Protection against encryptors in the corporate segment

Document structure:

Purpose of the document

This document provides information on a type of threat from the Trojware family known as encryptors (also sometimes referred to as encoders or cryptors). It also discusses the ways encryptors can infiltrate a system or corporate network, and the measures employed to protect a corporate network against this type of threat. In this document, you will learn the answers to the following questions:

- What are encryptors?
- How do they infiltrate a system or corporate network?
- How does infection and encryption occur?
- How to set up protection using the standard tools of system administration?
- How to set up protection using Kaspersky flagship product Kaspersky Endpoint Security 11.x?
- What must be done if an infection has occurred and files have been encrypted?

General information about encryptors

Malicious objects identified by Kaspersky as encryptors employ a hacker-implemented algorithm for encrypting data on the victim's computer so that the computer user can no longer utilize such data. The original, non-encrypted versions of the files are then deleted from the computer. After the data is encrypted, the hackers demand that the user pay a ransom to decrypt the files.

The program used to restore the data (decryptor) or code to unlock the system is sent to the victim only after the hacker receives the money. However, even if the ransom is paid, hackers don't always actually send a decryptor. The usual cost of a decryptor is from $300 to $500, and payment is accepted in the form of anonymous cryptocurrency such as bitcoins. Hackers usually give the victim 48 to 72 hours to pay the ransom, after which the ransom amount is increased. After the specified term expires, hackers may destroy the decryptor, thereby making the payment option impossible for restoring the files.

In cases of attacks on large organizations, the amount of a ransom can reach tens of thousands of dollars.

The real price

It should be understood that the real price of lost files for a business significantly exceeds the amount demanded by hackers because such lost files may include critical data such as a customer database, order database, or other critical information. To avoid such problems, maximum attention must be focused on creating effective protection against encryptors.

To avoid infection, you must thoroughly ensure the protection of your corporate network and definitely employ anti-virus software. Below are recommendations for setting up protection using **Kaspersky Endpoint Security 11.x for Windows** and **Kaspersky Security 10.1.2 for Windows Server**.

How an encryptor infiltrates a system

There are two main infiltration paths that allow a malicious object into a system: social engineering and known vulnerabilities.

Most frequently, an encryptor is attached to an email. To scare or mislead the user, such an email is supposedly sent from an official from some government agency such as the FBI, IRS, Justice Department, or some other organization. This induces the victim to open the file. The following attachment file extensions are the most commonly used:

- JS/JSE/WSF
- Doc/docx/DOCM
- HTA

If Microsoft Office files are used, the user must also permit macros to run when opening the document.

Under such a scenario, the encryptor loads and executes malicious code.

> Such emails are often supposedly sent on behalf of business partners of the company or by applicants for vacancies. The attachments of such emails often contain the words "contract", "invoice", "CV", and other related words.

Another common variant is the infection of a web resource with malicious code that redirects the user to a landing page containing **exploits**. Such a page analyzes the software used by the victim and employs an exploit aimed at the vulnerable applications detected. The following are used most frequently for attacks:

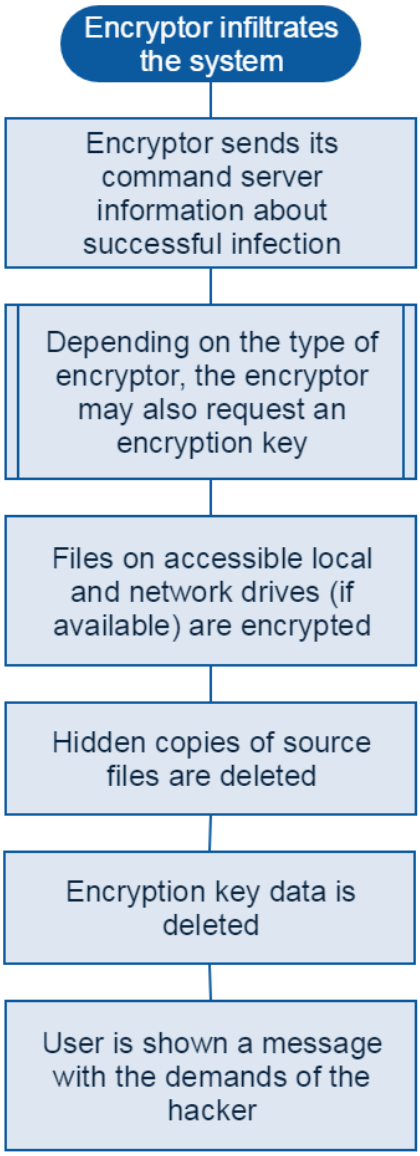
- Adobe Flash;
- Internet Explorer;
- Microsoft Silverlight.

In such a case, the user may become a victim of an encryptor by simply opening a page of an initially secure known website in a browser.

The following penetration methods are also widely used:

- If a **remote administration system** (for example, RDP) is enabled on a victim's computer, and weak passwords for system accounts are used, the hackers apply the password brute forcing technique. If the password was matched, they log in to the remote computer and run an encryptor manually.
- Attackers can hack a corporate network by exploiting vulnerabilities in web applications or services running on one or more computers that have Internet access. As a result, under certain conditions in a compromised corporate network, the attackers can run an encryptor on all computers.

Typical procedure of actions by an encryptor in a system



Which files are encrypted

Encryptors are most frequently aimed at modifying the following types of files:

Type of files	Extensions	Type of files	Extensions	Type of files	Extensions
Documents	.doc	***Archives***	.rar	***Databases***	.mdb
	.docx		.zip		.1cd
	.pdf		.7z		.sqlite
	.ppt		.tar		.sql
	.pptx		.gz		
	.rtf				
	.odt				
	.odp				
	.ods				
	.djvu				

Type of files	Extensions	Type of files	Extensions	Type of files	Extensions
Images	.jpg	***Multimedia***	.avi	***Other***	.kwm
	.jpeg		.mp3		.iso
	.bmp		.wav		.torrent
	.gif		.mkv		.php
	.png		.flac		.c
	.psd		.mp4		.cpp
	.cdr		.mov		.pas
	.dwg		.wmv		.cer
	.max				.key
	.3ds				.pst
					.lnk

A whole new level of encryptors

Hackers are constantly improving the technologies they use to create encryptors. They are not only encrypting individual files but are also starting to **encrypt file system tables**, which can destroy all information on a hard drive, including the operating system. Their further actions do not differ from an attack by any other encryptor – a screen appears with a demand for ransom. For more information about these types of encryptors, please refer to the **article in our blog**.

Another common attack type is **full disk encryption**. In this case, the entire hard disk partitions are encrypted. As a result, the OS cannot boot, and the infected computer displays a demand for ransom at the earliest boot stage.

Why it is not always possible to decrypt files

State-of-the-art encryptors employ complex encryption algorithms and key generation schemes. In particular, data is commonly encrypted based on an **AES** algorithm, and the AES key itself undergoes a second encryption based on an **RSA** algorithm. Even if the key is not additionally encrypted, it is still impossible to restore files encrypted based on the AES-256 (128) algorithm at the current state of development of computing capacities.

Additional complexity is caused by the fact that an individual encryption key is generated for each infected device. This means that even if you receive a decryptor for one computer, you will be unable to restore the data on all infected machines.

It is only possible to decrypt files in cases where the hackers implement their own encryption algorithm or common algorithms containing errors. However, such situations are unlikely.

Where malicious objects are most frequently stored

Encryptors are most frequently stored in and run from the following folders:

Location (directory)	Address template	Note
APPDATA	Drive:\Documents and Settings\%UserName%\Application Data\ Drive:\Users\%UserName%\AppData\Roaming\ "%USERPROFILE%\AppData\Local" "%USERPROFILE%\Local Settings\Application Data"	*for NT/2000/XP* *for Vista/7/8* *for Vista/7/8* *for NT/2000/XP*

Location (directory)	Address template	Note
TEMP (temporary system directory)	%TEMP%\???????.tmp\ %TEMP%\???????.tmp\??\ %TEMP%\???????\ %WINDIR%\Temp	*Example:* temp\vum35a5.tmp *Example:* temp\7ze5418.tmp\mp *Example:* temp\pcrdd27
Temporary directory of web browser	"%USERPROFILE%\Local Settings\Temporary Internet Files\" "%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\" ..\temporary internet files\content.ie5\ ..\temporary internet files\content.ie5\????????\	*for NT/2000/XP* *for Vista/7/8* *"?" = a-z, 0-9*
Desktop	"%UserProfile%\Desktop\"	
Recycle Bin	Drive:\Recycler\ Drive:\$Recycle.Bin\ Drive:\$Recycle.Bin\s-1-5-21-??????????-??????????-??????????-1000	 *"?" = 0-9*
Windows system directory	"%WinDir%" "%SystemRoot%\system32\"	
Directory for user documents	%USERPROFILE%\MyDocuments\ %USERPROFILE%\MyDocuments\Downloads	
Directory for downloading files via a browser	%USERPROFILE%\Downloads	
Startup directory	%USERPROFILE%\Start Menu\Programs\Startup	

Vulnerable platforms

Note that state-of-the-art encryptors are capable of corrupting files not only in a **Windows** operating system. Also at risk are computers running **macOS**, smartphones and tablets running **Android** OS, and objects in a **virtual infrastructure** (**VDI**). Such devices can also be used by hackers to distribute malicious objects within a corporate network that is not the original target of an attack.

There is also a risk of file encryption on **network-attached storage devices** (**NAS**). This is done by exploiting vulnerabilities in the software of specific models of NAS devices. In this case, user files on mapped drives are encrypted.

To prevent such a possibility, you must ensure the protection of all devices using corporate network resources regardless of the platform on which they are operating.

Reasons for infection

Based on the results of investigations conducted by Kaspersky virus analysts, there are a number of common reasons for system infection.

% of total number of reasons		Reason for infection
37 %		Failure to detect malware *(new types)*
21 %	**48 %**	Use of an outdated version of a product
16 %		Absence of anti-virus protection
11 %		Outdated anti-virus databases
11 %		Use of a home product to protect server versions of Windows
5 %		Anti-virus protection is partially or fully disabled

Thus, the formal presence of a protection solution does not guarantee 100% protection. To minimize risks, software must be properly configured and updated.

In the incidents that were investigated, victims frequently used products that did not have the **System Watcher** * component, or this component was disabled.

** In KES 11.x, **System Watcher** is replaced by the 3 following components: **Application Behavior Detection**, **Exploit Prevention**, **Remediation Engine**.*

Organizing protection against encryptors

Effective defense against a data encryption threat requires a comprehensive approach to corporate network protection.

General recommendations on IT security

1. Improving the IT security competence of employees

People are often the most vulnerable point of a company's IT security. Therefore, you must regularly take measures aimed at increasing personnel knowledge of data security. Employees must be informed about the danger of receiving phishing emails, clicking on suspicious links, and other risky actions.

2. Use of different roles and restriction of rights for users to access network and corporate resources

Utilize system administration tools to minimize the risk of infection of each device and spreading of the infection over the corporate network:

- Users must not have local administrator rights unless they are absolutely necessary for the performance of their official duties. If this is the case, malicious software will not be able to run on a device that is attacked.
- Users must not have access to all network folders of the internal network with data write privileges. If this is the case and one computer is infected, the malicious object will not be able to spread to all network resources of the corporate network.
- Users must not have access to external network resources unless it is absolutely necessary for the performance of their official duties. If this is the case, there will be no possibility of clicking an infected link.

