kaspersky

Kaspersky Endpoint Security for Mac

© 2026 AO Kaspersky Lab

Contents

Kaspersky Endpoint Security overview

What's new in this version

Comparison of Kaspersky Endpoint Security functions depending on the Kaspersky Security Center management tool

Install and uninstall the application

- Distribution kit
- Hardware and software requirements
- Prepare for installation
- Install Kaspersky Endpoint Security
- Prepare the application for use
- Uninstall Kaspersky Endpoint Security

Start the application for the first time

Kaspersky Endpoint Security application interface

- Main application window
- Kaspersky Endpoint Security icon
- Application settings window

About notifications

Kaspersky Endpoint Security application licensing

- About the End User License Agreement
- About the license
- About subscription
- About the license certificate
- About the key
- About the activation code
- About the key file
- About data provision
- Activate Kaspersky Endpoint Security
- View license information
- Manage licenses and subscriptions
- Comparison of application functionality depending on license type for workstations

Perform common tasks

- Open and quit the application
- View the status of computer protection
- View the operating status of installed components
- Disable and resume computer protection
- Use Protection Center
- Perform scan tasks
- Configure the automatic start of a scheduled scan task
- Update application databases
- What to do if file access is blocked
- Restore a file that has been deleted or disinfected by the application
- View the application operation report
- What to do if notification windows appear

Advanced configuration of the application
- Computer protection scope
- File Threat Protection
- Web Threat Protection
- Mail Threat Protection
- Network Threat Protection
- Firewall
- Behavior Detection
- Scan
- Update tasks
- Local tasks
  - External Disks Scan task
- Backup
- Reports
- Managed Detection and Response
- Endpoint Detection and Response (KATA)
- Endpoint Detection and Response Optimum
  - Integration with Endpoint Detection and Response Optimum
  - Scan for indicators of compromise
  - Move file to Quarantine
  - Get file
  - Delete file
  - Start process
  - Terminate process
  - Execution prevention
  - Computer network isolation
  - Cloud Sandbox
- FileVault Disk Encryption
- Password protection
- Exploit Prevention
- Remediation Engine
- Web Control
- Device Control

Participate in Kaspersky Security Network

Check the integrity of application components

Manage the application via Kaspersky Security Center Administration Console
- Deploy Kaspersky Endpoint Security on a corporate network
- Update Kaspersky Endpoint Security version 11.1 or later to version 12.2
- Prepare for remote installation of Kaspersky Endpoint Security
  - Install the Kaspersky Endpoint Security administration plug-in
  - Install Network Agent locally
  - Install Network Agent using Apple Remote Desktop
  - Install Network Agent using Kaspersky Security Center
  - Install Network Agent using the SSH protocol
  - Uninstall Network Agent locally

- Manage Network Agent from the command line
  - Start/stop Network Agent on a remote computer
  - Check the connection between a client computer and Administration Server manually. Klnagchk utility
  - Connect a remote computer to Administration Server manually. Klmover utility
  - Uninstall Network Agent
- Install and uninstall Kaspersky Endpoint Security
  - Install the application using the SSH protocol
  - Install the application using Kaspersky Security Center
  - Create an installation package
  - Uninstall the application using Kaspersky Security Center
- Start and stop the application via Kaspersky Security Center
- Create and manage tasks
  - Create tasks
  - Start and stop tasks manually
  - Import and export tasks
  - View tasks
  - Manage task-specific settings
- Create and manage policies
  - Create a policy
  - View the list of policies
  - Configure policy settings
  - Change the policy status
  - Export a policy to a KLP file
  - Import a policy from a KLP file
- Create and manage policy profiles
- Generate a report on detected objects
- Get a recovery key for an encrypted disk

Remote administration of the application via Kaspersky Security Center Web Console and Cloud Console

- Install the Kaspersky Endpoint Security web plug-in
- Create policies
  - Configure Advanced Threat Protection settings
  - Configure Essential Threat Protection settings
    - Configure File Threat Protection settings
    - Configure Web Threat Protection settings
    - Configure Network Threat Protection settings
  - Configure Security Controls
  - Configure Data Encryption
  - Configure Detection and Response settings
    - Configure Managed Detection and Response
    - Configure Endpoint Detection and Response
    - Configure Endpoint Detection and Response (KATA)
  - Configure Update settings
  - Configure Additional Settings

- Create tasks
  - Configure the Scan task settings
  - Configure the Add key task settings
  - Configure the Update task
- Get a recovery key for an encrypted drive

Manage the application from the command line
- View command line help
- Run malware scan
- Update the application
- Roll back the last update
- Start/stop a component or task
- View status and statistics of a component or task
- Export protection settings
- Activate the application
- Install the system extension
- Configure network connections
- Remove license keys
- Return codes of the command line
- Quit the application
- Uninstall the application
- Detection and Response management commands
  - Manage Execution prevention
  - Manage Network isolation

Contact Technical Support
- How to get technical support
- Technical support via Kaspersky CompanyAccount
- Acquire information for Technical Support
- Use a trace file
- Create a trace file

Sources of information about the application

Appendices
- Known issues and limitations
- List of objects scanned by extension
- Masks in paths to files and folders
- IOC file requirements
- Supported script interpreters for Execution prevention
- How to add the Kaspersky Endpoint Security certificate to the Mozilla Firefox certificate storage

Information about third-party code

Trademark notices

Kaspersky Endpoint Security overview

The Kaspersky Endpoint Security application protects computers running macOS against malware and other computer security threats.

File Threat Protection

File Threat Protection safeguards the computer's file system in real time by intercepting and analyzing any attempts to access files. Learn more.

Web Threat Protection

Web Threat Protection secures information sent and received by the computer over the HTTP and HTTPS protocols in Safari, Google Chrome™, and Firefox™. Learn more.

Mail Threat Protection

Mail Threat Protection scans the attachments of incoming and outgoing email messages for malware and other threats. The component provides computer protection with the help of anti-malware databases, the Kaspersky Security Network cloud service, and heuristic analysis. Learn more.

Network Threat Protection

Network Threat Protection prevents intrusions into the operating system. This component protects against cyberattackers (who use port scanning and brute-force attacks) and the malware they install (including malware that tries to send personal data to criminals). Learn more.

Firewall

Firewall blocks unauthorized connections to the computer while working on the internet or local network. Firewall also controls the network activity of applications on the computer. This allows you to protect your corporate LAN from identity theft and other attacks. The component provides computer protection with the help of anti-malware databases, the Kaspersky Security Network cloud service, and predefined network rules. Learn more.

Behavior Detection

The Behavior Detection component receives information about the actions of applications on your computer and provides it to other protection components to improve their performance. It also performs the selected action as a response to malware activity. Learn more.

Exploit Prevention

The Exploit Prevention component detects program code that takes advantage of vulnerabilities on the computer to exploit administrator privileges or to perform malicious activities. Learn more.

Remediation Engine

The Remediation Engine lets Kaspersky Endpoint Security roll back actions that have been performed by malware in the operating system. Learn more.

Scan

The Kaspersky Endpoint Security application detects and neutralizes malware and other computer security threats on demand in the specified scan scope. Kaspersky Endpoint Security can run a full scan of the computer, a quick scan of critical areas, and a scan of the specified scope. Learn more.

Update

Kaspersky Endpoint Security updates application databases and modules from Kaspersky update servers, distribution points, or other sources specified by your system administrator and creates backup copies of all updated files to allow a rollback of the last update. Learn more.

Backup

Kaspersky Endpoint Security creates a backup copy of infected files prior to any attempt to disinfect or delete them, making it possible for you to restore them. Learn more.

Reports

Kaspersky Endpoint Security generates reports about events and actions involving application components. Learn more.

Notifications

Kaspersky Endpoint Security uses notifications to inform you about certain events in the operation of Kaspersky Endpoint Security. Notifications can be accompanied by sound. Learn more.

Protection Center

Kaspersky Endpoint Security displays protection status messages in Protection Center. Protection Center shows information on the status of computer protection and how to eliminate computer security problems and threats. Learn more.

Remote management of the application via Kaspersky Security Center

You can remotely manage protection of computers with Kaspersky Endpoint Security installed: receive information on the current computer protection status, remotely fix issues, respond to computer security threats, enable or disable protection components (File Threat Protection, Web Threat Protection, Network Threat Protection, Behavior Detection), enable or disable Web Control, Managed Detection and Response, Endpoint Detection and Response, and Endpoint Detection and Response (KATA), run scan tasks, update application databases, run startup disk encryption, and manage Kaspersky Endpoint Security licenses and subscriptions. You can use the following tools to manage Kaspersky Endpoint Security:

- Kaspersky Security Center Administration Console. Learn more.
- Kaspersky Security Center Web Console and Cloud Console. Learn more.

Note: The functionality supported by Kaspersky Endpoint Security depends on which management tool you use.

FileVault Disk Encryption

Kaspersky Endpoint Security allows FileVault encryption to be managed remotely. Encryption prevents unauthorized users from accessing sensitive data stored on the startup disk of the user's computer.

Note: The FileVault Disk Encryption feature is available in Kaspersky Security Center 10 SP3 or later. For more information, contact Kaspersky Technical Support.

Web Control

You can remotely manage access to websites that users visit. You can allow or block access to specific web addresses or groups of web addresses. Also you can allow or block access to certain categories of websites based on their content. Learn more.

Device Control

Device Control manages user access to devices that are installed on or connected to the computer. This lets you protect the computer from infection when such devices are connected, and prevent loss or leaks of data. Learn more.

Managed Detection and Response

The Managed Detection and Response component facilitates interaction with the Kaspersky Managed Detection and Response service that continuously detects and eliminates security threats aimed at your organization. Learn more.

Endpoint Detection and Response

The Endpoint Detection and Response component facilitates interaction with the Kaspersky Endpoint Detection and Response solution. This solution combines automatic detection of threats with the ability to react to these threats to counteract advanced attacks including new exploits, ransomware, fileless attacks, as well as methods using legitimate system tools. Learn more.

Endpoint Detection and Response (KATA)

The Endpoint Detection and Response (KATA) component facilitates interaction with the Kaspersky Anti Targeted Attack Platform solution. This solution promptly detects advanced threats, such as targeted attacks, advanced persistent threats, zero-day attacks, and others. Learn more.

What's new in this version

This Help applies to Kaspersky Endpoint Security for Mac version 12.2.

Kaspersky Endpoint Security offers the following new features and improvements:

- The new macOS 27 Golden Gate is now supported.
- The new macOS 26 Tahoe is now supported.
- We added the new Mail Threat Protection, Device Control, Firewall, Remediation Engine, and Exploit Prevention components.
- Now you can activate the Managed Detection and Response component from the Kaspersky Endpoint Security application.
- Improved the visibility of response actions for alert details.
- Now you can manage the Behavior Detection component in the Web Console.
- We added alert summaries.
- Now you will be notified that an object is a critical system one before any response actions are performed.
- Now you can edit IOC files directly in the Web Console when creating or editing IOC Scan task settings.
- Now you can move detected objects to Quarantine from the alert details.
- We added warnings for restricted actions for the Network Isolation task.
- General bug fixes and improvements.

Comparison of Kaspersky Endpoint Security functions depending on the Kaspersky Security Center management tool

The functionality supported by Kaspersky Endpoint Security depends on which management tool you use (see the table below).

You can use the following tools to manage Kaspersky Endpoint Security:

- Kaspersky Security Center Administration Console. A Microsoft Management Console (MMC) snap-in installed on the Kaspersky Security Center administrator's workstation.
- Kaspersky Security Center Web Console. A component of Kaspersky Security Center that is installed on the Administration Server. You can work with the Web Console using a browser on any computer that has access to the Administration Server.
- Kaspersky Security Center Cloud Console. The cloud version of Kaspersky Security Center.

Comparison of Kaspersky Endpoint Security features

Feature	Kaspersky Security Center		
	Administration Console	Web Console	Cloud Console
Advanced Threat Protection			
Kaspersky Security Network	✓	✓	✓
Behavior Detection	✓	✓	
Exploit Prevention	✓	✓	
Remediation Engine	✓	✓	
Essential Threat Protection			
File Threat Protection	✓	✓	✓
Web Threat Protection	✓	✓	✓
Network Threat Protection	✓	✓	✓
Mail Threat Protection	✓	✓	
Firewall	✓	✓	
Security Controls			
Web Control	✓	✓	✓
Device Control	✓	✓	
Data Encryption			
FileVault Disk Encryption	✓	✓	✓
Recovery key	✓	✓	✓
Detection and Response			
Managed Detection and Response	✓	✓	✓
Endpoint Detection and Response		✓	
Endpoint Detection and Response (KATA)	✓	✓	✓
Tasks			

Feature	Kaspersky Security Center		
	Administration Console	Web Console	Cloud Console
Add key	✓	✓	✓
Update	✓	✓	✓
Quick Scan	✓	✓	
Rollback	✓	✓	✓
Scan	✓	✓	✓

Install and uninstall the application

Distribution kit

The distribution kit includes the Kaspersky Endpoint Security installation package, which contains the following files:

- Files that are required to install the application in any of the available ways.
- The license_<loc>.txt file with the End User License Agreement.

  The End User License Agreement specifies the terms of use of the application.

Unpack the zipped installation package to access its files.

Hardware and software requirements

Kaspersky Endpoint Security has the following hardware and software requirements:

- Processor type: Intel, Apple silicon
- 4 GB of memory (RAM)
- 5 GB of free disk space
- Operating system macOS 13, 14, 15, 26, or 27
- Internet connection

Supported browsers:

- Safari
- Chrome
- Firefox

Kaspersky Endpoint Security is compatible with the following virtualization tools:

- Parallels Desktop 16 for Mac Business Edition or later
- VMware Fusion™ 11.5 Professional
- VMware Fusion 12 Professional
- VMware Fusion 13 Pro

MDM profiles can be deployed with the Jamf and Apple servers. If you use other servers, see the article on the Technical Support website (Knowledge Base).

You can manage Kaspersky Endpoint Security remotely via Kaspersky Security Center. Kaspersky Security Center 14.2 or later is required for managing Kaspersky Endpoint Security using the administration plug-in for Kaspersky Security Center Administration Console and the web plug-in for Kaspersky Security Center Web Console.

Note: To manage Kaspersky Endpoint Security for Mac 12.2 via Kaspersky Security Center, you must install Network Agent version 15 on remote computers.

Prepare for installation

Before installing the application on your computer, it is recommended to do the following:

- Make sure that your computer meets the hardware and software requirements.
- Remove Kaspersky Internet Security for Mac or any other anti-malware applications to avoid system conflicts and maximize system performance.

Note: Before installing Kaspersky Endpoint Security remotely, we recommend that you download the KES_for_macOS11_and_later.zip archive from Kaspersky Technical Support website and apply the KES_for_macOS11_and_later_profile.mobileconfig configuration profile on the client computer using Apple Remote Management tools. This will allow Kaspersky Endpoint Security to get the following: permissions to install the kernel extension and the system extension, full disk access, and permissions to configure network connections. To learn more about the configuration profile and other options, visit the Technical Support website.

Install Kaspersky Endpoint Security

Important: Kaspersky experts recommend installing Kaspersky Endpoint Security only as described in this Help.

You can install Kaspersky Endpoint Security in one of the following ways:

- Locally, from the distribution kit downloaded from the Kaspersky website.
- Remotely using Apple Remote Desktop.
- Remotely via Kaspersky Security Center Administration Console.
- Remotely via Kaspersky Security Center Web Console or Kaspersky Security Center Cloud Console.

  For detailed information about deploying Kaspersky applications using Kaspersky Security Center Web Console, see the Kaspersky Security Center Help. For detailed information about deploying Kaspersky applications using Kaspersky Security Center Cloud Console, see the Kaspersky Security Center Cloud Console Help.

Perform a standard installation of Kaspersky Endpoint Security

1. Unpack the ZIP archive from the distribution kit.
2. Open the .dmg file from the contents of the unpacked archive.
3. In the window that opens, double-click **Install Kaspersky Endpoint Security**.

   The Kaspersky Endpoint Security Installation Assistant opens.
4. Click **Install**.
5. Follow the steps of the Installation Assistant to complete the installation.

When the installation is finished, Kaspersky Endpoint Security starts automatically. You don't have to restart your computer.

Note: If this installation method is used, the Endpoint Detection and Response (KATA), Endpoint Detection and Response (Optimum), and Cloud Sandbox components are not installed.

Perform a custom installation of Kaspersky Endpoint Security

1. Unpack the ZIP archive from the distribution kit.
2. Open the .dmg file from the contents of the unpacked archive.
3. In the window that opens, double-click **Install Kaspersky Endpoint Security**.

   The Kaspersky Endpoint Security Installation Assistant opens.
4. Click **Customize**, select or deselect checkboxes next to components that you don't want to install and click **Continue**.
5. Follow the steps of the Installation Assistant to complete the installation.

When the installation is finished, Kaspersky Endpoint Security starts automatically. You don't have to restart your computer.

Install Kaspersky Endpoint Security remotely using Apple Remote Desktop

1. On your Mac, choose **Apple menu** > **System Settings** > **General** > **Sharing**.
2. Select the **Remote Management** checkbox.
3. On another Mac that you want to be a server, install Apple Remote Desktop. For more information on Apple Remote Desktop, refer to Apple Support.
4. Open Apple Remote Desktop.
5. In the **Remote Desktop** window, click **Scanner** on the left and select the devices on which you want to install Kaspersky Endpoint Security.
6. Click **Install**.
7. In the prompt for administrator credentials, enter an administrator name and password and click **Add**.

8. Click + and select the .dmg file with the Kaspersky Endpoint Security installation package.
9. Click **Install**.

Installation of Kaspersky Endpoint Security starts on the selected devices.

Prepare the application for use

After Kaspersky Endpoint Security is installed, you can do the following:

- Activate Kaspersky Endpoint Security. When the application is activated, Kaspersky Endpoint Security starts protecting your computer, you can regularly update application databases and modules, perform malware scan tasks, and send requests to Technical Support.

  The Managed Detection and Response component is activated separately in the Kaspersky Security Center Administration or Web Console.

  If the Endpoint Detection and Response component is not supported by your current license, you need to activate Kaspersky Endpoint Detection and Response separately.
- Assess the status of computer protection.
- Update Kaspersky Endpoint Security.
- Scan your computer for malware.

Uninstall Kaspersky Endpoint Security

1. Open the DMG file of the application distribution kit.
2. In the window with the contents of the distribution kit, double-click **Uninstall Kaspersky Endpoint Security**.

   The Kaspersky Endpoint Security uninstaller starts.
3. In the uninstaller window, click **Uninstall**.
4. In the prompt for administrator credentials, enter an administrator name and password and confirm that you want to uninstall Kaspersky Endpoint Security.

   Uninstallation of Kaspersky Endpoint Security starts.
5. Read the information about completion of uninstallation and click **Quit** to quit the uninstaller.

Kaspersky Endpoint Security is now uninstalled from your computer. You don't have to restart your computer after uninstalling the application.

Start the application for the first time

Kaspersky Endpoint Security starts on your computer right after installation. To protect your Mac right away, the application prompts you to perform the basic setup:

- Grant the necessary permissions to Kaspersky Endpoint Security to protect your Mac against malware, network attacks and internet threats.

  For more information about the permissions you are granting, click ?.

- Activate Kaspersky Endpoint Security.

Note: An internet connection is required for basic setup of Kaspersky Endpoint Security.

Start Kaspersky Endpoint Security for the first time

1. In the **Essential Protection** window, do the following actions to ensure that File Threat Protection and Web Threat Protection function properly:

   - If you want the Kaspersky Endpoint Security application to work properly, allow the application to scan every file on your Mac. To do this, click **Allow** next to the **Full disk access** item and follow the instructions on the screen.

   - If you want Kaspersky Endpoint Security to inspect URLs and network packets before they can harm your Mac, install the system extension. To do this, click **Install** next to the **System extension** item and follow the instructions on the screen.

   - If you want the system extension to work properly, allow network content filtering. To do this, click **Allow** next to the **Network content filtering** item and follow the instructions on the screen.

   - If you want Kaspersky Endpoint Security to search for malware and internet threats in encrypted HTTPS traffic, install the trusted certificate. To do this, click **Install** next to the **Trusted certificate** item and follow the instructions on the screen.

   Important: The Kaspersky Endpoint Security application will not work properly without granting these permissions. You must grant all permissions in the **Essential Protection** window.

2. Click **Continue**.

The main application window opens.

Kaspersky Endpoint Security application interface

Main application window

Open the main application window

In the menu bar, click the application icon and choose **Kaspersky Endpoint Security**.

The main application window of Kaspersky Endpoint Security contains interface elements that provide access to the main functions of the application.

The main application window is divided into two parts:

- The left part contains the sidebar, which lets you navigate the application and quickly access its main functions.
- The central part displays the contents of the section selected in the sidebar and lets you manage data.

Sidebar

The sidebar of the main application window has the following options:

Monitoring	Click to open the **Monitoring** page, which provides information on what Kaspersky Endpoint Security is doing to protect your computer.
Protection Center	Click to view your computer protection status. Learn more.
Security	Click to view the operating status of installed components. Learn more.
Scan	Click to manage scan tasks. Learn more.
Update	Click to manage update tasks. Learn more.
License	Click to activate the application or view information about your license. Learn more.

Controls of the **Monitoring** page

The **Monitoring** page displays the protection status indicator, provides information on what Kaspersky Endpoint Security is doing to protect your computer, and contains the following controls.

Protection Center	Informs you about computer protection problems. Learn more.
Reports	Allows you to view events that occurred during operation of the application, individual components, and tasks. Learn more.
Backup	Allows you to view a list of saved copies of infected files that the application has deleted. Learn more. Learn more.

Threat Detection	Allows you to view information about threat detection technologies applied by Kaspersky Endpoint Security and the number of threats detected by these technologies.
Kaspersky Security Network	Displays the status of the connection between Kaspersky Endpoint Security and Kaspersky Security Network, and also global Kaspersky Security Network statistics.

Kaspersky Endpoint Security icon

As soon as Kaspersky Endpoint Security is installed, the Kaspersky Endpoint Security icon appears in the menu bar. When the application is activated, the application icon shows the status of the application. If the application icon is active ( ), it means that all or some of the protection components are enabled. If the application icon is inactive ( ), then all of the protection components are disabled.

Open the application icon menu

In the menu bar, click the application icon.

By default, the application icon is always displayed in the menu bar. You can remove the application icon from the menu bar.

Remove the application icon from the menu bar

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.

2. On the **Interface** tab, in the **Application icon** section, deselect the **Show in menu bar** checkbox.

When you open the application window, the application icon also appears in the **Dock**.

From the application icon menu, you can access the main application window and perform the following actions:

- Disable computer protection.
- Resume computer protection.
- Open Protection Center.
- Start Quick Scan.
- Run an update.
- Open the application settings window.
- Quit Kaspersky Endpoint Security.

Application settings window

Open the application settings window

Do one of the following:

- In the menu bar, click the application icon and choose **Settings**.
- In the menu bar, click **Kaspersky Endpoint Security** > **Settings**.
- If Kaspersky Endpoint Security is running, click the application icon in the **Dock** and choose **Settings**.

Application settings can be accessed quickly using the following tabs in the upper part of the settings window:

- **Essential**. On this tab, you can enable or disable computer protection and configure File Threat Protection, Web Threat Protection, and Network Threat Protection settings.
- **Scan**. On this tab, you can configure the settings of scan tasks and scheduled startup of scan tasks.
- **Threats**. On this tab, you can select the categories of objects to be detected, create Trusted Zone, and configure Backup settings.
- **Advanced**. On this tab, you can join or opt out of participating in Kaspersky Security Network.
- **Update**. On this tab, you can configure application update settings or roll back to the previous version of application databases.
- **Interface**. On this tab, you can configure settings for the Kaspersky Endpoint Security icon, notifications, and reports, and enable or disable the logging of debugging information in a trace file.

Using the  button, you can block users without administrator rights from editing the Kaspersky Endpoint Security settings. This button is in the lower part of the application settings window. To edit the settings, you must enter the administrator's credentials.

Clicking the ? button opens the Kaspersky Endpoint Security Help, which describes all the settings in the current application window. You can also open the help topic for the active application window by selecting **Open Help for This Window** in the **Help** menu.

About notifications

Kaspersky Endpoint Security displays notifications to inform you of application events. Depending on the version of the operating system installed on the computer, notifications appear in the operating system's Notification Center. The appearance of notifications depends on the options set in the operating system's Notification settings.

Kaspersky Endpoint Security events are divided into three types according to their importance:

- *Critical* – events that pose a dangerous threat to computer security (detection of malicious objects, vulnerabilities, problems with Kaspersky Endpoint Security). Critical events require your immediate attention. We recommend that you not disable notifications about critical events.
- *Important* – events that do not require your immediate attention but may pose a threat to computer security in the future.
- *Informational* – events reported for your information.

Disable notifications

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.

2. On the **Interface** tab, in the **Notifications** section, deselect the **Enable notifications** checkbox.

Enable logging non-critical events

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.

2. On the **Interface** tab, in the **Reports** section, select the **Log non-critical events** checkbox to receive notifications about informational Kaspersky Endpoint Security events.

Regardless of whether notifications are enabled or disabled, the application reports include information about events that occur while Kaspersky Endpoint Security is running.

Notifications can be accompanied by sound (for example, notifications about a detected malware). You can disable the sound alert.

Logging of non-critical events considerably increases the total size of the report file. Note, that this setting applies only to File Threat Protection.

Disable sound alerts that accompany notifications

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.

2. On the **Interface** tab, in the **Notifications** section, deselect the **Turn on alert sounds on malware detection** checkbox.

If an action is required in response to an event, Kaspersky Endpoint Security displays a notification window. For example, when the application detects a malicious object, it prompts you to delete or disinfect the object. The notification window disappears from the screen only after one of the actions is selected.

Kaspersky Endpoint Security application licensing

About the End User License Agreement

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

Important: Carefully read the License Agreement before you start using the application.

You can view the terms of the End User License Agreement by using the following methods:

- During installation of Kaspersky Endpoint Security
- By reading the license.txt document in the application installation folder

By installing Kaspersky Endpoint Security, you confirm that you understand and accept the terms of the End User License Agreement. If you don't accept the terms of the End User License Agreement, cancel installation of Kaspersky Endpoint Security and don't use the application.

About the license

A *license* is a time-limited right to use Kaspersky Endpoint Security, granted under the terms of the signed License Contract (End User License Agreement).

The scope of services and validity period depend on the license under which the application is used.

The following license types are provided:

- *Trial*

  A free license intended for trying out the application. A trial license usually has a short term.

  When a trial license expires, all Kaspersky Endpoint Security features become disabled. To continue using the application, you need to purchase a commercial license.

  You can use the application under a trial license for only one trial period.

- *Commercial*

  A paid license.

  When a commercial license expires, key features of the application become disabled. To continue using Kaspersky Endpoint Security, you must renew your commercial license. After a commercial license expires, you cannot continue using the application and must remove it from your device.

  We recommend renewing your license before it expires, to ensure uninterrupted protection against all security threats.

About subscription

A *subscription for Kaspersky Endpoint Security* is a purchase order for the application with specific parameters (expiry date, number of devices protected). You can order a subscription for Kaspersky Endpoint Security from your service provider (such as your ISP). You can manage your subscription in the member area on the service provider's website. For example, you can renew or cancel your subscription, reduce its term, or change the number of devices protected under your subscription.

A subscription can be limited (for one year, for example) or unlimited (without an expiration date). To keep Kaspersky Endpoint Security working after expiration of a limited subscription term, you have to renew it manually. An unlimited subscription is renewed automatically as long as you have paid the service provider in advance.

If you use the application under a limited subscription, when the subscription expires you will be given a grace period to renew your subscription. The application remains functional during the grace period.

After your subscription to updates expires and after the grace period for subscription renewal ends, Kaspersky Endpoint Security remains functional but stops updating application databases.

After your subscription to updates and protection expires and after the grace period for subscription renewal ends, Kaspersky Endpoint Security stops protecting your computer.

To use Kaspersky Endpoint Security under subscription, you have to add the activation code received from the service provider. When you use the application under subscription, you cannot use a different activation code for renewing your subscription. You can apply a different activation code only after the subscription expires or if you cancel the subscription. To cancel your subscription, contact the service provider from which you bought Kaspersky Endpoint Security.

Note: A different subscription activation code can be applied only when the active key is deleted. The subscription doesn't have a key file. You can't add the subscription as a reserve key. A reserve key cannot be added when the subscription is used.

If you are already using Kaspersky Endpoint Security under a valid license but want to use the application under subscription instead, remove the current active key so that you can activate the application using a subscription key. The activation code that was previously used to activate the application on this computer can be used on a different computer.

Note: Possible subscription options may vary with each service provider. Some service providers may also choose not to provide a grace period for renewing subscriptions.

About the license certificate

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

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

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

About the key

A *key* is a sequence of bits that you can apply to activate and then use the application in accordance with the terms of the End User License Agreement. Keys are generated by Kaspersky specialists.

You can add a key to the application using one of the following methods: by applying a *key file* or by entering an *activation code*. The key is displayed in the application interface as a unique alphanumeric sequence after you add it to the application.

The key may be blocked by Kaspersky in case the terms of the License Agreement have been violated. If the key has been blocked, you need to add another one if you want to use the application.

A key can be active or reserve.

An *active key* is a key that is currently used by the application. An active key can be added for a trial or commercial license or a subscription. The application cannot have more than one active key.

A *reserve key* is a key that entitles the user to use the application, but is not currently in use. The reserve key automatically becomes active when the license associated with the current active key expires. A reserve key can be added only if an active key has already been added.

A trial license key can be added as the active key. A key for the trial license cannot be added as the reserve key. A reserve key cannot be added when the trial license key is active.

About the activation code

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

To activate the application by using the activation code, you need internet access in order to connect to Kaspersky activation servers.

If you have lost your activation code after installing the application, contact the Kaspersky partner from whom you purchased the license.

About the key file

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

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

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 your key file, perform any of the following actions:

- Contact the license seller.
- Receive a key file through Kaspersky website by using your available activation code.

About data provision

End User License Agreement

When activating Kaspersky Endpoint Security by the activation code, in order to verify legitimate use of the application and to provide statistical information on the distribution and use of Kaspersky products, you agree to automatically provide the following information during use of Kaspersky Endpoint Security:

- The type, version and localization of the installed Software.
- The versions of the installed updates.
- The identifier of the computer and the identifier of the Software installation on the computer.
- The activation code and unique activation identifier for the current license.
- The type, version and word size of the operating system.
- The name of the virtual environment when the Software is installed in a virtual environment.
- The identifiers of the Software components that are active at the time the information is provided.
- The supported data source.
- Timeout.
- Date and time on the user's computer.

- Protocol version.
- Protocol content type.
- Protocol content length.
- The type of data compression used.
- The type of signature on the activation ticket.
- Regional Activation Center identifier.
- Activation code hash calculated using the SHA1 algorithm.
- Ticket body hash calculated using the SHA1 algorithm.
- License ticket creation date and time.
- License activation identifier.
- Current license ticket identifier.
- License ticket sequence identifier.
- Date and time of license activation.
- Date and time of license expiration.
- License status.
- License version.
- The unique identifier of the user's computer.
- License ticket header version.
- Application name.
- Transferred data type.
- Transferred data scheme version.
- The full version of the operating system.
- Description of the used virtual machine.
- List of IDs for compatible applications.

When you use Kaspersky update servers to download the updates, in order to increase the efficiency of the update procedure, you agree to periodically provide the following information for the application identification during database and module updates:

- Software ID (AppID).
- Active license ID.

- Unique software installation ID (InstallationID).
- Unique update task launch ID (SessionID).
- Version of application (BuildInfo).

Kaspersky Security Network (KSN) Statement

Use of the KSN may increase the Software's speed of reaction to information and network security threats. The declared purpose is achieved by:

- Determining the reputation of scanned objects.
- Identifying information security threats that are new and challenging to detect, and their sources.
- Taking prompt measures to increase the protection of the data stored and processed by a user with the computer.
- Reducing the likelihood of false positives.
- Increasing the efficiency of application components.
- Investigating an infection of a user's computer.
- Improving the performance of the Kaspersky products.
- Receiving reference information about the number of objects with known reputation.
- Promptly identifying and correcting errors related to the installation, removal, and updating of the product.

During use of the KSN, Kaspersky will automatically receive and process data. The data transmitted by the user depends on the type of license installed and the Kaspersky Security Network use settings specified.

If you use a license for 1-4 nodes, Kaspersky will automatically receive and process the following data during use of the Kaspersky Security Network:

- Information about the license used: the type and validity period of the license, number of days till license expiration, identifier of the partner from whom the license was purchased, Regional Activation Center identifier, checksum of the activation code, ticket body hash calculated using the SHA1 algorithm, license ticket creation date and time, license information identifier, license ticket identifier, license ticket sequence identifier, unique identifier of the user's computer, date from which the license ticket is valid, date to which the license ticket is valid, license ticket current state, ticket header version, license version, ticket header signature certificate identifier, checksum of the key file, ticket header signer serial number, authentication token.

- Full version of installed Software; type of installed Software; Software update ID; ID of reputation service; protocol type ID; ID of a regional activation center; version of list of revoked Software service's decisions; ID of the triggered record in the Software's anti-virus databases; timestamp of the triggered record in the Software's anti-virus databases; type of the triggered record in the Software's anti-virus databases; unique ID of the instance of application installation on the computer; license activation date; license expiration date; license identifier; status of the license used by the Software; checksum type for the object being processed; name of the detected malware or legitimate software that can be used to damage the user's device or data; checksum of the object being processed; checksum of the Software activation code; full version of the Software; unique device ID; Software ID; checksum of the Software key file; ID of the information model used to provide the Software license; identifier of the certificate used to sign the Software license ticket header; the Software license ticket create date and time; the Software license ticket checksum; the Software license ticket version; the Software activation code version; format of the data in the request to Rightholder infrastructure; current license ticket ID; the Software component ID; the result of the Software action; error code; accessed address of the web service (URL, IP); port number; web address of the source of the web service request (referrer); public key of the certificate; digital certificate thumbprint of the scanned object and hashing algorithm.

If you use a license for 5 or more nodes, Kaspersky will automatically receive and process the following data during use of the Kaspersky Security Network:

- Information about the version of the operating system (OS) and service packs installed on the computer, version and checksums (MD5, SHA2-256, SHA1) of the OS kernel file, parameters of the OS run mode; OS version, OS build number, OS update number, OS edition, extended information about the OS edition; OS Service Pack version; date and time of the OS launch; processing delay time of the event about OS action in the behavioral analysis subsystem; number of delayed OS action events of the current type; processing delay time of the event about OS action in the proactive defense subsystem; number of processed OS action events; number of processed synchronous OS action events; total delay of all OS action events of the current type; processing delay time of the event about OS action in the persistent event storage subsystem; total delay of all OS action events; number of waiting synchronous OS action events; date and time of received event of an action in the OS.

- Information about the failed last OS reboot: number of failed reboots.

- Information about the Rightholder's installed application and the anti-virus protection status: Software installation ID (PCID); Software database record version; unique identifier of the instance of application installation on the computer, application type, ID of application type, the full version of the application installed, the identifier of the application settings version, the identifier of the computer type, the unique identifier of the computer on which the application is installed, the unique User identifier in the Rightholder's services, locale language and operation state, version of the installed Software components and their operation state, version of the protocol used to connect with the Rightholder's services; full version of installed Software; type of installed Software; Software update ID; ID of reputation service; protocol type ID; ID of a regional activation center; version of list of revoked Software service's decisions; ID of the triggered record in the Software's anti-virus databases; timestamp of the triggered record in the Software's anti-virus databases; type of the triggered record in the Software's anti-virus databases; Unique ID of the instance of application installation on the computer; license activation date; license expiration date; license identifier; status of the license used by the Software; checksum type for the object being processed; name of the detected malware or legitimate software that can be used to damage the user's device or data; checksum of the object being processed; checksum of the Software activation code; full version of the Software; Software ID; checksum of the Software key file; ID of the information model used to provide the Software license; identifier of the certificate used to sign the Software license ticket header; the Software license ticket create date and time; the Software license ticket checksum; the Software license ticket version; the Software activation code version; format of the data in the request to Rightholder infrastructure; current license ticket ID; the Software component ID; the result of the Software action; error code; accessed address of the web service (URL, IP); port number; web address of the source of the web service request (referrer); number of update-apply cycles for anti-virus databases; date and time when the anti-virus databases were last updated and applied; release date and time of the Software's databases; version of the Software's component; Software update ID; type of the installed Software; date and time of System Watcher start; installation date and time for the Software; probability of sending statistics by System Watcher; code of the event that took longer than the standard time to process by System Watcher; database processing time of the event that took longer than the standard time to process by System Watcher; maximum allowed time for processing an event by System Watcher; processing time of the event that took longer than the standard time to process by System Watcher; total number of events that took longer than the standard time to process by System Watcher.

- Information about all processed objects and operations: Software verdict on the object being processed; directory code; size of the object being processed; checksum (SHA256) of the object being processed; number of the detected software in the System Watcher context; date and time of detecting software by System Watcher; detect characteristics; ID of the triggered record in the Software's anti-virus databases; reason of detecting software by System Watcher; checksum (MD5) of the object being processed; result of the module integrity check; name of the object being processed; type of the triggered Software anti-virus databases record; path to the object being processed; the name of the scanned object; the date and time of the scan; the URL- and Referrer addresses from which it was downloaded; the size of scanned files and the paths to them; the archive sign; the date and time of the file's creation; the name, size and checksums (MD5, SHA2-256) of the packer (if the file was packed); the file's entropy; the file's type; the file type code; the executable file sign, ID and format; the object's checksum (MD5, SHA2-256); the type and value of the object's supplementary checksum; data about the object's digital signature (certificate): data on the certificate's publisher, number of starts of the object since the last statistics delivery, ID of the application's scanning task, the means of receiving information about the object's reputation, the value of the target filter, technical parameters of the applicable detection technologies; path to the object being processed; directory code.

- For executable files: the entropy of the file sections, reputation verification flag or file signature flag, name, type, ID type, checksum (MD5) and the size of the application that was loaded by the object being validated, the application path and template paths, an attribute indicating presence in the Autorun list, date of entry, the list of attributes, name of the packer, information about the digital signature of the application: the publisher certificate, the name of the uploaded file in the MIME format, file build date and time.

- Information about the applications launched and their modules: checksums (MD5, SHA2-256) of running files, size, attributes, creation date, name of the packer (if the file was packed), names of files, information about processes running on the system (process ID (PID), process name, information about the account the process was started from, the application and command that started the process, the full path to the process's files, and the starting command line, a description of the application that the process belongs to (the name of the application and information about the publisher), as well as the digital certificates being used and information needed to verify their authenticity or information about the absence of a file's digital signature), and information about the modules loaded into the processes: their names, sizes, types, creation dates, attributes, checksums (MD5, SHA2-256, SHA1), the paths to them, PE-file header information, names of packers (if the file was packed), information about the availability and validity of these statistics, identifier of the mode for generating the statistics being sent.

- If threats or vulnerabilities are detected, in addition to information about the detected object, information is provided about the identifier, version, and type of the record in the anti-virus database, the name of the threat based on the Kaspersky classification, the date and time of the last update of the anti-virus database, executable file name, the checksum (MD5) of the application file that requested the URL where the threat was detected, the IP address (IPv4 or IPv6) of the detected threat, the vulnerability identifier and its threat level, the URL and Referrer of the web page where the vulnerability was detected.

- If a potentially malicious object is detected, information is provided about data in the processes' memory.

- Network attack information: IP address of the attacking computer and number of the port on the user's computer targeted by the network attack, ID of the attack protocol, name and type of attack.

- Information about network connections: version and checksums (MD5, SHA2-256, SHA1) of the file from which process was started that opened the port, the path to the process's file and its digital signature, local and remote IP addresses, numbers of local and remote connection ports, connection state, timestamp of the port's opening.

- The URL and IP address of the web page where harmful or suspicious content was detected, the name, size, and checksum of the file that requested the URL, the identifier, weight and degree of the rule used to reach a verdict, the objective of the attack.

- Information about updates of the installed application and anti-virus databases: status of completion of the update task, type of error that may have occurred during the update process, the number of unsuccessful updates, the identifier of the application component that performs updates.

- Information about the use of Kaspersky Security Network (KSN): KSN identifier, application identifier, full version of the application, depersonalized IP address of the user's device, indicators of the quality of fulfillment of KSN requests, indicators of the quality of the processing of KSN packets, indicators of the number of KSN requests and information about the types of KSN requests, date and time when statistics began being sent, date and time when statistics finished being sent, information about KSN configuration updates: identifier of the active configuration, identifier of the configuration received, error code of the configuration update.

- Information about system log events: event time, name of the log where the event has been detected, type and category of event, name of the event source and event description.

- Information to determine the reputation of files and URL-addresses: the URL-address at which the reputation is being requested and the Referrer, the connection's protocol type, the internal identifier of the application type, the number of the port being used, the User identifier, checksum of the scanned file (MD5), type of the detected threat, information about the record used to detect a threat (record identifier for the anti-virus databases, the record timestamp and type); public key of the certificate; digital certificate thumbprint of the scanned object and hashing algorithm.

- Data on the application territorial distribution: date of the application installation and activation, ID of the partner providing the license for the application activation, application ID, application language localization ID, license serial number for the application activation, KSN participation sign.

- Information about the license used: the type and validity period of the license, number of days till license expiration, identifier of the partner from whom the license was purchased, Regional Activation Center identifier, checksum of the activation code, ticket body hash calculated using the SHA1 algorithm, license ticket creation date and time, license information identifier, license ticket identifier, license ticket sequence identifier, unique identifier of the user's computer, date from which the license ticket is valid, date to which the license ticket is valid, license ticket current state, ticket header version, license version, ticket header signature certificate identifier, checksum of the key file, ticket header signer serial number, authentication token.

- Information about hardware installed on the computer: type, name, model name, firmware version, parameters of built-in and connected devices.

- Information about the device: device ID.

- Information about the operation of the Web Control component: component version, categorization reason, additional information about categorization reason, categorized URL, host IP address of blocked/categorized object.

In addition, in order to achieve the declared purpose of increasing the effectiveness of protection provided by the application, Kaspersky may receive objects that could be exploited by intruders to harm the computer and create information security threats. Such objects are:

- Executable or non-executable files or parts thereof

- Computer's RAM areas

- Sectors involved in the OS boot process

- Network traffic data packages

- Web pages and emails containing suspicious or malicious objects

- Description of classes and class instances for the WMI storage

- Application activity reports

Application activity reports contain the following information about the files and processes:

- Name, size, and version of the file being sent, its description and checksums (MD5, SHA2-256, SHA1), format ID, its manufacturer's name, the name of the application the file belongs to, the fully qualified path to the file on the computer and the path template code, date and time of file creation and update.

- Certificate validity start and end dates and times if the file being sent has a digital signature, date and time when the certificate was signed, name of the certificate issuer, information about the certificate holder, impression and public key of the certificate and algorithms used to calculate them, certificate serial number.

- Name of the account that had run the process.

- Checksums (MD5, SHA2-256, SHA1) for the name of the computer that is running the process.

- Process' windows headers.

- ID for the anti-virus databases, name of the identified threat according to the Kaspersky classification.

- Information about the license used for the application, license ID, its type and expiry date.

- Computer's local time at the moment the information was provided.

- The names and paths of the files that were accessed by the process.
- URL- and IP addresses that were accessed by the process.
- URL- and IP addresses from which the running file was downloaded.

In addition, in order to achieve the declared purpose with respect to preventing false positives, the Rightholder may receive trusted executable and non-executable files or their parts.

Read Kaspersky Security Network Statement

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.

2. On the **Advanced** tab, click **Show KSN Statement**.

Kaspersky Endpoint Security saves the following information in a Trace file:

- Information about the device and operating system (unique device ID, device type, MAC addresses of network devices, operating system type, operating system version).
- Information about the operation of the application and its modules.
- Information about the subscription (subscription type, region).
- Information about the language locale, application ID, application customization, application version, unique application installation ID, unique computer ID.
- Information about the anti-malware protection status of the computer, as well as all processed and detected objects (the name of the detected object, date and time of detection, the web address from which it was downloaded, the names and sizes of infected files and paths to them, the IP address of the attacking computer and the number of the computer port targeted by the network attack, list of malware activity, and unwanted web addresses), and the relevant actions and decisions taken by the application and the user.
- Information about applications downloaded by the user (web address, attributes, file size, and information about the process that downloaded the file).
- Information about the launched applications and application modules (size, attributes, creation date, PE header details, region, name, location, and packers).
- Information about interface errors and usage of the interface of the installed Kaspersky application.
- Information about network connections: the IP address of the remote computer and the user's computer, the numbers of ports used to establish the connection, and the network protocol of the connection.
- Information about network packets received and sent by the computer over IT and telecom networks.
- Information about email and instant messages sent and received.
- Information about web addresses visited: the time when the connection was established using an open protocol, data on the website login and password, and the content of cookies.
- Public certificate of the server.

Trace files contain only the information necessary to fix defects in the application. Kaspersky uses trace files to investigate incidents associated with errors in the operation of the Kaspersky Endpoint Security application.

By default, the creation of trace files is disabled. You can enable generation of trace files in the application settings.

Trace files can only be manually sent to Kaspersky. The application does not send trace files to Kaspersky automatically.

You can choose how trace files are sent to Kaspersky.

Before sending trace files to Kaspersky, please review the data they contain.

Important: Trace files may contain personal or sensitive information. By sending trace files to Kaspersky, you agree to provide to Kaspersky all data contained in the trace files you send and you consent to the method used to send them.

Files (or their parts) that may be exploited by intruders to harm the computer or data may be also sent to Kaspersky to be examined additionally.

Kaspersky protects any information received in accordance with law and applicable Kaspersky rules. Data is transmitted over a secure channel.

Participation in Kaspersky Security Network is voluntary. The decision to participate is made when you install the application. However, you can change your decision later at any time.

Activate Kaspersky Endpoint Security

Important: Before activating Kaspersky Endpoint Security, make sure that the date and time that set on your computer match the actual date and time.

Activating the application involves adding a key to the application. The Managed Detection and Response component is activated separately. To use this component, you must activate Kaspersky Managed Detection and Response in the Kaspersky Security Center Administration or Web Console.

If the Endpoint Detection and Response component is not supported by your current license, you need to activate Kaspersky Endpoint Detection and Response separately.

Note: An internet connection is required to activate the application.

Activate the trial version

1. Open the main application window.
2. On the sidebar of the main application window, click **License**.

   The **License** window opens.
3. In the **License** window, click **Activate**.

   Kaspersky Endpoint Security connects to Kaspersky activation servers and sends data for verification. If verification is successful, the application receives and adds a key for the free trial version.

Important: A trial version of Kaspersky Endpoint Security can be activated only if the application has not been previously activated on the computer.

Activate the application with an activation code

1. Open the main application window.
2. On the sidebar of the main application window, click **License**.

   The **License** window opens.
3. In the **License** window, enter the activation code that you received when purchasing Kaspersky Endpoint Security.
4. Click **Activate**.

   Note: An activation code is a unique combination of twenty Latin letters and numbers in the form xxxxx-xxxxx-xxxxx-xxxxx.

   The application connects to Kaspersky activation servers and sends the activation code to verify its authenticity. If the activation code is successfully verified, the application automatically receives and adds the license key.

   Note: Depending on the activation code that you have received, you may need to fill out a registration form.

   If activation code verification fails, a corresponding notification is displayed. In this case, contact the software vendor that supplied you with this activation code.

After you have activated the application with the activation code, you can view the following information in the **License** window:

- License or subscription status
- Active keys
- Reserve keys (if any)
- License type and the number of computers on which you can use the application under the current license or subscription
- Application features that are available under the current license or subscription
- License expiration date and time
- Number of days until the license expires

View license information

View license information

1. Open the main application window.
2. On the sidebar of the main application window, click **License**.

   The **License** window opens.

The **License** window may contain the following information:

- License or subscription status
- Active keys
- Reserve keys (if any)
- License type and the number of computers on which you can use the application under the current license or subscription
- Application features that are available under the current license or subscription
- License expiration date and time
- Number of days until the license expires

Manage licenses and subscriptions

You have to renew the license if the license associated with the active key has expired and no reserve key has been added. When the license expires, the application continues to operate with limited functionality (updates, Kaspersky Security Network, Web Control, and FileVault Disk Encryption via Kaspersky Security Center become unavailable). You can still use all application components and run malware scans, but only with the anti-malware databases that were installed before the license expired.

Important: When your anti-malware databases are out of date, your computer is at increased risk of infection.

Renew a license

1. On the sidebar of the main application window, click **Protection Center**.

   The **Protection Center** window opens.
2. In the **Protection Center** window, click **Renew**.

   A webpage opens, with information on renewing your license through the Kaspersky online store or Kaspersky partners. When you renew a license via an online store, an activation code for Kaspersky Endpoint Security is sent to the email address specified in the order form after you complete the payment.

When you use the application under subscription, Kaspersky Endpoint Security automatically contacts the activation server at specific intervals until your subscription expires.

If you use the application under an unlimited subscription, Kaspersky Endpoint Security renews your subscription without requiring any action from you.

If you use the application under a limited subscription and the grace period for renewing the subscription is over, Kaspersky Endpoint Security notifies you of this and stops trying to automatically renew the subscription and updating the application databases.

You can renew your subscription manually by contacting the vendor that sold you Kaspersky Endpoint Security.

Renew your subscription

1. Open the main application window.
2. On the sidebar of the main application window, click **License**.

   The **License** window opens.
3. In the **License** window, click **Visit service provider website**.

The website of your service provider opens.

Your subscription status may become out of date. In this case, you need to manually update the status of your subscription. If you do not have a current subscription, Kaspersky Endpoint Security stops updating the application databases (if you have subscription to updates) or stops protecting the computer (if you have a subscription to updates and protection).

Update subscription status

1. Open the main application window.
2. On the sidebar of the main application window, click **License**.

   The **License** window opens.
3. In the **License** window, click the ↻ button.

Comparison of application functionality depending on license type for workstations

The set of Kaspersky Endpoint Security functionality available on workstations depends on the license type (see table below).

Comparison of Kaspersky Endpoint Security features

Feature	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert
Advanced Threat Protection						
Kaspersky Security Network	✓	✓	✓	✓	✓	✓

Feature	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert
Behavior Detection	✓	✓	✓	✓	✓	✓
Exploit Prevention	✓	✓	✓	✓	✓	✓
Remediation Engine	✓	✓	✓	✓	✓	✓
Essential Threat Protection						
File Threat Protection	✓	✓	✓	✓	✓	✓
Web Threat Protection	✓	✓	✓	✓	✓	✓
Mail Threat Protection	✓	✓	✓	✓	✓	✓
Firewall	✓	✓	✓	✓	✓	✓
Network Threat Protection	✓	✓	✓	✓	✓	✓
Security Controls						
Device Control	✓	✓	✓	✓	✓	✓
Web Control	✓	✓	✓	✓	✓	✓
Data Encryption						
FileVault Disk Encryption	–	✓	✓	✓	✓	✓
Detection and Response						
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓
Kaspersky Sandbox *(Kaspersky Sandbox license must be purchased separately)*	✓	✓	✓	✓	✓	✓

Perform common tasks

Open and quit the application

As soon as you complete installation, the application starts automatically and the application icon appears in the menu bar.

Open the application

In the menu bar, click the application icon and choose **Kaspersky Endpoint Security**.

Quit the application

In the menu bar, click the application icon and choose **Quit**.

When you quit the application, the application process is removed from computer memory.

Important: After you quit the Kaspersky Endpoint Security application, the computer is no longer protected and may become infected, which puts your data at risk of being lost.

View the status of computer protection

The protection status indicator, which is shaped like a shield and located in the main application window, informs you about computer protection problems. Depending on the status of computer protection, the color of the indicator can change. If Kaspersky Endpoint Security detects any security threats, a message about threats appears in the main application window and the indicator changes color.

The indicator color can change in the following ways:

- **Green**. Your computer is appropriately protected.

  A green indicator signifies that anti-malware databases are up to date and all application components have been configured as recommended by Kaspersky. No malicious objects have been detected, or any detected malicious objects have been neutralized.

- **Yellow**. The level of computer protection is reduced.

  A yellow indicator signifies that Kaspersky Endpoint Security is aware of a problem. Such problems include minor deviations from the recommended protection settings or slightly outdated application databases.

- **Red**. Your computer is at risk of infection.

  A red indicator signifies that there are dangerous problems that may lead to computer infection and data loss. For example, the anti-malware application databases are extremely out of date, the application is not activated, or malicious objects have been detected.

  We recommend that you fix any problems and deal with the security threats as soon as possible.

View the operating status of installed components

Kaspersky Endpoint Security lets you check the status of installed application components in the **Security** window. The indicator next to the name of each component reflects its status.

View component status

1. Open the main application window.
2. On the sidebar of the main application window, click **Security**.

   The **Security** window opens.

The following status indicators may be displayed:

●	The component is running.
🔒	The component is running and managed by a security policy.
●	The component has malfunctioned.
🔒	The component has malfunctioned and is managed by a security policy.
●	The component is turned off.
🔒	The component is turned off and managed by a security policy.
⏸	The component is paused.
🔑	The component is not supported by the current license.

Note: For some components, you may also use the 3-dot menu next to the name of the component to open a report or configure component settings.

Disable and resume computer protection

By default, Kaspersky Endpoint Security starts after the operating system starts up, and protects your computer until it is turned off. All protection components (File Threat Protection, Web Threat Protection, and Network Threat Protection) are enabled and running.

You can disable protection completely or disable specific protection components.

Important: Kaspersky strongly advises against disabling protection or protection components, because disabling them may lead to computer infection and data loss.

When computer protection is disabled:

- The application icon in the menu bar is inactive.
- The protection status indicator in the main application window is red.

When one or more protection components are disabled, the protection status indicator is red or yellow.

Note: Disabling or pausing protection components does not affect scan tasks or the update task.

You can disable/resume computer protection in one of the following ways:

- From the application icon
- From the application settings window
- From the **Protection** menu

Disable/resume computer protection from the application icon

1. In the menu bar, click the application icon and choose **Turn Protection Off**/**Turn Protection On**.

   When you turn off protection, a prompt for administrator credentials appears.

2. In the prompt for administrator credentials, enter an administrator name and password and confirm that you want to turn off protection.

Disable/resume computer protection from the application settings window

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.

2. On the **Essential** tab, in the **General** section, deselect/select the **Enable protection** checkbox.

Disable/resume computer protection from the menu bar

In the menu bar, click **Protection** > **Turn Protection Off**/**Turn Protection On**.

Important: If you disable computer protection, it will not be re-enabled automatically when Kaspersky Endpoint Security starts again. You have to re-enable computer protection manually.

Disable a protection component

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.

2. On the **Essential** tab, in the **<component name>** section, deselect the **Enable <component name>** checkbox.

Important: If you disable a protection component, it will not be re-enabled automatically when Kaspersky Endpoint Security starts again. You have to re-enable the protection component manually.

Enable a protection component

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.

2. On the **Essential** tab, in the **<component name>** section, select the **Enable <component name>** checkbox.

To enable computer protection or protection components, you can also use Protection Center. Disabling computer protection or disabling protection components puts your computer at much higher risk of infection. This is why Protection Center informs you when computer protection is disabled.

Use Protection Center

Protection Center is a Kaspersky Endpoint Security feature that helps you analyze and fix problems and computer security threats.

Open Protection Center

On the sidebar of the main application window, click **Protection Center**.

In Protection Center, you can find information about active threats, view the state of application databases, and find out whether any component protection is disabled.

Note: If your organization's system administrator enables Web Control to block access to dangerous web resources, Kaspersky Endpoint Security displays the **Web Control is enabled** notification in Protection Center.

For each problem or threat, Kaspersky Endpoint Security suggests actions that you can perform to resolve the problem or threat. For example, if Kaspersky Endpoint Security detects infected files on the computer, you can click **Disinfect**. If the anti-malware databases are out of date, you can click **Update**. You can fix a problem or neutralize a threat immediately or later.

Fix a problem or neutralize a threat immediately

Click the button with the name of a recommended action to fix the problem or neutralize the threat.

The application performs the selected action.

If you close Protection Center without neutralizing dangerous threats, the protection status indicator in the main application window remains red to remind you of these threats.

Perform scan tasks

The default Full Scan task is included in Kaspersky Endpoint Security. While running this task, the application scans the computer's memory, startup objects, and all internal drives for viruses and other malware.

Perform a full computer scan

1. On the sidebar of the main application window, click **Scan**.

   The **Scan** window opens.

2. Click the **Full Scan** button.

A full scan of the computer starts.

