# **ESET Tech Center**

Kennisbank > ESET Endpoint Encryption > Diagnostics > How do I generate a memory dump manually?

## How do I generate a memory dump manually?

Steef | ESET Nederland - 2021-07-07 - Reacties (0) - Diagnostics

#### Issue

• ESET technical support has asked you to generate a memory dump file for analysis to help them resolve an issue with your computer.

### Solution

#### Before you begin:

- Only follow the steps below if you have been advised to do so by ESET technical support
- In most cases, ESET technical support will request your SysInspector log in addition to a memory dump. <u>View instructions to collect and submit a SysInspector log.</u>
- The steps will vary depending on what type of keyboard you have (PS/2 or USB). To determine your keyboard type, open the Control Panel, double-click Keyboard, and then click the Hardware tab. Your keyboard will be listed in the Devices section.

	Keyboard Properties	8	
eed Hardware	•		
evices:			
Name		Туре	
Standard PS/2 Keyboard		Keyboards	
Device Propert	ies		
Manufacturer:	(Standard keyboards)		
Location:	plugged into keyboard port		
Device status:	This device is working properly.		
		Properties	
	ОКС	ancel Apply	

## I. Configure memory dump settings

1. Press the Windows key + **R**, type **sysdm.cpl** into the **Open** field and click **OK**.

🖅 Run	22
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
<u>O</u> pen:	sysdm.cpl 🗸
1	OK Cancel <u>B</u> rowse

## Figure 1-2

2. Select the **Advanced** tab and click **Settings** in the **Startup and Recovery** section.

Computer Name       Hardware       Advanced       System Protection       Remote         You must be logged on as an Administrator to make most of these changes.       Performance         Visual effects, processor scheduling, memory usage, and virtual memory       Settings
You must be logged on as an Administrator to make most of these changes. Performance Visual effects, processor scheduling, memory usage, and virtual memory Settings
Performance Visual effects, processor scheduling, memory usage, and virtual memory Settings
Visual effects, processor scheduling, memory usage, and virtual memory
Settings
User Profiles
Desktop settings related to your logon
Settings
Startup and Recovery
System startup, system failure, and debugging information
2 Settings
Environment Variables
OK Cancel Apply



 The **Dump file** section allows you to set the location where new memory dump files are saved. The **%SystemRoot%** string is a Microsoft Windows variable that stands for the root directory of your Microsoft Windows installation (typically the default value is *C:Windows*).

In the **Write debugging information** section, you can select the type of memory dump (we recommend that you use the **Complete** setting, see Figure 1-4). **Don't see the Complete memory dump option?** If the **Complete memory dump** option is missing, <u>click here for instructions</u>.

 <u>Click to bookmark this article before you continue</u> and then click **OK** to restart your computer. After your computer restarts, continue to part II to generate a memory dump manually.

tup and Recovery	×
ystem startup Default operating system:	
Windows 7	
<ul> <li>Time to display list of operating systems: 30 seconds</li> <li>Time to display recovery options when needed: 30 seconds</li> </ul>	
ystem failure	
<ul> <li>Write an event to the system log</li> <li>✓ Automatically restart</li> </ul>	
Write debugging information Complete memory dump	
Dump file: %SystemRoot%\MEMORY.DMP	
Overwrite any existing file	
	1



#### II. Generate a memory dump manually

#### Use caution when editing the registry

Make only the edits specified below to the system registry. Unnecessary changes to the registry can negatively affect system performance.

- Press the Windows key + R to open a Run dialog, type regedit and click OK. If you are prompted by Windows, click Yes.
- In the Registry Editor window, expand HKEY\_LOCAL\_MACHINE → SYSTEM → CurrentControlSet → Services → kbdhid → Parameters. PS/2 keyboards

If you are using a PS/2 keyboard, expand **HKEY\_LOCAL\_MACHINE**  $\rightarrow$  **System**  $\rightarrow$  **CurrentControlSet**  $\rightarrow$  **Services**  $\rightarrow$  **i8042prt**  $\rightarrow$  **Parameters** (we are using a USB keyboard in this example—kbhid is expanded in Figure 2-1).

 Right-click in the right pane and select New → DWORD or DWORD (32-bit value) depending on your operating system.