3. Regular backup copying of data

To have the capability for restoring corrupt files, you should regularly create backup copies of data. If backup copies are available, the effects of an encryptor attack can be easily rectified.

Recommendations on creating and storing backup copies

Note that backup copies of files can also be attacked by an encryptor. State-of-the-art encryptors often destroy backup copies that were created by tools of the operating system. If this happens, it is impossible to roll back to previous restore points.

To prevent such a situation, it is recommended to adhere to the following rules:

- Store backup copies outside of the computer, such as on removable drives or in cloud-based data vaults.
- Store backup copies in encrypted containers.

If this is the case, the encryptor will not be able to receive access to backup copies or otherwise corrupt them.

It is also recommended to create backup copies of important data frequently enough to have the capability to restore the most recent versions of documents in case of an attack by an encryptor.

4. Regular check for OS security updates and their installation

Encryptors, like other types of threats, exploit known vulnerabilities of the operating system to conduct attacks. The developers of operating systems employ updates to rectify vulnerabilities. Installation of operating system updates will reduce the potential capabilities for attacks.

This is also true for application updates. Many applications are also potentially vulnerable to attacks by hackers. For that reason, you should regularly check for updated versions of utilized applications and install them. Developers of applications strive to rectify vulnerabilities in their products by releasing patches and updates.

5. Installation of an anti-virus solution and regular update of its databases

As indicated earlier, most successful attacks by encryptors are due to the lack of a protection solution on the computer, or due to outdated databases of such a solution. Every minute, an enormous amount of threats emerge all over the world. Their operating algorithms are becoming more and more complex and "smart". Use of an anti-virus product with the latest databases can minimize the possibility of an encryptor infiltrating a device or corporate network. Moreover, additional configuring of such a product can provide you with the capability to counteract even the latest threats that have not yet been included in anti-virus databases.

The next section of this document will examine the capabilities of Kaspersky Endpoint Security 11.x for Windows and Kaspersky Security 10 for Windows Server in the context of providing comprehensive protection against encryptors (including those that have not yet been detected by signature-based methods).

6. Using strong account passwords

It is recommended to use strong (complex) passwords for all system accounts, and not to open remote administration access (using RDP or other systems) directly via the Internet. Instead, you should arrange for remote access using a VPN connection.

Recommendations on configuring and using Kaspersky solutions for protection against encryptors

The Kaspersky products known as **Kaspersky Endpoint Security 11.x** for Windows and **Kaspersky Security 10 for Windows Server** ensure protection of devices against all actions of encryptors, and they accomplish this with minimal additional configuration.

Protection of workstations

Basic settings

The following are the main components tasked with handling threats of infection by an encryptor:

- **Mail Threat Protection** – scans incoming emails for malicious attachments and for phishing links and other dangerous links in the body and subject of emails.

- **Web Threat Protection** – scans web traffic and blocks access to dangerous web resources.
- **File Threat Protection** – scans objects on local disks of the workstation.
- **Application Behavior Detection**, **Exploit Prevention**, **Remediation Engine** – analyze the actions of applications in the system and compare them with malicious patterns that have been included in databases. In case of a match, the components block the suspicious application and roll back the system changes performed by the malicious object.

The listed components do not require additional configuring to ensure proper protection. Their default security levels set by Kaspersky experts are sufficient to prevent encryptors from infiltrating computers, provided that the application version and databases are up to date.

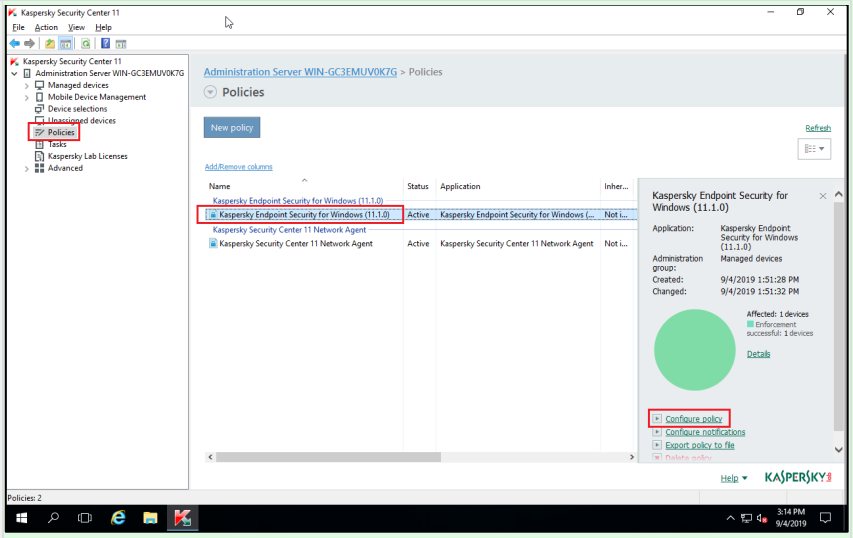
Kaspersky Security Network

Note that all components mentioned hereinafter combine the use of specific signatures and the cloud knowledge base of **Kaspersky Security Network** (**KSN**). Although it takes some time for a new malicious object to be added to a database and for databases to be distributed to all machines in an organization, data about a new threat is instantly entered into KSN. The cloud database enables detection of the latest encryptors even before data about them is entered into the databases of products.

You can make sure that the basic protection components are enabled by checking the Kaspersky Endpoint Security policy settings.

Configuration instructions

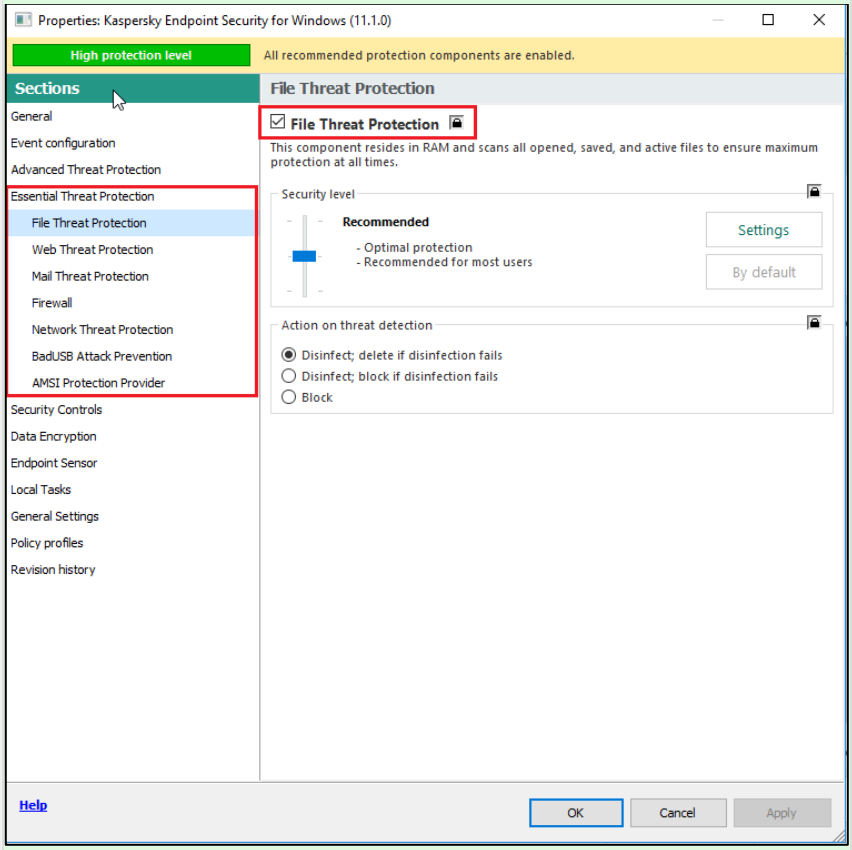
Open the active **Kaspersky Endpoint Security** policy in Kaspersky Security Center and select **Configure policy**.

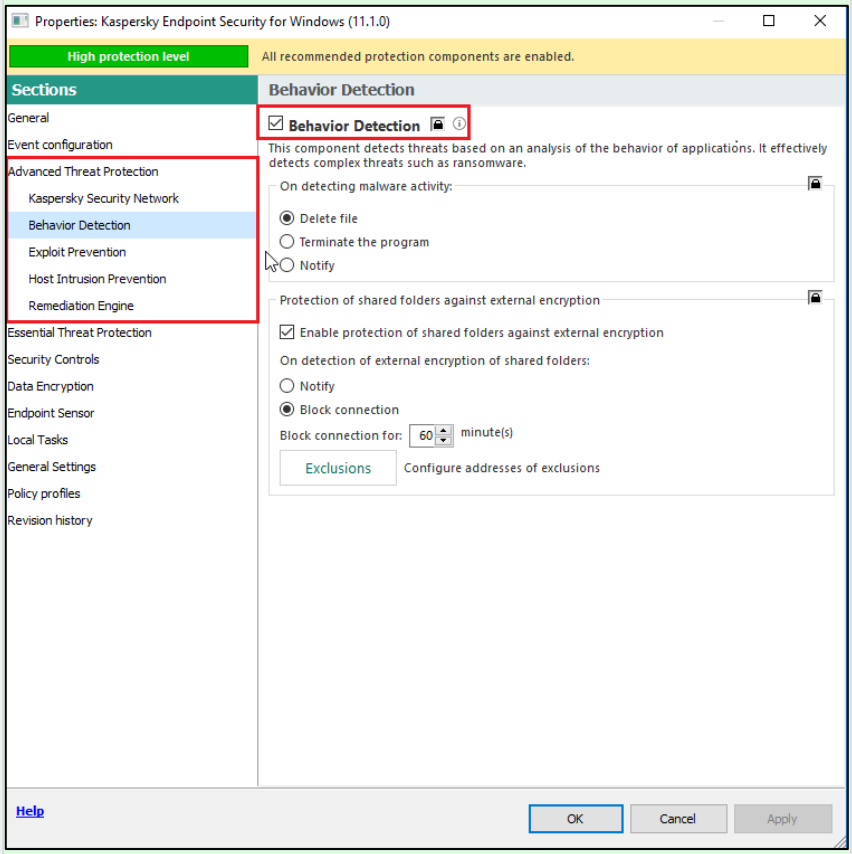


Select the **Essential Threat Protection → File Threat Protection** section on the left.

Make sure that the *<component name>* parameter selected, and that the lock button to the right of the parameter is recessed.

Perform this check for the other components of the **Essential Threat Protection** and **Advanced Threat Protection** tabs.





Additional settings

An additional level of protection can be set by configuring **Application Control** and **Host Intrusion Prevention**. These components let you block the startup of unknown and suspicious applications, and to configure permissions to access vulnerable types of files or an external network.

Blocking startup of applications from temporary folders and removable drives

As was indicated earlier, in the majority of cases, malicious objects received from the web or from email attachments are started from the system directory AppData (Application Data), the temporary system folder TEMP, or a folder containing temporary files of a browser. In addition, a malicious object could also infiltrate a computer from removable media.

