Kaspersky Endpoint Agent Management plug-in version 3.10 and Kaspersky Endpoint Agent Web plug-in version 3.10 are compatible with Kaspersky Endpoint Agent versions 3.7 and later.

Requirements for Kaspersky Endpoint Agent operation as a part of Kaspersky Endpoint Detection and Response Optimum solution

For Kaspersky Endpoint Agent operation as a part of Kaspersky Endpoint Detection and Response Optimum solution:

- Kaspersky Security Center 12.1 or Kaspersky Security Center Cloud Console must be installed.
- The application must be managed using Kaspersky Security Center 12.1 Web Console or using the Cloud Administration Console, respectively.
- Kaspersky Endpoint Agent must be installed as part of the following EPP applications:
  - Kaspersky Endpoint Agent 3.9 as a part of:
    - Kaspersky Endpoint Security 11 for Windows: 11.4, 11.5.
    - Kaspersky Security 11 for Windows Server.
  - Kaspersky Endpoint Agent 3.10 as a part of:
    - Kaspersky Endpoint Security 11.6 for Windows.

Kaspersky Endpoint Agent 3.10 cannot be installed as part of Kaspersky Security for Windows Server. Kaspersky Endpoint Agent 3.9 can be installed as a part of Kaspersky Security 11 for Windows Server, and then it can be separately updated to version 3.10.

Kaspersky Endpoint Agent 3.10 integration with other Kaspersky applications and solutions

Kaspersky Endpoint Agent 3.10 can be integrated with the following Kaspersky applications and solutions:

- Kaspersky Security Center 11 and 12.1.
- Kaspersky Security Center Cloud Console.
- Kaspersky Sandbox 1.0.
- Kaspersky Anti Targeted Attack Platform 3.7, 3.7.1, 3.7.2.
- Kaspersky Endpoint Detection and Response Optimum 1.0.

Kaspersky Endpoint Agent compatibility with anti-virus applications of other vendors

One of the following anti-virus applications from other vendors can be installed on the computers where you want to install Kaspersky Endpoint Agent:

- Symantec Endpoint Protection.
- Trend Micro Maximum Security.
- Sophos Endpoint Protection.
- ESET NOD32 Business Edition Smart Security.
- BitDefender GravityZone Advanced Business Security.
- McAfee Endpoint Security 10.6.1.

Proper operation of Kaspersky Endpoint Agent is not guaranteed if several anti-virus applications from other vendors are installed simultaneously.

If RealTimes Desktop Service is installed on the computers where Kaspersky Endpoint Agent will be installed, it is recommended to uninstall it before installing Kaspersky Endpoint Agent.

What's new

The following features and improvements are implemented in Kaspersky Endpoint Agent 3.9:

Known errors have been fixed in the new version of Kaspersky Endpoint Agent. The new application version also includes all the functionalities of the previous versions and introduces new features:

- Incident card generation: Kaspersky Endpoint Agent generates a detailed card with important data about a security incident on the device. An incident card is generated in Administration Server Web Console based on the detection event received from the compatible Kaspersky Endpoint Protection Platform application. You can also initiate a chain of response actions: create an execution prevention rule for an untrusted object; search for similar incidents in the device group based on the selected indicators of compromise (IOC); isolate untrusted object; isolate a compromised device from the network.
- Visualization of the Attack Spread Path: for each created incident card, Kaspersky Endpoint Agent creates an interactive graph that describes the deployment stages of the detected attack in time. The created graph

includes information about the modules involved in the attack and the actions performed by these modules.

- Integration with Kaspersky Managed Detection and Response service.
- Integration with Kaspersky Security 11 for Windows Server, which is scheduled for release in summer 2020, as part of the following software solutions:
  - Kaspersky Anti Targeted Attack Platform
  - Kaspersky Sandbox
  - Kaspersky Endpoint Detection and Response Optimum
  - Kaspersky Managed Detection and Response
- Kaspersky Endpoint Agent web plug-in is implemented for managing the application using Administration Server Web Console interface. Web plug-in provides the ability to manage the following functions:
  - General Kaspersky Endpoint Agent settings
  - Integration with Kaspersky Sandbox
  - Integration with Kaspersky Endpoint Detection and Response Optimum
  - Integration with Kaspersky Managed Detection and Response
  - Integration with Kaspersky Security Network
  - Activation and update
- Integration with Kaspersky Security Center Cloud Console within the functions of Kaspersky Endpoint Detection and Response Optimum.

Limitations of the current Kaspersky Endpoint Agent version

Kaspersky Endpoint Agent 3.9 has the following limitations:

1. Limitations for filling out an incident card and creating a graph of the threat development chain:
   - If detection is related to SMB session on the device, the incident card does not display full information about the incident, and the graph of the threat development chain is not available.
   - If detection is caused by Kaspersky Sandbox, the graph of the threat development chain is not available for asynchronous detections in the incident card (for synchronous detections, the graph is available).
   - If the detection is caused by downloading a malicious file from the Internet or by blocking a phishing website, only the object's web address is displayed in the graph of the threat development chain; the event that caused the link to be clicked is not displayed.
2. If more than one application is specified as the value of the Application criterion when configuring the settings of network isolation exclusions, Kaspersky Endpoint Agent allows connection only for the first application in the list. Network connections for other applications specified in the list will be ignored. This limitation is reproduced when isolating devices with Windows 7 or Windows Server 2008 R2 operating systems.

3. Kaspersky Endpoint Agent can double-display data about a triggered object when displaying the results of IOC Scan task.

4. The installer cannot stop Kaspersky Endpoint Agent service until the service is initialized. For example, the installer returns the "Invalid password" error when trying to remove or modify the configuration of the application immediately after installation is completed, since initialization of Kaspersky Endpoint Agent service is not completed and the service cannot be stopped.

5. If localization of Kaspersky Endpoint Agent differs from localization of Kaspersky Endpoint Agent management plug-in for Kaspersky Security Center, some settings may not be displayed correctly in the outputs of the "show" commands in the command console.

6. When trying to launch Kaspersky Endpoint Agent installer with the permissions of a user whose account contains Chinese characters, the installer fails. It is recommended to install the application with the Local System account permissions, for example, start installation using Kaspersky Security Center.

7. Kaspersky Endpoint Agent 3.9 cannot be restored or uninstalled from the device if the integrity of the agent.exe module (Kaspersky Endpoint Agent 3.9 command line utility) is violated.

8. Kaspersky Endpoint Agent installer cannot be launched on a device with the operating system to which the active CodeIntegrity policy is applied.

9. In Kaspersky Endpoint Agent properties in the Administration Console (in the General section), data about the application installation status is displayed incorrectly.

10. Objects quarantined by Kaspersky Endpoint Agent cannot be sent from Kaspersky Security Center quarantine to Kaspersky for analysis.

11. The check boxes corresponding to the "Read" and "Perform operations with device selections" permissions that are displayed in the group of settings for role-based access control (RBAC) in the Administration Console, in the section with permissions for managing Kaspersky Endpoint Agent plug-in, do not apply to the group of settings in Kaspersky Security Center. If you select these check boxes, the "Read" and "Perform operations with device selections" permissions will not be restricted for the specified users.

12. When generating event selections, the filters are not applied to some of Kaspersky Endpoint Agent events published in Kaspersky Security Center Administration Console.

13. The agent.exe --help command does not support output of help for one specified command. The full list of all commands supported by the utility is displayed in the console.

14. The name of the workgroup, but not the name of the user is displayed in the User field in the properties of the object quarantined to the Administration Server repository.

Quick Start Guide

The following scenarios for Kaspersky Endpoint Agent initial configuration are possible:

- Configuring Kaspersky Endpoint Agent on a device running Kaspersky Security Center Web Console.
- Configuring Kaspersky Endpoint Agent on a device running Kaspersky Security Center Cloud Console.

Installing Kaspersky Endpoint Security for Windows and Kaspersky Endpoint Agent

The scenario consists of the following steps:

1. **Installing Kaspersky Security Center Web Console**

   For detailed information on installing Kaspersky Security Center Web Console, refer to Kaspersky Security Center Help.

2. **Configuring the set of Kaspersky Endpoint Security for Windows components**

   Kaspersky Endpoint Agent is included in Kaspersky Endpoint Security for Windows distribution kit and can be installed together with Kaspersky Endpoint Security for Windows or by modifying the set of Kaspersky Endpoint Security for Windows components.

   For detailed information on installing Kaspersky Endpoint Security for Windows, refer to Kaspersky Endpoint Security for Windows Help.

   For detailed information on modifying the set of Kaspersky Endpoint Security for Windows components, refer to Kaspersky Endpoint Security for Windows Help.

3. **Installing Kaspersky Endpoint Agent Management web plug-in**

   For detailed information on installing management web plug-ins, refer to Kaspersky Security Center Help.

4. **Initial configuration of Kaspersky Endpoint Agent web plug-in**

   Activate Kaspersky Endpoint Agent and create Kaspersky Endpoint Agent policy.

5. **Configuring threat report**

   Configure a threat report for viewing incident cards.

Installing Kaspersky Endpoint Agent on a device with Kaspersky Endpoint Security for Windows using Kaspersky Security Center Cloud Console

The scenario consists of the following steps:

1. **Configuring the set of Kaspersky Endpoint Security for Windows components**

   Kaspersky Endpoint Agent is included in Kaspersky Endpoint Security for Windows distribution kit and can be installed together with Kaspersky Endpoint Security for Windows or by modifying the set of Kaspersky Endpoint Security for Windows components.

   For detailed information on installing Kaspersky Endpoint Security for Windows, refer to Kaspersky Endpoint Security for Windows Help.

   For detailed information on modifying the set of Kaspersky Endpoint Security for Windows components, refer to Kaspersky Endpoint Security for Windows Help.

2. **Initial configuration of Kaspersky Endpoint Agent web plug-in**

Activate Kaspersky Endpoint Agent and create Kaspersky Endpoint Agent policy.

For detailed information on working with Kaspersky Security Center Cloud Console, refer to Kaspersky Security Center Cloud Console Help.

3. **Configuring threat report**

Configure a threat report for viewing incident cards.

Installing and uninstalling Kaspersky Endpoint Agent

Kaspersky Endpoint Agent can be installed separately or as part of Kaspersky Endpoint Protection Platform applications (hereinafter also referred to as "EPP").

For Kaspersky Endpoint Agent operation as a component of Kaspersky Endpoint Detection and Response Optimum, Kaspersky Endpoint Agent must be installed as part of Kaspersky Endpoint Security 11 for Windows (11.4, 11.5, 11.6) or Kaspersky Security 11 for Windows Server.

Kaspersky Endpoint Agent 3.10 cannot be installed as part of Kaspersky Security for Windows Server. Kaspersky Endpoint Agent 3.9 can be installed as a part of Kaspersky Security 11 for Windows Server, and then it can be separately updated to version 3.10.

For instructions on how to obtain a distribution kit of a compatible EPP application and install Kaspersky Endpoint Agent as part of EPP, refer to the compatible EPP Help.

By default, Kaspersky Endpoint Agent is not selected for installation as part of compatible EPP. You need to manually select Kaspersky Endpoint Agent for installation in the list of EPP components.

When the application is installed as part of EPP, installation settings can be passed using the install_props.json configuration file. For this purpose, first place the install_props.json file into the same folder as the endpointagent.msi file.

This section contains information on how to install Kaspersky Endpoint Agent on a device *separately* (not as a part of EPP), how to update the application from the previous version, and how to remove the application from a device.

Separate installation of Kaspersky Endpoint Agent

For Kaspersky Endpoint Agent operation as a component of Kaspersky Endpoint Detection and Response Optimum, Kaspersky Endpoint Agent must be installed as part of Kaspersky Endpoint Security 11 for Windows (11.4, 11.5, 11.6) or Kaspersky Security 11 for Windows Server.

Kaspersky Endpoint Agent 3.10 cannot be installed as part of Kaspersky Security for Windows Server. Kaspersky Endpoint Agent 3.9 can be installed as a part of Kaspersky Security 11 for Windows Server, and then it can be separately updated to version 3.10.

For instructions on how to obtain a distribution kit of a compatible EPP application and install Kaspersky Endpoint Agent as part of EPP, refer to the compatible EPP Help.

By default, Kaspersky Endpoint Agent is not selected for installation as part of compatible EPP. You need to manually select Kaspersky Endpoint Agent for installation in the list of EPP components.

Stand-alone Kaspersky Endpoint Agent installation can be performed:

- Locally using the Installation Wizard.
- Locally using the command line.
- Remotely using Kaspersky Security Center.
- Remotely using Microsoft Windows Group Policy Management Editor (for details, visit the Microsoft Technical Support website).

For remote installation, the settings can be passed using the install_props.json configuration file. For this purpose, first place the install_props.json file into the same folder as the endpointagent.msi file.

Preparing for Kaspersky Endpoint Agent installation

Before installing Kaspersky Endpoint Agent on a device or updating the application from the previous version, make sure, that the following conditions are met:

- The device complies with the hardware and software requirements.
- You have the permissions, required for the application installation.

If any of these conditions is not met, the corresponding notification is displayed.

Installing and uninstalling Kaspersky Endpoint Agent locally

This section contains information on how to install Kaspersky Endpoint Agent locally on a device.

Installing Kaspersky Endpoint Agent using the Installation Wizard

The interface of the application Installation Wizard consists of a sequence of windows corresponding to the application installation steps.

To install the application or update it from a previous version using the application Installation Wizard,

copy the endpointagent.msi file which is included in the distribution kit to the user device and run it.

The application Installation Wizard starts.

After Kaspersky Endpoint Agent is installed on the device, the Installation Wizard can be launched on this device in one of the following modes:

- **Modify** the settings of the installed application.
- **Restore** the damaged application modules.

- **Uninstall** the application from the device.

Removing Kaspersky Endpoint Agent using the Installation and Uninstallation Wizard

You can uninstall Kaspersky Endpoint Agent using standard Microsoft Windows installation and uninstallation tools. To uninstall the application, a wizard is launched. As a result of its operation all application components are removed from the device.

All data that is stored locally on the device, except for trace and dump files, is deleted from the device when the application is uninstalled.

Installing, restoring and uninstalling the application using the command line

Kaspersky Endpoint Agent can be installed and uninstalled using the msi package, by setting the values of MSI properties in a standard way. For more information on using standard Windows Installer commands and keys, refer to the documentation provided by Microsoft.

For Kaspersky Endpoint Agent operation as a component of Kaspersky Endpoint Detection and Response Optimum or Kaspersky Managed Detection and Response, Kaspersky Endpoint Agent must be installed as part of Kaspersky Endpoint Security 11 for Windows (11.4, 11.5, 11.6) or Kaspersky Security 11 for Windows Server.

For instructions on how to obtain a distribution kit of a compatible EPP application and install Kaspersky Endpoint Agent as part of EPP, refer to the compatible EPP Help.

By default, Kaspersky Endpoint Agent is not selected for installation as part of compatible EPP. You need to manually select Kaspersky Endpoint Agent for installation in the list of EPP components.

This section provides the instructions on how to install Kaspersky Endpoint Agent on a device *separately* (not as part of EPP) using the command line, how to restore the application, and how to remove it from the device.

Installing Kaspersky Endpoint Agent

An example of installing the application in the quiet mode with the default settings is shown below. After starting the application installation in the quiet mode, your participation in the installation process is not required.

Installing Kaspersky Endpoint Agent in the quiet mode requires acceptance of the terms and conditions of End User License Agreement and Privacy Policy. Use the `EULA=1` and `PRIVACYPOLICY=1` parameters only if you have fully read, understood and accept the terms of the End User License Agreement and Privacy Policy.

Example:

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

Repairing Kaspersky Endpoint Agent

An example of restoring the application in the quiet mode is shown below. After starting the application restoration in the quiet mode, your participation in the restoration process is not required.

Example:
```
msiexec /i endpointagent.msi REINSTALL=ALL /qn
```

Uninstalling Kaspersky Endpoint Agent

An example of uninstalling the application in the quiet mode is shown below. After starting the application uninstallation in the quiet mode, your participation in the uninstallation process is not required.

Example:
```
msiexec /i {F83015D5-0368-4A99-8CD4-A109769EB16F} REMOVE=ALL /qn
```
If the application is protected by the password:
```
msiexec /i {F83015D5-0368-4A99-8CD4-A109769EB16F} REMOVE=ALL UNLOCK_PASSWORD=
<password> /qn
```

All data that is stored locally on the device, except for trace and dump files, is deleted from the device when the application is uninstalled.

Installing Kaspersky Endpoint Agent using Kaspersky Security Center

Kaspersky Endpoint Agent can be installed using a remote installation task in Kaspersky Security Center. Installation consists of the following steps:

1. Creating installation package.
2. Creating remote installation task.

Kaspersky Security Center also supports other methods of installing applications on groups of managed devices. For more information about installation using a remote installation task and other installation methods, refer to *Kaspersky Security Center Help*.

Creating Kaspersky Endpoint Agent installation package

Installation package is a set of files generated for remote installation of a Kaspersky application using Kaspersky Security Center. The installation package contains the required settings to install the application and ensure its operation immediately after installation. The installation package is created on the basis of files with the kpd and kud extensions included in the application distribution package.

Creating an installation package in the Administration Console.

To create an installation package:

1. In the Administration Console, select **Administration Server** → **Advanced** → **Remote installation** → **Installation packages**.
2. Click the **Additional actions** button and select **View current versions of Kaspersky applications** from the drop-down list.

   The list of current versions of Kaspersky applications is displayed.
3. Select Kaspersky Endpoint Agent installation package.
4. Click the **Download application and create an installation package** button.

   The installation package is displayed in the list of installation packages.
5. To change the installation package properties, in the context menu of the installation package, select **Properties**.

   The properties window of Kaspersky Endpoint Agent installation package opens. You can configure:

   - The set of application components
   - Application installation folder
   - Application recovery mode
   - The settings of the key file for activating the application

The new installation package is available in the list of installation packages. You can use this installation package for a remote installation task.

Creating an installation package in the Web Console and in the Cloud Console.

To create an installation package:

1. In the main Web Console window, select **Discovery and Deployment → Deployment and Assignment → Installation packages**.

   The list of installation packages downloaded to Kaspersky Security Center opens.

2. Click the **Add** button.

   The New Package Wizard starts.

3. On the first screen of the wizard, select **Create installation package for Kaspersky application**.

   A list of installation packages available on Kaspersky web servers is displayed. The list contains installation packages for only the applications that are compatible with the current version of Kaspersky Security Center.

4. Select Kaspersky Endpoint Agent installation package.

   This opens a window containing information about the installation package.

5. Read the information and click **Download and create installation package**.

   If the distribution package cannot be converted to an installation package, the **Download distribution package** button is displayed instead of the **Download and create installation package** button. In this case, do the following:

   a. Click the **Download distribution package** button to download the distribution package to your computer.

      Wait for the download to finish.

   b. Close the installation package creation wizard window and restart the wizard.

   c. On the first page of the wizard, select **Create installation package from file**.

   d. On the second page of the wizard, specify the path to the distribution package file on your computer.

   e. Follow the instructions of the wizard.

6. When you create the installation package, accept the terms and conditions of the License Agreement and the Privacy Policy.

7. After download is complete, click **Close**.

   The selected installation package is downloaded to the Administration Server shared folder, into the Packages subfolder. The downloaded installation package is displayed in the list of installation packages.

8. To change the installation package properties, click on the installation package name.

   The properties window of Kaspersky Endpoint Agent installation package opens. You can configure:

   - The set of application components
   - Application installation folder
   - Application recovery mode
   - The settings of the key file for activating the application

The new installation package is available in the list of installation packages. You can use this installation package for a remote installation task.

Creating Kaspersky Endpoint Agent remote installation task

The Remote application installation task is intended for remote installation of Kaspersky Endpoint Agent using Kaspersky Security Center. To install the application, the task uses the application installation package.

Creating remote installation task in the Administration Console.

To create a remote installation task:

1. In the Administration Console, open the **Administration Server** → **Tasks** folder.

   A list of tasks appears.

2. Click **Create a task**.

   The task creation wizard starts. Follow its steps.

Step 1. Selecting the task type

Select **Kaspersky Security Center Administration Server** → **Remote application installation**.

Step 2. Selecting the installation package

In the list of installation packages, select Kaspersky Endpoint Agent installation package.

You can modify the installation package properties in Kaspersky Security Center, for example, select the application components to be installed on the computer.

