kaspersky

Kaspersky Endpoint Agent

Contents

Kaspersky Endpoint Agent Help

Kaspersky Endpoint Agent is an application that 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).

The functionalities of Kaspersky Endpoint Agent application depend on the software solution within which the application is used.

This Help provides instructions for managing and configuring Kaspersky Endpoint Agent without reference to a specific solution. Some of the functions described herein may not be available within the solution you use.

Complete information about Kaspersky Endpoint Agent for Windows as part of the software solution you use, as well as complete information about the solution itself, is provided in the Help of the corresponding solution:

- *Kaspersky Anti Targeted Attack Platform Help*
- *Kaspersky Sandbox Help*
- *Kaspersky Endpoint Detection and Response Optimum Help*
- *Kaspersky Managed Detection and Response Help*

For information about Kaspersky Endpoint Agent for Linux, refer to the Help of the solution that includes the application:

- *Kaspersky Anti Targeted Attack Platform Help*
- *Kaspersky Managed Detection and Response Help*

Kaspersky Endpoint Agent

Kaspersky Endpoint Agent is an application that 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.ini`	Configuration file required for creating installation package for English version of Kaspersky Endpoint Agent using Kaspersky Security Center.
`agent\kpd.loc\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.

What's new

Known errors have been fixed in Kaspersky Endpoint Agent 3.12 for Windows. This application version also includes all the functionalities of the previous versions and introduces new features:

- Kaspersky Endpoint Agent 3.12 supports license subscriptions.
- Support for the following operating system versions is implemented:
  - Windows 10 21H2
  - Windows 11 21H2
  - Windows Server 20H2
- Compatibility between Kaspersky Endpoint Agent 3.12 and Kaspersky Anti Targeted Attack Platform version 4.0 is implemented.
- The capability is implemented to scan files and memory of the protected devices for signatures of malicious activity using YARA rules. You can start scan using Kaspersky Anti Targeted Attack Platform interface or using the command line in Kaspersky Endpoint Agent 3.12.
- Kaspersky Endpoint Agent 3.12 supports the task of collecting autorun lists from protected devices for Kaspersky Anti Targeted Attack Platform is implemented.
- The capability for Kaspersky Anti Targeted Attack Platform users to manage the services on the protected device is implemented.
- The capability is added to transfer IP addresses of the protected devices to Kaspersky Anti Targeted Attack Platform server for filtering events by IP address.
- Proxy server settings for connecting Kaspersky Endpoint Agent to Kaspersky Anti Targeted Attack Platform, Kaspersky Industrial CyberSecurity for Networks, and Kaspersky Sandbox server are extended. You can configure access using Windows domain group policies, browser or local WinHTTP settings. You can also connect Kaspersky Endpoint Agent directly to Kaspersky Security Network, without using a proxy server.
- Information for creating an incident card for the Administration Server is now sent only when Kaspersky Endpoint Detection and Response Optimum is used.

Hardware and software requirements

Hardware and software requirements

Minimum hardware requirements for workstations:

- Processor: 1.4 GHz (single core).
- RAM: 1 GB.
- Free disk space: 500 MB.

Minimum hardware requirements for servers:

- Processor: 1.4 GHz (single core).
- RAM: 512 MB.
- Free disk space: 500 MB.

Supported operating systems for workstations:

- Windows 7 SP1 Home / Professional / Enterprise / Ultimate 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.

Supported server operating systems:

- Windows Server 2008 SP2 Standard / Enterprise 64-bit.
- Windows Server 2008 R2 SP1 Foundation / Standard / Enterprise 64-bit.
- Windows Server 2012 Foundation / Standard / Enterprise / Datacenter 64-bit.
- Windows Server 2012 R2 Foundation / Standard / Enterprise / Datacenter 64-bit.
- Windows Server 2016 Essentials / Standard / Datacenter 64-bit.
- Windows Server 2019 Essentials / Standard / Datacenter 64-bit.
- Windows Server 2020 H2 Standard Core / Datacenter Core 64-bit.

Supported embedded operating systems:

- Windows Embedded Standard 7 SP1 32-bit / 64-bit.

The following operating systems are supported only for Kaspersky Industrial CyberSecurity for Networks integration scenarios:

- Windows XP SP2 Professional 32-bit.
- Windows Vista SP2 32-bit / 64-bit.
- Windows Server 2003 SP2 Standard / Enterprise 32-bit / 64-bit.
- Windows XP Embedded (POS Ready) 32-bit.
- Windows Embedded 8.0 Standard 32-bit / 64-bit.
- Windows Embedded 8.1 Industry Pro 32-bit / 64-bit.
- Windows 10 IoT Enterprise 32-bit / 64-bit.

When creating an installation package using Kaspersky Security Center 12 and later, to install Kaspersky Endpoint Agent on the devices running Windows XP, use the installation startup file (setup.exe) from the installation package created using Kaspersky Security Center 10.5.

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

Kaspersky Endpoint Agent 3.12 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 3.12 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 version 3.7 and later can be updated to Kaspersky Endpoint Agent version 3.12. Update is possible for the previous application versions installed either as part of the Endpoint Protection Platform application, or separately.

Kaspersky Endpoint Agent 3.12 Management plug-in and Kaspersky Endpoint Agent 3.12 Web plug-in are compatible with Kaspersky Endpoint Agent 3.7 and later.

Integration between Kaspersky Endpoint Agent 3.12 and Kaspersky Endpoint Protection Platform applications

Kaspersky Endpoint Agent 3.12 can be integrated with the following Kaspersky Endpoint Protection Platform applications (hereinafter also referred to as EPP):

- Kaspersky Endpoint Security for Windows: 11.4, 11.5, 11.6, 11.7.
- Kaspersky Security for Windows Server: 11, 11.0.1.
- Kaspersky Industrial CyberSecurity for Nodes: 3.0.
- Kaspersky Security for Virtualization 5.1.x Light Agent and 5.2 Light Agent.

For information on the available Endpoint Detection and Response features, refer to the corresponding EPP application help.

Kaspersky Endpoint Agent 3.12 integration with other Kaspersky applications and solutions

Kaspersky Endpoint Agent 3.12 can be integrated with the following Kaspersky applications and solutions:

- Kaspersky Security Center 13, 13.1 and 13.2.
- Kaspersky Security Center Cloud Console.

- Kaspersky Sandbox 1.0.
- Kaspersky Anti Targeted Attack Platform 4.0.
- Kaspersky Endpoint Detection and Response Optimum 1.0.

Supported integration scenarios for Kaspersky Endpoint Agent 3.12 and their limitations

Supported integration scenarios and their limitations

EPP application	EPP version	Version of Kaspersky software solution			Limitations
		Kaspersky Sandbox	Kaspersky Anti Targeted Attack Platform	Kaspersky Endpoint Detection and Response Optimum	
Kaspersky Endpoint Security for Windows	11.4	1.0	4.0	1.0	• Kaspersky Endpoint Agent does not send data about the **AMSI scan** event to Kaspersky Anti Targeted Attack Platform
	11.5, 11.6, 11.7	1.0	4.0	1.0	No
Kaspersky Security for Windows Server	11, 11.0.1	1.0	4.0	1.0	• Kaspersky Endpoint Agent does not send data about the **AMSI scan** event to Kaspersky Anti Targeted Attack Platform
Kaspersky Security for Virtualization Light Agent	5.1.x	No	4.0	No	• Kaspersky Endpoint Agent does not send data about the **AMSI scan** event to Kaspersky Anti Targeted Attack Platform
	5.2	1.0	4.0	1.0	

Limitations of the current Kaspersky Endpoint Agent version

Kaspersky Endpoint Agent 3.12 has the following limitations:

1. The component that prohibits opening of documents does not prevent a document that meets the applicable rule criteria from opening, if the document is opened using OLE Automation.
2. Before sending telemetry events to KATA Central Node, Kaspersky Endpoint Agent saves data to the event queue. If the event queue exceeds 10,000 unprocessed events, some events will be deleted and will not be sent

to KATA Central Node.

3. If Kaspersky Endpoint Agent is running on devices with the Windows 7 operation system, the application excludes data about network connections related to processes with PID=4 and PID=0 from telemetry.

4. If Kaspersky Endpoint Agent is used on the same device with Kaspersky Endpoint Security, and the file system level encryption (FLE) component is installed in Kaspersky Endpoint Security, Kaspersky Endpoint Agent does not register telemetry events about loading modules (LoadImage) and does not send these events to KATA Central Node.

5. 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.

6. If search of compromise indicators involves parsing text strings, the "is" condition takes into account the spaces, and the indicator description in the IOC file must be screened with CDATA characters. For example, to detect an object with the copyright "Copyright (C) 1998-2017 John Smith" by the "is" condition, the indicator description must be specified in the following format: <Content type="string"><![CDATA[Copyright (C) 1998-2017 John Smith]]></Content>. To simplify description of the indicators, the "contains" condition can also be used.

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

8. The installer cannot stop the soyuz 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 the soyuz service is not completed and the service cannot be stopped.

9. When scanning objects using the FileItem IOC document, Kaspersky Endpoint Agent skips objects with restricted access, for example, files that are used by other applications at the time of scanning. Kaspersky Endpoint Agent returns a false negative scan result for such objects.

10. 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.

11. When searching for indicators in the modules loaded into the address space, Kaspersky Endpoint Agent skips cases when the system loads x64 modules into x32 processes. For example, the following cases will not be detected: loading wowcpu64.dll into system32 or loading ntdll into system32. This limitation is reproduced in Windows Server 2008 R2 and Windows 7 x64 operating systems.

12. 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.

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

14. The capability to run and execute Kaspersky Endpoint Agent service (soyuz.exe) with the PPL flag is implemented. This functionality is provided by the klelaml.sys driver. Violation of the klelaml.sys driver integrity results in the operating system loading failure. In this case, it is recommended to use Windows system recovery utilities. The absence of the klelaml.sys driver when the PPL flag is enabled for the soyuz.exe process does not lead to the operating system failure, but results in Kaspersky Endpoint Agent crash. In this case, it is recommended to run the application installer and perform recovery in the quiet mode with the REINSTALL=Drivers.klelam key.

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

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

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

18. 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.

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

20. Cosmetic errors in the application interface have not been fixed, such as trimmed text in the control interface.

21. 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.

22. 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.

23. The agent.exe command line utility does not support operation with Cyrillic characters. For example, if a node whose address contains Cyrillic characters is specified in the list of Kaspersky Sandbox nodes in Kaspersky Endpoint Agent settings, the output of the --sandbox=show command may contain errors.

24. 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.

25. After installing, restoring, modifying the set of components or uninstalling Kaspersky Endpoint Agent, it is recommended to reboot the operating system as soon as possible. It is necessary because configuration of some application settings can be completed only at the moment when the operating system starts.

26. When creating an installation package using Kaspersky Security Center 12 and later, to install Kaspersky Endpoint Agent on the devices running Windows XP, use the installation startup file (setup.exe) from the installation package created using Kaspersky Security Center 10.5.

27. To install Kaspersky Endpoint Agent on devices running Windows XP by means of Kaspersky Security Center 13.2 and later, use the standard Kaspersky Endpoint Agent 3.12 distribution package, rather than the installation package created in Kaspersky Security Center.

28. If the start schedule for a group task is set to "On application launch", the task execution status is updated with a delay in the task execution history. For this reason, in some cases, the task execution history will not display the task execution statuses.

Installing and uninstalling Kaspersky Endpoint Agent

This section contains information on how to install Kaspersky Endpoint Agent on a device, how to update the application from the previous version, and how to remove the application from a device.

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 Kaspersky Endpoint Agent

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.

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.

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 {2948C53C-650C-4F06-89CB-A80BA858F02A} REMOVE=ALL /qn
```
If the application is protected by the password:
```
msiexec /i {2948C53C-650C-4F06-89CB-A80BA858F02A} 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*.

When creating an installation package using Kaspersky Security Center 12 and later, to install Kaspersky Endpoint Agent on the devices running Windows XP, use the installation startup file (setup.exe) from the installation package created using Kaspersky Security Center 10.5.

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.

When creating an installation package using Kaspersky Security Center 12 and later, to install Kaspersky Endpoint Agent on the devices running Windows XP, use the installation startup file (setup.exe) from the installation package created using Kaspersky Security Center 10.5.

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.

Installing Kaspersky Endpoint Agent administration tools

This section contains information on how to install Kaspersky Endpoint Agent Management plug-in for managing Kaspersky Endpoint Agent using Kaspersky Security Center Administration Console or Kaspersky Endpoint Agent Management web plug-in for managing Kaspersky Endpoint Agent using Kaspersky Security Center Web Console.

Installing and updating Kaspersky Endpoint Agent Management plug-in

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

To install Kaspersky Endpoint Agent Management plug-in,

copy the klcfginst.msi file from the distribution kit to the device with Kaspersky Security Center Administration Console installed and run the file.

The application Installation Wizard starts.

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

The update is available only for Kaspersky Endpoint Agent Management plug-in 3.7 and later.

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.

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.

Updating Kaspersky Endpoint Agent from the previous version

If Kaspersky Endpoint Agent 3.12 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 3.12 installation, and the previous version of the application is automatically uninstalled. To connect to Kaspersky Security Center and migrate data from the previous version, you need to create an account. The account uses the default name: AutoIOC_Admin and the password specified by the user.

Only Kaspersky Endpoint Agent version 3.7 and later can be updated to Kaspersky Endpoint Agent version 3.12. 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 and later. 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.

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.

  When installed on a device running Microsoft Windows XP, the klncapxp.sys driver is registered instead of klncap.sys.

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\klncapxp]
- [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 contains information about the basic concepts related to Kaspersky Endpoint Detection and Response Optimum licensing.

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 Agent 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 Agent 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 Agent database updates are not available). To continue using Kaspersky Endpoint Agent 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 Agent. You receive the activation code at the email address that you provided when purchasing the software solution that includes Kaspersky Endpoint Agent or when ordering a trial version of this software solution.

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 the Kaspersky Lab partner from whom you purchased the license.

You can use the activation code in the following cases:

- To create a license key

  After adding the license key that corresponds to the activation code, Kaspersky Endpoint Agent switches to operation in the full-function mode. Kaspersky Endpoint Agent supports deletion of the added key. After the key is deleted, Kaspersky Endpoint Agent switches to limited functionality mode.

  Kaspersky Endpoint Agent prevents from adding a key in the following cases:

  - The activation code is incompatible with Kaspersky Endpoint Agent: the activation code is used for another product, or has expired.
  - The key has been added to the deny-list.

- To create and use a reserve key

  Kaspersky Endpoint Agent automatically applies the reserve key upon expiration or after deletion of the primary key. If the primary key has not been added, Kaspersky Endpoint Agent prevents from adding a reserve key.

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 the software solution that includes Kaspersky Endpoint Agent or when ordering a trial version of this software solution.

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 Administration Console or in Kaspersky Security Center Web Console.
  - 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:

- Execution of the jobs received from the Central Node component and the sending the results to the Central Node component is stopped.

  The application sends a message to the Central Node component that the activation status of Kaspersky Endpoint Agent is changed.

  Connection with the Central Node component is not broken. Kaspersky Endpoint Agent continues to accept jobs for creating tasks and changing settings from the Central Node component, but it does not start these tasks and does not enable network isolation and Execution prevention.

- Telemetry is not sent.

- Creation of the threat development chain graph 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: Get file, Run application, 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 keys using Kaspersky Security Center, refer to *Kaspersky Security Center Help*.

To view information about an active license in Kaspersky Security Center Administration Console:

1. In the **Managed devices** folder of the Administration Console tree, select the folder with the name of the administration group, which includes the required device.

2. In the workspace, select the **Devices** tab.

3. Select the device for which you want to configure Kaspersky Endpoint Agent settings.

4. Select **Properties** in the device context menu.

   The device properties window opens.

5. Select the **Applications** section.

   A list of Kaspersky applications installed on the device is displayed in the window.

6. Select Kaspersky Endpoint Agent and open its properties window in one of the following ways:

   - Double-click the application name.
   - In the application context menu, select **Properties**.
   - Click the **Properties** button under the list of Kaspersky applications.

7. Select the **Keys** section.

Information about the current license is displayed in the window.

To view information about an active license in Kaspersky Security Center Web Console:

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.

Kaspersky Endpoint Agent application data

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.

Devices with Kaspersky Endpoint Agent installed store data prepared for automatic submission to Kaspersky Sandbox server, KATA server, and to Kaspersky Security Center. 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 of the solution that includes Kaspersky Endpoint Agent must ensure security of the devices with Kaspersky Endpoint Agent and the servers with the listed data independently. The solution 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.

The specific set of data depends on the solution as a part of which Kaspersky Endpoint Agent is used.

Service data

Service data of Kaspersky Endpoint Agent include:

- Data that is stored in configuration files as a result of configuring the settings by an administrator.
- Data processed during automatic Threat Response.
- Data processed during integration with Kaspersky Sandbox.
- Data processed during integration with KATA Central Node.
- Data processed during integration with Kaspersky Industrial CyberSecurity for Networks.

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 that are processed during automatic response and integration with Kaspersky Sandbox:

1. Processed files and data entered by the user during configuration of Kaspersky Endpoint Agent settings:
   - Access password for Kaspersky Endpoint Agent.
   - Quarantined files.
   - Kaspersky Endpoint Agent settings.
   - 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.
   - Public key of the certificate used for integration with Kaspersky Sandbox.
2. Kaspersky Endpoint Agent cache:
   - Time when scan results were written to the cache.
   - MD5 hash of the scan task.
   - Scan task identifier.
   - Scan result for the object.
3. Queue of the object scan requests:
   - ID of the object in the queue.
   - Time when the object was placed in the queue.
   - Processing status of the object in the queue.
   - ID of the user session in the operating system where the object scan task was created.

- System identifier (SID) of the operating system user whose account was used to create the object scan task.
- MD5 hash of the object scan task.

4. Information about the tasks for which Kaspersky Endpoint Agent awaits scan results from Kaspersky Sandbox:
   - Time when the object scan task was received.
   - Object processing status.
   - ID of the user session in the operating system where the object scan task was created.
   - Identifier of the object scan task.
   - MD5 hash of the object scan task.
   - System identifier (SID) of the operating system user whose account was used to create the task.
   - XML schema of the automatically created IOC.
   - MD5 or SHA256 hash of the scanned object.
   - Processing errors.
   - Names of the objects for which the scan task was created.
   - Scan result for the object.

When integrated with the KATA Central Node component, Kaspersky Endpoint Agent stores the following data locally:

1. Processed files and data entered by the user during configuration of Kaspersky Endpoint Agent settings:
   - 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.
     - Public key of the certificate used for integration with KATA Central Node.
     - Public key of the certificate used for integration with Kaspersky Sandbox.
     - License data.
2. Data required for integration with KATA Central Node:

- Updatable telemetry filtering schemes.
- Telemetry event packet queue.
- Cache of IOC file identifiers received from KATA Central Node.
- Objects to be passed to the server within the Get file task.
- The Get forensic task results reports.

When integrated with Kaspersky Industrial CyberSecurity for Networks server, Kaspersky Endpoint Agent stores the following data locally:

1. Processed files and data entered by the user during configuration of Kaspersky Endpoint Agent settings:
   - 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.
     - Public key of the certificate used for integration with Kaspersky Industrial CyberSecurity for Networks.
     - License data.
2. Data required for integration with Kaspersky Industrial CyberSecurity for Networks:
   - Updatable telemetry filtering schemes.
   - Telemetry event packet queue.

Data on events 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.
- Kaspersky Sandbox detections.
- Kaspersky Sandbox events.
- Kaspersky Endpoint Agent IOC files generated during automatic response.
- Object scan results.
- Kaspersky Sandbox server certificates.
- 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.
- Errors while interacting with application servers.
- 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 in requests to Kaspersky Sandbox

When integrating with Kaspersky Sandbox, the following data from requests to Kaspersky Sandbox is stored locally on the device:

- MD5 hash of the scan task.
- Scan task identifier.
- Scanned object and all related files.

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 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.
- Browser name.
- Browser version.
- Time when the web resource was last accessed.
- URL from the HTTP request.
- Name of the account used for the HTTP request.
- File name of the process that made the HTTP request.
- Full path to the file of the process that made the HTTP request.
- Windows identifier (PID) of the process that made the HTTP request.
- HTTP referer (HTTP request source URL).
- URI of the resource requested over HTTP.
- Information about the HTTP user agent (the application that made the HTTP request).
- HTTP request execution time.
- Unique identifier of the process that made the HTTP request.

Data in YARA Scan results

Kaspersky Endpoint Agent automatically transfers YARA scan results to Kaspersky Anti Targeted Attack Platform to build a threat development chain.

The data is temporarily stored locally in the queue for sending task execution results to Kaspersky Anti Targeted Attack Platform server. After sending, the data is deleted.

YARA scan results contain the following data:

- MD5 hash of the file
- SHA256 hash of the file
- Full name of the file
- File path
- File size
- 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

Data in requests to the KATA Central Node component

When integrated with the Central Node component, the following data is stored locally on the device with Kaspersky Endpoint Agent installed.

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 from Kaspersky Endpoint Agent requests to the Central Node component:

1. In the synchronization requests:
    - Unique Kaspersky Endpoint Agent identifier
    - Basic part of the server web address
    - Device name
    - Device IP-address

- Device MAC address
- Local time on the device
- Self-defense status of Kaspersky Endpoint Agent
- Name and version of the operating system that is installed on the device
- Kaspersky Endpoint Agent version
- Versions of the application settings and task settings
- Task statuses in Kaspersky Endpoint Agent: identifiers of running tasks, execution statuses, execution error codes
- Statuses of Kaspersky Endpoint Agent settings: type of settings being used, version of settings, status of applying the settings, error codes of applying the settings

2. In requests for obtaining files from the server:

- Unique identifiers of files
- Unique Kaspersky Endpoint Agent identifier
- Unique identifiers of certificates
- Basic part of the web address of the server with the Central Node component installed
- Host IP-address

3. In the reports on task execution results:

- Host IP-address
- Information about the objects detected during IOC scan or YARA scan
- Flags of the additional actions performed by Kaspersky Endpoint Agent upon completion of tasks (for example, `"deleteFileAfterReboot": false`)
- Task execution errors and return codes
- Task completion statuses
- Task completion time
- Versions of the settings used for execution of the tasks
- Information about the objects submitted to the server, quarantined objects, and objects restored from the quarantine: paths to objects, MD5 and SHA256 hashes, identifiers of quarantined objects
- Information about the processes started or stopped on the device with Kaspersky Endpoint Agent installed upon the server request: PID and UniquePID, error code, MD5 and SHA256 hashes of the objects
- Information about the services started or stopped on the device upon the server request: service name, startup type, error code, MD5 and SHA256 hashes of file images of the services

- Information about the objects for which a memory dump was made for YARA scan (paths, dump file identifier)
- Files requested by the server
- Telemetry packets
- Data on running processes:
  - Executable file name, including full path and extension
  - Process autorun parameters
  - Process ID
  - Login session ID
  - Login session name
  - Date and time when the process was started
  - MD5 hash of the object
  - SHA256 hash of the object
- Data on files:
  - File path
  - File name
  - File size
  - File attributes
  - Date and time when the file was created
  - Date and time when the file was last modified
  - File description
  - Company name
  - MD5 hash of the object
  - SHA256 hash of the object
  - Registry key (for autorun points)
- Data in errors that occur when information about objects was retrieved:
  - Full name of the object that was processed when an error occurred
  - Error code

4. Telemetry data:

- Host IP-address
- Data type in the registry prior to the committed update operation
- Data in the registry key prior to the committed change operation
- The text of the processed script or a part of it
- Type of the processed object
- Way of passing a command to the command interpreter

Data from the requests of the Central Node component to Kaspersky Endpoint Agent:

1. Task settings:
   - Task type
   - Task schedule settings
   - Names and passwords of the accounts under which the tasks can be run
   - Versions of settings
   - Identifiers of quarantined objects
   - Paths to the objects
   - MD5 and SHA256 hashes of the objects
   - Command line to start the process with the arguments
   - Flags of the additional actions performed by Kaspersky Endpoint Agent upon completion of the task
   - IOC file identifiers to be retrieved from the server
   - IOC files
   - Service name
   - Service startup type
   - Folders for which the results of the Get forensic task must be received
   - Masks of the object names and extensions for the Get forensic task
2. Network isolation settings:
   - Types of settings
   - Versions of settings
   - Lists of network isolation exclusions and exclusion settings: traffic direction, IP addresses, ports, protocols, and full paths to executable files
   - Flags of additional actions performed by Kaspersky Endpoint Agent

- Time of automatic isolation disabling

3. Settings for prevention executing of files and opening of documents:

   - Types of settings
   - Versions of settings
   - Lists of execution prevention rules and rule settings: paths to objects, types of objects, MD5 and SHA256 hashes of objects
   - Flags of additional actions performed by Kaspersky Endpoint Agent

4. Event filtering settings:

   - Module names
   - Fill paths to objects
   - MD5 and SHA256 hashes of the objects
   - Identifiers of the entries in Windows event log
   - Digital certificate settings
   - Traffic direction, IP addresses, ports, protocols, full paths to executable files
   - User names
   - User logon types
   - Types of telemetry events for which filters are applied

Data in requests to Kaspersky Industrial CyberSecurity for Networks server

During integration with Kaspersky Industrial CyberSecurity for Networks, the following data can be stored locally on the device with Kaspersky Endpoint Agent in the %ProgramData%\Kaspersky Lab\Endpoint Agent\4.0\Data\Cache\Queue\Kics 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.