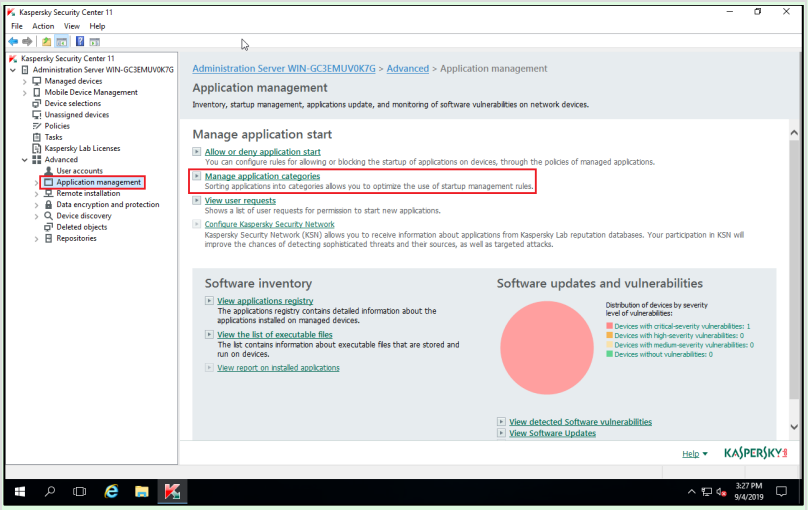
Use of **Application Control** enables elimination of these risks. You can properly configure protection in two stages:

- Create an application category and specify potentially dangerous paths in this category
- Create a rule within a policy blocking the startup of applications from this category

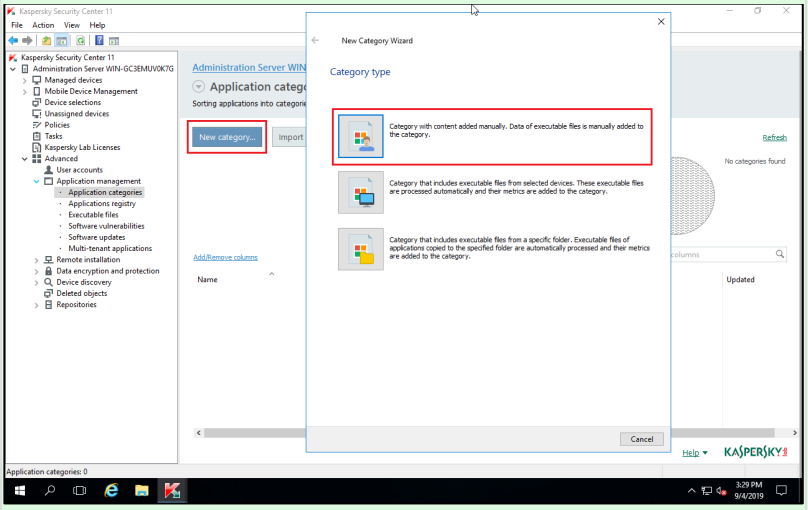
Configuration instructions

Create a category:

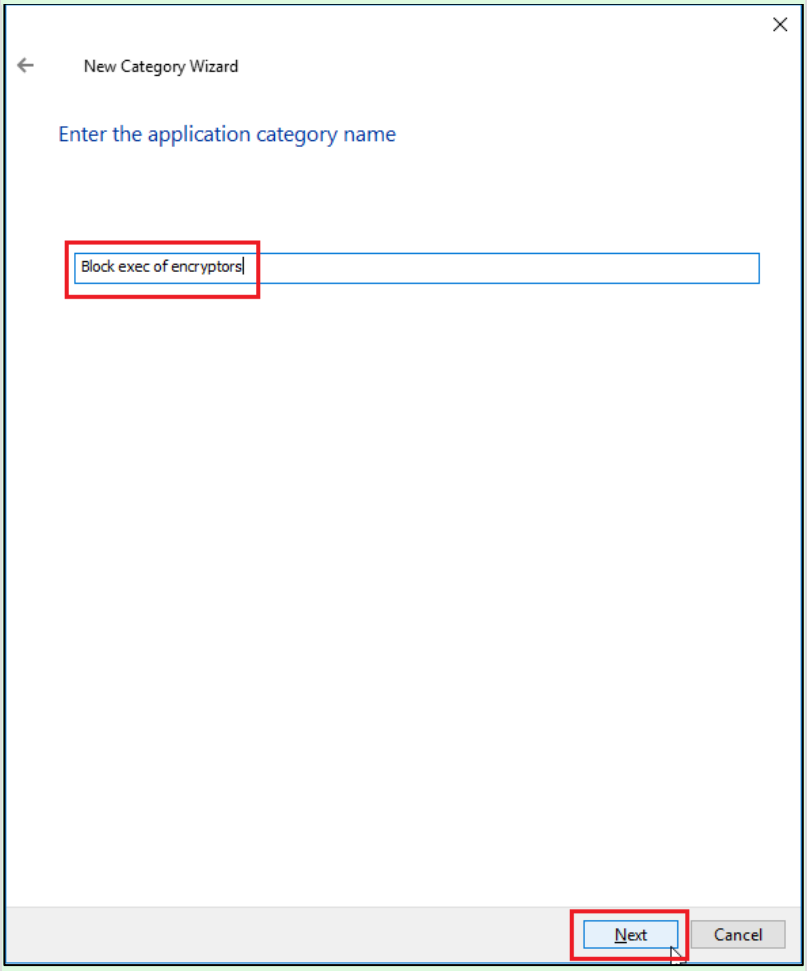
In Kaspersky Security Center, select **Application management → Manage application categories**.



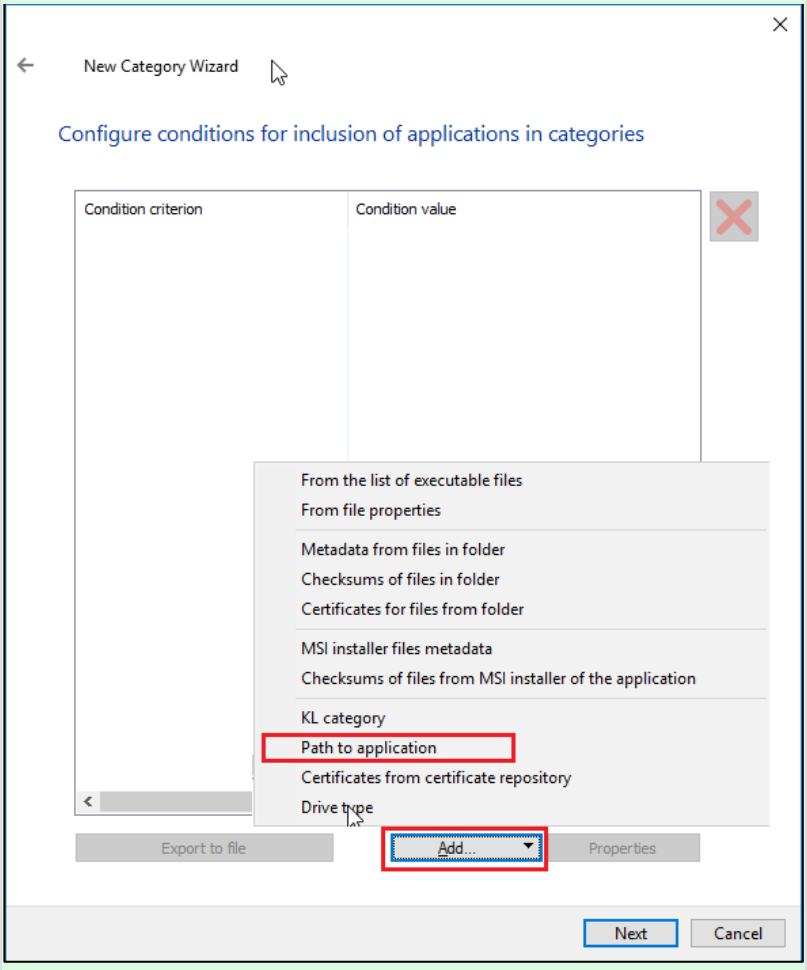
Click **New category** in the upper part of the section and select **Category with content added manually** in the *New Category Wizard*.



Name the category **Block exec of encryptors** and click **Next**.

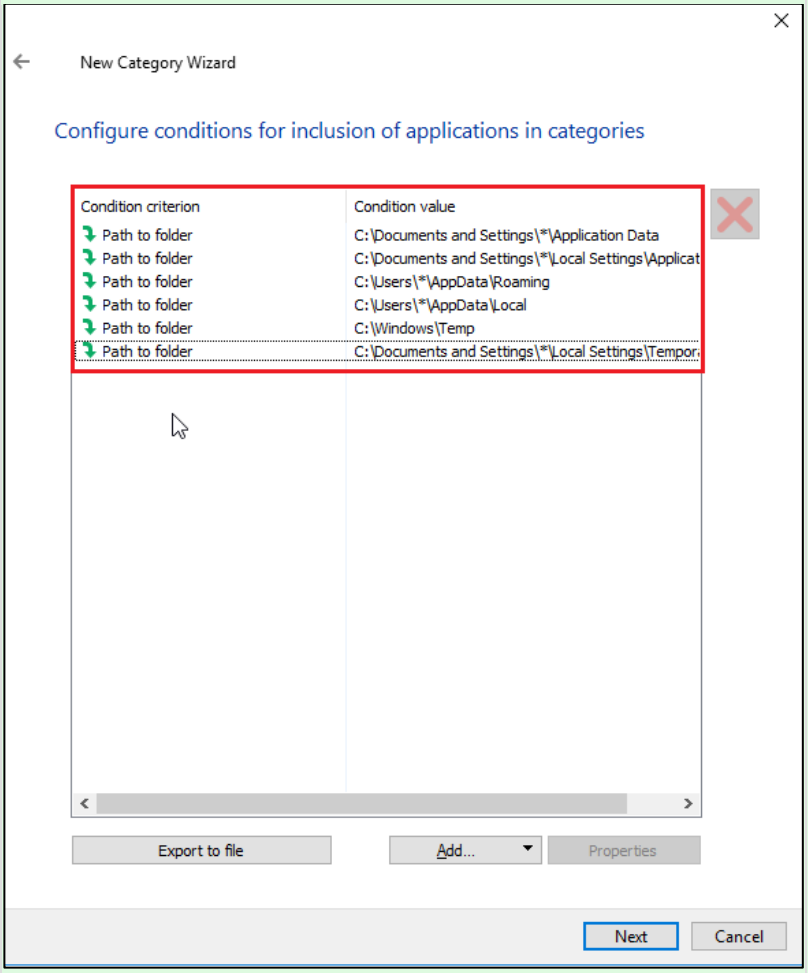


Click **Add** → **Path to application** to add a path.