Step 3. Optional

The Network Agent can be installed together with Kaspersky Endpoint Agent. The Network Agent provides interaction between the Administration Server and the client computer. If the Network Agent is already installed on the computer, it is not re-installed.

If you want to install the Network Agent together with Kaspersky Endpoint Agent, select the Network Agent installation package.

Step 4. Settings

Configure the following additional application settings:

- **Force installation package download**. Select the application installation method:
  - **Using Network Agent**. If the Network Agent is not installed on the computer, first the Network Agent is installed using the operating system tools. Than Kaspersky Endpoint Agent is installed using the Network Agent tools.
  - **Using operating system resources through distribution points**. The installation package is transferred to the client computers using the operating system resources through distribution points. You can select this option if there is at least one distribution point in your network. For details on distribution point operation, refer to *Kaspersky Security Center Help*.
  - **Using operating system resources through Administration Server**. Files will be delivered to the client computers by means of the operating system using the Administration Server. This option can be selected if the Network Agent is not installed on the client computer, but the client computer is in the same network as the Administration Server.
- **Behavior of devices managed by other Servers**. Select how to install Kaspersky Endpoint Agent. If more than one Administration Server is installed in the network, these Administration Servers can detect the

same client computers. It can result in remote installation of the same application on one client computer from several Administration Servers and in other conflicts.

- **Do not install application if it is already installed**. Clear this check box if you want, for example, to install an earlier version of the application.

Step 5. Selecting how to restart the operating system

Select the action to be performed if the computer must be restarted.

Step 6. Selecting devices to assign the task to

Select the devices on which Kaspersky Endpoint Agent will be installed.

Step 7. Selecting an account to run the task

Select an account to install the Network Agent using the operating system. In this case, administrator permissions are required to access the computer. You can add multiple accounts. If an account does not have the required permissions, the installation wizard uses the next account in the list. You do not need to select an account to install Kaspersky Endpoint Agent using the Network Agent.

Step 8. Configuring task schedule settings

Configure the task start schedule. For example, manually or when the computer is idle.

Step 9. Defining the task name

Enter the task name, for example, `Installing Kaspersky Endpoint Agent`.

Step 10. Finishing task creation

Complete the wizard operation. If required, select the **Run task after wizard finishes** check box. You can monitor the task progress in the task properties. The application will be installed in quiet mode.

Creating remote installation task in the Web Console and in the Cloud Console

To create a remote installation task:

1. In the main Web Console window select **Devices** → **Tasks**.

   A list of tasks appears.

2. Click the **Add** button.

   The task creation wizard starts. Follow its steps.

Step 1. Configuring the general task settings

Configure the general task settings:

1. In the **Application** drop-down list, select **Kaspersky Security Center**.
2. In the **Task type** drop-down list, select **Remote application installation**.
3. In the **Task name** field, enter a short description, for example, `Installing Kaspersky Endpoint Agent`.
4. In the **Devices to which the task will be assigned** section, select the task scope.

Step 2. Selecting computers for installation

At this step, select the computers on which Kaspersky Endpoint Agent will be installed in accordance with the selected task scope.

Step 3. Configuring the installation package settings

At this step, configure the installation package settings:

1. Select Kaspersky Endpoint Agent installation package.
2. Select the Network Agent installation package.

   The selected version of the Network Agent will be installed together with Kaspersky Endpoint Agent. The Network Agent provides interaction between the Administration Server and the client computer. If the Network Agent is already installed on the computer, it is not re-installed.

3. In the **Force installation package download** section, select the application installation method:

   - **Using Network Agent**. If the Network Agent is not installed on the computer, first the Network Agent is installed using the operating system tools. Than Kaspersky Endpoint Agent is installed using the Network Agent tools.
   - **Using operating system resources through distribution points**. The installation package is transferred to the managed devices using the operating system resources through distribution points. You can select this option if there is at least one distribution point in your network. For details on distribution point operation, refer to *Kaspersky Security Center Help*.
   - **Using operating system resources through Administration Server**. Files will be delivered to the managed devices by means of the operating system using the Administration Server. This option can be

selected if the Network Agent is not installed on the managed device, but the managed device is in the same network as the Administration Server.

4. In the **Maximum number of concurrent downloads** field, specify the limit on the number of installation package download requests to the Administration Server. Limit on the number of requests allows avoiding network overload.

5. In the **Number of installation attempts** field, specify the limit on the number of application installation attempts. If Kaspersky Endpoint Agent installation completes with an error, the task automatically starts installation again.

6. If required, clear the **Do not install application if it is already installed** check box. This will allow, for example, installing an earlier version of the application.

7. If required, clear the **Verify operating system type before downloading** check box. This will allow avoiding download of the application distribution package if the computer operating system does not meet the software requirements. If you are sure that the computer operating system meets the software requirements, you can skip this check.

8. If required, select the **Assign package installation in Active Directory group policies** check box. Kaspersky Endpoint Agent installation is performed manually using the Network Agent or Active Directory. To install the Network Agent, the remote installation task must be started with the domain administrator permissions.

9. If required, select the **Prompt the user to close running applications** check box. Kaspersky Endpoint Agent installation requires computer resources. For the user convenience, the application installation wizard prompts to close running applications before starting installation. It will prevent slowdowns in operation of other applications and possible computer malfunctions.

10. In the **Behavior of devices managed by other Servers** section, select the method of Kaspersky Endpoint Agent installation. If more than one Administration Server is installed in the network, these Administration Servers can detect the same client computers. It can result in remote installation of the same application on one client computer from several Administration Servers and in other conflicts.

Step 4. Selecting how to restart the operating system

Select the action to be performed if the computer must be restarted.

Step 5. Selecting an account to run the task

Select an account to install the Network Agent using the operating system. In this case, administrator permissions are required to access the computer. You can add multiple accounts. If an account does not have the required permissions, the installation wizard uses the next account in the list. You do not need to select an account to install Kaspersky Endpoint Agent using the Network Agent.

Step 6. Finishing task creation

Complete the wizard operation by clicking the **Finish** button. The new task appears in the task list. To run the task, select the check box next to the task and click **Run**. The application will be installed in quiet mode.

Updating Kaspersky Endpoint Agent from the previous version

If Kaspersky Endpoint Agent 3.10 is installed on a device with a previous version of Kaspersky Endpoint Agent, all the data that can be migrated is saved and used during Kaspersky Endpoint Agent 3.10 installation, and the previous version of the application is automatically uninstalled.

Only Kaspersky Endpoint Agent versions 3.7, 3.8, and 3.9 can be updated to Kaspersky Endpoint Agent version 3.10. Update is possible for the previous application versions installed either as part of the Endpoint Protection Platform application, or separately.

If Endpoint Sensor version 3.6.X is installed and used on the device as part of Kaspersky Endpoint Security, Endpoint Sensor must be disabled before installing Kaspersky Endpoint Agent in order to avoid possible conflicts between the applications.

When updating a previous version of Kaspersky Endpoint Agent, protected by the password, you must pass this password to the installer by one of the following ways:

- When installing the application locally using the installation wizard interface or interactively using the command line, specify the password at the appropriate step.
- When installing the application locally using the command line in the quiet mode, specify the password as the value of the `UNLOCK_PASSWORD` key.
- When installing the application remotely using Kaspersky Security Center, pass the current password in the installation package settings.

When updating Kaspersky Endpoint Agent as part of EPP, you can pass the password as the value of the `UNLOCK_PASSWORD` key in the install_props.json configuration file.

The application password passed through the install_props.json configuration file is stored in the file in non-encrypted form. To reduce the probability of unauthorized access to this data, it is recommended to restrict access to the install_props.json file and delete it from the device after installing or updating the application.

When installing Kaspersky Endpoint Agent by updating it from the previous version, if the version being updated was activated earlier, the new application version is automatically activated by the license key used for the application version being updated. The license term remains unchanged. When updating the application with an expired license, the new application version works in limited functionality mode after installation.

Only when being updated from Kaspersky Endpoint Agent 3.7, the application can be activated during update. The key file can be passed using one of the specified methods.

Starting from version 3.10, Kaspersky Managed Protection (also referred to as KMP) usage cannot be configured by means of Kaspersky Endpoint Agent. If usage of the KMP service was enabled in the previous Kaspersky Endpoint Agent version, the KMP service continues functioning after the application is updated to version 3.10. After the application update, you can disable the KMP service only using Kaspersky Endpoint Agent Administration Plug-in or Kaspersky Endpoint Agent Web Plug-in of versions earlier then 3.10.

Repairing Kaspersky Endpoint Agent

If you launch Kaspersky Endpoint Agent installer in the Repair mode, it will check and restore the integrity of all damaged application modules and system registry keys created during application installation.

You can run the installer in the Repair mode in one of the following ways:

- Locally using Kaspersky Endpoint Agent Installation Wizard.
- Locally using the command line.
- Remotely using Kaspersky Security Center by performing one of the following actions (for details, refer to *Kaspersky Security Center Help*):
  - By selecting the **Repair application if it is already installed** check box when creating the installation package.
  - By specifying the `REINSTALL=ALL` parameter when creating a custom installation package.

If Kaspersky Endpoint Agent installer is launched in the Repair mode and *the application repair is not required*, the installer does not perform any changes on the device.

If Kaspersky Endpoint Agent installer is launched in the Repair mode and *the application is not installed on the device*, application installation will start.

If Kaspersky Endpoint Agent installer is launched in the Repair mode locally using the command line or remotely using Kaspersky Security Center, and the *settings of the installed application differ from the settings specified in the installer*, the installer will be launched in the mode for changing the settings of the installed application.

Installing Kaspersky Endpoint Agent administration tools

This section contains information on how to install Kaspersky Endpoint Agent Management web plug-in to manage Kaspersky Endpoint Agent in Kaspersky Security Center Web Console.

Installing and updating Kaspersky Endpoint Agent Management web plug-in

Kaspersky Endpoint Agent Management web plug-in must be installed to manage Kaspersky Endpoint Agent using Kaspersky Security Center Web Console.

You can install the web plug-in in one of the following ways:

- Using the Initial Setup Wizard of Kaspersky Security Center Web Console.

- From the list of available distribution packages in Kaspersky Security Center Web Console.

  For detailed information on installing management web plug-ins, refer to Kaspersky Security Center Help.

- By downloading the distribution package to Kaspersky Security Center Web Console from a third-party source.

  To install the web plug-in, add a ZIP archive with the distribution package of Kaspersky Endpoint Agent web plug-in to the Web Console interface (Console settings → Plug-ins). You can download the web plug-in distribution kit, for example, from Kaspersky website.

Updating previously installed version of Kaspersky Endpoint Agent Management web plug-in

When installing a plug-in on a device with a previous plug-in version:

- All the setting values (including the created and configured policies, group and local tasks) are migrated to the new plug-in version, and the previously installed plug-in version is automatically removed.
- The Kaspersky Endpoint Agent settings that were not available in the plug-in version being updated are set to default values and can be configured.

  > To apply previously unavailable settings after updating the plug-in, change the desired policy or task and save your changes.

- Policy templates created in the previous plug-in version are available in the new plug-in version.

You can use the new plug-in to manage previous Kaspersky Endpoint Agent versions. However, Kaspersky Endpoint Agent does not support the settings that have appeared in the new plug-in version. Unsupported settings are not applied.

Changes in the system after Kaspersky Endpoint Agent installation

Windows Installer service performs the following changes on the protected device during Kaspersky Endpoint Agent installation:

- Creates Kaspersky Endpoint Agent folders.
- Registers Kaspersky Endpoint Agent keys in the system registry.
- Registers Kaspersky Endpoint Agent services and drivers.

Kaspersky Endpoint Agent folders on the protected device

When Kaspersky Endpoint Agent is installed, the following folders are created on the device:

- The default Kaspersky Endpoint Agent installation folder that contains Kaspersky Endpoint Agent executable files:
  - In 32-bit version of Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Endpoint Agent\
  - In 64-bit version of Microsoft Windows: %ProgramFiles (x86)%\Kaspersky Lab\Endpoint Agent\

- Folder containing Kaspersky Endpoint Agent (x86) drivers:
  - In 32-bit version of Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Endpoint Agent\drivers\<OS version>\<driver name>
  - In 64-bit version of Microsoft Windows: %ProgramFiles (x86)%\Kaspersky Lab\Endpoint Agent\drivers\x64\<OS version>\<driver name>
- Folders containing IOC files:
  - In 32-bit version of Microsoft Windows:
    - %ProgramFiles%\Kaspersky Lab\Endpoint Agent\openioc
    - %ProgramFiles%\Kaspersky Lab\Endpoint Agent\openioc\1.0
    - %ProgramFiles%\Kaspersky Lab\Endpoint Agent\openioc\1.1
  - In 64-bit version of Microsoft Windows:
    - %ProgramFiles (x86)%\Kaspersky Lab\Endpoint Agent\openioc
    - %ProgramFiles (x86)%\Kaspersky Lab\Endpoint Agent\openioc\1.0
    - %ProgramFiles (x86)%\Kaspersky Lab\Endpoint Agent\openioc\1.1
- Folders containing Kaspersky Endpoint Agent system files:
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\Cache
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\Cache\Images
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\Cache\Queue
- %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\Cache\Queue\Kata
- %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\Cache\Queue\Kmp
- %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\Cache\Queue\Syslog
- %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\Hunts
- %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\killchain
- %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Settings
- %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Tasks
- %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\DSKM
- %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Temp
- %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Temp\Tasks

- %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Bases
- Folder containing system files for Kaspersky Security Network operation.
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Ksn
- Folder containing quarantined files:
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Quarantine
- Folder containing files restored from the quarantine:
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Restored
- Folder containing Kaspersky Security Center policy configuration files:
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Policy
- Folders containing system files for Kaspersky Sandbox operation:
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Sandbox
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Sandbox\Queue
- Folder containing files of updatable components:
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Update
- Folder containing shortcut files for the Start menu:
  - %ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Kaspersky Endpoint Agent

Kaspersky Endpoint Agent services and drivers

The following Kaspersky Endpoint Agent services are registered and started under the system account (SYSTEM):

- SOYUZ.exe is the main Kaspersky Endpoint Agent service that manages its tasks and operation processes.
- VOSTOK.dll (executed in proton.exe) is a service that provides interaction between Kaspersky Endpoint Agent and the Central Node component.
- ANGARA.dll (executed in proton.exe) is a service that provides interaction between Kaspersky Endpoint Agent and EPP in scenarios of Kaspersky Sandbox integration.

The following Kaspersky Endpoint Agent drivers are registered on the device:

- klsnsr.sys is Event Tracing for Windows (ETW) driver.
- klncap.sys is ETW network packet analyzer.

System registry keys

As a result of Kaspersky Endpoint Agent installation, the following registry keys are created:

Registry keys are listed in the 32-bit application view.

- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\SOYUZ\4.0.0.0\ProdDispla
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\SOYUZ\4.0.0.0\ProdVersi
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\SOYUZ\4.0.0.0\Connecto
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\SOYUZ\4.0.0.0\Connecto
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\SOYUZ\4.0.0.0\NagentMi
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\SOYUZ\4.0.0.0\Connecto
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\SOYUZ\4.0.0.0\Installer\UninstallString
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\SOYUZ\4.0.0.0\Installer\UninstallString
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\SOYUZ\4.0.0.0\Installer\ProductCode
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\NoPPL]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\BFESDDL]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\CrashDump\Enable]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\CrashDump\Folder]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\CrashDump\Enable(Example)]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\CrashDump\Folder(Example)]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Environment\EnableKillChain]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Environment\SvmUpdateMode]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Environment\MsiPath]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Environment\AgentPath]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Environment\EventsExpirationTimeout]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Install\InstallID]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Install\InstallTime]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Install\InstallLCID]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Install\InstallLocalization]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Install\InstallPlatformType]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Install\Version]

- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Trace\Configuration]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Trace\Configuration(Example)]
- [HKEY_CURRENT_USER\Software\KasperskyLab\SOYUZ\StartMenu]
- [HKEY_CURRENT_USER\Software\KasperskyLab\SOYUZ\UninstallShortcut2]
- [HKEY_CURRENT_USER\Software\KasperskyLab\SOYUZ\RelNotes]
- [HKEY_CURRENT_USER\Software\KasperskyLab\SOYUZ\License]
- [HKEY_CURRENT_USER\Software\KasperskyLab\SOYUZ\Ksn]
- [HKEY_CURRENT_USER\Software\KasperskyLab\SOYUZ\Kmp]
- [HKEY_CURRENT_USER\Software\KasperskyLab\SOYUZ\ProductUrl]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\angara]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klelaml]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klncap]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klsnsr]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vostok]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\soyuz]

Application licensing

This section provides license information.

About the End User License Agreement

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

Read through the terms of the End User License Agreement carefully before you start using the application.

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

- During Kaspersky Endpoint Detection and Response Optimum installation.
- By reading the license.txt document. This document is included in the application distribution kit.

You accept the terms of the End User License Agreement when you confirm your consent to the End User License Agreement during installation of the application. If you do not accept the terms of the End User License Agreement, you must abort application installation and must not use the application.

About the license

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

A valid license entitles you to the following kinds of services:

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

The scope of services and validity period depend on the type of license under which the application was activated.

The following types of licenses are available:

- *Trial* – a free license for users to get to know the application.

  Trial licenses have a short validity period. When the trial license expires, all the functions of Kaspersky Endpoint Detection and Response Optimum become unavailable. To continue using the application, you need to purchase a commercial license.

  You can activate the application under a trial license only once.

- *Commercial* – a paid license that is provided when you purchase Kaspersky Security.

  When the commercial license expires, the application continues operation with limited functionality (for example, Kaspersky Endpoint Detection and Response Optimum database updates are not available). To continue using Kaspersky Endpoint Detection and Response Optimum in fully functional mode, renew your commercial license.

It is recommended to extend the validity period of the license before its expiration date to ensure maximum protection.

About the license certificate

The *License Certificate* is a document provided together with the key file or activation code.

The License Certificate contains the following license information:

- License key or order number
- Information about the license user
- Information about the application that can be activated by the license
- Restrictions on the number of licensing units (for example, devices on which the application can be used under the license)
- License start date
- License expiration date or validity period
- License type

About license key

License key is a sequence of bits with can be used to activate and the application for further usage in accordance with the terms of the End User License Agreement. License key is generated by Kaspersky experts.

You can add a license key to the application in one of the following ways: apply a *key file* or enter an *activation code*. After you add a key to the application, the license key is displayed in the application interface as a unique alphanumeric sequence.

The license key may be blocked by Kaspersky, if the terms of the End User License Agreement are violated. If the license key is blocked, you need to add another license key for proper application operation.

There are two types of license keys: active and additional (backup).

Active license key is currently used for the application operation. A license key for a trial or commercial license can be added as the active key. The application cannot have more than one active license key.

Additional (backup) license key confirms your right to use the application, but is not currently in use. The additional license key automatically becomes active when the license associated with the current active license key expires. An additional license key can be added only if an active license key is already added.

A trial license key can only be added as an active license key. A trial license key cannot be added as an additional license key.

About the activation code

Activation code is a unique sequence of twenty Latin letters and numbers. Activation code is used to add a license key that activates Kaspersky Endpoint Detection and Response Optimum. You receive the activation code at the email address that you provided when purchasing Kaspersky Endpoint Detection and Response Optimum or when ordering a trial version of Kaspersky Endpoint Detection and Response Optimum.

To activate the application using the activation code, Internet access is required to connect to Kaspersky activation servers.

If the activation code was lost after activation of the application, you can restore the activation code. You may need the activation code to register Kaspersky CompanyAccount, for example. To restore the activation code, contact Kaspersky Technical Support.

About the key file

Key file is a file with the .key extension that you receive from Kaspersky. Key files are intended to add a license key for activation of the application.

You receive the key file at the email address that you provided when purchasing Kaspersky Endpoint Detection and Response Optimum or when ordering a trial version of Kaspersky Endpoint Detection and Response Optimum.

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

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

To restore the key file, perform one of the following actions:

- Contact the license distributor.
- Get the key file on Kaspersky website based on the available activation code.

Kaspersky Endpoint Agent activation

This section contains information about Kaspersky Endpoint Agent activation.

Managing Kaspersky Endpoint Agent activation

You can activate Kaspersky Endpoint Agent in one of the following ways:

- During the application installation:
  - By specifying the key file at a certain step of the Installation Wizard.
  - By placing the key file in the same folder with the endpointagent.msi file before starting the application installation in the quiet mode (including remote installation).
  - By specifying the path to the key file using the `LICENSEKEYPATH` parameter when installing the application in the quiet mode (including remote installation).