The default Quick Scan task is included in Kaspersky Endpoint Security. While running this task, the application scans the critical areas of the computer (memory, startup objects, and system folders) for viruses and other malware.

Perform a quick computer scan

1. On the sidebar of the main application window, click **Scan**.

   The **Scan** window opens.

2. Click the **Quick Scan** button.

A quick scan of the computer starts.

If you want to scan an individual object (such as an internal disk, folder, file, or removable disk) for viruses and other malware, you can run the Custom Scan task.

Scan a selected item

Do one of the following:

- Right-click a selected item and choose **Scan for Malware**.
- Drag a selected item to the application icon in the Dock.
- Drag a selected item onto the **Scan** window.

You can view the results of completed scan tasks in the **Reports** window.

Note: Kaspersky Endpoint Security does not scan files that are located in OneDrive or iCloud storage or other cloud storages. Please exclude these files from the scan scope. Otherwise, the scan task may finish with the *Infected File Not Deleted* error.

Configure the automatic start of a scheduled scan task

You can create a schedule for starting the Quick Scan and Full Scan tasks. Kaspersky Endpoint Security automatically scans the entire computer or specified areas of the computer in accordance with the configured schedule.

Schedule a scan task from the Scan window

1. On the sidebar of the main application window, click **Scan**.

   The **Scan** window opens.

2. Click **Schedule Scan**.

   A dialog opens where you can set the schedule.

3. Select the **Full Scan** or **Quick Scan** checkbox.

4. Specify the scanning frequency and the scan start time.
5. Click **OK**.

Schedule a scan task from the Settings window

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.
2. On the **Scan** tab, click **Schedule**.
3. In the window that opens, select the checkbox next to the name of the scan task you want to start on a schedule.
4. Configure the scan task frequency and time.
5. Click **OK** to save changes made to the scan task schedule.

You can view scan task results in the **Reports** window.

Update application databases

Dedicated Kaspersky update servers are the main source of updates for Kaspersky Endpoint Security. Kaspersky Endpoint Security can also use distribution points, local folders, or other web servers as an *update source*.

Note: An internet connection is required to download updates from the update servers.

By default, Kaspersky Endpoint Security periodically checks for updates on Kaspersky update servers. If new updates are available on a server, Kaspersky Endpoint Security downloads them in the background and installs them on your computer.

Start an update of Kaspersky Endpoint Security

1. On the sidebar of the main application window, click **Update**.

   The **Update** window opens.
2. Click **Update**.

   The application checks for updates. If updates are available, the application downloads and installs them on your computer.

You can also start an update task in one of the following ways:

- Click the application icon and choose **Update**.
- In the menu bar, choose **Protection** > **Update**.

You can change the way Kaspersky Endpoint Security updates the application databases. By default, the application updates databases automatically.

Enable/disable automatic downloads of Kaspersky Endpoint Security database updates

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.

2. On the **Update** tab, in the **Databases** section, select/deselect the **Download updates automatically** checkbox.

You can view the results of completed update tasks in the **Reports** window.

Note: Updates functionality (including providing anti-malware signature updates and codebase updates), as well as KSN functionality may not be available in the software in the U.S.

What to do if file access is blocked

The Kaspersky Endpoint Security application blocks access to infected files and applications. If a file is infected, it must be disinfected before you can access it.

Disinfect a detected object

1. In the menu bar, choose **Protection** > **Detected Objects**.

   The **Detected Objects** window opens.

2. In the **Detected Objects** section, click ••• next to the required file and choose **Disinfect**.

   The application starts disinfecting the selected object. While disinfection is in progress, the application shows a dialog where you can choose the action to take on the object.

Disinfect all detected objects

1. In the menu bar, choose **Protection** > **Detected Objects**.

   The **Detected Objects** window opens.

2. In the **Detected Objects** section, click **Disinfect All**.

   The application starts disinfecting detected objects. While disinfection is in progress, the application shows a notification window where you can choose the action to take on the object. If you select the **Apply to all** checkbox in the notification window when choosing an action, the application applies the same action to all files of this type.

If you know for sure that the files being blocked by File Threat Protection are safe, you can include them in Trusted Zone.

Restore a file that has been deleted or disinfected by the application

Sometimes it is not possible to save files in their entirety during the disinfection process. If a disinfected file contained important information that is partly or completely inaccessible following disinfection, you can attempt to restore the original file from its backup copy.

Restore a file that has been deleted or modified by the application during disinfection

1. In the menu bar, choose **Protection** > **Detected Objects**.

   The **Detected Objects** window opens.

2. In the **Back up** section, click ••• next to the file that you want to restore.

   The pop-up menu opens.

3. Choose **Restore File**.

   A window for specifying the file name, tag, and folder to which the file will be restored opens. By default, the original file name and location are already specified.

4. Specify the file name and folder to which the file will be restored.

5. Click **Save**.

   The application restores the file to the specified location with the specified name.

You need to scan the file for malware immediately after restoring it. It is possible that the object can be disinfected using updated databases without becoming corrupted.

Important: We recommend that you not restore backup copies of files unless restoring them is absolutely necessary, because doing so could lead to a computer infection.

View the application operation report

You can view a Kaspersky Endpoint Security report listing all detected objects on the **Processed objects** tab. System events are displayed on the **System events** tab. Additionally, a separate detailed report is created for each of the following application components: File Threat Protection, Web Threat Protection, Network Threat Protection, Behavior Detection, and scan and update tasks.

Open the Reports window

In the menu bar, choose **Protection** > **Reports**.

What to do if notification windows appear

Application notifications, in the form of notification windows, inform you of application events that require your attention.

If a notification appears on the screen, select one of the suggested options. The optimal option is the one set as the default option by Kaspersky experts.

Advanced configuration of the application

Computer protection scope

Objects detected by Kaspersky Endpoint Security are divided into categories based on various attributes. The application always searches for viruses, worms, Trojans, and malicious tools. These programs may cause significant damage to your computer. To ensure more reliable protection for your computer, you can extend the list of detectable objects by enabling the application to check for legitimate software that can be used by intruders to damage your computer or personal data.

The objects that Kaspersky Endpoint Security protects against are grouped as follows:

- **Viruses, worms, Trojans, malicious tools, adware, and auto-dialers**.

  This category includes:

  - All types of malware.
  - Software that can inconvenience you by showing advertisements (such as banners) on your computer or replacing search results in your browser with advertising websites.
  - Applications that establish hidden phone connections through a modem.

  Protection against all types of malware is the minimum necessary security level. In accordance with the recommendations of Kaspersky experts, Kaspersky Endpoint Security always monitors objects that belong to this category.

- **Legitimate software that can be used by intruders to damage your computer or personal data**. This category includes legitimate software that can be used by intruders to damage your computer or personal data, such as remote administration applications.

Select the categories of objects to detect

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.

2. On the **Threats** tab, in the **Objects to detect** section, select the checkboxes next to the categories of objects to detect.

   Note: Kaspersky Endpoint Security always protects your computer against viruses, worms, Trojans, malicious tools, adware, and auto-dialers. Accordingly, it is not possible to deselect the checkbox for this category.

Depending on the selected categories of objects to detect, Kaspersky Endpoint Security uses some or all of its anti-malware databases when running File Threat Protection, Web Threat Protection, and scan tasks.

Note: If Kaspersky Endpoint Security classifies an application as malware but you believe it is safe, you can add this application to Trusted Zone.

Trusted Zone is a list of objects that Kaspersky Endpoint Security does not scan or monitor. You may need to add objects to Trusted Zone if, for example, Kaspersky Endpoint Security blocks access to a file, application, or website even though you are absolutely sure that this object, application, or web address is harmless.

When an application is added to Trusted Zone, its file and network activities (including suspicious ones) are no longer monitored. However, Kaspersky Endpoint Security continues to scan the executable file and process of the trusted application.

Note: When an administrator configures the policy to prohibit editing Trusted Zone, users cannot go to Trusted Zone settings.

Add/remove a file or folder to/from the list of trusted files and folders

1. In the menu bar, click the application icon and choose **Settings**.
   The application settings window opens.
2. On the **Threats** tab, in the **Exclusions** section, click **Trusted Zone**.
   The Trusted Zone settings window opens.
3. On the **Files and Folders** tab, edit the list of trusted files and folders:
   - To add a file or folder to the list:
     a. Click +.
        A dialog where you can select a file or folder opens.
     b. Select a file or folder that you want to add.
     c. Click **Open**.
   - To remove a file or folder from the list:
     a. Select a file or folder that you want to remove from the list of trusted files and folders.
     b. Click –.
4. Click **OK**.

Add/remove a trusted web address to/from the list of trusted web addresses

1. In the menu bar, click the application icon and choose **Settings**.
   The application settings window opens.
2. On the **Threats** tab, in the **Exclusions** section, click **Trusted Zone**.
   The Trusted Zone settings window opens.
   You can also open this window by clicking the **Trusted Zone** button in the **General** section of the **Essential** tab.

3. On the **Web Addresses** tab, edit the list of trusted web addresses:

   - To add a web address to the list:

     a. Click +.

     b. Enter the web address that you want to add to the list.

     c. Click **OK**.

   - To remove a web address from the list:

     a. Select a web address that you want to remove.

     b. Click –.

4. Click **OK**.

By default, the list of trusted web addresses is empty.

Add/remove a trusted application to/from the list of trusted applications

1. In the menu bar, click the application icon and choose **Settings**.
   The application settings window opens.

2. On the **Threats** tab, in the **Exclusions** section, click **Trusted Zone**.
   The Trusted Zone settings window opens.
   You can also open this window by clicking the **Trusted Zone** button in the **General** section of the **Essential** tab.

3. On the **Trusted applications** tab, edit the list of trusted applications:

   - To add an application to the list:

     a. Click +.
     A window where you can specify the parameters of the required application opens.

     b. Specify the following parameters of the application you want to add:

     - **Path**
     - **Code signing requirement**

     Note: You can either enter values of these two parameters manually or click the **Select** button and select the application you want to add in the window that opens. In this case, the values of these parameters will be inserted automatically.

c. In the **Options** section, select at least one type of activity that you do not want to be monitored by the Kaspersky Endpoint Security application:

- **Do not monitor file activity**
- **Do not monitor network activity**

d. Click **OK**.

- To remove an application from the list:

a. Select an application you want to remove.

b. Click –.

By default, the list of trusted applications is empty.

Edit a trusted application

1. In the menu bar, click the application icon and choose **Settings**.
   The application settings window opens.
2. On the **Threats** tab, in the **Exclusions** section, click **Trusted Zone**.
   The Trusted Zone settings window opens.
   You can also open this window by clicking the **Trusted Zone** button in the **General** section of the **Essential** tab.
3. On the **Trusted applications** tab, select an application you want to edit.
4. Click **Edit**.
5. In the window that opens, edit the application's parameters.
6. Click **OK**.

Enable monitoring of a trusted web address

1. In the menu bar, click the application icon and choose **Settings**.
   The application settings window opens.
2. On the **Threats** tab, in the **Exclusions** section, click **Trusted Zone**.
   The Trusted Zone settings window opens.
3. On the **Web Addresses** tab, deselect the checkbox next to a web address that you want the Kaspersky Endpoint Security application to monitor.
4. Click **OK**.

File Threat Protection

File Threat Protection prevents infection of the computer's file system. The component starts during startup of the operating system, remains in computer memory, and scans for malware all files that are opened, saved, or run on your computer and on all connected disks. If you disable File Threat Protection, it will not start at operating system startup. You will have to re-enable File Threat Protection manually.

Enable/disable File Threat Protection

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.

2. On the **Essential** tab, in the **File Threat Protection** section, select/deselect the **Enable File Threat Protection** checkbox.

   You can also enable File Threat Protection in Protection Center. Disabling computer protection or disabling protection components puts your computer at much higher risk of infection. This is why Protection Center informs you when protection is disabled.

You can create a protection scope for File Threat Protection.

Add/remove a file or folder to/from the protection scope

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.

2. On the **Essential** tab, in the **File Threat Protection** section, click **Protection Scope**.

   A window with a list of objects that File Threat Protection scans opens. By default, File Threat Protection scans all objects located on internal, removable, and network disks connected to your computer.

   > **Note:** You can skip scanning of the read-only system volume to significantly reduce scanning time. By default, File Threat Protection does not scan the read-only system volume.

3. In the **Protection scope** section, add/remove the objects to/from the protection scope:

   - To add a file or folder to the protection scope:

     a. Click +.

        A pop-up menu where you can select objects to add to the protection scope opens.

     b. In the pop-up menu, choose the **Files and Folders** item.

        A dialog where you can select a file or folder opens.

     c. Select a file or folder that you want to add to the protection scope.

     d. Click **Open**.

- To remove a file or folder from the protection scope:

  a. Select an object in the list of protection scope objects.

  b. Drag the selected object from the window or click –.

4. If you want to scan the read-only system volume, in the **Optimization** section, deselect the **Skip scanning of read-only system volume** checkbox.

   Important: Optimization might be disabled for security reasons.

5. Click **Save**.

Add/remove an object on the list of default objects to/from the protection scope

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.

2. On the **Essential** tab, in the **File Threat Protection** section, click **Protection Scope**.

   A window with a list of objects that File Threat Protection scans opens. By default, File Threat Protection scans all objects located on internal, removable, and network disks connected to your computer.

   Note: You can skip scanning of the read-only system volume to significantly reduce scanning time. By default, File Threat Protection does not scan the read-only system volume.

3. In the **Protection scope** section, add/remove the objects on the list of default objects to/from the protection scope:

   - To add an object on the list of default objects to the protection scope:

     a. Click +.

        A pop-up menu where you can select objects to add to the protection scope opens.

     b. In the pop-up menu, select an object that you want to add to the protection scope (for example, **All Internal Disks**).

   - To remove an object on the list of default objects from the protection scope:

     a. Select an object in the list of protection scope objects.

     b. Drag the selected object from the window or click –.

4. If you want to scan the read-only system volume, in the **Optimization** section, deselect the **Skip scanning of read-only system volume** checkbox.

   Important: Optimization might be disabled for security reasons.

5. Click **Save**.

Disable protection of an object in the protection scope

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.

2. On the **Essential** tab, in the **File Threat Protection** section, click **Protection Scope**.

   A window with a list of objects that File Threat Protection scans opens. By default, File Threat Protection scans all objects located on internal, removable, and network disks connected to your computer.

   > **Note:** You can skip scanning of the read-only system volume to significantly reduce scanning time. By default, File Threat Protection does not scan the read-only system volume.

3. Deselect the checkbox next to an object in the list of protection scope objects.

4. Click **Save**.

Enable scanning of the read-only system volume

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.

2. On the **Essential** tab, in the **File Threat Protection** section, click **Protection Scope**.

   A window with a list of objects that File Threat Protection scans opens. By default, File Threat Protection scans all objects located on internal, removable, and network disks connected to your computer.

   > **Note:** You can skip scanning of the read-only system volume to significantly reduce scanning time. By default, File Threat Protection does not scan the read-only system volume.

3. In the **Optimization** section, deselect the **Skip scanning of read-only system volume** checkbox.

   > **Important:** Optimization might be disabled for security reasons.

4. Click **Save**.

When you or an application attempt to access a file included in the protection scope, File Threat Protection checks iSwift databases for information about the file, and uses this information to decide whether to scan the file.

Recognizing malicious objects is possible thanks to *signature analysis*, a way of searching for threats based on threat descriptions included in the anti-malware databases. In addition to signature analysis, File Threat Protection uses heuristic analysis and other scanning technologies.

If a threat is detected in a file, Kaspersky Endpoint Security identifies the type of the detected malware (for example, *virus* or *Trojan*). Then the application displays a notification about the detected object and performs an action on the object based on your File Threat Protection settings.

Select the action that File Threat Protection performs after detecting an infected file

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.

2. On the **Essential** tab, in the **File Threat Protection** section, select the action that File Threat Protection performs after detecting an infected file.

Before attempting to disinfect or delete an infected file, Kaspersky Endpoint Security saves a backup copy for subsequent restoration or disinfection.

Information about File Threat Protection and all detected objects is logged in a report.

Note: If File Threat Protection stops running with an error, you can view the report and try to start the component again. If the problem is not solved, you can contact Kaspersky Technical Support.

View the File Threat Protection report

1. In the menu bar, choose **Protection** > **Reports**.

   The **Reports** window opens.

2. Open the **File Threat Protection** tab.

Web Threat Protection

When you use the internet, your computer is at risk of infection by malware and other computer security threats. Computer security threats may penetrate your computer when you download free programs or visit websites that have been attacked by hackers. In addition, network worms may attack your computer as soon as your computer establishes an internet connection, even before you open a web address or download a file.

Kaspersky Endpoint Security protects information that your computer sends and receives via the HTTP and HTTPS protocols in Safari, Chrome, or Firefox.

Note: Kaspersky Endpoint Security monitors web traffic on the ports most frequently used for HTTP and HTTPS data transfer. Kaspersky Endpoint Security scans encrypted connections (HTTPS) only if the **Check secure connections (HTTPS)** checkbox in the **General** section is selected.

Enable/disable Web Threat Protection

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.

2. On the **Essential** tab, in the **Web Threat Protection** section, select/deselect the **Enable Web Threat Protection** checkbox.

You can also enable Web Threat Protection via Protection Center. Disabling computer protection or disabling protection components puts your computer at much higher risk of infection. This is why Protection Center informs you when protection is disabled.

Important: If you disable Web Threat Protection, it will not be re-enabled automatically when Kaspersky Endpoint Security starts again or when the operating system restarts. You have to re-enable Web Threat Protection manually.

Web Threat Protection scans web traffic based on the settings recommended by Kaspersky. Malicious objects are recognized using signature analysis, heuristic analysis, and data from Kaspersky Security Network.

Checking links on websites for phishing threats and malicious web addresses makes it possible to avoid *phishing attacks*. *Phishing attacks* usually take the form of email messages from criminals, who pretend to be financial institutions (such as banks) and send links to fraudulent websites. In these emails, the criminals try to trick the user into visiting a phishing website and entering confidential data (such as your bank card number or the name and password for your online bank account). A phishing attack can be disguised, for example, as a message from your bank with a link to its official website, but in reality, the link takes you to an exact copy of the bank's official website created by impostors.

Web Threat Protection monitors your web traffic for attempts to visit a phishing website; it blocks access to such websites. To check links on websites for phishing threats and malicious web addresses, Kaspersky Endpoint Security uses the application databases, heuristic analysis, and data from Kaspersky Security Network.

Web traffic scan algorithm

Each website or file that you or an application accesses via the HTTP and HTTPS protocols is intercepted and scanned for malicious code by Web Threat Protection:

- If a website or file contains malicious code, Kaspersky Endpoint Security can block it and display a notification that the requested file or website is infected.
- If the file or website does not contain malicious code, you can access it immediately.

Select the action that Web Threat Protection performs after detecting a dangerous web traffic object

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.

2. On the **Essential** tab, in the **Web Threat Protection** section, select the action that Web Threat Protection performs after detecting a dangerous web traffic object.

Information about Web Threat Protection and all detected dangerous web traffic objects is logged in a report.

Note: If Web Threat Protection stops running with an error, you can view the Web Threat Protection report and try to restart the component. If the problem is not solved, you can contact Kaspersky Technical Support.

View the Web Threat Protection report

1. In the menu bar, choose **Protection** > **Reports**.

   The **Reports** window opens.

2. Open the **Web Threat Protection** tab.

Mail Threat Protection

The Mail Threat Protection component scans the attachments of incoming and outgoing email messages for malware and other threats. The component provides computer protection with the help of anti-malware databases, the Kaspersky Security Network cloud service, and heuristic analysis.

The application supports the following mail clients: Apple Mail, Microsoft Outlook, Mozilla Thunderbird, Canary Mail, Spark, Mimestream, Airmail, Post Box, Boxy Suite 2, Twobird, Shift, Clean Email, eM Client, Superhuman, Polymail, HEY, Mail+ for Gmail, Spike mail.

By default, Mail Threat Protection is enabled. You can disable Mail Threat Protection if necessary.

Enable/disable Mail Threat Protection using the Web Console

1. In the main window of the Web Console, select **Assets (Devices)** > **Policies & profiles**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.

3. Select the **Application settings** tab.
4. Go to **Essential Threat Protection** > **Mail Threat Protection**.
5. Turn on/off the **Mail Threat Protection** toggle switch.
6. If Mail Threat Protection is enabled, select the action to be performed by the application when malware is detected:

   - **Delete**
   - **Block**

7. If necessary, in the **Advanced settings** section configure the time limit for checking archives or the maximum size of the archive for scanning.
8. Save your changes.

Enable/disable Mail Threat Protection using the Administration Console

1. Start the Administration Console.
2. Maximize the **Administration Server <Server name>** node.
3. In the console tree, click **Managed devices**.
4. In the workspace, select the **Policies** tab.

5. Right-click the policy you want to configure and choose **Properties**.

6. In the **Properties** window, select **Essential Threat Protection** > **Mail Threat Protection**.

7. Select or deselect the **Enable Mail Threat Protection** checkbox.

8. In the **Action on threat detection** section, select the action to be performed when Kaspersky Endpoint Security detects a threat.

9. If necessary, in the **Mail Threat Protection: settings** section configure the time limit for checking archives or the maximum size of the archive for scanning.

10. Click **OK** to save your changes.

11. Do one of the following to apply the changes to the policy:

    - Click **Apply** to remain in the **Properties: <Policy name>** window after saving changes.
    - Click **OK** to close the **Properties: <Policy name>** window after saving changes.

Enable/disable Mail Threat Protection using the Kaspersky Endpoint Security application

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.

2. On the **Essential** tab, in the **Mail Threat Protection** section, select or deselect the **Enable Mail Threat Protection** checkbox.

3. If the **Enable Mail Threat Protection** checkbox is selected, select the action to be performed when Kaspersky Endpoint Security detects a threat.

4. If necessary, configure the time limit for checking archives or the maximum size of the archive for scanning.

View the Mail Threat Protection report

1. In the menu bar, choose **Protection** > **Reports**.

   The **Reports** window opens.

2. Open the **Mail Threat Protection** tab.

Network Threat Protection

Kaspersky Endpoint Security protects your computer against network attacks.

A *network attack* is an attempt to break into the operating system of a remote computer. Criminals attempt network attacks to establish control over the operating system, cause denial of service in the operating system, or access sensitive information. To achieve these goals, criminals either carry out direct attacks, such as port scanning and brute-force attacks, or use malware installed on the computer being attacked.

Network attacks can be divided into the following types:

- *Port scanning*. This type of network attack is usually performed to prepare for a more dangerous network attack. An intruder scans UDP/TCP ports that use network services on the target computer and determines the target computers' vulnerability to other, more dangerous types of network attacks. Port scanning also allows the intruder to determine the operating system on the target computer and select appropriate network attacks for that operating system.

- *DoS attacks* or network attacks causing a denial of service. Such network attacks cause the target operating system to become unstable or completely inoperable.

  The main types of DoS attacks are:

  - Transmission of specially designed network packets that are not expected by the target computer, thus causing the target operating system to malfunction or crash.

  - Sending a large number of network packets to a remote computer over a short period. All the target computer's resources are used to process the network packets sent by the intruder. As a result, the computer stops performing its functions.

- *Network intrusion attacks*. Such network attacks are designed to "hijack" the target computer's operating system. This is the most dangerous type of network attack, because if the attack is successful, then the intruder gains total control over the operating system.

  This type of network attack is used when the intruder wants to obtain confidential data (such as bank card numbers or passwords) from a remote computer or secretly use the remote computer for his or her own purposes (such as attacking other computers from this computer).

Enable/disable Network Threat Protection

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.

2. On the **Essential** tab, in the **Network Threat Protection** section, select/deselect the **Enable Network Threat Protection** checkbox.

You can also enable Network Threat Protection in Protection Center. Disabling computer protection or disabling protection components puts your computer at much higher risk of infection. This is why Protection Center informs you when protection is disabled.

Important: If you disable Network Threat Protection, it will not be re-enabled automatically when Kaspersky Endpoint Security starts again or after the operating system restarts. You have to re-enable Network Threat Protection manually.

When the application detects dangerous network activity, Kaspersky Endpoint Security automatically adds the IP address of the attacking computer to the list of blocked computers, unless the attacking computer is in the list of trusted computers.

Edit the list of blocked computers

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.

2. On the **Essential** tab, in the **Network Threat Protection** section, select the **Enable Network Threat Protection** checkbox.

3. Click **Settings**.

   A window with a list of trusted computers and a list of blocked computers opens.

4. Open the **Blocked computers** tab.

5. If you are sure that the blocked computer is not a threat, select the IP address of the computer in the list and click **Unblock**.

   A confirmation dialog opens.

6. In the confirmation dialog, select one of the following:

   - If you want to unblock the computer, click **Unblock**.

     Kaspersky Endpoint Security unblocks the IP address.

   - If you want Kaspersky Endpoint Security to never block the selected IP address, click **Unblock and Exclude**.

     Kaspersky Endpoint Security unblocks the IP address and adds it to the list of trusted computers.

7. Click **Save**.

You can create and edit the list of trusted computers. The Kaspersky Endpoint Security application doesn't block the IP addresses of these computers automatically even after dangerous network activity is detected from them.

Edit the list of trusted computers

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.

2. On the **Essential** tab, in the **Network Threat Protection** section, select the **Enable Network Threat Protection** checkbox.

3. Click **Settings**.

   A window with a list of trusted computers and a list of blocked computers opens.

4. Open the **Trusted computers** tab.

5. Edit the list of trusted computers:

   - To add an IP address to the list of trusted computers:

     a. Click +.

     b. In the field that appears, enter the IP address of the computer that you trust to be safe.

   - To remove an IP address from the list of trusted computers:

     a. Select an IP address in the list.

     b. Click –.

- To edit an IP address in the list of trusted computers:

  a. Select an IP address in the list.

  b. Click **Edit**.

  c. Change the IP address.

6. Click **Save**.

When a network attack is detected, Kaspersky Endpoint Security logs information about the attack in a report.

Note: If the Network Threat Protection component stops running with an error, you can view the report and try to restart the component. If the problem is not solved, you can contact Kaspersky Technical Support.

View the Network Threat Protection report

1. In the menu bar, choose **Protection** > **Reports**.

   The **Reports** window opens.

2. Open the **Network Threat Protection** tab.

Firewall

Firewall blocks unauthorized connections to the computer while working on the internet or local network. Firewall also controls the network activity of applications on the computer. This allows you to protect your corporate LAN from identity theft and other attacks. The component provides computer protection with the help of anti-malware databases, the Kaspersky Security Network cloud service, and predefined network rules.

Network Rule Priorities

Each rule has a priority. The higher a rule is on the list, the higher its priority. If network activity is added to several rules, Firewall regulates network activity according to the rule with the highest priority.

Network connection types

Firewall allows you to control network activity depending on the type of the network connection. You can change the type of the network connection in the Kaspersky Endpoint Security settings.

The following network connection types are available:

- **Public network**. The network is not protected by antimalware applications, firewalls, or filters (such as Wi-Fi in a cafe). When the user operates a computer that is connected to such a network, Firewall blocks access to files and printers of this computer. External users are also unable to access data through shared folders and remote access to the desktop of this computer. Firewall assigns Public network type to the internet by default. You cannot change the type of the internet.

- **Local network**. Network for users with restricted access to files and printers on this computer (such as for a corporate LAN or home network).

- **Trusted network**. Safe network in which the computer is not exposed to attacks or unauthorized data access attempts. Firewall permits any network activity within networks with this status.

Manage the Firewall component in the Administration Console

1. Start the Administration Console.
2. Maximize the **Administration Server <Server name>** node.
3. In the console tree, click **Managed devices**.
4. In the workspace, select the **Policies** tab.
5. Right-click the policy you want to configure and choose **Properties**.
6. In the **Properties** window, select **Essential Threat Protection** > **Firewall**.
7. Select or deselect the **Enable Firewall** checkbox.
8. In the **Firewall settings** section, click the **Settings** button and add, edit, delete, or change priority of the rules.
9. In the **Available networks** section, click the **Settings** button and add, edit, delete, or change the type of the networks.
10. Click **OK** to save your changes.
11. Do one of the following to apply the changes to the policy:
    - Click **Apply** to remain in the **Properties: <Policy name>** window after saving changes.
    - Click **OK** to close the **Properties: <Policy name>** window after saving changes.

Manage the Firewall component in the Web Console

1. In the main window of the Web Console, select **Assets (Devices)** > **Policies & profiles**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Essential Threat Protection** > **Firewall**.
5. Turn on/off the **Firewall** toggle switch.

6. In the **Firewall settings** section, click the **Network packet rules** button and add, edit, delete, or change priority of the rules.

7. In the **Available networks** section, click the **Network settings** button and add, edit, or change the type of the networks.

8. Save your changes.

Manage the Firewall component in the Kaspersky Endpoint Security application

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.

2. On the **Essential** tab, in the **Firewall** section, select or deselect the **Enable Firewall** checkbox.

3. If necessary, click the **Settings** button and configure the Firewall settings:

   - On the **Network packet rules** tab, you can add, edit, delete, or change priority of the rules.

   - On the **Available networks** tab, you can add, edit, or change the type of the networks.

As a result, if Firewall is enabled, Kaspersky Endpoint Security controls network activity and blocks unauthorized network connections to your computer.

View the Firewall report

1. In the menu bar, choose **Protection** > **Reports**.

   The **Reports** window opens.

2. Open the **Firewall** tab.

Behavior Detection

The Behavior Detection component receives data on the actions of applications on your computer and provides this information to other protection components to improve their performance. The Behavior Detection component uses applications' Behavior Stream Signatures (BSS). If application activity matches a behavior stream signature, Kaspersky Endpoint Security performs the selected response action. Kaspersky Endpoint Security functionality based on behavior stream signatures provides proactive defense for the computer.

By default, Behavior Detection is enabled and runs in the mode recommended by Kaspersky experts. You can disable Behavior Detection if necessary.

Enable/disable Behavior Detection using the Web Console

1. In the main window of the Web Console, select **Assets (Devices)** > **Policies & profiles**.

2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.

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

4. Go to **Advanced Threat Protection** > **Behavior Detection**.

5. Turn on/off the **Behavior Detection** toggle switch.

6. If Behavior Detection is enabled, select one of the following actions to be performed when malware activity is detected:

   - **Block**

     If this option is selected, the Kaspersky Endpoint Security application terminates the application when detecting malicious activity.

   - **Delete**

     If this option is selected, when detecting malicious activity the Kaspersky Endpoint Security application deletes the executable file of the malicious application and creates a backup copy of the file in Backup.

   - **Prompt for action**

     If this option is selected, then when malware activity is detected, the Kaspersky Endpoint Security application displays a notification window with information about the malicious object and prompts the user to choose the action to be taken by the Kaspersky Endpoint Security application. The available actions may vary depending on the status of the object.

7. If Behavior Detection and Protection of shared folders against external encryption are enabled, select one of the following actions to be performed upon detection of external encryption:

   - **Inform**

     If this option is selected, on detecting an attempt to modify files in shared folders, the Kaspersky Endpoint Security application adds information about this attempt to the list of active threats, adds an entry to local application reports, and sends information about the detected malicious activity to Kaspersky Security Center.

   - **Block attacking device for**

     If this option is selected, when the Kaspersky Endpoint Security application detects an attempt to modify files in shared folders, it blocks access to file modification (read only) for the session that initiated the malicious activity and creates backup copies of the modified files.

8. Save your changes.

Enable/disable Behavior Detection using the Administration Console

1. Start the Administration Console.

2. Maximize the **Administration Server <Server name>** node.

3. In the console tree, click **Managed devices**.

4. In the workspace, select the **Policies** tab.

5. Right-click the policy you want to configure and choose **Properties**.

6. In the **Properties** window, select **Advanced Threat Protection** > **Behavior Detection**

7. Select or deselect the **Behavior Detection** checkbox.

8. If necessary, in the **Action on malware activity detection** section, select the action to be performed when malware activity is detected.

9. Click **OK** to save your changes.

10. Do one of the following to apply the changes to the policy:

    - Click **Apply** to remain in the **Properties: <Policy name>** window after saving changes.
    - Click **OK** to close the **Properties: <Policy name>** window after saving changes.

Enable/disable Behavior Detection using the Kaspersky Endpoint Security application

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.

2. On the **Advanced** tab, in the **Behavior Detection** section, select or deselect the **Enable Behavior Detection** checkbox.

3. If the **Enable Behavior Detection** checkbox is selected, select one of the following actions to be performed when malware activity is detected:

   - **Block**

     If this option is selected, the Kaspersky Endpoint Security application terminates the application when detecting malicious activity.

   - **Delete**

     If this option is selected, when detecting malicious activity the Kaspersky Endpoint Security application deletes the executable file of the malicious application and creates a backup copy of the file in Backup.

   - **Prompt for action**

     If this option is selected, then when malware activity is detected, the Kaspersky Endpoint Security application displays a notification window with information about the malicious object and prompts the user to choose the action to be taken by the Kaspersky Endpoint Security application. The available actions may vary depending on the status of the object.

As a result, if Behavior Detection is enabled, Kaspersky Endpoint Security uses behavior stream signatures to analyze applications' activity in the operating system.

Important: We do not recommend to disable Behavior Detection unless absolutely necessary because doing so will reduce the effectiveness of protection components. To detect threats, the protection components may request data collected by the Behavior Detection component.

Scan

File Threat Protection and Web Threat Protection provide real-time computer protection, but we also recommend that you regularly scan your computer for malware and other computer security threats. Computer scanning is necessary to prevent the spread of malware that has not been detected by the protection components.

Kaspersky Endpoint Security contains the following built-in scan tasks:

- **Full Scan**.

  A malware scan of the computer's memory, startup objects, and all internal disks.

- **Quick Scan**.

  A malware scan of only critical areas of the computer: memory, startup objects, and system folders.

- **Custom Scan**.

  A malware scan of a specified object (file, folder, internal disk, or removable disk).

- **External Disks Scan**

  A malware scan of external disks that is performed when an external disk is connected to the computer.

When the application performs a scan task, malicious objects are recognized through signature analysis. In addition to signature analysis, Kaspersky Endpoint Security uses heuristic analysis and other scanning technologies.

The **Scan** window displays information about the progress of each running scan task (percent complete and time remaining) as well as the scan history (100 most recent scan tasks).

Start Full Scan and Quick Scan tasks

1. On the sidebar of the main application window, click **Scan**.

   The **Scan** window opens.

2. In the **Scan** window, click the **Full Scan** or **Quick Scan** button.

The scan task starts.

Start a Custom Scan task

1. On the sidebar of the main application window, click **Scan**.

   The **Scan** window opens.

2. To start the **Custom Scan** task, do one of the following:

   - Drag a file or folder onto the window.
   - Click **Choose** and open a file or folder.

The scan task starts.

Stop a scan task

1. On the sidebar of the main application window, click **Scan**.

   The **Scan** window opens.

2. In the **Scan** window, click the stop button ( ) next to the scan task that you want to stop.

   A confirmation dialog opens.

3. In the confirmation dialog, click **Stop**.

The scan task stops.

You can schedule a Full Scan or Quick Scan task.

Schedule a scan task from the Scan window

1. On the sidebar of the main application window, click **Scan**.

   The **Scan** window opens.

2. Click **Schedule Scan**.

   A dialog opens where you can set the schedule.

3. Select the **Full Scan** or **Quick Scan** checkbox.

4. Specify the scanning frequency and the scan start time.

5. Click **OK**.

Schedule a scan task from the Settings window

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.

2. On the **Scan** tab, click **Schedule**.

3. In the window that opens, select the checkbox next to the name of the scan task you want to start on a schedule.

4. Configure the scan task frequency and time.

5. Click **OK** to save changes made to the scan task schedule.

When an external disk is connected to the computer, the Kaspersky Endpoint Security application can automatically start scanning the disk, prompt to scan, or do nothing. You can select one of the options in the settings of the External Disk Scan task.

Select the action the Kaspersky Endpoint Security application performs when an external disk is connected to the computer

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.

2. On the **Scan** tab, in the list on the left, select **External Disks Scan**.

3. In the **When an external disk is connected** section, select the action that Kaspersky Endpoint Security performs when an external disk is connected.

The Full Scan and Quick Scan tasks already contain scan scopes. While performing the Full Scan task, the Kaspersky Endpoint Security application scans the computer's memory, startup objects, and all internal disks. While performing the Quick Scan task, the application scans computer memory, startup objects, and system folders. You can change the scan scope of the Quick Scan task.

Note: You can skip scanning of the read-only system volume to significantly reduce scanning time. By default, Kaspersky Endpoint Security does not scan the read-only system volume when performing a Quick Scan task and does scan it when performing a Full Scan task.

Note: Kaspersky Endpoint Security does not scan files that are located in OneDrive or iCloud storage or other cloud storages. Please exclude these files from the scan scope. Otherwise, the scan task may finish with the *Infected File Not Deleted* error.

Enable/disable scanning of the read-only system volume

1. In the menu bar, click the application icon and choose **Settings**.
   The application settings window opens.
2. On the **Scan** tab, in the list on the left, select the **Full Scan** or **Quick Scan** task.
3. In the **Optimization** section, deselect/select the **Skip scanning of read-only system volume** checkbox.

   Important: Optimization might be disabled for security reasons.

Add/remove a file or folder to/from the Quick Scan task scan scope

1. In the menu bar, click the application icon and choose **Settings**.
   The application settings window opens.
2. On the **Scan** tab, in the list on the left, select the **Quick Scan** task.
3. In the **Scan scope** section, click **Edit**.
   A window with the list of objects in the Quick Scan task scan scope opens.
4. Edit the list of scan scope objects:
   - To add a file or folder to the Quick Scan task scan scope:
     a. Click +.
        A pop-up menu where you can select objects to add to the scan scope appears.
     b. Choose the **Files and Folders** item.
        A dialog where you can select a file or folder opens.
     c. Select a file or folder that you want to add to the Quick Scan task scan scope.
     d. Click **Open**.

- To remove a file or folder from the Quick Scan task scan scope:

  a. Select an object that you want to remove.

  b. Drag the selected object from the window or click –.

5. Click **Save**.

Add an object on the default Quick Scan list to the Quick Scan task scan scope

1. In the menu bar, click the application icon and choose **Settings**.
   The application settings window opens.
2. On the **Scan** tab, in the list on the left, select the **Quick Scan** task.
3. In the **Scan scope** section, click **Edit**.
   A window with the list of objects in the scan scope opens.
4. Click +.
   A pop-up menu where you can select objects to add to the scan scope appears.
5. In the pop-up menu, select an object that you want to add to the scan scope (for example, **Memory**).
6. Click **OK**.

Disable protection of an object in the Quick Scan task scan scope

1. In the menu bar, click the application icon and choose **Settings**.
   The application settings window opens.
2. On the **Scan** tab, in the list on the left, select the **Quick Scan** task.
3. In the **Scan scope** section, click **Edit**.
   A window with the list of scan scope objects opens.
4. Deselect the checkbox next to the object in the list of scan scope objects.
5. Click **OK**.

If a threat is detected in a file, the application displays a notification and performs the specified action on the object. You can modify the action to perform when an object is detected.

Select the action that Kaspersky Endpoint Security performs after detecting infected files

1. In the menu bar, click the application icon and choose **Settings**.
   The application settings window opens.
2. On the **Scan** tab, select a task in the task list.
3. In the **Action** section, select the action that the application performs after detecting infected files.

Before disinfecting or deleting an infected file, Kaspersky Endpoint Security saves a copy of it in Backup, so you can restore the original file, if necessary.

Information about the results of scan tasks and all detected objects is logged in a report.

Note: If any errors occur while running a malware scan task, start the task again. If the new attempt to run the scan also results in an error, contact Kaspersky Technical Support.

View a scan task report

1. In the menu bar, choose **Protection** > **Reports**.

   The **Reports** window opens.

2. Open the **Scan** tab.

Update tasks

Timely updates of application databases ensure that your computer is always protected. File Threat Protection, Web Threat Protection, and scan tasks use application databases to detect and neutralize malware on your computer. Application databases are updated regularly with different kinds of threats and ways to neutralize them, so it is important that you update the databases regularly.

Kaspersky Endpoint Security downloads application databases and new application modules from Kaspersky update servers and installs them on your computer. Kaspersky Endpoint Security can also use distribution points, local folders, or other web servers.

Note: Internet access is required for connecting to the update servers and downloading updates. If you connect to the internet via a proxy server, you may need to configure the network settings.

Application database updates can be downloaded in one of the following ways:

- **Automatically**. Kaspersky Endpoint Security regularly checks Kaspersky update servers for updates. If a new update is available on the update server, Kaspersky Endpoint Security downloads the update in the background and installs it on your computer. This option is enabled by default.
- **Manually**. You can manually check for Kaspersky Endpoint Security updates at any time.

Enable/disable automatic downloads of Kaspersky Endpoint Security database updates

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.

2. On the **Update** tab, in the **Databases** section, select/deselect the **Download updates automatically** checkbox.

Check for Kaspersky Endpoint Security database updates

1. On the sidebar of the main application window, click **Update**.

   The **Update** window opens.

2. Click **Update**.

The application starts updating databases.

You can also start an update task in one of the following ways:

- Click the application icon and choose **Update**.
- In the menu bar, choose **Protection** > **Update**.

During an update, the application databases and modules are compared with the ones currently available on the update servers. If the latest version of the databases is installed on your computer, the **Update** window displays a message saying that the application databases are up to date. If the application version and application databases differ from those currently available on the update servers, only the missing components of the update are downloaded and installed on your computer. Incremental updates of application databases take less time and require less web traffic.

If you connect to the internet via a proxy server, you can configure the proxy server connection settings. Kaspersky Endpoint Security uses these settings to update application databases and download application module updates.

Configure a connection to a proxy server

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.

2. Select the **Update** tab.
3. In the **Proxy** section, select the **Use proxy server** checkbox and click **Settings**.

   A window opens, in which you can configure the proxy server connection settings.

4. Configure the connection to a proxy server.
5. Click **Save** to save the changes made to the proxy server connection settings.

Before updating the application databases Kaspersky Endpoint Security creates backup copies of them, so a rollback can be performed, if necessary. The rollback feature is useful if a new version of the application databases contains an incorrect signature that makes Kaspersky Endpoint Security block a safe application.

Note: If Kaspersky Endpoint Security databases become corrupted, we recommend that you start an update to download and install the latest version of application databases.

Roll back the last update

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.

2. Select the **Update** tab.
3. In the **Rollback** section, click **Roll Back Update**.

Kaspersky Endpoint Security provides a detailed report on the results of update tasks in the **Reports** window.

View an update task report

1. In the menu bar, choose **Protection** > **Reports**.
2. The **Reports** window opens.
3. Open the **Database Update** tab.

Note: Updates functionality (including providing anti-malware signature updates and codebase updates), as well as KSN functionality may not be available in the software in the U.S.

Local tasks

External Disks Scan task

Kaspersky Endpoint Security can scan all files that you run or copy, even if the file is located on an external disk. To prevent the spread of malware, you can configure automatic scans of external disks when they are connected to the device.

The following External Disks Scan settings can be configured:

- **The action that Kaspersky Endpoint Security performs when an external disk is connected.**

  Scan

  If this option is selected, Kaspersky Endpoint Security starts a malware scan task for the connected external disk.

  This option is selected by default.

  Do nothing

  If this option is selected, Kaspersky Endpoint Security does not scan the connected external disk.

- **The action that Kaspersky Endpoint Security performs upon detecting a malicious object.**

  Disinfect, delete if disinfection fails

  If this option is selected, Kaspersky Endpoint Security blocks access to the infected object and attempts to disinfect it without requesting confirmation from the user.

  If the object is disinfected, Kaspersky Endpoint Security saves it in its original location under the original file name. If disinfection fails, Kaspersky Endpoint Security deletes the infected objects that could not be disinfected.

  This option is selected by default.

  Prompt for action

  If this option is selected, Kaspersky Endpoint Security displays a notification window with information about the malicious object, and prompts the user to choose the action to be taken by Kaspersky Endpoint Security. The available actions may vary depending on the status of the object.

You can configure External Disks Scan in the Administration Console, Web Console, or in the Kaspersky Endpoint Security application.

How to configure External Disks Scan in the Administration Console (MMC)

1. Start Kaspersky Security Center Administration Console.
2. Maximize the **Administration Server <Server name>** node.
3. In the console tree, click **Managed devices**.
4. In the workspace, select the **Policies** tab.
5. Right-click the policy you want to configure and choose **Properties**.
6. In the **Properties** window, select **Local Tasks** > **External Disks Scan**.
7. Configure the task settings.
8. Click **OK** to save your changes.

How to configure running the External Disks Scan in the Web Console and Cloud Console

1. In the main window of the Web Console, select **Devices** > **Policies & profiles**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Select **Local Tasks** > **External Disks Scan**.
5. Configure the task settings.
6. Click OK to save your changes.

How to configure running the External Disks Scan in the application interface

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.
2. On the **Scan** tab, in the list on the left, select **External Disks Scan**.
3. In the **When an external disk is connected** section, select the action that Kaspersky Endpoint Security performs when an external disk is connected.

Backup

Sometimes the integrity of infected files cannot be preserved during the disinfection process. If a disinfected file contained important information that is partly or completely inaccessible following disinfection, you can restore the original file from Backup.

A *backup copy* is a copy of a dangerous file that is created when the file is disinfected or deleted. It is stored in Backup.

Backup is a special storage area that contains backup copies of files that have been deleted or modified during disinfection. The main function of Backup is to let the user restore an original file at any time. Files in Backup are saved in a special format and are not dangerous for the computer.

View the contents of Backup

1. In the menu bar, choose **Protection** > **Detected Objects**.

   The **Detected Objects** window opens.

2. In the **Back up** section, view the list of backed up files.

You can restore or remove backup copies of files from Backup.

Restore a backup copy of a file from Backup

1. In the menu bar, choose **Protection** > **Detected Objects**.

   The **Detected Objects** window opens.

2. In the **Back up** section, click ••• next to the file that you want to restore.

   The pop-up menu opens.

3. Choose **Restore File**.

   A window for specifying the file name, tag, and folder to which the file will be restored opens. By default, the original file name and location are already specified.

4. Specify the file name and folder to which the file will be restored.

5. Click **Save**.

The application restores the file to the specified location with the specified name.

You need to scan the file for malware immediately after restoring it. It is possible that the object can be disinfected using updated databases without becoming corrupted.

Important: We recommend that you not restore backup copies of files unless restoring them is absolutely necessary, because doing so could lead to a computer infection.

Remove a backup copy of a file from Backup

1. In the menu bar, choose **Protection** > **Detected Objects**.

   The **Detected Objects** window opens.

2. In the **Back up** section, do the following:

   - To delete all backup copies of files, click **Delete All**.
   - To delete the selected backup copy, click ••• next to it and choose **Delete Backed Up Copy**.

By default, the storage period for files in Backup is 30 days. When this period expires, the files are deleted. You can change the maximum Backup storage period for files or remove the limit on the storage period.

Configure the storage period for files in Backup

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.

2. On the **Threats** tab, in the **Backup** section, select the **Delete backed up objects after <number> days** checkbox and specify the period after which files stored in Backup are automatically deleted.

Reports

You can view a Kaspersky Endpoint Security report listing all detected objects on the **Processed objects** tab. System events are displayed on the **System events** tab. Additionally, a separate detailed report is created for each of the following application components: File Threat Protection, Web Threat Protection, Network Threat Protection, Behavior Detection, and scan and update tasks.

Open the Reports window

In the menu bar, choose **Protection** > **Reports**.

Kaspersky Endpoint Security can save reports in text format. This functionality may be useful if application components or tasks produce errors you cannot fix on your own and you need assistance from Kaspersky Technical Support. In this case, send the text report to Kaspersky Technical Support so our specialists can study the problem and fix it as quickly as possible.

Export a Kaspersky Endpoint Security component report or task report to a text file

1. In the menu bar, choose **Protection** > **Reports**.

   The **Reports** window opens.

2. In the left pane, select the tab with the desired report.

3. In the upper-right corner, click  .

4. In the window that opens, specify the file name, tags, and destination folder for the report.

5. Click **Save**.

By default, Kaspersky Endpoint Security doesn't log informational events in reports. You can allow logging of informational events.

Allow logging of informational events in reports

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.

2. On the **Interface** tab, in the **Reports** section, select the **Log non-critical events** checkbox to receive notifications about informational Kaspersky Endpoint Security events.

Managed Detection and Response

The Managed Detection and Response component was added in Kaspersky Endpoint Security in version 11.2. This component interacts with a solution known as Kaspersky Managed Detection and Response. *Kaspersky Managed Detection and Response (MDR)* continuously searches for, detects, and eliminates threats aimed at your organization. For detailed information about how the solution works, please refer to the *Kaspersky Managed Detection and Response Help*.

When interacting with Kaspersky Managed Detection and Response, the application lets you perform the following functions:

- Activate Managed Detection and Response using a BLOB configuration file.
- Execute commands from Kaspersky Managed Detection and Response.
- Send telemetry data to Kaspersky Managed Detection and Response for threat detection.

The Managed Detection and Response component has the following additional requirements:

- macOS 12 or later
- Intel-based Mac, Apple silicon
- Active Kaspersky Endpoint Security license

Integration with Kaspersky Managed Detection and Response

Integration with Kaspersky Managed Detection and Response consists of the following steps:

1. **Configuring the Kaspersky Security Network proxy server**

   The Kaspersky Security Network proxy server facilitates data exchange between computers and the Kaspersky Security Network cloud service infrastructure via the Administration Server instead of direct exchange.

   Load the Kaspersky Security Network configuration file in the Administration Server properties. The Kaspersky Security Network configuration file is located in the ZIP archive of the MDR configuration file. You can get the ZIP archive in the Kaspersky Managed Detection and Response Console. For details on configuring the Kaspersky Security Network proxy server, please refer to the *Kaspersky Security Center Help*.

   As a result, Kaspersky Endpoint Security will use Private KSN to determine the reputation of files, applications, and websites. The *"Infrastructure: Kaspersky Private Security Network"* operating status will be indicated in the policy settings in the Kaspersky Security Network section.

   Usage of Private KSN with Kaspersky Managed Detection and Response ensures that telemetry is sent to GDPR (General Data Protection Regulation) compliant servers. If Private KSN is not used, telemetry can be sent to the Global KSN. This may violate the laws of your country.

   Important: You must enable extended KSN mode for Managed Detection and Response to work.

2. **Activating Managed Detection and Response**

Load the BLOB configuration file in the Kaspersky Endpoint Security policy (see the instructions below). The BLOB file contains the client ID and information about the license for Kaspersky Managed Detection and Response. The BLOB file is located in the ZIP archive of the MDR configuration file. You can get the ZIP archive in the Kaspersky Managed Detection and Response Console. For detailed information about a BLOB file, please refer to the *Kaspersky Managed Detection and Response Help*.

Activate Managed Detection and Response in the Administration Console (MMC)

1. Start Kaspersky Security Center Administration Console.
2. Maximize the **Administration Server <Server name>** node.
3. In the console tree, click **Managed devices**.
4. In the workspace, select the **Policies** tab.
5. Right-click the policy you want to configure and choose **Properties**.
6. In the **Properties** window, select **Detection and Response** > **Managed Detection and Response**.
7. Select the **Managed Detection and Response** checkbox.
8. In the **MDR configuration file** block, click **Import** and select the BLOB file received in the Kaspersky Managed Detection and Response Console. The file has the .P7 extension.
9. Click **OK** to save your changes.

Activate Managed Detection and Response in the Web Console and Cloud Console

1. In the main window of Web Console, select **Devices** > **Policies and profiles**.
2. Click the name of the Kaspersky Endpoint Security for Mac policy.
3. The policy properties window opens.
4. Select the **Application settings** tab.
5. Select **Detection and Response** > **Managed Detection and Response**.
6. Turn on the **Managed Detection and Response** toggle switch.
7. Click **Import** and select the BLOB file that was obtained in the Kaspersky Managed Detection and Response Console. The file has the .P7 extension.
8. Save your changes.

As a result, Kaspersky Endpoint Security will verify the BLOB file. BLOB file verification includes checking the digital signature and the license term. If the BLOB file is successfully verified, Kaspersky Endpoint Security will load the file and send the file to the computer during the next synchronization with Kaspersky Security Center.

Endpoint Detection and Response (KATA)

Kaspersky Endpoint Security supports integration with the Kaspersky Endpoint Detection and Response component as part of the Kaspersky Anti Targeted Attack Platform solution. This solution is designed to promptly detect advanced threats, such as targeted attacks, advanced persistent threats, zero-day attacks, and others. For detailed information about how the solution works, please refer to the *Kaspersky Anti Targeted Attack Platform Help*.

When integration with Endpoint Detection and Response (KATA) is configured, the KATA server receives information about events that occur in the operation of Kaspersky Endpoint Security, threats discovered by the application, as well as information about processing these threats. To react to detected threats, Kaspersky Endpoint Security may then perform tasks started in the Kaspersky Anti Targeted Attack Platform web interface.

Endpoint Detection and Response (KATA) has the following additional requirements:

- Kaspersky Anti Targeted Attack Platform 6.0 or later.
- Kaspersky Security Center 14.2 or later.
- Integration with Endpoint Detection and Response (KATA) can be configured in the Kaspersky Security Center Administration Console (MMC), Web Console, or Cloud Console.

Integration with Kaspersky Endpoint Detection and Response (KATA)

Integration with Kaspersky Endpoint Detection and Response (KATA) consists of the following steps:

1. **Installing the Endpoint Detection and Response component**

   You can select the Endpoint Detection and Response component during installation of Kaspersky Endpoint Security.

2. **Activating Endpoint Detection and Response**

   If the Endpoint Detection and Response component is not supported by your current license, you need to activate Kaspersky Endpoint Detection and Response separately.

   You can check whether the Endpoint Detection and Response functionality is supported by the current license in the **License** window.

3. **Connecting to a KATA server**

   Kaspersky Anti Targeted Attack Platform requires establishing a trusted connection between Kaspersky Endpoint Security and a KATA server. To configure a trusted connection, you need to use a TLS certificate. You can download a TLS certificate in the Kaspersky Anti Targeted Attack Platform web interface. For detailed information about downloading a certificate, please refer to the *Kaspersky Anti Targeted Attack Platform Help*.

   By default, Kaspersky Endpoint Security checks the TLS certificate of only the KATA server. To make the connection more secure, you can enable two-way verification. To enable two-way verification, you need to use a password-protected crypto-container. For detailed information about downloading a crypto-container, please refer to the *Kaspersky Anti Targeted Attack Platform Help*.

Connect computers with Kaspersky Endpoint Security to a KATA server using the Administration Console

1. Start the Administration Console.
2. Maximize the **Administration Server <Server name>** node.
3. In the console tree, click **Managed devices**.
4. In the workspace, select the **Policies** tab.
5. Right-click the policy you want to configure and choose **Properties**.
6. In the **Properties** window, select **Detection and Response** > **Endpoint Detection and Response (KATA)**.
7. Select the **Endpoint Detection and Response (KATA)** checkbox.
8. Click **Server connection settings**.
9. In the **Server connection settings** window that opens, configure the following settings:
   - Click **Add TLS certificate** to select a TLS certificate that will be used to establish a trusted connection with a KATA server.
   - If you want to change the KATA server response timeout, specify the timeout in the **Timeout (s)** field. When the timeout runs out, Kaspersky Endpoint Security tries to connect to a different KATA server.
   - If you want to use two-way verification, select the **Use two-way verification** checkbox. Click **Load crypto-container** to select a crypto-container file and enter the password in the **Crypto-container password** field.
10. Click **Save**.
11. To add a KATA server, click **Add**.
12. In the **KATA server** window that opens, specify the server address and port and click **Save**.
13. Click **OK** to save your changes.

Connect computers with Kaspersky Endpoint Security to a KATA server using the Web Console

1. In the main window of the Web Console, select **Devices** > **Policies and profiles**.
2. Click the name of the Kaspersky Endpoint Security for Mac policy.
   The policy properties window opens.
3. Select the **Application settings** tab.
4. Select **Detection and Response** > **Endpoint Detection and Response (KATA)**.
5. Turn on the **Endpoint Detection and Response (KATA)** toggle switch.
6. Click **Server connection settings**.

7. In the **Server connection settings** dialog that opens, configure the following settings:

   - Click **Add TLS certificate** to select a TLS certificate that will be used to establish a trusted connection with a KATA server.
   - If you want to change the KATA server response timeout, specify the timeout in the **Timeout (s)** field. When the timeout runs out, Kaspersky Endpoint Security tries to connect to a different KATA server.
   - If you want to use two-way verification, select the **Use two-way verification** checkbox. Click **Load crypto-container** to select a crypto-container file and enter the password in the **Crypto-container password** field.