Data sent by Kaspersky Endpoint Agent to Kaspersky Industrial CyberSecurity for Networks server:

- Network interface data:
  - Network interface description
  - Domain
  - MAC address

    - Metric number
    - List of IP addresses that consists of a set of entries in the following format: IP address / subnet mask / gateway address
- Patch lists:
    - Patch number
    - Patch installation date
- Lists of installed EPP applications:
    - EPP application name
    - Application version
    - Application database version
    - Date of the last application update
    - List of license keys (number, type, expiration date, key status)
- Data on established network connections:
    - Local IP address
    - Local MAC address
    - Remote IP address
    - Remote MAC address
    - Gateway IP-address
    - Protocol type (according to IANA)

Data for creating a threat development chain

The data for building the threat development chain is stored in the %ProgramData%\Kaspersky Lab\Endpoint Agent\4.0\Data\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.

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.

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.

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;
- 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 Administration Server, using the Central Node component interface, 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 Administration Console	• 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 can be configured in the policy properties, and the settings of network isolation on demand (manually enabled settings) can be 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.
Central Node component	Network isolation management using the Central Node component is described separately.	Kaspersky Endpoint Agent retains network isolation settings received from the Central Node component in the device properties in Kaspersky Security Center.

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 name extensions and corresponding applications are listed in the following table.

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

Application name	Executable file	File name 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:

- AutoHotkey.exe

- AutoHotkeyA32.exe
- AutoHotkeyA64.exe
- AutoHotkeyU32.exe
- AutoHotkeyU64.exe
- InstallUtil.exe
- RegAsm.exe
- RegSvcs.exe
- autoit.exe
- cmd.exe
- control.exe
- cscript.exe
- hh.exe
- mmc.exe
- msbuild.exe
- mshta.exe
- msiexec.exe
- perl.exe
- powershell.exe
- python.exe
- reg.exe
- regedit.exe
- regedt32.exe
- regsvr32.exe
- ruby.exe
- rubyw.exe
- rundll32.exe
- runlegacycplelevated.exe
- wscript.exe

- wwahost.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.

Kaspersky Endpoint Agent supports three types of IOC Scan tasks:

- *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*.
- *IOC scan by IOC files downloaded manually via Kaspersky Anti Targeted Attack Platform web interface* allows application users to use IOC files to search for signs of targeted attacks, infected and probably infected objects in the event and detection database, and to scan computers with Kaspersky Endpoint Agent installed.

Different tasks are managed in different ways, have different configurable settings, and different task scopes. Description of each type of IOC Scan task is provided in the table below.

IOC Scan task types

Task type	Task description	Task scope
Standard IOC Scan tasks	These tasks are created and configured manually in Kaspersky Security Center or using the command line interface, without integration with third-party systems. IOC files prepared by the user are used to run the tasks. Task settings do not depend on the policy settings. The **Retrospective IOC scan** mode is available for tasks. You can specify the following actions to respond to the detected IOCs (not available when running the tasks from the command line): • Run on-demand scan tasks using EPP on the device. • Enable network isolation of the device. Viewing reports is available both in the task execution results as a summary table and in the Detected IOC card.	Local or group
Autonomous IOC Scan tasks	These tasks are created automatically if in Kaspersky Endpoint Agent policy, the **Run IOC Scan on a managed group of devices** action is selected in response to the threats detected by Kaspersky Sandbox.	Group

	Kaspersky Endpoint Agent generates an IOC file automatically. Operations with custom IOC files are not supported. Limited task management in Kaspersky Security Center is available for the user. In the policy settings you can specify the task start schedule and the scan area for the task. Tasks are automatically deleted in seven days after the last start or after creation if tasks were never started. You can specify the following actions to respond to the detected IOCs: • Run on-demand scan tasks using EPP on the device. • Quarantine the object and delete it from the device. Viewing reports is available both in the task execution results as a summary table and in the Detected IOC card.	
IOC Scan by IOC files downloaded manually via Kaspersky Anti Targeted Attack Platform web interface	IOC files are downloaded manually via Kaspersky Anti Targeted Attack Platform web interface. It is also possible to configure IOC scan schedule for computers with Kaspersky Endpoint Agent in the web interface of Kaspersky Anti Targeted Attack Platform. Task management using Kaspersky Security Center or using the command line is not supported. No actions are automatically performed when IOC is detected. Task settings do not depend on Kaspersky Endpoint Agent policies.	Not applicable

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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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.
- Only the files with IOC rules can be specified for the IOC Scan task. Files with other types of rules are not supported for the IOC Scan task.
- 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.

The table below shows the features and limitations of the OpenIOC standard supported by the application.

Features and limitations of the OpenIOC standard versions 1.0 and 1.1

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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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 IOC Scan tasks using Kaspersky Security Center or using Kaspersky Endpoint Agent command line interface, as well as download IOC files and configure IOC scan schedule in Kaspersky Anti Targeted Attack Platform web interface. The description of each IOC Scan task type and information on the available management capabilities for IOC Scan tasks are shown in the table below.

Managing IOC Scan tasks.

Task type	Using Kaspersky Security Center	Using the Central Node component	Using the command line interface
Standard IOC Scan task	• Creating, removing and starting the task manually. • Viewing detailed reports on the task execution results as a summary table and in the Detected IOCs card. • IOC collection export. • Configuring the following task settings in the task creation wizard or in the task properties after the task creation:	Task management is not applicable.	• Creating and running the task with the required settings. • Viewing data on the task execution.

	• IOC collection settings. • IOC scan settings. • Application actions when detecting IOC (network isolation of the device and start of the scan tasks using EPP on the device). • Task schedule settings. • Storage time for the task execution results on the Administration Server (unavailable in the task creation wizard).		

Autonomous IOC Scan task	• Configuring the task start settings.
	• Starting and removing the task manually.
	• Enabling response to the threats detected by Kaspersky Sandbox.
	• Adding an action to automatically create an Autonomous IOC Scan Task.
	• Viewing detailed reports on the task execution results as a summary table and in the Detected IOCs card.
	• IOC collection export.
	• Configuring the following settings in the task properties:
	  • Application actions when detecting IOC (quarantining an object and deleting it from the device; starting the scan tasks using EPP on the device).
	  • Task schedule settings.
	  • Storage time for the task execution results on the Administration Server.
		Task management is not applicable.	Task management is not applicable.

IOC Scan task created by Central Node	Task management is not applicable.	Downloading IOC files, configuring IOC scan schedule.	Task management is not applicable.

YARA scan

This section contains information about YARA scan and configuring the scan settings.

About YARA scan in Kaspersky Endpoint Agent

YARA scan is a process performed by Kaspersky Endpoint Agent to search for malicious activity signatures on devices using YARA files (signature files of the open YARA standard). Scan is performed recursively on local drives. Scan is not supported for network, connected and cloud resources.

Kaspersky Endpoint Agent supports the following types of YARA scan:

- *YARA files scan using the command line* – group or local tasks that are created and configured using the command line interface. YARA files prepared by the user are used to run the tasks.
- *YARA scan by the files downloaded manually via Kaspersky Anti Targeted Attack Platform web interface* allows application users to use YARA files to search for signs of targeted attacks, infected and probably infected objects in the event and detection database, and to scan computers with Kaspersky Endpoint Agent installed.

The scan types differ by the management capabilities and configurable settings. The YARA scan types are described in the following table.

YARA scan types

Scan type	Description
YARA files scan using the command line	The scan is started manually using the command line interface, without integration with the third-party systems. YARA files prepared by the user are used to run the scan. Scan settings do not depend on the policy settings. The scan results are available immediately after scan is completed in the command line.
YARA scan by the YARA files downloaded manually via Kaspersky Anti Targeted Attack Platform web interface	IOC files are downloaded manually via Kaspersky Anti Targeted Attack Platform web interface. It is also possible to configure YARA scan schedule for computers with Kaspersky Endpoint Agent in the web interface of Kaspersky Anti Targeted Attack Platform. Scan cannot be managed using the command line. There are no automatic actions when YARA rules are triggered. Scan settings do not depend on Kaspersky Endpoint Agent policies. For detailed information about this type of scan, refer to *Kaspersky Anti Targeted Attack Platform Help*.

Requirements for YARA files

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

When performing YARA scan, consider the following requirements and limitations related to YARA files:

- Kaspersky Endpoint Agent supports YARA files with the `yara` and `yar` extensions. These files use open standard for compromise indicators description – YARA version 4.0.2.
- Only the files with YARA rules can be specified for the YARA Scan task. Files with other types of rules are not supported for the YARA Scan task.
- If during scanning you download YARA files that are not supported by Kaspersky Endpoint Agent or contain syntax errors, the scan start will be terminated and the corresponding error message will be displayed.
- Identifiers of all YARA files that are used in the same YARA Scan task must be unique. The presence of YARA files with the same identifier can affect the correctness of the task execution results.

It is recommended to create one rule in one YARA file. This approach makes the scan results easier to read.

Managing YARA scan in Kaspersky Endpoint Agent

In Kaspersky Endpoint Agent, you can manage YARA scan using the command line interface.

The following actions are available in the command line interface:

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

Working with incident card

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

The incident card is deleted automatically 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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

The following prerequisites must be met to create a threat development chain:

- 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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

An incident card is available in the window that contains the list of incidents. The list of incidents is available in the **Report on threats** or in the **Alerts** subsection of the **Monitoring and reporting** section in Kaspersky Security Center Web Console or Kaspersky Security Center Cloud Console.

For the application to create a threat development chain, the preconditions for creating threat development chain must be met.

If you add a license key for EDR Optimum, the **Alerts** subsection will automatically appear in the main menu in the **Monitoring and reporting** section. You can also configure the display of the **Alerts** subsection in the properties of Kaspersky Security Center Web Console or Kaspersky Security Center Cloud Console interface. For detailed information refer to *Kaspersky Security Center Help*.

To view the incident card in the Alerts subsection:

1. In the main Web Console window open the **Monitoring and reporting** → **Alerts** section.
2. Select an incident and click the **more details** link.

   The incident card will be displayed.

To view the incident card in the Report on threats:

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.

   The incident card will be displayed.

Selecting an action on a file from the incident card

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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** button.

Creating IOC Scan task from the incident card

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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** 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** on the right side of the screen.
5. In the **Actions** 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 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 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 the 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.
Quit task, running 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	*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 IOC documents for which data is collected	When analyzing data on files (FileItem), the **Analyze file data (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 areas on 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 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 **Integration with Kaspersky Sandbox** 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*.

About the EDR notifications widget

The EDR notifications widget displays information about the number of incidents detected on the devices for the last month. The EDR notifications widget is available on the **Dashboard** tab in Kaspersky Security Center Web Console or in Kaspersky Security Center Cloud Console. From the EDR notifications widget, you can open the **Notifications** section that contains the list of incidents detected on devices.

To add the EDR notifications widget to the dashboard:

1. Go to the **Monitoring and reporting** → **Dashboard** section.
2. Click the **Add or restore web widget** button.
3. In the list of available web widgets, select the **Notifications** web widget from the **Threat statistics** category.
4. Click the **Add** button.

The web widget is added to the end of the dashboard.

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 received 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).

About integration with Kaspersky Anti Targeted Attack Platform

Kaspersky Anti Targeted Attack Platform is a solution for protection of an organization IT infrastructure and early detection of threats such as zero-day attacks, targeted attacks, and advanced persistent threats (hereinafter also referred to as APT). The application is intended for corporate users.

Kaspersky Anti Targeted Attack Platform includes two functional parts:

- Kaspersky Anti Targeted Attack (hereinafter also referred to as KATA) – protects the enterprise IT infrastructure perimeter.
- Kaspersky Endpoint Detection and Response (hereinafter also KEDR) – protects computers in the organization local network.

Kaspersky Endpoint Detection and Response includes the following components:

- Central Node.
- Kaspersky Endpoint Agent.

The components interact according to the following principle:

Kaspersky Endpoint Agent is installed on individual computers running Windows that are included in the organization IT infrastructure. The application constantly monitors processes, open network connections, and files being modified. Data about events on the computer is sent to the server with the Central Node component.

When integrating the Central Node server with Kaspersky Endpoint Agent, you can take the following measures to respond to the detected threats:

- Work with files and applications by executing tasks on the devices with Kaspersky Endpoint Agent installed.
- Configure policies to prevent files and processes from running on the selected devices with Kaspersky Endpoint Agent installed.
- Isolate individual devices with Kaspersky Endpoint Agent from the network.
- Work with TAA (IOA) rules for event classification and analysis.
- Work with OpenIOC files (files of the open standard for describing indicators of compromise, IOC files) to search for signs of targeted attacks, infected and possibly infected objects on the devices with Kaspersky Endpoint Agent and in the detection database.
- Work with open standard YARA files containing YARA rules to search for malicious activity signatures on the devices with Kaspersky Endpoint Agent.

You can configure integration between Kaspersky Endpoint Agent and KATA Central Node in Kaspersky Security Center Administration Console, in Kaspersky Security Center Web Console or using the command line interface locally on the device.

For complete information about Kaspersky Anti Targeted Attack Platform, as well as for information on configuring Kaspersky Endpoint Agent integration from KATA side, refer to *Kaspersky Anti Targeted Attack Platform Help*.

About integration with Kaspersky Managed Detection and Response

Kaspersky Managed Detection and Response (also referred to as MDR) delivers round-the-clock protection from the growing volume of threats that circumvent automated security barriers to organizations who struggle to find the expertise and staff, or for those with limited in-house resources. Unlike similar offerings on the market, this service leverages a proven track record of effective targeted attack research to ensure continuous defense against even the most complex threats. The service helps improve your corporate resilience to cyberthreats, while freeing up your existing resources to focus their attention on other tasks.

You integrate Kaspersky Endpoint Agent into the client infrastructure using Kaspersky Security Center. Kaspersky Endpoint Agent processes data and sends it to Kaspersky Managed Detection and Response via Kaspersky Security Network streams.

You can configure Kaspersky Endpoint Agent integration with MDR in Kaspersky Security Center Administration Console or in Kaspersky Security Center Web Console.

For complete information about Kaspersky Managed Detection and Response, as well as for information on configuring Kaspersky Endpoint Agent integration from MDR side, refer to *Kaspersky Managed Detection and Response Help*.

About integration with Kaspersky Sandbox

Kaspersky Sandbox detects and automatically blocks complex threats on the client devices (workstations, computers, servers, hereinafter also "workstations").

The solution is intended for corporate users.

Kaspersky Sandbox consists of the following components:

- Kaspersky Sandbox – responsible for the server side of the solution. Kaspersky Sandbox is installed on one or several servers within your organization network. The servers can be clustered. Virtual images of Microsoft Windows operating systems are deployed on the servers with Kaspersky Sandbox. The objects being scanned are launched in these virtual images. Kaspersky Sandbox analyzes the behavior of objects to detect malicious activity and complex threats in the organization IT infrastructure.

- Endpoint Protection Platform (hereinafter also EPP) – Kaspersky Endpoint Security for Windows and Kaspersky Security for Windows Server. Kaspersky Endpoint Security for Windows and Kaspersky Security for Windows Server are installed on workstations in your organization network and provide comprehensive protection of the workstations against various types of threats, network and fraudulent attacks.

- Kaspersky Endpoint Agent for Windows, which is installed as part of EPP. Kaspersky Endpoint Agent for Windows is installed on workstations and servers in your organization network and provides communication between EPP and Kaspersky Sandbox, as well as performs automatic response actions to detected threats configured in Kaspersky Security Center policies.

You can configure integration between Kaspersky Endpoint Agent and Kaspersky Sandbox in Kaspersky Security Center Administration Console or using the command line interface locally on the device.

For complete information about Kaspersky Sandbox, as well as for information on configuring Kaspersky Endpoint Agent integration from Kaspersky Sandbox side, refer to *Kaspersky Sandbox Help*.

About integration with Kaspersky Industrial CyberSecurity for Networks

Kaspersky Industrial CyberSecurity for Networks is designed to protect the infrastructure of industrial enterprises from information security threats and to ensure the continuity of technological processes. Kaspersky Industrial CyberSecurity for Networks analyzes industrial network traffic to detect deviations in the values of technological parameters, detect signs of network attacks, and monitor the operation and current state of devices in the network. The application is a part of Kaspersky Industrial CyberSecurity solution.

Kaspersky Industrial CyberSecurity for Nodes is a complex server and workstation security solution for IT threats in industrial control systems.

Kaspersky Endpoint Agent allows you to configure integration between Kaspersky Industrial CyberSecurity for Networks and Kaspersky Industrial CyberSecurity for Nodes. Kaspersky Endpoint Agent is installed on individual devices with Kaspersky Industrial CyberSecurity for Nodes installed. Data about events on the device, received by Kaspersky Industrial CyberSecurity for Nodes, is sent to Kaspersky Industrial CyberSecurity for Networks server by means of Kaspersky Endpoint Agent. Integration between the applications enhances Kaspersky Industrial CyberSecurity for Networks capabilities to investigate and respond to threats in industrial networks.

You can configure integration between Kaspersky Endpoint Agent and Kaspersky Industrial CyberSecurity for Networks in Kaspersky Security Center Administration Console, in Kaspersky Security Center Web Console, or using the command line interface locally on the device.

For complete information about Kaspersky Industrial CyberSecurity for Networks, as well as for information on configuring integration with Kaspersky Endpoint Agent from the side of Kaspersky Industrial CyberSecurity for Networks, refer to *Kaspersky Industrial CyberSecurity for Networks Help*.

Within integration with Kaspersky Industrial CyberSecurity for Networks, Kaspersky Endpoint Agent only sends telemetry data. Response actions to detected threats, network Isolation, and IOC Scan are not available.

Managing Kaspersky Endpoint Agent using Kaspersky Security Center Administration Console

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 Administration Console (hereinafter also referred to as *Administration Console*) provides the user interface for working with Kaspersky Security Center. Administration Console is implemented as an extension component to the Microsoft Management Console (MMC).

Kaspersky Endpoint Agent can be managed in Kaspersky Security Center Administration Console using Kaspersky Endpoint Agent Management plug-in.

This section contains the basic information about managing Kaspersky Endpoint Agent using Kaspersky Security Center Administration Console.

Managing Kaspersky Endpoint Agent policies

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

Creating Kaspersky Endpoint Agent policy

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To create a Kaspersky Endpoint Agent policy in Kaspersky Security Center:

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Click **Create a policy**.
   The policy creation wizard starts.
4. In the **Enter group policy name** window, perform the following actions:
   a. Enter the name that will be used for the new policy in the policy list.

b. If you want to import the settings of an existing Kaspersky Endpoint Agent policy to a new policy, perform the following actions:

1. Select the **Use the policy settings for previous application version** check box.
2. Click **Select** and in the window that opens, select the policy whose settings you want to import.
3. Click **OK**.

c. Click **Next**.

5. In the **New policy** window, select one of the following options and click **Next**:

- **Create a new policy and configure its settings**.
- **Create a new policy with default settings**.

If you enabled the **Use the policy settings for previous application version** setting at the previous step, the **Create a new policy and configure its settings** option is selected by default, and the settings specified in the imported policy are displayed during the policy creation. In this case, the switch in the upper right corner of each section with the policy settings, that shows if the policy is applied, depends on the position of the switches in the groups of settings of the imported policy.

6. In the **Select policy type** window, select the required Kaspersky Endpoint Agent deployment method:

- **Kaspersky Sandbox**
- **Endpoint Detection and Response Expert (KATA EDR)**

7. Click **Next**.

8. If you select the **Create a new policy and configure its settings** option, perform one of the following actions in all sequentially displayed settings windows:

- To configure the application settings in displayed sections during the policy creation:

  a. Click **Configure** next to the name of the required section.

  b. In the window that opens, configure the required settings and click **OK**.

  c. Click **Next**.

- To configure the application settings in the displayed section later, click **Next**.

Configuration of the application settings consists of the following steps:

The composition of the steps depends on the type of policy selected at the previous step and may differ from the one described.

- Configuring integration between Kaspersky Endpoint Agent and Kaspersky Sandbox.
- Configuring integration between Kaspersky Endpoint Agent and the KATA Central Node component.

- Configuring threat response settings.
- Configuring application repositories.
- Configuring application security settings.
- Configuring general application settings.

9. In the **Target group** window, select Kaspersky Security Center administration group to which the created policy will be applied by performing the following steps:

   a. Click **Browse**.

   The administration group selection window opens.

   b. Select the administration group from the list.

   For example, you can select the **Managed devices** group.

   c. If you want to create a subgroup in the **Managed devices** group:

      1. Click **New group**.
      2. In the window that opens, enter the name of the device subgroup.
      3. Click **OK**.

   d. Click **Next**.

10. In the **Creating a group policy for the application** window select one of the following policy statuses:
    - **Active policy** to activate the policy immediately after creation.
    - **Inactive policy** to activate the policy later.
    - **Out-of-office**. The policy becomes active when the computer leaves the corporate network.
11. Select the **Open policy properties after creation** check box, if you want to perform additional configuration of the policy immediately after creation.
12. Click **Finish**.

The created policy appears in the policy list.

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. The settings in the policy sections are divided into groups. You can enable either individual groups or all groups within one policy.

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

1. Open Kaspersky Security Center Administration Console.

2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.
4. Select the policy for which you want to enable the settings.
5. In the window that opens, select the section and group of settings to which the required setting belongs.
6. In the upper right corner of the settings group, change the switch from **Unaffected by policy** to **Under policy**.

All the settings of the group will be applied in the policy after the changes are saved.

Configuring Kaspersky Endpoint Agent settings

This section describes how to configure Kaspersky Endpoint Agent settings.