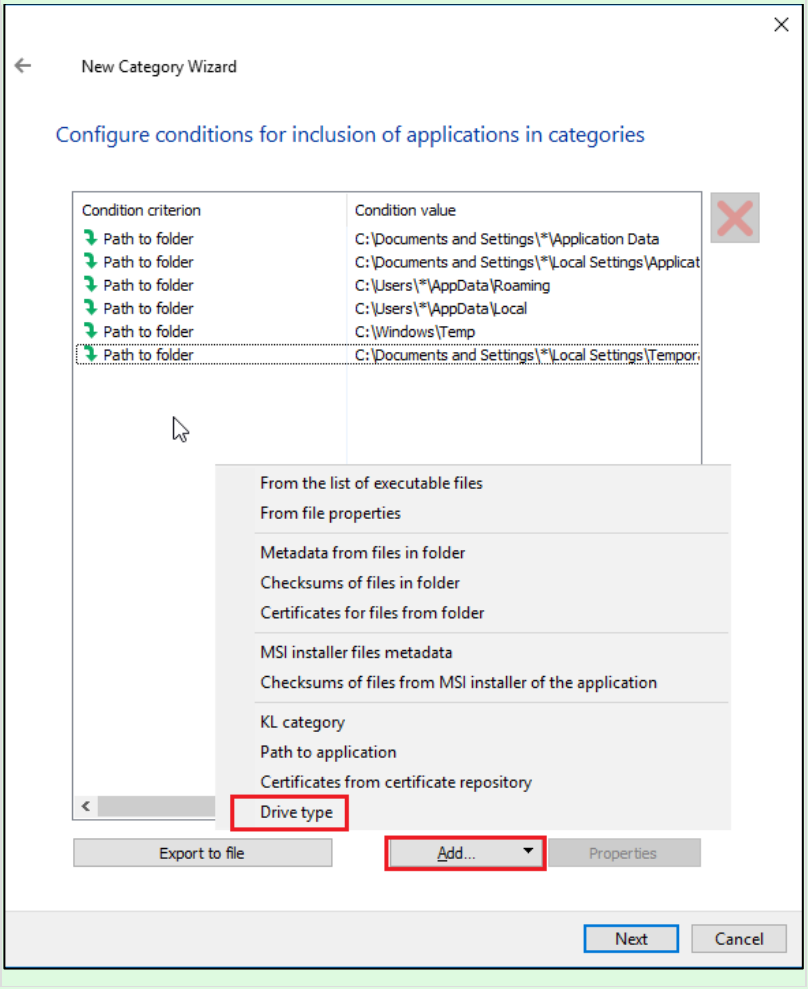


Add the paths (one-by-one) provided above by using masks:

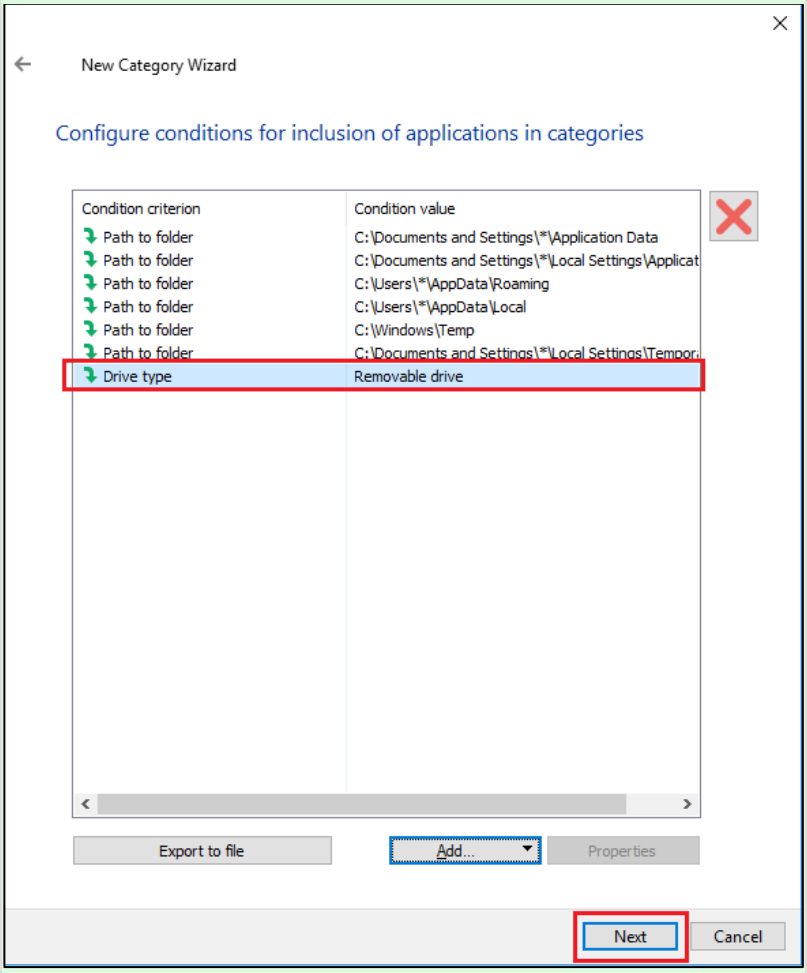
- **C:\Documents and Settings*\Application Data**
- **C:\Documents and Settings*\Local Settings\Application Data**
- **C:\Users*\AppData\Roaming**
- **C:\Users*\AppData\Local**
- **C:\Windows\Temp**
- **C:\Documents and Settings*\Local Settings\Temporary Internet Files**



Block startup of an application from removable drives. Click **Add** to add another condition and select **Drive type**.

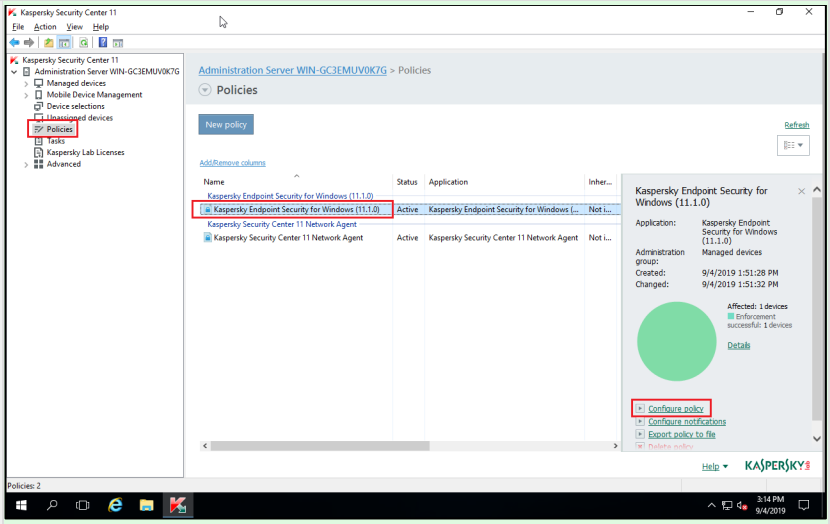


Make sure that **Drive type – Removable drive** has appeared in the list of conditions for including applications into the category. Click **Next**, click **Next** again, then click **Finish**.



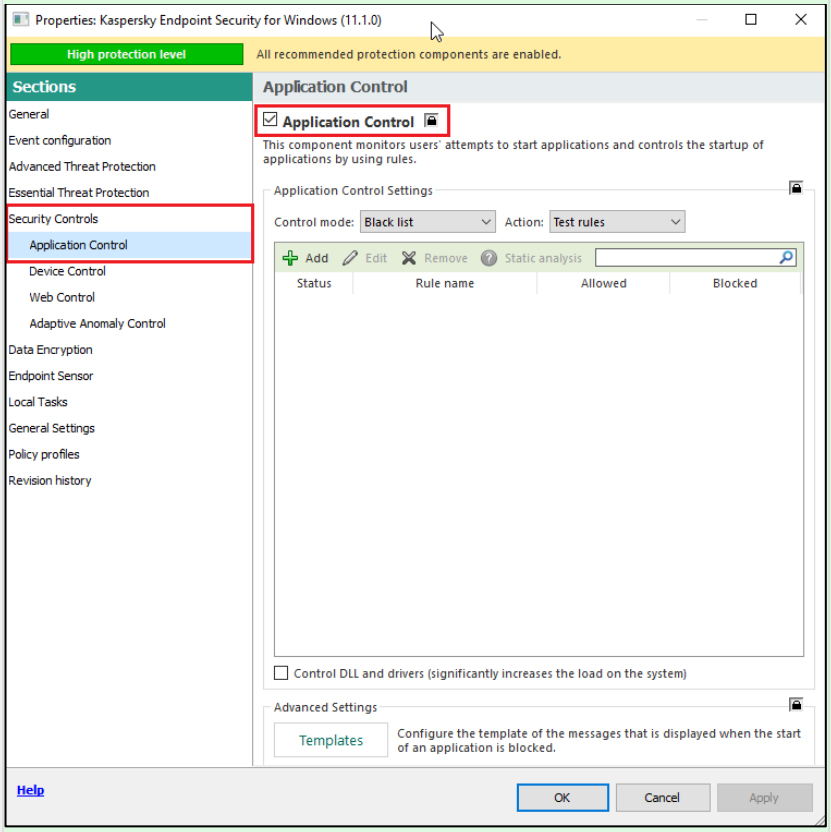
Add a blocking rule to the policy:

Open the active **Kaspersky Endpoint Security** policy in Kaspersky Security Center and select **Configure policy**.

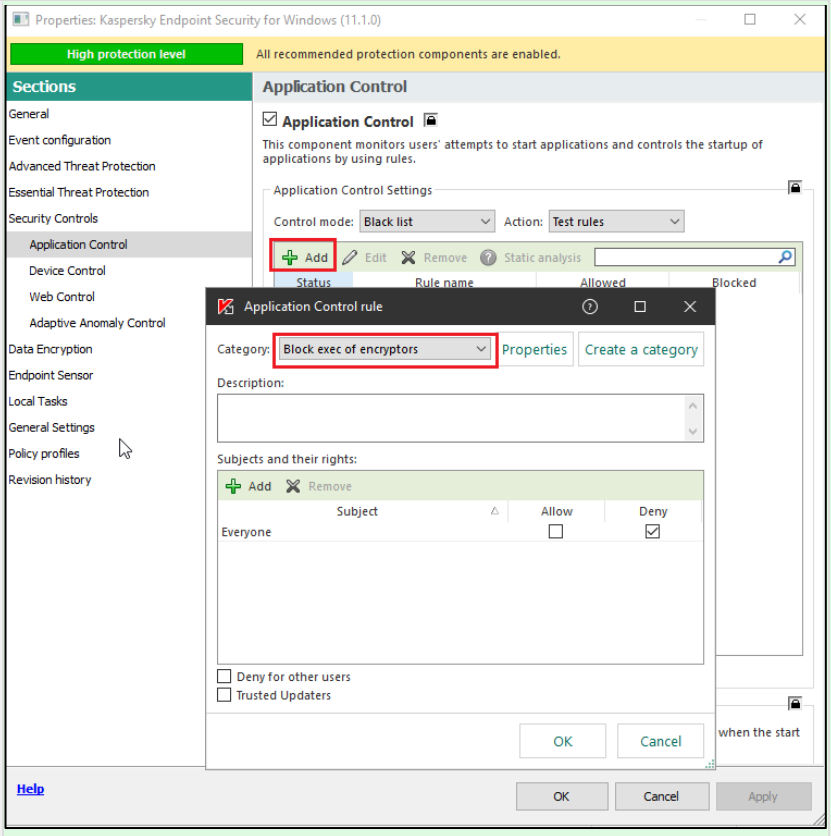


Select the **Security Controls → Application Control** tab.