8. Click **OK**.
9. To add a KATA server, click **Add**.
10. In the dialog that opens, specify the server address and port and click **OK**.
11. Save your changes.

As a result, computers will appear in the Kaspersky Anti Targeted Attack Platform web interface.

Endpoint Detection and Response Optimum

Starting with version 12.1, Kaspersky Endpoint Security for Mac includes a built-in agent for the Kaspersky Endpoint Detection and Response Optimum solution (hereinafter also "EDR Optimum"). This solution is designed to protect the corporate IT infrastructure from advanced cyber threats. The functionality of the solution combines automatic detection of threats with the ability to react to these threats to counteract advanced attacks including new exploits, ransomware, fileless attacks, as well as methods using legitimate system tools. For details about the solution, see the Kaspersky Endpoint Detection and Response Optimum Help.

Kaspersky Endpoint Detection and Response reviews and analyses threat development and provides *security personnel* or the *Administrator* with information about the potential attack that is necessary for a timely response. Kaspersky Endpoint Detection and Response displays alert details in a separate window. *Alert Details* is a tool for viewing the entirety of collected information about a detected threat. Alert details include, for example, the history of files appearing on the computer. For details about managing alert details, refer to the Kaspersky Endpoint Detection and Response Optimum Help.

Note: You can configure the EDR Optimum component in Web Console.

Endpoint Detection and Response settings

Parameter	Description
Network isolation	Automatic isolation of the computer from the network in response to detected threats. When network isolation is turned on, the application severs all active connections and blocks all new TCP/IP connections on the computer. The application leaves only the following connections active: • Connections listed in Network isolation exclusions. • Connections initiated by Kaspersky Endpoint Security services. • Connections initiated by the Kaspersky Security Center Network Agent.
Automatically unlock isolated computer in N hours	Network isolation can be turned off automatically after a specified time or manually. By default, Kaspersky Endpoint Security turns off Network isolation 8 hours after the start of the isolation.

Parameter	Description
Network Isolation Exclusions	List of rules for exclusions from network isolation. Network connections that match the rules are not blocked on computers when Network isolation is turned on. To configure Network isolation exclusions, you can use a list of standard network profiles. By default, exclusions include network profiles containing rules that ensure uninterrupted operation of devices with the DNS/DHCP server and DNS/DHCP client roles. You can also modify the settings of standard network profiles or define exclusions manually. **Important:** Exclusions specified in policy properties are applied only if Network isolation is turned on automatically in response to a detected threat. Exclusions specified in computer properties are applied only if Network isolation is turned on manually in computer properties in the Kaspersky Security Center console or in alert details.
Execution prevention	Execution prevention allows managing the running of executable files and scripts, as well as opening office format files. In this way, you can, for example, prevent the execution of applications that you consider insecure. As a result, the spreading of the threat can be stopped. Execution prevention supports a set of script interpreters. To use Execution prevention component, you need to add execution prevention rules. Execution prevention rule is a set of criteria that the application takes into account when reacting to an object execution, for example when blocking object execution. The application identifies files by their paths or checksums calculated using MD5 and SHA256 hashing algorithms.
Action on execution or opening of forbidden object	**Block and write to report**. In this mode, the application blocks the execution of objects or opening of documents that match prevention rule criteria. The application also publishes an event about attempts to execute objects or open documents to the Kaspersky Security Center event log and the unified logging system. **Log events only**. In this mode, Kaspersky Endpoint Security publishes an event about attempts to run executable objects or open documents that match prevention rule criteria to the Kaspersky Security Center event log and the unified logging system, but does not block the attempt to run or open the object or document. This mode is selected by default.
Cloud Sandbox	Cloud Sandbox is a technology that lets you detect advanced threats on a computer. Kaspersky Endpoint Security automatically forwards detected files to Cloud Sandbox for analysis. Cloud Sandbox runs these files in an isolated environment to identify malicious activity and decides on their reputation. Data on these files is then sent to Kaspersky Security Network. Therefore, if Cloud Sandbox has detected a malicious file, Kaspersky Endpoint Security will perform the appropriate action to eliminate this threat on all computers where this file is detected. **Note:** Cloud Sandbox technology is permanently enabled and is available to all Kaspersky Security Network users regardless of the type of license they are using.

Integration with Endpoint Detection and Response Optimum

To integrate with Kaspersky Endpoint Detection and Response, you must add the Endpoint Detection and Response Optimum (EDR Optimum) component and configure Kaspersky Endpoint Security.

Note: EDR Optimum and Endpoint Detection and Response (KATA) components are not compatible with each other.

The following conditions must be fulfilled for Endpoint Detection and Response to work:

- Kaspersky Security Center version is 13.2 or higher. In earlier versions of Kaspersky Security Center, it is impossible to activate the Endpoint Detection and Response feature.
- Kaspersky Endpoint Detection and Response administration plug-in is installed. This is a single plug-in for working with agents on Windows, Mac and Linux operating systems. When working with Endpoint Detection and Response Optimum, you will need the Kaspersky Endpoint Security administration plug-in to create threat response tasks and the EDR administration plug-in to view alert details.
- The EDR Optimum component as part of Kaspersky Endpoint Security supports interaction with the Kaspersky Endpoint Detection and Response Optimum 3.0 solution. Interaction with earlier versions of Kaspersky Endpoint Detection and Response Optimum is not supported.

- EDR Optimum can be managed in the Web Console.
- The application is activated and the functionality is covered by the license.
- The Endpoint Detection and Response component is turned on.

Integration with Kaspersky Endpoint Detection and Response Optimum

Integration with Kaspersky Endpoint Detection and Response Optimum consists of the following steps:

1. **Installing the Endpoint Detection and Response Optimum component**

   You can select the Endpoint Detection and Response component during installation of Kaspersky Endpoint Security.

2. **Activating Endpoint Detection and Response**

   If the Endpoint Detection and Response component is not supported by your current license, you need to activate Kaspersky Endpoint Detection and Response separately.

   You can check whether the Endpoint Detection and Response functionality is supported by the current license in the **License** window.

3. **Enabling Endpoint Detection and Response component**

   You can enable or disable the component in Kaspersky Endpoint Security for Mac policy settings.

   How to enable or disable the Endpoint Detection and Response component in the Web Console

   1. In the main window of the Web Console, select **Assets (Devices)** > **Policies & profiles**.
   2. Click the name of the Kaspersky Endpoint Security policy.
      The policy properties window opens.
   3. Select the **Application settings** tab.
   4. Go to **Detection and Response** > **Endpoint Detection and Response**.
   5. Turn on the **Endpoint Detection and Response** toggle switch.
   6. Save your changes.

Scan for indicators of compromise

An **Indicator of Compromise (IOC)** is a set of data about an object or activity that indicates unauthorized access to the computer (compromise of data). For example, many unsuccessful attempts to sign in to the system can constitute an Indicator of Compromise. The **IOC Scan** task allows finding Indicators of Compromise on the computer and taking threat response measures.

Kaspersky Endpoint Security searches for indicators of compromise using IOC files. IOC files are files containing the sets of indicators that the application tries to match to count a detection. IOC files must comply with the requirements for IOC files.

IOC Scan task run mode

Kaspersky Endpoint Detection and Response lets you create standard IOC Scan tasks to detect compromised data. Standard IOC scan task is a group or local task that is created and configured manually in the Web Console. Tasks are run using IOC files prepared by the user. If you want to add an indicator of compromise manually, please read the requirements for IOC files.

Creating an IOC Scan task

You can create IOC Scan tasks manually:

- In alert details (only for EDR Optimum).

  Alert Details is a tool for viewing the entirety of collected information about a detected threat. Alert details include, for example, the history of files appearing on the computer. For details about managing alert details, refer to the Kaspersky Endpoint Detection and Response Optimum Help.

- Using the Task Wizard.

To create an IOC Scan task:

1. In the main window of the Web Console, select **Assets (Devices)** > **Tasks**.

   The list of tasks opens.

2. Click **Add**.

   The **New task wizard** starts.

3. Configure the task settings:

   a. In the **Application** drop-down list, select Kaspersky Endpoint Security for Mac (12.2).

   b. In the **Task type** drop-down list, select **IOC Scan**.

   c. In the **Task name** field, enter a brief description.

   d. In the **Select devices to which the task will be assigned** block, select the task scope.

4. Select devices according to the selected task scope option.

5. In the **IOC Scan settings** section, load the IOC files to search for indicators of compromise. You can add an IOC file or generate one from a file containing file hashes or IP addresses.

   After loading the IOC files, you can view and edit the list of indicators from IOC files.

   Note: Adding or removing IOC files after running the task is not recommended. This can cause the IOC scan results to display incorrectly for prior runs of the task. To search indicators of compromise by new IOC files, it is recommended to add new tasks.

6. Configure actions on IOC detection:

   - **Isolate computer from the network**. If this option is selected, Kaspersky Endpoint Security isolates the computer from the network to prevent the threat from spreading. You can configure the duration of the isolation in Endpoint Detection and Response component settings.

   - **Move copy to Quarantine and delete object**. If this option is selected, Kaspersky Endpoint Security deletes the malicious object found on the computer. Before deleting the object, Kaspersky Endpoint Security creates a backup copy in case the object needs to be restored later. Kaspersky Endpoint Security moves the backup copy to Quarantine.

   - **Run critical areas scan**. If this option is selected, Kaspersky Endpoint Security runs the Quick Scan task. By default, Kaspersky Endpoint Security scans the memory, startup objects, and system folders.

7. Go to the **Advanced** section.

8. Select data types (IOC documents) that must be analyzed as part of the task.

   Note: Kaspersky Endpoint Security automatically selects data types (IOC documents) for the IOC Scan task in accordance with the content of loaded IOC files. It is not recommended to deselect data types.

   You can additionally configure scan scopes for the following data types:

   - **Processes – ProcessItem**
   - **Files – FileItem**
   - **Network ports – PortItem**
   - **User accounts – UserItem**
   - **ARP tables – ArpEntryItem**
   - **Hosts – SystemInfoItem**
   - **URLs – UrlHistoryItem**
   - **Routes – RouteEntryItem**

9. Click **OK**.

10. Enter the account credentials of the user whose rights you want to use to run the task. Click **Next**.

    Note: By default, Kaspersky Endpoint Security starts the task as the system user account (root).

11. At the **Finish task creation** step, click the **Finish** button to create the task and close the wizard.

    If you enabled the **Open task details when creation is complete** option, the task settings window opens. In this window, you can check the task parameters, modify them, or configure a task start schedule, if necessary.

12. Click the new task.

    The task properties window opens.

13. Select the **Schedule** tab.

14. Configure the task schedule.

    Note: Make sure the computer is turned on to run the task.

15. Click the **Save** button.

16. To run the task immediately regardless of the configured schedule, do the following:

    a. Select the checkbox next to the task.

17. Click the **Run** button.

    As a result, Kaspersky Endpoint Security runs the search for indicators of compromise on the computer. You can view the results of the task in task properties in the **Results** section. You can view the information about detected indicators of compromise in the task properties: **Application settings** > **IOC Scan results**.

Note: IOC scan results are kept for 30 days. After this period, Kaspersky Endpoint Security automatically deletes the oldest entries.

Move file to Quarantine

When reacting to threats, Kaspersky Endpoint Detection and Response can create *Move file to Quarantine* tasks. This is necessary to minimize the consequences of the threat. *Quarantine* is a special local storage on the computer. The user can quarantine files that the user considers dangerous for the computer. Quarantined files are stored in an encrypted state and do not threaten the security of the device. Kaspersky Endpoint Security uses Backup as a file storage. For details on managing Quarantine as part of solutions, please refer to the Kaspersky Endpoint Detection and Response Optimum Help.

You can create *Move file to Quarantine* tasks in the following ways:

- In alert details (only for EDR Optimum).

  Alert Details is a tool for viewing the entirety of collected information about a detected threat. Alert details include, for example, the history of files appearing on the computer. For details about managing alert details, refer to the Kaspersky Endpoint Detection and Response Optimum Help.

- Using the Task Wizard.

  You must enter the file path or hash (SHA256 or MD5), or both the file path and the file hash.

The *Move file to Quarantine* task has the following limitations:

- The file size must not exceed 100 MB.
- You can configure the task for EDR Optimum in Web Console.
- The Backup capacity is limited by the free disk space.

To create a Move file to Quarantine task:

1. In the main window of the Web Console, select **Assets (Devices)** > **Tasks**.

   The list of tasks opens.

2. Click **Add**.

   The **New task wizard** starts.

3. Configure the task settings:

   a. In the **Application** drop-down list, select Kaspersky Endpoint Security for Mac (12.2).

   b. In the **Task type** drop-down list, select **Move file to Quarantine**.

   c. In the **Task name** field, enter a brief description.

   d. Select one of the following options:

   - **Assign task to an administration group**

     The task is assigned to devices included in an administration group. You can specify one of the existing groups or create a new one.

     For example, you may want to use this option to run a task of sending a message to users if the message is specific for devices included in a specific administration group.

     If a task is assigned to an administration group, the **Security** tab is not displayed in the task properties window because group tasks are subject to the security settings of the groups to which they apply.

   - **Specify device addresses manually or import addresses from a list**

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

     You may want to use this option to execute a task for a specific subnet. For example, you may want to install a certain application on devices of accountants or to scan devices in a subnet that is probably infected.

   - **Assign task to a device selection**

     The task is assigned to devices included in a device selection. You can specify one of the existing selections.

     For example, you may want to use this option to run a task on devices with a specific operating system version.

4. Select devices according to the selected task scope option.

5. At the **Task scope** step, specify an administration group, devices with specific addresses, or a device selection.

   The available settings depend on the option selected at the previous step.

6. In the list of files, click **Add**.

   The file adding wizard starts.

7. In the **Please specify the file to move to Quarantine** drop-down list, select one of the options and fill in the required fields. To add the file, you must enter the full path to the file, or both file hash and the path.

8. If you want the task to be applicable to critical system objects, select the **Apply to critical system objects** checkbox.

9. Enter the account credentials of the user whose rights you want to use to run the task. Click **Next**.

   Note: By default, Kaspersky Endpoint Security starts the task as the system user account (root).

10. At the **Finish task creation** step, click the **Finish** button to create the task and close the wizard.

    If you enabled the **Open task details when creation is complete** option, the task settings window opens. In this window, you can check the task parameters, modify them, or configure a task start schedule, if necessary.

11. Click the new task.

    The task properties window opens.

12. Select the **Schedule** tab.

13. Configure the task schedule.

    Note: Make sure the computer is turned on to run the task.

14. Click the **Save** button.

15. To run the task immediately regardless of the configured schedule, do the following:

    a. Select the checkbox next to the task.

16. Click the **Run** button.

As a result, Kaspersky Endpoint Security moves the file to Quarantine.

The *Move file to Quarantine* task can finish with the *Access denied* error if you are trying to quarantine an executable file that is currently running. Create a terminate process task for the file and try again.

The *Move file to Quarantine* task can finish with the *Not enough space in Quarantine storage* error if you are trying to quarantine a file that is too large. Free up the disk space and try again.

Get file

You can get files from user computers. For example, you can configure getting an event log file created by a third-party application. To get the file, you must create a dedicated task. As a result of the execution of the task, the file is saved in Backup. You can download this file from Backup to your computer using Web Console. On the user's computer, the file remains in its original folder.

Important: The file size must not exceed 100 MB. The Backup capacity is limited by the free disk space.

To create a Get file task:

1. In the main window of the Web Console, select **Assets (Devices)** > **Tasks**.

   The list of tasks opens.

2. Click **Add**.

   The **New task wizard** starts.

3. Configure the task settings:

   a. In the **Application** drop-down list, select Kaspersky Endpoint Security for Mac (12.2).

   b. In the **Task type** drop-down list, select **Get file**.

   c. In the **Task name** field, enter a brief description.

   d. Select one of the following options:

   - **Assign task to an administration group**

     The task is assigned to devices included in an administration group. You can specify one of the existing groups or create a new one.

     For example, you may want to use this option to run a task of sending a message to users if the message is specific for devices included in a specific administration group.

     If a task is assigned to an administration group, the **Security** tab is not displayed in the task properties window because group tasks are subject to the security settings of the groups to which they apply.

   - **Specify device addresses manually or import addresses from a list**

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

     You may want to use this option to execute a task for a specific subnet. For example, you may want to install a certain application on devices of accountants or to scan devices in a subnet that is probably infected.

   - **Assign task to a device selection**

     The task is assigned to devices included in a device selection. You can specify one of the existing selections.

     For example, you may want to use this option to run a task on devices with a specific operating system version.

4. Select devices according to the selected task scope option. In the **Get file** window, click **Add**.

   The **Get file** dialog opens.

5. In the **Specify which file you need to get** drop-down list, select one of the options and fill in the required fields.

   To add the file, you must enter the full path to the file, or both file hash and the path.

6. Click **OK**.

   Settings of the file to be added will be displayed in the list of files.

7. Click **Next**.

8. Enter the account credentials of the user whose rights you want to use to run the task. Click **Next**.

   Note: By default, Kaspersky Endpoint Security starts the task as the system user account (root).

9. At the **Finish task creation** step, click the **Finish** button to create the task and close the wizard.

   If you enabled the **Open task details when creation is complete** option, the task settings window opens. In this window, you can check the task parameters, modify them, or configure a task start schedule, if necessary.

10. Click the new task.

    The task properties window opens.

11. Select the **Schedule** tab.

12. Configure the task schedule.

    Note: Make sure the computer is turned on to run the task.

13. Click the **Save** button.

14. To run the task immediately regardless of the configured schedule, do the following:

    a. Select the checkbox next to the task.

15. Click the **Run** button.

As a result, Kaspersky Endpoint Security creates a copy of the file and moves that copy to Backup. You can download the file from Backup in Web Console.

Delete file

You can remotely delete files using the *Delete file* task. For example, you can remotely delete a file when responding to threats.

To create a Delete file task:

1. In the main window of the Web Console, select **Assets (Devices)** > **Tasks**.

   The list of tasks opens.

2. Click **Add**.

   The **New task wizard** starts.

3. Configure the task settings:

   a. In the **Application** drop-down list, select Kaspersky Endpoint Security for Mac (12.2).

   b. In the **Task type** drop-down list, select **Delete file**.

   c. In the **Task name** field, enter a brief description.

d. Select one of the following options:

- **Assign task to an administration group**

  The task is assigned to devices included in an administration group. You can specify one of the existing groups or create a new one.

  For example, you may want to use this option to run a task of sending a message to users if the message is specific for devices included in a specific administration group.

  If a task is assigned to an administration group, the **Security** tab is not displayed in the task properties window because group tasks are subject to the security settings of the groups to which they apply.

- **Specify device addresses manually or import addresses from a list**

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

  You may want to use this option to execute a task for a specific subnet. For example, you may want to install a certain application on devices of accountants or to scan devices in a subnet that is probably infected.

- **Assign task to a device selection**

  The task is assigned to devices included in a device selection. You can specify one of the existing selections.

  For example, you may want to use this option to run a task on devices with a specific operating system version.

4. Select devices according to the selected task scope option.

5. In the **Specify which file you need to delete** drop-down list, select one of the options and fill in the required fields. To add the file, you must enter the full path to the file, or both file hash and the path.

6. If you want the task to be applicable to critical system objects, select the **Apply to critical system objects** checkbox.

7. Enter the account credentials of the user whose rights you want to use to run the task. Click **Next**.

   Note: By default, Kaspersky Endpoint Security starts the task as the system user account (root).

8. At the **Finish task creation** step, click the **Finish** button to create the task and close the wizard.

   If you enabled the **Open task details when creation is complete** option, the task settings window opens. In this window, you can check the task parameters, modify them, or configure a task start schedule, if necessary.

9. Click the new task.

   The task properties window opens.

10. Select the **Schedule** tab.

11. Configure the task schedule.

    Note: Make sure the computer is turned on to run the task.

12. Click the **Save** button.

13. To run the task immediately regardless of the configured schedule, do the following:

    a. Select the checkbox next to the task.

14. Click the **Run** button.

    As a result, Kaspersky Endpoint Security deletes the file from the computer. If the file is locked by a different process, the task is displayed as *Completed*, but the file itself is deleted only after the computer is restarted. After restarting the computer, confirm that the file is deleted.

The *Delete file* task can finish with the *Access denied* error if you are trying to delete an executable file that is currently running. Create a terminate process task for the file and try again.

Start process

You can remotely run files using the *Start process* task.

Important: You can configure the task for EDR Optimum in Web Console.

To create a Start process task:

1. In the main window of the Web Console, select **Assets (Devices)** > **Tasks**.

   The list of tasks opens.

2. Click **Add**.

   The **New task wizard** starts.

3. Configure the task settings:

   a. In the **Application** drop-down list, select Kaspersky Endpoint Security for Mac (12.2).

   b. In the **Task type** drop-down list, select **Start process**.

   c. In the **Task name** field, enter a brief description.

   d. Select one of the following options:

   - **Assign task to an administration group**

     The task is assigned to devices included in an administration group. You can specify one of the existing groups or create a new one.

     For example, you may want to use this option to run a task of sending a message to users if the message is specific for devices included in a specific administration group.

     If a task is assigned to an administration group, the **Security** tab is not displayed in the task properties window because group tasks are subject to the security settings of the groups to which they apply.

   - **Specify device addresses manually or import addresses from a list**

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

You may want to use this option to execute a task for a specific subnet. For example, you may want to install a certain application on devices of accountants or to scan devices in a subnet that is probably infected.

- **Assign task to a device selection**

  The task is assigned to devices included in a device selection. You can specify one of the existing selections.

  For example, you may want to use this option to run a task on devices with a specific operating system version.

4. Select devices according to the selected task scope option.
5. At the **Task scope** step, specify an administration group, devices with specific addresses, or a device selection.

   The available settings depend on the option selected at the previous step.
6. Configure the task settings:

   a. In the **Executable command** field, specify the command to execute on the local device.

   b. If necessary, specify the command line arguments in the **Command line arguments (optional)** field.

   c. If necessary, specify the path to the executable file in the **Path to the working folder (optional)** field.
7. At the **Finish task creation** step, click the **Finish** button to create the task and close the wizard.

   If you enabled the **Open task details when creation is complete** option, the task settings window opens. In this window, you can check the task parameters, modify them, or configure a task start schedule, if necessary.
8. Click the new task.

   The task properties window opens.
9. Select the **Schedule** tab.
10. Configure the task schedule.

    Note: Make sure the computer is turned on to run the task.
11. Click the **Save** button.
12. To run the task immediately regardless of the configured schedule, do the following:

    a. Select the checkbox next to the task.
13. Click the **Run** button.

As a result, Kaspersky Endpoint Security runs the command in silent mode and starts the process. You can view the results of the task in the task properties in the **Execution results** section.

Terminate process

You can remotely terminate processes using the *Terminate process* task. For example, you can remotely terminate an Internet speed testing utility that was started using the Start process task.

If you want to prohibit running a file, you can configure the Execution prevention component. You can prohibit the execution of executable files, scripts, office format files.

The *Terminate process* task has the following limitations:

- You can configure the task only for EDR Optimum in Web Console.

To create a Terminate process task:

1. In the main window of the Web Console, select **Assets (Devices)** > **Tasks**.

   The list of tasks opens.

2. Click **Add**.

   The **New task wizard** starts.

3. Configure the task settings:

   a. In the **Application** drop-down list, select Kaspersky Endpoint Security for Mac (12.2).

   b. In the **Task type** drop-down list, select **Terminate process**.

   c. In the **Task name** field, enter a brief description.

   d. Select one of the following options:

   - **Assign task to an administration group**

     The task is assigned to devices included in an administration group. You can specify one of the existing groups or create a new one.

     For example, you may want to use this option to run a task of sending a message to users if the message is specific for devices included in a specific administration group.

     If a task is assigned to an administration group, the **Security** tab is not displayed in the task properties window because group tasks are subject to the security settings of the groups to which they apply.

   - **Specify device addresses manually or import addresses from a list**

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

     You may want to use this option to execute a task for a specific subnet. For example, you may want to install a certain application on devices of accountants or to scan devices in a subnet that is probably infected.

   - **Assign task to a device selection**

     The task is assigned to devices included in a device selection. You can specify one of the existing selections.

     For example, you may want to use this option to run a task on devices with a specific operating system version.

4. Select devices according to the selected task scope option.

5. At the **Task scope** step, specify an administration group, devices with specific addresses, or a device selection.

   The available settings depend on the option selected at the previous step.

6. At this step of the wizard, in the **Please specify the file which processes should be terminated** drop-down list, select one of the options and fill in the required fields. To specify the file, you must enter the full path to the file, or both file hash and the path.

   > **Note:** If you're creating this task for a local device, you can specify the process by PID.

7. If you want the task to be applicable to critical system objects, select the **Apply to critical system objects** checkbox.

8. Enter the account credentials of the user whose rights you want to use to run the task. Click **Next**.

   > **Note:** By default, Kaspersky Endpoint Security starts the task as the system user account (root).

9. At the **Finish task creation** step, click the **Finish** button to create the task and close the wizard.

   If you enabled the **Open task details when creation is complete** option, the task settings window opens. In this window, you can check the task parameters, modify them, or configure a task start schedule, if necessary.

10. Click the new task.

    The task properties window opens.

11. Select the **Schedule** tab.

12. Configure the task schedule.

    > **Note:** Make sure the computer is turned on to run the task.

13. Click the **Save** button.

14. To run the task immediately regardless of the configured schedule, do the following:

    a. Select the checkbox next to the task.

15. Click the **Run** button.

    As a result, Kaspersky Endpoint Security terminates the process on the computer. For example, if a *Game* application is running and you terminate the *Game* process, the application is closed without saving data. You can view the results of the task in task properties in the **Results** section.

Execution prevention

Execution prevention allows managing the running of executable files and scripts, as well as opening office format files. In this way, you can, for example, prevent the execution of applications that you consider insecure. As a result, the spreading of the threat can be stopped. Execution prevention supports a set of script interpreters.

Execution prevention rule

Execution prevention manages user access to files with execution prevention rules. Execution prevention rule is a set of criteria that the application takes into account when reacting to an object execution, for example when blocking object execution. The application identifies files by their paths or checksums calculated using MD5 and SHA256 hashing algorithms.

You can create Execution prevention rules:

- In alert details (only for EDR Optimum).

  Alert Details is a tool for viewing the entirety of collected information about a detected threat. Alert details include, for example, the history of files appearing on the computer. For details about managing alert details, refer to the Kaspersky Endpoint Detection and Response Optimum Help.

- Using a group policy or local application settings. You must enter the file path or hash (SHA256 or MD5), or both the file path and the file hash.

You can also manage Execution prevention locally using the command line.

Note: It is impossible to block the startup of system-critical objects (SCO). SCOs are files that the operating system and the Kaspersky Endpoint Security for Mac application require to be able to run.

Execution prevention rule modes

The Execution prevention component can work in two modes:

- **Statistics only**

  In this mode, Kaspersky Endpoint Security publishes an event about attempts to run executable objects or open documents that match prevention rule criteria to the Kaspersky Security Center event log and the unified logging system, but does not block the attempt to run or open the object or document. This mode is selected by default.

- **Active**

  In this mode, the application blocks the execution of objects or opening of documents that match prevention rule criteria. The application also publishes an event about attempts to execute objects or open documents to the Kaspersky Security Center event log and the unified logging system.

Managing Execution prevention

Important: You can configure the component settings only in the Web Console.

To prevent execution:

1. In the main window of the Web Console, select **Devices** > **Policies and profiles**.
2. Click the name of the Kaspersky Endpoint Security for Mac policy.

   The policy properties window opens.
3. Select **Application settings** tab.
4. Go to **Detection and Response** > **Endpoint Detection and Response**.
5. Turn on the **Execution prevention** toggle switch.
6. In the **Action on execution or opening of forbidden object** block, select the component operating mode:

   - **Block and write to report**. In this mode, the application blocks the execution of objects or opening of documents that match prevention rule criteria. The application also publishes an event about attempts to execute objects or open documents to the Kaspersky Security Center event log and the unified logging system.
   - **Log events only**. In this mode, Kaspersky Endpoint Security publishes an event about attempts to run executable objects or open documents that match prevention rule criteria to the Kaspersky Security Center event log and the unified logging system, but does not block the attempt to run or open the object or document. This mode is selected by default.
7. Create a list of execution prevention rules:

   a. Click **Add**.

   b. In the dialog that opens, enter the name of the execution prevention rule (for example, Application A).

   c. In the **Type** drop-down list, select the object that you want to block: **Application**, **Script**, **Document**.

   If you select a wrong object type, Kaspersky Endpoint Security does not block the file or script.

   d. To add the file, you must enter the hash of the file (SHA256 or MD5), the full path to the file, or both the hash and the path.

   Note: If the file is located on a network drive, enter the file path in the following way: /Volumes/shared_folder_name/filename. If the file path contains a network drive letter, Kaspersky Endpoint Security does not block the file or script.

   a. Click **OK**.
8. Save your changes.

As a result, Kaspersky Endpoint Security blocks the execution of objects: running executable files and scripts, opening office format files. You can, however, for example, open a script file in a text editor even if running the script is prevented. When blocking the execution of an object, Kaspersky Endpoint Security displays a standard notification if notifications are enabled in application settings.

Computer network isolation

Computer network isolation allows automatically isolating a computer from the network in response to the detection of an indicator of compromise (IOC) – this is the automatic mode. You can turn on Network isolation manually while you are investigating the detected threat – this is the manual mode.

When Network isolation is turned on, the application severs all active connections and blocks all new TCP/IP network connections on the computer except the following connections:

- Connections listed in Network isolation exclusions.
- Connections initiated by Kaspersky Endpoint Security services.
- Connections initiated by the Kaspersky Security Center Network Agent.

Important: You can configure the component settings only in the Web Console.

Automatic Network isolation mode

You can configure Network isolation to be turned on automatically in response to an IOC detection. You can configure the automatic Network isolation mode with a group policy.

How to configure Network isolation to be turned on automatically in response to an IOC detection

1. In the main window of the Web Console, select **Devices** > **Tasks**.
2. The list of tasks opens.
3. Click the **IOC Scan** task of Kaspersky Endpoint Security.

   The task properties window opens.

   If necessary, create the IOC Scan task.
4. Select the **Application settings** tab.
5. In the **Action on IOC detection** block, select the **Alert and take response actions after an IOC is found** option and then the **Isolate computer from the network (8 hours)** checkbox.
6. Save your changes.
7. As a result, when an IOC is detected, the application isolates the computer from the network to prevent the threat from spreading.

You can configure Network isolation to be turned off automatically after a specified time elapses. By default, the application turns off Network isolation after 8 hours have passed from the time when it was turned on. You can also turn off Network isolation manually (see the instructions below). After turning off network isolation, the computer can use the Network without restrictions.

How to configure the delay for turning off Network isolation of a computer in automatic mode

1. In the main window of the Web Console, select **Devices** > **Policies & profiles**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.

3. Select the **Application settings** tab.
4. Go to **Detection and Response** > **Endpoint Detection and Response**.
5. In the **Network isolation** block, click **Configure computer unlock settings**.
6. In the window that opens, select the **Automatically unlock isolated computer in** checkbox and enter the delay for automatically turning off Network isolation.
7. Save your changes.

Manual Network isolation mode

You can manually turn Network isolation on and off. You can configure the manual Network isolation mode using the computer properties in the Kaspersky Security Center console.

You can turn on Network isolation:

- In alert details (only for EDR Optimum).

  Alert Details is a tool for viewing the entirety of collected information about a detected threat. Alert details include, for example, the history of files appearing on the computer. For details about managing alert details, refer to the Kaspersky Endpoint Detection and Response Optimum Help.
- Using local application settings.

How to turn on Network isolation of a computer manually

1. In the main window of the Web Console, select **Devices** > **Managed devices**.
2. Select the computer for which you want to configure local application settings.

   This opens the computer properties.
3. Select the **Applications** tab.
4. Click **Kaspersky Endpoint Security for Mac**.

   This opens the local application settings.
5. Select the **Application settings** tab.
6. Go to **Detection and Response** > **Endpoint Detection and Response**.
7. In the **Network isolation** block, click **Isolate computer from the network**.

You can configure Network isolation to be turned off automatically after a specified time elapses. By default, the application turns off Network isolation after 8 hours have passed from the time when it was turned on. After turning off network isolation, the computer can use the Network without restrictions.

How to configure the delay for turning off Network isolation of a computer in manual mode

1. In the main window of the Web Console, select **Devices** > **Managed devices**.
2. Select the computer for which you want to configure local application settings.
   This opens the computer properties.
3. Select the **Tasks** tab.
   This displays the list of tasks available on the computer.
4. Select the **Network isolation** task.
5. Select the **Application settings** tab.
6. In the window that opens, select the delay for turning off Network isolation.
7. Save your changes.

How to turn off Network isolation of a computer manually

1. In the main window of the Web Console, select **Devices** > **Managed devices**.
2. Select the computer for which you want to configure local application settings.
3. This opens the computer properties.
4. Select the **Applications** tab.
5. Click Kaspersky Endpoint Security for Mac.
6. This opens the local application settings.
7. Select the **Application settings** tab.
8. Go to **Detection and Response** > **Endpoint Detection and Response**.
9. In the **Network isolation** block, click **Unblock computer isolated from the network**.

You can also disable Network isolation locally using the command line.

Network isolation exclusions

You can configure Network isolation exclusions. Network connections that match the rules are not blocked on the computer when Network isolation is turned on.

To configure Network isolation exclusions, you can use a list of standard network profiles. By default, exclusions include network profiles containing rules that ensure uninterrupted operation of devices with the DNS/DHCP server and DNS/DHCP client roles. You can also modify the settings of standard network profiles or define exclusions manually (see instructions below).

Important: Exclusions specified in policy properties are applied only if Network isolation is turned on automatically in response to a detected threat. Exclusions specified in computer properties are applied only if Network isolation is turned on manually in computer properties in the Kaspersky Security Center console.

Note: An active policy does not prevent applying exclusions from Network isolation configured in computer properties because these parameters have different usage scenarios.

How to add a Network isolation exclusion in automatic mode

1. In the main window of the Web Console, select **Devices** > **Policies & profiles**.
2. Click the name of the Kaspersky Endpoint Security policy.
3. The policy properties window opens.
4. Select the **Application settings** tab.
5. Go to **Detection and Response** > **Endpoint Detection and Response**.
6. In the **Network isolation exclusions** block, click **Exclusions**.
7. This opens a window; in this window, click **Add from profile** and select standard network profiles for configuring exclusions.
8. Network isolation exclusions from the profile are added to the list of Network isolation exclusions. You can view the properties of network connections. If necessary, you can modify network connection settings.
9. If necessary, add a Network isolation exclusion manually. To do so, in the window with the list of exclusions, click **Add** and manually edit network connection settings.
10. Save your changes.

How to add a Network isolation exclusion in manual mode

1. In the main window of the Web Console, select **Devices** > **Managed devices**.
2. Select the computer for which you want to configure local application settings.
3. This opens the computer properties.
4. Select the **Tasks** tab.
5. This displays the list of tasks available on the computer.
6. Select the **Network isolation** task.
7. Select the **Application settings** tab.

8. In the window that opens, click **Exclusions**.
9. In the next window, click **Add from profile** and select standard network profiles for configuring exclusions.
10. Network isolation exclusions from the profile are added to the list of Network isolation exclusions. You can view the properties of network connections. If necessary, you can modify network connection settings.
11. If necessary, add a Network isolation exclusion manually. To do so, in the window with the list of exclusions, click **Add** and manually edit network connection settings.
12. Save your changes.

You can also view the Network isolation exclusion list locally using the command line. In this case, the computer must be isolated.

Cloud Sandbox

Cloud Sandbox is a technology that lets you detect advanced threats on a computer. Kaspersky Endpoint Security automatically forwards detected files to Cloud Sandbox for analysis. Cloud Sandbox runs these files in an isolated environment to identify malicious activity and decides on their reputation. Data on these files is then sent to Kaspersky Security Network. Therefore, if Cloud Sandbox detects a malicious file, Kaspersky Endpoint Security will perform the appropriate action to eliminate the threat on all computers where this file is detected.

Important: For Cloud Sandbox to operate, you must enable the use of Kaspersky Security Network.

Note: If you are using Kaspersky Private Security Network, Cloud Sandbox technology is not available.

To enable the Cloud Sandbox:

1. In the main window of the Web Console, select **Devices** > **Policies and profiles**.
2. Click the name of the Kaspersky Endpoint Security for Mac policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Detection and Response** > **Endpoint Detection and Response**.
5. Turn on the **Cloud Sandbox** toggle switch.
6. Save your changes.

Whenever there is a threat, Kaspersky Endpoint Security activates the counter for threats detected using Cloud Sandbox in the main application window in the **Threat detection** section. Kaspersky Endpoint Security will also indicate the Cloud Sandbox threat detection technology in the Report on threats in the Kaspersky Security Center console.

FileVault Disk Encryption

Note: The FileVault Disk Encryption feature is available in Kaspersky Security Center 10 SP3 or later. For more information, contact Kaspersky Technical Support.

Kaspersky Endpoint Security allows FileVault encryption to be managed remotely. Encryption prevents unauthorized users from accessing sensitive data stored on the startup disk of the user's computer.

When an administrator starts FileVault encryption on a computer from Kaspersky Security Center, Kaspersky Endpoint Security prompts a user of this computer to enter his or her credentials. Disk encryption starts only after the user provides the credentials, the computer is restarted, and 30 minutes have passed since the policy settings are received on the computer. The minimum interval between prompts for credentials is also 30 minutes.

To prevent the user from decrypting the startup disk of their Mac when FileVault encryption is enabled, an administrator needs to use JAMF to deploy an MDM profile prohibiting disk decryption. To decrypt the startup disk of a Mac with an MDM profile prohibiting disk decryption, the administrator first needs to remove the profile.

Note: If FileVault encryption management isn't enabled in Kaspersky Security Center, users with administrator rights can encrypt and decrypt their Mac startup disks from System Settings. For more information on FileVault, refer to Apple documentation.

If the computer has multiple computer accounts, FileVault encryption makes the disk inaccessible to all users except for the user who entered his or her credentials.

Allow other users to unlock the disk

1. Choose **Apple menu** > **System Settings** > **Privacy & Security**.
2. Click **FileVault**.

   The **FileVault** window opens.
3. Click **Enable Users**.
4. In the window that opens, select a user to authorize to unlock the computer.
5. Enter the password of the user's computer account and click **OK**.
6. Click **Continue**.

   The user can access the encrypted disk.

Note: Administrator rights are required to allow other users to unlock the disk.

If an administrator manages Kaspersky Endpoint Security via Kaspersky Security Center Administration Console, Web Console, or Cloud Console and a user of this computer forgets or loses his or her credentials and cannot access an encrypted disk, the administrator can get a recovery key.

How to get a recovery key using Kaspersky Security Center Administration Console

How to get a recovery key using Kaspersky Security Center Web Console and Cloud Console

Password protection

Kaspersky Endpoint Security allows limiting unwanted actions on users' devices by setting an administrator password.

If Password protection is enabled, Kaspersky Endpoint Security requires a password upon attempts to do any of the following:

- Configure application settings
- Exit the application
- Remove the license key
- Remove the application

  Note: Password protection restricts removal of Kaspersky Endpoint Security only when performed via the uninstaller.

- Restore quarantined files from Backup
- View reports.

Disabling Password protection does not disable the policy settings. If editing a setting is prohibited in the policy, it cannot be edited even if Password protection is disabled.

Enable Password protection using the Administration Console

1. Start the Administration Console.
2. Maximize the **Administration Server <Server name>** node.
3. In the console tree, click **Managed devices**.
4. In the workspace, select the **Policies** tab.
5. Right-click the policy you want to configure and choose **Properties**.
6. In the **Properties** window, select **Additional settings > User Interaction**.
7. In the **Password protection** section, select the **Enable password protection** checkbox.
8. In the **Password protection settings** window that opens, configure the following settings:
   - Enter the password in the **Password** field and enter it a second time in the **Confirm password** field.
   - In the **Require password to** section, select the required checkboxes to protect the corresponding actions on the user's device.
9. Click **OK** to save your changes.

10. Do one of the following to apply the changes to the policy:

    - Click **Apply** to remain in the **Properties: <Policy name>** window after saving changes.
    - Click **OK** to close the **Properties: <Policy name>** window after saving changes.

Edit Password protection settings using the Administration Console

1. Start the Administration Console.
2. Maximize the **Administration Server <Server name>** node.
3. In the console tree, click **Managed devices**.
4. In the workspace, select the **Policies** tab.
5. Right-click the policy you want to configure and choose **Properties**.
6. In the **Properties** window, select **Additional settings > User Interaction**.
7. In the **Password protection** section, click the **Settings** button.
8. In the **Password protection settings** window that opens, edit the settings you want to change.
9. Click **OK** to save your changes.

Enable Password protection using the Web Console

1. In the main window of the Web Console, select **Devices** > **Policies and profiles**.
2. Click the name of the Kaspersky Endpoint Security for Mac policy.
3. The policy properties window opens.
4. Select the **Application settings** tab.
5. Select **Additional Settings** > **User interaction**.
6. Turn on the **Password protection** toggle switch.
7. In the **Password protection settings** dialog that opens, configure the following settings:

    - Enter the password in the **Password** field and enter it a second time in the **Confirm password** field. By default, the password characters are hidden for security reasons. To view the password, click **Show**.
    - In the **Require password to** section, select the required checkboxes to protect the corresponding actions on the user's device.

8. Click **OK** to close the **Password protection settings** dialog.
9. Click **OK** to close the **User interaction** section.
10. Click **Save** to save the changes to the policy.

Edit Password protection using the Web Console

1. In the main window of the Web Console, select **Devices** > **Policies and profiles**.
2. Click the name of the Kaspersky Endpoint Security for Mac policy.
3. The policy properties window opens.
4. Select the **Application settings** tab.
5. Select **Additional Settings** > **User interaction**.
6. In the **Password protection** section, click the **Settings** button.
7. In the **Password protection settings** dialog that opens, edit the settings you want to change.
8. Click **OK** to close the **Password protection settings** dialog.
9. Click **OK** to close the **User interaction** section.
10. Click **Save** to save the changes to the policy.

Enable Password protection using the Kaspersky Endpoint Security application

1. In the menu bar, click the application icon and choose **Settings**.
   The application settings window opens.
2. On the **Interface** tab, in the **Password protection** section, select the **Enable password protection** checkbox.
3. In the window that opens, configure the following settings:
   - Enter the password in the **Password** field and enter it a second time in the **Confirm password** field.
   - In the **Require password to** section, select the required checkboxes to protect the corresponding actions on the user's device.
4. Click **OK**.

> **Note:** If you select **Change application settings** as a password protected action, you need to enter the password twice in order to change the Password protection settings.

Edit Password protection using the Kaspersky Endpoint Security application

1. In the menu bar, click the application icon and choose **Settings**.
   The application settings window opens.
2. On the **Interface** tab, in the **Password protection** section, click **Settings**.
3. In the window that opens, edit the settings you want to change.
4. Click **OK**.

Exploit Prevention

The Exploit Prevention component detects program code that takes advantage of vulnerabilities on the computer to exploit administrator privileges or to perform malicious activities. For example, exploits can utilize a buffer overflow attack. To do so, the exploit sends a large amount of data to a vulnerable application. When processing this data, the vulnerable application executes malicious code. As a result of this attack, the exploit can start an unauthorized installation of malware. When there is an attempt to run an executable file from a vulnerable application that was not performed by the user, Kaspersky Endpoint Security blocks this file from running or notifies the user.

By default, Exploit Prevention is enabled. You can disable Exploit Prevention if necessary.

Enable/disable Exploit Prevention using the Web Console

1. In the main window of the Web Console, select **Assets (Devices)** > **Policies & profiles**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Advanced Threat Protection** > **Exploit Prevention**
5. Turn on/off the **Exploit Prevention** toggle switch.
6. If Exploit Prevention is enabled, select one of the following actions to be performed when an exploit is detected:

   - **Block**

     If this option is selected, on detecting an exploit, Kaspersky Endpoint Security blocks the operations of this exploit and makes a log entry with information about this exploit.

   - **Inform**

     If this option is selected, when Kaspersky Endpoint Security detects an exploit it logs an entry containing information about the exploit and adds information about this exploit to the list of active threats.
7. Save your changes.

Enable/disable Exploit Prevention using the Administration Console

1. Start the Administration Console.
2. Maximize the **Administration Server <Server name>** node.
3. In the console tree, click **Managed devices**.
4. In the workspace, select the **Policies** tab.
5. Right-click the policy you want to configure and choose **Properties**.
6. In the **Properties** window, select **Advanced Threat Protection** > **Exploit Prevention**.

7. Select or deselect the **Exploit Prevention** checkbox.

8. If necessary, in the **On detecting exploit** section, select the action to be performed when Kaspersky Endpoint Security detects an exploit.

9. Click **OK** to save your changes.

10. Do one of the following to apply the changes to the policy:

    - Click **Apply** to remain in the **Properties: <Policy name>** window after saving changes.

    - Click **OK** to close the **Properties: <Policy name>** window after saving changes.

Enable/disable Exploit Prevention using the Kaspersky Endpoint Security application

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.

2. On the **Advanced** tab, in the Exploit Prevention section, select or deselect the **Enable Exploit Prevention** checkbox.

3. If the **Enable Behavior Detection** checkbox is selected, select one of the following actions to be performed when malware activity is detected:

    - **Block dangerous malware activity automatically**

      If this option is selected, on detecting an exploit, Kaspersky Endpoint Security blocks the operations of this exploit and makes a log entry with information about this exploit.

    - **Inform**

      If this option is selected, when Kaspersky Endpoint Security detects an exploit it logs an entry containing information about the exploit and adds information about this exploit to the list of active threats.

View the Exploit Prevention report

1. In the menu bar, choose **Protection** > **Reports**.

   The **Reports** window opens.

2. Open the **Exploit Prevention** tab.

Remediation Engine

The Remediation Engine lets Kaspersky Endpoint Security roll back actions that have been performed by malware in the operating system.

When rolling back malware activity in the operating system, Kaspersky Endpoint Security handles the following types of malware activity:

- **File activity**

Kaspersky Endpoint Security performs the following actions:

- Deletes executable files that were created by malware (on all media except network drives).
- Deletes executable files that were created by programs that have been infiltrated by malware.
- Restores files that have been modified or deleted by malware.

- **System activity**

  Kaspersky Endpoint Security performs the following actions:

  - Terminates processes that have been initiated by malware.
  - Terminates processes into which a malicious application has penetrated.
  - Does not resume processes that have been halted by malware.

- **Network activity**

  Kaspersky Endpoint Security performs the following actions:

  - Blocks the network activity of malware.

A rollback of malware actions can be started by the File Threat Protection or Behavior Detection component, or during a malware scan.

Rolling back malware operations affects a strictly defined set of data. Rollback has no adverse effects on the operating system or on the integrity of your computer data.

Enable/disable Remediation Engine in the Administration Console

1. Start the Administration Console.
2. Maximize the **Administration Server <Server name>** node.
3. In the console tree, click **Managed devices**.
4. In the workspace, select the **Policies** tab.
5. Right-click the policy you want to configure and choose **Properties**.
6. In the **Properties** window, select **Advanced Threat Protection** > **Remediation Engine**.
7. Select or deselect the **Remediation Engine** checkbox.
8. Click **OK** to save your changes.
9. Do one of the following to apply the changes to the policy:

   - Click **Apply** to remain in the **Properties: <Policy name>** window after saving changes.
   - Click **OK** to close the **Properties: <Policy name>** window after saving changes.

Enable/disable Remediation Engine in the Web Console

1. In the main window of the Web Console, select **Assets (Devices)** > **Policies & profiles**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Advanced Threat Protection** > **Remediation Engine**.
5. Turn on/off the **Remediation Engine** switch.
6. Save your changes.

Enable/disable Remediation Engine in the application interface

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.
2. On the **Advanced** tab, in the **Remediation Engine** section, select or deselect the **Enable Remediation Engine** checkbox.

As a result, if Remediation Engine is enabled, Kaspersky Endpoint Security will roll back the actions taken by malicious applications in the operating system.

Web Control

Web Control manages users' access to web resources. This helps reduce traffic and inappropriate use of work time. When a user tries to open a website that is restricted by Web Control, Kaspersky Endpoint Security will block access or show a warning.

You can block access to specific websites or selected categories of websites.

Note: The Kaspersky Endpoint Security application can only block access to websites that use HTTPS for connections. The application scans encrypted connections (HTTPS) only if the **Check secure connections (HTTPS)** checkbox in the **General** section on the **Essential** tab is selected.

Add a new rule in the Administration Console

1. Start the Administration Console.
2. Maximize the **Administration Server <Server name>** node.
3. In the console tree, click **Managed devices**.
4. In the workspace, select the **Policies** tab.
5. Right-click the policy you want to configure and choose **Properties**.
6. In the **Properties** window, select **Security Controls** > **Web Control**.

7. Select the **Enable Web Control** checkbox.
8. Click **Add**.
9. In the window that opens, enter a rule name.
10. If you want the rule to be active, select the **Active rule** checkbox.
11. Do one of the following:
    - If you want the rule to apply to specific web addresses, select the **Web address or a group of web addresses by mask** option.
    - If you want the rule to apply to specific website categories, select the **Website categories** option.
12. Click **Specify**.
13. In the window that opens, specify the rule scope.
14. Do one of the following:
    - If you want Kaspersky Endpoint Security to block access, select the **Block** option.
    - If you want Kaspersky Endpoint Security to allow access, select the **Allow** option.
    - If you want Kaspersky Endpoint Security to show a warning, select the **Show warning** option.
15. Click **OK** to save your changes.
16. Do one of the following to apply the changes to the policy:
    - Click **Apply** to remain in the **Properties: <Policy name>** window after saving changes.
    - Click **OK** to close the **Properties: <Policy name>** window after saving changes.

Add a new rule in the Web Console

1. In the main window of the Web Console, select **Assets (Devices)** > **Policies & profiles**.
2. Click the name of the Kaspersky Endpoint Security policy.
   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Security Controls** > **Web Control**.
5. Turn on the **Web Control** switch.
6. Click **Add**.
7. In the window that opens, enter a rule name.

8. Do one of the following:

    - If you want the rule to be active, select the **Active** option.
    - If you want the rule to be inactive, select the **Inactive** option.

9. Do one of the following:

    - If you want Kaspersky Endpoint Security to allow access, select the **Allow** option.
    - If you want Kaspersky Endpoint Security to block access, select the **Block** option.
    - If you want Kaspersky Endpoint Security to show a warning, select the **Show Warning** option.

10. Do one of the following:

    - If you want the rule to apply to specific website categories, select the **Categories** option and click **Select categories** to select the categories.
    - If you want the rule to apply to specific web addresses, select the **Individual addresses** option and add them to the table below.

11. Save your changes.

Note: Web Control settings cannot be managed in the Kaspersky Endpoint Security application.

Device Control

Device Control manages user access to devices that are installed on or connected to the computer. This lets you protect the computer from infection when such devices are connected, and prevent loss or leaks of data.

Device access levels

Device Control controls access at the following levels:

- **Device type**. For example, printers, removable drives, and CD/DVD drives.

  You can configure device access as follows:

    - Allow.
    - Block.
    - Block with exceptions (Wi-Fi only).

- **Trusted devices.** Trusted devices are devices to which users that are specified in the trusted device settings have full access at all times.

You can add trusted devices based on the following data:

- **Devices by ID**. Each device has a unique identifier (Hardware ID, or HWID). You can view the ID in the device properties by using operating system tools. Example of a device ID: SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000. Adding devices by ID is convenient if you want to add several specific devices.

- **Devices by model**. Each device has a vendor ID (VID) and a product ID (PID). You can view the IDs in the device properties by using operating system tools. Template for entering the VID and PID: VID_1234&PID_5678. Adding devices by model is convenient if you use devices of a certain model in your organization. This way, you can add all devices of this model.

- **Devices by ID mask**. If you are using multiple devices with similar IDs, you can add devices to the trusted list by using masks. The `*` character replaces any set of characters. Kaspersky Endpoint Security does not support the `?` character when entering a mask. For example, `WDC_C*`.

- **Devices by model mask**. If you are using multiple devices with similar VIDs or PIDs (for example, devices from the same manufacturer), you can add devices to the trusted list by using masks. The `*` character replaces any set of characters. Kaspersky Endpoint Security does not support the `?` character when entering a mask. For example, `VID_05AC&PID_*`.

Manage the Device Control component in the Administration Console

1. Start the Administration Console.
2. Maximize the **Administration Server <Server name>** node.
3. In the console tree, click **Managed devices**.
4. In the workspace, select the **Policies** tab.
5. Right-click the policy you want to configure and choose **Properties**.
6. In the **Properties** window, select **Security Controls** > **Device Control**.
7. Select the **Device Control** checkbox.
8. On the **Types of devices** tab, configure access rules for device types and Wi-Fi networks.
9. On the **Trusted devices** tab, configure access rules for individual devices or device groups.
10. Click **OK** to save your changes.
11. Do one of the following to apply the changes to the policy:
    - Click **Apply** to remain in the **Properties: <Policy name>** window after saving changes.
    - Click **OK** to close the **Properties: <Policy name>** window after saving changes.

Manage the Device Control component in the Web Console

1. In the main window of the Web Console, select **Assets (Devices)** > **Policies & profiles**.
2. Click the name of the Kaspersky Endpoint Security policy.
   The policy properties window opens.

3. Select the **Application settings** tab.
4. Go to **Security Controls** > **Device Control**.
5. Turn on the **Device Control** switch.
6. In the **Device Control settings** section, configure access rules for devices, types of devices, and Wi-Fi networks.
7. Save your changes.

Note: Device Control settings cannot be managed in the Kaspersky Endpoint Security application.

As a result, if Device Control is enabled, the application relays information about connected devices to Kaspersky Security Center. You can view the list of connected devices in Kaspersky Security Center in the **Advanced** → **Repositories** → **Hardware folder**.

View the Device Control report

1. In the menu bar, choose **Protection** > **Reports**.

   The **Reports** window opens.
2. Open the **Device Control** tab.

Participate in Kaspersky Security Network

When you participate in Kaspersky Security Network, the Kaspersky Endpoint Security application statistics are automatically sent to Kaspersky to enhance protection of your Mac.

Note: Kaspersky doesn't receive, process, or store any personal data without your explicit consent.

Participation in Kaspersky Security Network is voluntary. The decision to participate is made when you install the application. However, you can change your decision later at any time.

Enable Kaspersky Security Network

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.

2. On the **Advanced** tab, in the **KSN** section, click **Show KSN Statement** to view the Kaspersky Security Network Statement.

3. If you want Kaspersky Endpoint Security to use information about the reputation of files, web resources, and applications received from Kaspersky Security Network and you accept all the terms of the Statement, select the **Participate in Kaspersky Security Network** checkbox.

4. In the window that opens, click **Confirm**.

The **Participate in Kaspersky Security Network** and **Enable extended KSN mode** checkboxes will be selected.

Note: By default, Kaspersky Endpoint Security uses the Extended KSN mode. *Extended KSN mode* is a mode in which Kaspersky Endpoint Security sends additional data to Kaspersky. If you do not want to provide these data to Kaspersky, deselect the **Enable extended KSN mode** checkbox.

Data provided to Kaspersky when using Kaspersky Security Network

If the **Participate in Kaspersky Security Network** checkbox is selected and the **Enable extended KSN mode** checkbox is unselected, Kaspersky Endpoint Security provides to Kaspersky the following data:

- Information about the license used: the type and validity period of the license, number of days till license expiration, identifier of the partner from whom the license was purchased, Regional Activation Center identifier, checksum of the activation code, ticket body hash calculated using the SHA1 algorithm, license ticket creation date and time, license information identifier, license ticket identifier, license ticket sequence identifier, unique identifier of the user's computer, date from which the license ticket is valid, date to which the license ticket is valid, license ticket current state, ticket header version, license version, ticket header signature certificate identifier, checksum of the key file, ticket header signer serial number, authentication token.

- Full version of installed Software; type of installed Software; Software update ID; ID of reputation service; protocol type ID; ID of a regional activation center; version of list of revoked Software service's decisions; ID of the triggered record in the Software's anti-virus databases; timestamp of the triggered record in the Software's anti-virus databases; type of the triggered record in the Software's anti-virus databases; unique ID of the instance of application installation on the computer; license activation date; license expiration date; license identifier; status of the license used by the Software; checksum type for the object being processed; name of the detected malware or legitimate software that can be used to damage the user's device or data; checksum of the object being processed; checksum of the Software activation code; full version of the Software; unique device ID; Software ID; checksum of the Software key file; ID of the information model used to provide the Software license; identifier of the certificate used to sign the Software license ticket header; the Software license ticket create date and time; the Software license ticket checksum; the Software license ticket version; the Software activation code version; format of the data in the request to Rightholder infrastructure; current license ticket ID; the Software component ID; the result of the Software action; error code; accessed address of the web service (URL, IP); port number; web address of the source of the web service request (referrer); public key of the certificate; digital certificate thumbprint of the scanned object and hashing algorithm.

