kaspersky

Performance Best Practices

Kaspersky Endpoint Security for Windows

Evgeniya Kirikova
Kaspersky

04.12.2020

kaspersky

Kaspersky Endpoint Security for Windows:

Performance Best Practices

About this document

Here you can find some recommendations how to configure protection in Kaspersky Endpoint Security for Windows and reduce the impact on the system.

Contact support If you follow recommendations listed in this document but still experience performance issues.

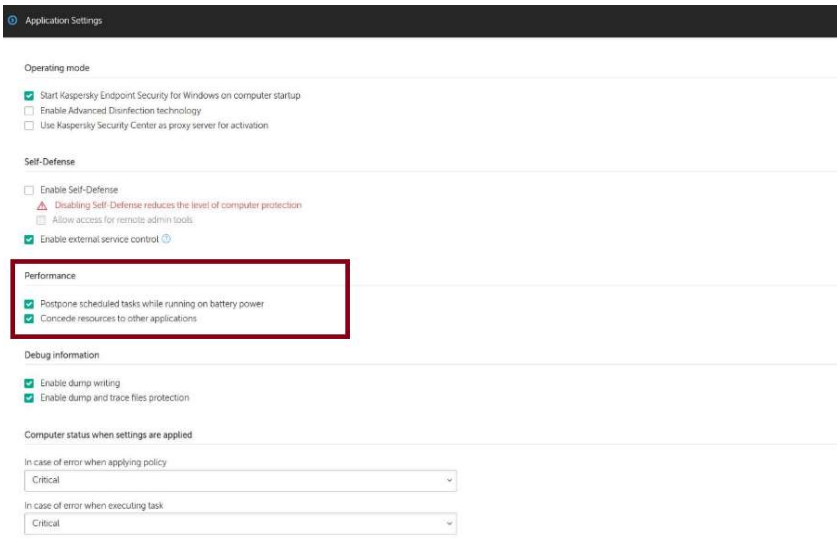
Contents

General recommendations

1. Use the latest versions of Kaspersky Endpoint Security for Windows, as they contain the latest fixes and improvements, including performance related.

2. We recommend you to use all protection components with default settings. They provide the optimal balance between protection level and performance recommended by our experts.

3. Check KES for Windows policy and make sure that general performance settings are enabled (KES policy → General → Application settings):



Use Background Scan instead of any other scan tasks (workstations)

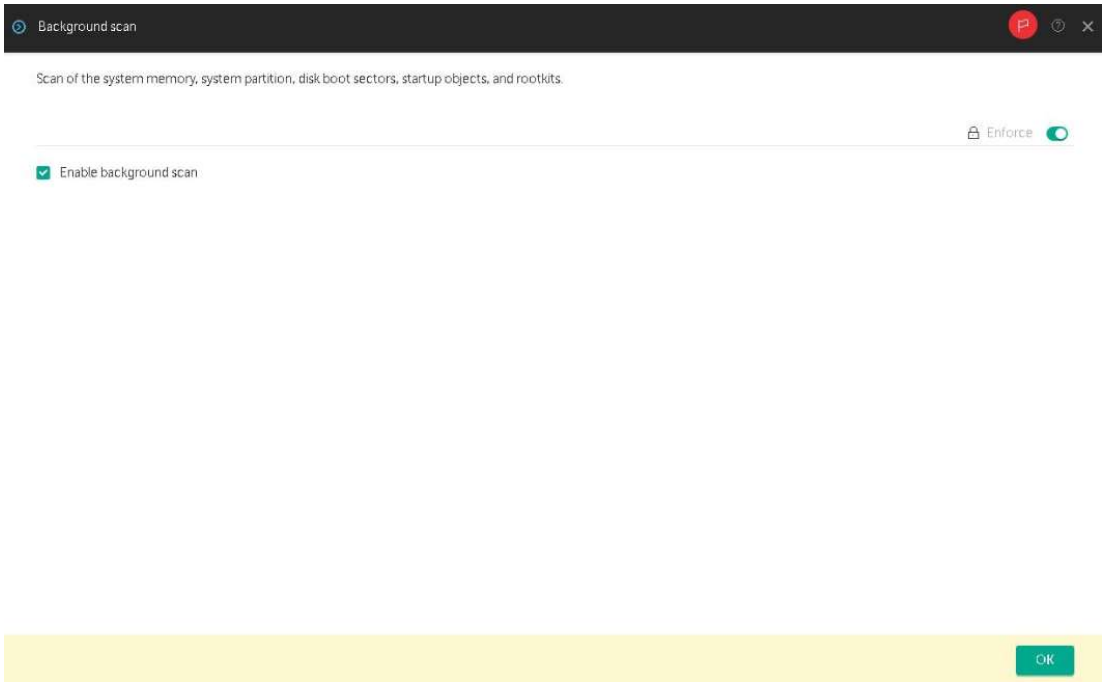
Since KES for Windows 11.1.0, recommendations for **workstations** are to use the Background Scan task instead of any other scan tasks if not absolutely necessary.