#### Figure 2-1

1. Name the key CrashOnCtrlScroll. Type 1 into the Value data field and click OK.



#### Figure 2-2

- 1. Close Registry Editor and restart your computer.
- Once your computer has started, press and hold the right CTRL key on your keyboard (you must use the right and not the left) and then press the Scroll Lock

key (located in the upper right on most keyboards) twice. The Windows forced crash dialog will run and a memory dump will be generated. Your computer may restart as a result.

3. Once your computer has started, navigate to your system's root directory (C:Windows by default) and locate the file named **MEMORY.DMP**. Respond to the last email from your case with ESET technical support and notify them that you are ready to submit your memory dump file. An ESET technical support agent will contact you with instructions to submit the file for analysis.

rganize 🔻 📄 Open	Burn Compatibility files	New folder			•	(
Favorites	Name	Date modified	Туре	Size		
i institut	1.00010000	7/13/2009 9:51 PM	Text Document	0 KB		
-Trentindi	10.10xxxxx.10.x00	11/20/2010 3:21 AM	Application extens	50 KB		
🗰 offices (Rivers	and independent	11/20/2010 4:24 AM	Application	70 KB		
A PRODUCT PROFESSION	and a manifest state	2/24/2011 10:19 PM	Application	2,805 KB		
	/ 1000001000000000000000000000000000000	5/20/2011 3:14 PM	Text Document	3 KB		
1.000000		5/20/2011 3:14 PM	Text Document	1 KB		
	March addressed Bri	2/10/2012 10:36 PM	Application	66 KB		
- companies	The International Contractory	4/23/2013 6:54 AM	Application	2,630 KB		
Charles ( Charles )	-Theorem	6/5/2013 10:47 AM	Text Document	6 KB		
·		6/5/2013 10:47 AM	Text Document	4 KB		
an and the state of the state o		6/5/2013 12:29 PM	Text Document	2 KB		
_	10001.00000	6/5/2013 3:33 PM	Text Document	4 KB		
	C. Hermanik	6/6/2013 11:22 AM	Text Document	10 KB		
O	MEMORY.DMP	6/21/2013 1:30 PM	DMP File	433,844 KB		
<b>–</b>		8/28/2013 3:02 PM	PROPERTIES File	6 KB		
	100 L 100 L	11/22/2013 12:04	Configuration sett	1 KB		
	ALL INVALUENCE	12/6/2013 12:04 PM	Configuration sett	1 KB		
	18881	12/13/2013 12:19	Text Document	202 KB		
		12/19/2013 6:46 AM	Text Document	4 KB		
	V MANAGAMAN DE LA PARA PARA	1/23/2014 4:31 PM	Text Document	1,506 KB		
	1 december and a second second	1/24/2014 8:24 AM	DAT File	66 KB		
	1 0001 0001	1/24/2014 8:24 AM	Text Document	66 KB		

#### Figure 2-3

#### Forcing a crash dump through NotMyFault.exe:

If you are unable to use the keyboard combination to trigger the crash and the system can be accessed while the problem is occurring, use the Microsoft Sysinternals NotMyFault tool to generate the crash dump. Follow these steps:

- Download the NotMyFault tool from <u>http://download.sysinternals.com/files/NotMyFault.zip.</u>
- 2. Click Start, Run, type cmd, and click OK.
- 3. At the command line, type NotMyFault.exe /crash, and then press Enter. The system crashes with Bug Check D1. A dump file is then written to the specified location.

#### **Troubleshooting: No Complete memory dump option**

- 1. Click **Start**  $\rightarrow$  **Run**, type **regedit.exe** into the blank field and then click **OK**.
- 2. Use the tree to navigate to and select the the following key:

HKEY\_LOCAL\_MACHINESYSTEMCurrentControlSetControlCrashControl

- 3. Double-click the  $\ensuremath{\textbf{CrashDumpEnabled}}$  data value to edit it.
- 4. Change the value to 1.
- 5. Click **OK**.
- 6. Restart the computer.

The **Complete memory dump** option is now enabled and can be selected from **Write debugging information** drop-down menu.

Gerelateerde inhoud

- Create a full memory dump of a VMware virtual machine
- 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
- How do I use ESET Log Collector?