Make sure that the check box next to the **Application Control** heading is selected, and that the lock button to the right of the setting is recessed.

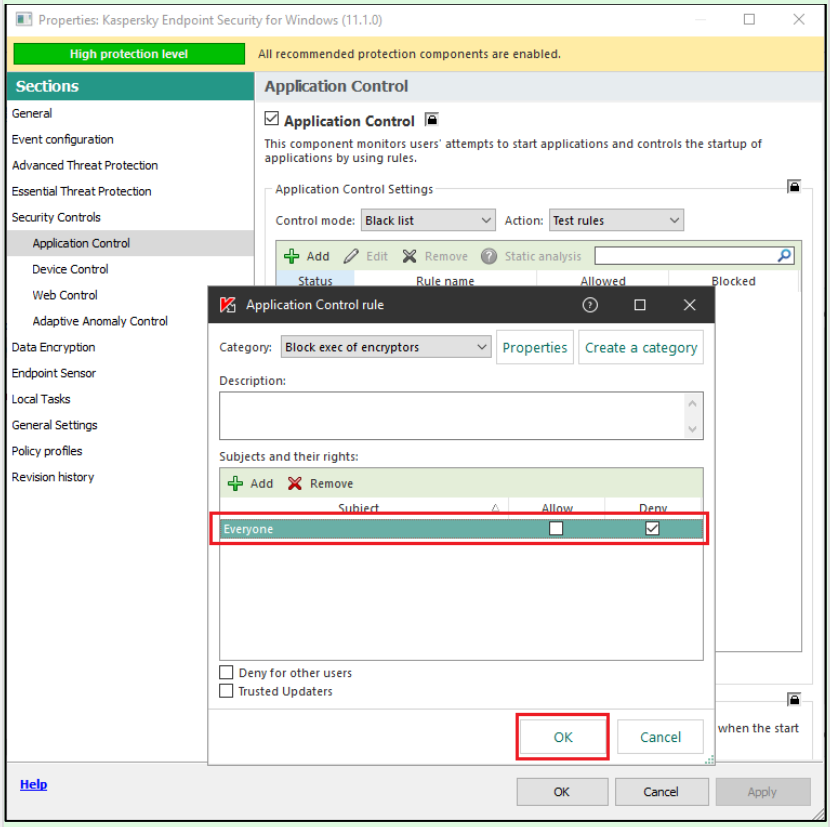


To add a rule, click **Add** and select the created category **Block exec of encryptors**.

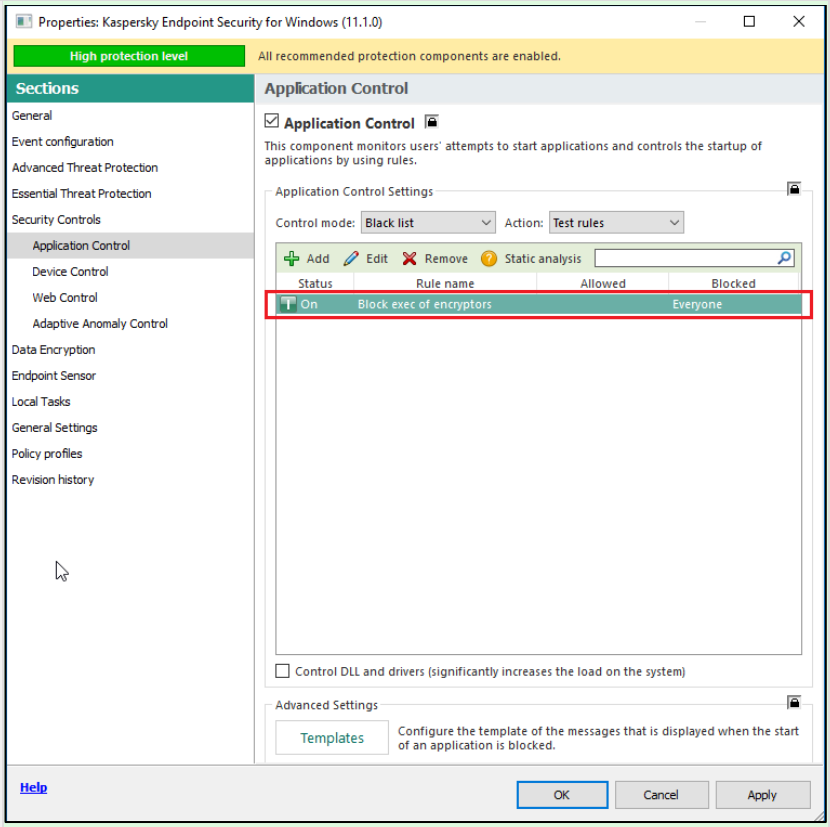


In the **Subjects and their rights** field, make sure that the **Deny** action is selected for the **Everyone** group.

Click **OK**.

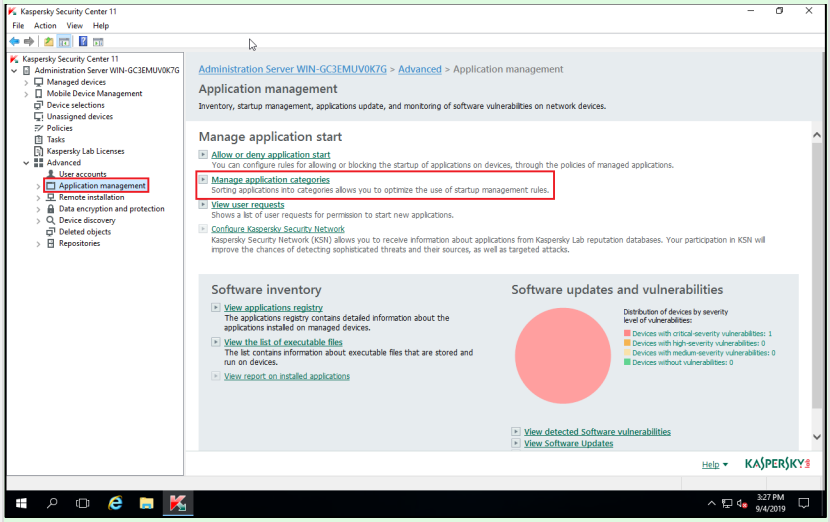


Make sure that the **Block exec of encryptors** rule has appeared in the list of **Application Control** rules and that the **On** value has been set in the status column.

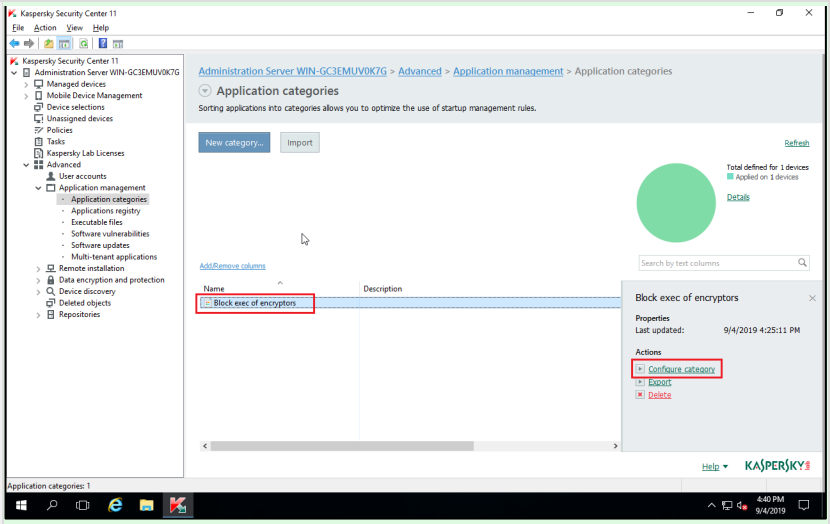


If the rule blocks useful applications, configure exclusions for them:

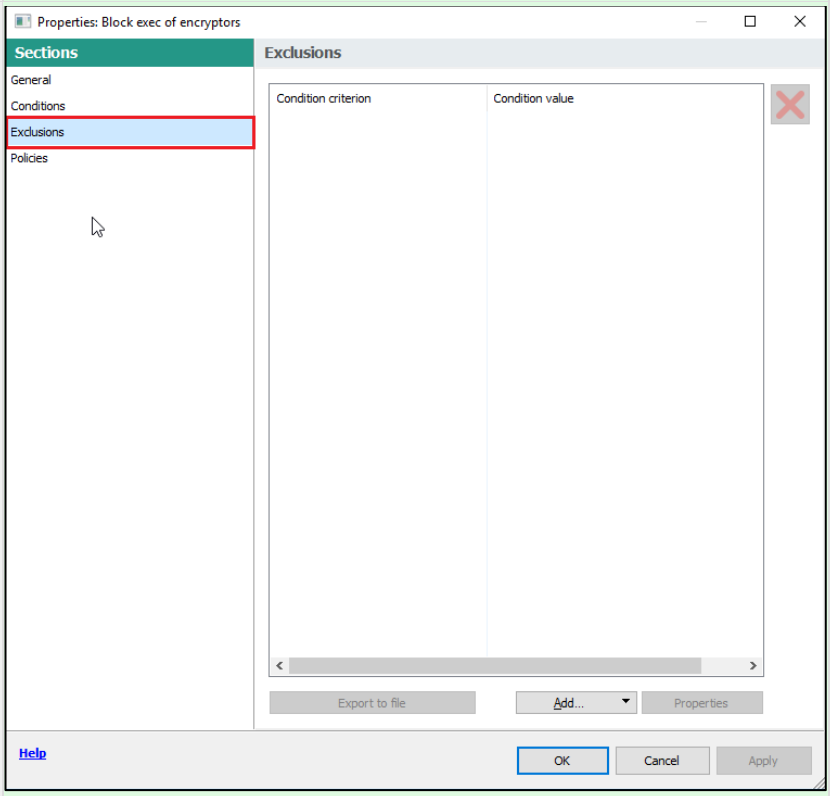
In the Administration Console, select **Application management → Manage application categories**.



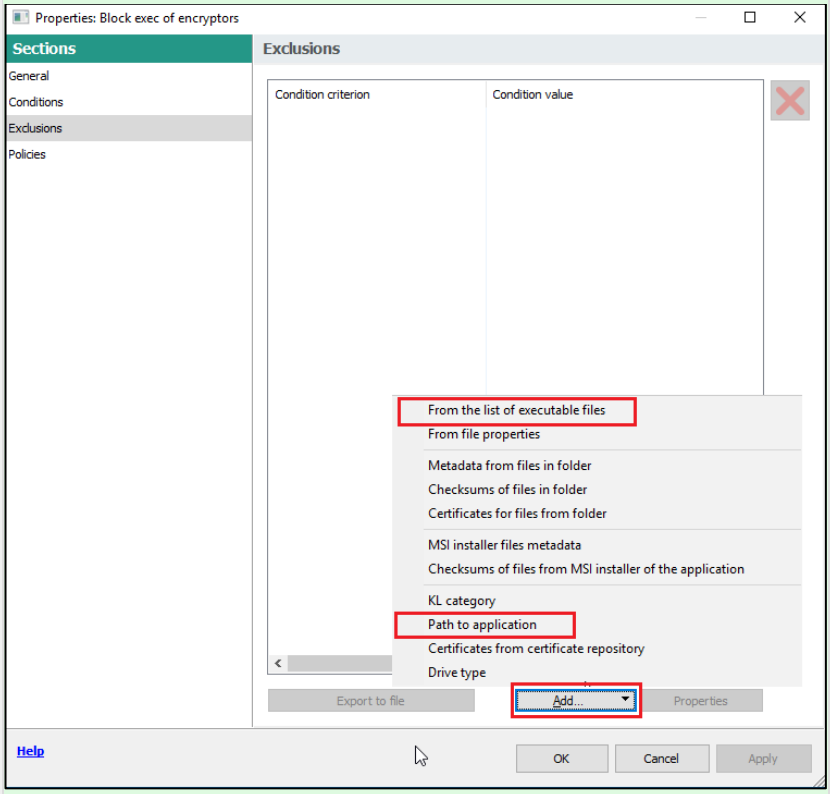
Open the **Configure category** window for the **Block exec of encryptors** category.