If there are several key files in the folder, Kaspersky Endpoint Agent will be activated using the key file with the latest license expiration date.

If Kaspersky Endpoint Agent installer does not detect a key file suitable for Kaspersky Endpoint Agent activation, the application will be installed without activation.

When installing Kaspersky Endpoint Agent by updating it from the previous version, if the version being updated was activated earlier, the new application version is automatically activated by the license key used for the application version being updated. The license term remains unchanged. When updating the application with an expired license, the new application version works in limited functionality mode after installation.

Only when being updated from Kaspersky Endpoint Agent 3.7, the application can be activated during update. The key file can be passed using one of the specified methods.

- After the application installation:
  - Using the application activation task in Kaspersky Security Center.
  - Using the command line locally on the device.

You can use Kaspersky Security Center as a proxy server for Kaspersky Endpoint Agent activation.

You can view information about the current license in Kaspersky Security Center in the **Kaspersky licenses** section, in the device properties or using the command line.

For detailed information on managing keys using Kaspersky Security Center, refer to *Kaspersky Security Center Help*.

After the license expires, the application continues to work in limited functionality mode.

Functional limitations after the license expiration

When the license expires, the following limitations arise in the operation of Kaspersky Endpoint Agent functional components:

- Telemetry data is not collected.
- Creation of the threat development chain is not available.
- Network isolation cannot be enabled.

  If network isolation was enabled when the license expired, the application disables network isolation in accordance with the specified settings for automatic disabling of network isolation.
- Execution prevention cannot be enabled.

  If Execution prevention was enabled when the license expired, the application stops blocking objects that fall under the specified Execution prevention rules.

- The following tasks stop and cannot be started: Run process, Terminate process, Delete file.
- The Standard IOC Scan tasks stop and cannot be started.
- KSN/KPSN usage terminates.

When you try to use the listed application functional components after the license expires, the application creates the critical `LicenseViolation` event in the Windows event log and in Kaspersky Security Center Administration Server log. When working using the command line, the application returns code `8` (`AccessDenied`).

Viewing information about the current license

You can view information about the current license in Kaspersky Security Center in the **Kaspersky licenses** section or in the device properties in the **Keys** section. For detailed information on managing licenses using Kaspersky Security Center, refer to *Kaspersky Security Center Help*.

To view information about the current license on a specific device:

1. On the **Devices** tab, select **Managed devices**.
2. Click the name of the device you want.
3. In the device properties window that opens, select the **Applications** tab.
4. In the list of applications, select **Kaspersky Endpoint Agent**.
5. In the application properties window that opens, select the **General** tab and open the **License** section.

The general information about active and backup license keys is displayed.

About data provisioning

Do not use Kaspersky Endpoint Agent on the devices for which data submission is prohibited by the policy of your organization.

In order to provide basic functionality and audit, as well as to expedite solutions to arising problems by Kaspersky Technical Support experts, Kaspersky Endpoint Agent stores and processes data locally.

Data prepared for automatic submission to Kaspersky Security Center is stored on devices with Kaspersky Endpoint Agent installed. Files are stored on the devices with Kaspersky Endpoint Agent installed in plain, non-encrypted form in the default folder for storing files before submission.

The administrator must ensure security of the devices with Kaspersky Endpoint Agent installed and Kaspersky Security Center servers with data listed above. The administrator is responsible for access to this information.

This section contains the following information about personal data stored on the devices with Kaspersky Endpoint Agent installed and transferred to Kaspersky Security Center or to Kaspersky servers:

- Content of stored data
- Storage location
- Storage duration
- User access to data

The received information is protected by Kaspersky in accordance with the requirements established by the law and the current Kaspersky rules. Data is transmitted via encrypted communication channels.

All data that is stored locally on the device, except for trace and dump files, is deleted from the device when the application is uninstalled.

Service data

Service data are stored in the %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\<product version> file. Data in the Settings subfolder are encrypted using the Encrypting File System (EFS). The data is stored until Kaspersky Endpoint Agent is uninstalled.

The data can be automatically sent to Kaspersky Security Center.

By default, these files can be accessed only by users with System (full access) and Administrator (read and execute) permissions. The %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\<product version> folder and the Restored subfolder are also accessible to users with User (read only) permissions.

All data that is stored locally on the device, except for trace and dump files, is deleted from the device when the application is uninstalled.

Kaspersky Endpoint Agent stores the following data:

- Quarantined files.
- Kaspersky Endpoint Agent settings:
  - Access password for Kaspersky Endpoint Agent.
  - Credentials of operating system users for starting tasks with certain user permissions.
  - Authentication credentials for Kaspersky Security Center Administration Server.
  - Authentication credentials for the proxy server.
  - Addresses of custom update sources.

Data in Windows Event Log

Data on the events in Windows Event Log is stored in the %SystemRoot%\System32\Winevt\Logs\Kaspersky-Security-Soyuz%4Product.evtx file in a plain and non-encrypted form. The data is stored until Kaspersky Endpoint Agent is uninstalled.

The data can be automatically sent to Kaspersky Security Center.

By default, only users with System and Administrator permissions have read access to the files. Kaspersky Endpoint Agent does not manage access permissions to this folder and the files in this folder. The access is managed by the system administrator.

Event data can contain information about:

- User sessions in the operating system.
- User accounts in the operating system (userID).
- Errors occurred during object scan tasks execution.
- Object scan tasks.
- Object scan results.
- The object scan queue.
- Changes of Kaspersky Endpoint Agent.
- Changes of Kaspersky Security Center policies.
- Changes of object scan task status.
- Kaspersky Security Center policies.
- Quarantined objects.
- Automatic Threat Response actions.

- Objects blocked by Execution prevention rules.
- Results of the Delete file tasks.
- Results of the Terminate process tasks.
- Results of the Run application tasks.
- Results of the Get file tasks.
- Current Kaspersky Endpoint Detection and Response Optimum license.
- Application activation status.

All data that is stored locally on the device, except for trace and dump files, is deleted from the device when the application is uninstalled.

Data provided when using the activation code

When Kaspersky Endpoint Agent is activated using the activation code, the following data is sent to the activation server:

- Type, identifier, version and localization of the installed Kaspersky Endpoint Agent application.
- Device identifier.
- Identifier of Kaspersky Endpoint Agent installation on the computer.
- Activation code and unique identifier of the current license activation.
- Kaspersky Endpoint Agent activation time.
- Type, version and bitness of the operating system.

For data transfer, the secure HTTPS protocol is used with SSL/TLS encryption.

Data for creating a threat development chain

The data for building the threat chain is stored in the %APPDATA%\killchain\detects folder in open unencrypted form. By default, this data is stored for 7 days. The data is automatically sent to Kaspersky Security Center.

All data that is stored locally on the device, except for trace and dump files, is deleted from the device when the application is uninstalled.

By default, only users with System and Administrator permissions have read access to the files. Kaspersky Endpoint Agent does not manage access permissions to this folder and the files in this folder. The access is managed by the system administrator.

Data for creating a threat development chain may contain the following information:

- Incident date and time.
- Detection name.
- Scan mode.
- Status of the last action related to the detection.
- Reason why the detection processing failed.
- Detected object type.
- Detected object name.
- Threat status after the object is processed by EPP.
- Reason why execution of actions on the object failed.
- Actions performed by EPP to roll back malicious actions (for EPPs that support rollback of malicious actions).
- Information about the processed object:
  - Unique identifier of the process.
  - Unique identifier of the parent process.
  - Unique identifier of the process file.
  - Windows process identifier.
  - Process command line.
  - User account that started the process.
  - Code of the logon session in which the process is running.
  - Type of the session in which the process is running (for example, "interactive", "remote interactive").
  - Integrity level of the process being processed.
  - Membership of the user account that started the process in the privileged local and domain groups (for example, Administrators, Domain Administrators, Enterprise Administrators, Schema Administrators).
  - Identifier of the processed object.
  - Full name of the processed object.
  - Identifier of the protected device.
  - Full name of the object (local file name or downloaded file web address).
  - MD5 hash of the processed object.
  - SHA256 hash of the processed object.
  - Type of the processed object.

- Creation date of the processed object.
- Date when the processed object was last modified.
- Size of the processed object.
- Attributes of the processed object.
- Organization that signed the processed object.
- Result of the processed object digital certificate verification.
- Security identifier (SID) of the processed object.
- The time zone identifier of the processed object.
- Web address of the processed object download (only for files on disk).
- Name of the application that downloaded the file.
- MD5 hash of the application that downloaded the file.
- SHA256 hash of the application that downloaded the file.
- Name of the application that last modified the file.
- MD5 hash of the application that last modified the file.
- SHA256 hash of the application that last modified the file.
- Number of the processed object starts.
- Date and time when the processed object was first started.
- Unique identifiers of the file.
- Full name of the file (local file name or downloaded file web address).
- Path to the processed Windows registry variable.
- Name of the processed Windows registry variable.
- Value of the processed Windows registry variable.
- Type of the processed Windows registry variable.
- Indicator of the processed registry key membership in the startup point.
- Web address of the processed web request.
- Link source of the processed web request.
- User agent of the processed web request.
- Type of the processed web request ("GET" or "POST").

- Local IP port of the processed web request.
- Remote IP port of the processed web request.
- Connection direction (inbound or outbound) of the processed web request.
- Identifier of the process into which the malicious code was embedded.

Data received as a result of IOC Scan task execution

Kaspersky Endpoint Agent automatically submits data on the IOC Scan task execution results to Kaspersky Security Center to create a threat development chain.

The data is stored in Kaspersky Security Center database. By default, this data is stored for 7 days.

The data in the IOC Scan task execution results may contain the following information:

- IP address from the ARP table.
- Physical address from the ARP table.
- DNS record type and name.
- IP address of the protected device.
- Physical address (MAC-address) of the protected device.
- Identifier in the event log entry.
- Data source name in the log.
- Log name.
- User.
- Event time.
- MD5 hash of the file.
- SHA256 hash of the file.
- Full name of the file (including path).
- File size.
- Remote IP address to which connection was established during scan.
- Remote port to which connection was established during scan.
- Local adapter IP address.
- Port open on the local adapter.

- Protocol as a number (in accordance with the IANA standard).
- Process name.
- Process arguments.
- Path to the process file.
- Windows identifier (PID) of the process.
- Windows identifier (PID) of the parent process.
- User account that started the process.
- Date and time when the process was started.
- Service name.
- Service description.
- Path and name of the DLL service (for svchost).
- Path and name of the service executable file.
- Windows identifier (PID) of the service.
- Service type (for example, a kernel driver or adapter).
- Service status.
- Service launch mode.
- User account name.
- Volume name.
- Volume letter.
- Volume type.
- Windows registry value.
- Registry hive value.
- Registry key path (without hive and value name).
- Registry setting.
- System (environment).
- Operating system name and version.
- Network name of the protected device.
- Domain or group the protected device belongs to.

Data on acceptance the terms of KSN Statement

If you agree with the terms and conditions of KSN (Kaspersky Security Network) Statement, the application automatically sends this information to Kaspersky.

Data on acceptance of the terms and conditions of the Statement can be stored locally in the %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\<application version>\Data\ folder.

All data that is stored locally on the device, except for trace and dump files, is deleted from the device when the application is uninstalled.

The following data is sent to Kaspersky when you accept or decline the terms and conditions of KSN Statement:

- Statement identifier (KSN, EULA).
- Statement version.
- Statement agreement flag (1 – Statement accepted, 0 – Statement declined).
- Date when the Statement was accepted or declined.

Kaspersky can use this data to generate statistical information.

Providing extended Kaspersky Endpoint Agent diagnostic information to the Technical Support specialists

To provide support in case of Kaspersky Endpoint Agent malfunction, the Technical Support specialists may ask you to perform the following actions for debugging purposes:

- Activate the functionality for receiving advanced diagnostic information.
- Additionally configure individual application components that cannot be changed by standard user interface tools.
- Change the settings for storing and sending the received diagnostic information.
- Set up interception and saving of network traffic to a file.

All information required to perform the listed actions (description of the sequence of steps, changeable settings, configuration files, scripts, additional command line features, debugging modules, specialized utilities, etc.), as well as the composition of data analyzed for debugging purposes, will be announced by the Technical Support specialists. The advanced diagnostic information is stored on the user computer. Automatic transfer of the stored data to Kaspersky is not performed.

The actions listed above can only be performed under the guidance of the Technical Support specialists following the instructions received from them. Unassisted modification of the application settings in the ways not described in the application documentation or in the recommendations from the Technical Support specialists can lead to slowdowns and malfunctions of the operating system, decrease of the computer protection level, as well as to a violation of the availability and integrity of the processed information.

Data in trace and dump files

Kaspersky Endpoint Agent can write debug information to the trace files in accordance with the specified settings. Trace files are used for the purposes of technical support during the operation of Kaspersky Endpoint Agent.

Kaspersky Endpoint Agent dump files are generated by the operating system during application crashes and are overwritten by the next crash.

Trace and dump files may contain personal data of users or confidential data of your organization.

Do not use Kaspersky Endpoint Agent on the devices for which data submission is prohibited by the policy of your organization.

By default, Kaspersky Endpoint Agent does not record debug information.

Trace and dump files are not automatically sent outside the device on which they were generated. The content of trace files can be viewed using standard text file viewers.

Trace and dump files are stored permanently and are not deleted when Kaspersky Endpoint Agent is uninstalled.

Debug information can be useful for Technical Support.

No special mechanisms are provided for limiting access to trace and dump files. The administrator can configure this data to be written to a protected folder.

The path to the trace and dump file folder is not configured by default. To use the trace and dump folder, the administrator must specify it.

Data in trace and dump files can contain:

- Actions performed by Kaspersky Endpoint Agent on the device.
- Information about objects processed by Kaspersky Endpoint Agent.
- Errors arising during the operation of Kaspersky Endpoint Agent.

Network isolation

This section contains information about network isolation and how to configure it.

About network isolation in Kaspersky Endpoint Agent

Kaspersky Endpoint Agent provides the ability to isolate devices from the network on demand (manually) or automatically as in response to detections.

After enabling network isolation, the application breaks all active network connections on the devices and blocks all new TCP/IP network connections, except for the connections listed below:

- connections specified as network isolation exclusions;
- connections initiated by the services of compatible EPP application;
- connections initiated by the services of Kaspersky Endpoint Agent;
- connections initiated by Kaspersky Security Center Network Agent.

Enabling and disabling network isolation

Network isolation of the device can be enabled manually or automatically, as a result of response to detections.

Network isolation can be disabled automatically after a specified period of time or manually.

If the **Automatically disable network isolation after** check box is not selected in the network isolation settings and the time interval is not specified, network isolation will be disabled automatically after five hours since it was enabled.

After disabling network isolation, the device can work in the network without restrictions imposed by Kaspersky Endpoint Agent during network isolation.

Network isolation exclusions

You can configure network isolation exclusions. Network connections that meet the conditions of the specified rules will not be blocked on the devices after network isolation is enabled.

To simplify configuration of network isolation exclusions, a list of network profiles (sets of predefined rules) is available in the application. The list and contents of the network profiles cannot be edited.

Exclusions can be specified both as part of network profiles and separately. Exclusions specified separately from the network profiles are called *custom exclusions*.

By default, exclusions include network profiles, consisting of rules that ensure uninterrupted operation of devices with the DNS/DHCP server and DNS/DHCP client roles.

If you change the settings of the exclusion that was specified in the network profile, this exclusion will become custom.

Exclusions specified in the policy properties are applied only if network isolation is automatically enabled by the application in response to detection. Exclusions specified in the device properties are applied only if network isolation is enabled manually.

The active policy does not block the usage of network isolation exclusions specified in the device properties, since the scenarios for applying these settings are different.

About managing network isolation in Kaspersky Endpoint Agent

You can manage network isolation using Kaspersky Security Center or through the command line interface on the protected device. Information on managing network isolation by all these methods is shown in the next table.

Managing network isolation

Management interface	Capabilities	Notes
Kaspersky Security Center	• Enabling and disabling network isolation. • Configuring automatic disabling of network isolation. • Configuring device user notification about network isolation. • Configuring exclusions from network isolation.	The settings of automatic network isolation are configured in the policy properties, and the settings of network isolation on demand (manually enabled settings) are configured in the properties of an individual device. Manual enabling and disabling network isolation for a group of device in a policy is not available.
Command line	• Getting information about the current status and settings of the device network isolation. • Disabling network isolation on a device.	Network isolation cannot be enabled and network isolation setting cannot be configured using the command line interface.

Execution prevention

This section contains information about the Execution prevention function and how to configure its settings.

About Execution prevention

You can manage execution prevention rules for executable files and scripts, as well as for opening office-format files on the selected devices. For example, you can prevent launching the applications whose usage is considered unsafe on the selected device with Kaspersky Endpoint Agent installed. The application identifies the files by their paths or checksums using MD5 and SHA256 hash algorithms.

Execution prevention rule is a set of criteria that are considered when preventing an object from execution. The object must meet all the criteria of the Execution prevention rule in order for the application to block it from execution.

Settings of the Execution prevention rules can be managed using Kaspersky Security Center or from the command line.

When Kaspersky Endpoint Agent 3.9 is used, the prevention rules do not apply to files located on CDs or in ISO images. Execution or opening of such files is *not* blocked by the application.

Execution prevention rules mode

You can select one of the following modes of applying Execution prevention rules:

- **Statistics only**.

  In this mode, Kaspersky Endpoint Agent records to the Windows Event Log and to Kaspersky Security Center an event about attempts to execute objects or open documents that meet the criteria of the Execution prevention rules, but does not block execution or opening these objects.

- **Active**.

  In this mode, Kaspersky Endpoint Agent blocks execution of the objects or opening the documents that meet criteria of the Execution prevention rules.

When you enable Execution prevention in Kaspersky Security Center, the **Statistics only** mode is selected by default.

User notification about a triggered Execution prevention rule

You can select the **Notify device user about prevention** option. If Execution prevention is used in the **Active** mode and the **Notify device user about prevention** option is selected, pop-up notifications will be displayed on the protected devices with information about the triggered Execution prevention rules. If the device user does not close the pop-up notification, it will close automatically in 60 seconds after it appears. By default, the **Notify device user about prevention** option is disabled.

Managing Execution prevention

Execution prevention settings can be managed using Kaspersky Security Center or from the command line.

You can perform the following actions using Kaspersky Security Center:

- Enable and disable Execution prevention.
- Select application mode of Execution prevention rules.
- Configure user notification about a triggered Execution prevention rule.
- Configure the list of Execution prevention rules.
- Enable Execution prevention from the incident card.

Using the command line, you can disable Execution prevention or view the current Execution prevention settings.

Supported file extension for the Execution prevention feature

Kaspersky Endpoint Agent supports prevention of opening office-format files by means of certain applications. The supported file extensions and corresponding applications are listed in the following table.

Supported file extensions to prevent opening files by means of certain applications

Application name	Service name	File extension
Microsoft Word	winword.exe	• rtf • doc • dot • docm • docx • dotx • dotm • docb
WordPad	wordpad.exe	• docx • rtf
Microsoft Excel	excel.exe	• xls • xlt • xlm • xlsx

		• xlsm • xltx • xltm • xlsb • xla • xlam • xll • xlw
Microsoft PowerPoint	powerpnt.exe	• ppt • pot • pps • pptx • pptm • potx • potm • ppam • ppsx • ppsm • sldx • sldm
Adobe Acrobat Microsoft Edge Google Chrome	acrord32.exe MicrosoftEdge.exe chrome.exe	• pdf

Supported script execution interpreters

The script execution prevention is processed by Kaspersky Endpoint Agent if the script is launched using one of the following interpreters:

- cmd.exe

- reg.exe
- regedit.exe
- regedt32.exe
- cscript.exe
- wscript.exe
- mmc.exe
- msiexec.exe
- mshta.exe
- rundll32.exe
- runlegacycplelevated.exe
- control.exe
- explorer.exe
- regsvr32.exe
- wwahost.exe
- powershell.exe
- perl.exe
- hh.exe
- msbuild.exe
- python.exe
- InstallUtil.exe
- RegSvcs.exe
- RegAsm.exe
- ruby.exe
- rubyw.exe
- autoit.exe
- AutoHotkey.exe
- AutoHotkeyU32.exe
- AutoHotkeyA32.exe

- AutoHotkeyU64.exe
- AutoHotkeyA64.exe

Kaspersky Endpoint Agent supports execution prevention of Java applications running in the Java runtime environment (java.exe and javaw.exe processes).