If the **Participate in Kaspersky Security Network** and **Enable extended KSN mode** checkboxes are selected, Kaspersky Endpoint Security provides to Kaspersky the following data:

- Information about the version of the operating system (OS) and service packs installed on the computer, version and checksums (MD5, SHA2-256, SHA1) of the OS kernel file, parameters of the OS run mode; OS version, OS build number, OS update number, OS edition, extended information about the OS edition; OS Service Pack version; date and time of the OS launch; processing delay time of the event about OS action in the behavioral analysis subsystem; number of delayed OS action events of the current type; processing delay time of the event about OS action in the proactive defense subsystem; number of processed OS action events; number of processed synchronous OS action events; total delay of all OS action events of the current type; processing delay time of the event about OS action in the persistent event storage subsystem; total delay of all OS action events; number of waiting synchronous OS action events; date and time of received event of an action in the OS.

- Information about the failed last OS reboot: number of failed reboots.

- Information about the Rightholder's installed application and the anti-virus protection status: Software installation ID (PCID); Software database record version; unique identifier of the instance of application installation on the computer, application type, ID of application type, the full version of the application installed, the identifier of the application settings version, the identifier of the computer type, the unique identifier of the computer on which the application is installed, the unique User identifier in the Rightholder's services, locale language and operation state, version of the installed Software components and their operation state, version of the protocol used to connect with the Rightholder's services; full version of installed Software; type of installed Software; Software update ID; ID of reputation service; protocol type ID; ID of a regional activation center; version of list of revoked Software service's decisions; ID of the triggered record in the Software's anti-virus databases; timestamp of the triggered record in the Software's anti-virus databases; type of the triggered record in the Software's anti-virus databases; Unique ID of the instance of application installation on the computer; license activation date; license expiration date; license identifier; status of the license used by the Software; checksum type for the object being processed; name of the detected malware or legitimate software that can be used to damage the user's device or data; checksum of the object being processed; checksum of the Software activation code; full version of the Software; Software ID; checksum of the Software key file; ID of the information model used to provide the Software license; identifier of the certificate used to sign the Software license ticket header; the Software license ticket create date and time; the Software license ticket checksum; the Software license ticket version; the Software activation code version; format of the data in the request to Rightholder infrastructure; current license ticket ID; the Software component ID; the result of the Software action; error code; accessed address of the web service (URL, IP); port number; web address of the source of the web service request (referrer); number of update-apply cycles for anti-virus databases; date and time when the anti-virus databases were last updated and applied; release date and time of the Software's databases; version of the Software's component; Software update ID; type of the installed Software; date and time of System Watcher start; installation date and time for the Software; probability of sending statistics by System Watcher; code of the event that took longer than the standard time to process by System Watcher; database processing time of the event that took longer than the standard time to process by System Watcher; maximum allowed time for processing an event by System Watcher; processing time of the event that took longer than the standard time to process by System Watcher; total number of events that took longer than the standard time to process by System Watcher.

- Information about all processed objects and operations: Software verdict on the object being processed; directory code; size of the object being processed; checksum (SHA256) of the object being processed; number of the detected software in the System Watcher context; date and time of detecting software by System Watcher; detect characteristics; ID of the triggered record in the Software's anti-virus databases; reason of detecting software by System Watcher; checksum (MD5) of the object being processed; result of the module integrity check; name of the object being processed; type of the triggered Software anti-virus databases record; path to the object being processed; the name of the scanned object; the date and time of the scan; the URL- and Referrer addresses from which it was downloaded; the size of scanned files and the paths to them; the archive sign; the date and time of the file's creation; the name, size and checksums (MD5, SHA2-256) of the packer (if the file was packed); the file's entropy; the file's type; the file type code; the executable file sign, ID and format; the object's checksum (MD5, SHA2-256); the type and value of the object's supplementary checksum; data about the object's digital signature (certificate): data on the certificate's publisher, number of starts of the object since the last statistics delivery, ID of the application's scanning task, the means of receiving information about the object's reputation, the value of the target filter, technical parameters of the applicable detection technologies; path to the object being processed; directory code.

- For executable files: the entropy of the file sections, reputation verification flag or file signature flag, name, type, ID type, checksum (MD5) and the size of the application that was loaded by the object being validated, the application path and template paths, an attribute indicating presence in the Autorun list, date of entry, the list of attributes, name of the packer, information about the digital signature of the application: the publisher certificate, the name of the uploaded file in the MIME format, file build date and time.

- Information about the applications launched and their modules: checksums (MD5, SHA2-256) of running files, size, attributes, creation date, name of the packer (if the file was packed), names of files, information about processes running on the system (process ID (PID), process name, information about the account the process was started from, the application and command that started the process, the full path to the process's files, and the starting command line, a description of the application that the process belongs to (the name of the application and information about the publisher), as well as the digital certificates being used and information needed to verify their authenticity or information about the absence of a file's digital signature), and information about the modules loaded into the processes: their names, sizes, types, creation dates, attributes, checksums (MD5, SHA2-256, SHA1), the paths to them, PE-file header information, names of packers (if the file was packed), information about the availability and validity of these statistics, identifier of the mode for generating the statistics being sent.

- If threats or vulnerabilities are detected, in addition to information about the detected object, information is provided about the identifier, version, and type of the record in the anti-virus database, the name of the threat based on the Kaspersky classification, the date and time of the last update of the anti-virus database, executable file name, the checksum (MD5) of the application file that requested the URL where the threat was detected, the IP address (IPv4 or IPv6) of the detected threat, the vulnerability identifier and its threat level, the URL and Referrer of the web page where the vulnerability was detected.

- If a potentially malicious object is detected, information is provided about data in the processes' memory.

- Network attack information: IP address of the attacking computer and number of the port on the user's computer targeted by the network attack, ID of the attack protocol, name and type of attack.

- Information about network connections: version and checksums (MD5, SHA2-256, SHA1) of the file from which process was started that opened the port, the path to the process's file and its digital signature, local and remote IP addresses, numbers of local and remote connection ports, connection state, timestamp of the port's opening.

- The URL and IP address of the web page where harmful or suspicious content was detected, the name, size, and checksum of the file that requested the URL, the identifier, weight and degree of the rule used to reach a verdict, the objective of the attack.

- Information about updates of the installed application and anti-virus databases: status of completion of the update task, type of error that may have occurred during the update process, the number of unsuccessful updates, the identifier of the application component that performs updates.

- Information about the use of Kaspersky Security Network (KSN): KSN identifier, application identifier, full version of the application, depersonalized IP address of the user's device, indicators of the quality of fulfillment of KSN requests, indicators of the quality of the processing of KSN packets, indicators of the number of KSN requests and information about the types of KSN requests, date and time when statistics began being sent, date and time when statistics finished being sent, information about KSN configuration updates: identifier of the active configuration, identifier of the configuration received, error code of the configuration update.

- Information about system log events: event time, name of the log where the event has been detected, type and category of event, name of the event source and event description.

- Information to determine the reputation of files and URL-addresses: the URL-address at which the reputation is being requested and the Referrer, the connection's protocol type, the internal identifier of the application type, the number of the port being used, the User identifier, checksum of the scanned file (MD5), type of the detected threat, information about the record used to detect a threat (record identifier for the anti-virus databases, the record timestamp and type); public key of the certificate; digital certificate thumbprint of the scanned object and hashing algorithm.

- Data on the application territorial distribution: date of the application installation and activation, ID of the partner providing the license for the application activation, application ID, application language localization ID, license serial number for the application activation, KSN participation sign.

- Information about the license used: the type and validity period of the license, number of days till license expiration, identifier of the partner from whom the license was purchased, Regional Activation Center identifier, checksum of the activation code, ticket body hash calculated using the SHA1 algorithm, license ticket creation date and time, license information identifier, license ticket identifier, license ticket sequence identifier, unique identifier of the user's computer, date from which the license ticket is valid, date to which the license ticket is valid, license ticket current state, ticket header version, license version, ticket header signature certificate identifier, checksum of the key file, ticket header signer serial number, authentication token.

- Information about hardware installed on the computer: type, name, model name, firmware version, parameters of built-in and connected devices.

- Information about the device: device ID.

- Information about the operation of the Web Control component: component version, categorization reason, additional information about categorization reason, categorized URL, host IP address of blocked/categorized object.

Note: Depending on Kaspersky Security Center settings, you can participate in Kaspersky Private Security Network instead of Kaspersky Security Network. Kaspersky Endpoint Security notifies you when it switches from Kaspersky Private Security Network to Kaspersky Security Network and prompts you to accept the terms of the Kaspersky Security Network Statement. For detailed information about participating in Kaspersky Private Security Network, see the Kaspersky Security Center Help.

Kaspersky Security Network infrastructure

Kaspersky Endpoint Security supports the following Kaspersky Security Network infrastructural solutions:

- *Global KSN* is the solution used by most Kaspersky applications. KSN participants receive information from Kaspersky Security Network and send Kaspersky information about objects detected on the user's computer to be analyzed additionally by Kaspersky analysts and to be included in the reputation and statistical databases of Kaspersky Security Network.

- *Private KSN* is a solution that enables users of computers hosting Kaspersky Endpoint Security or other Kaspersky applications to obtain access to Kaspersky Security Network reputation databases, and to other statistics without sending data to Kaspersky Security Network from their own computers. Private KSN is designed for corporate customers who are unable to participate in Kaspersky Security Network for any of the following reasons:

  - Local workstations are not connected to the internet.

  - Transmission of any data outside the country or outside the corporate LAN is prohibited by law or restricted by corporate security policies.

By default, Kaspersky Security Center uses Global KSN. You can configure the use of Private KSN in the Kaspersky Security Center Administration Console (MMC) and Kaspersky Security Center Web Console. It is not possible to configure the use of Private KSN in the Kaspersky Security Center Cloud Console.

KSN Proxy

Computers managed by Kaspersky Security Center Administration Server can interact with Kaspersky Security Network via the KSN Proxy service.

The KSN Proxy service provides the following capabilities:

- The user's computer can query KSN and submit information to KSN even without direct access to the internet.
- The KSN Proxy service caches processed data, thereby reducing the load on the external network communication channel and speeding up receipt of the information requested by the user's computer.

For more details on the KSN Proxy service, see the Kaspersky Security Center Help.

Note: Updates functionality (including providing anti-malware signature updates and codebase updates), as well as KSN functionality may not be available in the software in the U.S.

Check the integrity of application components

Kaspersky Endpoint Security contains various binary modules in the form of dynamic linked libraries, executable files, configuration files, and interface files. Intruders might replace one or more application executable modules or files with other files containing malicious code. To prevent this, Kaspersky Endpoint Security can check the integrity of the application components. The application checks modules and files for unauthorized changes or corruption. If an application module or file has an incorrect checksum, it is considered to be corrupted.

The integrity of the application components is checked using the integrity_checker utility located in the /Library/Application Support/Kaspersky Lab/KAV/Binaries directory. This utility checks the integrity of the manifest file containing a list of application files whose integrity is critical for correct operation of the application component.

The integrity_check.xml manifest file, which is protected by Kaspersky cryptographic signature, is located in same directory as the integrity_checker utility (/Library/Application Support/Kaspersky Lab/KAV/Binaries).

Note: Root user account privileges are required to run the integrity_checker utility.

The integrity check can be performed using the utility that is installed together with the application or using the utility on a certified CD.

To check the integrity of application components, run the following command:

```
sudo "/Library/Application Support/Kaspersky Lab/KAV/Binaries/integrity_checker"
```

By default, the utility uses the integrity_check.xml file located in the /Library/Application Support/Kaspersky Lab/KAV/Binaries directory.

To display the Help for utility settings, run the following command:

```
--help
```

The result of checking each manifest file is displayed next to the name of the manifest file in the following format:

- `SUCCEEDED`—integrity of the files is confirmed (return code `0`)
- `FAILED`—integrity of the files is not confirmed (return code is not `0`)

Manage the application via Kaspersky Security Center Administration Console

Kaspersky Security Center is designed for centralized management of corporate network security. For detailed information about Kaspersky Security Center, see the Kaspersky Security Center Help.

You can also manage Kaspersky Endpoint Security via the application's graphical user interface, Kaspersky Security Center Web Console and Cloud Console, and the command line.

Deploy Kaspersky Endpoint Security on a corporate network

1. Deploy *Administration Server* on the network.

   Administration Server is a component of Kaspersky Security Center that centrally stores information about all Kaspersky applications that are installed within the corporate network and to manage these applications.

2. Install *Administration Console* on the Kaspersky Security Center administrator's workstation.

   Administration Console is a component of Kaspersky Security Center that provides a user interface for the administrative services of Administration Server and *Network Agent*. Network Agent coordinates the interaction between Administration Server and Kaspersky Endpoint Security installed on computers within the corporate network.

3. Install the Kaspersky Endpoint Security administration plug-in on the Kaspersky Security Center administrator's workstation.

   An *administration plug-in* is a dedicated component that provides an interface for managing Kaspersky applications through Administration Console. Each application has its own administration plug-in. The administration plug-in is provided for all Kaspersky applications that can be managed from Kaspersky Security Center.

4. Install Network Agent on remote Mac computers in one of the following ways:

   - Locally
   - Remotely using Apple Remote Desktop
   - Remotely via Kaspersky Security Center
   - Remotely using the SSH protocol

   Note: To manage Kaspersky Endpoint Security for Mac 12.2 via Kaspersky Security Center, you must install Network Agent version 15 on remote computers.

5. Install Kaspersky Endpoint Security on remote Mac computers in one of the following ways:

   - Locally
   - Remotely using Apple Remote Desktop
   - Remotely using the SSH protocol
   - Remotely via Kaspersky Security Center

   Important: If Kaspersky Internet Security for Mac or third-party anti-malware software is installed on remote computers, uninstall them before installing Kaspersky Endpoint Security.

For detailed information on how to deploy Administration Server and install Administration Console, see the Kaspersky Security Center Help.

Update Kaspersky Endpoint Security version 11.1 or later to version 12.2

Note: To manage Kaspersky Endpoint Security for Mac 12.2 via Kaspersky Security Center, you must install Network Agent version 15 on remote computers.

You can update Kaspersky Endpoint Security managed via Kaspersky Security Center from version 11.1 or later to version 12.2 in one of the following ways:

- Simultaneously update Kaspersky Endpoint Security to version 12.2 and Network Agent to version 15 on remote computers.
- First update Network Agent to version 15 and then update Kaspersky Endpoint Security to version 12.2.

When you update the application to a newer version, consider the following:

- To update Kaspersky Endpoint Security to version 12.2, macOS 12 or later is required.
- You need to download the KES_11.3_profile.zip archive from the Technical Support website to apply the new configuration profile.
- After updating Kaspersky Endpoint Security to version 12.2 two Kaspersky Filter and two Kaspersky Monitor items may appear in the Network settings.
- If you have Kaspersky Endpoint Security version 11.0.1 or earlier, to update application to version 12.2, you need to uninstall the application and update macOS to version 12 or later. Then you can install Kaspersky Endpoint Security version 12.2.

Note: Updates functionality (including providing anti-malware signature updates and codebase updates), as well as KSN functionality may not be available in the software in the U.S.

Prepare for remote installation of Kaspersky Endpoint Security

This section contains information about installation of the Kaspersky Endpoint Security administration plug-in on the Kaspersky Security Center administrator's workstation and installation of Network Agent on the remote computer.

Installation of the Kaspersky Endpoint Security administration plug-in and Network Agent is a prerequisite for installation of Kaspersky Endpoint Security via Kaspersky Security Center.

Install the Kaspersky Endpoint Security administration plug-in

The Kaspersky Endpoint Security administration plug-in provides an interface for managing Kaspersky Endpoint Security through Administration Console.

Install the Kaspersky Endpoint Security administration plug-in

1. On the Kaspersky Security Center administrator's workstation, unpack the archive with the Kaspersky Endpoint Security installation package files.
2. Open the folder with the Kaspersky Endpoint Security installation package files.
3. Double-click klcfginst.exe.

   Installation of the Kaspersky Endpoint Security administration plug-in starts.

Important: Before installing the Kaspersky Endpoint Security administration plug-in, close Administration Console on the Kaspersky Security Center administrator's workstation.

Install Network Agent locally

Network Agent coordinates the interaction between Administration Server and Kaspersky Endpoint Security installed on computers within the corporate network.

Install Network Agent locally

1. On the remote computer, open the folder with the Network Agent distribution kit.
2. Open the Network Agent distribution kit (DMG file).

   A window with the contents of the distribution kit opens.
3. In the window with the contents of the distribution kit, double-click **Kaspersky Network Agent**.
4. Confirm that you want to install Network Agent by clicking **Continue**.

5. In the **Introduction** window, click **Continue**.
6. In the **License** window, read the text of the Network Agent End User License Agreement between you and AO Kaspersky Lab and do the following:
   - To accept all the terms of the agreement and proceed with the installation, click **Continue**.
   - To print the text of the agreement, click **Print**.
   - To save the agreement as a text file, click **Save**.
7. In the confirmation window, do one of the following:
   - To proceed with the installation of Network Agent, click **Agree**.
   - To return to the text of the End User License Agreement, click **Read License**.
   - To cancel the installation, click **Disagree**.
8. In the **Settings** window, do the following:
   a. In the **Server** field, specify the IP address or DNS name of the server on which Kaspersky Security Center is installed.
   b. In the **Port** field, specify the port number for an unencrypted connection to the server.
   c. In the **SSL Port** field, specify the port number for an SSL connection to the server.
   d. If you want to launch Network Agent immediately after installation, select the **Run after installation** checkbox.

   If you do not want to use SSL to connect to the server, deselect the **Use SSL** checkbox. To proceed with the installation, click **Continue**.
9. In the **Installation Type** window, read the information about the disk on which Network Agent will be installed.

   To install Network Agent using the recommended settings, click **Install** and enter the administrator password to confirm your choice.

   Wait until the Network Agent installer finishes installing the application components.
10. Click **Close** to quit the installer.

Install Network Agent using Apple Remote Desktop

1. On a remote computer, choose **Apple menu** > **System Settings** > **General** > **Sharing**.
2. Select the **Remote Management** checkbox.
3. On another Mac that you want to be a server, install Apple Remote Desktop. For more information on Apple Remote Desktop, refer to Apple Support.
4. Open Apple Remote Desktop.

5. In the **Remote Desktop** window, click **Scanner** on the left and select the devices on which you want to install Network Agent.
6. Click **Copy**.
7. Click + and select the Network Agent installation files: the DMG file, the KUD file, and the SH file.
8. In the **Place items in** pop-up menu, choose **Top folder of the disk**.
9. Click **Copy**.
10. After the files are successfully copied, click **Unix**.
11. Enter the following command:

    ```
    cd /;
    ./install.sh --accept_eula -r <Administration Server address>
    ```

    where `<Administration Server address>` is DNS name or IP address of the Kaspersky Security Center Administration Server.

    Note: By entering this command, you accept the End User License Agreement.

12. Choose to run the command as **User** and type "root" into the field.
13. Click **Send**.

Installation of Network Agent starts on the selected devices.

Install Network Agent using Kaspersky Security Center

Kaspersky Security Center installs Network Agent on a client computer using an SSH connection.

Before installing Network Agent on a client computer, make sure that the following conditions are met:

- Kaspersky Security Center Administration Server is deployed on the corporate network.
- Administration Console is installed on the Kaspersky Security Center administrator's workstation.
- Remote Login is enabled on remote computers.
- A dedicated administrator account that will be used to run the remote installation task is created on a remote computer. You can use a domain account for the installation.
- The sudo password is disabled for the dedicated account.

Create a Network Agent installation package

1. Start Kaspersky Security Center Administration Console.
2. Maximize the **Administration Server <Server name>** node.
3. In the console tree, select the **Advanced** folder, then **Remote installation** subfolder, and then the **Installation packages** subfolder.

4. In the workspace, click **Create installation package**.

5. In the **Select installation package type** window, click **Create an installation package for a Kaspersky application**.

6. In the **Defining the installation package name** window, type the name of the new installation package in the **Name** field and click **Next**.

7. In the **Selecting the distribution package for installation** window, click **Browse**.

   The window for selecting a file for creating the installation package opens.

8. Open the folder with the contents of the Network Agent installation package and select the klnagent.kud file.

   The **Selecting the distribution package for installation** window shows the name and version of the application to be installed remotely using the file that has been added.

9. Click **Next**.

   The Kaspersky Endpoint Security installation package is created with the specified settings.

10. In the last window of the wizard, click **Finish** to exit the New package wizard.

Create a task for remote installation of Network Agent on a client computer

1. Start Kaspersky Security Center Administration Console.

2. Maximize the **Administration Server <Server name>** node.

3. Select the **Tasks** folder.

4. In the workspace, start the New task wizard by clicking **New task**.

5. Follow the steps of the New task wizard below to create a task for remote installation of Kaspersky Endpoint Security on the client computer.

To proceed to the next step of the wizard, click **Next**. To return to the previous step of the wizard, click ←. To exit the wizard at any step, click **Cancel**.

Note: The appearance of the buttons may vary depending on your version of Windows.

Step 1. Select the task type

1. In the **Select the task type** window, maximize the **Kaspersky Security Center Administration Server** node.

2. Select the **Install application remotely** task.

Step 2. Select the installation package

In the **Select installation package** window, do one of the following:

- If the Network Agent installation package with the required settings has been created previously, select it in the list of installation packages in the upper part of the **Select installation package** window.

- If the required installation package has not been created yet, click **New** to start the New package wizard.

Step 3. Configure the installation settings

In the **Settings** window, do the following:

1. Select the **Using operating system resources through Administration Server** checkbox.
2. Deselect all other checkboxes.

Step 4. Select an administration group to add computers to after installation

In the **Move to list of managed devices** window, select a group to which computers will be moved after the installation, if necessary.

Step 5. Define how to select the client computers for which the task will be created

In the **Select devices to which the task will be assigned** window, select the method you want to use to specify client computers:

- To select from among computers detected on the network by Administration Server, select the **Select networked devices detected by Administration Server** option.
- To specify the IP addresses of computers manually or import the IP addresses of computers from a file, select the **Specify device addresses manually or import addresses from list** option.
- To create a task for a selection of devices based on a preset criterion, select the **Assign task to a device selection** option.
- To select computers from a specific administration group, select the **Assign task to an administration group** option.

Step 6. Select client computers

In the window that opens (**Select devices**, **Device selection**, or **Select Administration group**, depending on the option you selected in the previous step), select the client computers, specify the IP addresses of computers, specify a computer selection, or select the administration group to which the task will be applied.

Step 7. Select the account to run the task

1. In the **Selecting an account to run the task** window, select the **Account required (Network Agent is not used)** checkbox.
2. Click **Add** > **Account**.

   The **Account** window opens.
3. Enter the login and password of the dedicated administrator account of a remote computer.
4. Click **OK**.

Step 8. Configure the task schedule

1. In the **Configure task schedule** window, select the start mode in the **Scheduled start** drop-down list.
2. If necessary, configure a scheduled task to start automatically (by specifying the task start date and time).
3. If you want to run tasks that the application was unable to start according to schedule (for example, because the computer was turned off at the scheduled time), select the **Run missed tasks** checkbox.

   Kaspersky Endpoint Security starts the task as soon as the obstacle preventing the task from being started is eliminated.

Step 9. Specify the task name

In the **Define the task name** window, in the **Name** field, enter the name of the task you are creating.

Step 10. Finish creating the task

In the **Finish task creation** window, do the following:

1. If you want the task to start as soon as the wizard is finished, select the **Run the task after the Wizard finishes** checkbox.
2. Click **Finish** to close the wizard.

Install Network Agent using the SSH protocol

One way to install Network Agent on a remote computer is by using the SSH protocol.

Make sure that the following requirements are met:

- Kaspersky Security Center Administration Server is deployed on the corporate network.
- Administration Console is installed on the Kaspersky Security Center administrator's workstation.
- The Network Agent installation package is created and stored in a shared folder of Administration Server.
- Remote Login is enabled on the remote computer.
- The computer account used to install Network Agent is included in sudoers.

For detailed information about installation packages, see the Kaspersky Security Center Help.

Install Network Agent using the SSH protocol

1. Start the SSH client on the administrator's workstation.
2. Connect to the remote computer.
3. Connect the shared folder of Administration Server as a network drive on the remote computer. To do this, enter the following commands in the SSH client:

   ```
   mkdir /Volumes/KLSHARE
   mount_smbfs //<administrator account>:<password>@<Administration Server IP address>/KLSHARE /Volumes/KLSHARE
   ```

   Parameter descriptions:

   - `<administrator account>` – Name of the administrator account on Administration Server.
   - `<password>` – Password of the administrator on Administration Server.
   - `<Administration Server IP address>` – IP address of the server hosting Kaspersky Security Center.
4. Run the installation script. To do this, enter the following command in the SSH client:

   ```
   cd /Volumes/KLSHARE/<klnagent_package_folder>
   ```

   where `<klnagent_package_folder>` is the folder, in which the Network Agent installation package is located.

```
sudo ./install.sh --accept_eula [-r <server>] [-p <port number>] [-s use_ssl 0|1]
[-l <SSL port number>] [-x use_proxy 0|1] [-a <proxy>] [-n <proxy login>] [-w
<proxy password>]
```

Parameter descriptions:

- `<server>` – IP address or DNS name of the server on which Kaspersky Security Center is installed.
- `<port number>` – Number of the port that will be used to establish an unencrypted connection to Administration Server. Port 14000 is used by default.
- `use_ssl 0|1` – Parameter that defines whether encryption will be used when establishing the connection between Network Agent and Administration Server. If the value is "0", an unencrypted connection is used. If the value is "1", the connection is established via the SSL protocol (default value).
- `<SSL port number>` – Number of the port that will be used to establish an encrypted connection to Administration Server using the SSL protocol. Port 13000 is used by default.
- `use_proxy 0|1` – Parameter that defines whether a proxy server will be used when connecting to the internet. If the value is "0", a proxy server is not used. If the value is "1", the connection is established via a proxy server (default value).
- `<proxy>` – IP address or DNS name of the proxy server.
- `<proxy_login>` – User account for connecting to the proxy server.
- `<proxy_password>` – Password for connecting to the proxy server.

Important: Administrator rights are required for executing this command.

5. Disconnect the network drive on the remote computer. To do this, enter the following command in the SSH client:
   ```
   umount /Volumes/KLSHARE
   ```
6. Check if Network Agent functions properly on the remote computer. To do this, enter the following commands in the SSH client:
   ```
   cd /Library/Application\ Support/Kaspersky\ Lab/klnagent/Binaries/
   sudo ./klnagchk
   ```
   If the check is successful, Network Agent functions properly.

Uninstall Network Agent locally

1. On the remote computer, open the folder with the Network Agent distribution kit.
2. Open the Network Agent distribution kit (DMG file).
   A window with the contents of the distribution kit opens.
3. In the window with the contents of the distribution kit, double-click **Network Agent Uninstaller**.
4. In the **Introduction** window, click **Continue**.
5. In the **Information** window, click **Uninstall**.

6. In the prompt for administrator credentials, enter an administrator name and password and confirm that you want to uninstall Network Agent.

   Uninstallation of Network Agent starts.

7. Read the information about the uninstallation and click **Finish** to quit the uninstaller.

Network Agent is now removed from the remote computer.

Manage Network Agent from the command line

This section contains information on how to manage Network Agent using the command line on a client computer.

You can stop Network Agent and start it again using the command line on a client computer.

You can also connect a remote computer to Administration Server manually using the klmover utility and check the connection between the remote computer and Administration Server using the klnagchk utility.

You can uninstall Network Agent.

Start/stop Network Agent on a remote computer

You can stop Network Agent and start it again on a client computer by using the command line.

Stop Network Agent

On the remote computer, launch the launchctl utility with the unload command from the command line.

Command syntax:

```
sudo launchctl unload /Library/LaunchDaemons/com.kaspersky.klnagent.plist
```

Start Network Agent

On the remote computer, launch the launchctl utility with the load command from the command line.

Command syntax:

```
sudo launchctl load /Library/LaunchDaemons/com.kaspersky.klnagent.plist
```

Important: Administrator rights are required to stop and start Network Agent.

Check the connection between a client computer and Administration Server manually. Klnagchk utility

Check the connection between a remote computer and Administration Server

On the remote computer, run the klnagchk utility from the command line.

The klnagchk utility is included in the Network Agent distribution kit.

After Network Agent has been installed, the klnagchk utility is located in the /Library/Application Support/Kaspersky Lab/klnagent/Binaries folder.

Depending on the parameters that you specify, the klnagchk utility performs the following operations when run from the command line:

- Displays the settings specified for the connection between Network Agent installed on the remote computer and Administration Server, or saves them in a file.
- Saves Network Agent statistics (since the last startup of Network Agent) and utility execution results in a file, or displays this information on the screen.
- Tries to establish a connection between Network Agent and Administration Server.
- If the utility can't establish a connection, it sends an ICMP packet to check the status of the computer on which Administration Server is installed.

Before running the utility, go to /Library/Application Support/Kaspersky Lab/klnagent/Binaries in the command line.

Command syntax:

```
sudo ./klnagchk [-logfile <file name>] [-sp] [-savecert <path to certificate file>] [-restart]
```

Important: Administrator rights are required to run the utility.

Parameter descriptions

`-logfile <file name>` – Save the settings of the connection between Network Agent and Administration Server and utility execution results in a file. If this parameter is not specified, the server connection settings, execution results, and error messages are displayed on the screen.

`-sp` – Display the password for proxy server authentication on the screen or save it in a file. This parameter is used if Network Agent connects to Administration Server via a proxy server. By default, this parameter is not used.

`-savecert <file name>` – Save the certificate for authentication on Administration Server in a specified file.

`-restart` – Restart Network Agent after the utility finishes running.

Example:
sudo ./klnagchk -logfile klnagchk.log -sp

Connect a remote computer to Administration Server manually. Klmover utility

Connect a remote computer to Administration Server

On the remote computer, run the klmover utility from the command line.

The klmover utility is included in the Network Agent installation package.

After Network Agent has been installed, the klmover utility is located in the /Library/Application Support/Kaspersky Lab/klnagent/Binaries folder.

Depending on the parameters that you specify, the klmover utility performs the following operations when run from the command line:

- Connects Network Agent to Administration Server with the specified parameters.
- Saves utility execution results in a file or displays them on the screen.

Before running the utility, go to /Library/Application Support/Kaspersky Lab/klnagent/Binaries in the command line.

Command line syntax:

```
sudo ./klmover [-logfile <file name>] [-address <server address>] [-pn <port number>]
[-ps <SSL port number>] [-nossl] [-cert <path to certificate file>] [-silent] [-dupfix]
```

Important: The administrator rights are required to run the utility.

Parameter descriptions

`-logfile <file name>` – Save execution results in a file. If this parameter is not specified, execution results and error messages are displayed on the screen.

`-address <server address>` – Address that Network Agent uses to connect to Administration Server. You can specify either the IP address or the DNS name of the server.

Note: You can also use the command with this parameter to change the address of the Administration Server to which remote computers are connected.

`-pn <port number>` – Number of the port that will be used to establish an unencrypted connection to Administration Server. Port 14000 is used by default.

`-ps <SSL port number>` – Number of the port that will be used to establish an encrypted connection to Administration Server via the SSL protocol. Port 13000 is used by default.

`-nossl` – Use an unencrypted connection to Administration Server. If this parameter is not specified, Network Agent will establish a secure connection to Administration Server via the encrypted SSL protocol.

`-cert <path to certificate file>` – Use the specified certificate file for authentication on a new Administration Server. If this parameter is not specified, Network Agent will receive a certificate at the first connection to Administration Server.

`-silent` – Run the utility in silent mode.

`-dupfix` – This parameter is used if Network Agent was installed in a way that differs from the methods described in this Help, for example, if it was recovered from a disk image with Network Agent installed. If automatic self-identification of Network Agent results in duplicate icons of the original computer and other computers in the Administration Console, try reconnecting the duplicate computers.

Note: When running the klmover utility, it is recommended to specify values for all parameters.

Example:
sudo ./klmover -logfile klmover.log -address 192.0.2.12 -ps 13001

The remote computer that is connected to Administration Server via Network Agent is called *a client computer*.

Uninstall Network Agent

Command syntax:

```
sudo '/Library/Application Support/Kaspersky Lab/klnagent/Binaries/UninstallScript'
```

Install and uninstall Kaspersky Endpoint Security

This section describes remote installation and uninstallation of Kaspersky Endpoint Security on a client computer.

You can also install or uninstall Kaspersky Endpoint Security locally or via Kaspersky Security Center Web Console or Kaspersky Security Center Cloud Console.

Install the application using the SSH protocol

Before installing Kaspersky Endpoint Security on a remote computer, make sure that the following conditions are met:

- Kaspersky Security Center Administration Server is deployed on the corporate network.
- Administration Console is installed on the Kaspersky Security Center administrator's workstation.
- An installation package for Kaspersky Endpoint Security has been created and is located in a shared folder on Administration Server.
- A key file for Kaspersky Endpoint Security is located in the shared folder on Administration Server (optional).
- Remote Login is enabled on the remote computer.
- The computer account used to install the application is included in sudoers.

Install Kaspersky Endpoint Security on a client computer using the SSH protocol

1. Start the SSH client on the Kaspersky Security Center administrator's workstation.
2. Connect to the remote computer.
3. Connect the shared folder of Administration Server as a network drive on the remote computer. To do this, enter the following commands in the SSH client:
   ```
   mkdir /Volumes/KLSHARE
   mount_smbfs //<administrator account>:<password>@<Administration Server IP address>/KLSHARE /Volumes/KLSHARE
   ```
   Parameter descriptions:
   - `<administrator account>` – Name of the administrator account on Administration Server.
   - `<password>` – Password of the administrator on Administration Server.
   - `<Administration Server IP address>` – IP address of the server hosting Kaspersky Security Center.
4. Run the installation script. To do this, enter the following commands in the SSH client:
   ```
   cd /Volumes/KLSHARE/<KES package folder>
   ./install.sh --accept_eula
   ```
   where `<KES package folder>` is the folder, in which the Kaspersky Endpoint Security installation package is located.

   Important: Administrator rights are required for executing this command.
5. Disconnect the network drive on the remote computer. To do this, enter the following command in the SSH client:
   ```
   umount /Volumes/KLSHARE
   ```

Install the application using Kaspersky Security Center

Before installing Kaspersky Endpoint Security on a client computer, make sure that the following conditions are met:

- Kaspersky Security Center Administration Server is deployed on the corporate network.
- Administration Console is installed on the Kaspersky Security Center administrator's workstation.
- Network Agent is installed on the client computer.
- An installation package for Kaspersky Endpoint Security has been created and is stored in the shared folder on Administration Server.
- A key file for Kaspersky Endpoint Security is stored in the shared folder on Administration Server (optional).
- The client computer is added to the **Managed devices** administration group on Administration Server (optional).

For detailed information about administration groups on Administration Server, see the Kaspersky Security Center Help.

To install Kaspersky Endpoint Security on a client computer using Kaspersky Security Center, you must create and start the **Install application remotely** task.

Create a task for remote installation of Kaspersky Endpoint Security on a client computer

1. Start Kaspersky Security Center Administration Console.
2. Maximize the **Administration Server <Server name>** node.
3. Select the **Tasks** folder.
4. In the workspace, start the New task wizard by clicking **New task**.
5. Follow the steps of the New task wizard below to create a task for remote installation of Kaspersky Endpoint Security on the client computer.

To proceed to the next step of the wizard, click **Next**. To return to the previous step of the wizard, click ←. To exit the wizard at any step, click **Cancel**.

Note: The appearance of the buttons may vary depending on your version of Windows.

Step 1. Select the task type

1. In the **Select the task type** window, maximize the **Kaspersky Security Center Administration Server** node.
2. Select the **Install application remotely** task.

Step 2. Select the installation package

In the **Select installation package** window, do one of the following:

- If the Kaspersky Endpoint Security installation package with the required settings has been created previously, select it in the list of installation packages in the upper part of the **Select installation package** window.
- If the required installation package has not been created yet, click **New** to start the New package wizard.

Step 3. Install additional applications

In the **Advanced** window, select the **Install Network Agent together with this application** and **<Network Agent installation package name>** checkboxes if you want to install Network Agent on the client computer also.

> **Note:** The installation package for Network Agent must be created beforehand. If it has not been created, click **Create** to start the New package wizard.

Step 4. Configure the installation settings

In the **Settings** window, configure the remote installation of the application.

Step 5. Select an administration group to add computers to after installation

In the **Move to list of managed devices** window, select a group to which computers will be moved after the installation, if necessary.

> **Note:** The **Move to list of managed devices** window appears if you select installation of Network Agent in step 3.

Step 6. Define how to select the client computers for which the task will be created

In the **Select devices to which the task will be assigned** window, select the method you want to use to specify client computers:

- To select from among computers detected on the network by Administration Server, select the **Select networked devices detected by Administration Server** option.
- To specify the IP addresses of computers manually or import the IP addresses of computers from a file, select the **Specify device addresses manually or import addresses from list** option.
- To create a task for a selection of devices based on a preset criterion, select the **Assign task to a device selection** option.
- To select computers from a specific administration group, select the **Assign task to an administration group** option.

Step 7. Select client computers

In the window that opens (**Select devices**, **Device selection**, or **Select Administration group**, depending on the option you selected in the previous step), select the client computers, specify the IP addresses of computers, specify a computer selection, or select the administration group to which the task will be applied.

Step 8. Select an account to run the task

In the **Selecting an account to run the task** window, select the **No account required (Network Agent installed)** checkbox.

It is assumed that you have installed Network Agent before starting this wizard.

Step 9. Configure the task schedule

1. In the **Configure task schedule** window, select the start mode in the **Scheduled start** drop-down list.
2. If necessary, configure a scheduled task to start automatically (by specifying the task start date and time).
3. If you want to run tasks that the application was unable to start according to schedule (for example, because the computer was turned off at the scheduled time), select the **Run missed tasks** checkbox.

   Kaspersky Endpoint Security starts the task as soon as the obstacle preventing the task from being started is eliminated.

Step 10. Specify the task name

In the **Define the task name** window, in the **Name** field, enter the name of the task you are creating.

Step 11. Finish creating the task

In the **Finish task creation** window, do the following:

1. If you want the task to start as soon as the wizard is finished, select the **Run the task after the Wizard finishes** checkbox.
2. Click **Finish** to close the wizard.

The task that you have created appears in the workspace of the **Tasks** folder.

Create an installation package

When you create the **Install application remotely** task, you can either use an existing installation package or create a new one. To view the list of the created Installation packages, click **Advanced** > **Remote installation** > **Installation packages**.

Create an installation package in Kaspersky Security Center

1. Start Kaspersky Security Center Administration Console.
2. Maximize the **Administration Server <Server name>** node.
3. In the console tree, select the **Advanced** folder, then **Remote installation** subfolder, and then the **Installation packages** subfolder.
4. In the workspace, click **Create installation package**.
5. In the **Select installation package type** window, click **Create an installation package for a Kaspersky application**.
6. In the **Defining the installation package name** window, type the name of the new installation package in the **Name** field and click **Next**.
7. In the **Selecting the distribution package for installation** window, click **Browse**.

   The window for selecting a file for creating the installation package opens.

8. Open the folder with the contents of the Kaspersky Endpoint Security installation package and select the kesmac.kud file.

   The **Selecting the distribution package for installation** window shows the name and version of the application to be installed remotely using the file that has been added.

9. Select the **Copy updates from repository to installation package** checkbox to copy application updates from the Kaspersky Security Center storage to the installation package, if necessary, and click **Next**.

   The installation package starts uploading to Administration Server. When the upload is finished, the **Installation Type** window opens.

10. In the **Installation Type** window, in the **Packages to install** section, select or deselect the checkboxes next to the names of the components that you want to skip during installation on the client computer, and click **Next**.

    The Kaspersky Endpoint Security installation package is created with the specified settings.

11. In the last window of the wizard, click **Finish** to complete the New package wizard.

Uninstall the application using Kaspersky Security Center

Before removing Kaspersky Endpoint Security from a client computer via Kaspersky Security Center, make sure the following conditions are met:

- Kaspersky Security Center Administration Server is deployed on the corporate network.
- Administration Console is installed on the Kaspersky Security Center administrator's workstation.
- Network Agent is installed on the client computer.

To uninstall Kaspersky Endpoint Security from the client computer via Kaspersky Security Center, you have to create and start the **Uninstall application remotely** task.

Important: Removing Kaspersky Endpoint Security from a client computer may lead to a risk of infection.

Create a task for remote uninstallation of Kaspersky Endpoint Security from a client computer

1. Start Kaspersky Security Center Administration Console.
2. Maximize the **Administration Server <Server name>** node.
3. Select the **Tasks** folder.
4. In the workspace, start the New task wizard by clicking **New task**.
5. Follow the steps of the New task wizard below to create a task for remote uninstallation of Kaspersky Endpoint Security from the client computer.

To proceed to the next step of the wizard, click **Next**. To return to the previous step of the wizard, click ←. To exit the wizard at any step, click **Cancel**.

Note: The appearance of the buttons may vary depending on your version of Windows.

Step 1. Select the task type

1. In the **Select the task type** window, maximize the **Kaspersky Security Center Administration Server** node.
2. Expand the **Advanced** child node.
3. Select the **Uninstall application remotely** task.

Step 2. Select the application to uninstall

In the **Select application to be uninstalled** window, select **Uninstall application supported by Kaspersky Security Center**.

Step 3. Configure uninstallation settings

In the **Settings** window, do the following:

1. In the **Application to be uninstalled** drop-down list, select **Kaspersky Endpoint Security for Mac 12.2**.
2. Click **Next**.
3. Configure remote uninstallation of the application.

Step 4. Select the operating system restart option

In the **Selecting an operating system restart option** window, select the **Do not restart the device** option.

Step 5. Define how to select client computers for which the task will be created

In the **Select devices to which the task will be assigned** window, select the method you want to use to specify client computers:

- To select from among computers detected on the network by Administration Server, select the **Select networked devices detected by Administration Server** option.
- To specify the IP addresses of computers manually or import the IP addresses of computers from a file, select the **Specify device addresses manually or import addresses from list** option.
- To create a task for a selection of devices based on a preset criterion, select the **Assign task to a device selection** option.
- To select computers from a specific administration group, select the **Assign task to an administration group** option.

Step 6. Select client computers

In the window that opens (**Select devices**, **Device selection**, or **Select Administration group**, depending on the option you selected in the previous step), select the client computers, specify the IP addresses of computers, specify a computer selection, or select the administration group to which the task will be applied.

Step 7. Select a user account to run the task

In the **Selecting an account to run the task** window, select the **No account required (Network Agent installed)** checkbox.

It is assumed that you have installed Network Agent before starting this wizard.

Step 8. Configure the task schedule

1. In the **Configure task schedule** window, select the start mode in the **Scheduled start** drop-down list.
2. If necessary, configure a scheduled task to start automatically (by specifying the task start date and time).
3. If you want to run tasks that the application was unable to start according to schedule (for example, because the computer was turned off at the scheduled time), select the **Run missed tasks** checkbox.

   Kaspersky Endpoint Security starts the task as soon as the obstacle preventing the task from being started is eliminated.

Step 9. Specify the task name

In the **Define the task name** window, in the **Name** field, enter the name of the task you are creating.

Step 10. Finish creating the task

In the **Finish task creation** window, do the following:

1. If you want the task to start as soon as the wizard is finished, select the **Run the task after the Wizard finishes** checkbox.
2. Click **Finish** to close the wizard.

The task that you have created appears in the workspace of the **Tasks** folder.

Start and stop the application via Kaspersky Security Center

You can start or stop Kaspersky Endpoint Security on a selected computer in the list of devices managed via Kaspersky Security Center.

Start or stop Kaspersky Endpoint Security via Kaspersky Security Center

1. Start Kaspersky Security Center Administration Console.
2. Maximize the **Administration Server <Server name>** node.
3. In the console tree, click **Managed devices**.
4. Select the administration group that contains the required client computer.
5. Select the **Devices** tab.
6. Select a computer from the list of client computers.
7. Open the **Properties: <Computer name>** window in one of the following ways:

   - Double-click the name of the client computer.
   - Right-click the client computer and choose **Properties** from the context menu.

8. Select the **Applications** section.

9. In the **Kaspersky applications installed on the device** list, right-click to open the context menu of the **Kaspersky Endpoint Security for Mac 12.2** item and do one of the following:

   - To start the application, select the **Start** item.
   - To stop the application, select the **Stop** item.

Important: After Kaspersky Endpoint Security is stopped, the client computer keeps running in unprotected mode, which may lead to a risk of infection.

Create and manage tasks

This section describes how to use Kaspersky Security Center to create and configure tasks that Kaspersky Endpoint Security performs on a client computer or a group of computers.

A task is a set of configurable actions that Kaspersky Endpoint Security performs on a client computer.

In Kaspersky Security Center, you can create the following tasks:

- Add key
- Quick Scan
- Rollback
- Scan
- Update

You can take the following actions on tasks:

- Start and stop tasks.
- Configure task settings.
- Track the progress of a task.
- Copy and move tasks from one group to another.
- Delete tasks.
- Import and export tasks.

For detailed information about tasks, see the Kaspersky Security Center Help.

Create tasks

When managing Kaspersky Endpoint Security via Kaspersky Security Center, you can create the following types of tasks:

- Local tasks. *A local task* is a task to run on a separate client computer.
- Group tasks. *A group task* is a task to run on computers in an administration group.
- Tasks for an arbitrary set of computers. You can create a task to be run on any computers regardless of whether they belong to an administration group or a computer selection.

Create a local task for a separate client computer

1. Start Kaspersky Security Center Administration Console.
2. Maximize the **Administration Server <Server name>** node.
3. In the console tree, click **Managed devices**.
4. Select the administration group that contains the required client computer.
5. In the workspace, select the **Devices** tab.
6. Select the computer from the list of client computers.
7. Open the **Properties: <Computer name>** window in one of the following ways:
   - Double-click the name of the client computer.
   - Right-click the client computer and choose **Properties** from the context menu.
8. In the **Properties: <Computer name>** window, select the **Tasks** section.

   The list of system tasks and custom tasks for the selected client computer is displayed in the workspace on the right.
9. Click **Add** in the lower part of the workspace.

   The New task wizard starts.
10. Follow the steps of the New task wizard to create a local task for a separate client computer.

Create a task for client computers in an administration group

1. Start Kaspersky Security Center Administration Console.
2. Maximize the **Administration Server <Server name>** node.
3. In the console tree, click **Managed devices**.
4. Select the administration group that contains the required client computer.
5. In the workspace, select the **Tasks** tab.

6. In the workspace, click **New task** to start the New task wizard.
7. Follow the steps of the New task wizard to create a task for client computers included in the administration group.

For detailed information on how to create group tasks, see the Kaspersky Security Center Help.

Create a task for an arbitrary set of computers

1. Start Kaspersky Security Center Administration Console.
2. Maximize the **Administration Server <Server name>** node.
3. In the console tree, click **Tasks**.
4. In the workspace, click **New task** to start the New task wizard.
5. Follow the steps of the New task wizard to create a task for an arbitrary set of computers.

To proceed to the next step of the wizard, click **Next**. To return to the previous step of the wizard, click ←. To exit the wizard at any step, click **Cancel**.

Note: The appearance of the buttons may vary depending on your version of Windows.

Step 1. Select an application and define the task type

1. In the **Select the task type** window, maximize the **Kaspersky Endpoint Security for Mac 12.2** node.
2. Select the type of the task you want to create:
   - To create a task for adding a key, select **Add key**.
   - To create a critical areas scan task, select **Quick Scan**.
   - To create a task to roll back the latest update, select **Rollback**.
   - To create a malware scan task, select **Scan**.
   - To create an update task, select **Update**.

Step 2. Configure settings for the selected task type

Depending on the task type selected during the previous step, the contents of the settings window may vary. This window is not displayed for the Rollback task.

Application activation

In the **Application activation** window, do the following:

1. Select an activation code or key from Kaspersky Security Center storage or add a key file stored on your computer.
2. If you want to add the specified key as a reserve key, select the **Add as reserve key** checkbox.

   The reserve key becomes active when the current active key expires.

Information about the specified key (key, key type, and key expiration date) is displayed in the **Application activation** window.

Update

Dedicated Kaspersky update servers are the main source of updates for Kaspersky Endpoint Security. Kaspersky Endpoint Security can also use distribution points, local folders, or other web servers as an *update source*.

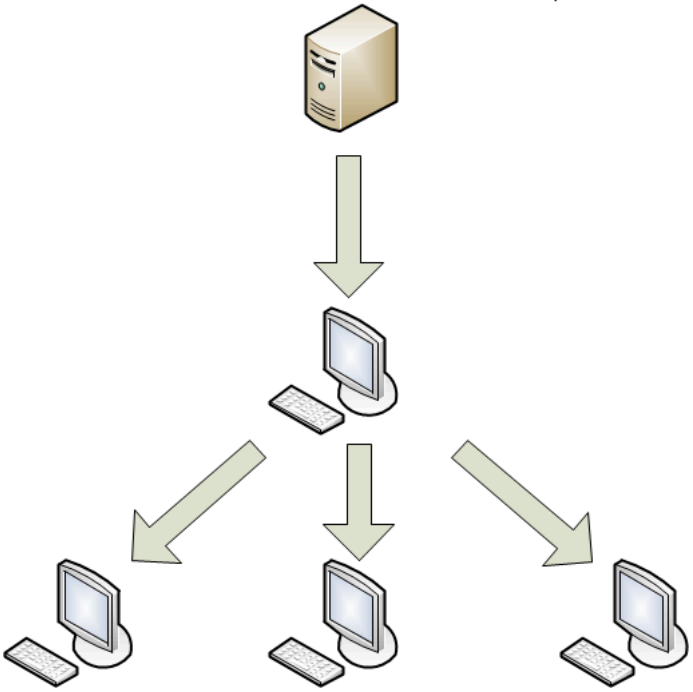
You can put downloaded updates in a local folder to update application databases and Kaspersky Endpoint Security modules on other computers on the corporate network in order to reduce the amount of internet traffic.

You can set up update distribution as follows:

1. One of the computers on the network receives the Kaspersky Endpoint Security update package from Kaspersky update servers or a different update source. The retrieved updates are placed in a shared local folder.

   Note: The shared local folder must be created in advance.

2. Other computers on the network refer to the shared local folder as the update source.



Distribution of updates via a local computer

If necessary, edit the Update task settings in the **Update** window:

1. To disable updates of application modules, deselect the **Update application modules** checkbox.
2. To change the update sources:
   a. Click **Settings**.
      The **Settings: Update** window opens.
   b. Select the checkboxes next to the update sources that you want to use.
3. To specify a different update source, click **Add**.
   The **Update source** window opens.
   a. Specify the web address of the update source or the path to a local or network folder that is an update source and click **OK**.
   b. Click **OK** to save changes and close the **Settings: Update** window.

Scan and Quick Scan

By default, Kaspersky Endpoint Security uses the **Recommended** security level, prompts the user for an action when it detects an infected object after the scan, and scans the following objects:

- All removable drives
- All internal drives

- All network drives
- Memory

Note: Kaspersky Endpoint Security does not scan files that are located in OneDrive or iCloud storage or other cloud storages. Please exclude these files from the scan scope. Otherwise, the scan task may finish with the *Infected File Not Deleted* error.

If necessary, edit the Scan settings in the **Scan** window:

1. Select one of the preset security levels or customize security settings.
2. Specify the action that Kaspersky Endpoint Security performs upon detecting an infected object.
3. Define a scan scope.

Step 3. Define how to select client computers for which the task will be created

Note: This step is not relevant for local or group tasks.

In the **Select devices to which the task will be assigned** window, select the method you want to use to specify client computers:

- To select from among computers detected on the network by Administration Server, select the **Select networked devices detected by Administration Server** option.
- To specify the IP addresses of computers manually or import the IP addresses of computers from a file, select the **Specify device addresses manually or import addresses from list** option.
- To create a task for a selection of devices based on a preset criterion, select the **Assign task to a device selection** option.
- To select computers from a specific administration group, select the **Assign task to an administration group** option.

Step 4. Select client computers

Note: This step is not relevant for local or group tasks.

In the window that opens (**Select devices**, **Device selection**, or **Select Administration group**, depending on the option you selected in the previous step), select the client computers, specify the IP addresses of computers, specify a computer selection, or select the administration group to which the task will be applied.

Step 5. Configure the task schedule

1. In the **Configure task schedule** window, select the start mode in the **Scheduled start** drop-down list.
2. If necessary, configure a scheduled task to start automatically (by specifying the task start date and time).

3. If you want to run tasks that the application was unable to start according to schedule (for example, because the computer was turned off at the scheduled time), select the **Run missed tasks** checkbox.

   Kaspersky Endpoint Security starts the task as soon as the obstacle preventing the task from being started is eliminated.

4. If you want Kaspersky Security Center to automatically determine the interval between task launches on different computers, select the **Use automatically randomized delay for task starts** checkbox.

   This helps to reduce the load on Kaspersky Security Center Administration Server.

5. To set the interval between task launches on different computers manually, select the **Use randomized delay for task starts within an interval of (min)** checkbox and specify the number of minutes.

   This helps to reduce the load on Kaspersky Security Center Administration Server.

Step 6. Specify the task name

In the **Define the task name** window, in the **Name** field, enter the name of the task you are creating.

Step 7. Finish creating the task

In the **Finish task creation** window, do the following:

1. If you want the task to start as soon as the wizard is finished, select the **Run the task after the Wizard finishes** checkbox.

2. Click **Finish** to close the wizard.

Start and stop tasks manually

Scheduled tasks are started and stopped automatically according to a schedule. However, you can start a task manually at any time.

> **Note:** Tasks are started on a client computer only if Network Agent is running. If Network Agent stops running, all active tasks are interrupted.

Start and stop tasks manually

1. Open the list of tasks that contains the task that you want to start or stop.

2. Select the task that you want to start or stop.

3. Start or stop the task in one of the following ways:

   - Right-click to display the context menu of the task and choose **Start** or **Stop**.

   - In the workspace, click **Start** or **Stop**.

   - Right-click to display the context menu of the task and choose **Properties**. In the window that opens, click **Start** or **Stop**.

Import and export tasks

You can export group tasks and tasks for an arbitrary set of computers to a file.

Export a task

1. Select the task list from which you want to export the task:
   - Select the administration group and then open the **Tasks** tab.
   - In the console tree, click **Tasks**.
2. Right-click the task you want to export and, in the task's shortcut menu, choose **All Tasks** > **Export**.
3. In the **Save As** window, specify the file name and location where the exported task will be saved.
4. Click **Save**.

Import a task

1. Select the task list to which you want to import the task:
   - Select the administration group and then open the **Tasks** tab.
   - In the console tree, click **Tasks**.
2. Import the task in any of the following ways:
   - In the task list's shortcut menu, select **All Tasks** > **Import**.
   - Click **Import task from file**.
3. In the **Open** window, specify the path to the task file you want to import.
4. Click **Open**.

   The task is displayed in the task list.

View tasks

You can view the list of tasks created for a specific computer, for computers in a specific administration group, or the list of all non-local tasks.

View tasks for a specific administration group

1. Start Kaspersky Security Center Administration Console.
2. Maximize the **Administration Server <Server name>** node.
3. In the console tree, click **Managed devices**.

4. Select the administration group that contains the required client computer.
5. In the workspace, select the **Tasks** tab.

The list of tasks for computers in the selected administration group is displayed.

View local tasks

1. Start Kaspersky Security Center Administration Console.
2. Maximize the **Administration Server <Server name>** node.
3. In the console tree, click **Managed devices**.
4. Select the administration group that contains the required client computer.
5. In the workspace, select the **Devices** tab.
6. Select the computer from the list of client computers.
7. Open the **Properties: <Computer name>** window in one of the following ways:
   - Double-click the name of the client computer.
   - Right-click the client computer and choose **Properties** from the context menu.
8. In the **Properties: <Computer name>** window, select the **Tasks** section.

The list of system tasks and custom tasks for the selected client computer is displayed in the workspace on the right.

View non-local tasks

1. Start Kaspersky Security Center Administration Console.
2. Maximize the **Administration Server <Server name>** node.
3. In the console tree, click **Tasks**.

The list of non-local tasks created for computers that may or may not be part of administration groups is displayed.

