ESET Tech Center

Knowledgebase > Diagnostics > How do I use ESET Log Collector?

How do I use ESET Log Collector?

Anish | ESET Nederland - 2024-02-14 - Comments (0) - Diagnostics

Issue

- How to use ESET Log Collector
- <u>See more information about ESET Log Collector</u>

Solution

How to use the ESET Log Collector youtube video (in Dutch): https://youtu.be/A4zuky_I-S4

macOS users | Linux users

ESET PROTECT users You can run ESET Log Collector on a remote client computer via ESET PROTECT <u>Diagnostics Client Task</u>.

- 1. Download the ESET Log Collector.
- 2. After the tool has finished downloading, double-click it to run the tool.
- 3. Click **I Accept** to accept the End User License Agreement (EULA).
- Select All in the Collection Profile drop-down menu unless ESET Technical Support instructs you to select a different option. <u>Read more about the Collection Profile</u> <u>options in Online Help.</u>

€ ESET Log Collector		- 0	×	
ESET Endpoint Security 10.0.2045.0			_	
Collection profile Default V		Collect	0	
Threat detection			^	
None Custom nan dies and loaded DLLs)				
System Configuration				
Devices info Services Registry key content				
Windows Updates PowerShell history				
ESET SysInspector log				
Network configuration Winsock LSP catalog				
WFP filters			~	
Logs age limit [days]	ESET logs collection mode			
30 ~	Original binary from disk		\sim	
Save archive as			_	
C: \Users\Steef\Downloads\ees_logs.zip				
Protect archive by password ④				
Operation log				
[16:54:15] ESET Log Collector v4.9.0.0 (02/06/2023) - 64 bit [16:54:15] Copyright (c) 1992-2023 ESET, spol. s r.o. All rights reserved. [16:54:15] [16:54:15] Detected product type: ees				
			~	
<			>	

5. Click **Browse** next to **Save archive as**, specify the location where you want to save archive files and then click **Save** (the archive filename is already pre-defined).

Save As						×
← → ~ ↑ ↓ > Tr	nis PC > Downloads	~	Ō	Search Downlo	ads	0
Organize 👻 New fold	ler				· · ·	?
🖈 Quick access	Name	Date modified	Туре		Size	
 OneDrive 		No items match your search				
💻 This PC						
3D Objects						
Desktop						
Downloads						
Music						
E Pictures						
📑 Videos						
🏪 Local Disk (C:)						
i Network						
File name: ees_l	logs.zip					~
Save as type: ZIP A				X		~
∧ Hide Folders				Save	Cance	

6. We advise to use the **Protect archive by password** option, because the output could contain sensitive data.

ESET Log Collector		_		Х
ESET Endpoint Security 10.0.2045.0				
Collection profile		Colle	ect	0
All ~				1
Artifacts to collect				
Windows Processes				^
Running processes (open handles and loaded DLLs)				
System Configuration				
Drives info				
Devices info				
Services Registry key content				
Windows Updates PowerShell history				
ESET SysInspector log				
Network configuration				
✓ Winsock LSP catalog				
WFP filters				
Complete Windows Registry content				~
Logs age limit [days]	ESET logs collection mode			
30 ~	Original binary from disk			\sim
Save archive as				
C:\Users\Steef\Downloads\ees_logs.zip				
Protect archive by password ④				
Operation log				
[16:54:15] ESET Log Collector v4.9.0.0 (02/06/2023) - 64 bit [16:54:15] Copyright (c) 1992-2023 ESET, spol. s r.o. All rights reserved. [16:54:15] [16:54:15] Detected product type: ees				
<			>	Ť

7. Click **Collect**. The collection might take some time to complete. The **Operation Log** window will display what operation is currently in progress.

en ESET Log Collector	– 🗆 X		
ESET Endpoint Security 10.0.2045.0 Collection profile Default	Collect		
Artifacts to collect Windows Processes Running processes (open handles and loader System Configuration Drives info Devices info Services Registry key content Windows Updates PowerShell history ESET SysInspector log Winsock LSP catalog WFP filters Complete Windows Registry content	d DLLs)		
Logs age limit [days] 30 Save archive as	ESET logs collection mode Original binary from disk V		
C:\Users\Steef\Downloads\ees_logs.zip	· · · · · · · · · · · · · · · · · · ·		
Protect archive by password ①			
Operation log [10:05:14] ESET Log Collector v4.9.0.0 (02/06/: [10:05:14] Copyright (c) 1992-2023 ESET, spol. [10:05:14] [10:05:14] Detected product type: ees			
<	>		

8. When the collection is finished, the "Files have been collected and archived" message will be displayed. This means that the collection was successful, and the archive file (for example, ees_logs.zip) is saved in the location specified in step 6. If you already have a case open with ESET Technical Support, you can submit the log files as an email attachment when you respond to ESET. If you do not have a case open, <u>contact ESET Technical Support</u>. If the output from the log collector is too large to e-mail, follow <u>this guide</u> for uploading large files.

Related Content

- Use ESET LogCollector on macOS and send the logs to ESET Technical Support
- Create a full memory dump of a VMware virtual machine
- How do I generate a memory dump manually?
- How to create a Wireshark log
- <u>Run the Info_get.command on a Linux machine and send the logs to ESET Technical</u> <u>Support</u>

- Using tcpdump on a MacOS
- Using Process Monitor to create log files
- Using tcpdump on a Virtual Appliance

Comments (0)