IOC Scan

This section contains information about IOC Scan tasks and how to their settings.

About IOC Scan tasks in Kaspersky Endpoint Agent

While executing IOC Scan tasks Kaspersky Endpoint Agent uses IOC files (indicators of compromise files of the OpenIOC open description standard) to search for these indicators on devices.

Standard IOC Scan tasks are group or local tasks that are created and configured manually in Kaspersky Security Center or through the command line interface. IOC files prepared by the user are used to run the tasks.

Autonomous IOC Scan tasks are group tasks that are created automatically in response to the threats detected by Kaspersky Sandbox. Kaspersky Endpoint Agent generates an IOC file automatically. Operations with custom IOC files are not supported. Tasks are automatically deleted in seven days after the last start or after creation if tasks were never started. For more information about autonomous IOC Scan tasks, see *Kaspersky Sandbox Help*.

You can specify the following actions to respond to the detected IOCs (not available when running the tasks from the command line):

- **Isolate device from the network** to enable network isolation of the device on which indicator of compromise is detected by Kaspersky Endpoint Agent.

  Not available for Autonomous IOC Scan tasks.

- **Quarantine and delete** to quarantine the detected object and remove it from the device.

- **Run critical areas scan** to make Kaspersky Endpoint Agent send a command to EPP application to scan critical areas on all the devices of the administration group on which indicators of compromise are detected.
  The task execution report the can be viewed in the task execution results as a pivot table, and on the IOC incident card.

The results of group IOC Scan tasks execution can be viewed in Kaspersky Security Center within 7 days since the task execution completed, or until the task is removed.

Requirements for IOC files

When creating IOC Scan tasks, consider the following requirements and limitations related to IOC files:

- Kaspersky Endpoint Agent supports IOC files with the ioc and xml extensions. These files use open standard for IOC description – OpenIOC versions 1.0 and 1.1.

- If, when creating the IOC Scan task, you upload some IOC files that are not supported by Kaspersky Endpoint Agent then when the task starts, the application will use only supported IOC files.

- If, when creating the IOC Scan task, none of the downloaded IOC files is supported by Kaspersky Endpoint Agent, the task can be started, but as a result of the task execution, no indicators of compromise will be detected.

- Semantic errors and IOC terms and tags in IOC files that are not supported by the application do not cause the task execution errors. The application just does not detect matches in such sections of IOC files.
- Identifiers of all IOC files that are used in the same IOC Scan task must be unique. The presence of IOC files with the same identifier can affect the correctness of the task execution results.
- The size of a *single* IOC file must not exceed 3 MB. Using larger files results in the failure of IOC Scan tasks. In this case, the *total* size of all added files in the IOC collection can exceed 3 MB.
- It is recommended to create one IOC file per each threat. This makes it easier to read the results of the IOC Scan task.

Features and limitations of the OpenIOC standard support by the application are listed in the following table.

Features and limitations of the OpenIOC versions 1.0 and 1.1 standard support.

Supported conditions	OpenIOC 1.0:
	
	`is`
	`isnot` (as an exclusion from the set)
	`contains`
	`containsnot` (as an exclusion from the set)
	OpenIOC 1.1:
	
	`is`
	`contains`
	`starts-with`
	`ends-with`
	`matches`
	`greater-than`
	`less-than`

Supported condition attributes	OpenIOC 1.1:
	
	`preserve-case`
	`negate`

Supported operators	`AND` `OR`
Supported data types	`date`: date (applicable conditions: `is`, `greater-than`, `less-than`) `int`: integer number (applicable conditions: `is`, `greater-than`, `less-than`) `string`: string (applicable conditions: `is`, `contains`, `matches`, `starts-with`, `ends-with`) `duration`: duration in seconds (applicable conditions: `is, greater-than, less-than`)
Data types interpretation details	The following data types are interpreted as string: `Boolean string`, `restricted string`, `md5`, `IP`, `sha256`, `base64Binary`. The application supports interpretation of the `Content` parameter specified as intervals for the following data types: `int` and `date`: OpenIOC 1.0: Using the `TO` operator in the `Content` field: `<Content type="int">49600 TO 50700</Content>`

	`<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>`
	`<Content type="int">[154192 TO 154192]</Content>`
	OpenIOC 1.1:
	Using the `greater-than` and `less-than` conditions
	Using the `TO` operator in the `Content` field
	The application supports interpretation of the `date` and `duration` data types if the indicators are specified in the `ISO 8601, Zulu time zone, UTC` format.

Supported IOC terms	The full list of supported IOC terms is provided in a separate table.

Supported IOC terms

The file that can be downloaded by the following link contains a table with a full list of supported IOC terms of the OpenIOC standard.

DOWNLOAD IOC_TERMS.XLSX FILE

Managing IOC Scan tasks in Kaspersky Endpoint Agent

You can manage standard IOC Scan tasks using Kaspersky Security Center or through the command line interface of Kaspersky Endpoint Agent.

You can perform the following actions using Kaspersky Security Center:

- Creating, removing and starting the task manually.
- Configuring task schedule settings.
- Configuring settings in the task properties.
- Viewing reports in the task execution results.

You can perform the following actions using the command line interface:

- Creating and running the task with the required settings.
- Viewing data on the task execution.

The user has limited control over autonomous IOC Scan tasks using Kaspersky Security Center. For more information about autonomous IOC Scan tasks, see *Kaspersky Sandbox Help*.

Managing the application using Kaspersky Security Center Web Console and Kaspersky Security Center Cloud Console

Kaspersky Security Center

Kaspersky Security Center provides centralized solution to the main tasks of managing and maintaining the organization network protection system. The application provides the administrator with access to detailed information about the security level of the organization network and allows configuring all the components of protection built based on Kaspersky applications.

Kaspersky Security Center enables remote installation, uninstallation, start and stop of Kaspersky Endpoint Agent, as well as configuration of the application settings, and start and stop of the application tasks. Kaspersky Security Center provides differentiation of access permissions to Kaspersky Endpoint Agent using the Role Based Access Control (RBAC) technology.

For detailed information on Kaspersky Security Center, refer to *Kaspersky Security Center Help*.

Kaspersky Security Center can be managed using *Kaspersky Security Center Web Console* (also referred to as *Web Console*). Web Console is a web interface for creating and managing the security system of a client organization network managed by Kaspersky Security Center.

Kaspersky Security Center Cloud Console

Kaspersky Security Center Cloud Console – is an application hosted and maintained by Kaspersky. You do not need to install Kaspersky Security Center Cloud Console on your computer or server. Kaspersky Security Center Cloud Console allows the administrator to install Kaspersky security applications on devices in the corporate network, remotely run scan and update tasks, and manage security policies of the managed applications. The administrator can use the detailed monitoring dashboard, where you can view snapshots of the corporate device statuses, detailed reports and detailed protection policy settings.

Kaspersky Security Center Cloud Console and Kaspersky Security Center enable remote installation, uninstallation, start and stop of Kaspersky Endpoint Agent, as well as configuration of the application settings, and start and stop of the application tasks.

Kaspersky Security Center Cloud Console is managed by the *Cloud Administration Console*, which is a web interface for creating and managing the client organization network protection system controlled by Security Center Cloud Console.

For detailed information on Kaspersky Security Center Cloud Console, refer to *Kaspersky Security Center Cloud Console Help*.

Managing Kaspersky Endpoint Agent

This section provides universal instructions for managing Kaspersky Endpoint Agent, which are suitable both for Kaspersky Security Center Web Console and Cloud Administration Console.

To manage Kaspersky Endpoint Agent using the Web Console, install Kaspersky Endpoint Agent Management web plug-in.

About Kaspersky Endpoint Agent web plug-in

Kaspersky Endpoint Agent Management web plug-in provides interaction between Kaspersky Endpoint Agent and Kaspersky Security Center Web Console. The web plug-in allows managing Kaspersky Endpoint Agent using the following tools: policies, tasks, and local application settings.

You can install the web plug-in in one of the following ways:

- Install web plug-in using the Initial Setup Wizard of Kaspersky Security Center Web Console.
- Install web plug-in from the list of available distribution packages in the Web Console.

  For detailed information on installing management web plug-ins, refer to Kaspersky Security Center Help.
- Download the distribution package to the Web Console from a third-party source.

  To install the web plug-in, add a ZIP archive with the distribution package of Kaspersky Endpoint Security web plug-in to the Web Console interface (Console settings → Plug-ins). You can download the web plug-in distribution kit, for example, from Kaspersky website.

The installer of Kaspersky Endpoint Agent and Kaspersky Endpoint Agent management plug-in automatically selects the application localization based on the operating system regional settings on the device where the application or management plug-in is installed:

- If the operating system uses the RU-RU locale, the Russian version of Kaspersky Endpoint Agent and Kaspersky Endpoint Agent management plug-in is installed.
- If the operating system uses any locale other than RU-RU, the English version of Kaspersky Endpoint Agent and Kaspersky Endpoint Agent management plug-in is installed.

Application localization affects the language of texts used to describe application modules in the system and when publishing application events to the Windows Event Log, as well as texts of Kaspersky Security Center reports. Kaspersky Endpoint Agent management plug-in localization affects the language of texts used in the application interface of Administration Console (interface of policies, group tasks, and application properties). The application localization cannot be configured manually.

Please note that if regional settings on managed devices and on the device with Kaspersky Endpoint Agent management plug-in do not match, localization of Kaspersky Endpoint Agent interface in the Administration Console and localization of events published by the application to Kaspersky Security Center reports may not match. Also, the localization of the application interface in the Administration Console and the localization of events published by the application to Kaspersky Security Center reports may differ from the localization of Administration Console interface and the compatible EPP interface in the Administration Console.

Managing Kaspersky Endpoint Agent policies

This section describes how to create Kaspersky Endpoint Agent policy and enable policy settings.

Creating Kaspersky Endpoint Agent policy

To create Kaspersky Endpoint Agent policy in Kaspersky Security Center Web Console:

1. In the main window select **Devices** → **Policies and profiles**.
2. Click the **Add** button.

   The policy creation wizard starts.
3. Select the Kaspersky Endpoint Agent application and click **Next**.
4. Select the required Kaspersky Endpoint Agent deployment method by selecting the appropriate check boxes:
   - **Kaspersky Sandbox integration**
   - **Endpoint Detection and Response Optimum**
   - **Endpoint Detection and Response Expert (KATA EDR)**

   Policy type and integration with Kaspersky Sandbox and KATA EDR cannot be selected in Kaspersky Security Center Cloud Console.
5. Click **Next**.
6. On the **General** tab, you can perform the following actions:
   - Change the policy name.
   - Select policy status:
     - **Active**. After the next synchronization, the policy will be used as active on the computer.
     - **Inactive**. Backup policy. An inactive policy can be made active, if required.
     - **Out-of-office**. The policy becomes active when the computer leaves the corporate network.
   - Configure the policy settings inheritance:
     - **Inherit settings from parent policy**. If this option is enabled, the policy settings are inherited from the upper-level policy. The policy settings cannot be modified if the **Force inheritance of settings in child policies** option is enabled in the parent policy.
     - **Force inheritance of settings in child policies**. If this option is enabled, the parent policy settings are applied to child policies. In the properties window of the child policy, the **Inherit settings from parent policy** option is automatically enabled and cannot be disabled.
7. On the **Application settings** tab, you can configure Kaspersky Endpoint Agent policy settings.
8. Click the **Save** button.

Enabling settings in Kaspersky Endpoint Agent policy

When you configure Kaspersky Endpoint Agent policy settings, by default these settings are saved, but are not applied until you enable them.

You can enable settings for the groups where these settings are located. You can enable either individual groups of settings or all groups of settings within one policy.

To enable the group of settings in Kaspersky Endpoint Agent policy:

1. Open the policy properties window.

   1. In the main Kaspersky Security Center Web Console window select **Devices** → **Policies and profiles**.
   2. Select the policy you want to configure.
   3. In the **<Policy name>** window that opens, select the **Application settings** tab.

2. Select the section and group of settings to which the required setting belongs.
3. In the upper right corner of the settings group, change the switch from **Undefined** to **Enforce**.

   All the settings of the group will be applied in the policy.

Configuring Kaspersky Endpoint Agent settings

This section describes how to configure Kaspersky Endpoint Agent settings.

Opening Kaspersky Endpoint Agent settings window

To open Kaspersky Endpoint Agent policy settings window:

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Policies and profiles**.
2. Select the policy you want to configure.
3. In the **<Policy name>** window that opens, select the **Application settings** tab.

To open Kaspersky Endpoint Agent settings window for an individual device:

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Managed devices**.
2. Select the device.
3. In the **<Device name>** window that opens, select the **Applications** tab.
4. Select **Kaspersky Endpoint Agent**.
5. In the window that opens, select the **Application settings** tab.

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

The settings of automatic network isolation are configured in the policy properties, and the settings of network isolation on demand (manually enabled settings) are configured in the properties of an individual device.

Configuring Kaspersky Endpoint Agent security settings

To ensure maximum security of the IT infrastructure in your organization, you can configure access of users and third-party processes to Kaspersky Endpoint Agent. To do so, you can:

- Restrict user permissions to manage the application settings and services.
- Protect actions in the application with a password.
- Enable the application self-defense mechanism.

Configuring user permissions

You can grant access to Kaspersky Endpoint Agent to individual users or groups of users. As a result, only specified users will be able to manage settings or services of the application.

To configure user permissions:

1. Do one of the following:

   - **Open the application properties window for an individual device**.

     1. In the main Kaspersky Security Center Web Console window select **Devices** → **Managed devices**.
     2. Select the device.
     3. In the **<Device name>** window that opens, select the **Applications** tab.
     4. Select **Kaspersky Endpoint Agent**.
     5. In the window that opens, select the **Application settings** tab.

   - **Open the policy properties window**.

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Policies and profiles**.
2. Select the policy you want to configure.
3. In the **<Policy name>** window that opens, select the **Application settings** tab.

2. In the **Application settings** section select the **Security settings** subsection.
3. In the **User permissions for application service management** group of settings, click the **Configure** button next to the name of the required setting (**User permissions for application management** or **Configure user permissions for application management**).

   To add users and user groups, specify the security descriptor strings using the Security Descriptor Description Language (SDDL).
4. If you configure the policy settings, in the upper right corner of the group of settings, change the switch from **Undefined** to **Enforce**.
5. Click **OK**.
6. Click the **Save** button.

Enabling Password protection

Unrestricted user access to the application and its settings can reduce the security level of the device. Password protection allows to limit user access to the application.

To enable password protection:

1. Do one of the following:

   - Open the application properties window for an individual device.

     1. In the main Kaspersky Security Center Web Console window select **Devices** → **Managed devices**.
     2. Select the device.
     3. In the **<Device name>** window that opens, select the **Applications** tab.
     4. Select **Kaspersky Endpoint Agent**.
     5. In the window that opens, select the **Application settings** tab.

   - Open the policy properties window.

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Policies and profiles**.
2. Select the policy you want to configure.
3. In the **<Policy name>** window that opens, select the **Application settings** tab.

2. In the **Application settings** section select the **Security settings** subsection.
3. In the **Password protection** group of settings select the **Apply password protection** check box.
4. Enter a password and confirm it.

   It is recommended to select the password that meets the following requirements:

   - Password must be at least 8 characters long.
   - Password must not contain user account name.
   - Password must not match the name of the device on which Kaspersky Endpoint Agent is installed.
   - Password must contain characters from at least three of the following groups:
     - uppercase characters (A-Z);
     - lowercase characters (A-Z) (a-z);
     - numbers (0-9);
     - special characters (!$#%).
5. If you configure the policy settings, in the upper right corner of the group of settings, change the switch from **Undefined** to **Enforce**.
6. Click **OK**.
7. Click the **Save** button.

Password protection is enabled. If a user attempts to perform a password protected action, the application prompts the user to enter the password.

The application does not check the strength of the specified password. We recommend that you use third-party tools to verify the strength of the password. The password is considered strong enough, if verification results confirm that the password cannot be guessed for at least 6 months.

The application does not prohibit from entering password after many attempts of entering incorrect password.

Enabling and disabling Self-Defense

The Self-Defense mechanism of Kaspersky Endpoint Agent provides protection from malware that tries to lock the application or delete it. The Self-Defense mechanism prevents alteration or deletion of application files on the hard drive, memory processes, and entries in the system registry.

To enable or disable Self-Defense:

1. Do one of the following:

   - Open the application properties window for an individual device.

     1. In the main Kaspersky Security Center Web Console window select **Devices** → **Managed devices**.
     2. Select the device.
     3. In the **<Device name>** window that opens, select the **Applications** tab.
     4. Select **Kaspersky Endpoint Agent**.
     5. In the window that opens, select the **Application settings** tab.

   - Open the policy properties window.

     1. In the main Kaspersky Security Center Web Console window select **Devices** → **Policies and profiles**.
     2. Select the policy you want to configure.
     3. In the **<Policy name>** window that opens, select the **Application settings** tab.

2. In the **Application settings** section select the **Security settings** subsection.
3. In the **Self-defense** group of settings, do one of the following:

   - Select the **Enable self-defense for application modules in memory** check box to enable the self-defense mechanism.
   - Clear the **Enable self-defense for application modules in memory** check box to disable the self-defense mechanism.

4. If you configure the policy settings, in the upper right corner of the group of settings, change the switch from **Undefined** to **Enforce**.
5. Click **OK**.
6. Click the **Save** button.

The Self-Defense mechanism is enabled or disabled.

Configuring Kaspersky Endpoint Agent connection settings to a proxy server

Proxy server connection settings are used for updating databases, activating the application, and external services.

To configure proxy server connection settings:

1. Do one of the following:

   - Open the application properties window for an individual device.

     1. In the main Kaspersky Security Center Web Console window select **Devices** → **Managed devices**.
     2. Select the device.
     3. In the **<Device name>** window that opens, select the **Applications** tab.
     4. Select **Kaspersky Endpoint Agent**.
     5. In the window that opens, select the **Application settings** tab.

   - Open the policy properties window.

     1. In the main Kaspersky Security Center Web Console window select **Devices** → **Policies and profiles**.
     2. Select the policy you want to configure.
     3. In the **<Policy name>** window that opens, select the **Application settings** tab.

2. In the **Application settings** section select the **Security settings** subsection.
3. Select one of the following proxy service usage options:

   - **Do not use proxy server**.
   - **Use proxy server with specified settings**.

4. If you select the **Use proxy server with specified settings** option, specify the address and port of the proxy server you want to connect to in the **Server name or IP address** and **Port** fields.

   The default port number is 8080.

5. If you want to use NTLM authentication for connecting to the proxy server:

   a. Select the **Use NTLM authentication by user name and password** check box.

   b. In the **User name** field, enter the name of the user, whose account will be used for proxy server authentication.

c. In the **Password** field, enter the password for connecting to the proxy server.

You can make password characters visible by clicking **Show** to the right of the **Password** field.

6. If you do not want to use the proxy server for internal addresses of your organization, select the **Bypass proxy server for local addresses** check box.

7. If you configure the policy settings, in the upper right corner of the group of settings, change the switch from **Undefined** to **Enforce**.

8. Click **OK**.

9. In the policy properties window, click **Save**.

Proxy server connection settings are configured.

Configuring Kaspersky Security Center as a proxy server for Kaspersky Endpoint Agent activation

To enable usage of Kaspersky Security Center as a proxy server for the application activation:

1. Do one of the following:

- Open the application properties window for an individual device.

    1. In the main Kaspersky Security Center Web Console window select **Devices** → **Managed devices**.
    2. Select the device.
    3. In the **<Device name>** window that opens, select the **Applications** tab.
    4. Select **Kaspersky Endpoint Agent**.
    5. In the window that opens, select the **Application settings** tab.

- Open the policy properties window.

    1. In the main Kaspersky Security Center Web Console window select **Devices** → **Policies and profiles**.
    2. Select the policy you want to configure.
    3. In the **<Policy name>** window that opens, select the **Application settings** tab.

2. In the **Application settings** section select the **Security settings** subsection.

3. In the **Licensing** group of settings, select the **Use Kaspersky Security Center as a proxy server when activating the application** check box.

4. If you configure the policy settings, in the upper right corner of the group of settings, change the switch from **Undefined** to **Enforce**.

5. Click **OK**.

6. In the policy properties window, click **Save**.

Kaspersky Security Center usage as a proxy server for Kaspersky Endpoint Agent activation is now enabled.

Configuring malfunction diagnosis

Kaspersky Endpoint Agent does not automatically create a folder for storing trace or dump files on the device. Specify a folder that is already available on the device.