Manage task-specific settings

View settings of a local task

1. Open the list of local tasks.
2. Select a task in the list and open the task settings in one of the following ways:
   - Double-click the task name.
   - Right-click to display the task's shortcut menu and select **Properties**.

View settings of a group task

1. Open the list of group tasks for an administration group.
2. Select a task in the list and open the task settings in one of the following ways:
   - Double-click the task name.
   - Right-click to display the task's shortcut menu and select **Properties**.
   - Click the **Configure task** link in the workspace.

View settings of a non-local task

1. Open the list of non-local tasks.
2. Select a task in the list and open the task settings in one of the following ways:
   - Double-click the task name.
   - Right-click to display the task's shortcut menu and select **Properties**.
   - Click the **Configure task** link in the workspace.

For more information about tasks, see the Kaspersky Security Center Help.

For local tasks, group tasks, or tasks for an arbitrary set of computers

Manage the Add key task settings

1. Open the window with the **Add key** task settings.
2. Select the **Application activation** section.
3. If necessary, add another key in one of the following ways:
   - To select a key or an activation code from among the activation codes added to the Kaspersky Security Center storage:
     a. Select the **Key or activation code** option.
     b. Click **Browse**.
     The **Keys and activation codes in Kaspersky Security Center storage** window opens.
     c. Select a key or activation code.
     d. Click **OK**.

- To add a key file:

  a. Select the **Key file** option.

  b. Click **Add**.

  The file selection window opens.

  c. Select a key file.

  d. Click **Open**.

> **Note:** The current key is deleted when a different key is added.

4. To add the specified key as a reserve key, select the **Add as reserve key** checkbox.

   The reserve key becomes active when the current key expires.

> **Note:** The reserve key expiration date must be later than the current key expiration date.

5. Save the changes in one of the following ways:

   - Click **Apply** to remain in the **Properties: <Task name>** window after saving changes.
   - Click **OK** to close the **Properties: <Task name>** window after saving changes.

Manage the Quick Scan task settings

1. Open the window with the **Quick Scan** task settings.
2. Select the **Quick Scan** section.
3. To change the level of security at which Kaspersky Endpoint Security runs the Quick Scan task, do one of the following in the **Security level** section:

   - Select a preset security level by moving the slider up or down the scale.

     You can select one of the following security levels:

     - **Maximum protection**. Kaspersky Endpoint Security performs the maximum monitoring of files that are opened, saved, or executed.
     - **Recommended**. Kaspersky Endpoint Security monitors files with the settings recommended by Kaspersky.

       This is the default security level.
     - **Maximum speed**. Kaspersky Endpoint Security monitors a minimum set of files. You can choose this security level if you want to use other applications that require significant memory resources.
   - Configure security settings manually:

     a. Click **Settings**.

     The **Settings: Scan** window opens.

b. On the **General** tab, in the **File types** section, select the types of files that should be scanned by Kaspersky Endpoint Security when running the Quick Scan task.

c. On the **General** tab, in the **Optimization** section, configure scan performance settings.

d. On the **General** tab in the **Compound files** section, select which compound files you want Kaspersky Endpoint Security to analyze for detectable objects.

e. On the **Advanced** tab, in the **Advanced settings** section, configure the use of iSwift technology and recording of information about detected objects in the application statistics.

f. On the **Advanced** tab, in the **Heuristic Analyzer** section, configure the use of Heuristic Analyzer and select the protection level to be applied by Heuristic Analyzer during malware scans.

g. Click **OK** to save changes and close the **Settings: Scan** window.

The security level changes to **Custom**.

- To restore the default settings, click **Default**.

  The security level changes to **Recommended**.

4. If necessary, in the **Action** section, select the action that Kaspersky Endpoint Security should perform when an infected object is detected.

5. To specify a scan scope, in the **Scan scope** section, click **Settings** and do the following in the **Scan scope** window that opens:

   a. If you want Kaspersky Endpoint Security to scan the computer memory, select the **Memory** checkbox.

   b. If you want Kaspersky Endpoint Security to scan the startup objects, select the **Login items** checkbox.

   c. If you want Kaspersky Endpoint Security to scan other additional files or folders, click **Add** and specify a file, folder, or mask for file or folder names.

   d. Click **OK** to save changes and close the **Scan scope** window.

6. Save the changes in one of the following ways:

   - Click **Apply** to remain in the **Properties: <Task name>** window after saving changes.

   - Click **OK** to close the **Properties: <Task name>** window after saving changes.

Manage the Scan task settings

1. Open the window with the **Scan** task settings.

2. Select the **Scan** section.

3. To change the level of security at which Kaspersky Endpoint Security runs the Scan task, do one of the following in the **Security level** section:

   - Select a preset security level by moving the slider up or down the scale.

You can select one of the following security levels:

- **Maximum protection**. Kaspersky Endpoint Security performs the maximum monitoring of files that are opened, saved, or executed.
- **Recommended**. Kaspersky Endpoint Security monitors files with the settings recommended by Kaspersky.

  This is the default security level.
- **Maximum speed**. Kaspersky Endpoint Security monitors a minimum set of files. You can choose this security level if you want to use other applications that require significant memory resources.

- Configure security settings manually:

  a. Click **Settings**.

  The **Settings: Scan** window opens.

  b. On the **General** tab, in the **File types** section, select the types of files that should be scanned by Kaspersky Endpoint Security when running the Scan task.

  c. On the **General** tab, in the **Optimization** section, configure scan performance settings.

  d. On the **General** tab in the **Compound files** section, select which compound files you want Kaspersky Endpoint Security to analyze for detectable objects.

  e. On the **Advanced** tab, in the **Advanced settings** section, configure the use of iSwift technology and recording of information about detected objects in the application statistics.

  f. On the **Advanced** tab, in the **Heuristic Analyzer** section, configure the use of Heuristic Analyzer and select the protection level to be applied by Heuristic Analyzer during malware scans.

  g. Click **OK** to save changes and close the **Settings: Scan** window.

  The security level changes to **Custom**.

- To restore the default settings, click **Default**.

  The security level changes to **Recommended**.

4. If necessary, in the **Action** section, select the action that Kaspersky Endpoint Security should perform when an infected object is detected.

5. To specify a scan scope, in the **Scan scope** section, click **Settings** and do the following in the **Scan scope** window that opens:

   a. If you want Kaspersky Endpoint Security to scan all removable drives, select the **All removable disks** checkbox.

   b. If you want Kaspersky Endpoint Security to scan all internal drives, select the **All internal disks** checkbox.

   c. If you want Kaspersky Endpoint Security to scan all network drives, select the **All network disks** checkbox.

   d. If you want Kaspersky Endpoint Security to scan the computer memory, select the **Memory** checkbox.

   e. If you want Kaspersky Endpoint Security to scan the startup objects, select the **Login items** checkbox.

f. If you want Kaspersky Endpoint Security to scan other files or folders, click **Add** and specify a file, folder, or mask for file or folder names.

g. Click **OK** to save changes and close the **Scan scope** window.

6. Save the changes in one of the following ways:

- Click **Apply** to remain in the **Properties: <Task name>** window after saving changes.
- Click **OK** to close the **Properties: <Task name>** window after saving changes.

Manage the Update task settings

1. Open the window with the **Update** task settings.
2. Select the **Update** section.
3. If you want Kaspersky Endpoint Security to update application modules along with application databases, select the **Update application modules** checkbox.
4. To choose an update source:

a. Click **Settings**.

The **Settings: Update** window opens.

b. Specify the update source in one of the following ways:

- If you want the application to download updates from Administration Server, select the **Kaspersky Security Center** checkbox.
- If you want the application to download updates from Kaspersky update servers, select the **Kaspersky update servers** checkbox.
- To add a different update source, click **Add** and, in the window that opens, enter the path to the update source.

  By default, Kaspersky Endpoint Security downloads updates from Kaspersky update servers.

c. Click **OK** to save changes and close the **Settings: Update** window.

5. Save the changes in one of the following ways:

- Click **Apply** to remain in the **Properties: <Task name>** window after saving changes.
- Click **OK** to close the **Properties: <Task name>** window after saving changes.

For local tasks only

Manage the File Threat Protection task settings

1. Open the list of local tasks for a client computer.
2. In the list of local tasks, select the File Threat Protection task and open its properties in one of the following ways:
   - Double-click the task name.
   - Right-click to display the task's shortcut menu and select **Properties**.
   - Click **Properties**.
3. Select the **File Threat Protection** section.
4. If necessary, configure the following settings:
   - Enable or disable File Threat Protection on the client computer.
   - To select one of the preset security levels, use the slider in the **Security level** section.
   - To configure the security settings manually, click **Settings** and in the **Settings: File Threat Protection** window that opens, do the following:
     a. On the **General** tab, in the **File types** section, select the types of files that Kaspersky Endpoint Security should scan when they are opened, executed, or saved.
     b. On the **General** tab, in the **Optimization** section, configure scan performance settings and select the scan technology, and select whether Kaspersky Endpoint Security will skip scanning of the read-only system volume on client computers.
     c. On the **General** tab, in the **Compound files** section, select which compound files should be scanned for detectable objects and set a restriction on scanning large objects.
     d. On the **Protection scope** tab, specify files or folders that should be scanned by File Threat Protection.
     By default, all objects located on removable, internal, and network drives connected to the client computer are scanned. You can add an object to the protection scope, modify an object on the list, temporarily disable scanning of an object on the list, or remove an object from the list.
     e. On the **Advanced** tab, in the **Scan mode** section, select the File Threat Protection mode.
     f. On the **Advanced** tab, in the **Pause task** section, enable or disable scheduled pausing of File Threat Protection and configure automatic pausing of tasks according to a schedule.
     g. On the **Advanced** tab, in the **Heuristic Analyzer** section, configure the use of Heuristic Analyzer by File Threat Protection.
     h. Click **OK** to save changes and close the **Settings: File Threat Protection** window.
   - In the **If a malicious object is detected** section, select the action that File Threat Protection performs upon detecting an infected object.

5. Save the changes in one of the following ways:

   - Click **Apply** to remain in the **Properties: File Threat Protection** window after saving changes.
   - Click **OK** to close the **Properties: File Threat Protection** window after saving changes.

Manage the Web Threat Protection task settings

1. Open the list of local tasks for a client computer.
2. In the list of local tasks, select the Web Threat Protection task and open its properties in one of the following ways:

   - Double-click the task name.
   - Right-click to display the task's shortcut menu and select **Properties**.
   - Click **Properties**.

3. Select the **Web Threat Protection** section.
4. If necessary, configure the following settings:

   - Enable or disable Web Threat Protection on the client computer.
   - To select one of the preset security levels, use the slider in the **Security level** section.
   - To configure the security settings manually, click **Settings** and in the **Settings: Web Threat Protection** window that opens, do the following:

     a. On the **General** tab, in the **Scan mode** section, enable or disable checking of web addresses against the database of malicious web addresses.

     b. On the **General** tab, in the **Anti-Phishing settings** section, enable or disable checking of web addresses against the database of phishing web addresses.

     c. On the **General** tab, in the **Anti-Phishing settings** section, enable or disable the use of Heuristic Analyzer for detecting phishing links.

     d. On the **Trusted web addresses** tab, enable or disable scanning of web traffic from trusted web addresses and create or edit a list of trusted web addresses.

     e. Click **OK** to save changes and close the **Settings: Web Threat Protection** window.

5. In the **If a malicious object is detected** section, select the action that Web Threat Protection performs upon detecting a dangerous object in web traffic.
6. Save the changes in one of the following ways:

   - Click **Apply** to remain in the **Properties: Web Threat Protection** window after saving changes.
   - Click **OK** to close the **Properties: Web Threat Protection** window after saving changes.

Manage the Quick Scan task settings

1. Open the list of local tasks for a client computer.
2. In the list of local tasks, select the Quick Scan task and open its properties in one of the following ways:
   - Double-click the task name.
   - Right-click to display the task's shortcut menu and select **Properties**.
   - Click **Properties**.
3. Select the **Scan** section.
4. If necessary, configure the following settings:
   - To select one of the preset security levels, use the slider in the **Security level** section.
   - To configure the security settings manually, click **Settings** and in the **Settings: Scan** window that opens, do the following:
     a. On the **General** tab, in the **File types** section, select the types of files that should be scanned by Kaspersky Endpoint Security.
     b. On the **General** tab, in the **Optimization** section, configure scan performance settings.
     c. On the **General** tab, in the **Compound files** section, select which compound files you want Kaspersky Endpoint Security to scan.
     d. On the **Advanced** tab, in the **Advanced settings** section, configure the use of iSwift technology and the saving of information about detected objects in the application statistics.
     e. On the **Advanced** tab, in the **Heuristic Analyzer** section, configure the use of Heuristic Analyzer and select the protection level to be applied by Heuristic Analyzer.
     f. Click **OK** to save changes and close the **Settings: Scan** window.
   - In the **Action** section, select the action that Kaspersky Endpoint Security should perform upon detecting an infected object.
   - To specify a scan scope, in the **Scan scope** section, click **Settings** and do the following in the **Scan scope** window that opens:
     - If you want Kaspersky Endpoint Security to scan objects in the default list, select the checkbox next to the relevant object.
     - If you want Kaspersky Endpoint Security to scan other files or folders, click **Add** and specify a file, folder, or mask for file or folder names.
     - Click **OK** to save changes and close the **Scan scope** window.
5. Save the changes in one of the following ways:
   - Click **Apply** to remain in the **Properties: Quick Scan** window after saving changes.
   - Click **OK** to close the **Properties: Quick Scan** window after saving changes.

Manage the Full Scan task settings

1. Open the list of local tasks for a client computer.
2. In the list of local tasks, select the Full Scan task and open its properties in one of the following ways:
   - Double-click the task name.
   - Right-click to display the task's shortcut menu and select **Properties**.
   - Click **Properties**.
3. Select the **Scan** section.
4. If necessary, configure the following settings:
   - To select one of the preset security levels, use the slider in the **Security level** section.
   - To configure the security settings manually, click **Settings** and in the **Settings: Scan** window that opens, do the following:
     a. On the **General** tab, in the **File types** section, select the types of files that should be scanned by Kaspersky Endpoint Security.
     b. On the **General** tab, in the **Optimization** section, configure scan performance settings.
     c. On the **General** tab, in the **Compound files** section, select which compound files you want Kaspersky Endpoint Security to scan.
     d. On the **Advanced** tab, in the **Advanced settings** section, configure the use of iSwift technology and the saving of information about detected objects in the application statistics.
     e. On the **Advanced** tab, in the **Heuristic Analyzer** section, configure the use of Heuristic Analyzer and select the protection level to be applied by Heuristic Analyzer.
     f. Click **OK** to save changes and close the **Settings: Scan** window.
   - In the **Action** section, select the action that Kaspersky Endpoint Security should perform upon detecting an infected object.
   - To specify a scan scope, in the **Scan scope** section, click **Settings** and do the following in the **Scan scope** window that opens:
     - If you want Kaspersky Endpoint Security to scan objects in the default list, select the checkbox next to the relevant object.
     - If you want Kaspersky Endpoint Security to scan other files or folders, click **Add** and specify a file, folder, or mask for file or folder names.
     - Click **OK** to save changes and close the **Scan scope** window.
5. Save the changes in one of the following ways:
   - Click **Apply** to remain in the **Properties: Full Scan** window after saving changes.
   - Click **OK** to close the **Properties: Full Scan** window after saving changes.

Manage the Custom Scan task settings

1. Open the list of local tasks for a client computer.
2. In the list of local tasks, select the Custom Scan task and open its properties in one of the following ways:
   - Double-click the task name.
   - Right-click to display the task's shortcut menu and select **Properties**.
   - Click **Properties**.
3. Select the **Scan** section.
4. If necessary, configure the following settings:
   - To select one of the preset security levels, use the slider in the **Security level** section.
   - To configure the security settings manually, click **Settings** and in the **Settings: Scan** window that opens, do the following:
     a. On the **General** tab, in the **File types** section, select the types of files that should be scanned by Kaspersky Endpoint Security.
     b. On the **General** tab, in the **Optimization** section, configure scan performance settings.
     c. On the **General** tab, in the **Compound files** section, select which compound files you want Kaspersky Endpoint Security to scan.
     d. On the **Advanced** tab, in the **Advanced settings** section, configure the use of iSwift technology and the saving of information about detected objects in the application statistics.
     e. On the **Advanced** tab, in the **Heuristic Analyzer** section, configure the use of Heuristic Analyzer and select the protection level to be applied by Heuristic Analyzer.
     f. Click **OK** to save changes and close the **Settings: Scan** window.
   - In the **Action** section, select the action that Kaspersky Endpoint Security should perform upon detecting an infected object.
   - To specify a scan scope, in the **Scan scope** section, click **Settings** and do the following in the **Scan scope** window that opens:
     - Click **Add** and specify a file, folder, or name mask of a file or folder.
     - Click **OK** to save changes and close the **Scan scope** window.
5. Save the changes in one of the following ways:
   - Click **Apply** to remain in the **Properties: Custom Scan** window after saving changes.
   - Click **OK** to close the **Properties: Custom Scan** window after saving changes.

Manage the Network Threat Protection task settings

1. Open the list of local tasks for a client computer.
2. In the list of local tasks, select the Network Threat Protection task and open its properties in one of the following ways:
   - Double-click the task name.
   - Right-click to display the task's shortcut menu and select **Properties**.
   - Click **Properties**.
3. Select the **Network Threat Protection** section.
4. If necessary, configure the following settings:
   - Enable or disable Network Threat Protection on the client computer.
   - In the **Network Threat Protection settings** section, select or deselect the **Block attacking computers for <value> min** checkbox and specify the value.
   - You can also specify the IP addresses of computers whose network activity will not be blocked. To do this, perform the following steps:
     a. Click **Exclusions**.
        The **Exclusions** window opens.
     b. Click **Add**.
        The **IP address** window opens.
     c. Specify the IP address of the computer whose network activity will not be blocked and click **OK**.
     d. Click **OK** to save changes and close the **Exclusions** window.
5. Save the changes in one of the following ways:
   - Click **Apply** to remain in the **Properties: Network Threat Protection** window after saving changes.
   - Click **OK** to close the **Properties: Network Threat Protection** window after saving changes.

Create and manage policies

This section contains information on how to create and configure policies for Kaspersky Endpoint Security.

A policy determines an application's settings and manages the ability to configure that application on computers within an administration group. An individual policy must be created for each application. You can create multiple policies for applications installed on computers in each administration group, but only one policy can be applied at a time to each application within an administration group.

Note: When creating and configuring a policy, you can allow or prohibit changes to any group of settings in policies using the and buttons.

You can perform the following actions on custom policies:

- Create policies.
- Configure policies.
- Copy or move policies from one group to another.
- Delete policies.
- Change the status of policies.
- Export policies to a file.
- Import policies from a file.

For detailed information about the Kaspersky Security Center policies, see the Kaspersky Security Center Help.

Create a policy

This section contains instructions on how to start the New policy wizard to create a policy.

Create a policy from the folder of an administration group

1. Start Kaspersky Security Center Administration Console.
2. Maximize the **Administration Server <Server name>** node.
3. In the console tree, click **Managed devices**.
4. Select the administration group that contains the required client computer.
5. In the workspace, select the **Policies** tab and click **New policy**.
   The New policy wizard opens.
6. Follow the steps of the New policy wizard to create a policy.

Create a policy from the Policies folder

1. Start Kaspersky Security Center Administration Console.
2. Maximize the **Administration Server <Server name>** node.
3. In the console tree, click **Policies**.

4. In the workspace, click **New policy**.

   The New policy wizard opens.

5. Follow the steps of the New policy wizard to create a policy.

To proceed to the next step of the wizard, click **Next**. To return to the previous step of the wizard, click ←. To exit the wizard at any step, click **Cancel**.

Note: The appearance of the buttons may vary depending on your version of Windows.

Step 1. Select an application

In the **Select the application for which you want to create a group policy** window, in the list of applications, select **Kaspersky Endpoint Security for Mac (12.2)**.

Step 2. Specify the name of the policy

1. In the **Enter a group policy name** window, in the **Name** field, specify the name of the policy that you are creating. The name can't contain the following symbols: " * < : > ? \ |.

2. Select the **Use policy settings for an earlier version of the application** checkbox if you want to import the settings from an existing Kaspersky Endpoint Security policy to a new policy.

Step 3. Specify protection settings

In the **Protection** window, configure the following settings if necessary:

- Configure protection settings for the operating system on the client computer.
- Configure Trusted zone.

  You can create a list of objects that Kaspersky Endpoint Security does not scan or monitor.
- Configure Trusted applications.

  You can create a list of applications whose network and file activity will not be monitored by Kaspersky Endpoint Security.
- Select types of objects to be detected.
- Disable or enable the start of scheduled tasks when the computer is running on battery power.
- Limit scan tasks' use of the CPU.

Step 4. Configure File Threat Protection settings

In the **File Threat Protection** window, do the following if necessary:

- Enable or disable File Threat Protection.

  By default, File Threat Protection is enabled.
- Select a security level.

  By default, the security level recommended by Kaspersky is selected.

- Configure File Threat Protection settings.
- Select the action to be performed upon detecting a malicious object.

Step 5. Configure Web Threat Protection settings

In the **Web Threat Protection** window, do the following if necessary:

- Enable or disable Web Threat Protection.
  By default, Web Threat Protection is enabled.
- Select a security level.
  By default, the security level recommended by Kaspersky is selected.
- Configure Web Threat Protection settings.
- Select the action to be performed upon detecting a malicious object in web traffic.

Step 6. Configure Network Threat Protection settings

In the **Network Threat Protection** window, do the following if necessary:

- Enable or disable Network Threat Protection.
  By default, Network Threat Protection is enabled.
- Configure Network Threat Protection settings.
- Create or edit a list of IP addresses of remote computers whose network activity will never be blocked by Kaspersky Endpoint Security.

Step 7. Configure update settings

In the **Update** window, do the following if necessary:

- Enable or disable updating of application modules.
- Specify update sources.

Step 8. Configure KSN settings

In the **Kaspersky Security Network** window, do the following if necessary:

- Read the full text of the Kaspersky Security Network Statement by clicking the **KSN Statement** button.
- View information about KSN infrastructure provided by Kaspersky Security Center.
- Enable or disable the use of Kaspersky Security Network.
- Enable or disable extended KSN mode.
- Enable or disable the use of a KSN proxy.
- Enable or disable the use of Kaspersky servers when the KSN proxy is unavailable.

Note: Use of Kaspersky Security Network and a KSN proxy on remote computers is available only if Kaspersky Security Center Administration Server is used as the proxy server. For detailed information about Administration Server properties, see the Kaspersky Security Center Help.

When Global KSN infrastructure is used by Kaspersky Security Center and you choose to participate in Kaspersky Security Network in policy settings, Kaspersky Endpoint Security statistics from client computers to which the policy is applied are automatically sent to Kaspersky to enhance protection of these computers.

Note: Kaspersky doesn't receive, process, or store any personal data without your explicit consent.

Data provided to Kaspersky when using Kaspersky Security Network in Global KSN infrastructure

If the **I agree to use Kaspersky Security Network** checkbox is selected and the **Enable extended KSN mode** checkbox is unselected, Kaspersky Endpoint Security provides to Kaspersky the following data:

- Information about the license used: the type and validity period of the license, number of days till license expiration, identifier of the partner from whom the license was purchased, Regional Activation Center identifier, checksum of the activation code, ticket body hash calculated using the SHA1 algorithm, license ticket creation date and time, license information identifier, license ticket identifier, license ticket sequence identifier, unique identifier of the user's computer, date from which the license ticket is valid, date to which the license ticket is valid, license ticket current state, ticket header version, license version, ticket header signature certificate identifier, checksum of the key file, ticket header signer serial number, authentication token.

- Full version of installed Software; type of installed Software; Software update ID; ID of reputation service; protocol type ID; ID of a regional activation center; version of list of revoked Software service's decisions; ID of the triggered record in the Software's anti-virus databases; timestamp of the triggered record in the Software's anti-virus databases; type of the triggered record in the Software's anti-virus databases; unique ID of the instance of application installation on the computer; license activation date; license expiration date; license identifier; status of the license used by the Software; checksum type for the object being processed; name of the detected malware or legitimate software that can be used to damage the user's device or data; checksum of the object being processed; checksum of the Software activation code; full version of the Software; unique device ID; Software ID; checksum of the Software key file; ID of the information model used to provide the Software license; identifier of the certificate used to sign the Software license ticket header; the Software license ticket create date and time; the Software license ticket checksum; the Software license ticket version; the Software activation code version; format of the data in the request to Rightholder infrastructure; current license ticket ID; the Software component ID; the result of the Software action; error code; accessed address of the web service (URL, IP); port number; web address of the source of the web service request (referrer); public key of the certificate; digital certificate thumbprint of the scanned object and hashing algorithm.

If the **I agree to use Kaspersky Security Network** and **Enable extended KSN mode** checkboxes are selected, Kaspersky Endpoint Security provides to Kaspersky the following data:

- Information about the version of the operating system (OS) and service packs installed on the computer, version and checksums (MD5, SHA2-256, SHA1) of the OS kernel file, parameters of the OS run mode; OS version, OS build number, OS update number, OS edition, extended information about the OS edition; OS Service Pack version; date and time of the OS launch; processing delay time of the event about OS action in the behavioral analysis subsystem; number of delayed OS action events of the current type; processing delay time of the event about OS action in the proactive defense subsystem; number of processed OS action events; number of processed synchronous OS action events; total delay of all OS action events of the current type; processing delay time of the event about OS action in the persistent event storage subsystem; total delay of all OS action events; number of waiting synchronous OS action events; date and time of received event of an action in the OS.

- Information about the failed last OS reboot: number of failed reboots.

- Information about the Rightholder's installed application and the anti-virus protection status: Software installation ID (PCID); Software database record version; unique identifier of the instance of application installation on the computer, application type, ID of application type, the full version of the application installed, the identifier of the application settings version, the identifier of the computer type, the unique identifier of the computer on which the application is installed, the unique User identifier in the Rightholder's services, locale language and operation state, version of the installed Software components and their operation state, version of the protocol used to connect with the Rightholder's services; full version of installed Software; type of installed Software; Software update ID; ID of reputation service; protocol type ID; ID of a regional activation center; version of list of revoked Software service's decisions; ID of the triggered record in the Software's anti-virus databases; timestamp of the triggered record in the Software's anti-virus databases; type of the triggered record in the Software's anti-virus databases; Unique ID of the instance of application installation on the computer; license activation date; license expiration date; license identifier; status of the license used by the Software; checksum type for the object being processed; name of the detected malware or legitimate software that can be used to damage the user's device or data; checksum of the object being processed; checksum of the Software activation code; full version of the Software; Software ID; checksum of the Software key file; ID of the information model used to provide the Software license; identifier of the certificate used to sign the Software license ticket header; the Software license ticket create date and time; the Software license ticket checksum; the Software license ticket version; the Software activation code version; format of the data in the request to Rightholder infrastructure; current license ticket ID; the Software component ID; the result of the Software action; error code; accessed address of the web service (URL, IP); port number; web address of the source of the web service request (referrer); number of update-apply cycles for anti-virus databases; date and time when the anti-virus databases were last updated and applied; release date and time of the Software's databases; version of the Software's component; Software update ID; type of the installed Software; date and time of System Watcher start; installation date and time for the Software; probability of sending statistics by System Watcher; code of the event that took longer than the standard time to process by System Watcher; database processing time of the event that took longer than the standard time to process by System Watcher; maximum allowed time for processing an event by System Watcher; processing time of the event that took longer than the standard time to process by System Watcher; total number of events that took longer than the standard time to process by System Watcher.

- Information about all processed objects and operations: Software verdict on the object being processed; directory code; size of the object being processed; checksum (SHA256) of the object being processed; number of the detected software in the System Watcher context; date and time of detecting software by System Watcher; detect characteristics; ID of the triggered record in the Software's anti-virus databases; reason of detecting software by System Watcher; checksum (MD5) of the object being processed; result of the module integrity check; name of the object being processed; type of the triggered Software anti-virus databases record; path to the object being processed; the name of the scanned object; the date and time of the scan; the URL- and Referrer addresses from which it was downloaded; the size of scanned files and the paths to them; the archive sign; the date and time of the file's creation; the name, size and checksums (MD5, SHA2-256) of the packer (if the file was packed); the file's entropy; the file's type; the file type code; the executable file sign, ID and format; the object's checksum (MD5, SHA2-256); the type and value of the object's supplementary checksum; data about the object's digital signature (certificate): data on the certificate's publisher, number of starts of the object since the last statistics delivery, ID of the application's scanning task, the means of receiving information about the object's reputation, the value of the target filter, technical parameters of the applicable detection technologies; path to the object being processed; directory code.

- For executable files: the entropy of the file sections, reputation verification flag or file signature flag, name, type, ID type, checksum (MD5) and the size of the application that was loaded by the object being validated, the application path and template paths, an attribute indicating presence in the Autorun list, date of entry, the list of attributes, name of the packer, information about the digital signature of the application: the publisher certificate, the name of the uploaded file in the MIME format, file build date and time.

- Information about the applications launched and their modules: checksums (MD5, SHA2-256) of running files, size, attributes, creation date, name of the packer (if the file was packed), names of files, information about processes running on the system (process ID (PID), process name, information about the account the process was started from, the application and command that started the process, the full path to the process's files, and the starting command line, a description of the application that the process belongs to (the name of the application and information about the publisher), as well as the digital certificates being used and information needed to verify their authenticity or information about the absence of a file's digital signature), and information about the modules loaded into the processes: their names, sizes, types, creation dates, attributes, checksums (MD5, SHA2-256, SHA1), the paths to them, PE-file header information, names of packers (if the file was packed), information about the availability and validity of these statistics, identifier of the mode for generating the statistics being sent.

- If threats or vulnerabilities are detected, in addition to information about the detected object, information is provided about the identifier, version, and type of the record in the anti-virus database, the name of the threat based on the Kaspersky classification, the date and time of the last update of the anti-virus database, executable file name, the checksum (MD5) of the application file that requested the URL where the threat was detected, the IP address (IPv4 or IPv6) of the detected threat, the vulnerability identifier and its threat level, the URL and Referrer of the web page where the vulnerability was detected.

- If a potentially malicious object is detected, information is provided about data in the processes' memory.

- Network attack information: IP address of the attacking computer and number of the port on the user's computer targeted by the network attack, ID of the attack protocol, name and type of attack.

- Information about network connections: version and checksums (MD5, SHA2-256, SHA1) of the file from which process was started that opened the port, the path to the process's file and its digital signature, local and remote IP addresses, numbers of local and remote connection ports, connection state, timestamp of the port's opening.

- The URL and IP address of the web page where harmful or suspicious content was detected, the name, size, and checksum of the file that requested the URL, the identifier, weight and degree of the rule used to reach a verdict, the objective of the attack.

- Information about updates of the installed application and anti-virus databases: status of completion of the update task, type of error that may have occurred during the update process, the number of unsuccessful updates, the identifier of the application component that performs updates.

- Information about the use of Kaspersky Security Network (KSN): KSN identifier, application identifier, full version of the application, depersonalized IP address of the user's device, indicators of the quality of fulfillment of KSN requests, indicators of the quality of the processing of KSN packets, indicators of the number of KSN requests and information about the types of KSN requests, date and time when statistics began being sent, date and time when statistics finished being sent, information about KSN configuration updates: identifier of the active configuration, identifier of the configuration received, error code of the configuration update.

- Information about system log events: event time, name of the log where the event has been detected, type and category of event, name of the event source and event description.

- Information to determine the reputation of files and URL-addresses: the URL-address at which the reputation is being requested and the Referrer, the connection's protocol type, the internal identifier of the application type, the number of the port being used, the User identifier, checksum of the scanned file (MD5), type of the detected threat, information about the record used to detect a threat (record identifier for the anti-virus databases, the record timestamp and type); public key of the certificate; digital certificate thumbprint of the scanned object and hashing algorithm.

- Data on the application territorial distribution: date of the application installation and activation, ID of the partner providing the license for the application activation, application ID, application language localization ID, license serial number for the application activation, KSN participation sign.

- Information about the license used: the type and validity period of the license, number of days till license expiration, identifier of the partner from whom the license was purchased, Regional Activation Center identifier, checksum of the activation code, ticket body hash calculated using the SHA1 algorithm, license ticket creation date and time, license information identifier, license ticket identifier, license ticket sequence identifier, unique identifier of the user's computer, date from which the license ticket is valid, date to which the license ticket is valid, license ticket current state, ticket header version, license version, ticket header signature certificate identifier, checksum of the key file, ticket header signer serial number, authentication token.

- Information about hardware installed on the computer: type, name, model name, firmware version, parameters of built-in and connected devices.

- Information about the device: device ID.

- Information about the operation of the Web Control component: component version, categorization reason, additional information about categorization reason, categorized URL, host IP address of blocked/categorized object.

When Private KSN infrastructure is used by Kaspersky Security Center and you choose to participate in Kaspersky Security Network in policy settings, Kaspersky Endpoint Security doesn't send statistics from client computers to which the policy is applied to Kaspersky.

After a policy is deleted or made inactive, KSN settings on a client computer return to the initial state.

Step 9. Configure user interaction settings

In the **User Interaction** window, configure the Kaspersky Endpoint Security settings for interaction with the user of the client computer if necessary.

Step 10. Configure network connection settings

In the **Network** window, do the following if necessary:

- Configure the connection to a proxy server.

- Enable or disable scanning of inbound and outbound HTTPS traffic.

- Select the certificate storage for checking encrypted HTTPS traffic in the Mozilla Firefox browser.
- Manage the list of trusted root certificates.
- Configure monitored ports.

  You can create a list of ports that are monitored by Kaspersky Endpoint Security.

Step 11. Configure Reports and Backup settings

In the **Reports and Backup** window, do the following if necessary:

- Configure settings for generating and storing reports.
- Configure settings for storing objects in Backup.

Step 12. Configure FileVault Disk Encryption

In the **FileVault Disk Encryption** window, do the following if necessary:

- Enable or disable FileVault disk encryption management for the user's startup disk.

  By default, FileVault disk encryption management is disabled.
- Choose the **Encrypt disk** option, if you want to encrypt the user's startup disk when the policy is applied to a client computer.

If the **Enable FileVault disk encryption management** checkbox is unselected, users with administrator rights can encrypt and decrypt their Mac startup disks from System Settings.

If the **Enable FileVault disk encryption management** checkbox and the **Encrypt disk** option are selected, users with administrator rights can't decrypt the startup disk of their Mac from System Settings.

If the **Enable FileVault disk encryption management** checkbox and the **Decrypt disk** option are selected, users with administrator rights can't encrypt the startup disk of their Mac from System Settings.

Step 13. Configure Web Control

In the **Web Control** window, do the following if necessary:

- Enable or disable Web Control.

  Note: If you enable Web Control to block access to dangerous web resources, Kaspersky Endpoint Security displays the **Web Control is enabled** notification in Protection Center on the remote computer. Kaspersky Endpoint Security displays notifications when the user accesses web resources blocked by Web Control on the remote computer if the **Check secure connections (HTTPS)** checkbox is selected in the **Network** window of the New policy wizard.
- Add a new rule for Web Control by clicking **Add**.

  You can enter a rule name, choose whether the rule is active, specify a rule area by creating a list of specific web addresses or selecting website categories, and select an action that Kaspersky Endpoint Security performs when a user accesses a website included in this rule.
- Edit, delete, or organize created rules in the list.

The order in which the rules are sorted determines the priority of their application by Kaspersky Endpoint Security.

Step 14. Configure Managed Detection and Response

In the **Managed Detection and Response** window, do the following if necessary:

- Enable or disable Managed Detection and Response.

  By default, Managed Detection and Response is disabled.

- Import or delete a configuration file for activating the Managed Detection and Response component on managed devices.

If the **Managed Detection and Response** checkbox is selected and the MDR configuration file is imported, the Managed Detection and Response component is active and interacts with the Kaspersky Managed Detection and Response service. This service constantly detects and eliminates security threats aimed at your organization.

Step 15. Configure Endpoint Detection and Response (KATA)

In the **Endpoint Detection and Response (KATA)** window, do the following if necessary:

- Enable or disable Endpoint Detection and Response (KATA).

  By default, Endpoint Detection and Response (KATA) is disabled.

- Configure server connection settings and add a TLS certificate.

- Add a KATA server.

If the **Endpoint Detection and Response (KATA)** checkbox is selected and a TLS certificate and a KATA server are added, the Endpoint Detection and Response (KATA) component is active and interacts with the Kaspersky Anti Targeted Attack Platform solution. This solution promptly detects advanced threats, such as targeted attacks, advanced persistent threats, zero-day attacks, and others.

Step 16. Configure External Disks Scan

In the **External Disks Scan** window, configure the following settings:

- The action that Kaspersky Endpoint Security performs when an external disk is connected.

- The action that Kaspersky Endpoint Security performs upon detecting a malicious object.

Step 17. Configure Behavior Detection

In the **Behavior Detection** window, do the following if necessary:

- Enable or disable Behavior Detection.

  By default, Behavior Detection is enabled.

- Select the action to be performed when malware activity is detected.

- Enable or disable protection of shared folders against external encryption.

  - Select the action to be performed when malware activity is detected.

Step 18. Configure Mail Threat Protection

In the **Mail Threat Protection** window, do the following if necessary:

- Enable or disable Mail Threat Protection.
  By default, Mail Threat Protection is enabled.
- Select the action to be performed upon detecting a malicious object.
- Configure Mail Threat Protection settings.

Step 19. Configure Exploit Prevention

In the **Exploit Prevention** window, do the following if necessary:

- Enable or disable Exploit Prevention.
  By default, Exploit Prevention is enabled.
- Select the action to be performed upon detecting an exploit.

Step 20. Configure Remediation Engine

In the **Remediation Engine** window, do the following if necessary:

- Enable or disable Remediation Engine.
  By default, Remediation Engine is enabled.

Step 21. Configure Device Control

In the **Device Control** window, do the following if necessary:

- Enable or disable Device Control.
  By default, Device Control is enabled.
- Configure Device Control settings.

Step 22. Configure Firewall

In the **Firewall** window, do the following if necessary:

- Enable or disable Firewall.
  By default, Firewall is enabled.
- Configure Firewall settings.

Step 23. Define the administration group to which the policy will be applied

In the **Target group** window, click **Browse** to select an administration group to which you want to apply the policy.

Step 24. Select the policy status and complete the creation of a policy

In the **Create the group policy for the application** window, do the following:

1. Select the status that will be assigned to the policy:

   - *Active policy*: the policy is applied to the selected administration group.
   - *Inactive policy:* the policy is not applied.
   - *Out-of-office policy:* the policy is applied to the selected administration group when the computers are disconnected from the corporate network.

   Note: You can create multiple policies for an application in an administration group, but only one of them can be active.

   For detailed information about policy statuses, see the Kaspersky Security Center Help.

2. Select the **Open policy properties immediately after it is created** checkbox if you want to review the policy settings after the policy is created.

3. Click **Finish** to close the New policy wizard.

   The policy that you have created appears on the **Policies** tab in the workspace of the relevant administration group. The policy is applied to client computers after their first synchronization with Administration Server.

You can edit the settings of the policy you have created. You can also prohibit or allow changes to each group of settings from a client computer using the and buttons for each group of settings. The button next to a group of settings signifies that the user of a client computer is not allowed to edit these settings on the user's computer. The button next to a group of settings signifies that the user of a client computer is allowed to edit these settings on the user's computer.

View the list of policies

You can create an unlimited number of various policies for applications installed on computers in each administration group, but only one policy can be applied to each application at a time within an administration group.

View the list of policies of an administration group

1. Start Kaspersky Security Center Administration Console.
2. Maximize the **Administration Server <Server name>** node.
3. In the console tree, click **Managed devices**.
4. Select the administration group that contains the required client computer.
5. In the workspace, select the **Policies** tab.

   The list of policies is displayed.

Configure policy settings

You can make changes to the policy that you created in Kaspersky Security Center and block any changes to its settings in the policies of subgroups and in task settings.

Kaspersky Endpoint Security policy settings include application settings and task settings.

Configure policy settings

1. Start Kaspersky Security Center Administration Console.
2. Maximize the **Administration Server <Server name>** node.
3. In the console tree, click **Managed devices**.
4. In the workspace, select the **Policies** tab.
5. Right-click the policy you want to configure and choose **Properties**.
6. In the **Properties: <Policy name>** window, configure the policy settings:

   - In the **Essential Threat Protection** section

     Configure the following File Threat Protection settings

     - Enable or disable File Threat Protection.
     - Select one of the preset security levels or configure security settings manually.
     - Select the action to be performed upon detecting a malicious object.

     Configure the following Web Threat Protection settings

     - Enable or disable Web Threat Protection.
     - Select one of the preset security levels or configure security settings manually.
     - Enable or disable checking of web addresses against the database of malicious web addresses.
     - Configure the Anti-Phishing settings.
     - Add trusted addresses whose traffic will not be scanned by Web Threat Protection.
     - Select the action to be performed upon detecting a malicious object in web traffic.

     Configure the following Mail Threat Protection settings

     - Enable or disable Mail Threat Protection.
     - Select the action to be performed upon detecting a malicious object.
     - Configure Mail Threat Protection settings.

Configure the following Network Threat Protection settings

- Enable or disable Network Threat Protection.
- Configure the Network Threat Protection settings.
- Specify the IP addresses of computers whose network activity will not be blocked.

Configure the following Firewall settings

- Enable or disable Firewall.
- Configure Firewall settings.

- In the **Advanced Threat Protection** section

  Configure the following KSN settings

  - Read the full text of the Kaspersky Security Network Statement by clicking **KSN Statement**.
  - Enable or disable the use of Kaspersky Security Network.
  - Enable or disable extended KSN mode.
  - Enable or disable Cloud mode.
  - Enable or disable the use of a KSN proxy.
  - Enable or disable the use of Kaspersky servers when the KSN proxy is unavailable.

  > **Note:** Use of Kaspersky Security Network and a KSN proxy on remote computers is available only if Kaspersky Security Center Administration Server is used as the proxy server. For detailed information about Administration Server properties, see the Kaspersky Security Center Help.

  Configure the following Behavior Detection settings

  - Enable or disable Behavior Detection.

    By default, Behavior Detection is enabled.
  - Select the action to be performed when malware activity is detected.

  Configure the following Exploit Prevention settings

  - Enable or disable Exploit Prevention.
  - Select the action to be performed upon detecting an exploit.

  Configure the following Remediation Engine settings

  Enable or disable Remediation Engine.

- In the **Security Controls** section

Configure the following Device Control settings

- Enable or disable Device Control.
- Configure Device Control settings.

Configure the following Web Control settings

- Enable or disable Web Control.
- Add a new rule for Web Control by clicking **Add**.
- Edit, delete, or organize created rules in the list.

- In the **Data Encryption** section

  Configure the following FileVault disk encryption settings

  - Enable or disable FileVault disk encryption management for client computers.
  - Encrypt or decrypt the startup disk on client computers.

    If the **Enable FileVault disk encryption management** checkbox is unselected, users with administrator rights can encrypt and decrypt their Mac startup disks from System Settings.

    If the **Enable FileVault disk encryption management** checkbox and the **Encrypt disk** option are selected, users with administrator rights can't decrypt the startup disk of their Mac from System Settings.

    If the **Enable FileVault disk encryption management** checkbox and the **Decrypt disk** option are selected, users with administrator rights can't encrypt the startup disk of their Mac from System Settings.

- In the **Detection and Response** section

  Configure the following Managed Detection and Response settings

  - Enable or disable Managed Detection and Response.
  - Import or delete a configuration file which is used to activate the Managed Detection and Response component on managed devices.

  Configure the following Endpoint Detection and Response (KATA) settings

  - Enable or disable Endpoint Detection and Response (KATA).
  - Configure server connection settings and add a TLS certificate.
  - Add a KATA server.

- In the **Local Tasks** section

  Configure the following External Disks Scan settings

  - The action that Kaspersky Endpoint Security performs when an external disk is connected.
  - The action that Kaspersky Endpoint Security performs upon detecting a malicious object.

- In the **Update** section

Configure the following Update settings

- Enable or disable updating application modules.
- Specify update sources.

- In the **Additional settings** section
  Configure the following protection settings
  - Enable or disable real-time protection of the client computer.
  - Enable or disable the start of Kaspersky Endpoint Security when the client computer starts.
  - Configure Trusted zone.
  - Configure Trusted applications.
  - Select types of objects to be detected.
  - Disable or enable the start of scheduled tasks when the computer is running on battery power.

  Configure the following network settings
  - Enable or disable the use of a proxy server.
  - Specify the proxy server address.
  - Enable or disable the use of a proxy server for local addresses.
  - Specify the user name and password for proxy server authentication.
  - Enable or disable scanning of inbound and outbound HTTPS traffic.
  - Select the certificate store for checking encrypted HTTPS traffic in the Mozilla Firefox browser.
  - Configure monitored ports.

  Configure the following Reports and Backup settings
  - Enable or disable saving of non-critical events in the report.
  - Enable or disable saving of recent events only.
  - Enable or disable removal of events after the specified period.
  - Specify the period for storing events.
  - Enable or disable removal of objects from Backup after the specified period.
  - Specify the period for storing objects in Backup.

Configure the following user interaction settings

- Enable or disable event notifications.
- Select how Kaspersky Endpoint Security will notify the user about events.
- Enable or disable displaying the Kaspersky Endpoint Security icon in the menu bar.
- Configure whether a user can open the Kaspersky Endpoint Security main window and use the application interface on the client computer.
- Enable or disable availability of the **Quit** item in the shortcut menu of the Kaspersky Endpoint Security icon on the client computer.
- Select the language used to display Kaspersky Security Center events.
- Configure the Kaspersky Endpoint Security settings available to users of the client computer.
- Configure Password protection to limit unwanted actions on users' devices.

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

Change the policy status

A policy status defines the operation of a policy. The policy can have active, out-of-office, or inactive status. You can change the policy status in policy settings.

Change the policy status

1. Start Kaspersky Security Center Administration Console.
2. Maximize the **Administration Server <Server name>** node.
3. In the console tree, click **Managed devices**.
4. Select the administration group that contains the required client computer.
5. In the workspace, select the **Policies** tab.
6. Right-click the policy whose state you want to change and choose **Properties** from the context menu.
7. In the **Properties: <Policy name>** window, select the **General** section.
8. In the **Policy status** section, select one of the following policy statuses:
   - **Active policy**. The policy is always applied to the selected administration group.
   - **Out-of-office policy**. The policy is applied to the selected administration group when client computers are disconnected from the corporate network.
   - **Inactive policy**. The policy is not applied to the selected administration group.
9. Click **OK** to save changes and close the **Properties: <Policy name>** window.

Export a policy to a KLP file

You can export a custom policy to a file to use the policy on another Administration Server.

Export a policy to a KLP file

1. Start Kaspersky Security Center Administration Console.
2. Maximize the **Administration Server <Server name>** node.
3. In the console tree, click **Managed devices**.
4. Select the administration group that contains the required client computer.
5. In the workspace, select the **Policies** tab.
6. Right-click the policy to display its context menu and choose **Export**.
   The **Save As** window opens.
7. Select the folder in which you want to save the KLP file for the policy.
8. Specify the file name.
9. Click **Save** to save the file in the selected folder.

Import a policy from a KLP file

You can import an existing policy with predefined settings from a file.

Import a policy from a KLP file

1. Start Kaspersky Security Center Administration Console.
2. Maximize the **Administration Server <Server name>** node.
3. In the console tree, click **Managed devices**.
4. Select the administration group that contains the required client computer.
5. In the workspace, select the **Policies** tab.
6. Open the file selection window in one of the following ways:
   - By clicking the **Import policy from file** button.
   - By right-clicking an empty area in the workspace to open the context menu and selecting the **Import** item.
7. Select a KLP file with a policy and click **Open**.

The imported policy is added to the list of policies in the workspace.

Create and manage policy profiles

A policy profile is a named set of variable settings for a policy, which is activated on a client computer when specific conditions are met. Activation of a profile modifies the policy settings in effect on the device when the policy profile is activated.

Create a policy profile

1. In the console tree, select the administration group for which you want to create a policy profile.
2. In the workspace, select the **Policies** tab.
3. Do one of the following to open the properties of the policy for which you want to create a profile:
   - Double-click the name of the policy.
   - Right-click the policy name to display the context menu and choose **Properties**.
   - Click the **Configure policy** link.
4. In the **Properties: <Policy name>** window, select the **Policy profiles** section.
5. In the workspace, click **Add**.
6. In the **Assigning policy profiles** window, read the information about policies and click **Next**.

   If you don't want to display this window when you create new policy profiles, select the **Do not show this window again** checkbox before clicking **Next**.
7. In the **Policy profile name** window, do the following to configure the policy profile:
   - Enter the name of the new policy profile.

     > **Note:** The name of a profile cannot include more than 100 characters.

   - In the **Policy profile state** section, select whether the policy profile is enabled or disabled.
   - In the drop-down list in the **Policy profile state** section, select whether the policy profile can be edited.
   - If you want to configure activation rules for the policy profile, select the **After closing the New policy profile wizard, proceed to configuring the policy profile activation rule** checkbox.
8. Click **Finish**.
9. If you have selected the **After closing the New policy profile wizard, proceed to configuring the policy profile activation rule** checkbox, proceed with the steps of the New Policy Profile Activation Rule Wizard.

The policy profile that you created appears in the **Policy profiles** section of the **Properties: <Policy name>** window.

Create a policy profile activation rule

1. In the console tree, select the administration group in which you want to create a policy profile activation rule.
2. In the workspace, select the **Policies** tab.
3. Do one of the following to open the properties of the policy:
   - Double-click the name of the policy.
   - Right-click the policy name to display the context menu and choose **Properties**.
   - Click the **Configure policy** link.
4. In the **Properties: <Policy name>** window, select the **Policy profiles** section.
5. In the workspace, select the policy profile for which you want to create an activation rule and click **Properties**.
   The **Properties: <Policy profile name>** window opens.
6. Select the **Activation rules** section.
7. In the workspace, click **Add**.
   The New policy profile activation rule wizard starts.

Follow the steps of the New policy profile activation rule wizard.

Modify a policy profile

1. In the console tree, select the administration group for which you want to modify a policy profile.
2. In the workspace, select the **Policies** tab.
3. Do one of the following to open the properties of the policy for which you want to modify a profile:
   - Double-click the name of the policy.
   - Right-click the policy name to display the context menu and choose **Properties**.
   - Click the **Configure policy** link.
4. In the **Properties: <Policy name>** window, select the **Policy profiles** section.
5. In the workspace, select the policy profile that you want to modify and click **Properties**.
   The **Properties: <Policy profile name>** window opens.
6. Configure the profile if necessary:
   - In the **General** section, rename the profile or enable/disable the profile by selecting/deselecting the **Enable profile** checkbox.
   - In the **Activation rules** section, create, edit, or delete the activation rules.

- In the **Devices** section, choose the devices to which the policy profile is applied.
- Edit the policy settings in the relevant sections.

7. Click **OK**.

If the policy profile is active, the modified settings will be applied after the client computer is synchronized with Administration Server. If the policy profile is inactive, they will be applied after the activation rule is triggered.

Change the priority of a policy profile

1. In the console tree, select the administration group for which you want to change the priority of a policy profile.
2. In the workspace, select the **Policies** tab.
3. Do one of the following to open the properties of the policy for which you want to change the priority of a policy profile:
   - Double-click the name of the policy.
   - Right-click the policy name to display the context menu and choose **Properties**.
   - Click the **Configure policy** link.
4. In the **Properties: <Policy name>** window, select the **Policy profiles** section.
5. In the workspace, select the policy profile whose priority you want to change.
6. Raise/lower the priority of the selected profile by clicking the  buttons.

Delete a policy profile

1. In the console tree, select the administration group for which you want to delete a policy profile.
2. In the workspace, select the **Policies** tab.
3. Do one of the following to open the properties of the policy for which you want to delete a profile:
   - Double-click the name of the policy.
   - Right-click the policy name to display the context menu and choose **Properties**.
   - Click the **Configure policy** link.
4. In the **Properties: <Policy name>** window, select the **Policy profiles** section.
5. In the workspace, select the profile that you want to delete and click **Delete**.

For detailed information about policy profiles, see the Kaspersky Security Center Help.

Generate a report on detected objects

Generate a report on detected objects

1. Start Kaspersky Security Center Administration Console.
2. Maximize the **Administration Server <Server name>** node.
3. In the console tree, click **Managed devices**.
4. Select the administration group that contains the required client computer.
5. Select the **Devices** tab.
6. Select the computer from the list of client computers.
7. Right-click the selected computer to open the context menu and choose **All tasks** > **View report on threats**.

   The generated report opens in a browser window.

You can find information about other ways to generate a report on objects detected by the application on the client computer in the Kaspersky Security Center Help.

Get a recovery key for an encrypted disk

If a user of a client computer forgets or loses his or her credentials and cannot access an encrypted disk, you can get a recovery key.

Get a recovery key

1. Start Kaspersky Security Center Administration Console.
2. Maximize the **Administration Server <Server name>** node.
3. In the console tree, select the **Advanced** folder, then **Data encryption and protection** subfolder, and then the **Encrypted drives** subfolder.
4. In the workspace, right-click the device with the encrypted disk to display the shortcut menu and select **Get recovery key for macOS**.

   A window with the recovery key opens.
5. Save the recovery key in any convenient way.

You can use this recovery key on a client computer to access the encrypted disk.

Remote administration of the application via Kaspersky Security Center Web Console and Cloud Console

Kaspersky Security Center Web Console (Web Console) is a web application intended to provide a centralized way to perform the main tasks related to managing and maintaining an organization's network security. Web Console is a Kaspersky Security Center component that provides a user interface for managing Kaspersky Endpoint Security in a browser window. For detailed information about Kaspersky Security Center Web Console, see the Kaspersky Security Center Help.

Kaspersky Security Center Cloud Console (Cloud Console) is a cloud-based solution for protecting and managing an organization's network. For detailed information about Kaspersky Security Center Cloud Console, see the Kaspersky Security Center Cloud Console Help.

You can also manage Kaspersky Endpoint Security via the application's graphical user interface, Kaspersky Security Center Administration Console, and the command line.

Install the Kaspersky Endpoint Security web plug-in

The Kaspersky Endpoint Security web plug-in enables interaction between Kaspersky Endpoint Security and Kaspersky Security Center. The web plug-in must be installed on a device that has Kaspersky Security Center Web Console installed. The functionality of the web plug-in is available to all administrators who have access to the Kaspersky Security Center Web Console in a browser.

You can install the web plug-in as follows:

- Using Quick Start Wizard of Kaspersky Security Center Web Console.

  Web Console automatically prompts you to run the Quick Start Wizard when connecting Web Console to the Administration Server for the first time. You can also run the Quick Start Wizard in the Web Console interface (**Discovery & Deployment** → **Deployment & Assignment** → **Quick Start Wizard**). The Quick Start Wizard can also check if the installed web plug-ins are up to date and download the necessary updates. For more details on the Quick Start Wizard for Kaspersky Security Center Web Console, please refer to the Kaspersky Security Center Help.

- Manually, using a distribution package to the Web Console from an external source.

  To install the web plug-in, add the ZIP-archive of the distribution package for the Kaspersky Endpoint Security web plug-in in the Web Console interface: **Console settings** > **Web plug-ins**. The distribution package of the web plug-in can be downloaded on the Kaspersky website.

To install the Kaspersky Endpoint Security web plug-in manually:

1. In the main window of the Kaspersky Security Center Web Console, select **Console settings** > **Web plug-ins**.

   A list of installed web plug-ins opens.

2. Start the installation of the Kaspersky Endpoint Security web plug-in by one of the following ways:

   - Installation from the list of Kaspersky web plug-ins:

     a. Click **Add**.

        A list of all available Kaspersky Web plug-ins opens. The list is updated automatically after new versions of web plug-ins are released.

     b. Find the Kaspersky Endpoint Security for Mac 12.2 web plug-in in the list and click its name.

     c. In the window that opens with a description of the web plug-in, click the **Install plug-in** button.

     d. Wait for the installation to complete and click **OK** in the information window.

   - Installation of the web plug-in from an external source (the archives required for installing the web plug-ins are included in the distribution kit):

     a. Click the **Add from file** button.

     b. In the window that opens, specify the path to the ZIP archive with the distribution kit for the web plug-in and the path to the signature file in TXT format. This file is in the archive with the web plug-in.

     c. Click **Add**.

     d. Wait for the installation to complete and click **OK** in the information window.

The new plug-in is displayed in the list of installed web plug-ins (**Console Settings** > **Web Plug-ins**).

Note: If you select a language that is not included in Kaspersky Endpoint Security distribution package in the properties of Kaspersky Security Center Administration Server, the License Agreement and the entire Kaspersky Security Center Web Console interface will be displayed in English.