Background Scan task settings have been optimized for workstations to provide a sufficient level of protection while reducing the impact on system performance. Background Scan scope include the following areas: kernel memory and system drive are scanned every week, and running processes, startup objects and boot sectors are scanned every day.

In latest versions of KES for Windows group scan tasks are not created by default and are not recommended to use on workstations as redundant and heavy. So there is no need in full scan or critical objects scan tasks on workstations if you use Background Scan task. Thus, if you have KES for Windows 11.1.0 or newer versions installed on your computers, then we strongly recommend making the following settings:

- **Enable Background Scan** in KES for Windows policy *for workstations* (see screenshot below).

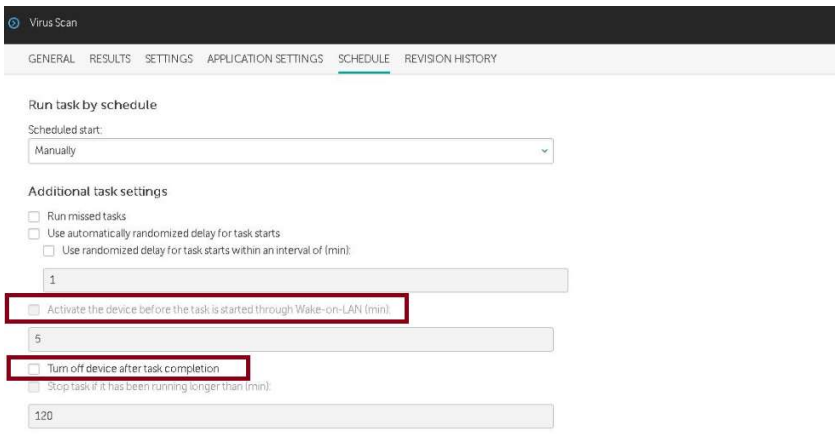
- Switch group malware scan tasks that you used *for workstations*, to manual mode and use them only in special cases (not recommended).



Scan settings recommendations (workstations)

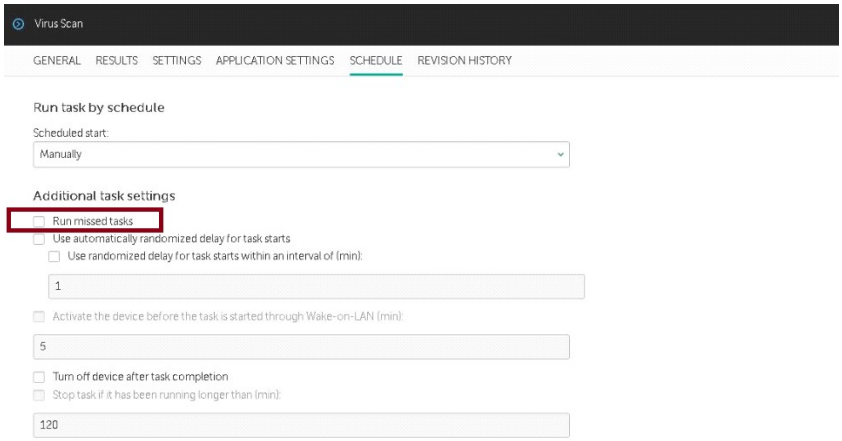
Beginning with KES 11.1.0 for Windows, if you enable Background Scan task *on workstation*, there is no need in regular full scan or critical objects scan tasks. These group scan tasks are not created by default and are not recommended for use as redundant and heavy.

But if you still need to use malware scan tasks on a regular basis (not recommended), then we ask you to pay attention to the settings described below, that will help you to decrease the impact on system performance.

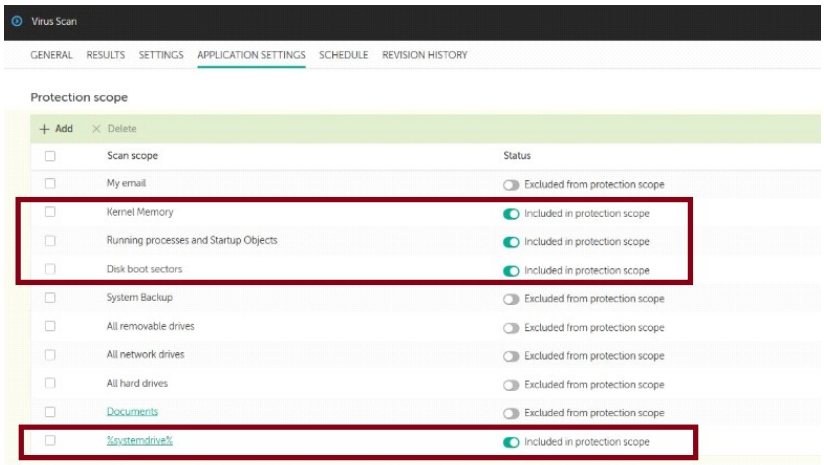


Scan time. If possible, configure scan tasks to run **outside the working hours**, when computers are on, but they are less loaded (servers) or virus scanning will not affect the users. For example, at night or on weekends.