Select the **Exclusions** tab.



Add conditions for excluding applications affected by the blocking rule.



Default Deny

A Default Deny policy is currently popular for setting up IT security. Under such a policy, all applications are blocked from starting until the user allows them to start. In such a case, malicious applications are also unable to begin executing their tasks.

Kaspersky products allow you to implement this policy. Recommendations on implementing this policy are provided in the course titled **KL032.10 Default Deny**.

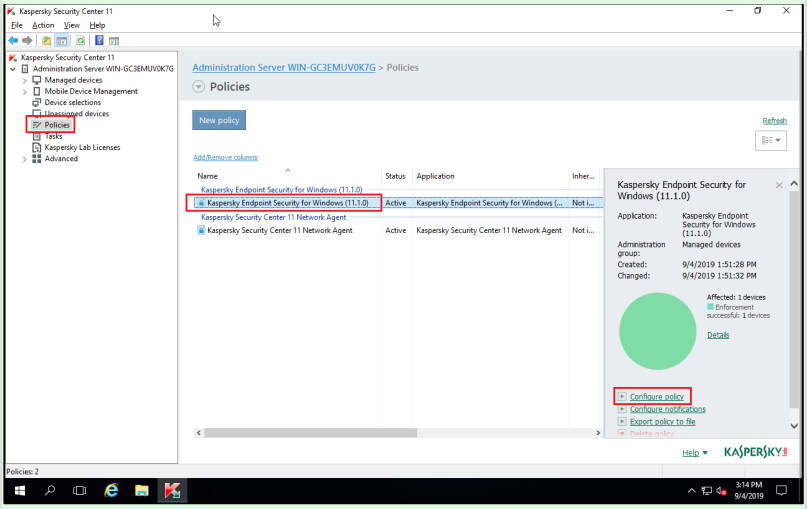
Blocking suspicious applications from modifying files

If suspicious applications are blocked from modifying files from the list presented above, an encryptor will not be able to inflict damage on user data even if it is somehow able to start despite correct configuration and operation of all protection components.

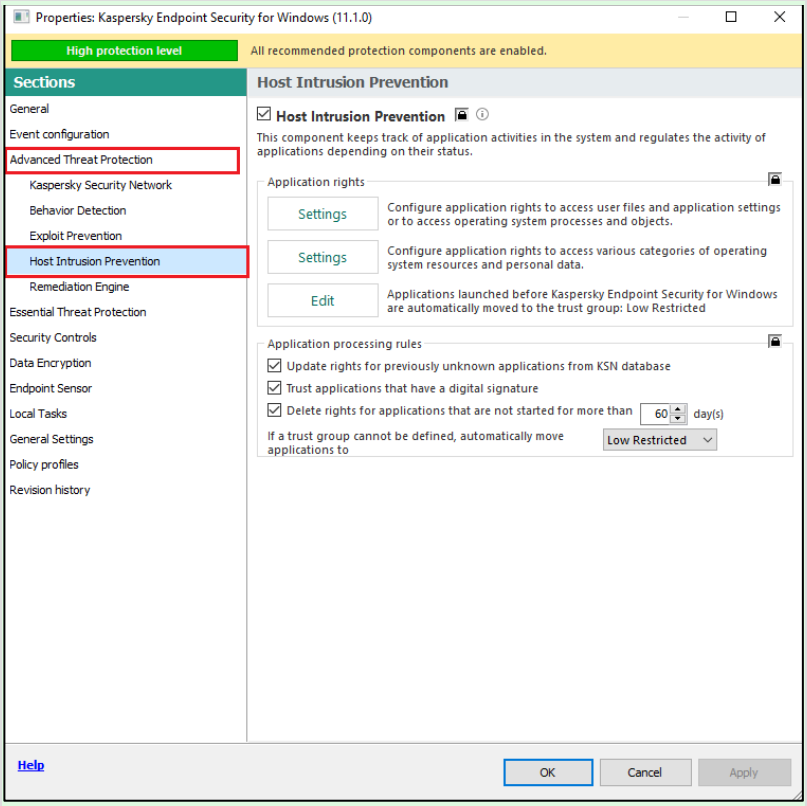
Use of **Host Intrusion Prevention** enables accomplishment of this task. To do this, you must allow only applications from the Trusted group to modify files.

Configuration instructions

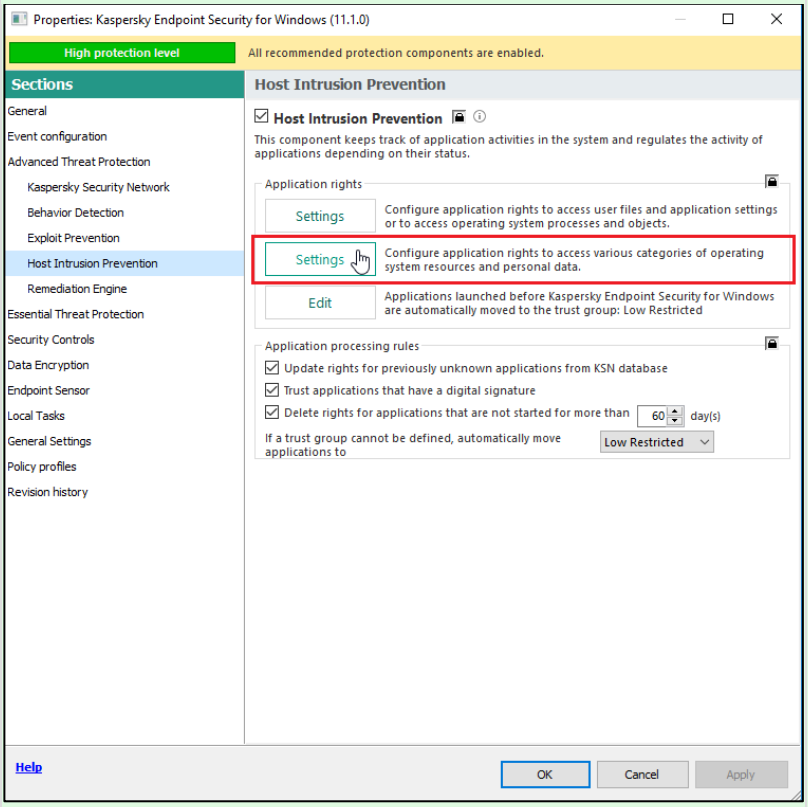
Open the active **Kaspersky Endpoint Security** policy in Kaspersky Security Center and select **Configure policy**.



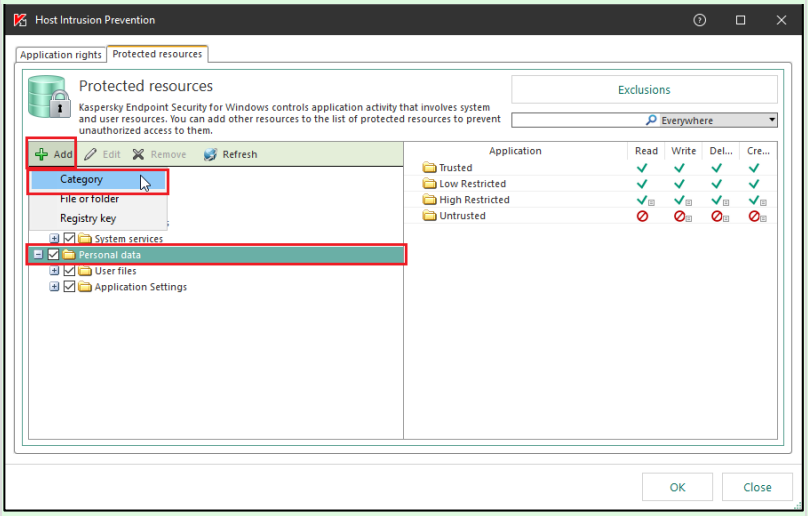
Select the **Advanced Threat Protection → Host Intrusion Prevention** tab.



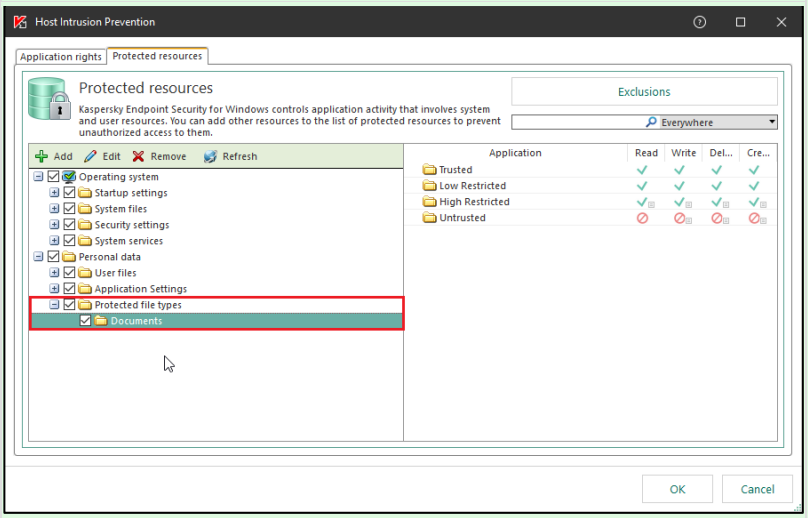
Click the **Settings** button to configure application rights to access operating system resources and personal data.



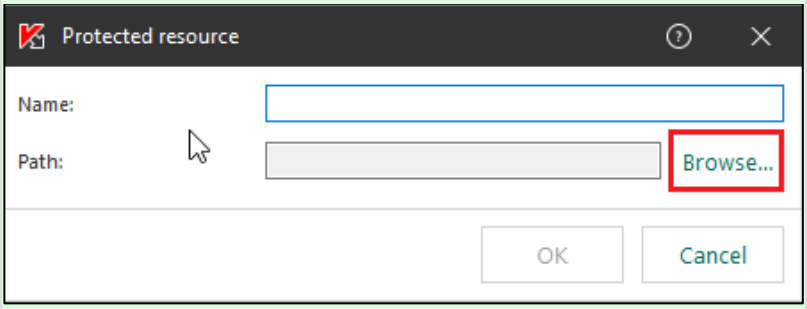
Select **Personal data**, click **Add**, and select **Category**.