Create policies

This section contains information on how to create and configure policies for Kaspersky Endpoint Security using Kaspersky Security Center Web Console and Cloud Console.

A policy determines an application's settings and manages the ability to configure that application on computers within an administration group. An individual policy must be created for each application. You can create multiple policies for applications installed on computers in each administration group, but only one policy can be applied at a time to each application within an administration group.

Note: When creating and configuring a policy, you can allow or prohibit changes to any group of settings in policies using the **Enforce** toggle switch.

Create a policy

1. In the **Devices** section on the left, select the **Policies & profiles** section.

2. Click **Add**.

3. Select the application for which you want to create a policy and click **Next**.

   The **New policy** window opens.

4. On the **General** tab, specify the policy name and configure the policy status and the policy settings inheritance options.

5. On the **Application settings** tab, configure the application settings that will be applied to Kaspersky Endpoint Security on the client computer when the policy is enforced.

6. Click **Save**.

You can perform the following actions on custom policies:

- Create policies.
- Configure policies.
- Copy or move policies from one group to another.
- Delete policies.
- Change the status of policies.

For detailed information about Kaspersky Security Center Web Console policies, see the Kaspersky Security Center Help.

For detailed information about Kaspersky Security Center Cloud Console policies, see the Kaspersky Security Center Cloud Console Help.

Note: After you create a policy profile for a Kaspersky Endpoint Security policy using Kaspersky Security Center Web Console and Cloud Console, you need to check that the settings are applied correctly on client computers.

Configure Advanced Threat Protection settings

In the **Advanced Threat Protection** section, you can choose whether Kaspersky Endpoint Security on client computers participates in Kaspersky Security Network and configure the use of KSN proxy.

Do the following if necessary:

- Read the full text of the Kaspersky Security Network Statement by clicking the **KSN Statement** link.
- View information about KSN infrastructure provided by Kaspersky Security Center by clicking the **KSN Statement** link.

Note: Global KSN infrastructure is used in Kaspersky Security Center by default. If you manage Kaspersky Endpoint Security via Kaspersky Security Center Web Console and depending on Kaspersky Security Center settings, you can participate in Kaspersky Private Security Network instead of Kaspersky Security Network. If you manage Kaspersky Endpoint Security via Kaspersky Security Center Cloud Console, participation in Kaspersky Private Security Network is unavailable. For detailed information about participating in Kaspersky Private Security Network, see the Kaspersky Security Center Help.

- Turn on/off the use of Kaspersky Security Network.
- Turn on/off extended KSN mode.
- Turn on/off Cloud mode.
- Enable or disable the use of a KSN proxy.
- Enable or disable the use of Kaspersky servers when the KSN proxy is unavailable.

Note: If you manage Kaspersky Endpoint Security via Kaspersky Security Center Web Console, use of Kaspersky Security Network and a KSN proxy on remote computers is available only if Kaspersky Security Center Administration Server is used as the proxy server. For detailed information about Administration Server properties, see the Kaspersky Security Center Help.
If you manage Kaspersky Endpoint Security via Kaspersky Security Center Cloud Console, you can use Kaspersky Security Network and a KSN proxy on remote computers through distribution points running a Windows operating system.

When Global KSN infrastructure is used by Kaspersky Security Center and you choose to participate in Kaspersky Security Network in policy settings, Kaspersky Endpoint Security statistics from client computers to which the policy is applied are automatically sent to Kaspersky to enhance protection of these computers.

Note: Kaspersky doesn't receive, process, or store any personal data without your explicit consent.

Data provided to Kaspersky when using Kaspersky Security Network in Global KSN infrastructure

If the **Kaspersky Security Network** toggle switch is enabled and the **Extended KSN mode** toggle switch is disabled, Kaspersky Endpoint Security running on client computers provides to Kaspersky the following data:

- Information about the license used: the type and validity period of the license, number of days till license expiration, identifier of the partner from whom the license was purchased, Regional Activation Center identifier, checksum of the activation code, ticket body hash calculated using the SHA1 algorithm, license ticket creation date and time, license information identifier, license ticket identifier, license ticket sequence identifier, unique identifier of the user's computer, date from which the license ticket is valid, date to which the license ticket is valid, license ticket current state, ticket header version, license version, ticket header signature certificate identifier, checksum of the key file, ticket header signer serial number, authentication token.
- Full version of installed Software; type of installed Software; Software update ID; ID of reputation service; protocol type ID; ID of a regional activation center; version of list of revoked Software service's decisions; ID of the triggered record in the Software's anti-virus databases; timestamp of the triggered record in the Software's anti-virus databases; type of the triggered record in the Software's anti-virus databases; unique ID of the instance of application installation on the computer; license activation date; license expiration date; license identifier; status of the license used by the Software; checksum type for the object being processed; name of the detected malware or legitimate software that can be used to damage the user's device or data; checksum of the object being processed; checksum of the Software activation code; full version of the Software; unique device ID; Software ID; checksum of the Software key file; ID of the information model used to provide the Software license; identifier of the certificate used to sign the Software license ticket header; the Software license ticket create date and time; the Software license ticket checksum; the Software license ticket version; the Software activation code version; format of the data in the request to Rightholder infrastructure; current license ticket ID; the Software component ID; the result of the Software action; error code; accessed address of the web service (URL, IP); port number; web address of the source of the web service request (referrer); public key of the certificate; digital certificate thumbprint of the scanned object and hashing algorithm.

If the **Kaspersky Security Network** and **Extended KSN mode** toggle switches are enabled, Kaspersky Endpoint Security running on client computers provides to Kaspersky the following data:

- Information about the version of the operating system (OS) and service packs installed on the computer, version and checksums (MD5, SHA2-256, SHA1) of the OS kernel file, parameters of the OS run mode; OS version, OS build number, OS update number, OS edition, extended information about the OS edition; OS Service Pack version; date and time of the OS launch; processing delay time of the event about OS action in the behavioral analysis subsystem; number of delayed OS action events of the current type; processing delay time of the event about OS action in the proactive defense subsystem; number of processed OS action events; number of processed synchronous OS action events; total delay of all OS action events of the current type; processing delay time of the event about OS action in the persistent event storage subsystem; total delay of all OS action events; number of waiting synchronous OS action events; date and time of received event of an action in the OS.

- Information about the failed last OS reboot: number of failed reboots.

- Information about the Rightholder's installed application and the anti-virus protection status: Software installation ID (PCID); Software database record version; unique identifier of the instance of application installation on the computer, application type, ID of application type, the full version of the application installed, the identifier of the application settings version, the identifier of the computer type, the unique identifier of the computer on which the application is installed, the unique User identifier in the Rightholder's services, locale language and operation state, version of the installed Software components and their operation state, version of the protocol used to connect with the Rightholder's services; full version of installed Software; type of installed Software; Software update ID; ID of reputation service; protocol type ID; ID of a regional activation center; version of list of revoked Software service's decisions; ID of the triggered record in the Software's anti-virus databases; timestamp of the triggered record in the Software's anti-virus databases; type of the triggered record in the Software's anti-virus databases; Unique ID of the instance of application installation on the computer; license activation date; license expiration date; license identifier; status of the license used by the Software; checksum type for the object being processed; name of the detected malware or legitimate software that can be used to damage the user's device or data; checksum of the object being processed; checksum of the Software activation code; full version of the Software; Software ID; checksum of the Software key file; ID of the information model used to provide the Software license; identifier of the certificate used to sign the Software license ticket header; the Software license ticket create date and time; the Software license ticket checksum; the Software license ticket version; the Software activation code version; format of the data in the request to Rightholder infrastructure; current license ticket ID; the Software component ID; the result of the Software action; error code; accessed address of the web service (URL, IP); port number; web address of the source of the web service request (referrer); number of update-apply cycles for anti-virus databases; date and time when the anti-virus databases were last updated and applied; release date and time of the Software's databases; version of the Software's component; Software update ID; type of the installed Software; date and time of System Watcher start; installation date and time for the Software; probability of sending statistics by System Watcher; code of the event that took longer than the standard time to process by System Watcher; database processing time of the event that took longer than the standard time to process by System Watcher; maximum allowed time for processing an event by System Watcher; processing time of the event that took longer than the standard time to process by System Watcher; total number of events that took longer than the standard time to process by System Watcher.

- Information about all processed objects and operations: Software verdict on the object being processed; directory code; size of the object being processed; checksum (SHA256) of the object being processed; number of the detected software in the System Watcher context; date and time of detecting software by System Watcher; detect characteristics; ID of the triggered record in the Software's anti-virus databases; reason of detecting software by System Watcher; checksum (MD5) of the object being processed; result of the module integrity check; name of the object being processed; type of the triggered Software anti-virus databases record; path to the object being processed; the name of the scanned object; the date and time of the scan; the URL- and Referrer addresses from which it was downloaded; the size of scanned files and the paths to them; the archive sign; the date and time of the file's creation; the name, size and checksums (MD5, SHA2-256) of the packer (if the file was packed); the file's entropy; the file's type; the file type code; the executable file sign, ID and format; the object's checksum (MD5, SHA2-256); the type and value of the object's supplementary checksum; data about the object's digital signature (certificate): data on the certificate's publisher, number of starts of the object since the last statistics delivery, ID of the application's scanning task, the means of receiving information about the object's reputation, the value of the target filter, technical parameters of the applicable detection technologies; path to the object being processed; directory code.

- For executable files: the entropy of the file sections, reputation verification flag or file signature flag, name, type, ID type, checksum (MD5) and the size of the application that was loaded by the object being validated, the application path and template paths, an attribute indicating presence in the Autorun list, date of entry, the list of attributes, name of the packer, information about the digital signature of the application: the publisher certificate, the name of the uploaded file in the MIME format, file build date and time.

- Information about the applications launched and their modules: checksums (MD5, SHA2-256) of running files, size, attributes, creation date, name of the packer (if the file was packed), names of files, information about processes running on the system (process ID (PID), process name, information about the account the process was started from, the application and command that started the process, the full path to the process's files, and the starting command line, a description of the application that the process belongs to (the name of the application and information about the publisher), as well as the digital certificates being used and information needed to verify their authenticity or information about the absence of a file's digital signature), and information about the modules loaded into the processes: their names, sizes, types, creation dates, attributes, checksums (MD5, SHA2-256, SHA1), the paths to them, PE-file header information, names of packers (if the file was packed), information about the availability and validity of these statistics, identifier of the mode for generating the statistics being sent.

- If threats or vulnerabilities are detected, in addition to information about the detected object, information is provided about the identifier, version, and type of the record in the anti-virus database, the name of the threat based on the Kaspersky classification, the date and time of the last update of the anti-virus database, executable file name, the checksum (MD5) of the application file that requested the URL where the threat was detected, the IP address (IPv4 or IPv6) of the detected threat, the vulnerability identifier and its threat level, the URL and Referrer of the web page where the vulnerability was detected.

- If a potentially malicious object is detected, information is provided about data in the processes' memory.

- Network attack information: IP address of the attacking computer and number of the port on the user's computer targeted by the network attack, ID of the attack protocol, name and type of attack.

- Information about network connections: version and checksums (MD5, SHA2-256, SHA1) of the file from which process was started that opened the port, the path to the process's file and its digital signature, local and remote IP addresses, numbers of local and remote connection ports, connection state, timestamp of the port's opening.

- The URL and IP address of the web page where harmful or suspicious content was detected, the name, size, and checksum of the file that requested the URL, the identifier, weight and degree of the rule used to reach a verdict, the objective of the attack.

- Information about updates of the installed application and anti-virus databases: status of completion of the update task, type of error that may have occurred during the update process, the number of unsuccessful updates, the identifier of the application component that performs updates.

- Information about the use of Kaspersky Security Network (KSN): KSN identifier, application identifier, full version of the application, depersonalized IP address of the user's device, indicators of the quality of fulfillment of KSN requests, indicators of the quality of the processing of KSN packets, indicators of the number of KSN requests and information about the types of KSN requests, date and time when statistics began being sent, date and time when statistics finished being sent, information about KSN configuration updates: identifier of the active configuration, identifier of the configuration received, error code of the configuration update.

- Information about system log events: event time, name of the log where the event has been detected, type and category of event, name of the event source and event description.

- Information to determine the reputation of files and URL-addresses: the URL-address at which the reputation is being requested and the Referrer, the connection's protocol type, the internal identifier of the application type, the number of the port being used, the User identifier, checksum of the scanned file (MD5), type of the detected threat, information about the record used to detect a threat (record identifier for the anti-virus databases, the record timestamp and type); public key of the certificate; digital certificate thumbprint of the scanned object and hashing algorithm.

- Data on the application territorial distribution: date of the application installation and activation, ID of the partner providing the license for the application activation, application ID, application language localization ID, license serial number for the application activation, KSN participation sign.

- Information about the license used: the type and validity period of the license, number of days till license expiration, identifier of the partner from whom the license was purchased, Regional Activation Center identifier, checksum of the activation code, ticket body hash calculated using the SHA1 algorithm, license ticket creation date and time, license information identifier, license ticket identifier, license ticket sequence identifier, unique identifier of the user's computer, date from which the license ticket is valid, date to which the license ticket is valid, license ticket current state, ticket header version, license version, ticket header signature certificate identifier, checksum of the key file, ticket header signer serial number, authentication token.

- Information about hardware installed on the computer: type, name, model name, firmware version, parameters of built-in and connected devices.

- Information about the device: device ID.

- Information about the operation of the Web Control component: component version, categorization reason, additional information about categorization reason, categorized URL, host IP address of blocked/categorized object.

When Private KSN infrastructure is used by Kaspersky Security Center and you choose to participate in Kaspersky Security Network in policy settings, Kaspersky Endpoint Security doesn't send statistics from client computers to which the policy is applied to Kaspersky.

Configure Essential Threat Protection settings

In the **Essential Threat Protection** section, you can configure the following components:

- File Threat Protection
- Web Threat Protection
- Network Threat Protection

You can open a window to configure component settings by clicking the corresponding link.

Configure File Threat Protection settings

In the **File Threat Protection** window, do the following if necessary:

- Turn on/off File Threat Protection.

  By default, File Threat Protection is turned on.

- Create a protection scope.
- Select the action to be performed upon detecting a malicious object.
- Select whether Kaspersky Endpoint Security will scan only new and modified files or all files.
- Select whether Kaspersky Endpoint Security will skip scanning of the read-only system volume on client computers.
- Select whether Kaspersky Endpoint Security will use iSwift technology while scanning files.

  Note: iSwift allows Kaspersky Endpoint Security to use a special algorithm to exclude certain objects from scanning, which helps increase the scan speed.

- Select which types of files Kaspersky Endpoint Security will scan.
- Select the actions Kaspersky Endpoint Security takes for compound files.

Configure Web Threat Protection settings

In the **Web Threat Protection** window, do the following if necessary:

- Turn on/off Web Threat Protection.

  By default, Web Threat Protection is turned on.

- Select the action to be performed upon detecting a malicious object in web traffic.
- Create or edit a list of trusted web addresses.

Configure Network Threat Protection settings

In the **Network Threat Protection** window, do the following if necessary:

- Turn on/off Network Threat Protection.

  By default, Network Threat Protection is enabled.

- Enable or disable blocking of attacking computers.
- Create or edit a list of IP addresses of remote computers whose network activity will never be blocked by Kaspersky Endpoint Security.

Configure Security Controls

In the **Security Controls** section, do the following if necessary:

- Turn on/off Web Control.

  Note: If you turn on Web Control to block access to dangerous web resources, Kaspersky Endpoint Security displays the **Web Control is enabled** notification in Protection Center on the remote computer. Kaspersky Endpoint Security displays notifications when the user accesses web resources blocked by Web Control on the remote computer if the **Secure connections (HTTPS) check** toggle switch is turned on in the **Network** window of the New policy wizard.

- Add rules that will define which web addresses or website categories will be monitored and managed by Web Control on a user's computer.
- Edit, delete, or organize created rules in the list.

  The order in which the rules are sorted determines the priority of their application by Kaspersky Endpoint Security.

Configure Data Encryption

In the **Data Encryption** section, you can turn on or off encryption of the client computer's startup disks to prevent unauthorized users from accessing sensitive data. By default, FileVault disk encryption is disabled.

Configure Detection and Response settings

In the **Detection and Response** section, you can configure the following components:

- Managed Detection and Response
- Endpoint Detection and Response
- Endpoint Detection and Response (KATA)

You can open a window to configure component settings by clicking the corresponding link.

Configure Managed Detection and Response

In the **Managed Detection and Response** window, do the following if necessary:

- Enable or disable the Managed Detection and Response component.
- Import or delete the MDR configuration file.

The Managed Detection and Response component provides interaction with Kaspersky Managed Detection and Response service that constantly detects and eliminates security threats aimed at your organization.

By default, Managed Detection and Response is disabled.

Configure Endpoint Detection and Response

In the **Endpoint Detection and Response** window, do the following if necessary:

- Enable or disable the Endpoint Detection and Response component.
- Configure the Network isolation settings for the user device:
  - Specify the delay for automatically turning off Network isolation.
  - Configure the Network isolation exclusions.
- Enable or disable Execution prevention.
- Select an action to be performed on execution or opening of forbidden object.
- Create a list of Execution prevention rules.
- Enable or disable Cloud Sandbox technology.

The Endpoint Detection and Response component combines automatic detection of threats with the ability to react to these threats to counteract advanced attacks including new exploits, ransomware, fileless attacks, as well as methods using legitimate system tools.

By default, Endpoint Detection and Response is disabled.

Configure Endpoint Detection and Response (KATA)

In the **Endpoint Detection and Response (KATA)** window, do the following if necessary:

- Enable or disable the Endpoint Detection and Response (KATA) component.
- Configure server connection settings:
  - Specify the KATA server response timeout.
  - Add a TLS certificate to configure a trusted connection.

    - Select whether Kaspersky Endpoint Security will use two-way verification to connect to a KATA server.
    - Load a password-protected crypto-container to enable two-way verification.
- Add a KATA server.
- Select whether Kaspersky Endpoint Security will use TTL for packets sent to a KATA server.
- Configure settings for sending data to KATA servers.
- Restrict the number of events transmitted to a KATA server by Kaspersky Endpoint Security.

The Endpoint Detection and Response (KATA) component facilitates interaction with the Kaspersky Anti Targeted Attack Platform solution, which promptly detects advanced threats, such as targeted attacks, advanced persistent threats, zero-day attacks, and others.

By default, Endpoint Detection and Response (KATA) is disabled.

Configure Update settings

In the **Update** section, do the following if necessary:

- Turn on/off updating of application modules.
- Add or delete update sources that will be used to update Kaspersky Endpoint Security.

Configure Additional Settings

In the **Additional Settings** section, do the following if necessary:

- Configure protection settings for the operating system on the client computer.
- Select types of objects to be detected.
- Disable or enable the start of scheduled tasks when the computer is running on battery power.
- Configure settings for generating and storing reports.
- Configure settings for storing objects in Backup.
- Configure the Kaspersky Endpoint Security settings for interaction with the user of the client computer.
- Configure the connection to a proxy server.
- Enable or disable scanning of inbound and outbound HTTPS traffic.
- Select the certificate storage for checking encrypted HTTPS traffic in the Mozilla Firefox browser.

- Configure monitored ports.
- Edit the lists of trusted files, folders, and applications that will not be monitored by Kaspersky Endpoint Security.

Create tasks

This section describes how to use Kaspersky Security Center Web Console and Cloud Console to create and configure tasks that Kaspersky Endpoint Security performs on a client computer or a group of computers managed by Kaspersky Security Center.

A task is a set of configurable actions that Kaspersky Endpoint Security performs on a client computer.

In Kaspersky Security Center Web Console and Cloud Console, you can create the following tasks:

- Scan
- Update
- Rollback
- Add key

Create a task

1. In the **Devices** section on the left, select the **Tasks** section.
2. Click **Add**.
   The Add task wizard starts.
3. In the **Application** drop-down list, select **Kaspersky Endpoint Security for Mac 12.2**.
4. In the **Task type** drop-down list, select the task you want to create.
5. If needed, edit the task name in the **Task name** field.
6. Select devices to which the task will be assigned.
7. Configure settings for the selected task type.
8. Complete the Add task wizard by clicking **Finish**.

> **Note:** If you select the **Open task details when creation is complete** check box in the **Finish task creation** window, you can proceed with modifying the default task settings. If you do not select this check box, the task is created with the default settings. You can modify the default task settings later, at any time.

You can take the following actions on tasks:

- Start and stop tasks.
- Configure task settings.

- Track the progress of a task.
- Copy and move tasks from one group to another.
- Delete tasks.

For detailed information about Kaspersky Security Center Web Console tasks, see the Kaspersky Security Center Help.

For detailed information about Kaspersky Security Center Cloud Console tasks, see the Kaspersky Security Center Cloud Console Help.

Configure the Scan task settings

On the **Application settings** tab, you can configure the **Scan** task settings for Kaspersky Endpoint Security on remote computers.

Open the Scan task settings

1. Go to **Devices** > **Tasks**.
2. Double-click a task with the **Scan** task type.
3. Click the **Application settings** tab.

You can do the following if necessary:

- Define a scan scope.
- Specify the action that Kaspersky Endpoint Security performs upon detecting an infected object.
- Select which types of files Kaspersky Endpoint Security will scan when running the Scan task.
- Configure the scan performance settings.
- Select which compound files Kaspersky Endpoint Security will analyze.

Note: Kaspersky Endpoint Security does not scan files that are located in OneDrive or iCloud storage or other cloud storages. Please exclude these files from the scan scope. Otherwise, the scan task may finish with the *Infected File Not Deleted* error.

Configure the Add key task settings

On the **Application settings** tab, you can configure the **Add key** task settings for Kaspersky Endpoint Security on remote computers.

Open the Add key task settings

1. Go to **Devices** > **Tasks**.
2. Double-click a task with the **Add key** task type.
3. Click the **Application settings** tab.

You can do the following if necessary:

- Make the current license key a reserve key.
- Select another key for activating Kaspersky Endpoint Security on a user's computer.
- Add a new license key to the Kaspersky Security Center repository.

Configure the Update task

On the **Application settings** tab, you can configure the **Update** task settings for Kaspersky Endpoint Security on remote computers.

Open the Update task settings

1. Go to **Devices** > **Tasks**.
2. Double-click a task with the **Update** task type.
3. Click the **Application settings** tab.

Dedicated Kaspersky update servers are the main source of updates for Kaspersky Endpoint Security. Kaspersky Endpoint Security can also use distribution points, local folders, or other web servers as an *update source*.

If you manage Kaspersky Endpoint Security via Kaspersky Security Center Web Console, the list of update sources includes Kaspersky update servers and Kaspersky Security Center servers by default. Kaspersky Endpoint Security downloads updates first from Kaspersky Security Center servers and then from Kaspersky update servers.

If you manage Kaspersky Endpoint Security via Kaspersky Security Center Cloud Console, the list of update sources includes Kaspersky update servers and distribution points by default. Kaspersky Endpoint Security downloads updates first from distribution points and then from Kaspersky update servers. For detailed information about distribution points, see the Kaspersky Security Center Help.

You can do the following if necessary:

- Enable or disable updating of application modules.
- Add or delete update sources that will be used to update Kaspersky Endpoint Security.

Get a recovery key for an encrypted drive

If a user of a client computer forgets or loses his or her credentials and cannot access an encrypted drive, you can get a recovery key.

Get a recovery key

1. Click the administrator account name in the lower left corner of the Kaspersky Security Center Web Console or Cloud Console window.
2. Choose **Interface options**.
3. In the dialog that opens, turn on the **Show Data encryption and protection** toggle switch to enable managing data encryption and click **Save**.
4. Go to **Operations** > **Data encryption and protection** > **Encrypted drives.**

   The list of encrypted devices opens.
5. Select the check box next to the device with the encrypted drive.
6. Click **Grant access to the device in offline mode**.
7. In the **Grant access to the device in offline mode** dialog, select the web plug-in for Kaspersky Endpoint Security and click **OK**.
8. Click **Get recovery key**.

   A recovery key appears in the current dialog window.
9. Save the recovery key in any convenient way.

You can use this recovery key on a client computer to access the encrypted drive.

The Installation type window

In the **Packages to install** section, you can select application components that will be installed on a client computer.

Scan

This check box adds the Scan component to the Kaspersky Endpoint Security installation package.

The check box is selected by default and cannot be cleared.

File Threat Protection

This check box enables/disables adding the File Threat Protection component to the Kaspersky Endpoint Security installation package.

If this check box is selected, the File Threat Protection component is included in the Kaspersky Endpoint Security installation package.

If this check box is cleared, the File Threat Protection component is not included in the Kaspersky Endpoint Security installation package.

This check box is selected by default.

Web Threat Protection

This check box enables/disables adding the Web Threat Protection component to the Kaspersky Endpoint Security installation package.

If this check box is selected, the Web Threat Protection component is included in the Kaspersky Endpoint Security installation package.

If this check box is cleared, the Web Threat Protection component is not included in the Kaspersky Endpoint Security installation package.

This check box is selected by default.

Network Threat Protection

This check box enables/disables adding the Network Threat Protection component to the Kaspersky Endpoint Security installation package.

If this check box is selected, the Network Threat Protection component is included in the Kaspersky Endpoint Security installation package.

If this check box is cleared, the Network Threat Protection component is not included in the Kaspersky Endpoint Security installation package.

This check box is selected by default.

Network Agent Connector

This check box adds the Network Agent Connector component to the Kaspersky Endpoint Security installation package.

The check box is selected by default and cannot be cleared.

The "License information" window

In the **License information** window, you can view information about a license, including its expiration date, the number of computers on which you can use Kaspersky Endpoint Security under this license, and the license type.

Add as reserve key

This check box enables/disables adding a specific key file or activation code as a reserve key.

If this check box is selected, Kaspersky Endpoint Security adds the specified key file or activation code as a reserve key.

If this check box is cleared, Kaspersky Endpoint Security adds the specified key file or activation code as the active key.

This check box is cleared by default.

The "Scan" window

Scan scope

Clicking this link opens a window where you can create the scan scope.

In the **If a malicious object is detected** section, you can select the action that Kaspersky Endpoint Security performs upon detecting an infected object.

Prompt user to take action after scan

Kaspersky Endpoint Security doesn't process objects until the scan is complete. At that point, Kaspersky Endpoint Security displays a notification with information about each infected object and prompts the user to select what action to take. The available options depend on the type of object.

This option is selected by default.

Prompt user to take action immediately

Kaspersky Endpoint Security displays a notification with information about each infected object that the application detects and prompts the user to select a further action. The available options depend on the type of object.

Do not prompt for action

Kaspersky Endpoint Security records information about detected objects in the report without processing them.

Disinfect automatically

This check box enables/disables disinfection of infected objects that Kaspersky Endpoint Security detects without prompting the user for confirmation.

If this check box is selected, Kaspersky Endpoint Security automatically disinfects infected objects.

If the check box is cleared, Kaspersky Endpoint Security skips infected objects.

This check box is available if the **Do not prompt for action** option is selected.

This check box is selected by default.

Disinfect, delete if disinfection fails

This check box enables/disables removal of infected or probably infected objects after an attempt to disinfect them fails.

If this check box is selected, Kaspersky Endpoint Security automatically removes infected objects that could not be disinfected.

If this check box is cleared, Kaspersky Endpoint Security does not remove infected objects that could not be disinfected.

This check box is displayed if the **Do not prompt for action** option is selected and the **Disinfect automatically** check box is selected.

This check box is selected by default.

In the **File types** section, you can select the format of files to be scanned by Kaspersky Endpoint Security.

Scan all files

Kaspersky Endpoint Security scans all file system objects that are executed, opened, or saved.

Scan applications and documents by content

Kaspersky Endpoint Security scans only objects that may be infected based on file format.

The list of file formats is defined by Kaspersky and is part of Kaspersky Endpoint Security databases.

Scan applications and documents by extension

Kaspersky Endpoint Security scans only objects that may be infected based on file extension.

The list of file extensions is defined by Kaspersky and is part of Kaspersky Endpoint Security databases.

Kaspersky Endpoint Security always scans files without extensions.

In the **Optimization** section, you can configure scan performance.

Scan only new and modified files

This check box enables/disables scanning of only those files that Kaspersky Endpoint Security recognizes as new or modified since the previous scan.

If this check box is selected, Kaspersky Endpoint Security scans only files that it recognizes as new or modified since the previous scan.

If this check box is cleared, Kaspersky Endpoint Security scans all files.

Skip scanning of read-only system volume

This check box disables/enables scanning of the read-only system volume by Kaspersky Endpoint Security.

If this check box is selected, Kaspersky Endpoint Security skips scanning of the read-only system volume to significantly reduce scanning time.

If this check box is cleared, Kaspersky Endpoint Security scans the read-only system volume.

This check box is selected by default.

Skip files larger than MB

This check box enables/disables excluding files larger than the specified size from scanning.

If this check box is selected, Kaspersky Endpoint Security skips files larger than the specified size.

If this check box is cleared, Kaspersky Endpoint Security scans files regardless of their size.

This check box is cleared by default.

By default, the size is set to 100 MB.

Skip if scan takes longer than s

This check box enables/disables the limit on the duration of file scans. Kaspersky Endpoint Security skips a file if scanning the file exceeds the specified time limit.

If this check box is selected, Kaspersky Endpoint Security skips a file if scanning the file exceeds the specified time limit.

If this check box is cleared, Kaspersky Endpoint Security scans files regardless of how much time the scan might take.

The default value is 30 seconds.

In the **Compound files** section, you can select the types of compound files that Kaspersky Endpoint Security scans.

Scan archives

This check box enables/disables scanning of archives.

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

If this check box is cleared, Kaspersky Endpoint Security skips archives during scans.

All

Kaspersky Endpoint Security scans all archives.

This option is available if the **Scan archives** check box is selected.

New only

Kaspersky Endpoint Security scans only new archives.

This option is available if the **Scan archives** check box is selected.

Scan password-protected archives

This check box enables/disables scanning of password-protected archives.

If this check box is selected, Kaspersky Endpoint Security scans password-protected archives.

If this check box is cleared, Kaspersky Endpoint Security skips password-protected archives during scans.

Scan embedded OLE objects

This check box enables/disables scanning of objects embedded in a file, such as Excel spreadsheets, macros, or email attachments.

If this check box is selected, Kaspersky Endpoint Security scans embedded OLE objects.

If this check box is cleared, Kaspersky Endpoint Security skips embedded OLE objects during scans.

All

Kaspersky Endpoint Security scans all OLE objects.

This option is available if the **Scan embedded OLE objects** check box is selected.

New only

Kaspersky Endpoint Security scans only new embedded OLE objects.

This option is available if the **Scan embedded OLE objects** check box is selected.

Scan email format files

This check box enables/disables scanning of files in email formats and email databases.

If this check box is selected, Kaspersky Endpoint Security scans files in email formats and email databases.

If this check box is cleared, Kaspersky Endpoint Security skips files in email formats and email databases during scans.

The "Scan scope" window

Add

Clicking this button opens a dialog where you can specify a file, folder, or file/folder mask to be added to the scan scope.

Delete

Clicking this button removes an object from the scan scope.

This button is available if the check box next to the object is selected.

You cannot delete the default objects included in the scan scope.

Scan scope

This column contains the objects scanned during a malware scan.

Status

The toggle switch in this column enables/disables scanning of the objects added to the scan scope.

If the toggle switch is turned on, Kaspersky Endpoint Security scans the corresponding object.

If the toggle switch is turned off, Kaspersky Endpoint Security doesn't scan the corresponding object.

Additional

This column indicates whether Kaspersky Endpoint Security scans subfolders of the corresponding object.

Note: Kaspersky Endpoint Security does not scan files that are located in OneDrive or iCloud storage or other cloud storages. Please exclude these files from the scan scope. Otherwise, the scan task may finish with the *Infected File Not Deleted* error.

The "Add scan scope" dialog

Enter a file name, folder name, or mask

Path to a file, folder, or file/folder mask.

Object is a folder

This check box enables/disables scanning of an object as a folder.

If this check box is selected, Kaspersky Endpoint Security scans the object that you have specified in the **Enter a file name, folder name, or mask** field as a folder.

If this check box is cleared, Kaspersky Endpoint Security scans the object that you have specified in the **Enter a file name, folder name, or mask** field as a file.

This check box is selected by default.

Include subfolders

This check box enables/disables scanning of subfolders in the folder specified in the **Enter a file name, folder name, or mask** field.

If this check box is selected, Kaspersky Endpoint Security scans subfolders during malware scans.

If this check box is cleared, Kaspersky Endpoint Security scans only the files directly in the folder specified in the **Enter a file name, folder name, or mask** field during malware scans.

This check box is selected by default.

Note: Kaspersky Endpoint Security does not scan files that are located in OneDrive or iCloud storage or other cloud storages. Please exclude these files from the scan scope. Otherwise, the scan task may finish with the *Infected File Not Deleted* error.

The File parameters window

The following types of file hashes are supported:

- **MD5**

  A hash of this type must be 32 characters long and contain 0-9, a-f, A-F.

- **SHA256**

  A hash of this type must be 64 characters long and contain 0-9, a-f, A-F.

The "Network" window

In the **Proxy server settings** section, you can configure use of a proxy server and settings to be used to connect to a proxy server.

Do not use proxy server

If this option is selected, Kaspersky Endpoint Security does not use a proxy server to connect to update sources for application databases and modules.

Use system proxy server settings

If this option is selected, Kaspersky Endpoint Security connects to update sources for application databases and modules using the proxy server settings configured in your operating system.

This option is selected by default.

Use specified proxy server settings

If this option is selected, Kaspersky Endpoint Security connects to update sources for application databases and modules using the proxy server settings you have specified.

Address

IP address or symbolic name of a proxy server.

This field is available if the **Use specified proxy server settings** option is selected.

Port

Proxy server port number.

The default port number is 8080.

This field is available if the **Use specified proxy server settings** option is selected.

Use authentication

This check box enables/disables the use of authentication when connecting to a proxy server.

If this check box is selected, Kaspersky Endpoint Security requires the user's credentials to connect to a proxy server.

If this check box is cleared, Kaspersky Endpoint Security does not require the user's credentials to connect to a proxy server.

This check box is selected by default.

This check box is available if the **Use specified proxy server settings** option is selected.

User name

User name for connecting to the proxy server.

This field is available if the **Use specified proxy server settings** option and the **Use authentication** check box are selected.

Password

Password for the specified user name.

This field is available if the **Use specified proxy server settings** option and the **Use authentication** check box are selected.

Show

Clicking this button shows the characters of the password you enter in the **Password** field.

Bypass proxy server for local addresses

This check box enables/disables use of a proxy server when updating application databases and modules from a local or network folder.

If this check box is selected, Kaspersky Endpoint Security does not use a proxy server when updating application databases and modules from a local or network folder.

If this check box is cleared, Kaspersky Endpoint Security uses a proxy server when updating application databases and modules from a local or network folder.

This check box is selected by default.

This check box is available if the **Use specified proxy server settings** option is selected.

In the **Check secure connections** section, you can define whether Kaspersky Endpoint Security scans secure connections (HTTPS).

Secure connections (HTTPS) check

The **Secure connections (HTTPS) check** toggle switch enables/disables scanning of secure connections established via the HTTPS protocol and displaying notifications when Web Control blocks the user's access to dangerous web resources.

If the **Secure connections (HTTPS) check** toggle switch is turned on, Kaspersky Endpoint Security does the following:

- Web Threat Protection scans data that is sent and received by your computer over the HTTPS protocol in Safari, Google Chrome, or Firefox.
- The application displays notifications when the user accesses web resources blocked by Web Control on the remote computer.

If the **Secure connections (HTTPS) check** toggle switch is turned off, Kaspersky Endpoint Security does the following:

- Web Threat Protection does not scan data that is sent and received by your computer via the HTTPS protocol.
- The application does not display notifications when the user accesses web resources blocked by Web Control on the remote computer.

This toggle switch is turned on by default.

In the **Select the certificate store for Firefox to use** section, you can select the certificate storage for checking encrypted HTTPS traffic in the Mozilla Firefox browser.

System Roots keychain (recommended)

If this option is selected, Kaspersky Endpoint Security uses a root certificate from the System Roots keychain to check encrypted HTTPS traffic in the Mozilla Firefox browser.

This option is selected by default.

Certificate store from Mozilla Firefox browser settings

If this option is selected, Kaspersky Endpoint Security uses the certificate from the browser certificate store.

In this case, you need to manually add the Kaspersky Endpoint Security certificate to the certificate store of the Mozilla Firefox browser. For more information, refer to How to add the Kaspersky certificate to the Mozilla Firefox certificate storage.

In the **Trusted root certificates** section, you can manage the list of trusted root certificates.

Manage trusted root certificates

Clicking this link opens a window where you can create a list of trusted root certificates to connect to the corresponding servers without notifications.

In the **Monitored ports** section, you can configure which ports are monitored by Kaspersky Endpoint Security.

Selected ports

Clicking this link opens a window where you can configure a list of ports that are monitored by Kaspersky Endpoint Security.

Enforce

When the **Enforce** toggle switch is turned on, Kaspersky Endpoint Security prohibits changing the values of task settings, application settings, policies of subgroups, and secondary Administration Servers on a local computer.

When the **Enforce** toggle switch is turned off, Kaspersky Endpoint Security allows changing the values of task settings, application settings, policies of subgroups, and secondary Administration Servers on a local computer.

The "Manage trusted root certificates" window

Add

Clicking this button opens a dialog for adding certificates that will be considered trusted.

Delete

Clicking this button removes the selected certificate from the list of trusted ones.

List of trusted certificates

A list displaying the names of the trusted root certificates.

The list is empty by default.

Enforce

When the **Enforce** toggle switch is turned on, Kaspersky Endpoint Security prohibits changing the values of task settings, application settings, policies of subgroups, and secondary Administration Servers on a local computer.

When the **Enforce** toggle switch is turned off, Kaspersky Endpoint Security allows changing the values of task settings, application settings, policies of subgroups, and secondary Administration Servers on a local computer.

The "Monitored ports" window

List of monitored ports

A list of ports for which you can configure monitoring of transmitted data.

By default, the list of ports contains ports that are frequently used by the most common services.

Add

Clicking this button opens a dialog where you can add a port you want to be monitored by Kaspersky Endpoint Security.

Delete

Clicking this button removes the selected port from the list.

This button is available if the check box next to the port is selected.

Port

This column contains the port numbers.

Status

This column contains a toggle switch that indicates the status of monitoring of data transmitted through the port.

If the status is **Monitored**, the traffic transmitted through the corresponding port is scanned by Kaspersky Endpoint Security.

If the status is **Not monitored**, the traffic transmitted through the corresponding port is not scanned by Kaspersky Endpoint Security.

Description

This column contains a description of the port.

The "Add port" dialog

Port entry field

The number of a port for which you want Kaspersky Endpoint Security to scan transmitted data.

Description entry field

Additional information about the port, for example, the port type.

The "Trusted Zone" window: The "Files and folders" section

Add

Clicking this button opens a dialog where you can add a file or folder to Trusted zone.

Delete

Clicking this button removes a selected file or folder from the list of exclusions.

This button is available if the check box next to the file or folder is selected.

File or folder

This column contains files or folders added to Trusted zone.

Status

The toggle switch in this column disables/enables scanning of the file or folder added to Trusted zone.

If the toggle switch is turned on, Kaspersky Endpoint Security doesn't scan the corresponding file or folder.

If the toggle switch is turned off, Kaspersky Endpoint Security scans the corresponding file or folder.

Comment

Information about the file or folder added to Trusted zone.

Enforce

When the **Enforce** toggle switch is turned on, Kaspersky Endpoint Security prohibits changing the values of task settings, application settings, policies of subgroups, and secondary Administration Servers on a local computer.

When the **Enforce** toggle switch is turned off, Kaspersky Endpoint Security allows changing the values of task settings, application settings, policies of subgroups, and secondary Administration Servers on a local computer.

The "Add exclusion" dialog

Enter a file name, folder name, or mask entry field

Path to a file or folder, or a file/folder mask that will be excluded from the protection scope.

Include subfolders

This check box enables/disables scanning of subfolders of the folder specified in the **Enter a file name, folder name, or mask** field.

If this check box is selected, Kaspersky Endpoint Security does not scan subfolders of the specified folder during malware scans.

If this check box is cleared, Kaspersky Endpoint Security only excludes files directly in the folder specified in the **Enter a file name, folder name, or mask** field during malware scans. Subfolders of the specified folder are scanned.

This check box is selected by default.

In the **Components** section, you can select components that will not scan the specified file or folder.

Any

Neither the Scan nor File Threat Protection component will not scan the specified file or folder.

From list

This option lets you select components.

File Threat Protection

If this check box is selected, the File Threat protection component will not scan the specified file or folder.
This check box is available if the **From list** option is selected.

Scan

If this check box is selected, the Scan component will not scan the specified file or folder.
This check box is available if the **From list** option is selected.

Comment entry field

Information about the file or folder added to Trusted zone.

In the **Status** section, you can select whether the exclusion is active or not.

Disabled

Kaspersky Endpoint Security scans the corresponding file or folder.

Enabled

Kaspersky Endpoint Security doesn't scan the corresponding file or folder.

The "Trusted Zone" window: The "Trusted applications" section

List of trusted applications

A list of trusted applications whose network activity will not be monitored by Kaspersky Endpoint Security.

Add

Clicking this button opens a dialog where you can enter a path to an application whose network activity will not be monitored by Kaspersky Endpoint Security.

Delete

Clicking this button removes the selected trusted application from the list.

This button is available if the check box next to the trusted application is selected.

Application

This column contains the application name or the last segment of the path to an application.

Status

This column contains a toggle switch that indicates the status of monitoring the application network activity.

If the status is **Enabled**, the network activity of the corresponding application is not monitored by Kaspersky Endpoint Security.

If the status is **Disabled**, the network activity of the corresponding application is monitored by Kaspersky Endpoint Security.

Path

This column contains the application path on the client computer, which you add manually.

Enforce

When the **Enforce** toggle switch is turned on, Kaspersky Endpoint Security prohibits changing the values of task settings, application settings, policies of subgroups, and secondary Administration Servers on a local computer.

When the **Enforce** toggle switch is turned off, Kaspersky Endpoint Security allows changing the values of task settings, application settings, policies of subgroups, and secondary Administration Servers on a local computer.

The "Add application" dialog

Path entry field

The path to an application whose network or file activity will not be monitored by the Kaspersky Endpoint Security application.

Code signing requirement

Requirements for the code signature of the application whose activity will not be monitored by Kaspersky Endpoint Security.

This is an optional parameter.

Options

In this section, you can select the types of activity that you do not want to be monitored by the Kaspersky Endpoint Security application.

Do not monitor file activity

This check box enables/disables monitoring of an application's operations with files on a client computer.

If this check box is selected, Kaspersky Endpoint Security doesn't monitor the application's file activity.

If this check box is cleared, Kaspersky Endpoint Security monitors the application's file activity.

This check box is selected by default.

Do not monitor network activity

This check box enables/disables monitoring of the application's inbound and outbound internet traffic on a client computer.

If this check box is selected, Kaspersky Endpoint Security doesn't monitor the application's network activity.

If this check box is cleared, Kaspersky Endpoint Security monitors the application's network activity.

This check box is selected by default.

The Additional Settings section

Protection

Clicking this link opens the **Protection** window where you can manage general settings for Kaspersky Endpoint Security installed on users computers and select the types of objects that Kaspersky Endpoint Security will detect.

Reports and Backup

Clicking this link opens the **Reports and Backup** window where you can manage reports and backup settings.

User interaction

Clicking this link opens the **User interaction** window where you can set up notifications displayed by Kaspersky Endpoint Security, the display language for events displayed in Kaspersky Security Center, and additional settings for Kaspersky Endpoint Security.

Network

Clicking this link opens the **Network** window where you can manage proxy server settings, enable or disable scanning of encrypted connections (HTTPS), select the certificate storage for checking encrypted HTTPS traffic in the Mozilla Firefox browser, and configure monitored ports.

Trusted zone

Clicking this link opens the **Trusted Zone** window where you can add exclusions for File Threat Protection or scan tasks and configure trusted applications.

The "Protection" window

In the **General** section, you can enable or disable file protection on a remote computer and configure automatic start of the application when the computer is turned on or the operating system is restarted.

Start the application at computer startup

This check box enables/disables automatic start of Kaspersky Endpoint Security when a remote computer is turned on or after its operating system is restarted.

If the check box is selected, Kaspersky Endpoint Security starts automatically when the remote computer is turned on or its operating system is restarted.

If the check box is cleared, Kaspersky Endpoint Security does not start automatically when the remote computer is turned on or its operating system is restarted.

This check box is selected by default.

Important: If you select this check box when Kaspersky Endpoint Security is not running, changes will be applied only after you start the application locally or using Kaspersky Security Center.

Enable protection

This check box enables/disables protection of a remote computer with Kaspersky Endpoint Security installed.

If this check box is selected, protection of the remote computer is enabled.

If this check box is cleared, protection of the remote computer is disabled.

This check box is selected by default.

In the **Types of objects to be detected** section, you can select the types of objects that Kaspersky Endpoint Security will detect.

Viruses, worms, Trojans, malicious tools, adware, and auto-dialers

This check box enables/disables detection of the following types of programs:

- All types of malware.
- Applications that show advertisements (such as banners) on your computer or replace the search results in your browser with advertising websites.
- Applications that surreptitiously establish phone connections through a computer's modem.

The check box is selected by default and cannot be cleared.

Legitimate software that can be used by intruders to damage user's computer or personal data

This check box enables/disables detection of applications that are not malicious or dangerous but which under certain circumstances may be used to harm a user's computer.

If the check box is selected, Kaspersky Endpoint Security detects legitimate software that can be used by intruders to damage a user's computer or personal data.

If the check box is cleared, Kaspersky Endpoint Security does not detect legitimate software that can be used by intruders to damage a user's computer or personal data.

This check box is cleared by default.

The **Advanced** section lets you enable energy-saving mode.

Skip scheduled tasks when running on battery power

This check box enables/disables the start of scheduled scan tasks on computers running on battery power.

If this check box is selected, Kaspersky Endpoint Security does not start scheduled scan tasks on computers running on battery power.

If this check box is cleared, Kaspersky Endpoint Security starts scheduled scan tasks on computers running on battery power.

This check box is selected by default.

Limit scan tasks' use of the CPU

Kaspersky Endpoint Security limits its use of the protected device's CPU for on-demand scan tasks to the value specified in the corresponding entry field.

Enabling this option can negatively affect the performance of Kaspersky Endpoint Security.

By default, this option is disabled.

Upper limit (in percentages)

Maximum allowed CPU utilization for scan tasks by Kaspersky Endpoint Security.

The entry field is available if the **Limit scan tasks' use of the CPU** option is selected.

> **Note:** This is a cumulative limit across all CPU cores. The CPU utilization shown in Activity Monitor is the sum of the utilization of each CPU core and therefore may exceed 100 percent.

Enforce

When the **Enforce** toggle switch is turned on, Kaspersky Endpoint Security prohibits changing the values of task settings, application settings, policies of subgroups, and secondary Administration Servers on a local computer.

When the **Enforce** toggle switch is turned off, Kaspersky Endpoint Security allows changing the values of task settings, application settings, policies of subgroups, and secondary Administration Servers on a local computer.

The "Reports and Backup" window

In the **Reports** section, you can configure settings for generating and storing reports on events that occur while Kaspersky Endpoint Security is running.

Delete reports after days

This check box enables/disables deletion of reports after the specified period.

If this check box is selected, Kaspersky Endpoint Security deletes reports after the specified period. By default, Kaspersky Endpoint Security stores reports for 30 days.

If this check box is cleared, Kaspersky Endpoint Security stores reports indefinitely.

This check box is selected by default.

Log non-critical events

This check box enables/disables logging of non-critical events (such as informational events) in the report. Non-critical events do not affect security.

If this check box is selected, Kaspersky Endpoint Security logs informational events in the report.

If this check box is cleared, Kaspersky Endpoint Security does not log informational events in the report.

This check box is cleared by default.

Keep only recent events

This check box enables/disables keeping only information about important events from the previous run of the task.

If this check box is selected, each time a task starts, Kaspersky Endpoint Security removes information about non-critical events from the previous run of the task but keeps important information (for example, about detected malware) in the report.

If this check box is cleared, Kaspersky Endpoint Security keeps all information from the previous run of the task.

This check box is cleared by default.

In the **Backup** section, you can specify how long objects can be stored in Backup.

Delete objects after days

This check box enables/disables removal of objects from Backup after the specified period.

If this check box is selected, Kaspersky Endpoint Security removes objects from Backup after the specified period. The default storage period is 30 days.

If this check box is cleared, Kaspersky Endpoint Security stores objects in Backup indefinitely.

This check box is selected by default.

Enforce

When the **Enforce** toggle switch is turned on, Kaspersky Endpoint Security prohibits changing the values of task settings, application settings, policies of subgroups, and secondary Administration Servers on a local computer.

When the **Enforce** toggle switch is turned off, Kaspersky Endpoint Security allows changing the values of task settings, application settings, policies of subgroups, and secondary Administration Servers on a local computer.

The "User interaction" window

In the **Application interface** section, you can configure whether the application icon is displayed in the menu bar on a remote computer and whether a user can open the Kaspersky Endpoint Security main window and use the application interface.

Show application icon in menu bar

This check box enables/disables the display of the application icon in the menu bar on a remote computer.

If this check box is selected, the application icon is displayed in the menu bar.

If this check box is cleared, the application icon is hidden from the menu bar.

This check box is selected by default.

Allow user to open application

This check box enables/disables a user's ability to open the Kaspersky Endpoint Security main window and use the application interface on a remote computer.

If this check box is selected, a user can open the Kaspersky Endpoint Security main window and use the application interface on a remote computer.

If this check box is cleared, Kaspersky Endpoint Security prevents a user from opening the main application window and hides the application interface on a remote computer.

This check box is selected by default.

In the **Notifications** section, you can enable notifications about Kaspersky Endpoint Security events and choose the preferred notification type.

Notifications

The **Notifications** toggle switch enables/disables notifications about Kaspersky Endpoint Security events.

If the **Notifications** toggle switch is turned on, Kaspersky Endpoint Security shows notifications about events that occur while Kaspersky Endpoint Security components are running.

If the **Notifications** toggle switch is turned off, Kaspersky Endpoint Security doesn't show notifications about events that occur while Kaspersky Endpoint Security components are running.

This toggle switch is turned on by default.

User notifications

Clicking this link opens a window where you can select the types of notifications to be used for all event types.

In the **Allow user to quit the application** section, you can configure whether Kaspersky Endpoint Security can be shut down by a user on a remote computer.

Show Quit in the application icon's context menu

This check box enables/disables availability of the **Quit** item in the context menu of the application icon shown in the menu bar.

If this check box is selected, the **Quit** item is available in the context menu of the application icon. The user of a remote computer can quit Kaspersky Endpoint Security on the remote computer.

If this check box is cleared, the **Quit** item is unavailable in the context menu of the application icon. The user of a remote computer cannot quit Kaspersky Endpoint Security on the remote computer.

This check box is selected by default.

In the **Events in Kaspersky Security Center** section, you can select the display language for Kaspersky Endpoint Security events in Kaspersky Security Center.

Display language

From this drop-down list, you can select the display language for Kaspersky Endpoint Security events in Kaspersky Security Center.

In the **Restrictions** section, you can allow local management of Kaspersky Endpoint Security keys and updates on a remote computer.

Allow user to manage updates locally

This check box enables/disables local management of Kaspersky Endpoint Security updates on a remote computer.

If this check box is selected, local management of Kaspersky Endpoint Security updates on a remote computer is enabled.

If this check box is cleared, Kaspersky Endpoint Security updates on a remote computer can be managed only using the Kaspersky Endpoint Security administration plug-in in Kaspersky Security Center.

This check box is selected by default.

Allow user to manage keys locally

This check box enables/disables local management of Kaspersky Endpoint Security keys on a remote computer.

If the check box is selected, local management of Kaspersky Endpoint Security keys on a remote computer is enabled.

If the check box is cleared, Kaspersky Endpoint Security keys on a remote computer can be managed only using the Kaspersky Endpoint Security administration plug-in in Kaspersky Security Center.

This check box is selected by default.

In the **Password protection** section, you can set and configure the password for limiting unwanted actions on users' devices.

Password protection

The **Password protection** toggle switch enables/disables password protection of unwanted actions on users' devices.

If the **Password protection** toggle switch is turned on, you can set and configure a password to limit user actions on their devices.

If the **Password protection** toggle switch is turned off, a user can perform an unwanted action without entering a password.

This toggle switch is turned off by default.

Turning on this toggle switch opens a window where you can configure the password for limiting unwanted actions on users' devices.

Settings

Clicking this button opens a window where you can configure the password for limiting unwanted actions on users' devices.

Enforce

When the **Enforce** toggle switch is turned on, Kaspersky Endpoint Security prohibits changing the values of task settings, application settings, policies of subgroups, and secondary Administration Servers on a local computer.

When the **Enforce** toggle switch is turned off, Kaspersky Endpoint Security allows changing the values of task settings, application settings, policies of subgroups, and secondary Administration Servers on a local computer.

The "User notifications" window

Events

This column lists events that might occur while Kaspersky Endpoint Security is running:

- **Critical events**. Events of crucial importance in terms of security.
- **Functional failure**. Events that cause the system to fail.
- **Important events**. Events that the user should attend to.
- **Informational events**. Events that are informational in nature.

Notifications

A notification is a pop-up message that notifies the user about an event.

The check box in the **Notifications** column enables/disables pop-up notifications about events of a particular category.

Sound

A sound notification associated with an event.

The check box in the **Sound** column enables/disables sound notifications for events of a particular category.

The "Update" section

Update application modules

This check box enables/disables updates of application modules. The application databases are always updated.

If this check box is selected, Kaspersky Endpoint Security updates application modules.

If this check box is cleared, Kaspersky Endpoint Security doesn't update application modules.

This check box is selected by default.

Update sources

This list contains the addresses of resources from which Kaspersky Endpoint Security downloads and installs updates of application databases and modules. You can specify a local or network folder, or an FTP or HTTP server as an update source.

By default, the list of update sources contains Kaspersky update servers.

If you manage Kaspersky Endpoint Security via Kaspersky Security Center Web Console, the list of update sources also includes Kaspersky Security Center servers by default.

If you manage Kaspersky Endpoint Security via Kaspersky Security Center Cloud Console, the list of update sources also includes distribution points by default. For detailed information about distribution points, see the Kaspersky Security Center Help.

You cannot remove the default update sources from the list.

Add

Clicking this button opens a dialog where you can specify the path to a local or network folder, or web address to be added to the list of update sources.

Delete

Clicking this button removes the selected update source from the list.

This button is available if the check box next to the update source is selected.

Update source

This column contains update sources for Kaspersky Endpoint Security.

Status

If the toggle switch in this column is turned on, Kaspersky Endpoint Security uses the corresponding update source from the **Update source** column to receive updates.

If the toggle switch in this column is turned off, Kaspersky Endpoint Security doesn't use the corresponding update source from the **Update source** column to receive updates.

Enforce

When the **Enforce** toggle switch is turned on, Kaspersky Endpoint Security prohibits changing the values of task settings, application settings, policies of subgroups, and secondary Administration Servers on a local computer.

When the **Enforce** toggle switch is turned off, Kaspersky Endpoint Security allows changing the values of task settings, application settings, policies of subgroups, and secondary Administration Servers on a local computer.

The "Add update source" dialog

Enter a path to a local or network folder, or a web address entry field

Address of the resource from which Kaspersky Endpoint Security copies updates.

You can specify a path to a local or network folder, or the web address or IP address of an FTP or HTTP server as the address of the resource.

You can specify the web address of an FTP server in the following format: ftp://<user name>:<password>@<host>:<port>.

In the **Status** section, you can define whether Kaspersky Endpoint Security uses the specified web address as an update source.

Disabled

The web address is added to the list of update sources, but Kaspersky Endpoint Security doesn't use this web address as an update source.

Enabled

The web address is added to the list of update sources and Kaspersky Endpoint Security uses this web address as an update source.

The "Data Encryption" section

FileVault disk encryption

The **FileVault disk encryption** toggle switch enables/disables FileVault disk encryption management.

If the **FileVault disk encryption** toggle switch is turned on, FileVault disk encryption can be applied to client computers from Kaspersky Security Center.

If the **FileVault disk encryption** toggle switch is turned off, FileVault disk encryption can't be applied to client computers from Kaspersky Security Center.

This toggle switch is turned off by default.

Note: If the **FileVault disk encryption** toggle switch is turned off, users with administrator rights can encrypt and decrypt their Mac startup disks from System Settings. For more information on FileVault, refer to Apple documentation.