To configure malfunction diagnosis:

1. Open the application properties window for an individual device.

    1. In the main Kaspersky Security Center Web Console window select **Devices** → **Managed devices**.
    2. Select the device.
    3. In the **<Device name>** window that opens, select the **Applications** tab.
    4. Select **Kaspersky Endpoint Agent**.
    5. In the window that opens, select the **Application settings** tab.

2. In the **Application settings** section select the **Malfunction diagnosis** subsection.

3. To enable logging of debug information to the trace files:

    a. Select the **Write debug information to trace files** check box.

    b. In the **Trace files folder** field, specify the folder to save the trace files.

4. To enable logging of dump files:

    a. Select the **Create dump files** check box.

    b. In the **Dump files folder** field, specify the folder to save the dump files.

5. Click **OK**.

6. Click the **Save** button.

Configuring KSN usage in Kaspersky Endpoint Agent

To protect your computer more effectively, Kaspersky Endpoint Security uses data received from users around the globe. Kaspersky Security Network is designed to receive such data.

Kaspersky Security Network (KSN) is an infrastructure of cloud services providing access to the online Kaspersky Knowledge Base that contains information about the reputation of files, web resources, and software. The use of data from Kaspersky Security Network ensures faster responses by the EPP application to objects that are not yet listed in anti-virus application databases, improves performance of some protection components, and reduces the likelihood of false positives.

Participation in Kaspersky Security Network allows Kaspersky to quickly acquire information about the types and sources of objects that are not yet listed in anti-virus application databases, develop methods for neutralizing such objects, and reduce the number of false positives.

When you use Kaspersky Security Network, certain statistical data collected while Kaspersky Endpoint Agent is running is automatically sent to Kaspersky. Files or their parts which may be exploited by intruders to harm the computer or data can be also sent to Kaspersky to be examined additionally.

No personal data is collected, processed, or stored. The types of data that Kaspersky Endpoint Agent sends to Kaspersky Security Network are described in the KSN Statement.

Participation in Kaspersky Security Network is voluntary. KSN usage is disabled by default. After enabling KSN usage, you can disable this option at any time.

Starting from version 3.10, Kaspersky Managed Protection (also referred to as KMP) usage cannot be configured by means of Kaspersky Endpoint Agent. If usage of the KMP service was enabled in the previous Kaspersky Endpoint Agent version, the KMP service continues functioning after the application is updated to version 3.10. After the application update, you can disable the KMP service only using Kaspersky Endpoint Agent Administration Plug-in or Kaspersky Endpoint Agent Web Plug-in of versions earlier then 3.10.

To enable KSN usage:

1. Do one of the following:

   - Open the application properties window for an individual device.

     1. In the main Kaspersky Security Center Web Console window select **Devices** → **Managed devices**.
     2. Select the device.
     3. In the **<Device name>** window that opens, select the **Applications** tab.
     4. Select **Kaspersky Endpoint Agent**.
     5. In the window that opens, select the **Application settings** tab.

   - Open the policy properties window.

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Policies and profiles**.
2. Select the policy you want to configure.
3. In the **<Policy name>** window that opens, select the **Application settings** tab.

2. In the **Kaspersky Security Network** section, click the **Read terms and conditions of the KSN Statement** link and perform the following actions:
   a. In the right part of the window, review the terms and conditions of KSN Statement.
   b. If you agree with terms and conditions of the Statement, select the **I confirm that I have fully read, understand, and accept the terms and conditions of this KSN Statement** check box.
   c. Click **OK**.
3. Select the **Enable Kaspersky Security Network (KSN) usage** check box.
4. If you configure the policy settings, in the upper right corner of the group of settings, change the switch from **Undefined** to **Enforce**.
5. Click **OK**.
6. In the policy properties window, click **Save**.

KSN usage is enabled.

Configure network isolation settings

This section describes how to configure the network isolation settings by means of Kaspersky Endpoint Agent Management plug-in.

Enabling and disabling network isolation

To enable or disable network isolation of a device:

1. Open the application properties window for an individual device.

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Managed devices**.
2. Select the device.
3. In the **<Device name>** window that opens, select the **Applications** tab.
4. Select **Kaspersky Endpoint Agent**.
5. In the window that opens, select the **Application settings** tab.

2. In the **Network Isolation** section select **General settings**.
3. In the **Isolate device** group of settings, select or clear the **Isolate this device from the network** check box.
4. Click **OK** to save the changes.

Manual enabling and disabling network isolation for a group of device in a policy is not available.

Enabling and disabling user notification about network isolation

The settings of automatic network isolation are configured in the policy properties, and the settings of network isolation on demand (manually enabled settings) are configured in the properties of an individual device.

To enable or disable the user notification about network isolation:

1. Do one of the following:
   - Open the application properties window for an individual device.
     1. In the main Kaspersky Security Center Web Console window select **Devices** → **Managed devices**.
     2. Select the device.
     3. In the **<Device name>** window that opens, select the **Applications** tab.
     4. Select **Kaspersky Endpoint Agent**.
     5. In the window that opens, select the **Application settings** tab.
   - Open the policy properties window.

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Policies and profiles**.
2. Select the policy you want to configure.
3. In the **<Policy name>** window that opens, select the **Application settings** tab.

2. In the **Network Isolation** section select **General settings**.
3. In the **Notification** group of settings select or clear the **Notify device user when device is isolated from the network** check box.
4. Click **OK** to save the changes.

Configuring automatic disabling of network isolation

The settings of automatic network isolation are configured in the policy properties, and the settings of network isolation on demand (manually enabled settings) are configured in the properties of an individual device.

To configure the settings for automatic disabling of network isolation:

1. Do one of the following:

   - Open the application properties window for an individual device.

     1. In the main Kaspersky Security Center Web Console window select **Devices** → **Managed devices**.
     2. Select the device.
     3. In the **<Device name>** window that opens, select the **Applications** tab.
     4. Select **Kaspersky Endpoint Agent**.
     5. In the window that opens, select the **Application settings** tab.

   - Open the policy properties window.

     1. In the main Kaspersky Security Center Web Console window select **Devices** → **Policies and profiles**.
     2. Select the policy you want to configure.
     3. In the **<Policy name>** window that opens, select the **Application settings** tab.

2. In the **Network Isolation** section select **General settings**.

3. In the **Device isolation terms** group of settings, do one of the following:

   - Clear the **Automatically end device isolation after** check box to disable automatic disabling of network isolation after a specified period of time.

     This feature is enabled by default.

   - Select the **Automatically end device isolation after** check box to enable automatic disabling of network isolation after a specified period of time.

4. In the **Notification** group of settings select or clear the **Notify device user when device is isolated from the network** check box.

5. Specify the period after which network isolation will be disabled.

   The default period is 30 minutes.

6. Click **OK** to save the changes.

If the **Automatically disable network isolation after** check box is not selected in the network isolation settings and the time interval is not specified, network isolation will be disabled automatically after five hours since it was enabled.

Configuring exclusions from network isolation

Exclusions specified in the policy properties are applied only if network isolation is automatically enabled by the application in response to detection. Exclusions specified in the device properties are applied only if network isolation is enabled manually.

The active policy does not block the usage of network isolation exclusions specified in the device properties, since the scenarios for applying these settings are different.

To configure the settings of network isolation exclusions:

1. Do one of the following:

   - Open the application properties window for an individual device.

     1. In the main Kaspersky Security Center Web Console window select **Devices** → **Managed devices**.
     2. Select the device.
     3. In the **<Device name>** window that opens, select the **Applications** tab.
     4. Select **Kaspersky Endpoint Agent**.
     5. In the window that opens, select the **Application settings** tab.

   - Open the policy properties window.

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Policies and profiles**.
2. Select the policy you want to configure.
3. In the **<Policy name>** window that opens, select the **Application settings** tab.

2. If you open the application properties window for an individual device, in the **Network Isolation** section, select **Exclusions**.
3. If you open the application policy properties window, in the **Network Isolation** section, select **Isolation on detection**.

   You can perform the following actions:

   - Add custom exclusion

     To add a custom exclusion:

     1. Click **Add**.

        The **Rule properties** window opens.
     2. Specify the required exclusion settings and click **OK**.

        The new rule is added to the exclusion list.

   - Add exclusions from the list of predefined network profiles

     To add exclusions from the list of predefined network profiles:

     1. Click **Add**.

        In the window that opens, select the required network profile from **Predefined network profiles list**.

        You can select several network profiles at once.
     2. Click **OK**.

        Exclusions from the selected network profiles are added to the list of exclusions.

   - Change the settings of the added exclusion

To change the settings of the added exclusion:

1. Click the name of the required rule.
2. The **Rule properties** window opens.
3. Make the required changes and click **OK**.

   The selected exclusion is changed.

If you change the settings of the exclusion that was specified in the network profile, this exclusion will become custom.

- Remove exclusion from the list

To remove an exclusion from the list:

1. In the **Exclusions** list, select the exclusion you want to remove.
2. Click the **Remove** button.

   The exclusion is removed from the list of exclusions.

4. Click **OK** to save the changes.

Configuring Execution prevention settings

This section describes how to configure Execution prevention.

Enabling Execution prevention

To enable Execution prevention:

1. Do one of the following:

   - Open the application properties window for an individual device.

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Managed devices**.
2. Select the device.
3. In the **<Device name>** window that opens, select the **Applications** tab.
4. Select **Kaspersky Endpoint Agent**.
5. In the window that opens, select the **Application settings** tab.

- Open the policy properties window.

  1. In the main Kaspersky Security Center Web Console window select **Devices** → **Policies and profiles**.
  2. Select the policy you want to configure.
  3. In the **<Policy name>** window that opens, select the **Application settings** tab.

2. Select the **Execution Prevention** section.
3. In the **Prevention mode** group of settings, select the **Enable the prevention of untrusted objects execution** check box.
4. In the **Apply prevention rules in mode** drop-down list, select the required mode for applying Execution prevention rules:

   - **Statistics only**.

     In this mode, Kaspersky Endpoint Agent records to the Windows Event Log and to Kaspersky Security Center an event about attempts to execute objects or open documents that meet the criteria of the Execution prevention rules, but does not block execution or opening these objects.

   - **Active**.

     In this mode, Kaspersky Endpoint Agent blocks execution of the objects or opening the documents that meet criteria of the Execution prevention rules.

   When you enable Execution prevention in Kaspersky Security Center, the **Statistics only** mode is selected by default.

5. If you configure the policy settings, in the upper right corner of the group of settings, change the switch from **Undefined** to **Enforce**.
6. Click **OK**.
7. Click the **Save** button.

Disabling Execution prevention

To disable Execution prevention:

1. Do one of the following:

   - Open the application properties window for an individual device.

     1. In the main Kaspersky Security Center Web Console window select **Devices** → **Managed devices**.
     2. Select the device.
     3. In the **<Device name>** window that opens, select the **Applications** tab.
     4. Select **Kaspersky Endpoint Agent**.
     5. In the window that opens, select the **Application settings** tab.

   - Open the policy properties window.

     1. In the main Kaspersky Security Center Web Console window select **Devices** → **Policies and profiles**.
     2. Select the policy you want to configure.
     3. In the **<Policy name>** window that opens, select the **Application settings** tab.

2. Select the **Execution Prevention** section.
3. In the **Prevention mode** group of settings, clear the **Enable the prevention of untrusted objects execution** check box.
4. If you configure the policy settings, in the upper right corner of the group of settings, change the switch from **Undefined** to **Enforce**.
5. Click **OK**.
6. Click the **Save** button.

Enabling and disabling user notification about Execution prevention

You can select the **Notify device user about prevention** option.

If Execution prevention is used in the **Active** mode and the **Notify device user about prevention** option is selected, pop-up notifications will be displayed on the protected devices with information about the triggered Execution prevention rules. If the device user does not close the pop-up notification, it will close automatically in 60 seconds after it appears. By default, the **Notify device user about prevention** option is disabled.

Execution prevention must be enabled.

To enable or disable the user notification about Execution prevention:

1. Do one of the following:

- Open the application properties window for an individual device.

  1. In the main Kaspersky Security Center Web Console window select **Devices** → **Managed devices**.
  2. Select the device.
  3. In the **<Device name>** window that opens, select the **Applications** tab.
  4. Select **Kaspersky Endpoint Agent**.
  5. In the window that opens, select the **Application settings** tab.

- Open the policy properties window.

  1. In the main Kaspersky Security Center Web Console window select **Devices** → **Policies and profiles**.
  2. Select the policy you want to configure.
  3. In the **<Policy name>** window that opens, select the **Application settings** tab.

2. Select the **Execution Prevention** section.
3. In the **Prevention mode** group of settings select or clear the **Notify device user about prevention** check box.
4. If you configure the policy settings, in the upper right corner of the group of settings, change the switch from **Undefined** to **Enforce**.
5. Click **OK**.
6. In the policy properties window, click **Save**.

Managing the set of Execution prevention rules

To configure the list of Execution prevention rules:

1. Do one of the following:

   - Open the application properties window for an individual device.

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Managed devices**.
2. Select the device.
3. In the **<Device name>** window that opens, select the **Applications** tab.
4. Select **Kaspersky Endpoint Agent**.
5. In the window that opens, select the **Application settings** tab.

- Open the policy properties window.

  1. In the main Kaspersky Security Center Web Console window select **Devices** → **Policies and profiles**.
  2. Select the policy you want to configure.
  3. In the **<Policy name>** window that opens, select the **Application settings** tab.

2. Select the **Execution Prevention** section.
3. You can do the following actions in the **Prevention rules** group of settings:
   - Add a prevention rule to the list.
   - Change a prevention rule settings.
   - Remove a prevention rule from the list.
4. If you configure the policy settings, in the upper right corner of the group of settings, change the switch from **Undefined** to **Enforce**.
5. Click **OK**.
6. In the policy properties window, click **Save**.

When Kaspersky Endpoint Agent 3.9 is used, the prevention rules do not apply to files located on CDs or in ISO images. Execution or opening of such files is *not* blocked by the application.

When using Kaspersky Endpoint Agent 3.10 or later to create a prevention rule based on the path to a file located on a CD or in an ISO image, specify the path in the following format: `\?\GLOBALROOT\Device\<device name>\<file path>`, where `<device name>` is the name of the CD-ROM drive or mounted ISO image in your system. For example, the path might be like this: `\?\GLOBALROOT\Device\CdRom1\some_file.exe`.

When specifying objects by the file path criterion, you can use file masks (using the? and * characters).

Configuring storage settings in Kaspersky Endpoint Agent

This section describes how to configure the quarantine settings and data synchronization settings with the Administration Server by means of Kaspersky Endpoint Agent Management plug-in.

About Kaspersky Endpoint Agent quarantine

Quarantine is a special local repository on a device with Kaspersky Endpoint Agent installed which is intended for storing files that are probably infected by viruses or cannot be disinfected at the time when they are detected. Quarantined files are stored in an encrypted form and therefore do not compromise your device's security.

By default, the local quarantine is located in the `%ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\<application version>\Quarantine` folder. By default, the objects restored from quarantine are stored in the `%ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\<application version>\Restored` folder.

Kaspersky Security Center generates a common list of quarantined objects on devices with Kaspersky Endpoint Agent installed. Network Agents on the devices submit information about quarantined files to the Administration Server.

Kaspersky Security Center does not copy files from quarantine to the Administration Server. All objects are stored on protected devices with Kaspersky Endpoint Agent installed. Objects are restored from the quarantine also on the protected devices.

About quarantine management in Kaspersky Endpoint Agent

You can use Kaspersky Security Center to configure quarantine settings, view the properties of the quarantined objects on the protected devices, delete quarantined objects, and restore objects from Quarantine. For detailed information on managing the quarantined objects using Kaspersky Security Center, refer to Kaspersky Security Center documentation.

In order for Kaspersky Endpoint Agent to send data about quarantined objects to Kaspersky Security Center Administration Server, the corresponding option must be enabled in the quarantine settings in Kaspersky Endpoint Agent policy. This option is enabled by default.

Using the command line interface on the device, you can view information about quarantine settings and properties of the quarantined objects.

Kaspersky Endpoint Agent quarantines object under the system account (SYSTEM).

Quarantined objects can be removed using the command line interface only with the permissions of the local account of the protected device user.

Configuring quarantine settings and restoration of objects from quarantine

To configure the quarantine settings:

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Policies and profiles**.
2. Select the policy you want to configure.
3. In the **<Policy name>** window that opens, select the **Application settings** tab.
4. In the **Repositories** section select the **Quarantine** subsection.
5. In the **Quarantine settings** section configure the quarantine settings:

   a. In the **Quarantine folder** field, enter the path to where you want to create the Quarantine folder on the devices or click **Browse** and select the path.

   The default path is `%SOYUZAPPDATA%\Quarantine\`. The Quarantine folder is created on all devices with Kaspersky Endpoint Agent at the following path: `%ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0`.

   The value of the `%ALLUSERSPROFILE%` variable depends on the operating system of the device where Kaspersky Endpoint Agent is installed.

   Example:
   If the device has the Windows 7 operating system installed and Kaspersky Endpoint Agent is installed on drive C, the path to the Quarantine folder is:
   `C:\ProgramData\Kaspersky Lab\Endpoint Agent\4.0\Quarantine`

   b. To configure the maximum quarantine size, select the **Maximum Quarantine size (MB)** check box and type the maximum size of quarantine in MB or select it from the list.

   For example, you can set the maximum quarantine size to 200 MB.

   When the maximum quarantine size is reached, Kaspersky Endpoint Agent publishes the corresponding event on Kaspersky Security Center server and in the Windows Event Log, but does not stop quarantining new objects.

   c. To specify the quarantine threshold (the space in quarantine remaining until the maximum quarantine size is reached), select the **Available space threshold (MB)** check box.

   For example, you can set the quarantine threshold value to 50 MB.

   When the quarantine threshold is reached, Kaspersky Endpoint Agent publishes the corresponding event on Kaspersky Security Center server and in the Windows Event Log, but does not stop quarantining new objects.

6. In the **Restoring objects from Quarantine** section, in the **Target folder for restored objects** field, specify the path to create the folder for objects restored from quarantine.

   The default path is `%SOYUZAPPDATA%\Restored\`. The Restored folder is created on all devices with Kaspersky Endpoint Agent at the following path: `%ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0`.

   The value of the `%ALLUSERSPROFILE%` variable depends on the operating system of the device where Kaspersky Endpoint Agent is installed.

   Example:
   If the device has the Windows 7 operating system installed and Kaspersky Endpoint Agent is installed on drive C, the path to the folder with the objects restored from quarantine is:
   `C:\ProgramData\Kaspersky Lab\Endpoint Agent\4.0\Restored`

7. In the upper right corner of the settings group, change the switch from **Undefined** to **Enforce**.
8. Click **Apply** and **OK**.

Quarantine settings and the folder for restoring objects from quarantine are configured.

Configuring data synchronization with the Administration Server

You can configure synchronization of data on quarantined objects on managed devices with Kaspersky Security Center Administration Server.

To configure data synchronization with the Administration Server:

1. Do one of the following:

   - Open the application properties window for an individual device.

     1. In the main Kaspersky Security Center Web Console window select **Devices** → **Managed devices**.
     2. Select the device.
     3. In the **<Device name>** window that opens, select the **Applications** tab.
     4. Select **Kaspersky Endpoint Agent**.
     5. In the window that opens, select the **Application settings** tab.

   - Open the policy properties window.

     1. In the main Kaspersky Security Center Web Console window select **Devices** → **Policies and profiles**.
     2. Select the policy you want to configure.
     3. In the **<Policy name>** window that opens, select the **Application settings** tab.

2. In the **Repositories** section select the **Synchronization with Administration Server** subsection.
3. Select the **Data about objects quarantined on managed devices**.
4. Click **OK**.
5. Click the **Save** button.

Data synchronization with the Administration Server is configured.

Configuring creation of the threat development chain

To create a threat development chain the specified prerequisites must be met.

You can enable creation of the threat development chain for the objects detected on managed devices. The threat development chain is displayed on the incident card.

To enable creation of the threat development chain:

1. Do one of the following:

   - Open the application properties window for an individual device.

     1. In the main Kaspersky Security Center Web Console window select **Devices** → **Managed devices**.
     2. Select the device.
     3. In the **<Device name>** window that opens, select the **Applications** tab.
     4. Select **Kaspersky Endpoint Agent**.
     5. In the window that opens, select the **Application settings** tab.

   - Open the policy properties window.