Opening Kaspersky Endpoint Agent settings window

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To open Kaspersky Endpoint Agent settings window:

1. Open Kaspersky Security Center Administration Console.
2. Expand the **Managed devices** node in Kaspersky Security Center Administration Console tree.
3. Select the administration group for which you want to configure application settings.
4. Perform one of the following actions in the details pane of the selected administration group:
   - To configure the application settings for a group of devices, select the **Policies** tab and open the **Properties: <Policy name>** window by double-clicking the policy name or by selecting **Properties** in the context menu.
   - To configure the application settings for a single device, select the **Devices** tab and perform the following actions:
     a. Open the **Properties: <Device name>** window by double-clicking the device name or by selecting **Properties** in the context menu.

b. Select the **Applications** section.

c. Open the **Application settings** window by double-clicking the application name or by clicking the **Properties** button under the list of applications.

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

Configuring Kaspersky Endpoint Agent security settings

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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.

Configuring user permissions

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
   - Double-click the policy name.
   - Select **Properties** in the policy context menu.

- Select the **Configure policy settings** item in the right part of the window.

4. In the **Application settings** section select the **Security settings** subsection.
5. In the **User permissions** group of settings, click the **Configure** button next to the name of the required setting.

   The permissions window for Kaspersky Endpoint Agent group opens.
6. In the upper block of settings for groups or users, select the group or user to which you want to grant permissions.
7. In the lower block of permission settings for groups or users, select check boxes in items with the required permissions.
8. Click **OK**.
9. In the upper right corner of the settings group, change the switch from **Unaffected by policy** to **Under policy**.
10. In the policy properties window, click **OK**.

User permissions for managing the application settings and services are configured and applied.

Enabling Password protection

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.
4. In the **Application settings** section select the **Security settings** subsection.
5. In the **Password protection** group of settings select the **Apply password protection** check box.
6. Enter a password and confirm it.

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

- Password is at least 8 characters long.
- Password does not user account name.
- Password does not match the name of the device on which Kaspersky Endpoint Agent is installed.
- Password contains characters from at least three of the following groups:
  - uppercase characters (A-Z);
  - lowercase characters (a-z);
  - numbers (0-9);
  - special characters (!$#%).

7. In the upper right corner of the settings group, change the switch from **Unaffected by policy** to **Under policy**.
8. Click **OK**.

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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:

- Double-click the policy name.
- Select **Properties** in the policy context menu.
- Select the **Configure policy settings** item in the right part of the window.

4. In the **Application settings** section select the **Security settings** subsection.
5. In the **Self-defense** group of settings, enable or disable the **Enable self-defense for application modules in memory** setting.

   The setting is enabled by default.
6. In the upper right corner of the settings group, change the switch from **Unaffected by policy** to **Under policy**.
7. Click **OK**.

The Self-Defense mechanism is enabled or disabled.

Configuring Kaspersky Endpoint Agent connection settings to a proxy server

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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

If you want to use a specified proxy server when connecting to KATA server, Kaspersky Sandbox server or Kaspersky Industrial CyberSecurity for Networks server, make sure that the **Connect using the proxy server if specified in the general settings** option is selected when configuring integration with KATA, Kaspersky Industrial CyberSecurity for Networks or Kaspersky Sandbox. This option is not selected by default.

To configure proxy server connection settings:

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.
4. In the **Application settings** section select the **Other settings** subsection.

5. Select one of the following proxy service usage options:

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

6. If you select the **Automatically detect proxy server address** option, the proxy server for further telemetry transmission is detected automatically.

7. 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.

8. If you want to use NTLM authentication (NT LAN Manager Network Authentication Protocol) 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.

9. 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.

10. Click the **Apply** button.

    As a result, you return to the policy properties window.

11. In the upper right corner of the settings group, change the switch from **Unaffected by policy** to **Under policy**.

12. Click **OK**.

Proxy server connection settings are configured.

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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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

1. Open Kaspersky Security Center Administration Console.

2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.
4. In the **Application settings** section select the **Other settings** subsection.
5. In the **Licensing** group of settings, select the **Use Kaspersky Security Center as a proxy server when activating the application** check box.
6. In the upper right corner of the settings group, change the switch from **Unaffected by policy** to **Under policy**.
7. Click **OK**.

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

Configure network isolation settings

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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

Enabling and disabling network isolation

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To enable or disable network isolation of a device:

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

1. In the **Managed devices** folder of the Administration Console tree, select the folder with the name of the administration group, which includes the required device.
2. In the workspace, select the **Devices** tab.
3. Select the device for which you want to configure Kaspersky Endpoint Agent settings.
4. Select **Properties** in the device context menu.

   The device properties window opens.
5. Select the **Applications** section.

   A list of Kaspersky applications installed on the device is displayed in the window.
6. Select Kaspersky Endpoint Agent and open its properties window in one of the following ways:
   - Double-click the application name.
   - In the application context menu, select **Properties**.
   - Click the **Properties** button under the list of Kaspersky applications.

2. In the **Network isolation** section select **General settings**.
3. In the **Isolate device** group of settings, enable or disable the **Isolate current device from the network** setting.
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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

The settings of automatic network isolation can be configured in the policy properties, and the settings of network isolation on demand (manually enabled settings) can be 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 enable or disable the **Notify the device user when device is isolated from the network** setting.
4. Click **OK** to save the changes.

Configuring automatic disabling of network isolation

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

The settings of automatic network isolation can be configured in the policy properties, and the settings of network isolation on demand (manually enabled settings) can be 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 **Managed devices** folder of the Administration Console tree, select the folder with the name of the administration group, which includes the required device.
2. In the workspace, select the **Devices** tab.
3. Select the device for which you want to configure Kaspersky Endpoint Agent settings.
4. Select **Properties** in the device context menu.

   The device properties window opens.
5. Select the **Applications** section.

   A list of Kaspersky applications installed on the device is displayed in the window.
6. Select Kaspersky Endpoint Agent and open its properties window in one of the following ways:
   - Double-click the application name.
   - In the application context menu, select **Properties**.
   - Click the **Properties** button under the list of Kaspersky applications.

- Open the policy properties window.

  1. Open Kaspersky Security Center Administration Console.
  2. In the console tree, open the **Policies** folder.
  3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
     - Double-click the policy name.
     - Select **Properties** in the policy context menu.
     - Select the **Configure policy settings** item in the right part of the window.

2. In the **Network isolation** section select **General settings**.
3. In the **Device isolation terms** group of settings enable or disable the **Automatically end device isolation after** option to enable or disable automatic disabling of network isolation after a specified period of time.
   - This feature is enabled by default.
4. Specify the period after which network isolation will be disabled.

   The default period is 30 minutes.
5. 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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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 **Managed devices** folder of the Administration Console tree, select the folder with the name of the administration group, which includes the required device.
  2. In the workspace, select the **Devices** tab.
  3. Select the device for which you want to configure Kaspersky Endpoint Agent settings.
  4. Select **Properties** in the device context menu.

     The device properties window opens.
  5. Select the **Applications** section.

     A list of Kaspersky applications installed on the device is displayed in the window.
  6. Select Kaspersky Endpoint Agent and open its properties window in one of the following ways:

     - Double-click the application name.
     - In the application context menu, select **Properties**.
     - Click the **Properties** button under the list of Kaspersky applications.

- Open the policy properties window.

  1. Open Kaspersky Security Center Administration Console.
  2. In the console tree, open the **Policies** folder.
  3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
     - Double-click the policy name.
     - Select **Properties** in the policy context menu.
     - Select the **Configure policy settings** item in the right part of the window.

2. If you open the application properties window for an individual device, in the **Network isolation** section, select **Exclusion rules**.
3. If you open the application policy properties window, in the **Network isolation** section, select **Isolation on detection**.
4. You can perform the following actions:

   - Add custom exclusion

     To add a custom exclusion:

     1. Click **Add**.
     2. In the drop-down list select **Add custom rule**.
        The **Rule properties** window opens.
     3. 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 **Modify**.
2. In the drop-down list select **Add from the network profile dictionary**.
3. In the window that opens, select the required network profile from **Predefined network profiles list**.
   At the bottom of the window, the description of the selected network profile is displayed.
4. If you want to view the exclusions that will be applied with the selected network profile, click the **Show rules list** button.
5. If you want to add the selected network profile to the list of applicable profiles, click **-->**.
   You can add several network profiles at once.
6. Click the **Add selected** button.
   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. Select the required exclusion in the **Exclusion rules** list.
2. Click the **View and edit** button.
3. The **Rule properties** window opens.
4. 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.

- Enable or disable exclusion

To enable an exclusion,

select the check box next to the exclusion name in the **Exclusion rules** list.

To disable an exclusion,

clear the check box next to the exclusion name in the **Exclusion rules** list.

- Remove exclusion from the list

To remove an exclusion from the list:

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

   The exclusion is removed from the list of exclusions.

5. To save changes, click **Apply**.

Configuring KSN usage in Kaspersky Endpoint Agent

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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 and later. 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. Open Kaspersky Security Center Administration Console.

2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.
4. Select the **Participation in KSN** section.
5. Review the KSN Statement.
6. 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.
7. Select the **Enable Kaspersky Security Network usage** check box.
8. If you want to use Kaspersky Security Center for telemetry transmission, select the **Use Kaspersky Security Center as a KSN proxy server** check box.
9. In the upper right corner of the settings group, change the switch from **Unaffected by policy** to **Under policy**.
10. Click **OK**.

KSN usage is enabled.

Configuring the integration of Kaspersky Endpoint Agent with Kaspersky Sandbox

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

This section contains information on configuring the integration of Kaspersky Endpoint Agent with Kaspersky Sandbox. Integration must be configured both on Kaspersky Endpoint Agent side using Kaspersky Security Center Administration Console, and on Kaspersky Sandbox side using the web interface.

Enabling and disabling integration with Kaspersky Sandbox

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To enable or disable integration with Kaspersky Sandbox:

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.
4. In the **Kaspersky Sandbox integration** section select the **Kaspersky Sandbox integration settings** subsection.
5. In the **Kaspersky Sandbox integration settings** group of settings, enable or disable the **Enable Kaspersky Sandbox integration** setting.
6. In the **Kaspersky Sandbox integration settings** group of settings, enable or disable the **Connect using the proxy server if specified in the general settings** option.

   This option is disabled by default. The application connects to Kaspersky Sandbox server only directly and does not use the general proxy server connection settings. You can enable this option if you want the application to use the general proxy server connection settings when connecting to Kaspersky Sandbox server.
7. In the upper right corner of the settings group, change the switch from **Unaffected by policy** to **Under policy**.
8. Click **OK**.

Integration with Kaspersky Sandbox is enabled (or disabled).

Configuring trusted connection between Kaspersky Sandbox and Kaspersky Endpoint Agent

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

You can configure a trusted connection between Kaspersky Sandbox and Kaspersky Endpoint Agent in the web interface of Kaspersky Sandbox server that is not included in the cluster.

If you have already merged servers into a cluster, remove the server from the cluster, then create a new cluster based on this server and add all the servers intended for Kaspersky Sandbox solution to the new cluster.

If the servers you need belong of another cluster, remove them from that cluster one by one and then add them to your cluster.

Installing and configuring a trusted connection between Kaspersky Sandbox and Kaspersky Endpoint Agent involves:

1. **Removing a server from the cluster (if the server belongs to a cluster)**
2. **Generating or uploading to the server a TLS certificate for connection with Kaspersky Endpoint Agent**
3. **Creating a new cluster based on this server**
4. **Removing all the servers that you want to add to this cluster from the clusters they currently belong to**
5. **Adding all required servers to the new cluster**
6. **Adding all servers belonging to Kaspersky Sandbox new cluster to Kaspersky Endpoint Agent list**
7. **Configuring a trusted connection with Kaspersky Sandbox on Kaspersky Endpoint Agent side**

Configuring trusted connection on Kaspersky Sandbox side

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To configure trusted connection, generate or upload a TLS certificate in Kaspersky Sandbox, save it on a computer, and then download it to Kaspersky Endpoint Agent.

To generate a TLS certificate for the connection of Kaspersky Sandbox with Kaspersky Endpoint Agent:

1. In Kaspersky Sandbox web interface window, select the **TLS certificates** section.
2. In the **TLS certificate for connecting to Kaspersky Endpoint Agent** section click the **Generate** button.
   The action confirmation window opens.
3. Click **Yes**.

   Kaspersky Sandbox generates a new TLS certificate. The browser page is automatically reloaded.

You can prepare the TLS certificate and upload it via Kaspersky Sandbox web interface.

The uploaded TLS certificate file must satisfy the following requirements:

- The file must contain the certificate itself and a private encryption key for the connection.
- The file must be in PEM format.
- The private key length must be 2048 bits or longer.

For more details about preparing TLS certificates for import, refer to OpenSSL documentation.

To upload the TLS certificate via Kaspersky Sandbox web interface:

1. In Kaspersky Sandbox web interface window, select the **TLS certificates** section.
2. In the **TLS certificate for connecting to Kaspersky Endpoint Agent** section click the **Upload** button.
   The file selection window opens.
3. Select the TLS certificate file that you want to upload and click **Open**.
   The file selection window closes.

The TLS certificate is added to Kaspersky Sandbox.

To save the TLS certificate file for the connection with Kaspersky Endpoint Agent on a computer:

1. In Kaspersky Sandbox web interface window, select the **TLS certificates** section.
2. In the **TLS certificate for connecting to Kaspersky Endpoint Agent** section click the **Download** button.

The TLS certificate file is saved in the Downloads folder of the browser.

Configuring trusted connection on Kaspersky Endpoint Agent side

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To configure trusted connection on Kaspersky Endpoint Agent side:

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.
4. In the **Kaspersky Sandbox integration** section select the **Kaspersky Sandbox integration settings** subsection.
5. In the **Kaspersky Sandbox integration settings** group of settings, enable the **Use trusted connection** setting.
6. Click the **Add new TLS certificate** button.
7. Perform one of the following actions to add a TLS certificate created on Kaspersky Sandbox side:

- Add a certificate file. Click **Browse**, and in the window that opens, select the certificate file and click **Open**.
- Copy and paste the contents of the certificate file to the **Paste TLS certificate data** field.

Kaspersky Endpoint Agent may have only one TLS certificate of Kaspersky Sandbox server. If you have added a TLS certificate before and then add a TLS certificate once again, only the last added certificate is valid.

8. Click **Add**.

   Information about the added TLS certificate is displayed in the **Kaspersky Sandbox integration settings** group of settings.

9. In the upper right corner of the settings group, change the switch from **Unaffected by policy** to **Under policy**.

10. Click **OK**.

Trusted connection to Kaspersky Sandbox server is configured.

Updating Kaspersky Sandbox TLS certificate data in Kaspersky Endpoint Agent

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

When replacing the TLS certificate of Kaspersky Sandbox server, you will need to update TLS certificate data in Kaspersky Endpoint Agent and reconfigure trusted connection with Kaspersky Sandbox.

To update Kaspersky Sandbox TLS certificate data in Kaspersky Endpoint Agent:

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.
4. In the **Kaspersky Sandbox integration** section select the **Kaspersky Sandbox integration settings** subsection and the **Kaspersky Sandbox integration settings** group of settings.
5. Select the **Use trusted connection** check box.
6. Click the **Add new TLS certificate** button.

   The **Adding new TLS certificate** window opens.

7. Perform one of the following actions to add a TLS certificate created on Kaspersky Sandbox side:

   - Add a certificate file. Click **Browse**, and in the window that opens, select the certificate file and click **Open**.
   - Copy and paste the contents of the certificate file to the **Paste TLS certificate data** field.

   Kaspersky Endpoint Agent may have only one TLS certificate of Kaspersky Sandbox server. If you have added a TLS certificate before and then add a TLS certificate once again, only the last added certificate is valid.

8. Click **Add**.

   Information about the added TLS certificate is displayed in the **Kaspersky Sandbox integration settings** group of settings.

9. In the upper right corner of the settings group, change the switch from **Unaffected by policy** to **Under policy**.

10. Click **OK**.

    As a result, Kaspersky Sandbox server TLS certificate data is updated and trusted connection with Kaspersky Sandbox is established.

Configuring the response timeout of Kaspersky Sandbox and request queue settings

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To configure the response timeout of Kaspersky Sandbox and processing queue settings for objects that Kaspersky Endpoint Agent sends to Kaspersky Sandbox:

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:

   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.

4. In the **Kaspersky Sandbox integration** section select the **Kaspersky Sandbox advanced settings** subsection.
5. In the **Timeout** group of settings, specify the maximum Kaspersky Sandbox response timeout.

   The default value is 5 seconds.

6. In the upper right corner of the settings group, change the switch from **Unaffected by policy** to **Under policy**.
7. In the **Kaspersky Sandbox requests queue** group of settings, in the **Queue folder** field specify the path to the folder where information about the requests sent to Kaspersky Sandbox will be stored.

   The default path is %SOYUZAPPDATA%\Sandbox\Queue.
8. In the **Maximum queue size (MB)** field, specify the maximum allowed size of the request queue in megabytes.

   The default value is 100 MB.
9. In the upper right corner of the settings group, change the switch from **Unaffected by policy** to **Under policy**.
10. Click **OK**.

Adding Kaspersky Sandbox servers to Kaspersky Endpoint Agent list

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

If you use Nginx as a proxy server between a device with Kaspersky Endpoint Agent installed and Kaspersky Sandbox server, configure the `client_max_body_size` setting. The value of the `client_max_body_size` setting must be equal to the maximum size of the object sent by Kaspersky Endpoint Agent to Kaspersky Sandbox for processing. Otherwise, Nginx will not send the objects whose size exceeds the specified value. The default value is 1 MB.

If you enabled the integration with Kaspersky Sandbox, you can add Kaspersky Sandbox servers to Kaspersky Endpoint Agent list. You can add several Kaspersky Sandbox servers.

Within the same policy, it is recommended to add servers that are part of the same cluster. If servers belong to different clusters, the outcome is unpredictable.

All servers in the cluster are peers regardless of which server was used as the base for creating the cluster. Processing the same object on any server in the cluster will yield the same result.

Kaspersky Sandbox balances load among the servers. Objects that Kaspersky Endpoint Agent sends for processing to Kaspersky Sandbox are processed on the least busy server.

To make Kaspersky Sandbox cluster process objects from Kaspersky Endpoint Agent, add to Kaspersky Endpoint Agent at least one server that is part of the cluster during the integration of Kaspersky Endpoint Agent with Kaspersky Sandbox.

The list of Kaspersky Sandbox servers of Kaspersky Endpoint Agent displays only the servers that you added to this list. Nevertheless, objects can be processed by any server in the cluster thanks to load balancing. The current list of servers in the cluster is displayed in the web interface of Kaspersky Sandbox.

It is recommended to add all servers of the cluster to Kaspersky Endpoint Agent.

Kaspersky Endpoint Agent can connect to a different Kaspersky Sandbox server in the list if one of the following errors occurs:

- Kaspersky Sandbox response timeout (connection timeout).
- Kaspersky Sandbox unavailable (error code 503 or 504).
- Self-diagnosis problem other than a license problem (error code 500).

When removing a server from the cluster, the following object processing scenarios are possible:

- If there is at least one server from this cluster with a valid IP address or fully qualified domain name (FQDN) in the list of Kaspersky Sandbox servers of Kaspersky Endpoint Agent, Kaspersky Sandbox continues to process objects from Kaspersky Endpoint Agent.
- If no servers from this cluster remain in the list of Kaspersky Sandbox servers of Kaspersky Endpoint Agent, or if IP addresses or fully qualified domain name of cluster servers are not valid, Kaspersky Sandbox cannot receive and process objects from Kaspersky Endpoint Agent.

  For correct processing of objects, at least one server from Kaspersky Sandbox cluster must be added to Kaspersky Endpoint Agent.

To add Kaspersky Sandbox servers to Kaspersky Endpoint Agent list:

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.
4. In the **Kaspersky Sandbox integration** section select the **Kaspersky Sandbox integration settings** subsection.
5. In the **Kaspersky Sandbox integration settings** group of settings, enable the **Enable Kaspersky Sandbox integration** setting.
6. In the **Kaspersky Sandbox integration settings** group of settings, enable or disable the **Connect using the proxy server if specified in the general settings** option.

   This option is disabled by default. The application connects to Kaspersky Sandbox only directly and does not use the general proxy server connection settings. You can enable this option if you want the application to use the general proxy server connection settings when connecting to Kaspersky Sandbox server.
7. In the **List of Kaspersky Sandbox servers** group of settings, click **Add**.

   The **Server properties** window opens.
8. Enter the IP address or fully qualified domain name of Kaspersky Sandbox server and the port used for connecting to the server.

9. Click **Add**.

   The added server is listed in the server table.

10. Repeat the steps to add each Kaspersky Sandbox server to the list.

11. In the upper right corner of the settings group, change the switch from **Unaffected by policy** to **Under policy**.

12. Click **OK**.

Kaspersky Sandbox servers are added to Kaspersky Endpoint Agent list.

Configuring Threat Response actions of Kaspersky Endpoint Agent to respond to threats detected by Kaspersky Sandbox

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

Kaspersky Endpoint Agent can perform actions in response to threats detected by Kaspersky Sandbox.

You can configure the following types of actions:

- *Local* – actions to be performed on each device where a threat is detected.
- *Group* – actions to be performed on all devices of the administration group for which the policy is configured.

Local actions:

- Quarantine and delete.

  When a threat is detected on a device, a copy of the object containing the threat is quarantined, and the object is deleted from the device.

- Notify device user.

  When a threat is detected on a device, a notification about the detected threat is displayed to the device user.

  The notification is displayed if the device is running under the user account same to the account under which the threat was detected.

  If the device is not running or is running under another user account, the notification is not displayed.

- Push Endpoint Protection Platform scanning on critical areas.

If a threat is detected on a device, Kaspersky Endpoint Agent sends a command to EPP to scan critical areas of the device. Critical areas include kernel memory, objects loaded at operating system startup, and boot sectors of the hard drive. For more details on configuring the scan settings refer to the documentation of EPP being used.

Group actions:

- **Run IOC Scanning on a managed group of devices**.

  If a threat is detected on any device of the administration group for which you configure the policy, Kaspersky Endpoint Agent scans all devices of this administration group for objects containing the detected threat.

- **Quarantine and delete when IOC is found**.

  If a threat is detected on any device of the administration group for which you configure the policy, Kaspersky Endpoint Agent scans all devices of this administration group for objects containing the detected threat. When an object which contains a threat is detected on devices of this administration group, a copy of the object containing the threat is quarantined, and the object is deleted from the device.

- **Push Endpoint Protection Platform scanning on critical areas when IOC is found**.

  If a threat is detected on any device of the administration group for which you configure the policy, Kaspersky Endpoint Agent sends a command to EPP to scan critical areas on all administration group's devices where the object containing the threat was detected. For more details on configuring the scan settings refer to the documentation of EPP being used.

To configure group threat response actions, set up the permissions of Kaspersky Security Center users, whose accounts you want use for managing IOC Scan tasks.

When configuring threat response actions, keep in mind that as a result of some actions, the object containing the threat may be deleted from the workstation where it was detected.

Enabling and disabling Threat Response actions

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To enable or disable Threat Response actions of Kaspersky Endpoint Agent for reacting to threats detected by Kaspersky Sandbox:

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.

3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
    - Double-click the policy name.
    - Select **Properties** in the policy context menu.
    - Select the **Configure policy settings** item in the right part of the window.
4. In the **Kaspersky Sandbox integration** section select the **Threat response** subsection.
5. In the **Actions** group of settings:
    - Select the **Take response actions on threats, detected by Kaspersky Sandbox** check box to enable Threat Response actions.
    - Clear the **Take response actions on threats, detected by Kaspersky Sandbox** check box to disable Threat Response actions.
6. In the upper right corner of the settings group, change the switch from **Unaffected by policy** to **Under policy**.
7. Click **Apply** and **OK**.