Encrypt disk

Kaspersky Endpoint Security displays a prompt for computer account credentials on client computers to which the policy is applied. When the user enters the credentials, Kaspersky Endpoint Security starts encrypting the user's startup disk.

If the **FileVault disk encryption** toggle switch is turned on and the **Encrypt disk** option is selected, users with administrator rights can't decrypt the startup disk of their Mac from System Settings.

Decrypt disk

Kaspersky Endpoint Security displays a prompt for computer account credentials on client computers to which the policy is applied. When the user enters the credentials, Kaspersky Endpoint Security starts decrypting the user's startup disk.

If the **FileVault disk encryption** toggle switch is turned on and the **Decrypt disk** option is selected, users with administrator rights can't encrypt the startup disk of their Mac from System Settings.

Enforce

When the **Enforce** toggle switch is turned on, Kaspersky Endpoint Security prohibits changing the values of task settings, application settings, policies of subgroups, and secondary Administration Servers on a local computer.

When the **Enforce** toggle switch is turned off, Kaspersky Endpoint Security allows changing the values of task settings, application settings, policies of subgroups, and secondary Administration Servers on a local computer.

The Detection and Response section

Managed Detection and Response

Clicking this link opens a window where you can configure Managed Detection and Response settings.

Endpoint Detection and Response

Clicking this link opens a window where you can configure Endpoint Detection and Response settings.

Endpoint Detection and Response (KATA)

Clicking this link opens a window where you can configure Endpoint Detection and Response (KATA) settings.

The "Managed Detection and Response" window

Managed Detection and Response

The **Managed Detection and Response** toggle switch enables/disables the Managed Detection and Response component which interacts with the Kaspersky Managed Detection and Response service. This service constantly detects and eliminates security threats aimed at your organization.

If the **Managed Detection and Response** toggle switch is turned on and the MDR configuration file is imported, the Managed Detection and Response component is enabled.

If the **Managed Detection and Response** toggle switch is turned off, the Managed Detection and Response component is disabled.

This toggle switch is turned off by default.

Import

Clicking this button opens a window that lets you import the MDR configuration file into the Kaspersky Endpoint Security policy.

Delete configuration file

Clicking this button deletes the MDR configuration file from the Kaspersky Endpoint Security policy.

Enforce

When the **Enforce** toggle switch is turned on, Kaspersky Endpoint Security prohibits changing the values of task settings, application settings, policies of subgroups, and secondary Administration Servers on a local computer.

When the **Enforce** toggle switch is turned off, Kaspersky Endpoint Security allows changing the values of task settings, application settings, policies of subgroups, and secondary Administration Servers on a local computer.

The Endpoint Detection and Response window

Endpoint Detection and Response

The **Endpoint Detection and Response** toggle switch enables/disables the Endpoint Detection and Response component, which interacts with the Kaspersky Endpoint Detection and Response solution. This solution protects computers against complicated threats, including new exploits, ransomware, and fileless attacks.

If the **Endpoint Detection and Response** toggle switch is turned on, the Endpoint Detection and Response component is enabled.

If the **Endpoint Detection and Response** toggle switch is turned off, the Endpoint Detection and Response component is disabled.

This toggle switch is turned off by default.

In the **Network isolation** section, you can configure settings for isolating computers from the network in response to the detection of an indicator of compromise.

Configure computer unlock settings

Clicking this link opens a window where you can specify the delay for automatically turning off Network isolation.

Exclusions

Clicking this link opens a window where you can specify network connections which are not blocked on the computer after Network isolation is automatically enabled.

In the **Execution prevention** section, you can configure settings for running of executable files and scripts and opening of office format files.

Execution prevention

The **Execution prevention** toggle switch enables/disables Execution prevention.

If the **Execution prevention** toggle switch is turned on, you can create and edit the list of execution prevention rules and select an action to be performed when forbidden objects are executed or opened.

If the **Execution prevention** toggle switch is turned off, you cannot manage the objects that users execute or open on their devices.

This toggle switch is turned off by default.

Action on execution or opening of forbidden object

Block and write to report

If this mode is selected, the application blocks the execution of objects or opening of documents that match prevention rule criteria. The application also publishes an event about attempts to execute objects or open documents to the Kaspersky Security Center event log and the unified logging system.

Log events only

If this mode is selected, Kaspersky Endpoint Security publishes an event about attempts to run executable objects or open documents that match prevention rule criteria to the Kaspersky Security Center event log and the unified logging system, but does not block the attempt to run or open the object or document. This mode is selected by default.

Add

Clicking this button opens a dialog where you can create a new execution prevention rule.

Edit

Clicking this button opens a dialog where you can edit an existing execution prevention rule.

This button is available if a rule is selected in the list of rules.

Delete

Clicking this button removes an execution prevention rule from the list of rules.

This button is available if a rule is selected in the list of rules.

In the **Cloud Sandbox settings** section, you can enable or disable the Cloud Sandbox component.

Cloud Sandbox

The **Cloud Sandbox** toggle switch enables/disables Cloud Sandbox technology which helps to detect advanced threats on a computer. Kaspersky Endpoint Security automatically forwards detected files to Cloud Sandbox for analysis. Cloud Sandbox runs these files in an isolated environment to identify malicious activity and decides on their reputation. Data on these files is then sent to Kaspersky Security Network. Therefore, if Cloud Sandbox detects a malicious file, Kaspersky Endpoint Security will perform the appropriate action to eliminate the threat on all computers where this file is detected.

If the **Cloud Sandbox** toggle switch is turned on, Cloud Sandbox technology is enabled.

If the **Cloud Sandbox** toggle switch is turned off, Cloud Sandbox technology is disabled.

This toggle switch is turned off by default.

Enforce

When the **Enforce** toggle switch is turned on, Kaspersky Endpoint Security prohibits changing the values of task settings, application settings, policies of subgroups, and secondary Administration Servers on a local computer.

When the **Enforce** toggle switch is turned off, Kaspersky Endpoint Security allows changing the values of task settings, application settings, policies of subgroups, and secondary Administration Servers on a local computer.

The Computer unlock settings window

Automatically unlock isolated computer in

This check box enables/disables automatic turning off of Network isolation after a specified time.

If this check box is selected, you can specify the delay for automatically turning off Network isolation of a computer.

If this check box is cleared, Kaspersky Endpoint Security turns off Network isolation 8 hours after isolation begins.

This check box is selected by default.

Hours

The interval after which Network isolation will be automatically turned off.

This field is available for editing only if the **Automatically unlock isolated computer in** check box is selected.

The Network Isolation Exclusions window

Network Isolation Exclusions

This list contains the network connections that you have added as Network isolation exclusions.

Add

Clicking this button opens a window where you can manually specify settings of the network connection to be added as an exclusion.

Add from profile

Clicking this button opens a window where you can select standard network profiles for configuring exclusions.

Delete

Clicking this button removes a network connection from the list of Network isolation exclusions.

This button is available if a connection is selected in the list of Network isolation exclusions.

The Rule options window

Rule name

Name of a Network isolation exclusion rule.

This is an optional setting.

Direction

Traffic direction.

Protocol

Protocol type.

Number

Protocol number.

The value must conform to the IANA list of Assigned Internet Protocol Numbers.

This field is available if the **Custom** protocol type is selected.

Local port or range

Local port or range of the computer for which Network isolation exclusions are being configured.

Remote port or range

Remote port or range of the computer for which Network isolation exclusions are being configured.

Remote address

Network address of the computer for which Network isolation exclusions are being configured.

Applications

This checkbox lets you to add an application that is allowed to initiate a network connection added to Network isolation exclusions on the isolated computer.

If this checkbox is selected, you can add such an application.

If this checkbox is cleared, a network connection added to Network isolation exclusions can be initiated by any application on the isolated computer.

This checkbox is cleared by default.

Add

Clicking this button opens a window where you can specify a path to an application that is allowed to initiate a network connection added to Network isolation exclusions.

Edit

Clicking this button opens a window where you can edit a path to an added application.

This button is available if an application is selected in the list.

Delete

Clicking this button deletes an added application.

This button is available if an application is selected in the list.

The Prevention rule window

Name

The rule name.

Type

Type of the object that you want to block.

In the **Path to object** section, you can select whether to specify the full path to the object to be forbidden. If you select to specify the path, enter its value in the corresponding field.

In the **Object checksum** section, you can select whether to specify the checksum for the object to be forbidden. If you select to specify the checksum, select its type and enter its value in the corresponding field.

The "Endpoint Detection and Response (KATA)" window

Endpoint Detection and Response (KATA)

The **Endpoint Detection and Response (KATA)** toggle switch enables/disables the Endpoint Detection and Response (KATA) component which interacts with the Kaspersky Anti Targeted Attack Platform solution. This solution promptly detects advanced threats, such as targeted attacks, advanced persistent threats, zero-day attacks, and others.

If the **Endpoint Detection and Response (KATA)** toggle switch is turned on, the Endpoint Detection and Response (KATA) component is enabled.

If the **Endpoint Detection and Response (KATA)** toggle switch is turned off, the Endpoint Detection and Response (KATA) component is disabled.

This toggle switch is turned off by default.

Server connection settings

Clicking this link opens a dialog where you can configure settings for connecting to KATA servers.

KATA servers

This list contains the KATA servers that you have added.

Add

Clicking this button opens a dialog where you can configure a connection to a KATA server.

Edit

Clicking this button opens a dialog where you can edit an existing connection to a KATA server.

This button is available if a server is selected in the list of servers.

Delete

Clicking this button removes a KATA server from the list of servers.

This button is available if a server is selected in the list of servers.

Address

IP address of a KATA server.

Port

Port number of a KATA server.

Send sync request to KATA server every (min)

The interval between sync requests sent to a KATA server.

The default value is 5 minutes.

Use TTL when sending events

This check box enables/disables TTL for packets sent by Kaspersky Endpoint Security to a KATA server. The TTL mechanism limits the lifespan of event packets to the value specified in the **TTL (h)** field.

If this check box is selected, TTL is enabled.

If this check box is cleared, TTL is disabled.

This check box is selected by default.

TTL (h)

The lifespan of packets sent by Kaspersky Endpoint Security to a KATA server.

The default value is 24 hours.

In the **Data transmission settings** section, you can configure settings for sending data to KATA servers.

Maximum event transmission delay (s)

The interval at which Kaspersky Endpoint Security sends events to a KATA server.

The default value is 30 seconds.

Maximum number of events per packet

The maximum number of events sent by Kaspersky Endpoint Security to a KATA server per packet.

The default value is 1024 events.

In the **Request throttling** section, you can restrict the number of transmitted events.

Enable request throttling

This check box enables/disables restricting the number of events sent by Kaspersky Endpoint Security to a KATA server.

If this check box is selected, the number of events sent by the application is restricted.

If this check box is cleared, the number of events sent by the application is not restricted.

This check box is selected by default.

Maximum number of events per hour

The maximum number of events that Kaspersky Endpoint Security sends to a KATA server per hour. Kaspersky Endpoint Security resumes sending events after an hour.

The default value is 3000 events per hour.

Percentage of event limit excess

The threshold for events of the same type (as a percentage).

Kaspersky Endpoint Security restricts transmission of events of a particular type if the ratio of events of that type to the total number of events exceeds the configured threshold.

The default value is 15 percent.

Enforce

When the **Enforce** toggle switch is turned on, Kaspersky Endpoint Security prohibits changing the values of task settings, application settings, policies of subgroups, and secondary Administration Servers on a local computer.

When the **Enforce** toggle switch is turned off, Kaspersky Endpoint Security allows changing the values of task settings, application settings, policies of subgroups, and secondary Administration Servers on a local computer.

The "KATA server" window

Address

IP address of a KATA server.

Port

Port number of a KATA server.

The default value is 443.

The "Server connection settings" window

Timeout (s)

The KATA server response timeout. When the timeout runs out, Kaspersky Endpoint Security tries to connect to a different KATA server.

The default value is 10 seconds.

In the **Server TLS certificate** section, you can add or remove a TLS certificate and view information about the certificate you added.

Add TLS certificate

Clicking this button opens a window where you can select a TLS certificate that will be used to establish a trusted connection with a KATA server.

Remove

Clicking this button removes the current TLS certificate.

This button is available if a TLS certificate has been added.

In the **Additional connection security** section, you can configure enhanced protection for the connection between Kaspersky Endpoint Security and a KATA server.

Use two-way verification

This check box enables/disables two-way verification that makes the connection between Kaspersky Endpoint Security and a KATA server more secure. To use two-way verification, you need to load a crypto-container.

If this check box is selected, Kaspersky Endpoint Security uses two-way verification to connect to a KATA server.

If this check box is cleared, Kaspersky Endpoint Security doesn't use two-way verification to connect to a KATA server.

This check box is cleared by default.

Load crypto-container

Clicking this button opens a window where you can select a crypto-container that will be used for two-way verification. The crypto-container file has the .PFX extension.

Note: The crypto-container must be password-protected. It is not possible to add a crypto-container with a blank password.

Crypto-container password

The password for the crypto-container used for two-way verification.

The "Security Controls" section

Web Control

The **Web Control** toggle switch enables/disables Web Control.

If the **Web Control** toggle switch is turned on, you can create rules to manage websites that users visit on remote computers.

If the **Web Control** toggle switch is turned off, you can't manage websites that users visit on remote computers.

This toggle switch is turned off by default.

Rule list

This list contains rules that you have created to manage websites that users visit on remote computers.

The order in which the rules are sorted determines the priority of their application by Kaspersky Endpoint Security.

Add

Clicking this button opens a window where you can create a new rule for Web Control.

Delete

Clicking this button removes the selected rule from the list of rules.

This button is available if the check box next to the rule is selected.

Move up

Clicking this button moves the selected rule up in the list of rules and raises the priority of its application by Kaspersky Endpoint Security.

Move down

Clicking this button moves the selected rule down in the list of rules and drops the priority of its application by Kaspersky Endpoint Security.

Name

The rule name.

State

The toggle switch in this column defines whether the rule is active or not.

You can turn on/off the toggle switch next to a corresponding rule to change the state of the rule.

Action

An action that Kaspersky Endpoint Security performs when the user visits a certain web address, group of web addresses, or category of websites affected by the rule.

You can change the assigned action by selecting another option in the corresponding shortcut menu in this column.

Enforce

When the **Enforce** toggle switch is turned on, Kaspersky Endpoint Security prohibits changing the values of task settings, application settings, policies of subgroups, and secondary Administration Servers on a local computer.

When the **Enforce** toggle switch is turned off, Kaspersky Endpoint Security allows changing the values of task settings, application settings, policies of subgroups, and secondary Administration Servers on a local computer.

The "Edit Rule" window

Enter rule name entry field

The rule name.

In the **State** section, you can set the rule to be active or inactive.

Active

If this option is selected, you create an active rule. It will be applied to the remote computer right after the policy is enforced.

Inactive

If this option is selected, you create an inactive rule. It will be pending when the policy is enforced.

In the **Action** section, you can select the action that Kaspersky Endpoint Security performs when the user visits a certain web address, group of web addresses, or category of websites affected by the rule.

Allow

If this option is selected, Kaspersky Endpoint Security allows the user to visit the web address, group of web addresses, or category of websites affected by the rule.

> **Note:** Kaspersky Endpoint Security allows to visit web resources on the remote computer if the **Secure connections (HTTPS) check** toggle switch is turned on in the **Network** window of the New policy wizard.

This option is selected by default.

Block

If this option is selected, Kaspersky Endpoint Security prevents the user from visiting the web address, group of web addresses, or category of websites affected by the rule.

> **Note:** Kaspersky Endpoint Security displays notifications when the user accesses web resources blocked by Web Control on the remote computer if the **Secure connections (HTTPS) check** toggle switch is turned on in the **Network** window of the New policy wizard.

Show Warning

If this option is selected, Kaspersky Endpoint Security shows a warning when the user attempts to visit the web address, group of web addresses, or category of websites affected by the rule.

In the **Rule area** section, you can choose to create a rule for a particular web address or a group of web addresses, or website categories.

Categories

If this option is selected, you create a rule for website categories.

Select categories

Clicking this link opens a dialog where you can select website categories affected by the rule.

Individual addresses

If this option is selected, you create a rule for a particular web address or a group of web addresses.

This option is selected by default.

Add

Clicking this button opens a dialog where you can specify a web address or web address mask affected by the rule.

Delete

Clicking this button removes the selected web address or web address mask from the list of web addresses affected by the rule.

This button is available if the check box next to the web address or web address mask is selected.

Address

Web addresses or web address masks affected by the rule.

The "Add web address" dialog

Enter a web address entry field

Web address or web address mask that will be affected by the rule.

The "Content categories" dialog

List of content categories

This list contains the list of website categories you can add to the rule.

The check box next to a website category name adds/removes websites belonging to this category to/from the rule.

All check boxes are cleared by default.

The Essential Threat Protection section

File Threat Protection

Clicking this link opens a window where you can set up File Threat Protection settings.

Web Threat Protection

Clicking this link opens a window where you can set up Web Threat Protection settings.

Network Threat Protection

Clicking this link opens a window where you can set up Network Threat Protection settings.

Mail Threat Protection

Clicking this link opens a window where you can set up Mail Threat Protection settings.

Firewall

Clicking this link opens a window where you can set up Firewall settings.

The "File Threat Protection" window

File Threat Protection

The **File Threat Protection** toggle switch enables/disables File Threat Protection.

If the **File Threat Protection** toggle switch is turned on, Kaspersky Endpoint Security performs real-time monitoring of the file system of the client computers to which the policy is applied.

If the **File Threat Protection** toggle switch is turned off, Kaspersky Endpoint Security doesn't protect the file system of the client computers to which the policy is applied.

This toggle switch is turned on by default.

In the **Protection scope** section, you can set up a protection scope by selecting one of the preset items or by adding files or folders of your choice.

Add

Clicking this button opens a dialog in which you can specify a file, folder, or mask to be added to the list of objects included in the protection scope.

Delete

Clicking this button removes an object from the protection scope.

This button is available if an object is selected in the list of protected objects.

You cannot delete the default objects included in the protection scope.

Protection scope

This column contains the objects that Kaspersky Endpoint Security scans when File Threat Protection is enabled.

By default, Kaspersky Endpoint Security scans the following objects:

- **All removable disks**. Kaspersky Endpoint Security scans all removable drives.
- **All internal disks**. Kaspersky Endpoint Security scans all internal drives.
- **All network disks**. Kaspersky Endpoint Security scans all network drives.

Status

If the toggle switch in this column is turned on, Kaspersky Endpoint Security scans the corresponding object in the **Protection scope** column when File Threat Protection is enabled.

If the toggle switch in this column is turned off, Kaspersky Endpoint Security doesn't scan the corresponding object in the **Protection scope** column when File Threat Protection is enabled.

Additional

This column indicates whether Kaspersky Endpoint Security scans subfolders of a corresponding object.

In the **If a malicious object is detected** section, you can select the action that Kaspersky Endpoint Security performs upon detecting a malicious object.

Prompt for action

Kaspersky Endpoint Security displays a notification window with information about the malicious object that has infected the file and prompts you to choose the action to be taken by Kaspersky Endpoint Security. Actions may vary depending on the status of the object.

This option is selected by default.

Disinfect, delete if disinfection fails

Kaspersky Endpoint Security blocks access to the infected file and attempts to disinfect it without requesting confirmation from the user.

If the file is disinfected, Kaspersky Endpoint Security saves it in its original location under the original file name. If disinfection fails, Kaspersky Endpoint Security deletes the infected file.

Disinfect, block if disinfection fails

Kaspersky Endpoint Security blocks access to the infected file and attempts to disinfect it without requesting confirmation from the user.

If the file is disinfected, Kaspersky Endpoint Security saves it in its original location under the original file name. If disinfection fails, Kaspersky Endpoint Security keeps the infected file in a blocked state in its original location.

In the **Optimization** section, you can configure scan performance and select the scanning algorithm.

Scan only new and modified files

This check box enables/disables scanning of only files that Kaspersky Endpoint Security recognizes as new or modified since the last scan.

If this check box is selected, Kaspersky Endpoint Security scans only files that it recognizes as new or modified since the last scan.

If this check box is cleared, Kaspersky Endpoint Security scans all files.

This check box is selected by default.

Skip scanning of read-only system volume

This check box disables/enables scanning of the read-only system volume by Kaspersky Endpoint Security.

If this check box is selected, Kaspersky Endpoint Security skips scanning of the read-only system volume to significantly reduce scanning time.

If this check box is cleared, Kaspersky Endpoint Security scans the read-only system volume.

This check box is selected by default.

Use iSwift

This check box enables/disables use of iSwift technology during scanning. iSwift allows Kaspersky Endpoint Security to use a special algorithm to exclude certain objects from scanning, which helps increase the scan speed.

If this check box is selected, Kaspersky Endpoint Security uses iSwift during scanning.

If this check box is cleared, Kaspersky Endpoint Security does not use iSwift during scanning.

This check box is selected by default.

In the **File types** section, you can select which files will be scanned by Kaspersky Endpoint Security when File Threat Protection is enabled.

Scan all files

Kaspersky Endpoint Security scans all file system objects that are executed, opened, or saved.

Scan applications and documents by content

Kaspersky Endpoint Security scans only objects that may be infected based on their content.

Scan applications and documents by extension

Kaspersky Endpoint Security scans only objects that may be infected based on their file extension.

The list of extensions is defined by Kaspersky and is included in Kaspersky Endpoint Security databases.

Kaspersky Endpoint Security always scans files without extensions.

In the **Compound files** section, you can select the types of compound files that Kaspersky Endpoint Security scans when File Threat Protection is enabled.

Scan archives

This check box enables/disables scanning of archives. For the list of extensions, refer to the Kaspersky Endpoint Security Help.

If the check box is selected, Kaspersky Endpoint Security scans archives.

If this check box is cleared, Kaspersky Endpoint Security skips archives during scans.

Scan installation packages

This check box enables/disables scanning of installation packages.

If this check box is selected, Kaspersky Endpoint Security scans installation packages.

If this check box is cleared, Kaspersky Endpoint Security skips installation packages during scans.

Scan embedded OLE objects

This check box enables/disables scanning of objects embedded in a file, such as Excel spreadsheets, macros, or email attachments.

If this check box is selected, Kaspersky Endpoint Security scans embedded OLE objects.

If this check box is cleared, Kaspersky Endpoint Security skips embedded OLE objects during scans.

Do not extract archives larger than MB

This check box enables/disables a limit on the size of archives to be scanned.

If this check box is selected, Kaspersky Endpoint Security skips archives larger than the specified value during scans.

If this check box is cleared, Kaspersky Endpoint Security extracts and scans archives regardless of their size.

This check box is available if the **Scan archives** check box is selected.

Postpone extraction of archives larger than MB

An option that limits the size of archives to be scanned.

If this check box is selected, Kaspersky Endpoint Security scans all archives whose size exceeds the set limit, but does so with a lower priority two minutes after detecting such an archive.

If this check box is cleared, Kaspersky Endpoint Security scans all archives with equal priority.

This check box is available if the **Scan archives** check box is selected.

Enforce

When the **Enforce** toggle switch is turned on, Kaspersky Endpoint Security prohibits changing the values of task settings, application settings, policies of subgroups, and secondary Administration Servers on a local computer.

When the **Enforce** toggle switch is turned off, Kaspersky Endpoint Security allows changing the values of task settings, application settings, policies of subgroups, and secondary Administration Servers on a local computer.

The "Add protection scope" dialog

Enter a file name, folder name, or mask entry field

Path to a file, folder, or file/folder mask.

Object is a folder

This check box enables/disables scanning of an object as a folder.

If this check box is selected, Kaspersky Endpoint Security scans the object that you have specified in the **Enter a file name, folder name, or mask** field as a folder.

If this check box is cleared, Kaspersky Endpoint Security scans the object that you have specified in the **Enter a file name, folder name, or mask** field as a file.

This check box is selected by default.

Include subfolders

This check box enables/disables scanning of subfolders in the folder specified in the **Enter a file name, folder name, or mask** field.

If this check box is selected, Kaspersky Endpoint Security scans subfolders during malware scans.

If this check box is cleared, Kaspersky Endpoint Security scans only the files directly in the folder specified in the **Enter a file name, folder name, or mask** field during malware scans.

This check box is selected by default.

The "Web Threat Protection" window

Web Threat Protection

The **Web Threat Protection** toggle switch enables/disables Web Threat Protection.

If the **Web Threat Protection** toggle switch is turned on, Web Threat Protection scans data sent and received by your computer over the HTTP and HTTPS protocols in Safari, Google Chrome, or Firefox.

If the **Web Threat Protection** toggle switch is turned off, Web Threat Protection does not scan data sent and received by your computer via web browsers.

This toggle switch is turned on by default.

In the **If a malicious object is detected** section, you can select the action that Kaspersky Endpoint Security performs upon detecting a malicious object.

Prompt for action

Kaspersky Endpoint Security displays a notification window with information about the type of malware that has infected the web traffic object and prompts you to choose the action to be taken by Kaspersky Endpoint Security on this object. The available actions may vary depending on the status of the object.

This action is selected by default.

Block automatically

Kaspersky Endpoint Security automatically blocks access to dangerous web traffic objects.

In the **Trusted web addresses** section, you can create or edit a list of trusted web addresses and enable or disable scanning of traffic from web addresses on this list.

Do not scan web traffic from trusted web addresses

This check box enables/disables scanning of web traffic from trusted web addresses.

If this check box is selected, Kaspersky Endpoint Security does not scan web traffic from trusted web addresses.

If this check box is cleared, Kaspersky Endpoint Security scans web traffic from trusted web addresses.

This check box is cleared by default.

List of web addresses

This list contains trusted web addresses.

You can clear the check box next to a web address on the list. If the check box is cleared, Web Threat Protection scans web traffic from the web address.

The list is available if the **Do not scan web traffic from trusted web addresses** check box is selected.

Add

Clicking this button opens a dialog where you can enter a web address or web address mask to be added to the list of trusted web addresses.

Delete

Clicking this button removes the selected web address or web address mask from the list of trusted web addresses.

This button is available when a web address or web address mask is selected in the list of trusted web addresses.

Web address

This column contains trusted web addresses.

Status

If the toggle switch in this column is turned on, Kaspersky Endpoint Security doesn't scan the corresponding object from the **Web address** column when Web Threat Protection is enabled and the **Do not scan web traffic from trusted web addresses** check box is selected.

If the toggle switch in this column is turned off, Kaspersky Endpoint Security scans the corresponding object from the **Web address** column when Web Threat Protection is enabled and the **Do not scan web traffic from trusted web addresses** check box is selected.

Enforce

When the **Enforce** toggle switch is turned on, Kaspersky Endpoint Security prohibits changing the values of task settings, application settings, policies of subgroups, and secondary Administration Servers on a local computer.

When the **Enforce** toggle switch is turned off, Kaspersky Endpoint Security allows changing the values of task settings, application settings, policies of subgroups, and secondary Administration Servers on a local computer.

The "Add web address" dialog

Enter a web address entry field

A web address or web address mask whose traffic will not be scanned by Web Threat Protection.

In the **Status** section, you can define whether Kaspersky Endpoint Security scans the traffic from this web address or group of web addresses.

Disable

The web address or web address mask is added to the list of **Trusted web addresses**, but Kaspersky Endpoint Security scans their traffic.

Enable

The web address or web address mask is added to the list of **Trusted web addresses** and Kaspersky Endpoint Security doesn't scan their traffic.

The "Network Threat Protection" window

Network Threat Protection

The **Network Threat Protection** toggle switch enables/disables Network Threat Protection.

If the **Network Threat Protection** toggle switch is turned on, Kaspersky Endpoint Security protects the remote computer against network attacks.

If the **Network Threat Protection** toggle switch is turned off, Kaspersky Endpoint Security does not protect the remote computer against network attacks.

This toggle switch is turned on by default.

In the **Network Threat Protection settings** section, you can modify the period for which Kaspersky Endpoint Security blocks attacking computers.

Block attacking computers for min

This check box enables/disables adding attacking computers to the list of blocked computers for the specified period.

If this check box is selected, Kaspersky Endpoint Security adds attacking computers to the list of blocked computers for the specified period.

If this check box is cleared, Kaspersky Endpoint Security does not block attacking computers.

This check box is selected by default.

By default, attacking computers are blocked for 60 minutes.

In the **Exclusions** section, you can create or edit a list of IP addresses of remote computers whose network activity will never be blocked by Kaspersky Endpoint Security.

List of IP addresses

This list contains IP addresses of remote computers whose network activity is never blocked by Kaspersky Endpoint Security.

Add

Clicking this button opens a dialog where you can enter the IP address of a remote computer.

Delete

Clicking this button removes the selected IP address from the list of IP addresses.

This button is available if the IP address of a remote computer is selected in the list of IP addresses.

Enforce

When the **Enforce** toggle switch is turned on, Kaspersky Endpoint Security prohibits changing the values of task settings, application settings, policies of subgroups, and secondary Administration Servers on a local computer.

When the **Enforce** toggle switch is turned off, Kaspersky Endpoint Security allows changing the values of task settings, application settings, policies of subgroups, and secondary Administration Servers on a local computer.

The "Add exclusion" dialog

Enter an IP address entry field

IP address of a remote computer.

The "Advanced Threat Protection" section

In the **KSN settings** section, you can configure the use of Kaspersky Security Network.

Kaspersky Security Network

The **Kaspersky Security Network** toggle switch enables/disables participation in Kaspersky Security Network.

If the **Kaspersky Security Network** toggle switch is turned on, the client computers to which the policy is applied participate in Kaspersky Security Network.

If the **Kaspersky Security Network** toggle switch is turned off, the client computers to which the policy is applied do not participate in Kaspersky Security Network.

This toggle switch is turned off by default.

Extended KSN mode

The **Extended KSN mode** toggle switch enables/disables sending of additional data from the remote computer to Kaspersky in order to improve protection of client computers and the usability of Kaspersky Endpoint Security.

If **Extended KSN mode** is turned on, client computers under the policy provide both data required for detection services functioning and additional data to Kaspersky Security Network.

If **Extended KSN mode** is turned off, client computers under the policy provide only data required for detection services functioning and don't provide additional data to Kaspersky Security Network.

The **Extended KSN mode** toggle switch is turned off by default.

The toggle switch is turned on automatically if you turn on the **Kaspersky Security Network** toggle switch, but you can turn it off.

Data provided to Kaspersky when using Kaspersky Security Network in Global KSN infrastructure

If the **Kaspersky Security Network** toggle switch is enabled and the **Extended KSN mode** toggle switch is disabled, Kaspersky Endpoint Security running on client computers provides to Kaspersky the following data:

- Information about the license used: the type and validity period of the license, number of days till license expiration, identifier of the partner from whom the license was purchased, Regional Activation Center identifier, checksum of the activation code, ticket body hash calculated using the SHA1 algorithm, license ticket creation date and time, license information identifier, license ticket identifier, license ticket sequence identifier, unique identifier of the user's computer, date from which the license ticket is valid, date to which the license ticket is valid, license ticket current state, ticket header version, license version, ticket header signature certificate identifier, checksum of the key file, ticket header signer serial number, authentication token.

- Full version of installed Software; type of installed Software; Software update ID; ID of reputation service; protocol type ID; ID of a regional activation center; version of list of revoked Software service's decisions; ID of the triggered record in the Software's anti-virus databases; timestamp of the triggered record in the Software's anti-virus databases; type of the triggered record in the Software's anti-virus databases; unique ID of the instance of application installation on the computer; license activation date; license expiration date; license identifier; status of the license used by the Software; checksum type for the object being processed; name of the detected malware or legitimate software that can be used to damage the user's device or data; checksum of the object being processed; checksum of the Software activation code; full version of the Software; unique device ID; Software ID; checksum of the Software key file; ID of the information model used to provide the Software license; identifier of the certificate used to sign the Software license ticket header; the Software license ticket create date and time; the Software license ticket checksum; the Software license ticket version; the Software activation code version; format of the data in the request to Rightholder infrastructure; current license ticket ID; the Software component ID; the result of the Software action; error code; accessed address of the web service (URL, IP); port number; web address of the source of the web service request (referrer); public key of the certificate; digital certificate thumbprint of the scanned object and hashing algorithm.

If the **Kaspersky Security Network** and **Extended KSN mode** toggle switches are enabled, Kaspersky Endpoint Security running on client computers provides to Kaspersky the following data:

- Information about the version of the operating system (OS) and service packs installed on the computer, version and checksums (MD5, SHA2-256, SHA1) of the OS kernel file, parameters of the OS run mode; OS version, OS build number, OS update number, OS edition, extended information about the OS edition; OS Service Pack version; date and time of the OS launch; processing delay time of the event about OS action in the behavioral analysis subsystem; number of delayed OS action events of the current type; processing delay time of the event about OS action in the proactive defense subsystem; number of processed OS action events; number of processed synchronous OS action events; total delay of all OS action events of the current type; processing delay time of the event about OS action in the persistent event storage subsystem; total delay of all OS action events; number of waiting synchronous OS action events; date and time of received event of an action in the OS.

- Information about the failed last OS reboot: number of failed reboots.

- Information about the Rightholder's installed application and the anti-virus protection status: Software installation ID (PCID); Software database record version; unique identifier of the instance of application installation on the computer, application type, ID of application type, the full version of the application installed, the identifier of the application settings version, the identifier of the computer type, the unique identifier of the computer on which the application is installed, the unique User identifier in the Rightholder's services, locale language and operation state, version of the installed Software components and their operation state, version of the protocol used to connect with the Rightholder's services; full version of installed Software; type of installed Software; Software update ID; ID of reputation service; protocol type ID; ID of a regional activation center; version of list of revoked Software service's decisions; ID of the triggered record in the Software's anti-virus databases; timestamp of the triggered record in the Software's anti-virus databases; type of the triggered record in the Software's anti-virus databases; Unique ID of the instance of application installation on the computer; license activation date; license expiration date; license identifier; status of the license used by the Software; checksum type for the object being processed; name of the detected malware or legitimate software that can be used to damage the user's device or data; checksum of the object being processed; checksum of the Software activation code; full version of the Software; Software ID; checksum of the Software key file; ID of the information model used to provide the Software license; identifier of the certificate used to sign the Software license ticket header; the Software license ticket create date and time; the Software license ticket checksum; the Software license ticket version; the Software activation code version; format of the data in the request to Rightholder infrastructure; current license ticket ID; the Software component ID; the result of the Software action; error code; accessed address of the web service (URL, IP); port number; web address of the source of the web service request (referrer); number of update-apply cycles for anti-virus databases; date and time when the anti-virus databases were last updated and applied; release date and time of the Software's databases; version of the Software's component; Software update ID; type of the installed Software; date and time of System Watcher start; installation date and time for the Software; probability of sending statistics by System Watcher; code of the event that took longer than the standard time to process by System Watcher; database processing time of the event that took longer than the standard time to process by System Watcher; maximum allowed time for processing an event by System Watcher; processing time of the event that took longer than the standard time to process by System Watcher; total number of events that took longer than the standard time to process by System Watcher.

- Information about all processed objects and operations: Software verdict on the object being processed; directory code; size of the object being processed; checksum (SHA256) of the object being processed; number of the detected software in the System Watcher context; date and time of detecting software by System Watcher; detect characteristics; ID of the triggered record in the Software's anti-virus databases; reason of detecting software by System Watcher; checksum (MD5) of the object being processed; result of the module integrity check; name of the object being processed; type of the triggered Software anti-virus databases record; path to the object being processed; the name of the scanned object; the date and time of the scan; the URL- and Referrer addresses from which it was downloaded; the size of scanned files and the paths to them; the archive sign; the date and time of the file's creation; the name, size and checksums (MD5, SHA2-256) of the packer (if the file was packed); the file's entropy; the file's type; the file type code; the executable file sign, ID and format; the object's checksum (MD5, SHA2-256); the type and value of the object's supplementary checksum; data about the object's digital signature (certificate): data on the certificate's publisher, number of starts of the object since the last statistics delivery, ID of the application's scanning task, the means of receiving information about the object's reputation, the value of the target filter, technical parameters of the applicable detection technologies; path to the object being processed; directory code.

- For executable files: the entropy of the file sections, reputation verification flag or file signature flag, name, type, ID type, checksum (MD5) and the size of the application that was loaded by the object being validated, the application path and template paths, an attribute indicating presence in the Autorun list, date of entry, the list of attributes, name of the packer, information about the digital signature of the application: the publisher certificate, the name of the uploaded file in the MIME format, file build date and time.

- Information about the applications launched and their modules: checksums (MD5, SHA2-256) of running files, size, attributes, creation date, name of the packer (if the file was packed), names of files, information about processes running on the system (process ID (PID), process name, information about the account the process was started from, the application and command that started the process, the full path to the process's files, and the starting command line, a description of the application that the process belongs to (the name of the application and information about the publisher), as well as the digital certificates being used and information needed to verify their authenticity or information about the absence of a file's digital signature), and information about the modules loaded into the processes: their names, sizes, types, creation dates, attributes, checksums (MD5, SHA2-256, SHA1), the paths to them, PE-file header information, names of packers (if the file was packed), information about the availability and validity of these statistics, identifier of the mode for generating the statistics being sent.

- If threats or vulnerabilities are detected, in addition to information about the detected object, information is provided about the identifier, version, and type of the record in the anti-virus database, the name of the threat based on the Kaspersky classification, the date and time of the last update of the anti-virus database, executable file name, the checksum (MD5) of the application file that requested the URL where the threat was detected, the IP address (IPv4 or IPv6) of the detected threat, the vulnerability identifier and its threat level, the URL and Referrer of the web page where the vulnerability was detected.

- If a potentially malicious object is detected, information is provided about data in the processes' memory.

- Network attack information: IP address of the attacking computer and number of the port on the user's computer targeted by the network attack, ID of the attack protocol, name and type of attack.

- Information about network connections: version and checksums (MD5, SHA2-256, SHA1) of the file from which process was started that opened the port, the path to the process's file and its digital signature, local and remote IP addresses, numbers of local and remote connection ports, connection state, timestamp of the port's opening.

- The URL and IP address of the web page where harmful or suspicious content was detected, the name, size, and checksum of the file that requested the URL, the identifier, weight and degree of the rule used to reach a verdict, the objective of the attack.

- Information about updates of the installed application and anti-virus databases: status of completion of the update task, type of error that may have occurred during the update process, the number of unsuccessful updates, the identifier of the application component that performs updates.

- Information about the use of Kaspersky Security Network (KSN): KSN identifier, application identifier, full version of the application, depersonalized IP address of the user's device, indicators of the quality of fulfillment of KSN requests, indicators of the quality of the processing of KSN packets, indicators of the number of KSN requests and information about the types of KSN requests, date and time when statistics began being sent, date and time when statistics finished being sent, information about KSN configuration updates: identifier of the active configuration, identifier of the configuration received, error code of the configuration update.

- Information about system log events: event time, name of the log where the event has been detected, type and category of event, name of the event source and event description.

- Information to determine the reputation of files and URL-addresses: the URL-address at which the reputation is being requested and the Referrer, the connection's protocol type, the internal identifier of the application type, the number of the port being used, the User identifier, checksum of the scanned file (MD5), type of the detected threat, information about the record used to detect a threat (record identifier for the anti-virus databases, the record timestamp and type); public key of the certificate; digital certificate thumbprint of the scanned object and hashing algorithm.

- Data on the application territorial distribution: date of the application installation and activation, ID of the partner providing the license for the application activation, application ID, application language localization ID, license serial number for the application activation, KSN participation sign.

- Information about the license used: the type and validity period of the license, number of days till license expiration, identifier of the partner from whom the license was purchased, Regional Activation Center identifier, checksum of the activation code, ticket body hash calculated using the SHA1 algorithm, license ticket creation date and time, license information identifier, license ticket identifier, license ticket sequence identifier, unique identifier of the user's computer, date from which the license ticket is valid, date to which the license ticket is valid, license ticket current state, ticket header version, license version, ticket header signature certificate identifier, checksum of the key file, ticket header signer serial number, authentication token.

- Information about hardware installed on the computer: type, name, model name, firmware version, parameters of built-in and connected devices.

- Information about the device: device ID.

- Information about the operation of the Web Control component: component version, categorization reason, additional information about categorization reason, categorized URL, host IP address of blocked/categorized object.

Cloud mode

The **Cloud mode** toggle switch enables/disables the application operating mode in which Kaspersky Endpoint Security uses a light version of anti-malware databases. This mode is available only if the participation in Kaspersky Security Network is enabled. The light version of anti-malware databases lets you use approximately half of the computer RAM that would otherwise be used with the full databases. If you do not participate in Kaspersky Security Network or if cloud mode is disabled, Kaspersky Endpoint Security downloads the full version of anti-malware databases from Kaspersky servers.

If the toggle button is switched on, Kaspersky Endpoint Security uses the light version of anti-malware databases, which reduces the load on operating system resources.

Note: Kaspersky Endpoint Security downloads the light version of anti-malware databases during the next update after the check box was selected.

If the toggle button is switched off, Kaspersky Endpoint Security uses the full version of anti-malware databases.

Note: Kaspersky Endpoint Security downloads the full version of anti-malware databases during the next update after the check box was cleared.

KSN Statement

Clicking this link opens a window where you can read the text of the Kaspersky Security Network Statement and accept the terms of participation in Kaspersky Security Network.

Note: If you manage Kaspersky Endpoint Security via Kaspersky Security Center Web Console and depending on Kaspersky Security Center settings, you can participate in Kaspersky Private Security Network instead of Kaspersky Security Network. If you manage Kaspersky Endpoint Security via Kaspersky Security Center Cloud Console, participation in Kaspersky Private Security Network is unavailable. For detailed information about participating in Kaspersky Private Security Network, see the Kaspersky Security Center Help.

In the **KSN Proxy settings** section, you can configure the KSN Proxy settings.

Use KSN Proxy

This check box enables/disables the use of a proxy server when connecting to Kaspersky Security Network.

If the check box is selected, Kaspersky Endpoint Security uses a proxy server to connect to Kaspersky Security Network.

If the check box is cleared, Kaspersky Endpoint Security connects to Kaspersky Security Network directly.

This check box is cleared by default.

Use Kaspersky servers when KSN Proxy is unavailable

This check box enables/disables use of Kaspersky services if the KSN proxy is not available.

If this check box is selected, Kaspersky Endpoint Security uses Kaspersky servers when the KSN proxy is unavailable.

If this check box is cleared, Kaspersky Endpoint Security does not use Kaspersky servers when the KSN proxy is unavailable.

This check box is cleared by default.

This check box is available if the **Use KSN Proxy** check box is selected.

Enforce

When the **Enforce** toggle switch is turned on, Kaspersky Endpoint Security prohibits changing the values of task settings, application settings, policies of subgroups, and secondary Administration Servers on a local computer.

When the **Enforce** toggle switch is turned off, Kaspersky Endpoint Security allows changing the values of task settings, application settings, policies of subgroups, and secondary Administration Servers on a local computer.

The "Participation in Kaspersky Security Network/Kaspersky Private Security Network" window

Learn more

Clicking this link opens a new browser window where you can read the text of the Kaspersky Security Network Statement or Kaspersky Private Security Network Statement.

I accept the terms of participation in Kaspersky Security Network/Kaspersky Private Security Network

The computers to which the policy is applied participate in Kaspersky Security Network/Kaspersky Private Security Network.

I do not accept the terms of participation in Kaspersky Security Network/Kaspersky Private Security Network

The computers to which the policy is applied don't participate in Kaspersky Security Network/Kaspersky Private Security Network.

Note: If you manage Kaspersky Endpoint Security via Kaspersky Security Center Cloud Console, participation in Kaspersky Private Security Network is unavailable. For detailed information about participating in Kaspersky Private Security Network, see the Kaspersky Security Center Help.

The "Grant access" dialog

Get recovery key

Clicking this button generates a recovery key required to access an encrypted disk on a client computer.

Manage the application from the command line

You can manage the Kaspersky Endpoint Security application from the command line.

Note: After updates of Kaspersky Endpoint Security modules are installed, the version of the application client in the command line may differ from the installed version of the application.

Command line syntax:

```
kav <command> <parameters>
```

Each command has its own range of supported parameters.

View command line help

Use the following command to view information about the application command line syntax:

```
kav -? | help
```

Run malware scan

Command syntax:

```
kav scan <scan scope> <action> <file types> <exclusions> <report parameters> <advanced parameters>
```

Note: To run a malware scan, you can also use tasks created in the application by starting one from the command line. The task is started with the parameters that are specified in the Kaspersky Endpoint Security interface.

Parameter descriptions

`<scan scope>` – This parameter specifies a list of objects that are to be scanned for malicious code. You can include several parameters separating them with a space.

Note: Kaspersky Endpoint Security does not scan files that are located in OneDrive or iCloud storage or other cloud storages. Please exclude these files from the scan scope. Otherwise, the scan task may finish with the *Infected File Not Deleted* error.

The following values are possible:

- `<files>` – List of paths to files and/or folders to be scanned. You can specify absolute or relative paths to the files. Items in the list are separated by a space.

  > **Note:** If the name of an object or the path to it includes a space or special characters (such as $, &, or @), the name should be encased in single quotes (' '), or each of the special characters should be escaped by adding a backslash (\) immediately before it. If reference is made to a specific folder, all files and folders in this folder are scanned.

- `-all` – Full scan of your computer.
- `-remdrives` – All removable drives.
- `-fixdrives` – All internal drives.
- `-netdrives` – All network drives.
- `-@:<filelist.lst>` – Path to the file with a list of objects and folders within the scan scope. The file must be in text format and each scan object must be listed in a separate line. Only an absolute path to the file may be entered.

`<action>` – This parameter determines the action to take on malicious objects that are detected during the scan. If this parameter is not defined, the default action is the one corresponding to the value `-i8`.

The following values are possible:

- `-i0` – Take no actions on the object, only save information about the object in a report.
- `-i1` – Disinfect infected objects, skip them if they cannot be disinfected.
- `-i2` – Disinfect infected objects, delete them if they cannot be disinfected; do not delete containers, except for those with executable headers (SFX archives).
- `-i3` – Disinfect infected objects, delete them if they cannot be disinfected; delete containers completely if infected files inside them cannot be deleted.
- `-i4` – Delete infected objects; delete containers completely if infected files inside them cannot be deleted.
- `-i8` – Prompt the user for action if an infected object is detected (used by default).
- `-i9` – Prompt the user for action when the scan is completed.

`<file types>` – This parameter defines the file types that are subject to malware scan. By default, if this parameter is not defined, only files that may be potentially infected (based on the file contents) are scanned.

The following values are possible:

- `-fe` – Scan only files that may be potentially infected (based on the file extension).
- `-fi` – Scan only files that may be potentially infected (based on the file content). This parameter is used by default.
- `-fa` – Scan all files.

<exclusions> – This parameter defines the objects to exclude from scanning. You can include several parameters separating them with a space.

The following values are possible:

- -e:a – Do not scan archives.
- -e:b – Do not scan email databases.
- -e:m – Do not scan email messages in text format.
- -e:<mask> – Do not scan objects by mask.
- -e:<seconds> – Skip objects that are scanned for longer than the specified length of time (in seconds).
- -es:<size> – Skip objects with size larger than the specified value (in megabytes).

<report parameters> – These parameters define the format of the report containing the scan results. You can specify an absolute or relative path to the report file. If this parameter is not defined, scan results are displayed and all events are shown.

The following values are possible:

- -r:<report file> – Log only important events to the specified report file.
- -ra:<report file> – Log all events to the specified report file.

<advanced parameters> – Parameters that define the use of malware scan technologies and configuration files:

- -iSwift=<on|off> – Enable/disable the use of iSwift.
- -c:<configuration file> – Define the path to the configuration file that contains the application settings for malware scan tasks. You can specify an absolute or relative path to the file. If this parameter is not specified, the values set in the application interface are used together with the values that are already specified in the command line.

Example:
Start scan of the folders ~/Documents, /Applications, and the file named my test.exe:

```
kav scan ~/Documents /Applications 'my test.exe'
```

Scan the objects listed in the file objects2scan.txt. Use the scan_settings.txt configuration file. When the scan is complete, create a report to log all events:

```
kav scan -@:objects2scan.txt -c:scan_settings.txt -ra:scan.log
```

A sample configuration file:

```
-netdrives -@:objects2scan.txt -ra:scan.log
```

Update the application

Command syntax:

```
kav update <update source> <report parameters> <advanced parameters>
```

Parameter descriptions

`<update source>` – An HTTP server or a network or local folder from which updates are downloaded. If a path is not selected, the update source will be taken from the application update settings.

`<report parameters>` – These parameters define the format of the report on the scan results. You can specify an absolute or relative path to the report file. If this parameter is not defined, update results are displayed and all events are shown.

The following values are possible:

- `-r:<report file>` – Log only important events to the specified report file.
- `-ra:<report file>` – Log all events to the specified report file.

`<advanced parameters>` – A parameter that defines use of a configuration file.

`-c:<configuration file>` – Defines the path to a configuration file that contains the application settings for updating the application. You can specify an absolute or relative path to the file. If this parameter is not defined, the values set in the application interface are used.

Example:
Update the application databases from the default source, logging all events in the report:

```
kav update -ra:avbases_upd.txt
```

Update the Kaspersky Endpoint Security modules using the parameters of the updateapp.ini configuration file:

```
kav update -app=on -c:updateapp.ini
```

Roll back the last update

Command syntax:

```
kav rollback <report parameters>
```

Important: Administrator rights are required to run this command.

Parameter descriptions

`<report parameters>` – This parameter defines the format of the report containing the results of the update rollback. You can specify an absolute or relative path to the report file. If this parameter is not defined, rollback results are displayed and all events are shown.

The following values are possible:

- `-r:<report file>` – Log only important events to the specified report file.
- `-ra:<report file>` – Log all events to the specified report file.

Example:
`kav rollback -ra:rollback.txt`

Start/stop a component or task

The start command syntax:

```
kav start <task or component name> <report parameters>
```

The stop command syntax:

```
kav stop <task or component name>
```

Important: Administrator rights are required to run the stop command.

Parameter descriptions

`<task or component name>` – Specify one of the following values:

- `fm` or `file_monitoring` – File Threat Protection
- `wm` or `web_monitoring` – Web Threat Protection
- `ids` – Network Threat Protection
- `full` or `scan_my_computer` – Full Scan task
- `scan_objects` – Custom Scan task
- `quick` or `scan_critical_areas` – Quick Scan task
- `updater` – Update task
- `rollback` – Rollback task

`<report parameters>` – These parameters define the format of the report on the component or task results. You can specify an absolute or relative path to the report file. If this parameter is not defined, Kaspersky Endpoint Security displays results in accordance with parameters configured in the graphical user interface.

Note: `<report parameters>` is only available for `scan_objects`, `updater`, and `rollback` values.

The following values are possible:

- `-r:<report file>` – Kaspersky Endpoint Security logs only important events to the specified report file.
- `-ra:<report file>` – Kaspersky Endpoint Security logs all events to the specified report file.

Note: Components and tasks started from the command prompt are run with the parameters configured in the graphical user interface.

Example:
To enable the File Threat Protection component, enter the following command in the command line:

```
kav start fm
```

To stop the Full Scan task from the command line, enter the following command:

```
kav stop scan_my_computer
```

View status and statistics of a component or task

The status command syntax:

```
kav status <task or component name>
```

The statistics command syntax:

```
kav statistics <task or component name>
```

Parameter descriptions

`<task or component name>` – Specify one of the following values:

- `fm` or `file_monitoring` – File Threat Protection
- `wm` or `web_monitoring` – Web Threat Protection
- `mail_monitoring` – Mail Threat Protection
- `ids` – Network Threat Protection
- `firewall` – Firewall
- `behaviordetection` – Behavior Detection
- `exploitprevention` – Exploit Prevention
- `remediationengine` – Remediation Engine
- `devicecontrol` – Device Control
- `webcontrol` – Web Control

- `full` or `scan_my_computer` – Full Scan task
- `scan_objects` – Custom Scan task
- `quick` or `scan_critical_areas` – Quick Scan task
- `externalstoragesscanner` – Removable Disk Scan task
- `updater` – Update task
- `rollback` – Rollback task
- `diskencryption` – FileVault Disk Encryption
- `edroptimum` – Endpoint Detection and Response Optimum
- `edrkata` – Endpoint Detection and Response (KATA)
- `cloudsandbox` – Cloud Sandbox
- `mdr` – Managed Detection and Response

Note: If the status command is run without specifying a value for the `<task or component name>` parameter, the status of all tasks and components of the application is displayed. For the statistics command, a value must be specified for the `<task or component name>` parameter.

Export protection settings

Command syntax:

```
kav export <task or component name> <export file>
```

Parameter descriptions

`<task or component name>` – Specify one of the following values:

- `fm` or `file_monitoring` – File Threat Protection
- `wm` or `web_monitoring` – Web Threat Protection
- `ids` – Network Threat Protection
- `full` or `scan_my_computer` – Full Scan task
- `scan_objects` – Custom Scan task
- `quick` or `scan_critical_areas` – Quick Scan task

- `updater` – Update task
- `rollback` – Rollback task

`<export file>` – Path to the file to which the application settings are exported. You can specify an absolute or relative path to the file.

Example:
```
kav export fm fm_settings.txt
```

Activate the application

You can activate Kaspersky Endpoint Security by applying a key file.

Command syntax:

```
kav license /add <key file or key activation code>
```

Parameter descriptions

`<key file>` – Application key file with .key extension.

`<key activation code>` – Activation code in XXXX-XXXX-XXXX-XXXX format.

Example:
```
kav license /add ./1AA111A1.key
kav license /add A11A1-11111-1A1AA-1A11A
```

Install the system extension

Command syntax:

```
kav activatesystemextension /sysext
```

Note: You need to grant Kaspersky Endpoint Security permissions in the **Privacy & Security** settings to finish installing the extension.

Configure network connections

You can configure network connections for Web Threat Protection and Network Threat Protection components.

Command syntax:

```
kav activatesystemextension /webav
```

Note: You need to grant Kaspersky Endpoint Security permissions for network content filtering to finish the configuration.

Remove license keys

You can remove all license keys that are currently added to the application.

Command syntax:

```
kav license /del
```

Important: Administrator rights are required to run this command.

Return codes of the command line

The general codes may be returned by any command from the command line. The return codes include general codes as well as codes specific to a certain task.

Syntax of the command for receiving the return code:

```
echo $?
```

General return codes:

- `0` – Operation completed successfully
- `1` – Invalid parameter value
- `2` – Unknown error
- `3` – Task completion error
- `4` – Task canceled

Malware scan task return codes:

- `101` – All malicious objects processed
- `102` – Malicious objects detected

Quit the application

Command syntax:

```
kav exit
```

Important: Administrator rights are required to run this command.

Uninstall the application

Use the following sequence of commands to uninstall Kaspersky Endpoint Security from the command line:

```
sudo /Library/Application\ Support/Kaspersky\ Lab/klnagent/Binaries/UninstallScript
sudo /Library/Application\ Support/Kaspersky\ Lab/KAV/Binaries/UninstallScript
sudo rm -rf /Library/Application\ Support/Kaspersky\ Lab/ /Applications/Kaspersky
```

Important: Administrator privileges are required to uninstall the application.

Detection and Response management commands

You can use the command line to manage built-in functionality of the Detection and Response solution. You can manage Detection and Response solutions if management using the Kaspersky Security Center console is not possible.

Manage Execution prevention

You can view the client computer's Execution prevention settings and disable Execution prevention on the client computer.

Command syntax:

```
kav prevention </disable | /show>
```

Command descriptions

`/disable` - The command for turning off the Execution prevention on the client computer.

`/show` - The command for displaying the current Execution prevention settings, including the mode and the list of execution prevention rules.

Manage Network isolation

You can view the host's Network isolation settings and disable Network isolation on the host.

Command syntax:

```
kav isolation </off | /status>
```

Command descriptions

`/off` - The command for turning off Network isolation.

Important: Administrator rights are required to run this command.

`/status` - The command for displaying the Network isolation status and exclusions.

Note: These commands must be run simultaneously.

Contact Technical Support

This section describes how to get technical support and the terms on which it is available.

How to get technical support

If you can't find a solution to your issue in the Kaspersky Endpoint Security documentation or in any of the sources of information about Kaspersky Endpoint Security, contact Kaspersky Technical Support. Technical Support specialists will answer all your questions about installing and using Kaspersky Endpoint Security.

Note: Kaspersky provides support of Kaspersky Endpoint Security during its lifecycle (see the application support lifecycle page). Before contacting Technical Support, please read the support rules.