     1. In the main Kaspersky Security Center Web Console window select **Devices** → **Policies and profiles**.
     2. Select the policy you want to configure.
     3. In the **<Policy name>** window that opens, select the **Application settings** tab.

2. In the **Repositories** section select the **Synchronization with Administration Server** subsection.
3. In the **Synchronization with the Administration Server** group of settings, select the **Send data for creation of the threat development chain** check box.
4. If you configure the policy settings, in the upper right corner of the **Synchronization with the Administration Server** group of settings, change the switch from **Undefined** to **Enforce**.
5. Click **OK**.
6. Click the **Save** button.

Creation of the threat development chain is configured.

Configuring integration between Kaspersky Endpoint Agent and Kaspersky Managed Detection and Response

Before performing the following steps, get the MDR configuration file. It contains a configuration file (BLOB) required for integration.

If you want Kaspersky Endpoint Agent to process data about events generated by Kaspersky Industrial CyberSecurity for Networks and send this data to Kaspersky Managed Detection and Response, configure interaction with Kaspersky Security Center in the settings of Kaspersky Industrial CyberSecurity for Networks. For detailed information on configuring interaction between the applications, refer to *Kaspersky Industrial CyberSecurity for Networks Help*.

To configuring integration between Kaspersky Endpoint Agent and Kaspersky Managed Detection and Response using Kaspersky Security Center Web Console:

1. Open Kaspersky Security Center Web Console.
2. Open the **Devices** → **Policies and profiles** tab.
3. In the list of policies, select the name of Kaspersky Endpoint Agent policy that you want to configure.

   This opens the policy settings window.
4. On the **Application settings** tab, select **Managed Detection and Response**.
5. In the **Managed Detection and Response settings** group, do the following:

   a. Switch the toggle button to **Managed Detection and Response enabled**.

   b. Click the **Upload configuration file (BLOB)** button and select the BLOB configuration file to load.

   By downloading the Managed Detection and Response configuration file, you agree to automatically send the specified data from the device with Kaspersky Endpoint Agent installed to Kaspersky for processing. Do not download the configuration file, if you do not want the specified information to be processed.

   c. In the **User ID** field, enter an arbitrary value.

   d. In the upper right corner of the settings group, change the switch from **Undefined** to **Enforce**.
6. Click **Save** to save the changes.

Integration between Kaspersky Endpoint Agent and Kaspersky Managed Detection and Response is configured.

MDR operation when using Kaspersky Endpoint Agent simultaneously with Kaspersky Endpoint Security

Kaspersky Endpoint Security 11 or later with the current database version supports interaction with MDR. In Kaspersky Endpoint Security 11.6.0 or later, interaction with MDR is available immediately after installation.

If you use Kaspersky Endpoint Agent to work with MDR and install Kaspersky Endpoint Security of the version that supports interaction with MDR or update Kaspersky Endpoint Security 11 or later databases to the current version, MDR stops working with Kaspersky Endpoint Agent and becomes available for work with Kaspersky Endpoint Security. At that:

- Switching between Kaspersky Endpoint Agent and Kaspersky Endpoint Security is performed in quiet mode.
- Kaspersky Endpoint Agent allows for configuring settings for interaction with MDR, but these settings are not applied on the device.

- If Kaspersky Endpoint Security is not available (for example, you uninstalled the application), MDR can start working with Kaspersky Endpoint Agent if you restart the Kaspersky Endpoint Agent service.
- The Managed Detection and Response component remains in the *Running* status in Kaspersky Endpoint Agent settings on the device, since Kaspersky Endpoint Agent continues to communicate with MDR (for example, to resume working with the solution if necessary).

Working with incident card

The incident card is deleted one month after it was created.

The incident card provides information required to analyze the incident, as well as perform actions in response to the incident.

The following information is displayed in the incident card:

- Threat development chain graph. The graph displays the chain of actions in the system that result in the incident.
- General incident information.
- Information about the protected device on which the incident occurred.
- Information about the object detected during the incident.

You can perform the following actions on the incident card:

- Isolate the device on which the incident occurred.
- Quarantine file.
- Prevent execution of file detected during the incident.
- Create an IOC Scan task.

You can also use the functionality for working with untrusted objects available in Endpoint Protection Platform applications. For example, can also use the standard Kaspersky Security Center Web Console tools to add a file to Kaspersky Endpoint Security for Windows Application Launch Control allow list or to send a file to Kaspersky experts for analysis. For details, refer to *Kaspersky Endpoint Security for Windows Help*.

Configuring a threat report for viewing incident cards

To configure a threat report for viewing incident cards:

1. In the main Web Console window open the **Monitoring and reporting** → **Reports** section.
2. Click the report name – **Report on threats**.
3. In the report properties window that opens, go to the **Fields** tab.

4. Make sure that the **Open incident** field is available in the list of report fields in the **Detailed fields** group of settings.

5. If the **Open incident** field is not available in the list, follow these steps:

   a. Click the **Add** button.

   b. At the right side of the window, select the **Open incident** field from the drop-down list.

   c. Click **OK**.

6. Click the **Save** button.

Viewing the incident card is configured in the Report on threats settings.

Prerequisites for creating threat development chain

To create a threat development chain the following prerequisites must be met:

- A compatible version of Endpoint Protection Platform (Kaspersky Security for Windows Server 11 or higher or Kaspersky Endpoint Security for Windows 11.4.0 or higher) is installed on the managed device with Kaspersky Endpoint Agent.
- Kaspersky Endpoint Agent is activated with Kaspersky EDR Optimum or Kaspersky EDR Expert key.
- Kaspersky Endpoint Agent and Endpoint Protection Platform are managed by Kaspersky Security Center Web Console.
- Kaspersky Endpoint Agent web plug-in is installed on a device with Kaspersky Security Center Web Console installed.
- An active policy is applied to the device. Creation of a threat development chain and forced usage of these settings is enabled in the properties of this policy.

  If a policy is not applied to a managed device, creation of the threat development chain must be enabled in the application properties.

  By default, creation of the threat development chain is disabled in the application properties for the managed device.

Viewing the incident card

To view the incident card:

1. In the main Web Console window open the **Monitoring and reporting** → **Reports** section.

2. Select the **Report on threats** option and click the **Show report** button.

3. In the report window on the **Details** tab, select the incident and click the **Present** link.

Selecting an action on a file from the incident card

For the Execution prevention rules to be applied on the device where the incident occurred, the active Kaspersky Endpoint Agent policy must be applied to this device. If the device, on which the incident occurred, is not managed by an active policy, the Execution prevention rule will not be created.

To select an action on a file from an incident card:

1. Open the incident card.
2. To quarantine the file detected during the incident, in the **File** section click the **Quarantine** button.
3. To prevent execution of a file detected during the incident, in the **File** section click the **Prevent execution** button.

When Kaspersky Endpoint Agent 3.9 is used, the prevention rules do not apply to files located on CDs or in ISO images. Execution or opening of such files is *not* blocked by the application.

Isolating a device from the incident card

To isolate a device from an incident card:

1. Open the incident card.
2. To isolate the device on which the incident occurred, in the **Device** section, click the **Isolate device from the network** button.

Creating IOC Scan task from the incident card

To create an IOC Scan task from the incident card:

1. Open the incident card.
2. On the **All incident events** tab, select the items from which you want to create an IOC Scan task.
3. Click the **IOC Scan task creation** button.
4. Do one of the following:
   - If you want the compromise indicator to be triggered when any of the selected objects is detected, select **OR (any IOC found)** on the right side of the screen.
   - If you want the compromise indicator to be triggered when all the selected objects are detected, select **AND (all IOC found)** on the right side of the screen.

5. In the **Actions when IOC is found** group of settings, select one of the following actions:

   - **Isolate device from the network** to enable network isolation of the device on which indicator of compromise is detected by Kaspersky Endpoint Agent.
   - **Quarantine and delete** to quarantine the detected object and remove it from the device.
   - **Run Endpoint Protection Platform scan of critical areas on the device** to make Kaspersky Endpoint Agent send a command to EPP application to scan critical areas on all the devices of the administration group on which indicator of compromise is detected.

6. Click **Create task**.

The default settings of the IOC Scan tasks created from the incident card are described in the following table. You can change these values in the settings of the created task.

Default settings of the IOC Scan task created from the incident card

Parameter	Default value	Description
Settings on the Schedule tab		
Run by schedule	Selected.	The task is started according to the schedule, with the specified settings.
Frequency	**At specified time**	The task is started once, at the specified date and time.
Start time	15 minutes after the task creation.	The task is started at the specified time.
Start date	Task creation date.	The task is started at the specified date.
Stop task if runs longer than	Selected. The default value is one hour.	The application quits the task after the specified time since the task is started, regardless of the task execution progress.
Cancel schedule from	*Not* selected.	Automatic cancellation of the task start schedule is not used.
Run missed tasks	Selected.	The application restarts the task that was not started by schedule for some reason. For example, if Kaspersky Endpoint Agent was not running at the scheduled task start time.
Randomize the task start time within the interval	Selected. The default value is 10 minutes.	The task will start at an arbitrary time within the specified interval since the moment specified in the **Start time** field.
Settings in the Advanced section		
Select data types (IOC documents) to analyze during IOC scanning	When analyzing data on files (FileItem), the **Analyze data of files (FileItem)** option is selected. In the additional settings of the IOC document, in the **Search for Indicators of Compromise in the following areas** group of settings, the **Critical file areas on the device** option is selected.	The application checks critical areas on the device, and the folder where a dangerous object was initially detected. The following areas are considered critical: • Temporary files in the folders of the system and user accounts.

		• Temporary files in the operating system folder and in the %TEMP% folder for the Local System account, if the paths are different.
	When analyzing data in the Windows registry (RegistryItem), the **Analyze data of Windows Registry (RegistryItem)** option is selected.	The application checks the paths of user-defined registry keys.

By default, Kaspersky Endpoint Agent 3.9 uses the settings specified in the **Kaspersky Sandbox integration** section, in the **Threat Response** group of the settings, for IOC Scan tasks created from the incident card. For detailed information refer to *Kaspersky Sandbox Help*.

Managing Kaspersky Endpoint Agent tasks

This section describes how to manage Kaspersky Endpoint Agent tasks.

Creating tasks

To create a task:

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Tasks**.
2. Click the **Add** button.

   The task creation wizard starts.
3. In the **Application** drop-down list, select **Kaspersky Endpoint Agent**.
4. In the **Task type** drop-down list, select the required task type and follow the wizard instructions.
5. To change the default values of the task settings immediately after its creation, select the **Open task details when creation is complete** check box on the **Finish task creation** page.

   If you do not select this check box, the task will be created with the default settings. You can change these settings later at any time for the following task types:

   - Activation of Application
   - IOC Scan
   - Delete file
   - Quarantine file
   - Terminate process
   - Run process

- Databases and Modules Update

6. Click **Finish**.

The task will be created and displayed in the list of tasks.

The created task can be started manually or automatically according to a schedule.

Viewing the table of tasks

To view the list of tasks,

in the main Web Console window select **Devices** → **Tasks**.

A list of tasks appears. The tasks are grouped by the names of the applications for which they are created.

Deleting a task from the list

To remove tasks from the list of the tasks on Kaspersky Security Center server:

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Tasks**.
   A list of tasks appears.
2. In the list of tasks, select the check boxes next to the tasks that you want to delete.
3. Click the **Delete** button.
   The action confirmation window opens.
4. Click **Yes**.

Selected tasks are deleted from the list.

Configuring task schedule settings

To configure the scheduled task start:

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Tasks**.
2. To open the task settings window, click the task name.
3. On the **Schedule** tab in the **General** section, change the toggle button from **Schedule disabled** to **Run by schedule**.
4. In the **Frequency** drop-down list select one of the following options: **At specified time**, **Every hour**, **Every day**, **Every week** or **On application launch**.

5. If you select the **At specified time** option, specify the day and time to start the task.

6. If you select one of the following options: **Every hour**, **Every day** or **Every week**, configure the following settings:

    a. In the **Every** field, specify the task run frequency. For example, once a day or twice a week on Tuesdays and Thursdays.

    b. In the **Start time** and **Start date** fields, select the date and time from which the schedule applies.

7. To configure advanced schedule settings, select the **Advanced** section and perform the following steps:

    a. If you want to set maximum timeout for the task execution, select the **Stop task if runs longer than** check box and specify the number of hours and minutes after which the task will automatically terminate.

    b. If you want the task schedule to be valid until a certain date, select the **Cancel schedule from** check box and specify the expiration date for the schedule.

    c. If you want the application to start the tasks that were not completed on time as soon as possible, select the **Run missed tasks** check box.

    d. If you want to avoid simultaneous access of a large number of devices to the Administration Server as well as to run the task on workstations not precisely according to the schedule, but randomly within a certain time interval, select the **Randomize the task start time within the interval** check box and specify the start interval in minutes.

8. Click the **Save** button.

Starting tasks manually

The application starts the tasks according to the schedule specified in the properties of each task. You can start the task manually at any time.

To start the task manually:

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Tasks**.

2. In the list of tasks, select the check box next to the task that you want to start.

3. Click **Start**.

The task will be started. You can check the task status in the **Status** column or by clicking the **Result** button.

Creating Kaspersky Endpoint Agent activation tasks

You can activate Kaspersky Endpoint Agent using a license key from Kaspersky Security Center key store. For detailed information on managing license keys using Kaspersky Security Center, refer to *Kaspersky Security Center Help*.

To create Kaspersky Endpoint Agent activation task:

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Tasks**.
2. Click the **Add** button.

   The task creation wizard starts.
3. In the **Application** drop-down list, select **Kaspersky Endpoint Agent**.
4. In the **Task type** drop-down list, select **Activation of Application**.
5. In the **Task name** field, specify the display name of the task.
6. To create a task for devices of a specific Administration Server group, perform the following actions:
   a. In the **Selecting devices to which the task is assigned** group of settings, select the **Group of devices** option and click **Next**.
   b. Select the desired Administration Server group and click **Next**.
7. To create a task for specific devices by the range of IP addresses, NetBIOS names, DNS names, or select devices from the list devices detected in the network by the Administration Server, perform the following actions:
   a. In the **Selecting devices to which the task is assigned** group of settings, select the **Selected or imported from the list** option and click **Next**.
   b. Add devices to the list by the required criteria and click **Next**.
8. To create a task for devices of a specific selection, perform the following actions:
   a. In the **Selecting devices to which the task is assigned** group of settings, select the **Selection** option and click **Next**.
   b. Select the desired selection from the list and click **Next**.
9. In the **Select a license key** window, select the required license key from the list of Kaspersky Security Center keys available in the key storage.
10. If you want to add this license key as an additional one to automatically renew the license, select the **Add this key as additional** check box.
11. Click **Next**.
12. In the **Selecting an account to run a task** window, select the required account and click **Next**.
13. To change the default values of the task settings immediately after its creation, select the **Open task details when creation is complete** check box on the **Finish task creation** page.
14. Click **Finish**.

The task will be created and displayed in the list of tasks.

The created task can be started manually or automatically according to a schedule.

Configuring Database and application module update task

Task creation is performed before, as an individual step.

If you selected the **Open task details when creation is complete** check box on the **Finish task creation** page during the task creation, proceed to step 4 of the following instruction.

To configure the Database and application module update task settings:

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Tasks**.
2. To open the task settings window, click the task name.
3. Select the **Application settings** tab.
4. Select the **Connection settings** section.
5. If you use Kaspersky Security Center, in the **Update source** group of settings, select one of the following options:
   - **Kaspersky Security Center Administration Server**.
   - **Kaspersky update servers**.
   - **Custom HTTP or FTP servers or network folders**.
6. If you use Kaspersky Security Center Cloud Console, in the **Update source** group of settings, select one of the following options:
   - **Distribution points**. Devices with Network Agent installed are used as update source.

     Detailed information on using the distribution points is available in Kaspersky Security Center Cloud Console Help.
   - **Kaspersky update servers**. Kaspersky update servers are used as update source.
7. If required, select the **Use Kaspersky update servers if specified servers are not available** check box.

   Not available in Kaspersky Security Center Cloud Console.
8. If you select **Custom HTTP or FTP servers or network folders** as database update source, do the following:

   Not available in Kaspersky Security Center Cloud Console.

   a. Click the **Settings** link to open the **Custom update sources** window.

   b. Add the update sources to the list by following these steps:

1. Click the **Add** button.
2. In the dialog box that opens, in the **URL** field, enter the address of the update server (HTTP or FTP), or the path to the network folder or local folder containing the update files, and click **OK**.
3. If you want to use the database update source, switch the toggle button next to its address to **Enable**.

   Follow the same steps to add each update source.

4. Click **OK**.

   The **Custom update sources** window closes.

9. Select the **Update settings** section.
10. In the **Update settings** section, select the conditions for the application to check for the availability of application module updates:
    - **Do not check for available updates**. Kaspersky Endpoint Agent will not check the availability of application module updates.
    - **Only check for available critical software modules updates**. Kaspersky Endpoint Agent will check the availability only for important application module updates.
    - **Download and install critical software modules updates**. Kaspersky Endpoint Agent will check the availability of application module updates and download and install critical application module updates.
11. If you want the application to display a notification about all scheduled application modules updates available in the update source, select the **Receive information about available scheduled software modules updates** check box.
12. Click the **Save** button.

The created task can be started manually or automatically according to a schedule.

Managing Standard IOC Scan tasks

Standard IOC Scan tasks are created manually in Kaspersky Security Center or using the command line interface.

This section provides instructions on how to manage Standard IOC Scan tasks.

Configuring Standard IOC Scan task

Task creation is performed before, as an individual step.

If you selected the **Open task details when creation is complete** check box on the **Finish task creation** page during the task creation, proceed to step 4 of the following instruction.

To configure the settings of a Standard IOC Scan task:

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Tasks**.
2. To open the task settings window, click the task name.
3. Select the **Application settings** tab.
4. In the **IOC scan settings** section, configure the IOC collection by following these steps:
   a. In the **IOC files** group of settings click the **Redefine IOC files** button.
   b. In the dialog that opens, click the **Add IOC files** button and specify the IOC files that you want to use for the task.
      You can select multiple IOC files for a single IOC Scan task.
   c. Click **OK** to close the dialog box.

      If, when creating the IOC Scan task, you upload some IOC files that are not supported by Kaspersky Endpoint Agent then when the task starts, the application will use only supported IOC files.

   d. To view the list of all IOC files that are included in the IOC collection, as well as to obtain information about each IOC file, do the following:
      1. Click the link with the names of all downloaded IOC files in the **IOC files** group of settings.
         The **IOC contents ()** window opens.
      2. To view detailed information about an individual IOC file, click the name of the required IOC file in the list of files on the **IOC collection** tab.
         In the window that opens, information about the selected IOC file is displayed.
      3. To close the window with information about the selected IOC file, click the **OK** or **Cancel**.
      4. To view information about all downloaded IOC files at once, open the **IOC data** tab.
         Information about each downloaded IOC file is displayed in the workspace of the window.
      5. If you do not want to use a specific IOC file when the IOC Scan task is executed, on the **IOC collection** tab, switch the toggle button next to the IOC file name from **Include** to **Exclude**.
      6. Click **OK** to save the changes and close the **IOC contents ()** window.
   e. To export the created IOC collection, click **Export IOC collection**.
      In the window that opens, specify the name of the file and select the folder where you want to save it.
   f. Click the **Save** button.
      The application creates a ZIP file in the specified folder.
5. In the **IOC scan settings** configure the response actions when indicator of compromise is found:
   a. In the **Actions** group of settings, select the **Take response actions after an indicator of compromise is found** check box.

b. Select the **Isolate device from the network** check box to enable network isolation of the device on which indicator of compromise is detected by Kaspersky Endpoint Agent.

c. Select the **Quarantine and delete** check box to quarantine the detected object and remove it from the device.

d. Select the **Run Endpoint Protection Platform scan of critical areas on the device** check box so that Kaspersky Endpoint Agent sends a command to EPP application to scan critical areas on all the devices of the administration group on which indicators of compromise are detected.

If the **Quarantine and delete** or **Run critical areas scan** option is enabled, Kaspersky Endpoint Agent may recognize the detected files as infected and delete them from the device as a response action.

6. In the **Advanced** section, select data types (IOC documents) that you want to analyze during the task execution and configure the additional scan settings:

a. In the **Select data types (IOC documents) to analyze during IOC scanning** group of settings, select the check boxes next to the required IOC documents.

Depending on the loaded IOC files, some check boxes may be disabled.