Adding Threat Response actions to the action list of the current policy

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To add Threat Response actions to the list of actions of the current policy:

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
    - Double-click the policy name.
    - Select **Properties** in the policy context menu.
    - Select the **Configure policy settings** item in the right part of the window.
4. In the **Kaspersky Sandbox integration** section select the **Threat response** subsection.
5. In the **Actions** group of settings, select the **Take response actions on threats, detected by Kaspersky Sandbox** check box, if it is not selected.
6. Click **Add** and in the drop-down list, select one of the following actions:
    - Quarantine and delete

When a threat is detected on a device, a copy of the object containing the threat is quarantined, and the object is deleted from the device.

- **Notify device user**

  When a threat is detected on a device, a notification about the detected threat is displayed to the device user.

  The notification is displayed if the device is running under the user account same to the account under which the threat was detected.

  If the device is not running or is running under another user account, the notification is not displayed.

- **Push Endpoint Protection Platform scanning on critical areas**

  If a threat is detected on a device, Kaspersky Endpoint Agent sends a command to EPP to scan critical areas of the device. Critical areas include kernel memory, objects loaded at operating system startup, and boot sectors of the hard drive. For more details on configuring the scan settings refer to the documentation of EPP being used.

- **Run IOC Scan on a managed group of devices**

  If a threat is detected on any device of the administration group for which you configure the policy, Kaspersky Endpoint Agent scans all devices of this administration group for objects containing the detected threat.

- **Quarantine and delete when IOC is found**

  If a threat is detected on any device of the administration group for which you configure the policy, Kaspersky Endpoint Agent scans all devices of this administration group for objects containing the detected threat. When an object which contains a threat is detected on devices of this administration group, a copy of the object containing the threat is quarantined, and the object is deleted from the device.

- **Push Endpoint Protection Platform scanning on critical areas when IOC is found**

  If a threat is detected on any device of the administration group for which you configure the policy, Kaspersky Endpoint Agent sends a command to EPP to scan critical areas on all administration group's devices where the object containing the threat was detected. For more details on configuring the scan settings refer to the documentation of EPP being used.

The action is added to the **Current actions** list.

When configuring threat response actions, keep in mind that as a result of some actions, the object containing the threat may be deleted from the workstation where it was detected.

7. To remove an action, select it in the table and click **Remove**.

8. In the upper right corner of the settings group, change the switch from **Unaffected by policy** to **Under policy**.

9. Click **Apply** and **OK**.

Configuring authentication on the Administration Server for Autonomous IOC Scan tasks

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

If you want Kaspersky Endpoint Agent to create Autonomous IOC Scan tasks when responding to threats, configure authentication on the Administration Server.

The application uses a special Administration Server user account, which has limited permissions and is intended only for creating Autonomous IOC Scan tasks.

The special account can only be created in the **Threat Response** window in Kaspersky Endpoint Agent policy properties or in the application properties of an individual device. The special account must be created on the Administration Server only once and its password must be used to configure **Threat Response** settings in the properties of other devices or other policies of the same Administration Server.

It is not possible to change the password of the special account created for Autonomous IOC Scan tasks. If you forget the password of this account, delete it using standard Kaspersky Security Center tools and create it again in the **Threat response** window.

To configure authentication on the Administration Server for Autonomous IOC Scan tasks:

1. Open Kaspersky Security Center Administration Console.

2. In the console tree, open the **Policies** folder.

3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:

   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.

4. In the **Kaspersky Sandbox integration** section select the **Threat response** subsection.

5. To check for availability of a special account for Autonomous IOC Scan tasks, or to create such account:

   a. In the **Authentication on Administration Server** group of settings, click the **Check for the user** button.

   The settings in the **Authentication on Administration Server** group are editable only if the **Run IOC Scan for a managed group of devices** option is selected in the **Selected actions** list.

   b. In the window that opens, in the **Connection to Administration Server** group of settings, enter the data for connecting to the Administration Server, as well as login and password of the Administration Server account having the permissions to create new users.

c. Click the **Connect and check for the user** button.

d. In the pop-up window, review the information on availability of a special account and close it.

e. If the account does not exist and you want to create it, in the **Password** field of the **Creating special user for Autonomous IOC Scan tasks** group of settings, specify a password with the length of 8–16 characters and click the **Create special user** button.

The **Creating special user for Autonomous IOC Scan tasks** group of settings becomes editable only after existence of a special account is checked.

f. Click **Exit** to close the **Administration Server user for Autonomous IOC Scan tasks** window.

6. In the **Administration Server password** field of the **Authentication on Administration Server** group of settings, enter the password for the special account created for the Autonomous IOC Scan tasks.

7. In the upper right corner of the settings group, change the switch from **Unaffected by policy** to **Under policy**.

8. Click **OK**.

Authentication on the Administration Server for Autonomous IOC Scan tasks is configured.

Device protection from legitimate applications that can be used by cybercriminals

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

You can enable detection of legitimate applications that can be used by cybercriminals to harm your organization local network. Kaspersky Endpoint Agent considers such applications as posing threats and performs threat response actions on them.

Legitimate applications are allowed to be installed and used on devices and are designed to perform user tasks. However, some types of legitimate applications, when used by cybercriminals, may harm devices or organization local network. If cybercriminals gain access to such applications or deploy them on devices, they can use functions of such applications to violate security of the devices or organization local network.

Such applications include IRC clients, dialers, file download applications, computer system activity monitors, password utilities, Internet servers for FTP, HTTP or Telnet services.

To enable detection of potentially harmful legitimate applications:

1. Open Kaspersky Security Center Administration Console.

2. In the console tree, open the **Policies** folder.

3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:

- Double-click the policy name.

- Select **Properties** in the policy context menu.

- Select the **Configure policy settings** item in the right part of the window.

4. In the **Kaspersky Sandbox integration** section select the **Threat response** subsection.
5. In the **Additional** group of settings select the **Enable detection of legitimate applications, which can be exploited by adversaries** check box.
6. In the upper right corner of the settings group, change the switch from **Unaffected by policy** to **Under policy**.
7. Click **Apply** and **OK**.

Detection of legitimate applications that can be used by cybercriminals to harm your organization local network is enabled.

Configuring start of Autonomous IOC Scan tasks

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

When Kaspersky Sandbox detects a threat, Kaspersky Endpoint Agent automatically creates IOC Scan tasks for all devices (search for MD5 hashes of objects in which the threat was detected).

To configure start of Autonomous IOC Scan tasks:

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.
4. In the **Kaspersky Sandbox integration** section select the **Threat response** subsection.
5. In the **Additional** group of settings click **Configure**.

   The **IOC Scan settings** window opens.
6. In the **Scanning area** group of settings, select one of the following areas where Kaspersky Endpoint Agent will search for IOCs:
   - **File areas, containing system drives**.
   - **Critical file areas**.
7. In the **Scan start** group of settings, select one of the following options to start IOC Scan tasks:

- **Manual start**. IOC Scan tasks will be created automatically, but will not be started. You can start a single task or all tasks manually.
- **Immediately on a Kaspersky Sandbox detect**. IOC Scan tasks will be automatically created and started.
- **Start within the specified period**. IOC Scan tasks will be created automatically, and will be started within the specified period. For example, outside of working hours from 8:00 p.m. to 7:00 a.m.

  If you select the **Start within the specified period** option, specify the start and end of the period in the **Period start time (hh:mm)** and **Period end time (hh:mm)** fields.

  All IOC Scan tasks that were automatically created *before the beginning* of the specified period will start at any time *within* the specified period.

  All IOC Scan tasks that were automatically created *within* the specified period will start immediately *after creation*.

  All IOC Scan tasks that were automatically created *after the end* of the specified period will start *during the next task execution period*.

  For example, if you configured the tasks to run during the period from 8:00 p.m. to 7:00 a.m.:

  - Tasks that were automatically created at 7 p.m. are started at any arbitrary time from 8:00 p.m. to 7:00 a.m.
  - Tasks that were automatically created at 9 p.m. are started at 9 p.m.
  - Tasks that were automatically created at 8:00 a.m. are started during the next task execution period, from 8:00 p.m. to 7:00 a.m.

8. Click **OK**.

   The **IOC Scan settings** window closes.

9. In the upper right corner of the settings group, change the switch from **Unaffected by policy** to **Under policy**.

10. Click **Apply** and **OK**.

Start of Autonomous IOC Scan tasks is configured.

Configuring integration between Kaspersky Endpoint Agent and KATA Central Node

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

This section contains information on how to configure integration between Kaspersky Endpoint Agent and the KATA Central Node component using Kaspersky Security Center Administration Console.

Enabling and disabling integration with KATA Central Node

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

If you use Nginx as a proxy server between a device with Kaspersky Endpoint Agent installed and KATA server, configure the `client_max_body_size` setting. The value of the `client_max_body_size` setting must be equal to the maximum size of the object sent by Kaspersky Endpoint Agent to KATA for processing. Otherwise, Nginx will not send the objects whose size exceeds the specified value. The default value is 1 MB.

To enable or disable integration with the KATA Central Node component:

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.
4. In the **KATA integration** section select the **KATA Central Node** subsection.
5. In the **Connection settings** group, enable or disable integration with KATA Central Node. If you enabled the integration, specify the IP address or the fully qualified domain name of the KATA server and the port used for connecting to the server.
6. In the **Connection settings** group, enable or disable the **Connect using the proxy server if specified in the general settings** option.

   This option is disabled by default. The application connects to the KATA server only directly and does not use the general proxy server connection settings. You can enable this option if you want the application to use the general proxy server connection settings when connecting to the KATA server.
7. In the upper right corner of the settings group, change the switch from **Unaffected by policy** to **Under policy**.
8. Click **OK**.

Integration with KATA Central Node is enabled or disabled.

Configuring trusted connection with KATA Central Node

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To configure trusted connection between Kaspersky Endpoint Agent and KATA Central Node, perform the following actions on Kaspersky Endpoint Agent side:

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.
4. In the **KATA integration** section select the **KATA Central Node** subsection.
5. In the **Connection settings** group of settings, select the **Use trusted connection** check box.
6. Click the **Add new TLS certificate** button.
   The **Adding new TLS certificate** window opens.
7. Perform one of the following actions to add a TLS certificate:
   - Add a certificate file. Click **Browse**, and in the window that opens, select the certificate file and click **Open**.
   - Copy and paste the contents of the certificate file to the **Paste TLS certificate data** field.

   Kaspersky Endpoint Agent may have only one KATA server TLS certificate. If you have added a TLS certificate before and then add a TLS certificate once again, only the last added certificate is valid.
8. Click **Add**.
   Information about the added TLS certificate is shown in the **TLS certificate data** group of settings.
9. If you want to configure additional connection protection by a user certificate, click the **Advanced connection protection** button.
10. In the **Advanced connection protection** window that opens, do the following:
    a. Select the **Secure connection with the client certificate** check box.
    b. Click the **Upload** button and in the window that opens select the PFX archive and click **Open**.
    c. Enter the password for the PFX archive.
    d. Click **OK**.
11. In the upper right corner of the settings group, change the switch from **Unaffected by policy** to **Under policy**.

12. Click **OK**.

Trusted connection to KATA server is configured.

Configuring synchronization settings between Kaspersky Endpoint Agent and KATA Central Node

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To configure synchronization settings between Kaspersky Endpoint Agent and KATA Central Node:

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.
4. In the **KATA integration** section select the **KATA Central Node** subsection.
5. In the **Connection settings** group of settings, configure the following settings:
   - **Timeout (sec.)**. Specify the maximum KATA server response timeout. The default value is 10 seconds.
   - **Send synchronization request to KATA server every (min.)**. Specify the time interval for sending requests for synchronization Kaspersky Endpoint Agent settings and tasks with KATA Central Node. You can specify a value from 1 to 60 minutes. The default value is 5 minutes.
   - Select or clear the **Consider TTL period when sending events** check box. The check box is cleared by default.

     If the check box is selected, Kaspersky Endpoint Agent does not send information about the processes that are started again to the KATA server. Kaspersky Endpoint Agent does not consider the launch of the process as repeated if the process is started after the end of the TTL period.
   - If you select the **Consider TTL period when sending events** check box, specify the time in the **TTL period (min.)** field. The default value is 1440 minutes.
6. In the upper right corner of the settings group, change the switch from **Unaffected by policy** to **Under policy**.
7. Click **OK**.

Configuring data submission settings

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To configure data submission settings:

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.
4. In the **KATA integration** section select the **General** subsection.
5. In the **Data submission settings** group, do the following:
   - Specify the value in the **Maximum event transmission time (sec.)** field.
     The default value is 30 seconds.
   - Specify the value in the **Maximum number of events in a package** field.
     The default value is 1024 events in a package.
6. In the upper right corner of the settings group, change the switch from **Unaffected by policy** to **Under policy**.
7. Click **OK**.

Configuring request throttling settings

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

The request throttling feature allows restricting the flow of events with low importance from Kaspersky Endpoint Agent to the Central Node component. Event importance is evaluated by the application.

To configure the request throttling settings:

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.
4. In the **KATA integration** section select the **General** subsection.
5. In the **Request throttling** group of settings, you can perform the following actions:
   - Enable or disable the **Enable request throttling** setting.

     The setting is enabled by default.
   - Specify the number of events in the **Maximum number of events per hour** field.

     The application analyzes telemetry data flow and restricts transmission of events with low importance if the number of transmitted events tends to exceed the value specified in this field. The default value is 3000 events per hour.
   - Specify the threshold for the flow of events of the same type with low importance in the **Percentage of event limit excess** field.

     If the flow of events of the same type with low importance exceeds the threshold value specified in this field as a percentage of the total number of events, transmission of events of this type is restricted. You can specify a value from 5% to 100%. The default value is 15%.
6. In the upper right corner of the settings group, change the switch from **Unaffected by policy** to **Under policy**.

   The default switch position is **Under policy**.
7. Click **OK**.

Configuring integration between Kaspersky Endpoint Agent and Kaspersky Industrial CyberSecurity for Networks

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

This section contains information on how to configure integration between Kaspersky Endpoint Agent and Kaspersky Industrial CyberSecurity for Networks using Kaspersky Security Center Administration Console.

Enabling integration with Kaspersky Industrial CyberSecurity for Networks

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To enable integration with Kaspersky Industrial CyberSecurity for Networks:

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.
4. In the **KATA integration** section select the **KICS for Networks** subsection.

   In the **Connection settings** group, enable or disable integration with Kaspersky Industrial CyberSecurity for Networks. If you enabled the integration, specify the IP address or the fully qualified domain name of the Kaspersky Industrial CyberSecurity for Networks server and the port used for connecting to the server.
5. In the **Connection settings** group, enable the **Connect using the proxy server if specified in the general settings** option.

   This option is disabled by default. The application connects to Kaspersky Industrial CyberSecurity for Networks server only directly and does not use the general proxy server connection settings. You can enable this option if you want the application to use the general proxy server connection settings when connecting to Kaspersky Industrial CyberSecurity for Networks server.
6. In the upper right corner of the settings group, change the switch from **Unaffected by policy** to **Under policy**.
7. Click **OK**.

Integration with Kaspersky Industrial CyberSecurity for Networks is enabled.

Configuring trusted connection with Kaspersky Industrial CyberSecurity for Networks

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To configure trusted connection between Kaspersky Endpoint Agent and Kaspersky Industrial CyberSecurity for Networks, perform the following actions on Kaspersky Endpoint Agent side:

1. Open Kaspersky Security Center Administration Console.

2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.
4. In the **KATA integration** section select the **KICS for Networks** subsection.
5. In the **Connection settings** group of settings, select the **Use trusted connection** check box.
6. Click the **Add new TLS certificate** button.
   The **Adding new TLS certificate** window opens.
7. Perform one of the following actions to add a TLS certificate:
   - Add a certificate file. Click **Browse**, and in the window that opens, select the certificate file and click **Open**.
   - Copy and paste the contents of the certificate file to the **Paste TLS certificate data** field.

   Kaspersky Endpoint Agent may have only one TLS certificate for the Kaspersky Industrial CyberSecurity for Networks server. If you have added a TLS certificate before and then add a TLS certificate once again, only the last added certificate is valid.
8. Click **Add**.
   Information about the added TLS certificate is shown in the **TLS certificate data** group of settings.
9. If you want to configure additional connection protection by a user certificate, click the **Advanced connection protection** button.
10. In the **Advanced connection protection** window that opens, do the following:
    a. Select the **Secure connection with the client certificate** check box.
    b. Click the **Upload** button and in the window that opens select the PFX archive and click **Open**.
    c. Enter the password for the PFX archive.
    d. Click **OK**.
11. In the upper right corner of the settings group, change the switch from **Unaffected by policy** to **Under policy**.
12. Click **OK**.

Trusted connection to Kaspersky Industrial CyberSecurity for Networks server is configured.

Configuring synchronization settings between Kaspersky Endpoint Agent and Kaspersky Industrial CyberSecurity for Networks

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To configure synchronization settings between Kaspersky Endpoint Agent and Kaspersky Industrial CyberSecurity for Networks:

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.
4. In the **KATA integration** section select the **KICS for Networks** subsection.
5. In the **Connection settings** group, specify the maximum response timeout for Kaspersky Industrial CyberSecurity for Networks server in the **Timeout (sec.)** field.

   The default value is 10 seconds.
6. In the upper right corner of the settings group, change the switch from **Unaffected by policy** to **Under policy**.
7. Click **OK**.

Synchronization settings between Kaspersky Endpoint Agent and Kaspersky Industrial CyberSecurity for Networks server are configured and applied.

Configuring data submission settings

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To configure data submission settings:

1. Open Kaspersky Security Center Administration Console.

2. In the console tree, open the **Policies** folder.

3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:

   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.

4. In the **KATA integration** section select the **General** subsection.

5. In the **Data submission settings** group, do the following:

   - Specify the value in the **Maximum event transmission time (sec.)** field.
     The default value is 30 seconds.
   - Specify the value in the **Maximum number of events in a package** field.
     The default value is 1024 events in a package.

6. In the upper right corner of the settings group, change the switch from **Unaffected by policy** to **Under policy**.

7. Click **OK**.

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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or 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*.

Integration with Kaspersky Managed Detection and Response is available only for Kaspersky Endpoint Agent Management plug-in 3.9.2 and later.

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

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.
4. Select the **Managed Detection and Response** section.
5. In the **Managed Detection and Response settings** group, do the following:
   a. Select the **Enable Managed Detection and Response** check box.
   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 identifier** field, enter an arbitrary value.
6. In the policy properties window, click **OK**.

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).

Configuring EDR telemetry settings

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

This section contains information on how to configure exclusions for EDR telemetry that Kaspersky Endpoint Agent processes and sends to the server with the KATA Central Node component.

Enabling and configuring EDR telemetry exclusions

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

You can configure EDR telemetry exclusions using the Administration Console both in the properties of an individual device and in the policy settings for a group of devices.

To enable and configure EDR telemetry exclusions:

1. Do one of the following:

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

1. In the **Managed devices** folder of the Administration Console tree, select the folder with the name of the administration group, which includes the required device.
2. In the workspace, select the **Devices** tab.
3. Select the device for which you want to configure Kaspersky Endpoint Agent settings.
4. Select **Properties** in the device context menu.

   The device properties window opens.
5. Select the **Applications** section.

   A list of Kaspersky applications installed on the device is displayed in the window.
6. Select Kaspersky Endpoint Agent and open its properties window in one of the following ways:
   - Double-click the application name.
   - In the application context menu, select **Properties**.
   - Click the **Properties** button under the list of Kaspersky applications.

- Open the policy properties window.

  1. Open Kaspersky Security Center Administration Console.
  2. In the console tree, open the **Policies** folder.
  3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
     - Double-click the policy name.
     - Select **Properties** in the policy context menu.
     - Select the **Configure policy settings** item in the right part of the window.

2. Select the **EDR telemetry** → **Exclusions** section.
3. To enable usage of EDR telemetry exclusions, enable the **Use exclusions** setting in the **Exclusions** section.
4. To add a new exclusion:

   a. Click the **Add** button.

   b. In the **Rule properties** window that opens, configure the following exclusion criteria:

   The criteria are applied using logical AND.

   To create a rule, specify the value in the **Path** field and select at least one event type in the **Use this exclusion for the following event types** list.

If the **Network events** option is selected for the **Use this exclusion for the following event types** criterion, specify the full path to the file in the **Path** field.

The object for which you create an exclusion must be available on the protected device at the time the exclusion settings are applied. For example, if you first configure exclusion for a specific application, and then install that application on the protected device, this exclusion will not be applied.

- In the **General data** section, specify the values in the following fields:
  - **Path**. Full path to the file, including its name and extension. You can use file masks (using the ? and * characters), as well as system environment variables.
  - **Command line**. Command line to run the object.
  - **Parent folder path**. The path to the folder where the file is located.
- In the **Version information** section, specify the values in the following fields:
  - **Description**. The value of the FileDescription parameter from the resource of the RT_VERSION type (VersionInfo).
  - **Original file name**. The value of the OriginalFilename parameter from the resource of the RT_VERSION type (VersionInfo).
  - **Version**. The value of the FileVersion parameter from the resource of the RT_VERSION type (VersionInfo).
- In the **File data** section, specify the values in the following fields:
  - **MD5**. MD5 hash of the file.
  - **SHA256**. SHA256 hash of the file.
- In the **Use this exclusion for the following event types** list, select at least one of the following options:
  - **File modification**.
  - **Network events**.
  - **Interactive input in the console**. This option is selected by default.
  - **Loading the process module**.
  - **Changes in the Registry**.

c. Click **OK** to save the changes and close the **Rule properties** window.

The new rule is created and displayed in the list of exclusions.

5. To remove a rule from the list of exclusions, select the rule and click **Remove**.
6. To open the properties window for an existing rule and to change the specified criteria, select the rule in the list of exclusions and click **Edit**.

7. If you are configuring the policy settings, make sure that the switch in the upper right corner of the group of settings is set to **Under policy**. It is the default position of the switch.

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

EDR telemetry exclusions will be used according to the configured rules.

Configuring storage settings in Kaspersky Endpoint Agent

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To configure the quarantine settings:

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.
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. For example, if 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. For example, if 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 **Unaffected by policy** to **Under policy**.

8. Click **Apply** button and then click **OK**.

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

Configuring data synchronization with the Administration Server

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

You can configure synchronization of data on quarantined objects on managed devices with Kaspersky Security Center Administration Server. Data synchronization is required to manage quarantine using Kaspersky Security Center.

To configure data synchronization with the Administration Server:

1. Open Kaspersky Security Center Administration Console.

2. In the console tree, open the **Policies** folder.

3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
    - Double-click the policy name.
    - Select **Properties** in the policy context menu.
    - Select the **Configure policy settings** item in the right part of the window.
4. In the **Repositories** section select the **Synchronization with the Administration Server** subsection.
5. In the **Settings** section in the **Send the following data to Administration Server** subsection, select the **Data about objects, quarantined on managed devices** check box.
6. In the upper right corner of the settings group, change the switch from **Unaffected by policy** to **Under policy**.
7. Click **Apply** button and then click **OK**.

Data synchronization with the Administration Server is configured.

Configuring failure diagnosis

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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 failure diagnosis:

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

1. In the **Managed devices** folder of the Administration Console tree, select the folder with the name of the administration group, which includes the required device.
2. In the workspace, select the **Devices** tab.
3. Select the device for which you want to configure Kaspersky Endpoint Agent settings.
4. Select **Properties** in the device context menu.

   The device properties window opens.
5. Select the **Applications** section.

   A list of Kaspersky applications installed on the device is displayed in the window.
6. Select Kaspersky Endpoint Agent and open its properties window in one of the following ways:
   - Double-click the application name.
   - In the application context menu, select **Properties**.
   - Click the **Properties** button under the list of Kaspersky applications.

