Performance Best Practices

Kaspersky Endpoint Security for Windows

Evgeniya Kirikova Kaspersky

04.12.2020

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	2
Use Background Scan instead of any other scan tasks (workstations)	2
Scan settings recommendations (workstations)	3
Scan settings recommendations (servers)	6
Use Kaspersky Security Network	7

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):

	Application Settings
	Operating mode
	Start Kaspersky Endpoint Security for Windows on computer startup Enable Advanced Distriction technology Use Kaspersky Security Center a proxy server for activation
	Self-Defense
	Enabling Self-Defense Allow access for remote admin tools: Allow access for remote admin tools: Enable Sector Sector 20 Enable Sector Sector 20
ſ	Performance Performance
	C Concrete resources to other applications Debug information
	Enable dump writing Enable dump and trace files protection
	Computer status when settings are applied
	In case of error when applying policy Critical
	In case of error when executing task Critical ~

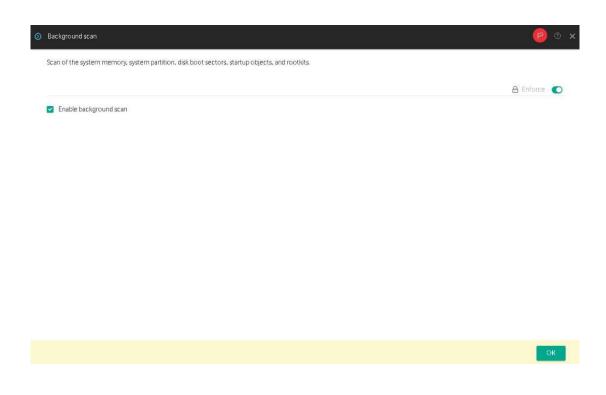
Use Background Scan instead of any other scan tasks (workstations)

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.

Virus Sca	an														
GENERA	L RE	SULTS	SETTING	GS A	PPLICA	tion se	TINGS	SCHEDULE	RE	/ISION	HISTOP	Y			
Run tas	sk by	sched	ule												
Schedule															
Manual	ly												1	~	
	missed automa		indomize	d dela	y for tas	k starts									
Use a	automa	tically r	indomize delay for				erval of (min):							
Use a	automa Ise ranc	itically r Iomized	delay for	task st	arts witi	hin an int		min): on-LAN (min)							
Use a	automa Ise ranc	itically r Iomized	delay for	task st	arts witi	hin an int									
Use a Use a U 1 Activ 5 	automa lse rand vate the	itically r Iomized e device	delay for	task st e task npletic	arts witl is starte n	hin an inti									

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.

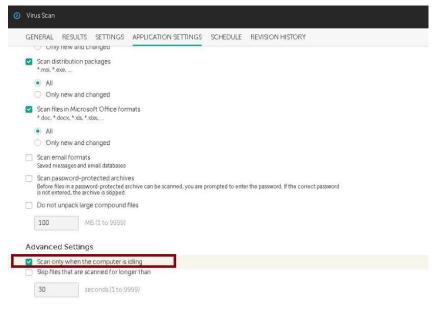
If you cannot arrange that users do not turn off their computers at night, use Wake-On-LAN to power on the computers at night and run the virus scan task instead of "Run missing tasks" option. Also, if you use Wake-On-Lan, you can use "Turn off device after task completion" option.

	n											
GENERAL	. RESULTS	SETTINGS	APPLICATION	SETTINGS	SCHEDULE	RE	VISION	N HISTOR	۲Y			
Run tas	k by sched	ule										
Schedule												
Manually	4									~		
Additio	nal task set	tings										
	at a search to set as											
	nissed tasks]										
🗌 Use a	utomatically r		lay for task start									
🗌 Use a	utomatically r		lay for task start starts within an		nin):							
🗌 Use a	utomatically r				min):							
Use a	utomatically r e randomized	delay for task	starts within an	interval of (r								
Use a	utomatically r e randomized	delay for task		interval of (r								
Use a	utomatically r e randomized	delay for task	starts within an	interval of (r								
Use a	utomatically r e randomized	delay for task	starts within an	interval of (r								
Use a Use a Use a Use a	utomatically r e randomized ate the device off device afte	delay for task before the ta r task comple	starts within an	interval of (r								
Use a Use a Use a Use a Activ Activ 5 Tum a	utomatically r e randomized ate the device off device afte	delay for task before the ta r task comple	starts within an k is started thro ion	interval of (r								

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.

Virus Scan			
GENERAL	RESULTS SETTINGS APPLICATION SETTINGS	SCHEDULE REVISION HISTORY	
Protection	scope		
+ Add	× Delete		
	Scan scope		Status
	My email		Excluded from protection scope
	Kernel Memory		Included in protection scope
	Running processes and Startup Objects		 Included in protection scope
	Disk boot sectors		Included in protection scope
	System Backup		Excluded from protection scope
	All removable drives		Excluded from protection scope
	All network drives		Excluded from protection scope
	All hard drives		Excluded from protection scope
	Documents		Excluded from protection scope
	%systemdrive%		Included in protection scope



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.

Viri	us Scan
	NERAL RESULTS SETTINGS APPLICATION SETTINGS SCHEDULE REVISION HISTORY
	Scan distribution packages *.msi, *.exe
	IIA 💿
	Only new and changed
	Scan files in Microsoft Office formats *.doc, *.docx, *.xls, *.xlsx,
	IIA 💿
	Only new and changed
	Scan email formats Seved messages and email databases
	Scan password-protected archives
	percremes in a password protected archive can be scanned, you are prompted to enter the password. If the correct password is not entered, the archive is skipped
n	Do not unpack large compound files
	100 MB (1 to 9999)
Ad	ivanced Settings
	Scan only when the computer is idling
	Skip files that are scanned for longer than

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.

Sections	Options
Seneral	- Security level
lotification	Recommended
chedule	Ontimal protection Settings
Options	Custom Scan 💿 🗙
ccount	
ixclusions from task scope tevision history	- Scan Scope Additional Scan methods ✓ Machine learning and signature analysis - Run r ✓ Heuristic analysis - Actio ✓ Iight scan medium scan Dis Ø ✓ Swift Technology ✓ IChecker Technology ✓
Help	OK Close

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 rescan 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 <u>https://www.kaspersky.com/enterprise-security/private-security-network</u>.
- 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.

	Kaspersky Security Network	
19	 The component settings are as recommended. 	
	KSN Settings	
	Kaspersky Security Network ENABLED Kaspersky Security Network ENABLED kaspersky Security Network (KSN) is a cloud-based knowledge base that contains information about the reputation over resources, and raitware. The use of data from Kaspersky Security Yorthoode ensures taster responses of the new threas, improve the performance of protection components, and relations the MeRHood of Table positives.	e application to
L	KSN provider: Private KSN	
L	C Extended KSN mode ENABLED	
Е	KSN Statement	
I	Cloud mode ENABLED () The application uses a light version of anti-virus databases which lowers the operating system load. This mode, is enabled or advalled after the application statutates are updated	
-	Computer status when KSN servers are unavailable	
	Critical	u]