Kaspersky Endpoint Agent automatically selects data types (IOC documents) for the IOC Scan task in accordance to the contents of the downloaded IOC files. It is not recommended to unselect data types manually.

b. If the **Analyze data of files (FileItem)** check box is selected, click the **Advanced for FileItem** link and in the **FileItem document scan settings** window that opens, select the scan areas on the protected device disks where to look for indicators of compromise.

You can select one of the predefined areas, or specify the paths to the desired areas manually.

c. Click **OK** to save the changes and close the **FileItem document scan settings** window.

d. If the **Analyze data of Windows Event Log (EventLogItem)** check box is selected, click the **Advanced for EventLogItem** link and in the **EventLogItem document scan settings** window that opens, configure additional event analysis settings:

- **Scan only events that are logged within the specified period**.

  If the check box is selected, only the events that were logged during the specified period are taken into account during the task execution.

- **Scan events that belong to the following channels**.

  List of channels that are analyzed during the task execution.

e. Click **OK** to save the changes and close the **FileItem document scan settings** window.

7. Click the **Save** button.

The created task can be started manually or automatically according to a schedule.

Viewing IOC Scan task execution results

To view the IOC Scan task execution results:

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Tasks**.
2. To open the task settings window, click the task name.
3. Select the **Application settings** tab.
4. Select the **Results** section.
5. In the **Device** drop-down list, select the devices, for which you want to view the results of IOC Scan task.

   A summary table with the task execution results on the selected devices is displayed.

   If compromise indicators are detected on devices, the **Result** column displays the *compromise indicators detected* link.
6. If you want to view detailed information on the detected compromise indicators on a specific device, do the following:

   a. Click the **indicator(s) of compromise detected** link in the row with the name of the desired device.

      The **IOC results** window opens that contains a list of all IOC files used in the task. If there is an object on the selected device that matches a certain compromise indicator, the **Status** column displays the *Match* value.

   b. Click the **matched** link in the row with the name of the desired IOC file.

      The **IOC incident card** window opens.

      IOC incident card contains information about objects on the device that match the conditions of the processed IOC file, as well as the text of the matched branches or individual conditions from this IOC file.

      > Viewing the IOC incident card is not available for IOC files, for which no matches were detected on the device during scan.

Configuring the Quarantine file task

If you suspect that an infected or probably infected file is on the computer, you can isolate it by moving it to quarantine.

> Task creation is performed before, as an individual step.

> If you selected the **Open task details when creation is complete** check box on the **Finish task creation** page during the task creation, proceed to step 4 of the following instruction.

To configure the Quarantine file task settings:

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Tasks**.
2. To open the task settings window, click the task name.
3. Select the **Application settings** tab.

4. In the **Please specify the file to be added to Quarantine** drop-down list, select one of the following values: **Specify the file by full path** or **Specify the file by folder path and checksum**.

5. If you select the **Specify the file by full path** option, specify the full path to the file in the **File full path** field.

6. If you select the **Specify the file by folder path and checksum** option, configure the following settings:

   - In the **Checksum type** drop-down list, select one of the following values: **MD5** or **SHA256**.
   - Specify the value in the **Checksum** field.
   - Specify the value in the **File folder path** field.

7. Click the **Save** button.

The created task can be started manually or automatically according to a schedule.

If the file is locked by another process, the task will be displayed with the *Completed* status, but the file itself will be quarantined only after the device is restarted. It is recommended to check if the task is completed successfully after the device is restarted.

The Quarantine file task may fail with the *Access denied* error if you try to quarantine an executable file which is currently running. To solve this problem, create the Terminate process task for this file, and try to create the Quarantine file task again.

Configuring the Delete file task

Task creation is performed before, as an individual step.

If you selected the **Open task details when creation is complete** check box on the **Finish task creation** page during the task creation, proceed to step 4 of the following instruction.

To configure the Delete file task settings:

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Tasks**.

2. To open the task settings window, click the task name.

3. Select the **Application settings** tab.

4. In the **File to be deleted** list click **Add**.

5. The **File to be deleted** dialog box opens.

6. In the **Please specify the file to be deleted** drop-down list, select one of the following values: **Specify the file by full path** or **Specify the file by folder path and checksum**.

7. If you select the **Specify the file by full path** option, specify the full path to the file in the **File full path** field.
8. If you select the **Specify the file by folder path and checksum** option, configure the following settings:
   - In the **Checksum type** drop-down list, select one of the following values: **MD5** or **SHA256**.
   - Specify the value in the **Checksum** field.
   - Specify the value in the **File folder path** field.
   - Select the **Include subfolders** check box for the application to delete all occurrences of the object not only in the specified folder, but also in all its subfolders.
9. Click **OK** to add the specified object to the **File to be deleted** list.

   You can specify several objects for deletion in one Delete file task.
10. Click the **Save** button.

The created task can be started manually or automatically according to a schedule.

If the file is locked by another process, the task will be displayed with the *Completed* status, but the file itself will be deleted only after the device is restarted. It is recommended to check if the file is deleted successfully after the device is restarted.

Deleting a file from a connected network drive is not supported.

Configuring the Run process task

Using the Run process task, you can run the required application or command on the device.

Task creation is performed before, as an individual step.

If you selected the **Open task details when creation is complete** check box on the **Finish task creation** page during the task creation, proceed to step 4 of the following instruction.

To configure the Run process task settings:

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Tasks**.
2. To open the task settings window, click the task name.
3. Select the **Application settings** tab.
4. To run the application using the command line (cmd.exe) or execute a command, type the required command in the **Executable command** field.
5. If you want to run the application directly, do the following:

a. Specify the path to the application executable file in the **Working folder** field.

b. Specify the keys for running the application in the **Arguments** field.

6. Click the **Save** button.

The created task can be started manually or automatically according to a schedule.

Configuring the Terminate process task

If you believe that a process running on the device could threaten the security of the device or the corporate LAN, you can terminate the process.

Task creation is performed before, as an individual step.

If you selected the **Open task details when creation is complete** check box on the **Finish task creation** page during the task creation, proceed to step 4 of the following instruction.

To configure the Terminate process task settings:

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Tasks**.
2. To open the task settings window, click the task name.
3. Select the **Application settings** tab.
4. In the **Path** field specify the path to the file of the process that you want to terminate.
5. In the **Checksum type** drop-down list, select one of the following values: **Not set**, **MD5** or **SHA256**.
6. If you select **MD5** or **SHA256**, specify the value in the **Checksum** field.
7. If you want the application to consider the character case in the path to the process file, select the **Path is case sensitive** check box.
8. Click the **Save** button.

The created task can be started manually or automatically according to a schedule.

Managing Kaspersky Endpoint Agent using the command line interface

Kaspersky Endpoint Agent can be managed using the command line interface. The functionality of the command line interface is provided by the Agent.exe utility. The Agent.exe utility is included in Kaspersky Endpoint Agent distribution kit and is installed on each device together with Kaspersky Endpoint Agent. It is installed to the `%ProgramFiles%\Kaspersky Lab\Endpoint Agent` folder (if 32-bit operating system is used on the device) or to the `% ProgramFiles(x86)%\Kaspersky Lab\Endpoint Agent` folder (if 64-bit operating system is used on the device).

Example:
If the device has x64 Windows operating system installed and you select to install Kaspersky Endpoint Agent on drive C, the Agent.exe utility is placed to the following folder:
`C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\`

To manage Kaspersky Endpoint Agent using the command line interface:

1. On the device, run a command line interpreter (for example, Command Prompt cmd.exe) with the permissions of the local administrator.
2. Using the `cd` command, navigate to the folder where the Agent.exe file is located.

   For example, you can type the following command `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` and press **ENTER**.
3. Type the following command: `agent.exe --<application setting you want to configure>=<action on the setting you want to execute>` and press **ENTER**.

   The command execution result (return code) is displayed.

To display help on all the application settings and their possible values,

run the following command: `agent.exe --help`

Managing Kaspersky Endpoint Agent activation

To manage application activation settings using the command line interface:

1. On the device, run a command line interpreter (for example, Command Prompt cmd.exe) with the permissions of the local administrator.
2. Using the `cd` command, navigate to the folder where the Agent.exe file is located.

   For example, you can type the following command `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` and press **ENTER**.
3. Enter one of the following commands and press **ENTER**:

   - To activate the application using the activation code or key file:

     `agent.exe --license=add <activation code or path to the key file>`

     To activate the application using the activation code, the protected device must be connected to the Internet.

- To specify an additional key to automatically renew the license:

  `agent.exe --license=reserve <activation code or path to the key file>`

- To remove the added primary or additional key:

  `agent.exe --license=delete <key serial number>`

- To view the status of added keys:

  `agent.exe --license=show`

Return codes of the `--license` command:

- `-305` – the added key has expired.
- `2` – undefined application error.
- `-302` – the added key is in the deny list.
- `-301` – the added key is not suitable for Kaspersky Endpoint Agent activation.
- `-303` – key file is damaged.
- `4` – syntax errors.
- `-304` – invalid path to the key file is specified.

Running Kaspersky Endpoint Agent database and module update

To perform Kaspersky Endpoint Agent application database and module update using the command line interface:

1. On the device, run a command line interpreter (for example, Command Prompt cmd.exe) with the permissions of the local administrator.
2. Using the `cd` command, navigate to the folder where the Agent.exe file is located.

   For example, you can type the following command `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` and press **ENTER**.
3. Run the following command and press **ENTER**:

   `agent.exe --update=bases|modules [--source=<addresses of custom database update sources separated by semicolons without space>|kl|ksc]`

   Command parameters when running Kaspersky Endpoint Agent database update

Parameter	Description
`--update=bases|modules`	Required parameter. Allows you to specify the type of update: • `--update=bases` starts application database update. • `--update=modules` starts application module update.
`--source=<addresses`	Optional parameter.

`of custom database update sources>|kl|ksc]`	Allows you to select a database update source. • `--source=<addresses of custom database update sources>` allows you to select the **Custom HTTP or FTP servers or network folders** option as database update source and specify the path to the network folder or IP, FTP or HTTP-address of the server from which the application downloads database updates. You can specify several addresses of custom database update sources separated by a semicolon without a space (";"). The application will download updates from the first available database update source. If all addresses are not available, the task will fail. • `--source=kl` allows you to select the **Kaspersky update servers** option as database update source. If the servers are not available, the task will fail. • `--source=ksc` allows you to select the **Kaspersky Security Center Administration Server** option as database update source. If the Administration Server is not available, the task will fail.

Return codes of the `--update=bases` command:

- -1 – command is not supported.
- 0 – command successfully executed.
- 1 – required argument is not passed to the command.
- 2 – general error.
- 4 – syntax error.
- 8 – permission error.
- 200 – all objects are valid.
- -206 – update files are not available in the specified database update source or have an unknown format.
- -209 – error connecting to the database update source.
- -232 – error connecting to the proxy server.
- -234 – error connecting to Kaspersky Security Center.
- -236 – application databases are corrupted.

Viewing information about quarantine settings and quarantined objects

To view information about the quarantine settings and quarantined objects using the command line interface:

1. On the device, run a command line interpreter (for example, Command Prompt cmd.exe) with the permissions of the local administrator.

2. Using the `cd` command, navigate to the folder where the Agent.exe file is located.

   For example, you can type the following command `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` and press **ENTER**.

3. Enter one of the following commands and press **ENTER**:

   - `agent.exe --quarantine=show [--pwd=<current user password>]`, to view a list of quarantined objects.

   The following information will be displayed on all objects in the Quarantine folder on the devices (the Quarantine folder is specified when quarantine settings are configured):

   - Identifiers of objects quarantined by the current moment (`ouid` parameter).
   - Names of quarantined objects (name + extension).
   - Date and time when the object was quarantined (UTC).
   - Original path to the quarantined file and default path for restoring the quarantined file (without file name).
   - Size of quarantined file (in bytes).
   - User account whose permissions were used to run the task for quarantining the file.
   - Object status:
     - `DETECT` if the file was quarantined by EPP or while performing actions in response to a threat detected by Kaspersky Sandbox. For example, as a result of the **Quarantine and delete** local action or the **Quarantine and delete when IOC is found** global action.
     - `CUSTOM` if the file was quarantined manually, as a result of the `--quarantine=add` command execution.
   - The way the file was quarantined:
     - `AUTOMATIC_<name of the application that detected a threat in the quarantined file>`, if the file was quarantined by EPP or while performing actions in response to a threat detected by Kaspersky Sandbox. For example, as a result of the **Quarantine and delete** local action or the **Quarantine and delete when IOC is found** global action.
     - `BY USER` if the file was quarantined manually, as a result of the `--quarantine=add` command execution.
   - `agent.exe --quarantine=limits`, to view the current values of the **Maximum Quarantine size (MB)** and **Available space threshold (MB)** settings, as well as the statuses of applying these settings (check box statuses) specified when configuring the quarantine.

Return codes of the `--quarantine` command:

- -1 – command is not supported.
- 0 – command successfully executed.
- 1 – required argument is not passed to the command.
- 2 – general error.

- 4 – syntax error.

Actions on quarantined objects

To perform actions on quarantined objects in Kaspersky Endpoint Agent using the command line interface:

1. On the device, run a command line interpreter (for example, Command Prompt cmd.exe) with the permissions of the local administrator.

2. Using the `cd` command, navigate to the folder where the Agent.exe file is located.

   For example, you can type the following command `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` and press **ENTER**.

3. Do the following and press **ENTER**:

   - To permanently delete the quarantined objects, execute the following command:

     `agent.exe --quarantine=delete --ouid=<` comma-separated quarantined object identifiers. Required parameter `> [--pwd=<` current user password `>]`.

     Objects with the specified identifiers will be deleted from the Quarantine folder on the devices. The Quarantine folder is specified when quarantine settings are configured.

   - To restore objects from quarantine, execute the following command:

     `agent.exe --quarantine=restore --ouid=<` comma-separated quarantined object identifiers. Required parameter `> [--path-type=<` one of the destination folder options to restore the objects from the quarantine: `original|custom|settings`. Optional parameter `> --path=<` path to the destination folder for restored objects. Required parameter if the `--path-type` parameter is passed and the `original>] value is specified [--action=<` one of the actions on the object: `replace|rename`. Optional parameter `>] [--pwd=<` current user password `>]`.

   - To quarantine an object, execute one of the following commands:

     - `agent.exe --quarantine=add [--file=<` full path to the object you want to quarantine `>] [--pwd=<` current user password `>]`.

     - `agent.exe --quarantine=add [--hash=<` hash of the object you want to quarantine. Required parameter. If you do not specify the full path to the object and pass the `--hashalg` parameter `>]--hashalg=<` one of the hash types: `md5|sha256`. Required parameter. If you do not specify the full path to the object `> [--file=<` path to the folder with the object that you want to quarantine `>] [--pwd=<` current user password `>]`.

Command parameters when performing actions on quarantined objects

Parameter	Description
`--ouid`	Required parameter. The parameter passes a unique numeric (int64) identifier of the quarantined object. Displayed when viewing information about quarantined objects (command `--quarantine=show`).
`--path-type=<original|custom|settings>`	The parameter describes the logic for the destination folder selection when restoring objects from quarantine. • If the parameter is not passed, the object will be restored to the original folder – the folder where the object was located before being quarantined. If the source folder is not available, the object

	will be restored to the folder specified when configuring quarantine settings. • If the parameter is passed with the `<original>` value, the object will be restored to the original folder – the folder where the object was located before being quarantined. If the source folder is not available, the object will be restored to the folder specified when configuring quarantine settings. • If the parameter is passed with the `<settings>` value, the object will be restored to the folder specified when configuring quarantine settings. If the folder is not available, the task fails. • If the parameter is passed with the `<custom>` value, the object will be restored to the folder, the path to which is specified as the value of the `--path` parameter. If the folder is not available, the task fails.
`--path=<`path to the destination folder for restored objects`>`	Required parameter if the `--path-type` parameter is passed with the `<custom>` value. This parameter defines the path where you want to create a folder for objects restored from the quarantine, if you do not want to use the folder where the object was located before being quarantined and the folder specified when configuring quarantine settings.
`--action=<replace|rename>`	This parameter defines the action that you want to perform on the object if the destination folder for restored objects already contains a file with name same to the name of the file you are restoring from quarantine. • If the parameter is not passed, the restored object will be renamed: the `_restored` suffix will be added to the original object name. • If the parameter is passed with the `<rename>` value, the restored object will be renamed: the `_restored` suffix will be added to the original object name. • If the parameter is passed with the `<replace>` value, the original object will be replaced with the restored object.
`--file=<`full path to the object you want to quarantine`>`	Required parameter if the `–hashalg` parameter is not passed. The parameter defines the full path to the object that you want to quarantine.
`--hashalg=<md5|sha256>`	Required parameter if the `–file` parameter is not passed and the full path to the object you want to quarantine is not specified. The parameter defines the hashing algorithm to calculate the checksum of the object you want to quarantine. The parameter can be passed with one of the following values: `<md5>` or `<sha256>`.
`--hash=<file checksum>`	Required parameter if the `–hashalg` parameter is passed. The parameter defines the checksum of the object you want to quarantine.
`--file=<folder that`	Required parameter if the –hashalg parameter is passed.

`contains the file>`	This parameter specifies the path to the folder which contains the object that you want to quarantine and whose hash is specified as the value of the `--hash` parameter.
`--pwd=<`current user password`>`	Allows you to specify the password of the user whose account is used to execute the command.

Return codes of the `--quarantine` command:

- -1 – command is not supported.
- 0 – command successfully executed.
- 1 – required argument is not passed to the command.
- 2 – general error.
- 4 – syntax error.

Starting, stopping and viewing the current application status

To start, stop, or view the current Kaspersky Endpoint Agent status using the command line interface:

1. On the device, run a command line interpreter (for example, Command Prompt cmd.exe) with the permissions of the local administrator.
2. Using the `cd` command, navigate to the folder where the Agent.exe file is located.

   For example, you can type the following command `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` and press **ENTER**.
3. Run the following command and press **ENTER**:

   ```
   agent.exe --product=<start|stop|state> [--pwd=<current user password>]
   ```

   Command parameters when starting, stopping, and viewing the current state of Kaspersky Endpoint Agent

Parameter	Description
`--product=<start|stop|state>`	Allows you to start, stop or view the current application status. • `--product=<start>` – starts the application. • `--product=<stop>` – stops the application. If password protection is configured for the application, a password is required to execute the `--product=<stop>` command. • `--product=<state>` – displays the current state of the application: started or stopped.
`--pwd=<current user password>`	Allows you to specify the password of the user whose account is used to execute the command.

Return codes of the `--product=<start|stop|state>` command:

- -1 – command is not supported.

- 0 – command successfully executed.
- 1 – required argument is not passed to the command.
- 2 – general error.
- 4 – syntax error.
- 8 – permission error.
- 9 – invalid operation (for example, an attempt to execute the `--product=start` command, if the application is already running).

Protecting the application with password

To restrict Kaspersky Endpoint Agent operations, which can result in decrease of protection level of the user computer and the data processed on this computer, as well as decrease of the application self-defense level, it is required to protect the application with password.

Password is required to execute the following commands in Kaspersky Endpoint Agent command line interface:

- `--sandbox=disable`
- `--sandbox=show`
- `--sandbox=enable --tls=no`
- `--sandbox=enable --pinned-certificate=<full path to the TLS certificate file for connecting Kaspersky Endpoint Agent with Kaspersky Sandbox>`
- `--quarantine=delete –ouid`
- `--quarantine=show`
- `--quarantine=restore`
- `--quarantine=add`
- `--product=stop`
- `--password=reset`
- `--isolation=disable`
- `--prevention=disable`
- `--selfdefense`
- `--license=delete`
- `--message-broker --type=kata <settings>`
- `--event --action=enable`

- `--event --action=disable`

To enter the password, use the `--pwd=<current user password>` parameter.

The password is also required when performing the following actions on the application:

- Application uninstallation and remote application uninstallation using Kaspersky Security Center
- Changing the set of the application components (`modify`)
- Application update (`upgrade`)
- Application repair (`repair`)
- Operations in the application installation wizard
- Operations in the command line interface

After enabling password protection and applying Kaspersky Security Center policy, a single password is applied to all devices of Kaspersky Endpoint Agent managed group.

After disabling password protection in the policy, password protection settings retain for the local device and can be edited.

The password is stored in the application settings in encrypted form (as a checksum).

To enter the password, use the `--pwd=<current user password>` parameter.

To configure Kaspersky Endpoint Agent password protection using the command line interface:

1. On the device, run a command line interpreter (for example, Command Prompt cmd.exe) with the permissions of the local administrator.
2. Using the `cd` command, navigate to the folder where the Agent.exe file is located.