You can contact Technical Support in one of the following ways:

- By visiting the Technical Support website
- By sending a request to Technical Support from the Kaspersky CompanyAccount portal

Technical support via Kaspersky CompanyAccount

Kaspersky CompanyAccount is a portal for companies that use Kaspersky applications. The Kaspersky CompanyAccount portal is designed to facilitate interaction between users and Kaspersky specialists through online requests. You can use Kaspersky CompanyAccount to track the status of your online requests and store a history of them as well.

You can register all of your organization's employees under a single account on 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.

Acquire information for Technical Support

For more effective support and troubleshooting of application problems, Technical Support specialists may ask you to change application settings temporarily for purposes of debugging during diagnostics. This may require doing the following:

- Activating the functionality that extracts extended diagnostic information.
- Fine-tuning the settings of individual application components, which are not available via standard user interface elements.
- Changing the settings of transmission of diagnostic information that is extracted.

Technical Support specialists will provide you with all the information needed to perform the listed operations and inform you about the scope of data to be acquired for debugging purposes. After the extended diagnostic information is extracted, it is saved on the user's computer. The data is not sent to Kaspersky automatically.

Use a trace file

After you report a problem to Kaspersky Technical Support specialists, they may ask you to generate a report with information about the operation of Kaspersky Endpoint Security and send it to Kaspersky Technical Support. Kaspersky Technical Support specialists may also ask you to create a *trace file*. The trace file makes it possible to perform a step-by-step examination of the execution of application commands and determine when errors occur.

Create a trace file

Tracing is an effective way of recording detailed information about application activity. Technical Support specialists use trace files to troubleshoot issues.

Create a trace file

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.

2. On the **Interface** tab, in the **Traces** section, select the **Enable tracing** checkbox.

Important: We recommend that you enable tracing only if asked to do so by a Kaspersky Technical Support specialist.

Trace files may require a lot of disk space. When you no longer need trace files, disable tracing.

Disable tracing

1. In the menu bar, click the application icon and choose **Settings**.

   The application settings window opens.

2. On the **Interface** tab, in the **Traces** section, deselect the **Enable tracing** checkbox.

Kaspersky Endpoint Security saves the following information in a trace file:

- Information about the device and operating system (unique device ID, device type, MAC addresses of network devices, operating system type, operating system version).
- Information about the operation of the application and its modules.
- Information about the subscription (subscription type, region).
- Information about the language locale, application ID, application customization, application version, unique application installation ID, unique computer ID.
- Information about the anti-malware protection status of the computer, as well as all processed and detected objects (the name of the detected object, date and time of detection, the web address from which it was downloaded, the names and sizes of infected files and paths to them, the IP address of the attacking computer and the number of the computer port targeted by the network attack, list of malware activity, and unwanted web addresses), and the relevant actions and decisions taken by the application and the user.
- Information about applications downloaded by the user (web address, attributes, file size, and information about the process that downloaded the file).
- Information about the launched applications and application modules (size, attributes, creation date, PE header details, region, name, location, and packers).
- Information about interface errors and usage of the interface of the installed Kaspersky application.
- Information about network connections: the IP address of the remote computer and the user's computer, the numbers of ports used to establish the connection, and the network protocol of the connection.
- Information about network packets received and sent by the computer over IT and telecom networks.
- Information about email and instant messages sent and received.
- Information about web addresses visited: the time when the connection was established using an open protocol, data on the website login and password, and the content of cookies.
- Public certificate of the server.

Trace files contain only the information necessary to fix defects in the application. Kaspersky uses trace files to investigate incidents associated with errors in the operation of the Kaspersky Endpoint Security application.

By default, the creation of trace files is disabled. You can enable generation of trace files in the application settings.

Trace files can only be manually sent to Kaspersky. The application does not send trace files to Kaspersky automatically.

You can choose how trace files are sent to Kaspersky.

Before sending trace files to Kaspersky, please review the data they contain.

Important: Trace files may contain personal or sensitive information. By sending trace files to Kaspersky, you agree to provide to Kaspersky all data contained in the trace files you send and you consent to the method used to send them.

Sources of information about the application

Kaspersky Endpoint Security page on the Kaspersky website

On the Kaspersky Endpoint Security page on the Kaspersky website, you can view general information about the application, its functions, and features.

Kaspersky Endpoint Security page in the Knowledge Base

The *Knowledge Base* is a section on the Kaspersky Technical Support website.

On the Kaspersky Endpoint Security page in the Knowledge Base, you can read articles that provide useful information, recommendations, and answers to frequently asked questions on how to buy, install, and use the application.

Articles in the Knowledge Base may provide answers to questions that relate both to Kaspersky Endpoint Security as well as to other Kaspersky applications. Articles in the Knowledge Base may also contain Kaspersky Technical Support news.

Go to the Knowledge Base from the Help pull-down menu

1. Choose **Help** > **Support**.
2. Click **Technical Support**.

Discuss Kaspersky applications on Kaspersky Support Forum

If your question does not require an immediate answer, you can discuss it with Kaspersky experts and other users on our Forum.

On the Forum, you can view discussion topics, post your comments, and create new discussion topics.

Go to the Forum from the Help pull-down menu

1. Choose **Help** > **Support**.
2. Click **Community**.

> **Note:** An internet connection is required to access website resources.

If you can't find a solution to your problem, contact Kaspersky Technical Support.

Help materials included with the application

The application includes full help and context help.

Full help provides information on how to configure and use Kaspersky Endpoint Security.

Context help provides information about Kaspersky Endpoint Security windows, describes Kaspersky Endpoint Security settings, and contains links to task descriptions where those settings are used.

Help can be included in the distribution kit or located on the Kaspersky website. An internet connection is required for viewing online help.

Online help (this help)

In this help, you can find information on how to:

- Prepare for the installation of the application, install and activate the application.
- Configure and use the application.
- Remotely manage the application via Kaspersky Security Center.

Appendices

This section provides information that complements the document text.

Known issues and limitations

Kaspersky Endpoint Security has following known issues and limitations:

- If an application that collects information and sends it to be processed is installed on your computer, the Kaspersky Endpoint Security application may classify this application as malware. To avoid this, you can exclude the application from scanning by configuring the Kaspersky Endpoint Security application as described in this document.
- Application functional settings can be modified by editing configuration files.
- In Kaspersky Security Center, local tasks may be listed twice in the properties of managed devices.
- Changing the update source for a local update task disables automatic execution of the update task.
- If you start a computer restart task via Administration Console with a message to the user that contains a semicolon (;), the task is displayed as completed but the user is not prompted to restart their Mac.
- To exclude Safari network traffic from scanning by Kaspersky Endpoint Security, you need to add the following paths to the exclusion list:
  - `/System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.N`
  - `/System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.N`
  - `/System/Library/PrivateFrameworks/SafariShared.framework/Versions/A/XPCServices/com.a`
  - `/System/Library/Frameworks/webkit2.framework/versions/a/xpcservices/com.apple.webkit`
- To exclude Google Chrome network traffic from scanning by Kaspersky Endpoint Security, you need to add the following path to the exclusion list:
  - `/Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/<VersionNumber>/Helpers/Google Chrome Helper.app/Contents/MacOS/Google Chrome Helper`
- After you create a policy profile for a Kaspersky Endpoint Security policy using Kaspersky Security Center Web Console and Cloud Console, you need to check that the settings are applied correctly on client computers.
- When enabling FileVault disk encryption in policy settings, users with administrator rights can decrypt the startup disk of their Mac from System Settings (System Preferences).
- Changes in the proxy server options will be applied only after Kaspersky Endpoint Security is restarted.
- Safari might not connect to a website with an untrusted certificate. You can add such a website to the exclusions or use another browser.

- After uninstalling Kaspersky Endpoint Security 11.2 or later remotely via Kaspersky Security Center, one of the application's system extension may remain in computer memory. After that, in rare cases, a problem with the full disk access permission may occur when installing Kaspersky Endpoint Security. In this case, we recommend to uninstall the application locally and reinstall it.
- The applications that need Rosetta might not be installed if Kaspersky Endpoint Security is running. To resolve the problem, quit Kaspersky Endpoint Security and try to reinstall the application.
- Alert details for threats detected within compound objects contain information only about the detected object itself without a graph of the threat development chain.
- When saving a password for Password protection, an error may occur. In this case, we recommend to uninstall and reinstall the application.
- Kaspersky Endpoint Security does not scan files that are located in OneDrive or iCloud storage or other cloud storages. Please exclude these files from the scan scope. Otherwise, the scan task may finish with the *Infected File Not Deleted* error.
- You cannot scan an object quarantined as a result of the Move file to Quarantine task.
- In Kaspersky Security Center, the device name is displayed correctly only if the NetBIOS name, computer name, and host name are the same.

List of objects scanned by extension

If when creating a scan task in Kaspersky Security Center, in the scan settings you have selected the **Scan applications and documents by extension** option, Kaspersky Endpoint Security performs malware scans on objects without extensions and objects with the following extensions:

General formats:

- txt
- csv
- htm
- html

Multimedia (audio/video) files:

- flv
- f4v
- avi

- 3gp
- 3g2
- 3gp2
- 3p2
- divx
- mp4
- mkv
- mov
- qt
- asf
- wmv
- rm
- rmvb
- vob
- dat
- mpg
- mpeg
- bik
- fcs
- mp3
- mpeg3
- flac
- ape
- ogg
- aac
- m4a
- wma
- ac3

- wav
- mka
- rm
- ra
- ravb
- mid
- midi
- cda

Image files:

- jpg
- jpe
- jpeg
- jff
- gif
- png
- bmp
- tif
- tiff
- emf
- wmf
- eps
- psd
- cdr
- swf

Executable and system files:

- exe
- dll
- scr
- ocx
- com
- sys
- class
- o
- so
- elf
- prx
- vb
- vbs
- js
- bat
- cmd
- msi
- deb
- rpm
- sh
- pl
- dylib

Documents and templates:

- doc
- dot
- docx
- dotx
- docm
- dotm
- xsl
- xls
- xlsx
- xltx
- xlsm
- xltm
- xlam
- xlsb
- ppt
- pot
- pps
- pptx
- potx
- pptm
- potm
- ppsx
- ppsm
- rtf
- pdf
- msg

- eml
- vsd
- vss
- vst
- vdx
- vsx
- vtx
- xps
- oxps
- one
- onepkg
- xsn
- odt
- ods
- odp
- sxw
- pub
- mdb
- accdb
- accde
- accdr
- accdc
- chm
- mht

Archives:

- zip
- 7z*
- 7-z
- rar
- iso
- cab
- jar
- bz
- bz2
- tbz
- tbz2
- gz
- tgz
- arj
- dmg
- smi
- img
- xar

Note: The actual format of a file may not match its file name extension.

Masks in paths to files and folders

A file name mask or *a folder name mask* represents the name and extension of a file or the name of a folder using common symbols.

You can use these symbols when you specify the protection scope, scan scope, and Trusted Zone:

- The tilde symbol (`~`) replaces `/Users/<user name>` in the path to a file or folder. For example, the path `~/Desktop` means that the protection scope includes Desktop folders of all users on computers that you want to protect.

- The asterisk symbol (`*`) takes the place of any set of characters in the file or folder name, except the `\` and `/` characters (which delimit the names of files and folders in paths to files and folders). For example, the mask `/*/*.txt` will include all paths to files with the TXT extension located in folders on the internal disk, but not in subfolders.

- Two consecutive asterisk symbols (`**`) take the place of any set of characters (including an empty set) in the file or folder name, including the `\` and `/` characters (which delimit the names of files and folders in paths to files and folders). For example, the mask `/Folder/**/*.txt` will include all paths to files with the TXT extension located in the folder named Folder and its subfolders. The mask must include at least one nesting level. The mask `/**/*.txt` is not a valid mask.

- The question mark (`?`) takes the place of any single character in the file or folder name, except the `\` and `/` characters (which delimit the names of files and folders in paths to files and folders). For example, the mask `/Folder/???.txt` will include paths to all files located in the folder named Folder that have the TXT extension and a name consisting of three characters.

IOC file requirements

When creating IOC Scan tasks, consider the following IOC file requirements and limitations:

- The application supports IOC files with the IOC, XML, and JSON extensions in the open standard OpenIOC versions 1.0 and 1.1 or STIX versions 2.0 and 2.1 for describing indicators of compromise.

- If, when creating an IOC Scan task on the command line, you upload IOC files, some of which are not supported, when the task is run, the application uses only the supported IOC files. If, when creating an IOC Scan task on the command line, all of the IOC files that you upload turn out to be unsupported, the task can still be run, but it will not detect any indicators of compromise. It is not possible to upload unsupported IOC files using Web Console or Cloud Console.

- Semantic errors and unsupported IOC terms and tags in IOC files do not cause task execution to fail. In such sections of IOC files, the application detects no match.

- The identifiers of all IOC files used in a single IOC Scan task must be unique. If there are IOC files with the same identifier, it might affect the task execution results.

- A single IOC file must not exceed 2 MB in size. Using larger files will cause IOC Scan tasks to terminate with an error. The total size of all files added to the IOC collection should not exceed 10 MB. If the total size of all files exceeds 10 MB, you need to split the IOC collection and create several IOC Scan tasks.

- It is recommended to create one IOC file per threat. This makes it easier to analyze the results of the IOC Scan task.

Features and limitations of the application's support for the IOC files are shown in the following table.

Features and limitations of support for IOC documents.

Supported conditions	OpenIOC 1.0:
	
	`is`
	`isnot` (as an exception from the set)
	`contains`
	`containsnot` (as an exception from the set)
	OpenIOC 1.1:
	
	`is`
	`contains`
	`starts-with`
	`ends-with`
	`matches`
	`greater-than`
	`less-than`
	STIX 2.0 and 2.1:
	
	`=`
	`!=`
	`>`
	`<`
	`=>`
	`<=`
	`in`
	`like`
	`matches`

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 (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`)

Features of data type interpretation	The `"boolean string"`, `"restricted string"`, `"md5"`, `"IP"`, `"sha256"`, `"base64Binary"` data types are interpreted as string.
	
	The application supports interpretation of the `Content` setting for the `int` and `date` data types when it is set in the form of intervals:
	
	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 set in `ISO 8601`, `Zulu Time Zone`, `UTC format`.

Supported script interpreters for Execution prevention

Execution prevention supports the following script interpreters:

- PkgUtil
- PkgInstaller

- /usr/bin/osascript
- /usr/bin/osacompile
- /usr/local/bin/python
- /usr/local/bin/python3
- /usr/bin/perl
- /usr/bin/ruby
- /bin/bash
- /bin/zsh
- /bin/sh
- /bin/dash
- /bin/csh
- /bin/ksh
- /bin/tcsh

Important: If the script specified in the execution prevention rule is opened by the already started PkgUtil or PkgInstaller script interpreters, execution of this script will not be blocked.

How to add the Kaspersky Endpoint Security certificate to the Mozilla Firefox certificate storage

If the browser uses the Mozilla Firefox certificate storage, you need to export and add the Kaspersky certificate to this certificate storage manually. Otherwise the browser will be unable to open HTTPS-pages.

Export the Kaspersky certificate

1. Open **Launchpad** > **Other** > **Keychain Access** on your Mac.
2. In the left pane of the window, click **System** and open the **Certificates** tab.
3. In the list of certificates, find **Kaspersky Web Anti-Virus Certification Authority**.
4. Right-click this certificate and choose **Export "Kaspersky Web Anti-Virus Certification Authority"**.
5. Select a location to save the certificate and click **Save**.

   The Kaspersky certificate is saved.

Add the Kaspersky certificate to the Mozilla Firefox certificate storage

1. Open Mozilla Firefox
2. In the upper right corner, click the menu button and select **Settings**.
3. In the left pane of the window, select **Privacy & Security**.
4. Scroll down to the **Certificates** section.
5. Click **View Certificates**.
6. In the window that opens, click **Import**.
7. Choose the Kaspersky certificate file and click **Open**.
8. Select the **Trust this CA to identify websites** and **Trust this CA to identify email users** checkboxes. Click **OK**.

   The Kaspersky certificate is imported to the Mozilla Firefox certificate storage. It is displayed in the list of certificates in the **Certificate Manager** window.

Important: Each time the Kaspersky Endpoint Security application is reinstalled, a new Kaspersky root certificate is generated. That means, you need to complete this procedure after each reinstallation of the Kaspersky Endpoint Security application.

Information about third-party code

Information about third-party code is contained in the legal_notices.txt file in the folder where the application has been installed.

Trademark notices

Registered trademarks and service marks are the property of their respective owners.

App Store, Apple, Apple Remote Desktop, FileVault, iCloud, Keychain, Launchpad, Mac, Mac Pro, macOS, Rosetta, Safari, and Xcode are trademarks of Apple Inc.

IOS is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Android, Chrome, Chromium, Google, and Google Chrome are trademarks of Google LLC.

Intel is a trademark of Intel Corporation or its subsidiaries.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Excel, IIS, Internet Explorer, Microsoft, Microsoft Edge, Windows, Windows Installer, Windows Phone, and WMI are trademarks of the Microsoft group of companies.

Firefox and Mozilla are trademarks of the Mozilla Foundation in the U.S. and other countries.

Java and JavaScript are registered trademarks of Oracle and/or its affiliates.

Parallels, the Parallels logo, and Coherence are trademarks or registered trademarks of Parallels International GmbH.

VMware and VMware Fusion are registered trademarks and/or trademarks of VMware, Inc. in the United States and other countries.

JAMF and Composer are registered or common law trademarks of JAMF SOFTWARE, LLC in the U.S. and other countries.

The "Password-protected archive detected" window

If Kaspersky Endpoint Security needs to scan a password-protected archive while File Threat Protection or a scan task is running, a notification window appears.

Archive

Path to the archive.

Password

Field for entering the password.

If you enter the password, Kaspersky Endpoint Security scans the archive for malware and other computer security threats.

Skip Protected Archives

Clicking this button skips the object and all objects of the same type.

Skip

Clicking this button skips the object.

The Proxy server authentication required dialog

User Name

Field for entering the user name for connecting to the proxy server.

Password

Field for entering the password.

Remember password

This checkbox enables/disables the use of the specified user name and password for authentication on the proxy server in the future.

This checkbox is unselected by default.

The "Object detected" dialog

When Kaspersky Endpoint Security detects a virus or other threat to computer security, a notification window appears on the screen.

Detected

The object name according to the Kaspersky Virus Encyclopedia classification.

Details

Clicking this button opens a page in the Kaspersky Virus Encyclopedia with information about the detected object.

Object

Path to the folder with the detected object, or the web address where the object was detected.

Apply to all

This checkbox enables/disables the selected action for all objects of the same type during the current session of File Threat Protection, Web Threat Protection, or a malware scan task.

The checkbox is unselected by default.

The current session of File Threat Protection or Web Threat Protection is defined as the time from when the component starts until it stops or until the application is shut down or restarted. The current session of malware scan tasks is defined as the time from the start of a malware scan task until its completion.

The buttons with the actions that can be performed on detected objects vary depending on the type of object detected.

You can select one of the following actions:

- **Disinfect**. Disinfect the object. Before performing disinfection, Kaspersky Endpoint Security creates a backup copy of the file in case you need to restore the original file.
- **Delete**. Delete the object. Before performing deletion, Kaspersky Endpoint Security creates a backup copy of the file in case you need to restore the original file.
- **Don't Block**. Allow access to a website considered to be a dangerous web traffic object.
- **Block**. Deny access to a website considered to be a dangerous web traffic object.
- **Delete Archive**. Delete the archive that contains the detected object.
- **Skip Protected Archives**. Skip password-protected archives during malware scans.
- **Skip**. Block access to the object but take no actions on it.

The Scan window



Clicking this button takes you back to the previous Kaspersky Endpoint Security window.



Clicking this button takes you forward to the next Kaspersky Endpoint Security window.



Clicking this button deletes all records of all malware scan tasks in the **Scan** window.

Schedule Scan

Clicking this button opens a dialog where you can schedule Full Scan or Quick Scan tasks.

Quick Scan

Clicking the start button ( ) in this section runs a Quick Scan task.

Full Scan

Clicking the start button ( ) in this section runs a Full Scan task.

Clicking this button stops the selected malware scan task.

This button is displayed if a malware scan task is running.

Settings

Clicking this button opens the **Scan** tab where you can configure scan tasks settings.

Choose

Clicking this button opens a dialog where you can choose a file or folder to scan.

In the lower part of the **Files and Folders** section, you can view the records of all malware scan tasks that have been performed for chosen files or folders.

Details

Clicking this button opens the malware scan task report window.

This button appears when you hover the pointer over a scan task.

Clear scan history

Clicking this button deletes all records of all malware scan tasks.

Show All

Clicking this button opens the **Detected Objects** window where you can view all detected objects.

Note: Kaspersky Endpoint Security does not scan files that are located in OneDrive or iCloud storage or other cloud storages. Please exclude these files from the scan scope. Otherwise, the scan task may finish with the *Infected File Not Deleted* error.

The Detected Objects window

The **Detected Objects** section contains malicious objects detected by the application.

Disinfect All

Clicking this button starts the disinfection of all malicious objects that have been detected.

Ignore All

Clicking this button removes all malicious objects from the list of malicious objects in the **Detected Objects** section.

•••

Clicking this button opens a pop-up menu where you can select one of the following actions to perform with a malicious object:

- **Disinfect**. Disinfect the object. Before disinfection, the Kaspersky Endpoint Security application creates a backup copy of the file so that it can be later restored or disinfected without risk of data loss.
- **Ignore**. Remove the object from the list of detected objects.

The **Other objects** section contains detected objects that aren't malicious but could be used by hackers to harm your computer or data.

Delete All

Clicking this button deletes all detected objects from your computer.

Ignore All

Clicking this button removes all detected objects from the list of detected objects in the **Other objects** section.

•••

Clicking this button opens a pop-up menu where you can select one of the following actions to perform with a detected object:

- **Delete**. Delete the detected object from your computer.
- **Ignore**. Remove the object from the list of detected objects.

The **Back up** section contains backup copies of detected objects.

Delete All

Clicking this button deletes all backup copies of detected objects from your computer.

•••

Clicking this button opens a pop-up menu where you can select one of the following actions to perform with a backed up object:

- **Delete Backed Up Copy**. Delete the backup copy of the detected object from your computer.
- **Restore File**. Restore the backup copy of the file selected in the list to its original location with the same name that the original file had before disinfection or deletion. If an object with the same name already exists at the original location (for example, if Kaspersky Endpoint Security created a copy of the original file before disinfection or if it disinfected the original file), a warning is displayed. You can change the location of the object that is being restored or rename it.

The License window



Clicking this button takes you back to the previous Kaspersky Endpoint Security window.



Clicking this button takes you forward to the next Kaspersky Endpoint Security window.

Note: This window varies depending on whether Kaspersky Endpoint Security is activated, and on the type of the license or subscription used.

This window may contain the following information:

- License or subscription status
- Active keys
- Reserve keys (if any)
- License type and the number of computers on which you can use the application under the current license or subscription
- Application features that are available under the current license or subscription
- License expiration date and time
- Number of days until the license expires

In this window, you may perform the following actions:

- Activate the application by entering an activation code.
- Go to a website with information on how to purchase a license at the Kaspersky online store.
- Open the Kaspersky Endpoint Security vendor's website with the information about subscription renewal.
- Update the status of your subscription.

For more information about Kaspersky Endpoint Security licensing, contact the system administrator in your organization.

The Essential tab

In the **General** section, you can enable or disable protection of the computer against malware and other computer security threats.

Enable protection

This checkbox enables/disables real-time protection against malware and other computer security threats.

This checkbox is selected by default.

Check secure connections (HTTPS)

This checkbox enables/disables scanning of encrypted connections (HTTPS) by Kaspersky Endpoint Security and displaying notifications when Web Control blocks the user's access to dangerous web resources.

This checkbox is unselected by default.

Trusted Zone

Clicking this button opens a window where you can edit Trusted Zone by creating a list of objects that you trust and do not want to scan for malware.

Settings

Clicking this button opens the window where you can manage the list of trusted root certificates and select the certificate store for checking encrypted HTTPS traffic in the Mozilla Firefox browser.

In the **File Threat Protection** section, you can enable or disable File Threat Protection and select the action that Kaspersky Endpoint Security performs when it detects an infected file.

Enable File Threat Protection

This checkbox enables/disables File Threat Protection.

This checkbox is selected by default.

Protection Scope

Clicking this button opens the window where you can create the protection scope.

Disinfect or delete malicious objects automatically

Kaspersky Endpoint Security blocks access to the infected file and attempts to disinfect it without requesting confirmation. Prior to performing disinfection, Kaspersky Endpoint Security saves a backup copy of the file in Backup. If the file has been disinfected, Kaspersky Endpoint Security saves it in its original location under the original file name. If disinfection fails, Kaspersky Endpoint Security keeps the infected file in a blocked state in its original location. Information about the detection of the infected object is logged in the **Processed objects** report.

Prompt for action

Kaspersky Endpoint Security displays a notification window with information about the malicious object that is suspected of infecting the file, and prompts you to choose the action to be taken by Kaspersky Endpoint Security. The actions may vary depending on the status of the object.

This action is selected by default.

In the **Web Threat Protection** section, you can enable or disable Web Threat Protection and select the action that Kaspersky Endpoint Security performs when it detects dangerous web traffic objects.

Enable Web Threat Protection

This checkbox enables/disables Web Threat Protection.

This checkbox is selected by default.

Block dangerous web traffic objects automatically

Kaspersky Endpoint Security blocks access to the website where a dangerous web traffic object was detected without requesting confirmation.

Prompt for action

Kaspersky Endpoint Security displays a notification window with information about the detected dangerous web traffic object, and prompts you to choose the action to be taken by Kaspersky Endpoint Security. The actions may vary depending on the status of the object.

This action is selected by default.

In the **Mail Threat Protection** section, you can enable or disable Mail Threat Protection and select the action that Kaspersky Endpoint Security performs when it detects malicious objects.

Enable Mail Threat Protection

This checkbox enables/disables Mail Threat Protection.

This checkbox is selected by default.

Delete malicious objects automatically

When Kaspersky Endpoint Security detects an infected object in an email message, it deletes the infected object and replaces the contents of the object with the text "The requested file infected with <virus name> has been deleted".

Block malicious objects automatically

When Kaspersky Endpoint Security detects an infected object in an email message, it replaces the email message subject with "Message is infected: <original subject>", with <original subject> being the original subject. The email message subject is replaced only for the POP3 protocol.

In the **Network Threat Protection** section, you can enable or disable protection against network attacks.

Enable Network Threat Protection

This checkbox enables/disables Network Threat Protection.

This checkbox is selected by default.

Settings

Clicking this button opens a window where you can create a list of trusted computers or view and edit the list of blocked computers.



Clicking this button prevents users without administrator privileges from changing the settings of the Kaspersky Endpoint Security application.



Clicking this button opens a prompt for administrator credentials. After you enter administrator credentials, application settings become editable.

The Protection scope window

In the **Protection scope** section, you can view and edit the protection scope.

All Removable Disks

This checkbox enables/disables real-time protection of all removable disks.

This checkbox is selected by default.

All Internal Disks

This checkbox enables/disables real-time protection of all internal disks.

This checkbox is selected by default.

All Network Disks

This checkbox enables/disables real-time protection of all network disks.

This checkbox is selected by default.

+

Clicking this button opens a list where you can select items to create the protection scope:

- **Files and Folders**. Selecting this item opens a dialog for adding a file or folder to the protection scope.
- **All Disks**. Selecting this item adds all removable disks, internal disks, and network disks of the computer to the protection scope.
- **All Removable Disks**. Selecting this item adds all removable disks of the computer to the protection scope.
- **All Internal Disks**. Selecting this item adds all internal disks of the computer to the protection scope.
- **All Network Disks**. Selecting this item adds all network disks of the computer to the protection scope.
- **Memory**. Selecting this item adds the computer memory to the protection scope.
- **Startup Objects**. Selecting this item adds all executable files launched at operating system startup to the protection scope. Scanning of startup objects makes it possible to detect rootkits.

The checkbox next to a list item enables/disables real-time protection of objects associated with this item.

–

Clicking this button deletes the selected item from the protection scope list.

Items included in the protection scope list by default cannot be removed.

In the **Optimization** section, you can configure whether Kaspersky Endpoint Security scans the read-only system volume.

Skip scanning of read-only system volume

This checkbox disables/enables scanning of the read-only system volume by Kaspersky Endpoint Security.

This checkbox is selected by default.

Important: Optimization might be disabled for security reasons.

The "Settings" window

On the **Trusted computers** tab, you can create a list of trusted computers. The Kaspersky Endpoint Security application doesn't block the IP addresses of these computers automatically even after dangerous network activity is detected from them.

The list of trusted computers is empty by default.

+

Clicking this button adds a field for entering the IP address of a trusted computer.

–

Clicking this button removes the selected IP address from the list of trusted computers.

Edit

Clicking this button makes the selected IP address available for editing.

On the **Blocked computers** tab, you can view and edit the list of blocked computers.

The Kaspersky Endpoint Security application blocks the computer with this IP address for one hour after dangerous network activity is detected from it.

IP address

This column displays the IP address of the blocked computer.

Incident time

This column displays the date and time when dangerous network activity was detected on the computer.

Unblock

Clicking this button removes the selected IP address from the list of blocked computers.

The "Scan" tab

List of malware scan tasks

Contains preset malware scan tasks:

- **Full Scan**. A malware scan of the computer's memory, startup objects, and all internal disks.
- **Quick Scan**. A malware scan of only critical areas of the computer: memory, startup objects, and system folders.
- **Custom Scan**. A malware scan of a specified object (file, folder, internal disk, or removable disk).
- **External Disks Scan**. A malware scan of external disks that is performed when an external disk is connected to the computer.

Note: Kaspersky Endpoint Security does not scan files that are located in OneDrive or iCloud storage or other cloud storages. Please exclude these files from the scan scope. Otherwise, the scan task may finish with the *Infected File Not Deleted* error.

In the **Scan scope** section, you can view and edit the scan scope for the Quick Scan task.

Edit

Clicking this button opens a window where you can view and edit the scan scope.

This button appears only when the Quick Scan task is selected in the list.

In the **Action** section, you can select the action that Kaspersky Endpoint Security performs when an infected file is detected, and schedule a task.

Disinfect or delete malicious objects automatically

Kaspersky Endpoint Security blocks access to the infected file and attempts to disinfect it without requesting confirmation. Prior to performing disinfection, Kaspersky Endpoint Security saves a backup copy of the file in Backup. If the file has been disinfected, Kaspersky Endpoint Security saves it in its original location under the original file name. If disinfection fails, Kaspersky Endpoint Security keeps the infected file in a blocked state in its original location. Information about the detection of the infected object is logged in the **Processed objects** report.

Prompt for action when the scan is complete

Kaspersky Endpoint Security postpones the processing of infected files that have been detected until the end of the scan. When the scan is complete, Kaspersky Endpoint Security displays notification windows that inform you of each detected infected object, and offers a choice of further actions. The actions may vary depending on the status of the object.

This action is selected by default.

In the **When an external disk is connected** section of the **External Disks Scan** tab, you can select the action that Kaspersky Endpoint Security performs when an external disk is connected.

Scan

If this option is selected, Kaspersky Endpoint Security starts a malware scan task for the connected external disk.

This option is selected by default.

Do nothing

If this option is selected, Kaspersky Endpoint Security does not scan the connected external disk.

In the **Optimization** section, you can configure whether Kaspersky Endpoint Security scans the read-only system volume when performing a Quick Scan or Full Scan task.

Skip scanning of read-only system volume

This checkbox disables/enables scanning of the read-only system volume by Kaspersky Endpoint Security.

This checkbox is selected by default for a Quick Scan task and unselected by default for a Full Scan task.

Important: Optimization might be disabled for security reasons.

CPU Usage

Clicking this button opens a dialog where you can enable or disable limiting the application's use of the protected device's CPU for scan tasks. If the **Limit CPU utilization by scans to** option is selected, you can specify the maximum allowed CPU utilization in the corresponding field.

Note: This is a cumulative limit across all CPU cores. The CPU utilization shown in Activity Monitor is the sum of the utilization of each CPU core and therefore may exceed 100 percent.

Enabling this option can negatively affect the performance of Kaspersky Endpoint Security.

By default, this option is disabled.

Schedule

Clicking this button opens a dialog where you can schedule Full Scan or Quick Scan tasks.



Clicking this button prevents users without administrator privileges from changing the settings of the Kaspersky Endpoint Security application.



Clicking this button opens a prompt for administrator credentials. After you enter administrator credentials, application settings become editable.

The "Scan scope" window

In this window, you can view and edit the scan scope of the Quick Scan task.

The checkbox next to an object in the list enables/disables scanning of that object.

+

Clicking this button opens a list for adjusting the scan scope:

- **Files and Folders**. Selecting this item opens a dialog for adding a file or folder to the scan scope.
- **All Disks**. Selecting this item adds all removable disks, internal disks, and network disks of the computer to the scan scope.
- **All External Disks**. Selecting this item adds all removable disks of the computer to the scan scope.
- **All Internal Disks**. Selecting this item adds all internal disks of the computer to the scan scope.
- **All Network Disks**. Selecting this item adds all network disks of the computer to the scan scope.
- **Memory**. Selecting this item adds the computer memory to the scan scope.
- **Startup Objects**. Selecting this item adds all executable files launched at operating system startup to the scan scope. Scanning of startup objects makes it possible to detect rootkits.

–

Clicking this button removes the selected item from the scan scope list.

Items included in the scan scope list by default cannot be removed.

In the **Optimization** section, you can configure whether the Kaspersky Endpoint Security application scans the read-only system volume when performing a scan task.

Skip scanning of read-only system volume

This check box disables/enables scanning of the read-only system volume by Kaspersky Endpoint Security.

If this check box is selected, Kaspersky Endpoint Security skips scanning of the read-only system volume to significantly reduce scanning time.

If this check box is cleared, Kaspersky Endpoint Security scans the read-only system volume.

This check box is selected by default.

Note: Kaspersky Endpoint Security does not scan files that are located in OneDrive or iCloud storage or other cloud storages. Please exclude these files from the scan scope. Otherwise, the scan task may finish with the *Infected File Not Deleted* error.

The "Threats" tab

In the **Objects to detect** section, you can configure the list of objects to be detected.

Viruses, worms, Trojans, malicious tools, adware, and auto-dialers

This category includes the following types of programs:

- All types of malware.
- Applications that show advertisements (such as banners) on your computer or replace the search results in your browser with advertising websites.
- Applications that surreptitiously establish phone connections through a computer's modem.

Kaspersky Endpoint Security always controls programs of this type.

The checkbox is always selected and cannot be unselected.

Legitimate software that can be used by intruders to damage your computer or personal data

This checkbox enables/disables control of legitimate applications that may be exploited by an intruder to harm the user's computer or data, such as remote administration applications.

The checkbox is unselected by default.

In the **Backup** section, you can specify the maximum storage period for objects in Backup.

Delete backed up objects after <number> days

This checkbox enables/disables deletion of objects from Backup after the specified storage period expires.

If the checkbox is selected, the application deletes objects from Backup after the length of time specified in the number field next to the checkbox. If the checkbox is unselected, objects are stored in Backup indefinitely.

By default, this checkbox is selected, and objects are stored in Backup for 30 days.

In the **Exclusions** section, you can create a list of files, folders, applications, and websites that you trust and do not want to scan for malware.

Trusted Zone

Clicking this button opens a window where you can edit Trusted Zone.

> **Note:** When an administrator configures the policy to prohibit editing Trusted Zone, users cannot go to Trusted Zone settings.



Clicking this button prevents users without administrator privileges from changing the settings of the Kaspersky Endpoint Security application.



Clicking this button opens a prompt for administrator credentials. After you enter administrator credentials, application settings become editable.

The Setup administrator password window

Password

Field for entering a password to limit unwanted actions on the device.

Confirm password

Field for confirming the password by entering it a second time.

Options

The list of actions that can be protected by the password. Select the required checkboxes to protect the corresponding actions on the device. You must select at least one checkbox.

Cancel

Clicking this button closes the window without saving changes.

OK

Clicking this button saves the administrator password settings and closes the window. After the changes are saved, you are prompted to enter the password when trying to perform an unwanted action on the device.

The Password protection settings window

Password

Field for entering a password to limit unwanted actions on users' devices.

Click **Show** to view the entered symbols.

Confirm password

Field for confirming a password by entering it a second time.

Click **Show** to view the entered symbols.

Require password to

The list of actions that can be protected by the password. Select the required check boxes to protect the corresponding actions on the user's device.

The Trusted applications tab

On the **Trusted applications** tab, you can create a list of applications that you don't want to be monitored by the Kaspersky Endpoint Security application.

By default, the list of Trusted Zone objects is empty.

+

Clicking this button opens a window where you can enter a path to an application, specify its code signing requirement and select the types of activity that Kaspersky Endpoint Security will not monitor.

–

Clicking this button removes the selected application from the Trusted Zone.

Edit

Clicking this button opens a window where you can edit parameters of the trusted application.

The Add trusted application window

Path

The path to an application whose activity will not be monitored by Kaspersky Endpoint Security.

> **Note:** Symbolic links cannot be used to specify paths in this field.

Select

Clicking this button opens a window where you can select an application whose activity ill not be monitored by Kaspersky Endpoint Security. In this case, values of the **Path** and **Code signing requirement** fields are inserted automatically.

Code signing requirement

Requirements for the code signature of the application whose activity will not be monitored by Kaspersky Endpoint Security.

This is an optional parameter.

In the **Options** section, you can select the type of activity that you do not want to be monitored by the Kaspersky Endpoint Security application.

Do not monitor file activity

This check box enables/disables monitoring of an application's operations with files on a client computer.

If this check box is selected, Kaspersky Endpoint Security doesn't monitor the application's file activity.

If this check box is cleared, Kaspersky Endpoint Security monitors the application's file activity.

This check box is selected by default.

Do not monitor network activity

This check box enables/disables monitoring of the application's inbound and outbound internet traffic on a client computer.

If this check box is selected, Kaspersky Endpoint Security doesn't monitor the application's network activity.

If this check box is cleared, Kaspersky Endpoint Security monitors the application's network activity.

This check box is selected by default.

Cancel

Clicking this button closes the window without saving changes.

OK

Clicking this button saves parameters of the trusted application and closes the window.

The Trusted files and folders tab

On the **Files and Folders** tab, you can create a list of files and folders that you don't want to be monitored by the Kaspersky Endpoint Security application.

By default, the list of the Trusted Zone objects is empty.

+

Clicking this button opens a dialog for selecting a file or folder.

–

Clicking this button removes the selected object from Trusted Zone.

The Trusted web addresses tab

On the **Web Addresses** tab, you can create a list of web addresses that you don't want to be monitored by the Kaspersky Endpoint Security application.

By default, the list of the Trusted Zone objects is empty.

+
Clicking this button adds a field for entering a web address.

You can use the following symbols when you specify the website address:

- The asterisk symbol (*) takes the place of any set of characters, except the \ and / characters.
- Two consecutive asterisk symbols (**) take the place of any set of characters (including an empty set), including the \ and / characters.
- The question mark (?) takes the place of any single character in the file or folder name, except the \ and / characters.

–
Clicking this button removes the selected web address from Trusted Zone.

The Advanced tab

In the **KSN** section, you can read the terms of the Kaspersky Security Network Statement and opt in or out of participating in Kaspersky Security Network.

Show KSN Statement

Clicking this button opens a window that displays the text of the Kaspersky Security Network Statement.

Kaspersky Endpoint Security can use Global or Private KSN infrastructure. If you participate in Kaspersky Security Network, Kaspersky Endpoint Security uses information about the reputation of files, web resources, and applications received from Kaspersky Security Network and provides data required for detection services functioning to Kaspersky Security Network.

Participate in Kaspersky Security Network

This checkbox enables/disables participation in Kaspersky Security Network.

Participate in Kaspersky Private Security Network

This checkbox enables/disables participation in Kaspersky Private Security Network. For more information about participating in Kaspersky Private Security Network, contact the system administrator in your organization.

Enable extended KSN mode

This checkbox enables/disables provision of additional data to Kaspersky Security Network in order to improve protection of your computer and the usability of Kaspersky Endpoint Security. You can find the list of data in the Kaspersky Security Network Statement and in the Kaspersky Endpoint Security Help.

This checkbox is selected automatically if the **Participate in Kaspersky Security Network** checkbox is selected, but you can deselect it.

Enable cloud mode

Cloud mode refers to the application operating mode in which Kaspersky Endpoint Security uses a light version of anti-malware databases. This mode is available only if the participation in Kaspersky Security Network is enabled. The light version of anti-malware databases lets you use approximately half of the computer RAM that would otherwise be used with the full databases. If you do not participate in Kaspersky Security Network or if cloud mode is disabled, Kaspersky Endpoint Security downloads the full version of anti-malware databases from Kaspersky servers.

If the toggle button is switched on, Kaspersky Endpoint Security uses the light version of anti-malware databases, which reduces the load on operating system resources.

Note: Kaspersky Endpoint Security downloads the light version of anti-malware databases during the next update after the check box was selected.

If the toggle button is switched off, Kaspersky Endpoint Security uses the full version of anti-malware databases.

Note: Kaspersky Endpoint Security downloads the full version of anti-malware databases during the next update after the check box was cleared.

In the **Behavior Detection** section, you can enable/disable the Behavior Detection component and select an action to perform when malware activity is detected.

Enable Behavior Detection

This checkbox enables/disables the Behavior Detection component, which receives information about the actions of applications on your computer and provides it to other protection components to improve their performance.

Block malware activity

If this option is selected, Kaspersky Endpoint Security terminates an application when malicious activity is detected.

Delete detected dangerous object

If this option is selected, Kaspersky Endpoint Security deletes the executable file of a malicious application and creates a backup copy of the file in Backup when malicious activity is detected.

Prompt for action

If this option is selected, then when malware activity is detected, the Kaspersky Endpoint Security application displays a notification window with information about the malicious object and prompts the user to choose the action to be taken by the Kaspersky Endpoint Security application. The available actions may vary depending on the status of the object.



Clicking this button prevents users without administrator privileges from changing the settings of the Kaspersky Endpoint Security application.



Clicking this button opens a prompt for administrator credentials. After you enter administrator credentials, application settings become editable.

The Update tab

In the **Databases** section, you can configure the mode of Kaspersky Endpoint Security database updates.

Download updates automatically

This checkbox enables/disables automatic updates of the application databases.

This checkbox is selected by default.

In the **Proxy** section, you can configure use of a proxy server for updating Kaspersky Endpoint Security.

Use proxy server

This checkbox enables/disables the use of a proxy server to connect to the internet when updating anti-malware databases and application modules.

The checkbox is selected by default.

Settings

Clicking this button opens a window where you can configure the proxy server connection settings.

In the **Rollback** section, you can roll back to the previous version of the application databases. You may need to roll back updates when the new version of application databases contains an incorrect signature that makes Kaspersky Endpoint Security block a safe application.

Roll Back Update

Clicking this button runs the rollback of application databases.



Clicking this button prevents users without administrator privileges from changing the settings of the Kaspersky Endpoint Security application.



Clicking this button opens a prompt for administrator credentials. After you enter administrator credentials, application settings become editable.

The "Proxy server settings" window

Use system proxy server settings

Kaspersky Endpoint Security uses the proxy server settings that are specified in the system settings of your Mac.

This action is selected by default.

Use specified proxy server settings

Kaspersky Endpoint Security uses the proxy server settings specified in this window.

Address

Field for entering the IP address or the domain name of a proxy server.

The field is available if the **Use specified proxy server settings** option is selected.

Port

Entry field for the number of the proxy server port used to update Kaspersky Endpoint Security.

The field is available if the **Use specified proxy server settings** option is selected.

The default value is 8080.

Use authentication

Authentication is the process of verifying the user name and password upon connecting to a proxy server.

This checkbox enables/disables authentication when connecting to a proxy server.

The checkbox is unselected by default.

User name

Field for entering the user name for authentication when connecting to the proxy server.

The field is available if the **Use authentication** checkbox is selected.

Password

Field for entering the password for authentication when connecting to the proxy server.

The field is available if the **Use authentication** checkbox is selected.

If you have not specified the user name and password or if the specified user name and password are rejected by the proxy server, a window opens where you must enter the user name and password for authentication on the proxy server. If authentication is successful, and the **Remember password** checkbox is selected in the request window, the user name and the password that you specified are applied in all cases in the future. If the **Remember password** checkbox in the user name and password input window is unselected, you will be prompted for the user name and password again at the next connection to the proxy server.

Bypass proxy server for local addresses

This checkbox enables/disables the use of a proxy server when updating the application from a local or network folder.

The checkbox is selected by default.

The Interface tab

In the **Notifications** section, you can set up notifications that Kaspersky Endpoint Security shows to inform you about various events.

Enable notifications

This checkbox enables/disables notifications about application events.

This checkbox is selected by default.

Turn on alert sounds on malware detection

This checkbox enables/disables sound alerts when Kaspersky Endpoint Security detects a malicious object.

This checkbox is selected by default.

In the **Application icon** section, you can configure the application icon to be displayed in the menu bar.

Show in menu bar

This checkbox enables/disables the display of the application icon in the menu bar.

In the **Reports** section, you can enable/disable logging of non-critical events in Kaspersky Endpoint Security reports.

Log non-critical events

This checkbox enables/disables logging of informational events in reports. As a rule, these events are not important for the security of your computer.

In the **Traces** section, you can enable or disable tracing.

Tracing is a way to record detailed information about the application's activity. Kaspersky Technical Support specialists use trace files to troubleshoot issues. You can enable application event logging to create trace files and send them to Technical Support if requested. By default, application event logging is disabled.

Important: Turn on tracing only when a Technical Support specialist asks you to do so.

Enable tracing

This checkbox enables/disables creation of trace files.

This checkbox is unselected by default.

In the **Password protection** section, you can enable password protection of unwanted actions on your computer.

Enable password protection

This checkbox enables/disables password protection of unwanted actions.

This checkbox is unselected by default.

Selecting this checkbox opens a window where you can set and configure the administrator password.

Settings

Clicking this button opens a window where you can edit an administrator password parameters.



Clicking this button prevents users without administrator privileges from changing the settings of the Kaspersky Endpoint Security application.



Clicking this button opens a prompt for administrator credentials. After you enter administrator credentials, application settings become editable.

The Mail Threat Protection settings window

Skip archives larger than N MB

If this checkbox is selected, Mail Threat Protection excludes archives attached to email messages from scanning if their size exceeds the specified value.

If this checkbox is cleared, Mail Threat Protection scans email attachment archives of any size.

The default value is 8 MB.

This checkbox is selected by default.

Limit the time for checking archives to N sec

If this checkbox is selected, the time that is allocated for scanning archives attached to email messages is limited to the specified period.

If this checkbox is cleared, the time that is allocated for scanning archives is not limited.

The default value is 5 seconds.

This checkbox is selected by default.

The Network packet rule window

Rule name

Network packet rule name.

In the **Action** section, you can select the action to be performed by Kaspersky Endpoint Security when it detects the network activity.

In the **Protocol** section, you can specify the protocol which the network rule applies to.

In the **Direction** section, you can specify the direction of network activity being monitored.

In the **TTL** section, you can specify the lifespan of network packets being monitored.

In the **Network adapters** section, you can specify the network adapters which the network rule applies to.

In the **Remote address** section you can specify the network addresses of the remote devices that can send and receive network packets.

In the **Local address** section, you can specify the local network addresses of the devices that can send and receive network packets.

Log events

This checkbox enables/disables logging of Firewall events.

If this checkbox is selected, Kaspersky Endpoint Security logs Firewall events in the report.

If this checkbox is cleared, Kaspersky Endpoint Security does not log Firewall events in the report.

This checkbox is unselected by default.

The Network adapter window

Adapter name

The network adapter name.

Interface type

From this drop-down list, you can select the interface type of the network adapter.

IP addresses

The list of IP addresses.

MAC addresses

The list of MAC addresses.

The Network adapters window

Name

This column contains the network adapter name.

Interface type

This column contains the interface type of the network adapter.

IP addresses

This column contains the IP addresses of the network adapter.

MAC addresses

This column display the MAC addresses of the network adapter.

The Local addresses window

Local addresses

This column contains the local addresses.

The Local address window

Type

This drop-down list allows you to specify the type of local IP entry you want the network rule to apply to.

IP address

IP address entry field. This field is available only if you select **IP address** in the **Type** drop-down list.

Range start

IP addresses range start entry field. This field is available only if you select **Range of IP addresses** in the **Type** drop-down list.

Range end

IP addresses range end entry field. This field is available only if you select **Range of IP addresses** in the **Type** drop-down list.

The Remote addresses window

Remote addresses

This column contains the remote addresses.

The Remote address window

Type

This drop-down list allows you to specify the type of remote address entry you want the network rule to apply to.

Address

IP address or DNS name entry field. This field is available only if you select **IP address or DNS name** in the **Type** drop-down list.

Range start

IP addresses range start entry field. This field is available only if you select **Range of IP addresses** in the **Type** drop-down list.

Range end

IP addresses range end entry field. This field is available only if you select **Range of IP addresses** in the **Type** drop-down list.

The Templates window

Network Rule Templates

This column contain network rule templates.

The Network packet rule tab

Network service

Name of the network rule.

Action

Action to be performed by Firewall on detecting the kind of network activity.

Address

Network addresses to which the network rule is applied.

The Available networks tab

Name

This column contains the network name.

Network status

This column contains the network status of the network.

IP address

This column contains network IP addresses.

The Available network window

Network name

The network name.

Network status

The network status drop-down list.

IP address

The network IP address.

The MAC address window

Type

This drop-down list allows you to specify the type of MAC address entry you want the network rule to apply to.

MAC address

MAC address entry field. This field is available only if you select **MAC address** in the **Type** drop-down list.

Mask

MAC address mask entry field. This field is available only if you select **MAC address mask** in the **Type** drop-down list.

Range start

MAC addresses range start entry field. This field is available only if you select **Range of MAC addresses** in the **Type** drop-down list.

Range end

MAC addresses range end entry field. This field is available only if you select **Range of MAC addresses** in the **Type** drop-down list.

The System events report

The right pane of the window contains a report on the operation of Kaspersky Endpoint Security.

Time

This column displays the date and time of the event.

Event

This column displays the status of the event.

Program Name

This column displays the name of the program in which the event occurred.

User

This column displays the name of the user who initiated this event.

User Type

This column displays the type of user who initiated this event.



Clicking this button opens a window where you can save the report as a TXT file.

The Processed objects report

The right pane of the window contains the list of all infected objects and dangerous web traffic objects detected by the Kaspersky Endpoint Security application.

Time

This column displays the time when the object was detected.

Object

This column displays the path to the location where the object was detected or the object's web address.

Status

This column displays the action that the application performed after detecting the object.

Detected

This column displays the type of the detected object according to the classification given by the Kaspersky Virus Encyclopedia.

Name

This column displays the name of the detected object according to the classification given by the Kaspersky Virus Encyclopedia.



Clicking this button opens a window where you can save the report as a TXT file.

The Database Update report

The right pane of the window contains reports on update tasks performed by the application.

Started

This column displays the start date and time of each update task. If the list of operations is expanded, this column also lists operations performed while updating the application, and the time they were performed.

Status

This column displays the status of an update task.

Size

This column displays the size of downloaded update files.

Average Speed

This column displays the speed of update file downloads.

End time

This column displays the completion time of an update task.

Clicking this button expands the list of operations included in the update task.

Clicking this button collapses the list of operations included in the update task.



Clicking this button opens a window where you can save the report as a TXT file.

The Scan report

The right pane of the window contains reports on scan tasks performed by Kaspersky Endpoint Security.

Task

This column displays the name of a scan task.

Status

This column displays the status of a scan task or the status of scanned objects.

Date

This column displays the date and time of a scan task.

Initiator

This column displays the user, application, or process that initiated a scan task.

Clicking this button expands the list of scanned objects.

Clicking this button collapses the list of scanned objects.



Clicking this button opens a window where you can save the report as a TXT file.

The File Threat Protection report

The right pane of the window contains a report on the operation of File Threat Protection.

Date

This column displays the date and time when the application accessed a scanned object.

Path

This column displays the path to the original location of a scanned object.

Status

This column displays the status of a scanned object.

Program Name

This column displays the application that accessed a scanned object.



Clicking this button opens a window where you can save the report as a TXT file.

The Web Threat Protection report

The right pane of the window contains a report on the operation of Web Threat Protection.

Date

This column displays the date and time the web traffic objects were detected.

URL

This column displays web traffic objects that have been detected by Web Threat Protection. For each detected web traffic object, the column specifies the web address where it was detected.

Status

This column displays the status of web traffic objects that have been detected.

Program Name

This column displays the program that accessed the detected web traffic objects.



Clicking this button opens a window where you can save the report as a TXT file.

The Mail Threat Protection report

The right pane of the window contains a report on the operation of Mail Threat Protection.

Date

This column displays the date and time when an infected object was detected in an email message.

Path

This column displays information about the email message where the infected object was detected.

Status

This column displays the action taken by Kaspersky Endpoint Security after detecting an infected object.

Program Name

This column displays the email client name.



Clicking this button opens a window where you can save the report as a TXT file.

The Network Threat Protection report

The right pane of the window contains a report on the operation of Network Threat Protection.

Date

This column displays the date and time when dangerous network activity was detected on the computer.

IP address

This column displays the IP address of the computer from which dangerous network activity was detected by Kaspersky Endpoint Security.

Status

This column displays the action taken by Kaspersky Endpoint Security after detecting dangerous network activity.

Attack Type

This column displays the type of network attack detected.

Local Port

This column displays the number of the local port through which an intrusion attempt was made.

Protocol

This column displays the type of protocol used to perform the attack.



Clicking this button opens a window where you can save the report as a TXT file.

The Endpoint Detection and Response report

The right pane of the window contains a report on the operation of the Endpoint Detection and Response component.

Date

This column displays the date and time of events.

Event

This column displays the status of events.



Clicking this button opens a window where you can save the report as a TXT file.

The Firewall report

The right pane of the window contains a report on the operation of Firewall.

Date

This column displays the date and time of events.

Event

This column displays the status of events.



Clicking this button opens a window where you can save the report as a TXT file.

The Exploit Prevention report

The right pane of the window contains a report on the operation of Exploit Prevention.

Date

This column displays the date and time of events.

Event

This column displays the status of events.



Clicking this button opens a window where you can save the report as a TXT file.

The Device Control report

The right pane of the window contains a report on the operation of Device Control.

Date

This column displays the date and time of events.

Event

This column displays the status of events.



Clicking this button opens a window where you can save the report as a TXT file.

The System Watcher report

The right pane of the window contains a report on the operation of the System Watcher component.

Date

This column displays the date and time of events.

Event

This column displays the status of events.



Clicking this button opens a window where you can save the report as a TXT file.

The User support window

This window provides the following information:

- Version of Kaspersky Endpoint Security
- Release date of databases currently used by Kaspersky Endpoint Security
- Version of the operating system installed on the computer

Technical Support

Clicking this button opens the Kaspersky Technical Support Knowledge Base, where you can find articles on Kaspersky Endpoint Security published by Kaspersky specialists.

Community

Clicking this button opens the community where you can discuss Kaspersky Endpoint Security with Kaspersky experts and other users.

Close

Clicking this button closes the user support window.

The Certificate settings window

On the **General** tab, you can select the certificate storage for checking encrypted HTTPS traffic in the Mozilla Firefox browser:

- **System Roots keychain (recommended)**
- **Certificate store from Mozilla Firefox browser settings**

  In this case, you need to manually add the Kaspersky Endpoint Security certificate to the certificate storage of the Mozilla Firefox browser. For more information, refer to How to add the Kaspersky Endpoint Security certificate to the Mozilla Firefox certificate storage.

On the **Trusted Certificates** tab, you can create a list of trusted root certificates to connect to the corresponding servers without notifications.

The trusted root certificate list is empty by default.

+

Clicking this button opens a dialog for adding certificates that will be considered trusted.

–

Clicking this button removes the selected certificate from the list of trusted ones.

Certificate Name

This column displays the names of the trusted root certificates.

Cancel

Clicking this button closes the window without saving changes.

Save

Clicking this button saves the current list of trusted root certificates and closes the window.

The Verify Certificate window

Show Certificate

Clicking this button opens a system window with information about the certificate.

Cancel

Clicking this button closes the window.

Add to Trusted

Clicking this button adds the certificate to the trusted certificates list. As a result, you will be able to connect to the corresponding server without notifications.

Connect

Clicking this button connects you to the server.

> **Note:** The available buttons may vary depending on the certificate type.

The Select Certificate window

List of available certificates

Select the checkbox next to a certificate to use it when connecting to the server.

Show Certificate

Clicking this button opens a system window with information about the certificate.

Cancel

Clicking this button closes the window.

Continue

Clicking this button continues connecting to the server using the selected certificate.