2. In the **Application settings** section select the **Failure diagnosis** subsection.
3. To enable logging of debug information to the trace files:
   a. Enable the **Write debug information to trace files** option.
   b. In the **Trace files folder** field, specify the path to the folder on the device where the application saves the trace files.

      Make sure that the specified folder is available on the managed device. Otherwise, the debug information will not be saved.

   c. In the **Maximum trace file size** field, specify the file size in megabytes.

      The default value is 50 MB. When the specified file size is reached, the application continues writing to a new file.
4. If you want the application to overwrite old trace files:
   a. Enable the **Overwrite old trace files** option.
   b. Enter the desired value in the **Maximum number of files per trace log** field.

      The default value is 1 file. When the specified number of files is reached, the application overwrites old files, starting with the oldest one. The specified limit is applied separately for each Kaspersky Endpoint Agent process being debugged, so the total number of files for all processes may exceed the specified value.
5. To enable logging of dump files:
   a. Enable the **Create dump files** option.

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

> Make sure that the specified folder is available on the managed device. Otherwise, the debug information will not be saved.

6. Click **OK**.

Failure diagnostics is configured and enabled for all Kaspersky Endpoint Agent processes that are currently running. Failure diagnostics files will be generated in the folders you specified.

Managing Kaspersky Endpoint Agent tasks

This section describes how to manage Kaspersky Endpoint Agent tasks.

Creating a local task

Local tasks are run on a specific device. For more information on tasks, refer to Kaspersky Security Center documentation.

To create a local task:

1. Open Kaspersky Security Center Administration Console.
2. In Kaspersky Security Center Administration Console tree, open the **Managed devices** folder.
3. In the **Managed devices** folder, select the folder with the name of the administration group, which includes the required device.
4. In the workspace, select the **Devices** tab.
5. Select the device for which you want to create a local task.
6. Do one of the following:
   - In the context menu of the device, select **All tasks** → **Create a task**.
   - In the context menu of the device, select **Properties** and in the **Properties: <Device name>** window that opens on the **Tasks** tab, click **Add**.
   - In the **Perform action** drop-down list, select the **Create a task** item.

   The task creation wizard starts.
7. Select the required task and click **Next**.
8. Follow the instructions of the task creation wizard.

Creating a group task

Group tasks are performed on the devices of the selected administration group. For more information on tasks, refer to Kaspersky Security Center documentation.

To create a group task:

1. Open Kaspersky Security Center Administration Console.
2. Do one of the following:
   - In the Administration Console tree, select the **Managed devices** folder to create a group task for all devices managed using Kaspersky Security Center.
   - In the **Managed devices** folder of the Administration Console tree, select the folder with the name of the administration group, which includes the required devices.
3. In the workspace, select the **Tasks** tab.
4. Click **Create a task**.
   The task creation wizard starts.
5. Select the required task and click **Next**.
6. Follow the instructions of the task creation wizard.

Viewing the table of tasks

To view the list of tasks on Kaspersky Security Center server:

1. Open Kaspersky Security Center Administration Console.
2. In Kaspersky Security Center Administration Console tree, open the **Tasks** folder.

A list of tasks appears.

Deleting a task from the list

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

1. Open Kaspersky Security Center Administration Console.
2. In Kaspersky Security Center Administration Console tree, open the **Tasks** folder.
3. In the task list, select the tasks that you want to delete and right-click them to open the context menu.
   A list of actions that you can perform on the tasks is displayed.

4. Select the **Delete** action.

   The action confirmation window opens.

5. Click **Yes**.

Selected tasks are deleted from the list.

Starting tasks manually

You can start the created tasks manually. For example, you can manually start the tasks for which scheduled start is not configured.

To start a single task manually:

1. Open Kaspersky Security Center Administration Console.
2. In Kaspersky Security Center Administration Console tree, open the **Tasks** folder.

   A list of tasks appears.

3. In the context menu of the desired task, select the **Run** action.

The task will run.

Starting tasks by schedule

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To configure the scheduled task start:

1. In the **Task schedule** section, select the **Run by schedule** check box.
2. In the **Frequency** list select one of the following options to run the tasks: **At specified time**, **Every hour**, **Every day**, **Every week**, **On application launch** or **After the application database update**.
3. If you select the **At specified time** option, specify the day and time to start the task in the **Run by schedule** section.
4. If you select one of the following options: **Every hour**, **Every day** or **Every week**, configure the following settings in the **Run by schedule** section:

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

   b. In the **Time** and **Date** lists, select the date and time from which the schedule applies.

5. To configure advanced schedule settings, click the **Advanced** button and configure the following settings in the **Advanced** window:

   - **Quit task, running longer than**

     Enable this setting if you want to set the task execution timeout. After the specified time, the task will automatically finish.

   - **Cancel schedule from**

     Enable this setting if you want to specify the schedule expiration date. After the specified date, the schedule will expire.

   - **Run missed tasks**

     Enable this option if you want the application to start the tasks that were not completed on time as soon as possible.

   - **Randomize the task run to every**

     Enable this option if you want to avoid simultaneous access of a large number of workstations to the Administration Server as well as to run the task on workstations not precisely according to the schedule, but randomly within the specified time interval.

6. Click **OK**.

Scheduled task start is configured and applied on the devices.

Viewing task execution results

You can view the task execution results during their storage period. You can also change the storage period for the task execution results.

It is not recommended to shorten the storage period for IOC Scan task execution results.

To view the task execution results:

1. Open Kaspersky Security Center Administration Console.
2. In Kaspersky Security Center Administration Console tree, open the **Tasks** folder.

   A list of tasks appears.
3. Select the task in the list and right-click it to open the task actions menu.
4. Select the **Results** menu item.

The **Task execution results** window opens.

Configuring the storage time for the task execution results on the Administration Server

By default, task execution results are stored on the Administration Server for seven days.

To configure storage time for the task execution results on the Administration Server:

1. Open Kaspersky Security Center Administration Console.
2. In Kaspersky Security Center Administration Console tree, open the **Tasks** folder.

   A list of tasks appears.
3. Select the task in the list and right-click it to open the task actions menu.
4. Select the **Properties** menu item.

   The task properties window opens.
5. In the left part of the window, select the **Notification** section.
6. Make sure, that the **On the Administration Server for (days)** check box is selected in the **Save information about results** section and specify for how many days you want to store the task execution results.
7. Click **Apply** button and then click **OK**.

It is not recommended to shorten the storage period for IOC Scan task execution results.

Creating Kaspersky Endpoint Agent activation task

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

You can activate Kaspersky Endpoint Agent using a key or activation code.

When activating the application using an activation code, data is sent to the activation server to verify the entered code.

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

To create Kaspersky Endpoint Agent activation task:

1. Run the **Application activation** task creation wizard for the desired scope in one of the following ways:

- Start the local task creation wizard.

  Local tasks are run on a specific device. For more information on tasks, refer to Kaspersky Security Center documentation.

  To create a local task:

  1. Open Kaspersky Security Center Administration Console.
  2. In Kaspersky Security Center Administration Console tree, open the **Managed devices** folder.
  3. In the **Managed devices** folder, select the folder with the name of the administration group, which includes the required device.
  4. In the workspace, select the **Devices** tab.
  5. Select the device for which you want to create a local task.
  6. Do one of the following:

     - In the context menu of the device, select **All tasks** → **Create a task**.
     - In the context menu of the device, select **Properties** and in the **Properties: <Device name>** window that opens on the **Tasks** tab, click **Add**.
     - In the **Perform action** drop-down list, select the **Create a task** item.

     The task creation wizard starts.
  7. Select the required task and click **Next**.
  8. Follow the instructions of the task creation wizard.

- Start the group task creation wizard.

Group tasks are performed on the devices of the selected administration group. For more information on tasks, refer to Kaspersky Security Center documentation.

To create a group task:

1. Open Kaspersky Security Center Administration Console.
2. Do one of the following:
   - In the Administration Console tree, select the **Managed devices** folder to create a group task for all devices managed using Kaspersky Security Center.
   - In the **Managed devices** folder of the Administration Console tree, select the folder with the name of the administration group, which includes the required devices.
3. In the workspace, select the **Tasks** tab.
4. Click **Create a task**.

   The task creation wizard starts.
5. Select the required task and click **Next**.
6. Follow the instructions of the task creation wizard.

2. If you want to activate the application using an activation code, perform the following actions in the **Activation settings** window:
   a. Select the **Activate with an activation code** option and click **Select**.
   b. In the window that opens, enter the activation code and click **OK**.
3. If you want to activate the application using a key file or a key from Kaspersky Security Center key storage, perform the following actions in the **Activation settings** window:
   a. Select the **Activate with a key file or key** option and click **Select**.
   b. In the drop-down list, select the key distribution method.
   c. If you select the **Key file from folder** option, in the window that opens, specify the location of the key file and click **Open**.
   d. If you select the **Key from Kaspersky Security Center storage** option, in the window that opens, select the key and click **OK**.

   For detailed information on Kaspersky Security Center key storage, refer to Kaspersky Security Center documentation.
4. If you want to add this license key as an additional one to automatically renew the license, select the **Use as additional key** check box.
5. Click **Next**.
6. In the **Schedule** window, configure the task schedule settings and click **Next**.

   For detailed information on configuring the settings in this window, refer to Kaspersky Security Center documentation.

7. In the **Selecting an account to run a task** window, specify the account to be used to run the task, and click **Next**.

   For detailed information on configuring the settings in this window, refer to Kaspersky Security Center documentation.

8. In the **Define the task name** window, enter the name of the task and click **Next**.

9. If you want to run the task immediately after creation, select the **Run task after wizard finishes** check box.

10. Click **Finish**.

    The application activation task is created for the selected device or device group.

Managing Kaspersky Endpoint Agent database and module update tasks

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

This section provides instructions on how to create and configure the Database and application module update task.

Creating Database and application module update task

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To create the Database and application module update task for Kaspersky Endpoint Agent in Kaspersky Security Center:

1. Open Kaspersky Security Center Administration Console.

2. In Kaspersky Security Center Administration Console tree, open the **Tasks** folder.

3. Click **Create a task**.

   The task creation wizard starts.

4. Select **Kaspersky Endpoint Agent** application to create the task, and the **Database and application module update** task type.

5. Click **Next**.

   The Database Update task creation wizard starts.

The Database Update task creation wizard consists of the following steps:

1. Selecting a database update source

Do the following:

1. In the **Database update source** section, select one of the following database update sources:
   - **Kaspersky Security Center Administration Server**.
   - **Kaspersky update servers**.
   - **Custom HTTP or FTP servers or network folders**.
2. If required, select the **Use Kaspersky update servers if specified servers are not available** check box.
3. If you select **Kaspersky update servers** as database update source and want to use a proxy-server to connect to it, select the **Use proxy server settings to connect to Kaspersky update servers** check box in the **Update source connection settings** section.
4. If you select **Custom HTTP or FTP servers or network folders** as database update source, do the following:
   a. Click the **Custom HTTP or FTP servers or network folders** link.
   b. Add update servers to the list:
      1. Click **Update servers**.
      2. In the new line, enter the address of the update server (HTTP or FTP), or the path to the network or local folder containing the update files.
      3. If you want to use this server to update databases, select the check box next to its address. You can also add servers to the list and clear the check boxes next to the addresses of the servers that you do not want to use now, but plan to use later.

         Perform the same steps to add each server.

      4. Click **OK**.
      5. The **Update servers** window closes.
   c. To use a proxy server to connect to update servers, select the **Use proxy server settings to connect to other servers** check box in the **Update source connection settings** section.

2. Configuring the application modules update settings

Do the following:

1. 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.

2. 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.

3. Configuring database update schedule

Do the following:

1. In the **Task schedule** section, select the **Run by schedule** check box.
2. In the **Frequency** list select one of the following options to run the tasks: **At specified time**, **Every hour**, **Every day**, **Every week**, **On application launch** or **After the application database update**.
3. If you select the **At specified time** option, specify the day and time to start the task in the **Run by schedule** section.
4. If you select one of the following options: **Every hour**, **Every day** or **Every week**, configure the following settings in the **Run by schedule** section:
   a. In the **Every** list, select the task run frequency. For example, once a day or twice a week on Tuesdays and Thursdays.
   b. In the **Time** and **Date** lists, select the date and time from which the schedule applies.
5. To configure advanced schedule settings, click the **Advanced** button and perform the following actions in the **Advanced** window:
   a. If you want to set maximum timeout for the task execution, select the **Quit task, running 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 Database Update 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 workstations 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 run to every** check box and specify the start interval in minutes.
   e. Click **OK**.

4. Selecting devices on which the task will be performed

   In the device selection window that opens, select devices to which you want to assign the task and click **Next**.

   For example, you can select the **Assign task to an administration group** option and select an administration group from the list.

5. Selecting Kaspersky Security Center user account which is used to run the task

In the **Selecting an account to run the task** window, do one of the following:

- Select the default account and click **Next**.
- Enter the user name and password to be used to start the task and click **Next**.

6. Defining the task name

   In the **Define the task name** window, enter the task name in the **Name** field, and click **Next**.

7. Running the task immediately after it is created

   If you want the task to start immediately after creation, select the **Run task after wizard finishes** check box and click **Finish**.

Configuring Database and application module update task

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

After creating the Database and application module update task, you can configure the settings for this task.

To configure the task settings:

1. Open Kaspersky Security Center Administration Console.
2. In Kaspersky Security Center Administration Console tree, open the **Tasks** folder.

   A list of tasks appears.
3. In the **Database and application module update** section, select the task in the list and right-click it to open the task action menu.
4. Select the **Properties** menu item.

   The task properties window opens.
5. In the left part of the window, select the group of settings that you want to configure.
6. In the right part of the window, make the necessary modifications and click **Apply** and **OK**.

You can configure the following task settings:

- Task name

Do the following:

1. Select the **General** section.
2. Change the task name in the top line.

- **Devices on which the task will be performed**

  The right part of the window displays current devices to which the task is assigned. Perform the following actions to add devices:

  1. Click the **Add** button.

     A window opens with a list of managed devices.

  2. Select the check boxes next to devices you want to add.
  3. If you want to add devices that are not in the list, click **Add** in the right part of the window and follow the steps to add devices.

     For example, you can specify device addresses manually or import them from the list.

     You can specify NetBIOS names, DNS names, IP addresses and IP address ranges of the devices to which you want to assign a task.

  For details on working with managed devices, refer to *Kaspersky Security Center Help*.

- **Database update source**

Do the following:

1. In the **Database update source** section, select one of the following database update sources:
   - **Kaspersky Security Center Administration Server**.
   - **Kaspersky update servers**.
   - **Custom HTTP or FTP servers or network folders**.
2. If required, select the **Use Kaspersky update servers if specified servers are not available** check box.
3. If you select **Kaspersky update servers** as database update source and want to use a proxy-server to connect to it, select the **Use proxy server settings to connect to Kaspersky update servers** check box in the **Update source connection settings** section.
4. If you select **Custom HTTP or FTP servers or network folders** as database update source, do the following:
   a. Click the **Custom HTTP or FTP servers or network folders** link.
   b. Add update servers to the list:
      1. Click **Update servers**.
      2. In the new line, enter the address of the update server (HTTP or FTP), or the path to the network or local folder containing the update files.
      3. If you want to use this server to update databases, select the check box next to its address. You can also add servers to the list and clear the check boxes next to the addresses of the servers that you do not want to use now, but plan to use later.

         Perform the same steps to add each server.

      4. Click **OK**.
      5. The **Update servers** window closes.
   c. To use a proxy server to connect to update servers, select the **Use proxy server settings to connect to other servers** check box in the **Update source connection settings** section.

- Configuring additional database update settings

Do the following:

1. 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.

2. 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.

- Database update schedule

Do the following:

1. In the **Task schedule** section, select the **Run by schedule** check box.
2. In the **Frequency** list select one of the following options to run the tasks: **At specified time**, **Every hour**, **Every day**, **Every week**, **On application launch** or **After the application database update**.
3. If you select the **At specified time** option, specify the day and time to start the task in the **Run by schedule** section.
4. If you select one of the following options: **Every hour**, **Every day** or **Every week**, configure the following settings in the **Run by schedule** section:
   a. In the **Every** list, select the task run frequency. For example, once a day or twice a week on Tuesdays and Thursdays.
   b. In the **Time** and **Date** lists, select the date and time from which the schedule applies.
5. To configure advanced schedule settings, click the **Advanced** button and perform the following actions in the **Advanced** window:
   a. If you want to set maximum timeout for the task execution, select the **Quit task, running 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 Database Update 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 workstations 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 run to every** check box and specify the start interval in minutes.
   e. Click **OK**.

- Kaspersky Security Center user account which is used to run the task

  In the **Selecting an account to run the task** window, do one of the following:

  - Select the default account and click **Next**.
  - Enter the user name and password to be used to start the task.

- Storage time for the task execution results on the Administration Server

Do the following:

1. Select the **Notification** section.
2. Make sure, that the **On the Administration Server for (days)** check box is selected in the **Save information about results** section, and specify for how many days you want to store the task execution results.

   By default, task execution results are stored on the Administration Server for 7 days.

Managing IOC Scan tasks in Kaspersky Endpoint Agent

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

This section describes how to manage IOC Scan tasks in Kaspersky Endpoint Agent using Kaspersky Endpoint Agent Management plug-in.

Managing Standard IOC Scan tasks

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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.

Only the files with IOC rules can be specified for the IOC Scan task. Files with other types of rules are not supported for the IOC Scan task.

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

Requirements for IOC files

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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.
- Only the files with IOC rules can be specified for the IOC Scan task. Files with other types of rules are not supported for the IOC Scan task.
- 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.

The table below shows the features and limitations of the OpenIOC standard supported by the application.

Features and limitations of the OpenIOC standard versions 1.0 and 1.1

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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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

Creating and configuring Standard IOC Scan task

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

Only the files with IOC rules can be specified for the IOC Scan task. Files with other types of rules are not supported for the IOC Scan task.

To create and configure a Standard IOC Scan task,

depending on the required task scope, perform one of the following actions:

- Start the local task creation wizard.

  Local tasks are run on a specific device. For more information on tasks, refer to Kaspersky Security Center documentation.

  To create a local task:

  1. Open Kaspersky Security Center Administration Console.
  2. In Kaspersky Security Center Administration Console tree, open the **Managed devices** folder.
  3. In the **Managed devices** folder, select the folder with the name of the administration group, which includes the required device.
  4. In the workspace, select the **Devices** tab.
  5. Select the device for which you want to create a local task.
  6. Do one of the following:
     - In the context menu of the device, select **All tasks** → **Create a task**.
     - In the context menu of the device, select **Properties** and in the **Properties: <Device name>** window that opens on the **Tasks** tab, click **Add**.
     - In the **Perform action** drop-down list, select the **Create a task** item.

     The task creation wizard starts.
  7. Select the required task and click **Next**.
  8. Follow the instructions of the task creation wizard.

- Start the group task creation wizard.

Group tasks are performed on the devices of the selected administration group. For more information on tasks, refer to Kaspersky Security Center documentation.

To create a group task:

1. Open Kaspersky Security Center Administration Console.
2. Do one of the following:
   - In the Administration Console tree, select the **Managed devices** folder to create a group task for all devices managed using Kaspersky Security Center.
   - In the **Managed devices** folder of the Administration Console tree, select the folder with the name of the administration group, which includes the required devices.
3. In the workspace, select the **Tasks** tab.
4. Click **Create a task**.

   The task creation wizard starts.
5. Select the required task and click **Next**.
6. Follow the instructions of the task creation wizard.

The task creation wizard allows you to configure the following settings:

- IOC collection

To configure IOC collection:

1. In the **IOC collection** group of settings click **Browse**.
2. In the context menu, do one of the following:
   - Select the **Select folder** item to add a group of IOC files to the IOC collection.
   - Select the **Select file** item to add one IOC file to the IOC collection.
3. Depending on your choice, do one of the following in the window that opens:
   - Specify the path to the folder with IOC files and click **OK**.
   - Specify the path to IOC file and click **Open**.

   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.
4. To view the list of all IOC files that are included in the IOC collection, as well as to get information about each IOC file, click **View**.

   The **IOC collection settings** window opens. In this window, you can exclude any file from the database by clearing the check box next to the name of the IOC file.
5. Click **OK** to save the changes and close the **IOC collection settings** window.
6. To export the created IOC collection, click **Export**.

   In the window that opens, specify the name of the file and select the folder where you want to save it.
7. Click the **Save** button.

   The application creates a ZIP file in the specified folder.

- Data types (IOC documents) to be analyzed during IOC scan

To select data types (IOC documents) that you want to analyze during IOC scan and configure the additional scan settings:

1. Click the **Configure IOC terms and documents** button.

   The **IOC terms and documents** window opens.

2. 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.

3. To configure additional settings for the selected ProcessItem IOC document:

   a. Click the **Advanced (ProcessItem)** button.

      The **ProcessItem document scan settings** window opens.

   b. In the **Indicators** group of settings, select data that you want to analyze during the task execution.

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

4. To configure additional settings for the selected FileItem IOC document:

   a. Click the **Advanced (FileItem)** button.

      The **FileItem document scan settings** window opens.

   b. On the **Indicators** tab, select data that you want to analyze during the task execution.

   c. On the **Scan areas** tab, select the areas on protected device drives where to look for indicators of compromise.

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

   d. On the **Exclusions** tab, select the **Apply exclusions** check box and specify the paths to the areas on the protected device drives that do not need to be scanned during the task execution.

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

5. To configure additional settings for the selected RegistryItem IOC document:

   a. Click the **Advanced (RegistryItem)** button.

      The **RegistryItem document scan settings** window opens.

   b. Specify the Windows registry keys to be scanned during the task execution.

      You can select to scan predefined registry keys or specify the list of required registry keys manually.

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

6. To configure additional settings for the selected EventLogItem IOC document:

   a. Click the **Advanced (EventLogItem)** button.

The **EventLogItem document scan settings** window opens.

b. To ignore the events that were logged before the specified moment, select the **List only events logged during the specified period** check box and specify date and time.

c. If necessary, in the bottom of the window, edit the predefined list of channels that are analyzed during the task execution.

d. Click **OK** to save the changes and close the **EventLogItem document scan settings** window.

7. Click **OK** to save the changes and close the window.

The saved settings will be applied when the task is executed.

- Retrospective IOC scan

Retrospective IOC scan is an operation mode of the IOC Scan task, when Kaspersky Endpoint Agent searches for indicators of compromise based on the data received during a time interval specified by the user. This mode is intended for searching for indicators of compromise based on the data on network activity of protected devices. Kaspersky Endpoint Agent analyzes data in the operating system logs and in browsers on devices.

The **Retrospective IOC scan** mode is available only for Standard IOC Scan tasks.

To enable the Retrospective IOC scan mode:

1. In the **Retrospective IOC Scan** group of settings enable the **Perform Retrospective IOC Scan within the interval** option.

2. Specify the time interval.

   During the task execution, the application analyzes data collected during the specified time interval, including the boundaries of the specified interval (from 00:00 on the start date until 23:59 on the end date). The default interval starts at 00:00 on the day preceding the task creation day and ends at 23:59 on the day when the task was created.

If during execution of the IOC Scan task with the **Perform Retrospective IOC Scan within the interval** option enabled the application does not find any data for the specified time interval to be analyzed, it does not inform about this. In this case, the application shows no indicators of compromise in the task completion report.

- Application actions on IOC detection

To configure Kaspersky Endpoint Agent actions on IOC detection:

1. In the **Actions** section, select the **Take actions when indicator of compromise is found** check box.
2. 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.
3. Select the **Send a command to Endpoint Protection Platform to scan the critical areas** 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.

When configuring the task settings in Kaspersky Security Center Administration Console, the **Do not perform actions on critical system files** check box is available only if the **Quarantine and delete** response action is selected for the task (this setting can be configured only in Kaspersky Security Center Web Console).

