ESET Tech Center

I've got a Blue Screen, what do I do?

Anish | ESET Nederland - 2019-07-17 - Comments (0) - Diagnostics

If your machine has crashed and you have started to get the Blue Screen (BSOD), then you will need to collect some information regarding the crash (as detailed from the check list below) so that we are better informed to determine the cause of the crash, then create a Support Ticket by clicking here and submit the information to us.

1. Collect the bug check code from event viewer (if present) or take a camera picture of the bluescreen itself.

If you are unsure of how to view the event viewer:

- Right click 'Computer' and click 'Manage'
- When the Computer management window is displayed, click the arrow/triangle next to Event Viewer to expand it, then expand 'Applications and Service Logs' and when the list is displayed, click 'ESET Endpoint Encryption'

At the top of the main window, all of the events surrounding ESET Endpoint Encryption will be displayed, double click the one which is named 'Error' under the 'Level' setting, when the window opens, either take a screen shot of the error or click the 'Copy' button in the bottom left hand corner of the window and paste the screen shot or event log details into the support ticket you are creating.

2. Stop the system auto restarting so you can see what the blue screen says.

If you are unsure of how to do this:

- Right click Computer and click 'Properties'
- When the system information window opens, click the 'Advanced system settings' link in the left hand pane
- When the System Properties window appears, click the bottom 'Settings' button within the 'Startup and Recovery' panel
- At the bottom of the Startup and Recovery window, there will be a pane named 'System failure', uncheck the box next to 'Automatically restart' and click 'OK'

3. What you were doing at time of crash?

Please include a step by step description of what you were doing at the time of the crash and if you have made any recent changes to your machine including any upgrades.

4. What version of the ESET Endpoint Encryption client is installed?

Please include the version number of ESET Endpoint Encryption which is installed on the machine, if you are unsure of how to do this then please refer to: KB27: How do I find which version of ESET Endpoint Encryption is installed? Note: If you send a diagnostic file as detailed in the next step this contains the version information required.

5. Send us a diagnostics file.

Please run our diagnostics utility on the affected machine and send us the resulting diagnostics log file which you will find on your desktop.

The diagnostics file can be downloaded from KB29: Where can I find the diagnostic program?

6. Set the size of the crash dump file so that the next time it crashes, you can send us a more detailed crash dump.

If you are unsure of how to do this:

- Windows 7: Right click Computer and click 'Properties'
  Windows 8.1 and newer: Right click the Start menu and select System
- When the System Information window opens, click the 'Advanced system settings' link in the left hand pane
- When the System Properties window appears, Click the bottom 'Settings' button within the 'Start-up and Recovery' panel
- At the bottom of the 'Start-up and Recovery' window, there will be a pane named 'System failure' within which is another pane named 'Write debugging information' which has a drop down box. If the list in the drop down box contains Complete Memory Dump', select it and click OK. If the option is not present an additional setting is required to enable it
- Tick 'Overwrite any existing file'

Enabling 'Complete Memory Dump' when it is not available.

- Close the 'Start-up and Recovery' Window
- Click the start menu and type Regedit to run the Registry Editor
- In the Registry Editor expand HKEY_LOCAL_MACHINE
- Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl
- Double click the value 'CrashDumpEnabled' and change the value to '1'
- Close the Registry Editor
- Click the bottom 'Settings' button within the 'Start-up and Recovery' panel and verify the drop down list now says 'Complete Memory Dump'

7. Zip the file and send it to us.

After the machine has Blue screened following setting the machine to generate a Kernel dump, you will find the Kernel dump by default as the %SystemRoot%\MEMORY.DMP. This usually expands to C:\Windows\memory.dmp. Right click on the file and move down to 'Send to' and then across to 'Compressed (zipped) folder' and zip the Kernel dump file in order to send to us for analysis.

Please note: If the crash dump you have created is larger than 10MB in size then it is unsuitable for email or for attaching to the support ticket. Please contact us for other methods to send the file, such as access to our FTP server.