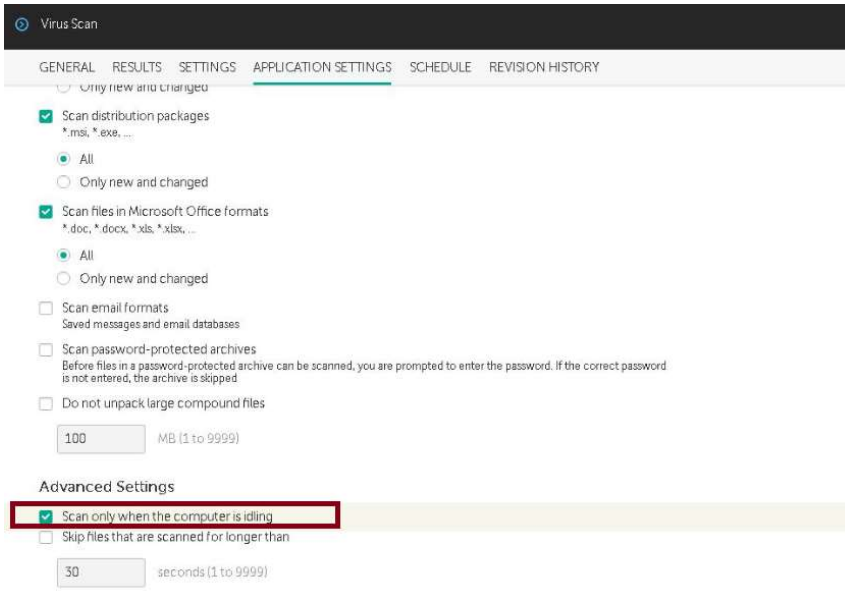
If you cannot arrange that users do not turn off their computers at night, use Wake-On-LAN to power on the computers at night and run the virus scan task instead of “Run missing tasks” option. Also, if you use Wake-On-Lan, you can use “Turn off device after task completion” option.



In cases of regular scan tasks (e.g. weekly) we do not recommend to use “Run missing tasks” option. Run missed tasks means the following: if computer is turned off at the scheduled time, the task will start as soon as the computer is switched on. So, if you schedule your group task to run every night, but computer was turned off, the task will start in the morning when the user turns on the computer. That may hamper user activities.

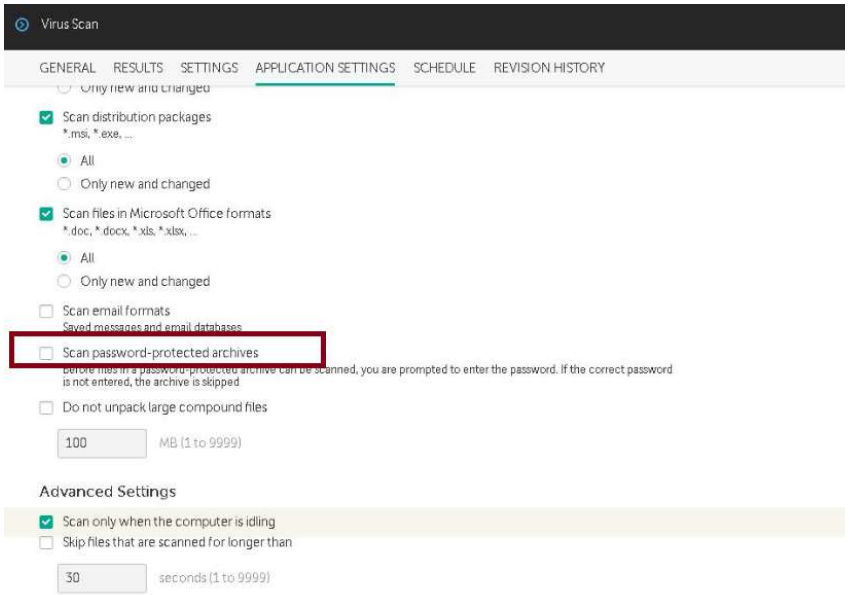


Scan scope. For tasks that are run on regular basis use the following areas when you schedule group scan task: kernel memory, running processes and startup objects, boot sectors, system disk.