- **Task start schedule**

To configure the schedule settings for IOC Scan task:

1. In the **Task schedule** section, select the **Run by schedule** check box.
2. In the **Frequency** list select one of the following options to run IOC Scan tasks: **At specified time**, **Every hour**, **Every day**, **Every week** or **On application launch**.
3. If you select the **At specified time** option, specify the day and time to start the task in the **Run by schedule** section.
4. If you select one of the following options: **Every hour**, **Every day** or **Every week**, configure the following settings in the **Run by schedule** section:
   a. In the **Every** list, select the task run frequency. For example, once a day or twice a week on Tuesdays and Thursdays.
   b. In the **Time** and **Date** lists, select the date and time from which the schedule applies.
5. To configure advanced schedule settings, click the **Advanced** button and perform the following actions in the **Advanced** window:
   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 IOC Scan 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 workstations 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 run to every** check box and specify the start interval in minutes.
   e. Click **OK**.

- Kaspersky Security Center user account to run the task

To select Kaspersky Security Center user account, under which you want to run the task,

perform one of the following actions in the group of settings for selecting account to start the task:

- Select the default account and click **Next**.
- Enter the name and password of the user, whose account permissions will be used to start the task.

- Task name

The task name cannot be longer than 100 characters long and cannot contain special characters ("* <>? \: |).

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.

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.

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.

Configuring Standard IOC Scan task

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

Only the files with IOC rules can be specified for the IOC Scan task. Files with other types of rules are not supported for the IOC Scan task.

To configure the Standard IOC Scan task settings:

1. Open Kaspersky Security Center Administration Console.
2. In Kaspersky Security Center Administration Console tree, open the **Tasks** folder.

   The list of tasks is displayed in the workspace.
3. Open the settings of the required task in one of the following ways:

   - Double-click the task name.
   - Open the policy context menu and select **Properties**.
   - Select a task and click **Configure task** in the right part of the window.

   The **Properties: <Task name>** window opens.
4. In the left part of the window, select the group of settings that you want to configure.
5. In the right part of the window, make the necessary changes and click **Apply** and then click **OK**.

   Configuration of the Standard IOC Scan task settings is finished.

You can configure the following task settings:

- Task name

  Do the following:

  1. Select the **General** section.
  2. Change the task name in the top line.

- Storage time for the task execution results on the Administration Server

  Do the following:

  1. Select the **Notification** section.
  2. Make sure, that the **On the Administration Server for (days)** check box is selected in the **Save information about results** section, and specify for how many days you want to store the task execution results.

     By default, task execution results are stored on the Administration Server for 7 days.

- IOC collection

To configure IOC collection:

1. In the **IOC collection** group of settings click **Browse**.
2. In the context menu, do one of the following:
   - Select the **Select folder** item to add a group of IOC files to the IOC collection.
   - Select the **Select file** item to add one IOC file to the IOC collection.
3. Depending on your choice, do one of the following in the window that opens:
   - Specify the path to the folder with IOC files and click **OK**.
   - Specify the path to IOC file and click **Open**.

   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.
4. To view the list of all IOC files that are included in the IOC collection, as well as to get information about each IOC file, click **View**.

   The **IOC collection settings** window opens. In this window, you can exclude any file from the database by clearing the check box next to the name of the IOC file.
5. Click **OK** to save the changes and close the **IOC collection settings** window.
6. To export the created IOC collection, click **Export**.

   In the window that opens, specify the name of the file and select the folder where you want to save it.
7. Click the **Save** button.

   The application creates a ZIP file in the specified folder.

- Retrospective IOC scan

Retrospective IOC scan is an operation mode of the IOC Scan task, when Kaspersky Endpoint Agent searches for indicators of compromise based on the data received during a time interval specified by the user. This mode is intended for searching for indicators of compromise based on the data on network activity of protected devices. Kaspersky Endpoint Agent analyzes data in the operating system logs and in browsers on devices.

The **Retrospective IOC scan** mode is available only for Standard IOC Scan tasks.

To enable the Retrospective IOC scan mode:

1. In the **Retrospective IOC Scan** group of settings enable the **Perform Retrospective IOC Scan within the interval** option.
2. Specify the time interval.

   During the task execution, the application analyzes data collected during the specified time interval, including the boundaries of the specified interval (from 00:00 on the start date until 23:59 on the end date). The default interval starts at 00:00 on the day preceding the task creation day and ends at 23:59 on the day when the task was created.

If during execution of the IOC Scan task with the **Perform Retrospective IOC Scan within the interval** option enabled the application does not find any data for the specified time interval to be analyzed, it does not inform about this. In this case, the application shows no indicators of compromise in the task completion report.

- Application actions on IOC detection

To configure Kaspersky Endpoint Agent actions on IOC detection:

1. In the **Actions** section, select the **Take actions when indicator of compromise is found** check box.
2. 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.
3. Select the **Send a command to Endpoint Protection Platform to scan the critical areas** 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.

When configuring the task settings in Kaspersky Security Center Administration Console, the **Do not perform actions on critical system files** check box is available only if the **Quarantine and delete** response action is selected for the task (this setting can be configured only in Kaspersky Security Center Web Console).

- Data types (IOC documents) to be analyzed during IOC scan

To select data types (IOC documents) that you want to analyze during IOC scan and configure the additional scan settings:

1. Open the **Advanced** section.
2. 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.

3. To configure additional settings for the selected ProcessItem IOC document:
   a. Click the **Advanced (ProcessItem)** button.

      The **ProcessItem document scan settings** window opens.

   b. In the **Indicators** group of settings, select data that you want to analyze during the task execution.

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

4. To configure additional settings for the selected FileItem IOC document:
   a. Click the **Advanced (FileItem)** button.

      The **FileItem document scan settings** window opens.

   b. On the **Indicators** tab, select data that you want to analyze during the task execution.

   c. On the **Scan areas** tab, select the areas on protected device drives where to look for indicators of compromise.

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

   d. On the **Exclusions** tab, select the **Apply exclusions** check box and specify the paths to the areas on the protected device drives that do not need to be scanned during the task execution.

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

5. To configure additional settings for the selected RegistryItem IOC document:
   a. Click the **Advanced (RegistryItem)** button.

      The **RegistryItem document scan settings** window opens.

   b. Specify the Windows registry keys to be scanned during the task execution.

      You can select to scan predefined registry keys or specify the list of required registry keys manually.

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

6. To configure additional settings for the selected EventLogItem IOC document:
   a. Click the **Advanced (EventLogItem)** button.

      The **EventLogItem document scan settings** window opens.

b. To ignore the events that were logged before the specified moment, select the **List only events logged during the specified period** check box and specify date and time.

c. If necessary, in the bottom of the window, edit the predefined list of channels that are analyzed during the task execution.

d. Click **OK** to save the changes and close the **EventLogItem document scan settings** window.

7. Click **OK** to save the changes and close the window.

The saved settings will be applied when the task is executed.

- IOC Scan task schedule

To configure the schedule settings for IOC Scan task:

1. In the **Task schedule** section, select the **Run by schedule** check box.
2. In the **Frequency** list select one of the following options to run IOC Scan tasks: **At specified time**, **Every hour**, **Every day**, **Every week** or **On application launch**.
3. If you select the **At specified time** option, specify the day and time to start the task in the **Run by schedule** section.
4. If you select one of the following options: **Every hour**, **Every day** or **Every week**, configure the following settings in the **Run by schedule** section:

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

   b. In the **Time** and **Date** lists, select the date and time from which the schedule applies.

5. To configure advanced schedule settings, click the **Advanced** button and perform the following actions in the **Advanced** window:

   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 IOC Scan 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 workstations 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 run to every** check box and specify the start interval in minutes.

   e. Click **OK**.

- Kaspersky Security Center user account to run the task

To select Kaspersky Security Center user account, under which you want to run the task,

perform one of the following actions in the group of settings for selecting account to start the task:

- Select the default account and click **Next**.
- Enter the name and password of the user, whose account permissions will be used to start the task.

- Excluding groups of devices from the task scope

To exclude groups of devices from the task scope, in the **Exclusions from task scope** section, select the groups of devices to which the task will not be applied.

Only the subgroups of the administration group to which the task applies can be excluded.

IOC collection export

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To export an IOC collection:

1. Open Kaspersky Security Center Administration Console.
2. In Kaspersky Security Center Administration Console tree, open the **Tasks** folder.
   A list of tasks appears.
3. In the **Run IOC Scan** section, select the task in the list and right-click it to open the task action menu.
4. Select the **Properties** menu item.
   The task properties window opens.
5. Select the **IOC Scan settings** section.
6. In the **IOC collection** section click **Export**.
7. In the window that opens, specify the name of the file and select the folder where you want to save it.
8. Click the **Save** button.
   The application creates a ZIP file in the folder you specified.

Viewing IOC Scan task execution results

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To view the IOC Scan task execution results:

1. Open Kaspersky Security Center Administration Console.
2. In Kaspersky Security Center Administration Console tree, open the **Tasks** folder.
   The list of tasks is displayed in the workspace.
3. Open the settings of the required task in one of the following ways:
   - Double-click the task name.
   - Open the policy context menu and select **Properties**.
   - Select a task and click **Configure task** in the right part of the window.

   The **Properties: <Task name>** window opens.
4. Select the **Results** section.
5. In the **Show task results for the device** list, select the devices for which you want to view the results of IOC Scan tasks.
6. To view detailed information about a particular task, double-click it.
7. To view detailed information about the detected indicator of compromise, click the **Show incident card** button.
   Detected IOC card contains information about objects 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 Detected IOC card is not available for IOC files, for which no indicators of compromise were detected during scan.

Managing Autonomous IOC Scan tasks

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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*.

Only the files with IOC rules can be specified for the IOC Scan task. Files with other types of rules are not supported for the IOC Scan task.

This section describes how to configure the settings of Autonomous IOC Scan tasks using Kaspersky Endpoint Agent Management plug-in.

Configuring user permissions to manage IOC Scan tasks

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

You need to configure Kaspersky Security Center user permissions, whose account will be used to manage IOC Scan tasks.

Only the files with IOC rules can be specified for the IOC Scan task. Files with other types of rules are not supported for the IOC Scan task.

To configure Kaspersky Security Center user permissions to manage IOC Scan tasks:

1. Open Kaspersky Security Center Administration Console.
2. Select **Administration Server**.
3. In the Administration Server context menu, select **Properties**.

   The property window for the Administration Server.
4. In the left part of the window, select the **Security** section.
5. Select Kaspersky Security Center user, whose account will be used to manage IOC Scan tasks.

   At the bottom of the window, the list of the selected user permissions is displayed, grouped by the applications that the user can manage using Kaspersky Security Center.
6. In the **Kaspersky Endpoint Agent** group of permissions expand the **Intrusion Prevention** section.
7. Select the check boxes in the **Allow** column for the following types of permissions: **Modify**, **Execute**, and **Perform actions on device selections**.
8. Click **Apply** and **OK**.

   Configuration of the user permissions to manage IOC Scan tasks is finished.

Configuring Autonomous IOC Scan task

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To configure settings of an Autonomous IOC Scan task:

1. Open Kaspersky Security Center Administration Console.
2. In Kaspersky Security Center Administration Console tree, open the **Tasks** folder.
   A list of tasks appears.
3. In the **Run IOC Scan** section, select the task in the list and right-click it to open the task action menu.
4. Select the **Properties** menu item.
   The task properties window opens.
5. In the left part of the window, select the group of settings that you want to change.
6. In the right part of the window, make the necessary modifications and click **Apply** and **OK**.

You can configure the following task settings:

- **Task name**

  Do the following:

  1. Select the **General** section.
  2. Change the task name in the top line.

- **Storage time for the task execution results on the Administration Server**

  Do the following:

  1. Select the **Notification** section.
  2. Make sure, that the **On the Administration Server for (days)** check box is selected in the **Save information about results** section, and specify for how many days you want to store the task execution results.

     By default, task execution results are stored on the Administration Server for 7 days.

- **Application actions on IOC detection**

To configure the application actions on IOC detection:

1. Select the **IOC Scan settings** section.
2. In the **Actions** group of settings, select the **Take response actions when indicator of compromise is found** check box.
3. Select the **Quarantine and delete** check box to quarantine the detected object and remove it from the device.
4. Select the **Send a command to Endpoint Protection Platform to scan the critical areas** 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 the object is detected.
5. Click the **Apply** button.

- IOC Scan task schedule

To configure the schedule settings for IOC Scan task:

1. In the **Task schedule** section, select the **Run by schedule** check box.
2. In the **Frequency** list select one of the following options to run IOC Scan tasks: **At specified time**, **Every hour**, **Every day**, **Every week** or **On application launch**.
3. If you select the **At specified time** option, specify the day and time to start the task in the **Run by schedule** section.
4. If you select one of the following options: **Every hour**, **Every day** or **Every week**, configure the following settings in the **Run by schedule** section:
   a. In the **Every** list, select the task run frequency. For example, once a day or twice a week on Tuesdays and Thursdays.
   b. In the **Time** and **Date** lists, select the date and time from which the schedule applies.
5. To configure advanced schedule settings, click the **Advanced** button and perform the following actions in the **Advanced** window:
   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 IOC Scan 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 workstations 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 run to every** check box and specify the start interval in minutes.
   e. Click **OK**.

- Kaspersky Security Center user account to run the task

  To select Kaspersky Security Center user account, under which you want to run the task,

  perform one of the following actions in the group of settings for selecting account to start the task:

  - Select the default account and click **Next**.
  - Enter the name and password of the user, whose account permissions will be used to start the task.

- Excluding groups of devices from the task scope

  To exclude groups of devices from the task scope, in the **Exclusions from task scope** section, select the groups of devices to which the task will not be applied.

  Only the subgroups of the administration group to which the task applies can be excluded.

IOC collection export

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To export an IOC collection:

1. Open Kaspersky Security Center Administration Console.
2. In Kaspersky Security Center Administration Console tree, open the **Tasks** folder.
   A list of tasks appears.
3. In the **Run IOC Scan** section, select the task in the list and right-click it to open the task action menu.
4. Select the **Properties** menu item.
   The task properties window opens.
5. Select the **IOC Scan settings** section.
6. In the **IOC collection** section click **Export**.
7. In the window that opens, specify the name of the file and select the folder where you want to save it.
8. Click the **Save** button.
   The application creates a ZIP file in the folder you specified.

Viewing IOC Scan task execution results

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To view the IOC Scan task execution results:

1. Open Kaspersky Security Center Administration Console.
2. In Kaspersky Security Center Administration Console tree, open the **Tasks** folder.

   The list of tasks is displayed in the workspace.
3. Open the settings of the required task in one of the following ways:

   - Double-click the task name.
   - Open the policy context menu and select **Properties**.
   - Select a task and click **Configure task** in the right part of the window.

   The **Properties: <Task name>** window opens.
4. Select the **Results** section.
5. In the **Show task results for the device** list, select the devices for which you want to view the results of IOC Scan tasks.
6. To view detailed information about a particular task, double-click it.
7. To view detailed information about the detected indicator of compromise, click the **Show incident card** button.

   Detected IOC card contains information about objects 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 Detected IOC card is not available for IOC files, for which no indicators of compromise were detected during scan.

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.

Managing Kaspersky Endpoint Agent policies

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

Creating Kaspersky Endpoint Agent policy

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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**
   - **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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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

Configuring Kaspersky Endpoint Agent security settings

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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);
  - 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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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, enable or disable the **Enable self-defense for application modules in memory** setting.
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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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

If you want to **Use proxy server with specified settings** when connecting to KATA or Kaspersky Sandbox server, make sure that the **Connect using the proxy server if specified in the general settings** option is selected when configuring integration with KATA, Kaspersky Industrial CyberSecurity or Kaspersky Sandbox. This option is not selected by default.

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 **Other settings** subsection.
3. Select one of the following proxy service usage options:

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

4. If you select the **Automatically detect proxy server address** option, the proxy server for further telemetry transmission is detected automatically.
5. 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.

6. 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.

7. 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.

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

9. Click **OK**.

10. 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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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 **Other 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.

Configure network isolation settings

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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

Enabling and disabling network isolation

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

The settings of automatic network isolation can be configured in the policy properties, and the settings of network isolation on demand (manually enabled settings) can be 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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

The settings of automatic network isolation can be configured in the policy properties, and the settings of network isolation on demand (manually enabled settings) can be 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 enable or disable the **Automatically disable network isolation after** setting.
4. Specify the period after which network isolation will be disabled.

   The default period is 30 minutes.
5. 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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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 **Exclusion rules**.
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 **Modify**.

        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 **Exclusion rules** 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 Kaspersky Endpoint Agent policy type

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

Selecting Kaspersky Endpoint Agent policy type is necessary in order for the list of settings displayed in the policy to correspond to the selected Kaspersky Endpoint Agent deployment method.

To configure the policy type:

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. In the **Application settings** section select the **Management and interface** subsection.

3. In the window that opens, select the required Kaspersky Endpoint Agent deployment method by selecting the appropriate check boxes:

   - **Kaspersky Sandbox**
   - **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.

4. Click **OK**.

Policy type is changed. The policy contains the settings for the selected Kaspersky Endpoint Agent deployment method.

Configuring KSN usage in Kaspersky Endpoint Agent

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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 and later. 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 Statement** 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 want to use Kaspersky Security Center for telemetry transmission, select the Use Kaspersky Security Center as a KSN proxy server check box.

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

KSN usage is enabled.

Configuring the integration of Kaspersky Endpoint Agent with Kaspersky Sandbox

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

Configuring the integration of Kaspersky Endpoint Agent with Kaspersky Sandbox is not available in Kaspersky Security Center Cloud Console interface.

This section contains information on configuring the integration of Kaspersky Endpoint Agent with Kaspersky Sandbox. Integration must be configured both on Kaspersky Endpoint Agent side using Kaspersky Security Center Web Console, and on Kaspersky Sandbox side using the web interface.

Enabling and disabling integration with Kaspersky Sandbox

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

Configuring the integration of Kaspersky Endpoint Agent with Kaspersky Sandbox is not available in Kaspersky Security Center Cloud Console interface.

To enable or disable integration with Kaspersky Sandbox:

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 Sandbox integration** section select the **Connection settings** subsection.
3. In the **Kaspersky Sandbox integration settings** group of settings, enable or disable the **Enable Kaspersky Sandbox integration** setting.
4. Enable or disable the **Connect using the proxy server if specified in the general settings** option.

   This option is disabled by default. The application connects to Kaspersky Sandbox server only directly and does not use the general proxy server connection settings. You can enable this option if you want the application to use the general proxy server connection settings when connecting to Kaspersky Sandbox server.
5. If you configure the settings in the policy properties window, 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.

Integration with Kaspersky Sandbox is enabled (or disabled) on Kaspersky Endpoint Agent side.

Configuring trusted connection on Kaspersky Endpoint Agent side

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

You can configure a trusted connection between Kaspersky Sandbox and Kaspersky Endpoint Agent in the web interface of Kaspersky Sandbox server that is not included in the cluster.

If you have already merged servers into a cluster, remove the server from the cluster, then create a new cluster based on this server and add all the servers intended for Kaspersky Sandbox solution to the new cluster.

If the servers you need belong of another cluster, remove them from that cluster one by one and then add them to your cluster.

To configure trusted connection on Kaspersky Endpoint Agent side:

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 Sandbox integration** section select the **Connection settings** subsection.
3. In the **Kaspersky Sandbox integration settings** group of settings, select the **Use trusted connection** check box.
4. Click the **Add new TLS certificate** button.

   The **Adding new TLS certificate** window opens.
5. Perform one of the following actions to add a TLS certificate created on Kaspersky Sandbox side:

   - Add a certificate file. Click **Upload**, and in the window that opens, select the certificate file and click **Open**.
   - Copy and paste the contents of the certificate file to the **TLS certificate data** field.

   Kaspersky Endpoint Agent may have only one TLS certificate of Kaspersky Sandbox server. If you have added a TLS certificate before and then add a TLS certificate once again, only the last added certificate is valid.
6. Click **OK**.

   Information about the added TLS certificate is displayed in the **Kaspersky Sandbox integration settings** group of settings.
7. If you configure the settings in the policy properties window, in the upper right corner of the group of settings, change the switch from **Undefined** to **Enforce**.
8. Click **OK**.
9. Click the **Save** button.

Trusted connection to Kaspersky Sandbox server is configured.

Adding Kaspersky Sandbox servers to Kaspersky Endpoint Agent list

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

If you use Nginx as a proxy server between a device with Kaspersky Endpoint Agent installed and Kaspersky Sandbox server, configure the `client_max_body_size` setting. The value of the `client_max_body_size` setting must be equal to the maximum size of the object sent by Kaspersky Endpoint Agent to Kaspersky Sandbox for processing. Otherwise, Nginx will not send the objects whose size exceeds the specified value. The default value is 1 MB.

If you enabled the integration with Kaspersky Sandbox, you can add Kaspersky Sandbox servers to Kaspersky Endpoint Agent list. You can add several Kaspersky Sandbox servers.

For a particular policy, add servers that are part of the same cluster. If servers belong to different clusters, the outcome is unpredictable.

To add Kaspersky Sandbox servers to Kaspersky Endpoint Agent list:

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 Sandbox integration** section select the **Connection settings** subsection.

3. Select the **Enable Kaspersky Sandbox integration** check box if it is cleared.

4. In the **Kaspersky Sandbox integration settings** group of settings, enable or disable the **Connect using the proxy server if specified in the general settings** option.

   This option is disabled by default. The application connects to Kaspersky Sandbox server only directly and does not use the general proxy server connection settings. You can enable this option if you want the application to use the general proxy server connection settings when connecting to Kaspersky Sandbox server.

5. In the **List of Kaspersky Sandbox servers** group of settings, click **Add**.

6. In the right part of the window, enter the IP address or fully qualified domain name of Kaspersky Sandbox server and the port used for connecting to the server.

7. Click **OK**.

   The added server is listed in the server table.

8. Repeat the steps to add each Kaspersky Sandbox server to the list.

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

10. Click **OK**.

11. Click the **Save** button.

Kaspersky Sandbox servers are added to Kaspersky Endpoint Agent list.

Configuring the response timeout of Kaspersky Sandbox and request queue settings

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To configure the response timeout of Kaspersky Sandbox and processing queue settings for objects that Kaspersky Endpoint Agent sends to Kaspersky Sandbox:

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 Sandbox integration** section select the **Kaspersky Sandbox advanced settings** subsection.
3. In the **Timeout** group of settings, specify the maximum Kaspersky Sandbox response timeout.

   The default value is 5 seconds.
4. In the upper right corner of the settings group, change the switch from **Unaffected by policy** to **Under policy**.
5. In the **Kaspersky Sandbox requests queue** group of settings, in the **Queue folder** field specify the path to the folder where information about the requests sent to Kaspersky Sandbox will be stored.

   The default folder is %SOYUZAPPDATA%\Sandbox\Queue.
6. In the **Maximum queue size (MB)** field, specify the maximum allowed size of the request queue in megabytes.

   The default value is 100 MB.
7. If you configure the settings in the policy properties window, 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**.

Configuring Threat Response actions of Kaspersky Endpoint Agent to respond to threats detected by Kaspersky Sandbox

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

Kaspersky Endpoint Agent can perform actions in response to threats detected by Kaspersky Sandbox.

You can configure the following types of actions:

- Local actions

  Local actions – actions to be performed on each device where a threat is detected:

  - **Quarantine and delete**.

    When a threat is detected on a device, a copy of the object containing the threat is quarantined, and the object is deleted from the device.

  - **Notify device user**.

    When a threat is detected on a device, a notification about the detected threat is displayed to the device user.