   For example, you can type the following command `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` and press **ENTER**.
3. Enter one of the following commands and press **ENTER**:
   - `agent.exe --password=state` to view the current password protection status of the application.
   - `agent.exe --password=set --pwd=<current user password> --new=<new user password>` to set a new user password.
   - `agent.exe --password=reset --pwd=<current user password>` to reset the user password.

Protecting application services with PPL technology

Protection of application services using the *Protected Process Light (PPL)* technology is implemented in Kaspersky Endpoint Agent.

Processes that are running with the PPL flag cannot be stopped or changed by other processes without the PPL flag.

Usage of the PPL flag for the application services allows you to protect the services from malicious external influences and attempts to compromise the application.

To configure protection of application services by the PPL technology using the command line interface:

1. On the device, run a command line interpreter (for example, Command Prompt cmd.exe) with the permissions of the local administrator.
2. Using the `cd` command, navigate to the folder where the Agent.exe file is located.

   For example, you can type the following command `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` and press **ENTER**.
3. Enter one of the following commands and press **ENTER**:

   - `agent.exe --ppl=show [--pwd=<current user password>]`, to view the current status of application services protection by the PPL technology.
   - `agent.exe --ppl=disable [--pwd=<current user password>]`, to disable the application services protection by the PPL technology.

Return codes of the `--ppl` command:

- 0 – command successfully executed.
- 2 – general error.
- 4 – syntax error.
- 8 – permission error.

Managing self-defense settings

To manage self-defense settings using the command line interface:

1. On the device, run a command line interpreter (for example, Command Prompt cmd.exe) with the permissions of the local administrator.
2. Using the `cd` command, navigate to the folder where the Agent.exe file is located.

   For example, you can type the following command `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` and press **ENTER**.
3. Run the following command and press **ENTER**:

   `agent.exe --selfdefense=<enable|disable>`

Managing network isolation

To manage network isolation using the command line interface:

Network isolation cannot be enabled and network isolation setting cannot be configured using the command line interface.

1. On the device, run a command line interpreter (for example, Command Prompt cmd.exe) with the permissions of the local administrator.
2. Using the `cd` command, navigate to the folder where the Agent.exe file is located.

   For example, you can type the following command `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` and press **ENTER**.
3. Enter one of the following commands:

   - `agent.exe --isolation=show`

     Displays the current network isolation settings of the device in the console, including the list of the specified exclusion network profiles, as well as the list of rules defined in the network profiles.

   - `agent.exe --isolation=disable`

     Disables network isolation of the device.
4. Press **ENTER**.

Return codes of the `--isolation` command:

- -1 – command is not supported by Kaspersky Endpoint Agent version installed on the device.
- 0 – command successfully executed.
- 1 – required argument is not passed to the command.
- 2 – general error.
- 4 – syntax error.
- 9 – invalid operation (for example, an attempt to disable network isolation if network isolation is not enabled).

Managing Standard IOC Scan tasks

Standard IOC Scan tasks are created manually in Kaspersky Security Center or using the command line interface.

To create and configure a Standard IOC Scan task using the command line interface:

1. On the device, run a command line interpreter (for example, Command Prompt cmd.exe) with the permissions of the local administrator.
2. Using the `cd` command, navigate to the folder where the Agent.exe file is located.

   For example, you can type the following command `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` and press **ENTER**.
3. Run the following command and press **ENTER**:

```
agent.exe --scan-ioc {[--path=<path to the folder with IOC files>] | [<full path to the IOC file>]} [--process=no] [--hint=<full path to the process executable file|full path to the file>] [--registry=no] [--dnsentry=no] [--arpentry=no] [--ports=no] [--services=no] [--system=no] [--users=no] [--volumes=no] [--eventlog=no] [--datetime=<event publication date>] [--channels=<list of channels>] [--files=no] [--drives=<all|system|critical|custom>] [--excludes=<list of exclusions>][--scope=<configurable list of folders>]
```

If the `--scan-ioc` command is passed only with the required parameters, Kaspersky Endpoint Agent performs scanning with the default settings.

If the `--scan-ioc` command is passed with the two required parameters at the same time (`--path=<path to the folder with IOC files>` and `<full path to the IOC file>`), Kaspersky Endpoint Agent scans all the submitted IOC files.

Command parameters for running and configuring Standard IOC Scan tasks

Parameters	Description
`--scan-ioc`	Required parameter. Starts the Standard IOC Scan tasks on the device.
`--path=<path to the folder with IOC files>`	Path to the folder with the IOC files that you want to scan. Required parameter, if the `<full path to the IOC file>` parameter is not specified.
`<full path to the IOC file>`	Full path to the IOC file with the ioc or xml extension that you want to scan. Required parameter, if the `--path=<path to the folder with IOC files>` parameter is not specified. Passed without the `--path` argument.
`--process=<no>`	Optional parameter. The parameter disables the analysis of process data during scan. If the parameter is passed with the `<no>` value, Kaspersky Endpoint Agent does not consider the processes running on the device when scanning. If the IOC file contains IOC terms of the ProcessItem IOC document, they are ignored (defined as no match). If the parameter is not passed, Kaspersky Endpoint Agent scans the process data only if the ProcessItem IOC document is described in the IOC file submitted for scan.
`--hint=<full path to the process executable file|full path to the file>`	Optional parameter. The parameter allows you to narrow the scope of analyzed data for checking the ProcessItem and FileItem IOC documents, by specifying a particular file. The parameter value can be set as: • `<full path to the executable process file>` – ProcessItem • `<full path to the file>` – FileItem The parameter can only be passed together with the `--process=yes` and `--files=yes` arguments.
`--dnsentry=no`	Optional parameter.

	The parameter disables analysis of data on records in local DNS cache (DnsEntryItem IOC document) during IOC scan. If the parameter is passed with the <no> value, Kaspersky Endpoint Agent does not scan local DNS cache. If the IOC file contains the terms of the DnsEntryItem IOC document, they are ignored (defined as no match). If the parameter is not passed, Kaspersky Endpoint Agent scans local DNS cache only if the DnsEntryItem IOC document is described in the IOC file submitted for scan.
`--arpentry=no`	Optional parameter. The parameter disables analysis of data on records in the ARP table (ArpEntryItem document) during IOC scan. If the parameter is passed with the <no> value, Kaspersky Endpoint Agent does not scan the ARP table. If the IOC file contains the terms of the ArpEntryItem IOC document, they are ignored (defined as no match). If the parameter is not passed, Kaspersky Endpoint Agent scans the ARP table only if the ArpEntryItem IOC document is described in the IOC file submitted for scan.
`--ports=no`	Optional parameter. The parameter disables analysis of data on ports that are open for listening (PortItem document) during IOC scan. If the parameter is passed with the <no> value, Kaspersky Endpoint Agent does not scan the table of active connections on the device. If the IOC file contains the terms of the PortItem IOC document, they are ignored (defined as no match). If the parameter is not passed, Kaspersky Endpoint Agent scans the table of active connections only if the PortItem IOC document is described in the IOC file submitted for scan.
`--services=no`	Optional parameter. The parameter disables analysis of data on services installed on the device (ServiceItem document) during IOC scan. If the parameter is passed with the <no> value, Kaspersky Endpoint Agent does not scan data on services installed on the device. If the IOC file contains the terms of the ServiceItem IOC document, they are ignored (defined as no match). If the parameter is not passed, Kaspersky Endpoint Agent scans the data on services only if the ServiceItem IOC document is described in the IOC file submitted for scan.
`--volumes=no`	Optional parameter. The parameter disables analysis of volume data (VolumeItem document) during IOC scan. If the parameter is passed with the <no> value, Kaspersky Endpoint Agent does not scan volume data on the device. If the IOC file contains the terms of the VolumeItem IOC document, they are ignored (defined as no match). If the parameter is not passed, Kaspersky Endpoint Agent scans the data on volumes only if the VolumeItem IOC document is described in the IOC file submitted for scan.
`--eventlog=no`	Optional parameter.

	The parameter disables analysis of data about Windows Event Log entries (EventLogItem document) during IOC scan. If the parameter is passed with the <no> value, Kaspersky Endpoint Agent does not scan Windows Event Log entries. If the IOC file contains the terms of the EventLogItem IOC document, they are ignored (defined as no match). If the parameter is not passed, Kaspersky Endpoint Agent scans Windows Event Log entries only if the EventLogItem IOC document is described in the IOC file submitted for scan.
`--datetime=<event publication date>`	Optional parameter. The parameter allows you to enable or disable accounting for date and time when the event was registered in the Windows Event Log when determining the IOC scan area for the corresponding IOC document. During IOC scan, Kaspersky Endpoint Agent will only process the events that were registered within the time interval between the specified date and time and the task execution time. Kaspersky Endpoint Agent allows you to specify the event registration date as the parameter value. Scan will be performed only for the events registered in the Windows Event Log between the specified date and the time when IOC scan is performed. If the parameter is not passed, Kaspersky Endpoint Agent scans events with any registration date. The TaskSettings::BaseSettings::EventLogItem::datetime parameter cannot be changed. This parameter is used only if the EventLogItem IOC document is described in the IOC file submitted for scan.
`--channel=<list of channels>`	Optional parameter. This parameter allows you to pass a list of the names of channels (logs) for which IOC scan is required. If this parameter is passed, Kaspersky Endpoint Agent considers only the events published in the specified logs when performing the IOC Scan task. The name of the log is specified as a string, in accordance with the name of the log (channel) specified in the properties of this log (the Full Name parameter) or in the properties of the event (the <Channel></Channel> parameter in the xml-scheme of the event). By default (including the case if the parameter is not passed), IOC scan is performed for the Application, System, and Security channels. Several values separated by space can be passed to the parameter. This parameter is used only if the EventLogItem IOC document is described in the IOC submitted for scan.
`--system=no`	Optional parameter. The parameter disables analysis of environment data (SystemInfoItem IOC document) during IOC scan. If the parameter is passed with the <no> value, Kaspersky Endpoint Agent does not analyze environment data. If the IOC file contains the terms of the SystemInfoItem IOC document, they are ignored (defined as no match).

	If the parameter is not passed, Kaspersky Endpoint Agent analyzes environment data only if the SystemInfoItem IOC document is described in the IOC file submitted for scan.
`--users=no`	Optional parameter. The parameter disables analysis of user data (UserItem IOC document) during IOC scan. If the parameter is passed with the `<no>` value, Kaspersky Endpoint Agent does not analyze data on the users created in the system. If the IOC file contains the terms of the UserItem IOC document, they are ignored (defined as no match). If the parameter is not passed, Kaspersky Endpoint Agent analyzes data on the users created in the system only if the UserItem IOC document is described in the IOC file submitted for scan.
`--files=no`	Optional parameter. The parameter disables analysis of data on files (FileItem IOC document) during IOC scan. If the parameter is passed with the `<no>` value, Kaspersky Endpoint Agent does not analyze data on files. If the IOC file contains the terms of the FileItem IOC document, they are ignored (defined as no match). If the parameter is not passed, Kaspersky Endpoint Agent analyzes data on files only if the FileItem IOC document is described in the IOC file submitted for scan.
`--drives=<all|system|critical|custom>`	Optional parameter. The parameter allows you to specify the IOC scan scope when analyzing data for the FileItem IOC document. The parameter can have one of the following values: • `<all>` – the application scans all available file areas. • `<system>` – the application scans only the files that are located in the folders where the operating system is installed. • `<critical>` – the application scans only temporary files that are located in user and system folders. • `<custom>` – the application scans only the files that are located in the areas specified by the user. If the parameter is not passed, critical areas are scanned.
`--Excludes=<list of exclusions>`	Optional parameter. The parameter allows you to specify exclusion scopes when analyzing data for the FileItem IOC document. Several values separated by space can be passed by the parameter. If the parameter is not passed, all folders are scanned, with no exclusions.
`--scope=<configurable list of folders>`	Optional parameter. The parameter becomes required if the `--drives=custom` parameter is passed.

	The parameter allows you to specify a list of scan areas. Several values separated by space can be passed by the parameter.

Return codes of the `--scan-ioc` command:

- `-1` – command is not supported by Kaspersky Endpoint Agent version installed on the device.
- `0` – command successfully executed.
- `1` – required argument is not passed to the command.
- `2` – general error.
- `4` – syntax error.

If the command execution completed successfully (code `0`) and indicators of compromise were detected during to command execution, Kaspersky Endpoint Agent displays the following data on the task execution results in the command line:

Data displayed by the application in the command line when IOC is detected.

`Uuid`	IOC file identifier from the header of the IOC file structure (`<ioc id="">` tag)
`Name`	IOC file description from the header of the IOC file structure (`<description> </description>` tag)
`Matched Indicator Items`	The list of identifiers of all triggered indicators.
`Matched objects`	Data on each IOC document for which a match was found.

Managing Execution prevention

To manage Execution prevention settings using the command line interface:

1. On the device, run a command line interpreter (for example, Command Prompt cmd.exe) with the permissions of the local administrator.
2. Using the `cd` command, navigate to the folder where the Agent.exe file is located.

   For example, you can type the following command `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` and press **ENTER**.
3. Enter one of the following commands and press **ENTER**:

- `agent.exe --prevention=disable`, to disable Execution prevention.
- `agent.exe --prevention=show`, to display the current Execution prevention settings in the command line.

Return codes of the `--prevention` command:

- -1 – command is not supported by Kaspersky Endpoint Agent version installed on the device.
- 0 – command successfully executed.

- 1 – required argument is not passed to the command.
- 2 – general error.
- 4 – syntax error.
- 9 – invalid operation (for example, an attempt to disable Execution prevention if it is already disabled).

Managing event filtering

To manage event filtering using the command line interface:

1. On the device, run a command line interpreter (for example, Command Prompt cmd.exe) with the permissions of the local administrator.
2. Using the `cd` command, navigate to the folder where the Agent.exe file is located.

   For example, you can type the following command `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` and press **ENTER**.
3. Run the following command and press **ENTER**:

   ```
   agent.exe --event =
   <createprocess|loadimage|registry|network|eventlog|filechange|accountloggon|codeinjecti
   --action=<enable|disable|show>
   ```

Configuring tracing

Kaspersky Endpoint Agent does not automatically create a folder for storing trace or dump files on the device. Specify a folder that is already available on the device.

To configure tracing in Kaspersky Endpoint Agent using the command line interface:

1. On the device, run a command line interpreter (for example, Command Prompt cmd.exe) with the permissions of the local administrator.
2. Using the `cd` command, navigate to the folder where the Agent.exe file is located.

   For example, you can type the following command `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` and press **ENTER**.
3. Enter one of the following commands and press **ENTER**:

   - `agent.exe --trace=enable --folder <path to the folder where you want to create trace files>` to enable tracing.

   Tracing will be enabled for all Kaspersky Endpoint Agent processes that are currently running. Trace files will be created in the folder you specified.

   - `agent.exe --trace=disable` to disable tracing.

Tracing will be disabled for all Kaspersky Endpoint Agent processes that are currently running.

- `agent.exe --trace=show` to view the current tracing status and the path to the folder to save the trace files.

The values of the `trace.enable` (`true`, if tracing is enabled or `false`, is tracing is disabled) and `trace.folder` (path to the folder) settings are displayed.

Return codes of the `--trace` command:

- -1 – command is not supported.
- 0 – command successfully executed.
- 1 – required argument is not passed to the command.
- 2 – general error.
- 4 – syntax error.
- 5 – object not found (the specified path to the tracing logs folder is not found).
- 9 – invalid operation (for example, an attempt to execute the `--trace=disable` command, if tracing is already disabled).

Configuring creation of dump files

To configure creation of dump files in Kaspersky Endpoint Agent using the command line interface:

1. On the device, run a command line interpreter (for example, Command Prompt cmd.exe) with the permissions of the local administrator.
2. Using the `cd` command, navigate to the folder where the Agent.exe file is located.

   For example, you can type the following command `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` and press **ENTER**.
3. Enter one of the following commands and press **ENTER**:

   - `agent.exe --dump=enable --folder <path to the folder where you want to create dump files>` to enable creation of dump files.

   Creation of dump files will be enabled for all Kaspersky Endpoint Agent processes that are currently running. Dump files will be created in the folder you specified.

   - `agent.exe --dump=disable` to disable dump creation.

   Creation of dump files will be disabled for all Kaspersky Endpoint Agent processes that are currently running.

   - `agent.exe --dump=show` to view the current dump creation status and the path to the folder with the dump files.

   The values of the `dump.enable` (`true`, if creation of dump files is enabled or `false`, if creation of dump files is disabled) and `dump.folder` (path to the folder) settings are displayed.

Return codes of the `--dump` command:

- -1 – command is not supported.
- 0 – command successfully executed.
- 1 – required argument is not passed to the command.
- 2 – general error.
- 4 – syntax error.
- 5 – object not found (could not find the specified path to the dump files folder).
- 9 – invalid operation (for example, an attempt to execute the `--dump=disable` command, if creation of dumps is already disabled).

Contact Technical Support

This section describes the ways to get technical support and the terms on which it is available.

How to get technical support

If you cannot find a solution to your issue in the application documentation or in other sources of information about the application, you are advised to contact Technical Support. Technical Support specialists will answer your questions about installing and using the application.

Kaspersky supports this application during its lifecycle (see Product Support Lifecycle page). Before contacting Technical Support, please read the technical support rules.

You can contact Technical Support by submitting a request to Kaspersky Technical Support from the Kaspersky CompanyAccount portal.

Technical Support via Kaspersky CompanyAccount

Kaspersky CompanyAccount is a portal for organizations that use Kaspersky applications. The Kaspersky CompanyAccount portal is designed to facilitate interaction between users and Kaspersky specialists via online requests. The Kaspersky CompanyAccount portal lets you monitor the progress of electronic request processing by Kaspersky specialists and store a history of electronic requests.

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

The Kaspersky CompanyAccount portal is available in the following languages:

- English
- Spanish
- Italian
- German
- Polish
- Portuguese
- Russian
- French
- Japanese

To learn more about Kaspersky CompanyAccount, visit the Technical Support website.

Glossary

End User License Agreement

A binding agreement between you and AO Kaspersky Lab, stipulating the terms on which you may use the application.

Endpoint Protection Platform (EPP)

Kaspersky applications installed on workstations or servers included in the organization IT infrastructure. These applications are used to protect the devices from viruses and other computer security threats. Hereinafter also referred to as EPP.

IOC

Indicator of Compromise. A set of data about a malicious object or action.

IOC file

A file that contains a set of compromise indicators that are compared to the indicators of an event. If the compared indicators match, the application considers the event to be a detection. The detection probability may increase if exact matches of data about the object with several IOC files were found during the scan.

Kaspersky Endpoint Agent

An application included in Kaspersky Endpoint Detection and Response Optimum solution.

Kaspersky Endpoint Agent is installed on individual devices in the organization IT infrastructure. The application constantly monitors the processes running on these devices, open network connections and the files being modified.

Kaspersky Endpoint Agent interacts with other Kaspersky solutions to detect comprehensive threats (such as targeted attacks).

OpenIOC

An open standard for Indicator of Compromise (IOC) description created on the basis of XML and containing over 500 various indicators of compromise.

Targeted attack

An attack targeted at a specific person or organization. Unlike mass attacks by computer viruses aimed at infecting maximum number of computers, targeted attacks can be aimed at infecting the network of a certain organization or even one server in the organization IT infrastructure. A special trojan program may be developed for each targeted attack.

TLS encryption

Encryption of the connection between two servers, providing secure data transfer between the servers in the Internet.

Tracing

Application debugging, during which the application stops after execution of each command, and the execution result is displayed.

Information about third-party code

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

Trademark notices

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

Google and Google Chrome are trademarks of Google, Inc.

Intel, Xeon, and Core are registered trademarks of Intel Corporation in the U.S. and/or other countries.

Microsoft, Active Directory, Excel, Word, PowerPoint, Hyper-V, Win32, Windows, and Windows Server are registered trademarks of Microsoft Corporation in the United States and other countries.

Adobe Acrobat is either registered trademark or trademark of Adobe Systems Incorporated in the United States and/or other countries.

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

McAfee is a trademark or registered trademark of McAfee, Inc. in the United States and other countries.

Symantec is a trademark or registered trademark of Symantec Corporation or its affiliates in the U.S. and other countries.

ESET and ESET NOD32 are trademarks or registered trademarks of ESET, spol. s r.o.

Trend Micro is a trademark of Trend Micro.