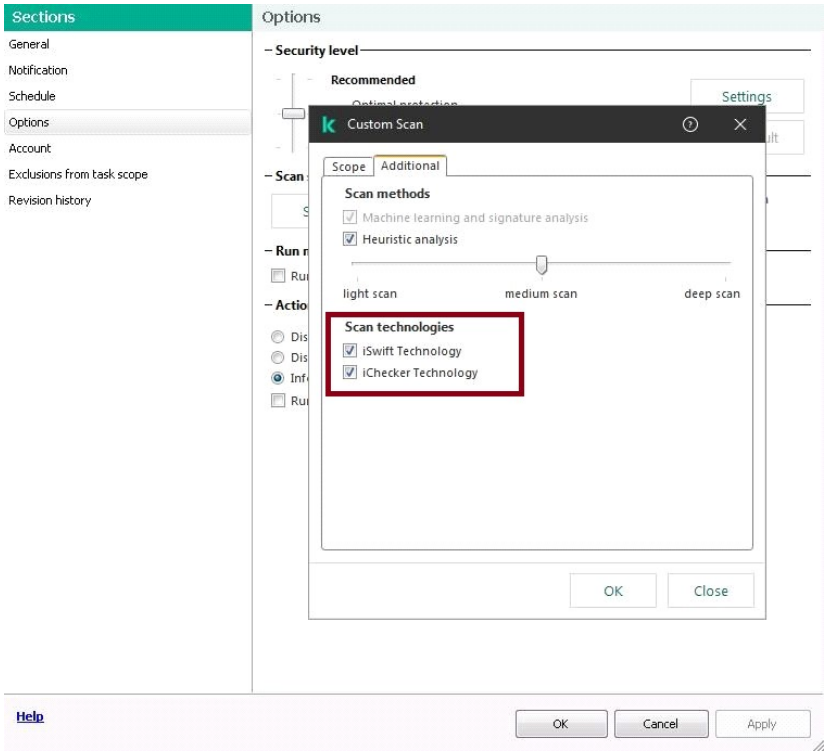
Use **idle scanning**, if you can't arrange scanning outside the working hours.

In this mode, scanning will be performed only when computer is not used (locked or a screensaver is active), otherwise, the task will be paused.



Do not enable password-protected archives scanning.

When scanning password-protected archives, Kaspersky Endpoint Security will prompt the active user for the password to unpack the archive. Since we recommend to run scheduled scans in off hours when there is no active user, there is no need in this option. Use this option in manual scans performed locally.



Do not turn off **iSwift and iChecker Technology** options, if you use MMC console (there is already no such option in Web console).

These parameters enable the mode when KES does not scan files at each access, but never completely trusts already scanned files; it has logic to re-scan them according to some triggers (for example, with newer antivirus databases).

Disabling these parameters either have no effect (if the Scan only new and changed files feature is enabled) or will lead to more scans and slow down the computer.

Scan settings recommendations (servers)

Use the following recommendations in group scanning tasks that are run on servers:

- **Scan time.** If possible, configure scan tasks to run **outside the working hours (or periods of minimal load on servers)**, when servers are less loaded, so scanning will not affect the users. For example, at night or on weekends.

- Do not turn off **iSwift and iChecker Technology** options, if you use MMC console (there is already no such option in Web console).
  These parameters enable the mode when KES does not scan files at each access, but never completely trusts already scanned files; it has logic to re-scan them according to some triggers (for example, with newer antivirus databases).

- **Do not enable password-protected archives scanning.** When scanning password-protected archives, Kaspersky Endpoint Security will prompt the active user for the password to unpack the archive. Since we recommend to run scheduled scans in off hours when there is no active user, there is no need in this option. Use this option in manual scans performed locally.

Use Kaspersky Security Network

We strictly recommend you to **use Kaspersky Security Network** as it gives you faster responses of the application to new threats, **improves the performance of protection components** and reduces false positives.

Kaspersky Security Network (KSN) is an infrastructure of cloud services providing access to the online database that contains worldwide information about reputation of files, web resources, and software.

Use following recommendations when you configure KSN usage:

- Use Kaspersky Security Network with “Extended KSN mode” option disabled, if you don’t want to send Kaspersky statistical information that is generated during participation in KSN.

- Use **Kaspersky Private Security Network**, if you don’t want to transmit any data to Kaspersky. Kaspersky Private Security Network (KPSN) is a private version of KSN that allows enterprises to boost their detection speed with access to real-time global threat intelligence without sharing any data outside their corporate network. For more information about KPSN visit https://www.kaspersky.com/enterprise-security/private-security-network.

- Enable **Cloud mode** if you enable KSN usage. Cloud mode refers to the application operating mode in which KES uses a light version of anti-virus databases. The light version of anti-virus databases utilizes less computer RAM that would otherwise be used with the usual databases. If you do not participate in KSN or if cloud mode is disabled, KES downloads the full version of anti-virus databases from Kaspersky servers.