    The notification is displayed if the device is running under the user account same to the account under which the threat was detected.

    If the device is not running or is running under another user account, the notification is not displayed.

  - **Push Endpoint Protection Platform scanning on critical areas**.

    If a threat is detected on a device, Kaspersky Endpoint Agent sends a command to EPP to scan critical areas of the device. Critical areas include kernel memory, objects loaded at operating system startup, and boot sectors of the hard drive. For more details on configuring the scan settings refer to the documentation of EPP being used.

- Group actions

  Group actions – actions to be performed on all devices of the administration group for which the policy is configured.

  - **Run IOC scanning on a managed group of devices**.

    If a threat is detected on any device of the administration group for which you configure the policy, Kaspersky Endpoint Agent scans all devices of this administration group for objects containing the detected threat.

  - **Quarantine and delete when IOC is found**.

    If a threat is detected on any device of the administration group for which you configure the policy, Kaspersky Endpoint Agent scans all devices of this administration group for objects containing the detected threat. When an object which contains a threat is detected on devices of this administration group, a copy of the object containing the threat is quarantined, and the object is deleted from the device.

  - **Push Endpoint Protection Platform scanning on critical areas when IOC is found**.

    If a threat is detected on any device of the administration group for which you configure the policy, Kaspersky Endpoint Agent sends a command to EPP to scan critical areas on all administration group's devices where the object containing the threat was detected. For more details on configuring the scan settings refer to the documentation of EPP being used.

When configuring threat response actions, keep in mind that as a result of some actions, the object containing the threat may be deleted from the workstation where it was detected.

If you want Kaspersky Endpoint Agent to create Autonomous IOC Scan tasks when responding to threats, configure authentication on the Administration Server.

The application uses a special Administration Server user account, which has limited permissions and is intended only for creating Autonomous IOC Scan tasks.

The special account can only be created in the **Threat Response** window in Kaspersky Endpoint Agent policy properties or in the application properties of an individual device. The special account must be created on the Administration Server only once and its password must be used to configure **Threat Response** settings in the properties of other devices or other policies of the same Administration Server.

It is not possible to change the password of the special account created for Autonomous IOC Scan tasks. If you forget the password of this account, delete it using standard Kaspersky Security Center tools and create it again in the **Threat response** window.

To configure Kaspersky Endpoint Agent response actions to threats detected by Kaspersky Sandbox:

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 Sandbox integration** section select the **Threat response** subsection.
3. Select the **Perform response actions to threats detected by Kaspersky Sandbox** check box.
4. In the **Current actions** list, select the check boxes for the actions you want to enable.

5. If you select the **Run IOC Scan for a managed group of devices** action, perform the following actions in the **Authentication on Administration Server** group of settings:

   a. Click the **Create special user** button.

   > Unavailability of the **Create special user** button indicates that a special account for the Autonomous IOC Scan tasks has already been created. Go to the step "d" of the instruction.

   b. In the window that opens, in the **Administration Server password** field, specify a password with the length of 8–16 characters and click the **Create user** button.

   c. Click **OK**.

   A special Administration Server account for Autonomous IOC Scan tasks is created.

   d. In the **Administration Server password** field, enter the password for the special account created for the Autonomous IOC Scan tasks.

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

7. Click **OK**.

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

Kaspersky Endpoint Agent response actions to threats detected by Kaspersky Sandbox are configured and ready to be applied on devices.

Enabling detection of legitimate applications that can be used by cybercriminals

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

You can enable detection of legitimate applications that could be used by cybercriminals to harm your organization computer network. Kaspersky Endpoint Agent considers such applications as threats and performs threat response actions on them.

Legitimate applications are allowed to be installed and used on user computers and are designed to perform user tasks. However, some types of legitimate applications, when used by cybercriminals, may harm user computers or organization computer network. If cybercriminals gain access to such applications or deploy them on user computers, they can use functions of such applications to violate security of the user computer or organization computer network.

Such applications include IRC clients, dialers, file download applications, computer system activity monitors, password utilities, Internet servers for FTP, HTTP or Telnet services.

If you want to enable detection of such applications:

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 Sandbox integration** section select the **Threat response** subsection.
3. In the **Additional** group of settings select the **Enable detection of legitimate applications, which can be exploited by adversaries** 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**.

Configuring IOC Scan tasks start

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To configure start of IOC Scan tasks:

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 Sandbox integration** section select the **Threat response** subsection.
3. In the **Additional** group of settings click the **Configure IOC Scan** link.
4. In the **Scanning area** group of settings in the right part of the window, select one of the following areas where Kaspersky Endpoint Agent will search for IOCs:
   - **System drives only**.
   - **Critical file areas**.
5. In the **Configure IOC Scan** group of settings, select one of the following options to start IOC Scan tasks:
   - **Manual start**.

     IOC Scan tasks will be created automatically, but will not be started. You can start every single task or all tasks manually.
   - **Now**.

     IOC Scan tasks will be automatically created and started.
   - **Start within the specified period**.

     IOC Scan tasks will be created automatically, and will be started within the specified period. For example, outside of working hours from 8:00 p.m. to 7:00 a.m.

     If you select the **Start within the specified period** option, specify the start and end of the period in the **Period start time (hh:mm)** and **Period end time (hh:mm)** fields.

     All IOC Scan tasks that were automatically created BEFORE the beginning of the specified period will start at any time WITHIN the specified period.

All IOC Scan tasks that were automatically created WITHIN the specified period will start immediately.

All IOC Scan tasks that were automatically created AFTER the beginning of the specified period will start the next day.

Example:
You have configured the tasks to run during the specified period from 8:00 p.m. to 7:00 a.m.:
Tasks that were automatically created at 7 p.m. are started at any arbitrary time from 8:00 p.m. to 7:00 a.m.
Tasks that were automatically created at 9 p.m. are started at 9 p.m.
Tasks that were automatically created at 8:00 a.m. are started during the next task execution period, from 8:00 p.m. to 7:00 a.m.

6. Click **OK**.
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**.

Configuring integration between Kaspersky Endpoint Agent and KATA Central Node

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

This section contains information on how to configure integration between Kaspersky Endpoint Agent and the KATA Central Node component using Kaspersky Security Center Web Console.

Enabling and disabling integration with KATA Central Node

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

If you use Nginx as a proxy server between a device with Kaspersky Endpoint Agent installed and KATA server, configure the `client_max_body_size` setting. The value of the `client_max_body_size` setting must be equal to the maximum size of the object sent by Kaspersky Endpoint Agent to KATA for processing. Otherwise, Nginx will not send the objects whose size exceeds the specified value. The default value is 1 MB.

To enable or disable integration with the KATA Central Node component:

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. In the **KATA integration** section select **KATA integration settings**.

   The **KATA integration settings** window opens.

3. In the **Connection settings** group of settings, do one of the following:

   - To enable integration with KATA Central Node:

     a. Select the **Enable KATA integration** check box.

     b. Specify the IP address or fully qualified domain name of the KATA server and the port used for connecting to the server.

   - To disable integration with KATA Central Node, clear the **Enable KATA integration** check box.

4. Enable or disable the **Connect using the proxy server if specified in the general settings** option.

   This option is disabled by default. The application connects to the KATA server only directly and does not use the general proxy server connection settings. You can enable this option if you want the application to use the general proxy server connection settings when connecting to the KATA server.

5. In the upper right corner of the settings group, change the switch from **Undefined** to **Enforce**.

   The default switch position is **Enforce**.

6. Click **OK**.

Integration with KATA Central Node is enabled or disabled.

Configuring trusted connection with KATA Central Node

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To configure trusted connection between Kaspersky Endpoint Agent and KATA Central Node, perform the following actions on Kaspersky Endpoint Agent side:

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. In the **KATA integration** section select **KATA integration settings**.
   The **KATA integration settings** window opens.
3. In the **Connection settings** group, select the **Use pinned certificate to protect connection** check box.
4. Click the **Add new TLS certificate** button.
   The window for adding a new TLS certificate opens.
5. Perform one of the following actions to add a TLS certificate:
   - Add a certificate file. Click **Upload**, and in the window that opens, select the certificate file and click **Open**.
   - Copy and paste the contents of the certificate file to the **TLS certificate data** field.

   Kaspersky Endpoint Agent may have only one KATA server TLS certificate. If you have added a TLS certificate before and then add a TLS certificate once again, only the last added certificate is valid.
6. Click **OK**.
   Information about the added TLS certificate is shown in the **TLS certificate data** group of settings.
7. If you want to configure additional connection protection by a user certificate, do the following:
   a. Select the **Secure connection with the client certificate** check box.
   b. Click the **Load Crypto-container** button.
   c. In the window that opens select the PFX archive and click **Open**.
   d. In the **Crypto-container password** field, enter the password for the PFX archive.
   e. Click **OK**.
8. In the upper right corner of the settings group, change the switch from **Undefined** to **Enforce**.
   The default switch position is **Enforce**.
9. Click **OK**.

Trusted connection to KATA server is configured.

Configuring synchronization settings between Kaspersky Endpoint Agent and KATA Central Node

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To configure synchronization settings between Kaspersky Endpoint Agent and KATA Central Node:

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. In the **KATA integration** section select **KATA integration settings**.

   The **KATA integration settings** window opens.

3. In the **Additional settings** group, configure the following settings:

   - **Timeout (sec.)**. Specify the maximum KATA server response timeout. The default value is 10 seconds.
   - **Send synchronization request to KATA server every (min.)**. Specify the time interval for sending requests for synchronization Kaspersky Endpoint Agent settings and tasks with KATA Central Node. You can specify a value from 1 to 60 minutes. The default value is 5 minutes.
   - Select or clear the **Consider TTL period when sending events** check box. The check box is cleared by default.

     If the check box is selected, Kaspersky Endpoint Agent does not send information about the processes that are started again to the KATA server. Kaspersky Endpoint Agent does not consider the launch of the process as repeated if the process is started after the end of the TTL period.
   - If you select the **Consider TTL period when sending events** check box, specify the time in the **TTL period (min.)** field. The default value is 1440 minutes.

4. In the upper right corner of the settings group, change the switch from **Undefined** to **Enforce**.

   The default switch position is **Enforce**.

5. Click **OK**.

Configuring data submission settings

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To configure data submission settings:

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. In the **KATA integration** section select **General settings**.

   The **General settings** window opens.

3. In the **Data submission settings** group, do the following:

   - Specify the value in the **Maximum event transmission time (sec.)** field.
   - Specify the value in the **Maximum number of events in a package** field.

4. In the upper right corner of the settings group, change the switch from **Undefined** to **Enforce**.

   The default switch position is **Enforce**.

5. Click **OK**.

Configuring request throttling settings

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

The request throttling feature allows restricting the flow of events with low importance from Kaspersky Endpoint Agent to the Central Node component.

To configure the request throttling settings:

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. In the **KATA integration** section select **General settings**.

   The **General settings** window opens.

3. In the **Request throttling** group of settings, you can perform the following actions:

   - Select or clear the **Enable request throttling** check box to enable or disable the feature.

This feature is enabled by default.

- Specify the value in the **Maximum number of events per hour** field.

  The application analyzes telemetry data flow and restricts transmission of events with low importance if the number of transmitted events tends to exceed the value specified in this field. The default value is 3000 events per hour.

- Specify the value in the **Percentage of event limit excess** field.

  If the flow of events of the same type with low importance exceeds the threshold value specified in this field as a percentage of the total number of events, transmission of events of this type is restricted. You can specify a value from 5% to 100%. The default value is 15%.

4. In the upper right corner of the settings group, change the switch from **Undefined** to **Enforce**.

   The default switch position is **Enforce**.

5. Click **OK**.

Configuring integration between Kaspersky Endpoint Agent and Kaspersky Industrial CyberSecurity for Networks

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

This section contains information on how to configure integration between Kaspersky Endpoint Agent and Kaspersky Industrial CyberSecurity for Networks using Kaspersky Security Center Web Console.

Enabling integration with Kaspersky Industrial CyberSecurity for Networks

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To enable integration with Kaspersky Industrial CyberSecurity for Networks:

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. In the **Telemetry receipt servers** section, select **Integration with KICS for Networks**.

   The **Integration with KICS for Networks** window opens.

3. In the **Connection settings** group of settings, select the **Enable integration with KICS for Networks** check box.

4. Specify the IP address or fully qualified domain name of the **KICS for Networks** server and the port used for connecting to the server.

5. Enable or disable the **Connect using the proxy server if specified in the general settings** option.

   This option is disabled by default. The application connects to Kaspersky Industrial CyberSecurity for Networks server only directly and does not use the general proxy server connection settings. You can enable this option if you want the application to use the general proxy server connection settings when connecting to Kaspersky Industrial CyberSecurity for Networks server.

6. In the upper right corner of the settings group, change the switch from **Undefined** to **Enforce**.

   The default switch position is **Enforce**.

7. Click **OK**.

Integration with Kaspersky Industrial CyberSecurity for Networks is enabled.

Configuring trusted connection with Kaspersky Industrial CyberSecurity for Networks

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To configure trusted connection between Kaspersky Endpoint Agent and Kaspersky Industrial CyberSecurity for Networks, perform the following actions on Kaspersky Endpoint Agent side:

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. In the **KATA integration** section, select **Integration with KICS for Networks**.

   The **Integration with KICS for Networks** window opens.

3. In the **Connection settings** group, select the **Use pinned certificate to protect connection** check box.

4. Click the **Add new TLS certificate** button.

   The window for adding a new TLS certificate opens.

5. Perform one of the following actions to add a TLS certificate:

   - Add a certificate file. Click **Upload**, and in the window that opens, select the certificate file and click **Open**.
   - Copy and paste the contents of the certificate file to the **TLS certificate data** field.

   Kaspersky Endpoint Agent may have only one TLS certificate for the KICS for Networks server. If you have added a TLS certificate before and then add a TLS certificate once again, only the last added certificate is valid.

6. Click **OK**.

   Information about the added TLS certificate is shown in the **TLS certificate data** group of settings.

7. If you want to configure additional connection protection by a user certificate, do the following:

   a. Select the **Secure connection with the client certificate** check box.

   b. Click the **Load Crypto-container** button.

   c. In the window that opens select the PFX archive and click **Open**.

   d. In the **Crypto-container password** field, enter the password for the PFX archive.

   e. Click **OK**.

8. In the upper right corner of the settings group, change the switch from **Undefined** to **Enforce**.

   The default switch position is **Enforce**.

9. Click **OK**.

Trusted connection to Kaspersky Industrial CyberSecurity for Networks server is configured.

Configuring synchronization settings between Kaspersky Endpoint Agent and Kaspersky Industrial CyberSecurity for Networks

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To configure synchronization settings between Kaspersky Endpoint Agent and Kaspersky Industrial CyberSecurity for Networks:

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. In the **KATA integration** section, select **Integration with KICS for Networks**.

   The **Integration with KICS for Networks** window opens.

3. In the **Additional settings** group, specify the maximum response timeout for the KICS for Networks server in the **Timeout (sec.)** field.

   The default value is 10 seconds.

4. In the upper right corner of the settings group, change the switch from **Undefined** to **Enforce**.

   The default switch position is **Enforce**.

5. Click **OK**.

Synchronization settings between Kaspersky Endpoint Agent and Kaspersky Industrial CyberSecurity for Networks server are configured and applied.

Configuring data submission settings

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To configure data submission settings:

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. In the **KATA integration** section select **General settings**.

   The **General settings** window opens.

3. In the **Data submission settings** group, do the following:

   - Specify the value in the **Maximum event transmission time (sec.)** field.
   - Specify the value in the **Maximum number of events in a package** field.

4. In the upper right corner of the settings group, change the switch from **Undefined** to **Enforce**.

   The default switch position is **Enforce**.

5. Click **OK**.

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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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

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

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 documentation.

To configure 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. Enable **KSN Usage**.

   Open the main window of Kaspersky Security Center Web Console.

5. In the Administration Console tree, configure the **Private KSN** settings (for information on configuring Kaspersky Security Network proxy server settings, refer to *Kaspersky Security Center Help*).

   Download Kaspersky Managed Detection and Response configuration file with the pkcs7 extension, which is included in the mdr_config.zip archive.

6. To continue configuring integration between Kaspersky Endpoint Agent and Kaspersky Managed Detection and Response, open the main window of Kaspersky Security Center Web Console.

7. Open the **Devices** → **Policies and profiles** tab.
8. In the list of policies, select the name of Kaspersky Endpoint Agent policy that you want to configure.
   This opens the policy settings window.
9. On the **Application settings** tab, select **Managed Detection and Response**.
10. 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.
    c. In the **User identifier** field, enter an arbitrary value.
    d. In the upper right corner of the settings group, change the switch from **Undefined** to **Enforce**.
11. 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).

Configuring EDR telemetry settings

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

This section contains information on how to configure exclusions for EDR telemetry that Kaspersky Endpoint Agent processes and sends to the server with the KATA Central Node component.

Enabling and configuring EDR telemetry exclusions

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

You can configure EDR telemetry exclusions using Kaspersky Security Center Web Console both in the properties of an individual device and in the policy settings for a group of devices.

To enable and configure EDR telemetry 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. In the **EDR telemetry** section, select **Exclusions**.
   The window for configuring EDR telemetry exclusion settings opens.
3. To enable usage of EDR telemetry exclusions, select the **Use exclusions** check box.
4. To add a new exclusion:
   a. Click the **Add** button.
   b. In the **Rule properties** window that opens, configure the following exclusion criteria:

The criteria are applied using logical AND.

To create a rule, specify the value in the **Path** field and select at least one event type in the **Use this exclusion for the following event types** list.

If the **Network events** option is selected for the **Use this exclusion for the following event types** criterion, specify the full path to the file in the **Path** field.

The object for which you create an exclusion must be available on the protected device at the time the exclusion settings are applied. For example, if you first configure exclusion for a specific application, and then install that application on the protected device, this exclusion will not be applied.

- In the **General data** section, specify the values in the following fields:
  - **Path**. Full path to the file, including its name and extension. You can use file masks (using the ? and * characters), as well as system environment variables.
  - **Command line**. Command line to run the object.
  - **Parent folder path**. The path to the folder where the file is located.
- In the **Version information** section, specify the values in the following fields:
  - **Description**. The value of the FileDescription parameter from the resource of the RT_VERSION type (VersionInfo).
  - **Original file name**. The value of the OriginalFilename parameter from the resource of the RT_VERSION type (VersionInfo).
  - **Version**. The value of the FileVersion parameter from the resource of the RT_VERSION type (VersionInfo).
- In the **File data** section, specify the values in the following fields:
  - **MD5**. MD5 hash of the file.
  - **SHA256**. SHA256 hash of the file.
- In the **Use this exclusion for the following event types** list, select at least one of the following options:
  - **File modification**.
  - **Network events**.
  - **Interactive input in the console**. This option is selected by default.
  - **Loading the process module**.
  - **Changes in the Registry**.

c. Click **OK** to save the changes and close the **Rule properties** window.

The new rule is created and displayed in the list of exclusions.

5. To remove a rule from the list of exclusions, select the check box next to the rule and click **Remove**.

6. To open the properties window for an existing rule and to change the specified criteria, select the check box next to the rule and click **Edit**.

7. If you are configuring the policy settings, make sure that the switch in the upper right corner of the group of settings is set to **Enforce**. It is the default position of the switch.

8. Click **OK** to save the changes and close the **Exclusions** window.

EDR telemetry exclusions will be used according to the configured rules.

Configuring Execution prevention settings

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

This section describes how to configure Execution prevention.

Enabling Execution prevention

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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 Execution prevention rules** 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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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. In the **Prevention rules** group of settings, select the **Do not perform actions on critical system files** check box if you want to exclude critical system files from the scope of prevention rules.
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. 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 Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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 specify the maximum size of quarantine in megabytes 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. 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 **Apply** and **OK**.

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

Configuring data synchronization with the Administration Server

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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 the Administration Server** subsection.
3. Select the **Synchronize data about objects in Quarantine 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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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 the Administration Server** subsection.
3. In the **Synchronization with the Administration Server** group of settings, select the **Threat development chain creation** 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 failure diagnosis

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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 failure 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 **Failure diagnosis** subsection.
3. To enable logging of debug information to the trace files:
   a. Enable the **Write debug information to trace files** option.
   b. In the **Trace files folder** field, specify the path to the folder on the device where the application saves the trace files.

      Make sure that the specified folder is available on the managed device. Otherwise, the debug information will not be saved.

   c. In the **Maximum trace file size** field, specify the file size in megabytes.

      The default value is 50 MB. When the specified file size is reached, the application continues writing to a new file.
4. If you want the application to overwrite old trace files:
   a. Enable the **Overwrite old trace files** option.
   b. Enter the desired value in the **Maximum number of files per trace log** field.

      The default value is 1 file. When the specified number of files is reached, the application overwrites old files, starting with the oldest one. The specified limit is applied separately for each Kaspersky Endpoint Agent process being debugged, so the total number of files for all processes may exceed the specified value.
5. To enable logging of dump files:
   a. Enable the **Create dump files** option.
   b. In the **Dump files folder** field, specify the folder to save the dump files.

      Make sure that the specified folder is available on the managed device. Otherwise, the debug information will not be saved.
6. Click **OK**.

Failure diagnostics is configured and enabled for all Kaspersky Endpoint Agent processes that are currently running. Failure diagnostics files will be generated in the folders you specified.

Managing Kaspersky Endpoint Agent tasks

This section describes how to manage Kaspersky Endpoint Agent tasks.

Creating tasks

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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.

You can start the created task manually or configure a scheduled task start.

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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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.

Viewing task execution results

You can view the task execution results during their storage period. You can also change the storage period for the task execution results.

It is not recommended to shorten the storage period for IOC Scan task execution results.

To view the task execution result:

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

   A list of tasks appears.

2. In the list of tasks that displays, click the task name.

   The task settings window opens.

3. Open the **Results** tab.

Information is displayed in the **Task execution results** list.

You can also view the **Last execution results** for the task on the **General** tab.

Configuring the storage time for the task execution results on the Administration Server

By default, task execution results are stored on the Administration Server for seven days.

To change the storage time for the task execution results on the Administration 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 that displays, click the task name.

   The task settings window opens.

3. Open the **Settings** tab.

4. In the **Notifications** section, click the **Settings** button.

5. Make sure that the **Store in the Administration Server database for (days)** option is selected in the **Select application behavior after the task completion** list and specify how long (in days) the result of the task execution will be stored.

6. Click **OK**.

7. Click the **Save** button.

The changes will be saved.

It is not recommended to shorten the storage period for IOC Scan task execution results.

Creating Kaspersky Endpoint Agent activation tasks

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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 **Use as additional key** 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.

You can start the created task manually or configure a scheduled task start.

Configuring Database and application module update task

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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 **Database 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 **Database 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 **Web address** 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.

You can start the created task manually or configure a scheduled task start.

Managing Standard IOC Scan tasks

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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.

Only the files with IOC rules can be specified for the IOC Scan task. Files with other types of rules are not supported for the IOC Scan task.

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

Requirements for IOC files

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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.
- Only the files with IOC rules can be specified for the IOC Scan task. Files with other types of rules are not supported for the IOC Scan task.
- 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.

The table below shows the features and limitations of the OpenIOC standard supported by the application.

Features and limitations of the OpenIOC standard versions 1.0 and 1.1

Supported	OpenIOC 1.0:

conditions	`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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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

Configuring Standard IOC Scan task

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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.

Only the files with IOC rules can be specified for the IOC Scan task. Files with other types of rules are not supported for the IOC Scan task.

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 collection** group of settings click the **Select IOC files** button.
   b. In the dialog that opens, click the **Select 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 collection** group of settings.

   The **IOC collection** 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 collection 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 collection** window.

e. To export the created IOC collection, click **Export**.