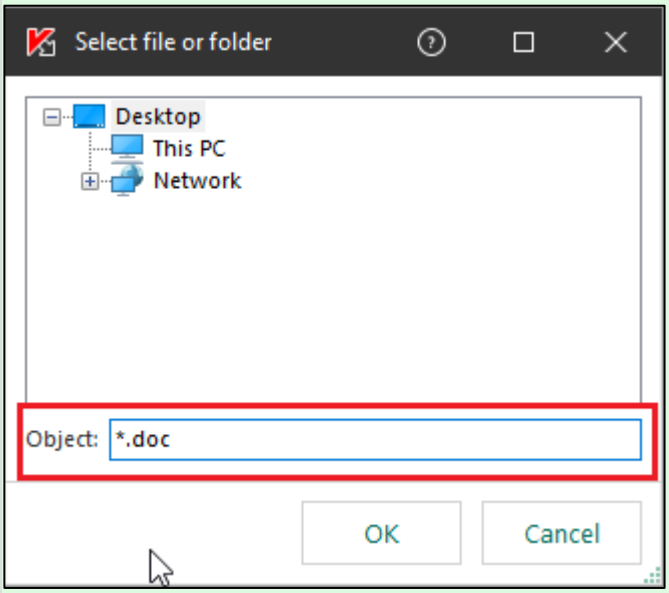


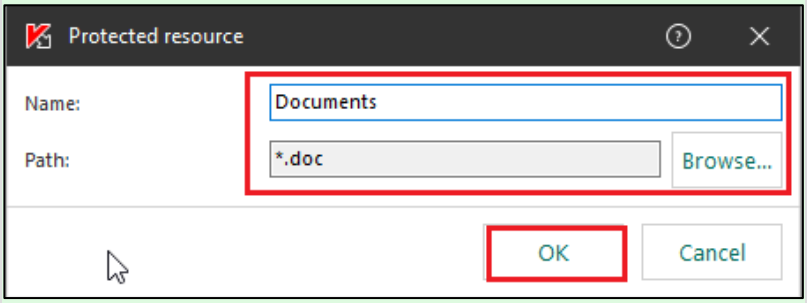
Create the category **Protected file types** and the subcategory **Documents**.



Click **Add** → **File or folder** and add to the **Documents** category the paths to the folders containing documents and the extensions of files containing documents such as *.**doc**. Repeat the last two steps to add all extensions specified in the table to the list of protected data.

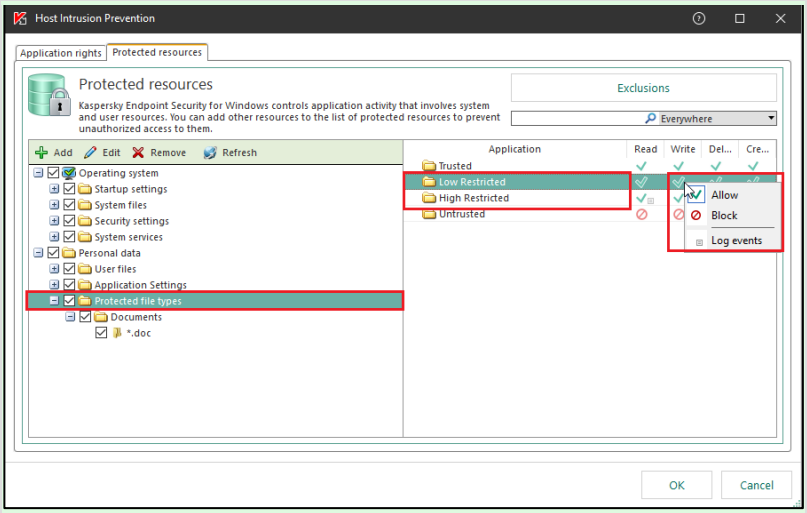


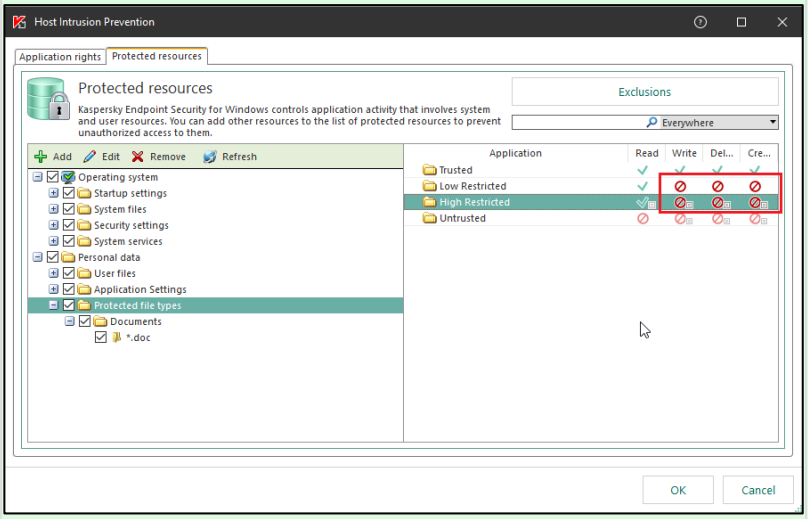




Configure the access permissions to the **Protected file types** group for applications belonging to the **Low Restricted** and **High Restricted** trust groups.

Block the actions **Write**, **Delete**, and **Create**.

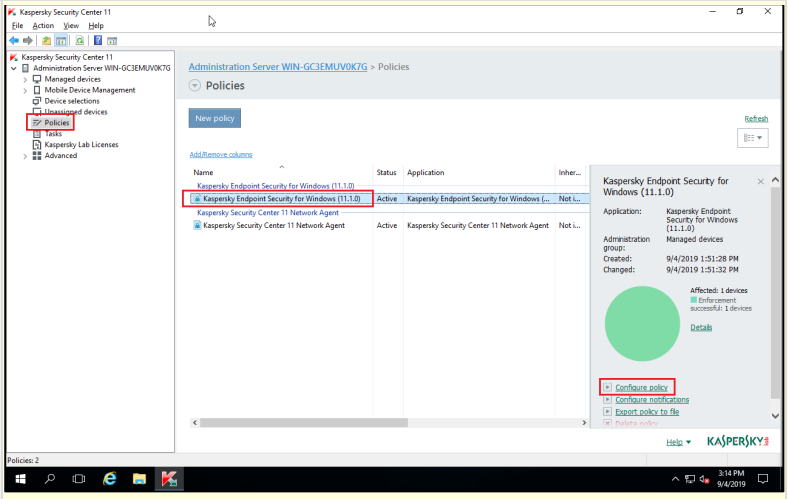




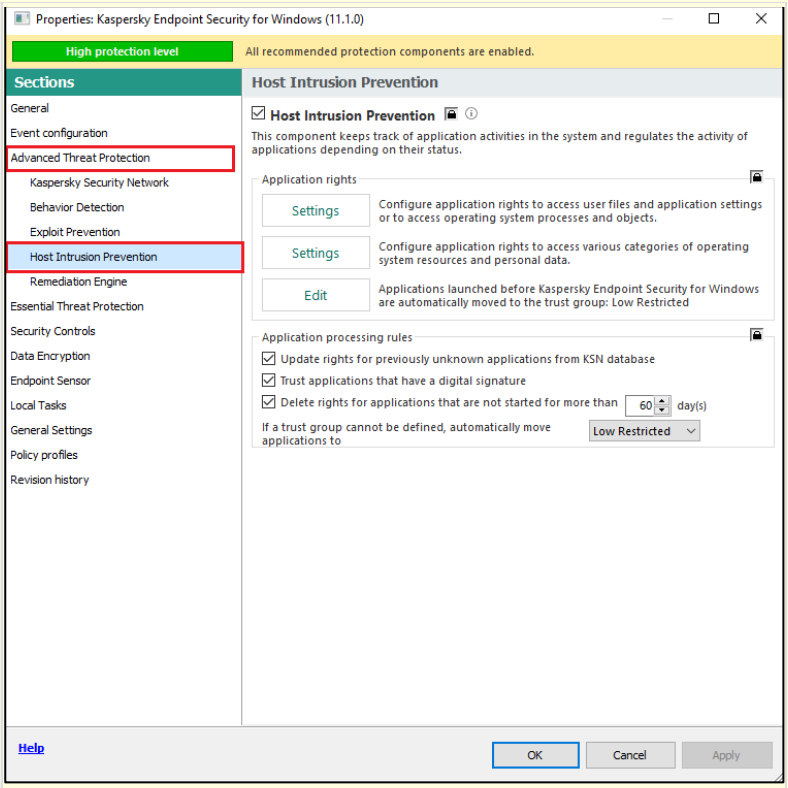
If a useful application ended up in the Low Restricted group and cannot work with documents

If a useful application ended up in the **Low Restricted** group and cannot work with documents, move the application to the **Trusted** category:

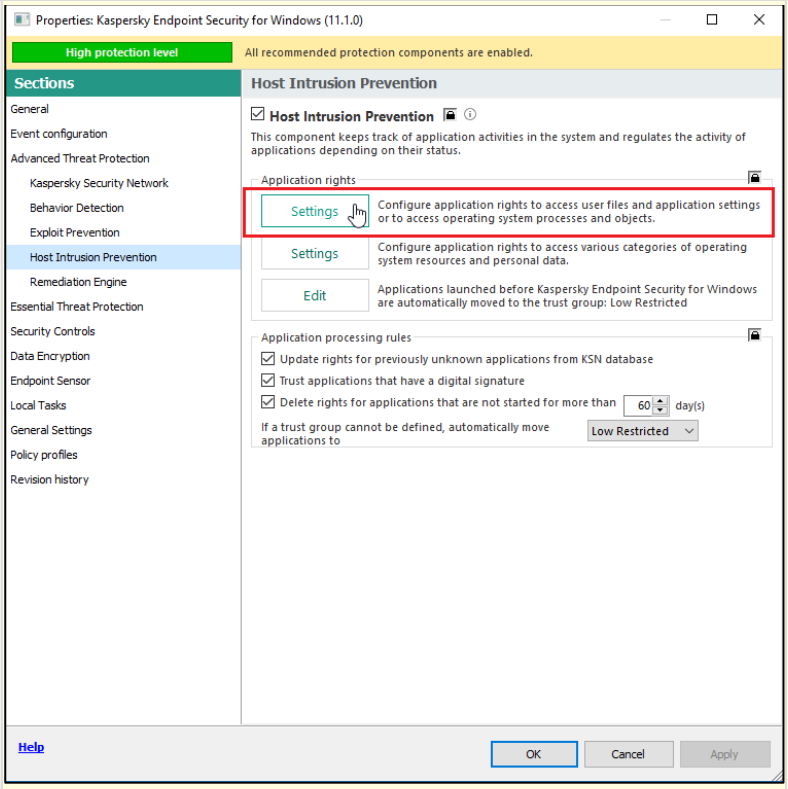
Open the active **Kaspersky Endpoint Security** policy in Kaspersky Security Center and select **Configure policy**.