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.

g. In the **Retrospective IOC scan** group of settings configure the settings for Retrospective IOC scan mode:

1. In the **Retrospective IOC Scan** group of settings enable the **Perform Retrospective IOC Scan within the interval** option.

2. Specify the time interval.

   During the task execution, the application analyzes data collected during the specified time interval, including the boundaries of the specified interval (from 00:00 on the start date until 23:59 on the end date). The default interval starts at 00:00 on the day preceding the task creation day and ends at 23:59 on the day when the task was created.

   If during execution of the IOC Scan task with the **Perform Retrospective IOC Scan within the interval** option enabled the application does not find any data for the specified time interval to be analyzed, it does not inform about this. In this case, the application shows no indicators of compromise in the task completion report.

h. In the **Actions** group of settings, configure the response actions on detecting the indicator of compromise:

1. Select the **Take response actions after an indicator of compromise is found** check box.

2. 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.

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

4. Select the **Run critical areas scan** 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.

i. In the **Protection of critical system files** group of settings, select the **Do not perform actions on critical system files** check box if you want to protect critical system files from being quarantined or deleted when an indicator of compromise is detected.

The option is available only if the **Quarantine and delete** option is selected in the **Actions** group of settings.

If this option is selected and an object is a critical system file, the application does not perform any actions on this object. This information is logged in the task execution report.

5. 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 **File** 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 **File** window.

d. If the **Analyze data of Windows Event Log (EventLogItem)** check box is selected, click the **Advanced for EventLogItem** link and in the **File** 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 **File** window.

6. Click the **Save** button.

You can start the created task manually or configure a scheduled task start.

Viewing IOC Scan task execution results

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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 **Results** 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 **compromise indicators detected** link in the row with the name of the desired device.

      The **IOC Scan 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 **Match** 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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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. In the **Actions after quarantining file** group of settings, select whether the file must be deleted from the protected device after quarantining.

   If the file is locked by another process, the file will be deleted only after the device is rebooted.

8. In the **Protection of critical system files** group of settings, select the **Do not perform actions on critical system files** check box if you want to exclude critical system files from the task scope.

   If this option is selected and an object is a critical system file, the application does not perform any actions on this object. This information is logged in the task execution report.

9. Click the **Save** button.

You can start the created task manually or configure a scheduled task start.

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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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 **Objects to delete** list click **Add**.
5. The **Object to delete** dialog box opens.
6. In the **Specify the file to delete** drop-down list, select one of the following values: **Specify the object by its full path** or **Specify the object by its 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 **Including 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 **Object to delete** list.

   You can specify several objects for deletion in one Delete file task.
10. In the **Protection of critical system files** group of settings, select the **Do not perform actions on critical system files** check box if you want to exclude critical system files from the task scope.

    If this option is selected and an object is a critical system file, the application does not perform any actions on this object. This information is logged in the task execution report.
11. Click the **Save** button.

You can start the created task manually or configure a scheduled task start.

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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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.

You can start the created task manually or configure a scheduled task start.

Configuring the Terminate process task

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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. In the **Protection of critical system files** group of settings, select the **Do not perform actions on critical system files** check box if you want to exclude critical system files from the task scope.

   If this option is selected and an object is a critical system file, the application does not perform any actions on this object. This information is logged in the task execution report.
9. Click the **Save** button.

You can start the created task manually or configure a scheduled task start.

Managing Kaspersky Endpoint Agent using the command line interface

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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.

Managing Kaspersky Endpoint Agent authentication

ONLY_FOR_CONTEXT_HELP:This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To manage the application authentication 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 --proxy={enable|disable|show} --mode={auto|custom} --server=<proxy server address> --port=<port number> --use-auth={yes|no} --proxy-user=<user name> --proxy-password=<user password> --bypass-local={yes|no}`

The authentication parameters are described in the following table.

Authentication parameters

Parameters	Description
`--proxy={enable|disable|show}`	Required parameter. This parameter controls connection to the proxy server. The following values are available: `enable` – enables proxy server usage. `disable` – disables proxy server usage. `show` – displays the current proxy server usage settings.
`--mode={auto|custom}`	Required parameter. The parameter sets the proxy server configuration mode. The following values are available: `auto` – automatic detection of the proxy server. `custom` – manual configuration of the proxy server access parameters.
`--server=<proxy server address>`	Required parameter. Specifies the proxy server address.
`--port=<port number>`	Required parameter. Specifies the proxy server connection port.
`--use-auth={yes|no}`	Optional parameter. This parameter indicates whether proxy server authentication is required. The following values are available: `yes` – user name and password must be specified to connect to the proxy server. `no` – connection to the proxy server is possible without specifying a user name and password. Used by default.
`--proxy-user=<user name>`	Optional parameter. Specifies the user name to connect to the proxy server. Empty by default.
`--proxy-password=<user password>`	Optional parameter. Specifies the password to connect to the proxy server. Empty by default.
`--bypass-local={yes|no}`	Optional parameter. This parameter sets the direct connection to local addresses without using a

	proxy server. Available values: `yes` – connections to the addresses of the current local network is established without a proxy server. Used by default. `no` – connections to the addresses of the current local network and to external addresses is established through a proxy server.

Configuring tracing

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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 to save the 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.

     Make sure that the specified folder is available on the managed device. Otherwise, trace files will not be created.

   - `agent.exe --trace=enable --folder <path to the folder where to save the trace files> --rotation=yes --rotate-file-size=<maximum file size, MB> --rotate-files-count=<maximum number of files>`, to enable tracing with overwriting old trace files when the values specified for the size and number of the trace files are reached.

     The specified limit on the number of files is applied separately for each Kaspersky Endpoint Agent process being debugged, so the total number of files for all processes may exceed the specified value. If you do not specify the `--rotate-file-size` or `--rotate-files-count` parameters (one or both) with the `--rotation=yes` parameter, the application uses the default values. The default value is 1 file of 50 MB.

   - `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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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.

     Make sure that the specified folder is available on the managed device. Otherwise, dump files will not be created.

   - `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).

Viewing information about quarantine settings and quarantined objects

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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 **Available space threshold (MB)** and **Threshold value for space available (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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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 contains the file>	Required parameter if the --hashalg parameter is passed. 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.

Managing Kaspersky Sandbox integration settings

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To manage the integration settings of Kaspersky Endpoint Agent with Kaspersky Sandbox 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**:

   ```
   --sync-period=<sync period>--sandbox=<enable|disable|show> [--tls=<yes|no>] --servers=<address>:<port> [--timeout=<maximum response timeout of Kaspersky Sandbox server>] [--pinned-certificate=<full path to the TLS certificate file for connection between Kaspersky Endpoint Agent and Kaspersky Sandbox>] --pwd=<current user password>
   ```

   Parameters of the `--sandbox` command when managing the integration settings of Kaspersky Endpoint Agent with Kaspersky Sandbox

Parameter	Description
`--sandbox=<enable|disable|show>`	Required parameter. Allows you to enable, disable, and view integration status of Kaspersky Endpoint Agent with Kaspersky Sandbox. • `--sandbox=<enable>` – enables integration. • `--sandbox=<disable>` – disables integration. • `--sandbox=<show>` – displays integration status of Kaspersky Endpoint Agent with Kaspersky Sandbox.

`--tls=<yes|no>`	Optional parameter. Allows you to enable or disable trusted connection between Kaspersky Sandbox and Kaspersky Endpoint Agent. • `--tls=<yes>` – enables trusted connection. • `--tls=<no>` – disables trusted connection.
`--servers=<address>:<port>`	Required parameter. Allows you to add Kaspersky Sandbox servers to Kaspersky Endpoint Agent list.
`--timeout=<maximum response timeout of Kaspersky Sandbox server>`	Optional parameter. Allows you to set the maximum response timeout of Kaspersky Sandbox server in milliseconds.
`--pinned-certificate=<full path to the TLS certificate file for connecting Kaspersky Endpoint Agent with Kaspersky Sandbox>`	Required parameter, if the `--tls` parameter is passed with the `<yes>` value. Allows you to add a TLS certificate for connecting Kaspersky Endpoint Agent with Kaspersky Sandbox.
`--pwd=<current user password>`	Allows you to specify the password of the user whose account is used to execute the command.

Managing integration settings with KATA Central Node component

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To manage the integration settings of Kaspersky Endpoint Agent with the KATA Central Node component 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 --message-broker=<enable|disable|show> --type=<kata> --use-proxy=<yes|no> --compression=<yes|no> --partitioning-strategy=<automatic|user> [--message-key=<message key> --topic=<topic> --partition=<user specific partition>] --tls=<yes|no> --servers=<address>:<port> [--timeout=<maximum response timeout of KATA server] [--pinned-certificate=<full path to the TLS certificate file>] [--client-certificate=<full path to the certificate file>] --client-password=<password for the PFX archive> --sync-period=<interval for sending synchronization requests>`

The `--message-broker` command parameters when managing the integration settings between Kaspersky Endpoint Agent and the KATA Central Node component

Parameter	Description
--message-broker=<enable|disable|show>	Required parameter. Allows you to enable, disable, and view status of the integration between Kaspersky Endpoint Agent and the KATA Central Node component. • `--message-broker=<enable>` – enables integration. • `--message-broker=<disable>` – disables integration. • `--message-broker=<show>` – displays integration status of Kaspersky Endpoint Agent with the KATA Central Node component.
--type=<kata>	Required parameter. Allows you to specify the KATA Central Node component for managing the integration settings of Kaspersky Endpoint Agent with this component.
--use-proxy=<yes|no>	Required parameter. Allows you to enable and disable application of a proxy server in the message broker to send messages to the KATA server.
`--compression=<yes|no>`	Optional parameter. Allows you to enable or disable compression of data transferred between Kaspersky Endpoint Agent and KATA Central Node. Enabled by default.
`---tls=<yes|no>`	Optional parameter. Allows you to enable or disable trusted connection between Kaspersky Endpoint Agent and the KATA Central Node component. • `--tls=<yes>` – enables trusted connection. • `--tls=<no>` – disables trusted connection.
`--servers=<address>:<port>`	Required parameter. Allows you to add a KATA server.
`--timeout=<maximum response timeout of KATA server>`	Optional parameter. Allows you to set the maximum response timeout of KATA server in milliseconds.
`--pinned-certificate=<full path to the TLS certificate file>`	Required parameter, if the `--tls` parameter is passed with the `<yes>` value. Allows you to add a TLS certificate for connecting Kaspersky Endpoint Agent with KATA server.
`--client-certificate=`	Allows you to add a user certificate for connecting Kaspersky Endpoint

<full path to the certificate file>	Agent with KATA server.
--client-password=<password for the PFX archive>	Allows you to enter the password for the PFX archive, containing a user certificate for connecting Kaspersky Endpoint Agent with KATA server.
--sync-period=<interval for sending synchronization requests>	Allows you to specify the time interval for sending requests for synchronization Kaspersky Endpoint Agent settings and tasks with KATA Central Node.
--throttling=<yes|no>	Allows you to enable or disable request throttling. The request throttling feature allows restricting the flow of events with low importance from Kaspersky Endpoint Agent to the Central Node component.
--event-limit=<number of events per hour>	Allows you to specify the maximum number of events per hour. The application analyzes telemetry data flow and restricts transmission of events with low importance if the number of transmitted events tends to exceed the specified value.
--exceed-limit=<threshold value>	Allows you to specify the threshold for exceeding the limit of events. If the flow of events of the same type with low importance exceeds the threshold value specified as a percentage of the total number of events, transmission of events of this type is restricted. You can specify a value from 5 to 100 (without % character).

Managing integration settings with Kaspersky Industrial CyberSecurity for Networks

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To manage the integration settings of Kaspersky Endpoint Agent with Kaspersky Industrial CyberSecurity for Networks 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 --message-broker=<enable|disable|show> --type=<kics> --compression=<yes|no> --tls=<yes|no> --servers=<address>:<port> [--pinned-certificate=<full path to the TLS certificate file>] [--client-certificate=<full path to the certificate file>] --client-password=<password for the PFX archive>`

   The `--message-broker` command parameters when managing the integration settings between Kaspersky Endpoint Agent and Kaspersky Industrial CyberSecurity for Networks

Parameter	Description

--message-broker=<enable|disable|show>	Required parameter. Allows you to enable, disable, and view status of the integration between Kaspersky Endpoint Agent and Kaspersky Industrial CyberSecurity for Networks. • `--message-broker=<enable>` – enables integration. • `--message-broker=<disable>` – disables integration. • `--message-broker=<show>` – displays integration status of Kaspersky Endpoint Agent with Kaspersky Industrial CyberSecurity for Networks.
`--type=<kics>`	Required parameter. Allows you to specify Kaspersky Industrial CyberSecurity for Networks as the application to integrate with.
`--compression=<yes|no>`	Optional parameter. Allows you to enable or disable compression of data transferred between Kaspersky Endpoint Agent and Kaspersky Industrial CyberSecurity for Networks server. Enabled by default.
`---tls=<yes|no>`	Optional parameter. Allows you to enable or disable trusted connection between Kaspersky Endpoint Agent and Kaspersky Industrial CyberSecurity for Networks. • `--tls=<yes>` – enables trusted connection. • `--tls=<no>` – disables trusted connection.
`--servers=<address>:<port>`	Required parameter. Allows you to specify Kaspersky Industrial CyberSecurity for Networks server data.
`--pinned-certificate=<full path to the TLS certificate file>`	Required parameter, if the `--tls` parameter is passed with the `<yes>` value. Allows you to add a TLS certificate for connecting Kaspersky Endpoint Agent with Kaspersky Industrial CyberSecurity for Networks server.
`--client-certificate=<full path to the certificate file>`	Allows you to add a user certificate for connecting Kaspersky Endpoint Agent with Kaspersky Industrial CyberSecurity for Networks server.
--client-password=<password for the PFX archive>	Allows you to enter the password for the PFX archive, containing a user certificate for connecting Kaspersky Endpoint Agent with Kaspersky Industrial CyberSecurity for Networks server.

Running Kaspersky Endpoint Agent database and module update

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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 of custom database update sources>|kl|ksc]`	Optional parameter. 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.

Starting, stopping and viewing the current application status

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

Protection of application services using the *Protected Process Light (PPL)* technology is implemented in Kaspersky Endpoint Agent.

Protection of application services using the Protected Process Light (PPL) technology can be applied only for the following operating systems:

- For workstations: Windows 10 version 1703 RS2 and above
- For servers: Windows Server 2016 version 1709 and above

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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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 event filtering

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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>
   ```

Managing network isolation

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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.

Only the files with IOC rules can be specified for the IOC Scan task. Files with other types of rules are not supported for the IOC Scan task.

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] [--network=no] [--url=no] [--drives=<all|system|critical|custom>] [--excludes=<list of exclusions>][--scope=<configurable list of folders>] [--retro]`

   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.
--network=no	Optional parameter. The parameter enables threat lookup based on the Network IOC document during IOC Scan. If the <no> value is set for the parameter, Kaspersky Endpoint Agent does not perform threat lookup based on the Network IOC document. If the IOC file contains the terms of the Network IOC document, they are ignored (defined as no match). If the parameter is not passed, Kaspersky Endpoint Agent enables threat lookup based on the Network IOC document only if the Network IOC document is described in the IOC file submitted for scan.
--url=no	Optional parameter.

	The parameter enables threat lookup based on the UrlHistoryItem IOC document during IOC Scan. If the <no> value is set for the parameter, Kaspersky Endpoint Agent does not perform threat lookup based on the UrlHistoryItem IOC document. If the IOC file contains the terms of the UrlHistoryItem IOC document, they are ignored (defined as no match). If the parameter is not passed, Kaspersky Endpoint Agent enables threat lookup based on the UrlHistoryItem IOC document only if the UrlHistoryItem 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.
`--retro`	Optional parameter. The parameter is used to start the task in the **Retrospective IOC scan** mode. In addition to this parameter, you can specify the time interval within which the application performs a retrospective IOC scan using the following parameters: • `--start-time=<interval start date and time>` • `--end-time=<interval end date and time>` Example: `agent.exe --scan-ioc --path=<path to the folder with IOC files> --retro --start-time=2021-05-21T10:30:00Z --end-time=2021-05-24T10:30:00Z`

	If the time interval is not specified, the interval that starts one day before the task was started and ends at the moment the task was launched is used.

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 the 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 where a match was detected.
`Date`	Creation date of the file where indicators of compromise were detected.
`Created`	Only for FileItem. Creation time of the object where indicators of compromise were detected.
`Pid`	Identifier of the process for which indicators of compromise were detected.
`Upid`	Unique identifier of the process for which indicators of compromise were detected.
`ParentPid`	Identifier of the parent object that contains the process for which indicators of compromise were detected.
`Username`	Name of the user who made changes to the object being scanned.
`StartTime`	The start time of the process for which indicators of compromise were detected.

Managing YARA scan

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

YARA scan is a process that you can create and configure manually using the command line interface. YARA files are used to run the scan.

Only the files with YARA rules can be specified for the YARA Scan task. Files with other types of rules are not supported for the YARA Scan task.

To run YARA scan 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-yara [<path the yara file>] [--path=<path to the folder with the yara rules>] [--fast-scan] [--tag-hint=<rule tag>] [--id-hint=<rule ID>] [--max-rules=<maximum number of scan rules>] [--timeout=<stop scan after the specified time in seconds>] [--recursive] [--scan_folders [<list of folders to be scanned>] [--scan-memory] [--scan-process <process name>][--max-size=<file size in bytes>] [--excludes <list of objects to be scanned>] [--includes <list of objects to be scanned>]`

   If the `--scan-yara` command is passed only with the required parameters, Kaspersky Endpoint Agent performs scanning with the default settings.

The scan parameters are described in the following table.

Command parameters when starting and configuring YARA scan

Parameters	Description
`--scan-yara [<full path the yara file>]`	Required parameter. Starts YARA scan on the device. The scan is performed according to the rules in the YARA files with the yara or yar extension. Several values separated by space can be passed to the parameter. At least one `<full path to the yara file>` value must be specified if the --path parameter is not specified. If the --path parameter is also specified in addition to the arguments of the --scan-yara parameter, the scan uses both the files with the YARA rules specified as the arguments and the files from the folder specified by the --path parameter.
`--path=<path to the folder with the yara files>`	Path to the folder with the YARA files that you want to scan. Required parameter, if the `<full path the yara file>` parameter is not specified.
`--fast-scan`	Optional parameter. The parameter starts the fast scan mode. For each scan object, one occurrence of the detected marker is logged, and duplicates of the detected markers are not logged. Usage of this parameter allows you to reduce the time for scanning large files. If the parameter is not passed, standard scan is performed and the duplicates of detected markers are logged.

`--tag-hint=<rule tag>`	Optional parameter. The parameter allows considering only the rules with the specified tag during scan. You can specify only one parameter value. Rules without tags or with tags other than those specified as the parameter value are ignored during scan. If the parameter is not passed, all the rules are considered during scan.
`--id-hint=<rule ID>`	Optional parameter. The parameter allows considering only the rules with the specified ID during scan. You can specify only one parameter value. Rules without IDs or with IDs other than those specified as the parameter value are ignored during scan. If the parameter is not passed, all the rules are considered during scan.
`--max-rules=<maximum number of scan rules>`	Optional parameter. The parameter sets the limit of unique triggered detection rules; scan stops upon exceeding this limit. If the parameter value is not specified or equals to 0, the scan is performed without limitations.
`--timeout=<stop scan after the specified time in seconds>`	Optional parameter. The parameter specifies the scan duration in seconds. The scan will be stopped after the specified time. If the parameter value is not specified or equals to 0, the scan is performed without limitations.
`--recursive`	Optional parameter. The parameter starts recursive scan of subfolders within the [<list of folders to be scanned>] value.
`--scan_folders [<list of folders to be scanned>]`	Optional parameter. The parameter starts scanning of files in the specified list of folders. If the value of the `<list of folders to be scanned>` parameter is not specified, scan is performed recursively for all local drives, except for network, cloud and connected drives.
`--scan-memory`	Optional parameter. The parameter starts memory scan for all running processes.
`--scan-process <process name>`	Optional parameter. The parameter starts memory scan only for specified processes. Standard masks are supported for the `<process name>` value: "`?`" and "`*`".
`--max-size=<file size in bytes>`	Optional parameter. Scan is performed only for the files that do not exceed the specified size. Larger files are skipped during scan.
`--includes <list of objects to be`	Optional parameter.

`scanned>`	The parameter allows you to limit the scan area. You can specify several parameter values separated by a space. Available values: • File name • File path • File name mask • File path mask Passed with the --scan-folders parameter. Example: --scan-folders c:*.* --recursive --includes *.exe c:\temp*.* *.dll – scan is performed for all files with the "exe" and "dll" extensions on the C: drive, and all files in the c:\temp folder will be scanned recursively.
`--excludes <list of objects to be scanned>`	Optional parameter. The parameter excludes the specified files or folders from scan. You can specify several parameter values separated by a space. Available values: • File name • File path • File name mask • File path mask Passed with the --scan-folders parameter. Example: --scan-folders c:*.* --excludes readme.txt c:\trusted*.* *.xml – the readme.txt files, all files from the c:\trusted folder, and all files with the xml extension in the root folder on the C: drive will be skipped during scan.

Return codes of the `--scan-yara` 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.
- `5` – one or more files with YARA rules specified as the parameter value not found.

If the command execution completed successfully (code `0`) and indicators of compromise were detected during the command execution, Kaspersky Endpoint Agent displays the scan results in the command line. The scan results are described in the following table:

Data displayed by the application in the command line when YARA signatures are detected.

`Offset`	Offset in the object scanned by Kaspersky Endpoint Agent.

`Data`	Signatures searched by Kaspersky Endpoint Agent during scanning.
`Object Name`	The name of the scanned object.
`Rule Name`	The name of the rule used during scan.

Managing Execution prevention

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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).

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 Kaspersky Endpoint Agent, you are advised to contact Technical Support. Technical Support specialists will answer your questions about installing and using Kaspersky Endpoint Agent.

Kaspersky provides support for the software solution that includes Kaspersky Endpoint Agent during its lifecycle (see the 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)

An integrated system of comprehensive endpoint protection (for example, mobile devices, computers or laptops) using various security technologies. Endpoint Protection Platform example is Kaspersky Endpoint Security for Business.

EPP application

An application included in a protection system for endpoint devices (Endpoint Protection Platform, or EPP). EPP applications are installed on endpoint devices within the IT infrastructure of an organization (for example, mobile devices, computers, or laptops). An example of an EPP application is Kaspersky Endpoint Security for Windows as part of the EPP solution Kaspersky Endpoint Security for Business.

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

Kaspersky Endpoint Agent is an application that 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.

Telemetry

Data that Kaspersky Endpoint Agent analyzes on the protected device and sends to the *Telemetry collection server*. Telemetry is a list of events that occurred on the protected device.

Telemetry collection server

The type of the server, Kaspersky Endpoint Agent can be integrated with. If integration is configured, Kaspersky Endpoint Agent sends *telemetry* to the server, receives tasks from the server, and generates reports on execution of these tasks.

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.

YARA file

YARA files are the files with the `yara` or `yar` extension that contain YARA rules.

YARA rules are the descriptions of signatures for targeted attacks and intrusions into the organization IT infrastructure. According to these rules, Kaspersky Endpoint Agent scans the objects. If the rule is executed, the analyzer issues an infection verdict with the corresponding details in the log.

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.

Apache and the Apache feather logo are trademarks of The Apache Software Foundation.

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.

Linux – is the registered trademark of Linus Torvalds in the U.S. and other countries.

Microsoft, Active Directory, Excel, Word, PowerPoint, PowerShell, Hyper-V, Win32, Windows, Windows Vista 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.