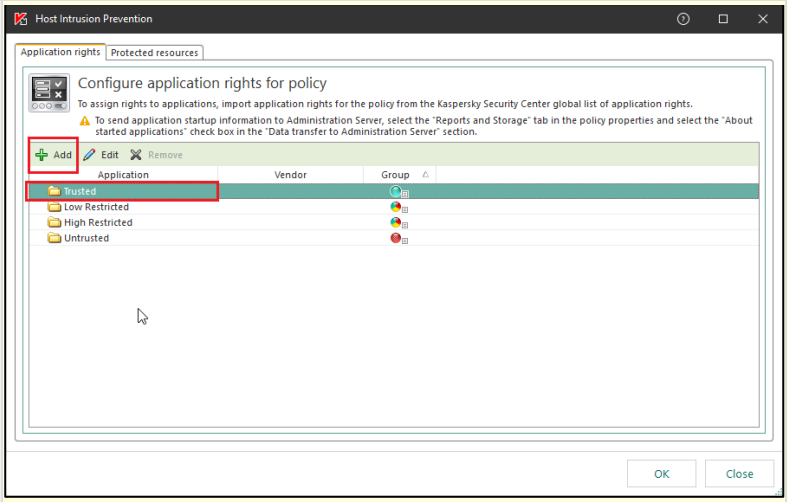
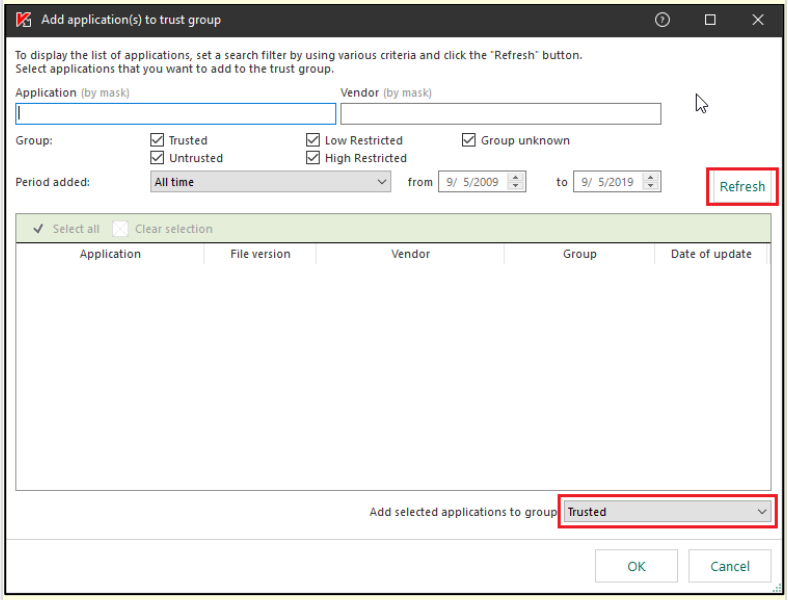


Select the **Advanced Threat Protection → Host Intrusion Prevention** tab.



Click the **Settings** button to configure application rights to access user files and application settings.



Select the **Trusted** group and click **Add**.	
Mark the necessary applications in the list and select the **Trusted** group in the lower right corner. If the list is empty, click the **Refresh** button.	

Protection of file servers

Protection of file servers is configured by using tasks of **Kaspersky Security 10.1.2 for Windows Server**. This is an individual product that blocks the spreading of encryptors over a network.

Basic settings

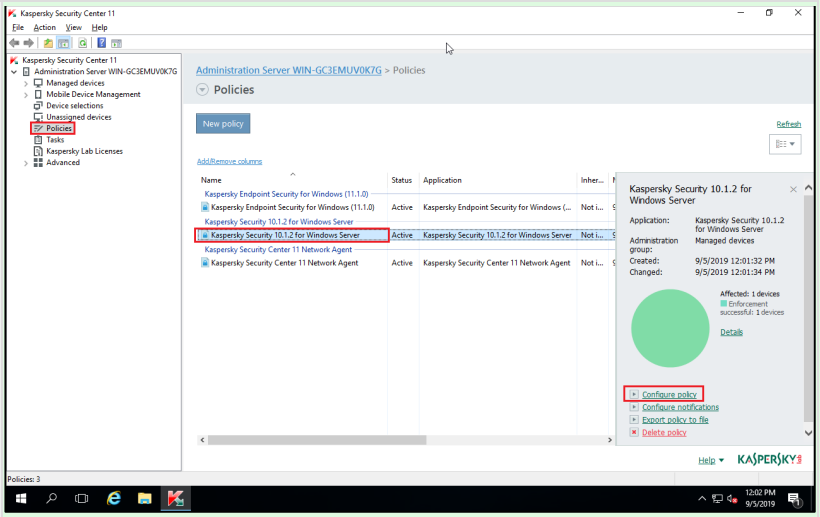
Protection of a server against penetration of malicious objects is provided by the **Real-Time File Protection** component. This component scans all files received by the server and can disinfect or delete infected files if necessary.

Additional settings

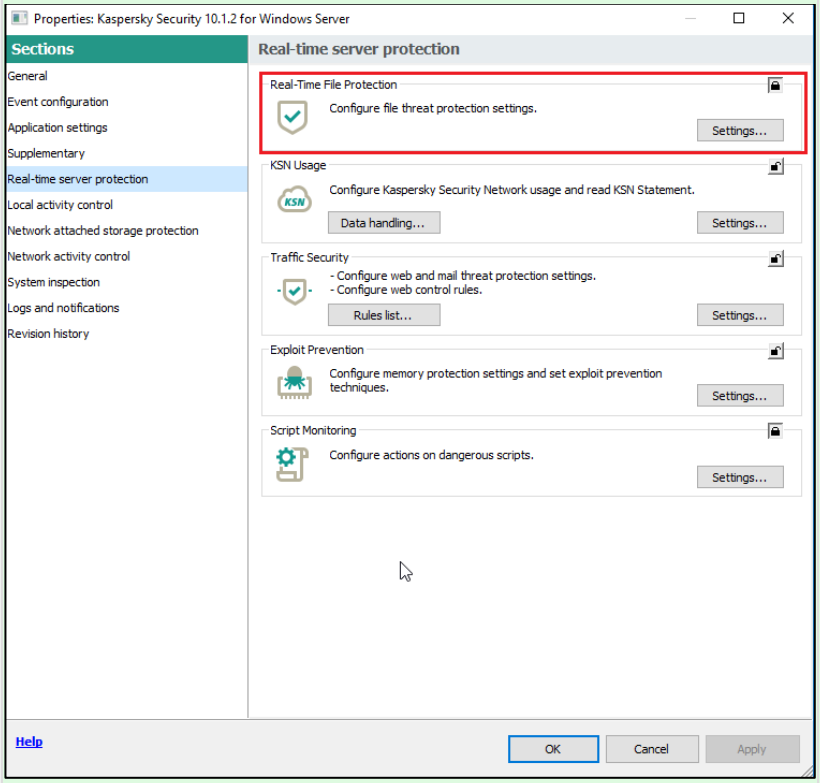
In addition to **Real-Time File Protection**, protection of network folders on servers against encryptors requires activation of **Anti-Cryptor**.

How to check if these tasks are running under a policy of Kaspersky Security 10 for Windows Server

Open the active **Kaspersky Security 10.1.2 for Windows Server** policy in Kaspersky Security Center and select **Configure policy**.

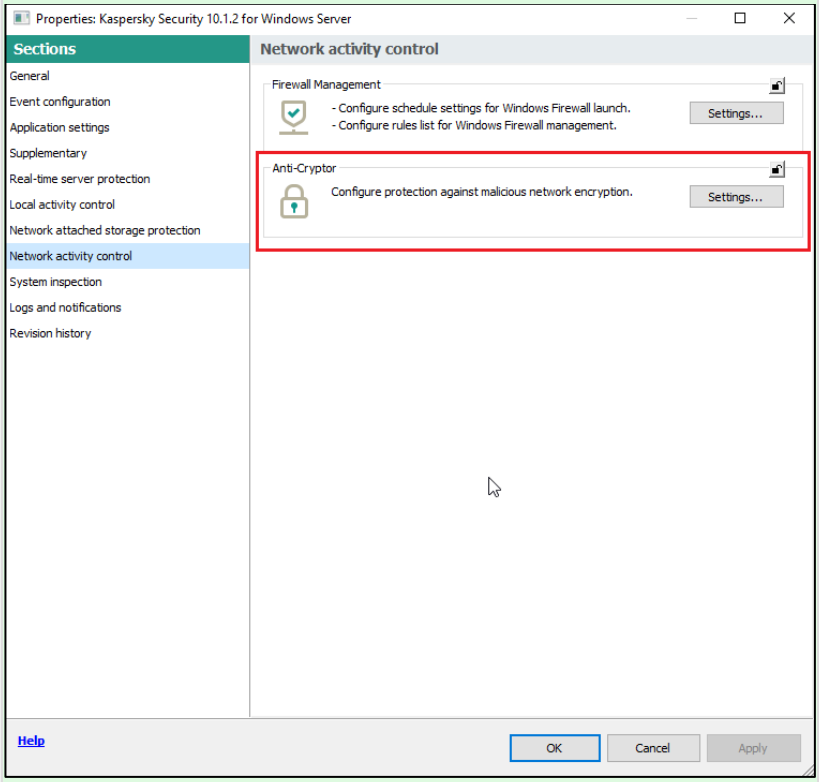


Select the **Real-time server protection** tab. Enter the settings of the **Real-Time File Protection** task and make sure that it is running.



Switch to the **Network activity control** tab. Enter the settings of the **Anti-Cryptor** task and make sure that it is running.

Do not forget to recess the lock icon for all tasks.



New in Kaspersky Security 10.1.x for Windows Server

*The **Untrusted Hosts Blocking** feature has been simplified: now the **Real-Time File Protection** and **Anti-Cryptor** components put identifiers for compromised hosts in the **Blocked Hosts** storage.*

You can disable the population of Blocked Hosts storage in the protection task settings. You can also view information about all blocked hosts in a list in the Application Console.

The Default Deny policy can also be configured to protect a server. It is implemented by using **Application Control** rules.

What to do if an infection occurs

If an encryptor nonetheless somehow infiltrated a device and has encrypted files, you must perform the following:

1. If backup copying of data was performed regularly, you can restore lost data from the backup copy.

You can also save 2–3 encrypted files or an email/malicious attachment, as well as reports and trace files of the anti-virus product so that you can send them to Kaspersky Technical Support specialists for analysis.

2. If you do not have a backup copy of files on a damaged system, you should try to restore the files using **decryptor utilities developed by Kaspersky**. It is likely that the encryptor that attacked the device is already known to Kaspersky experts and the files damaged by it can be decrypted.

The utilities are regularly updated. Newly detected decryption keys and algorithms are added to their databases. If you were unable to decrypt files on the first attempt, keep looking out for the release of updated versions of utilities. It is possible that the algorithm for decrypting your files will be added with the next update of the decryptor databases.

3. If you were unable to decrypt files using the utilities, you should contact Kaspersky Technical Support. Please attach the following data to your query:

- 2-3 encrypted files and their unencrypted originals (if available)
- the phishing email or the infected attachment (if feasible)

Due to the reasons indicated earlier, Kaspersky experts cannot guarantee that damaged files will be decrypted.

If the submitted modification of the encryptor had not been previously detected, a new signature will be added to the databases.

After a new signature has been added to the databases, you must run a full scan of the device that was attacked. You should connect the device to the network only after completing a scan and disinfection (if required).