**Hangs, Crashes & BSOD**

Please search KB articles and relevant release notes to identify a match with any existing known issues before escalating.

# User Mode dumps on Windows

1. **Download debug tool from Microsoft:**

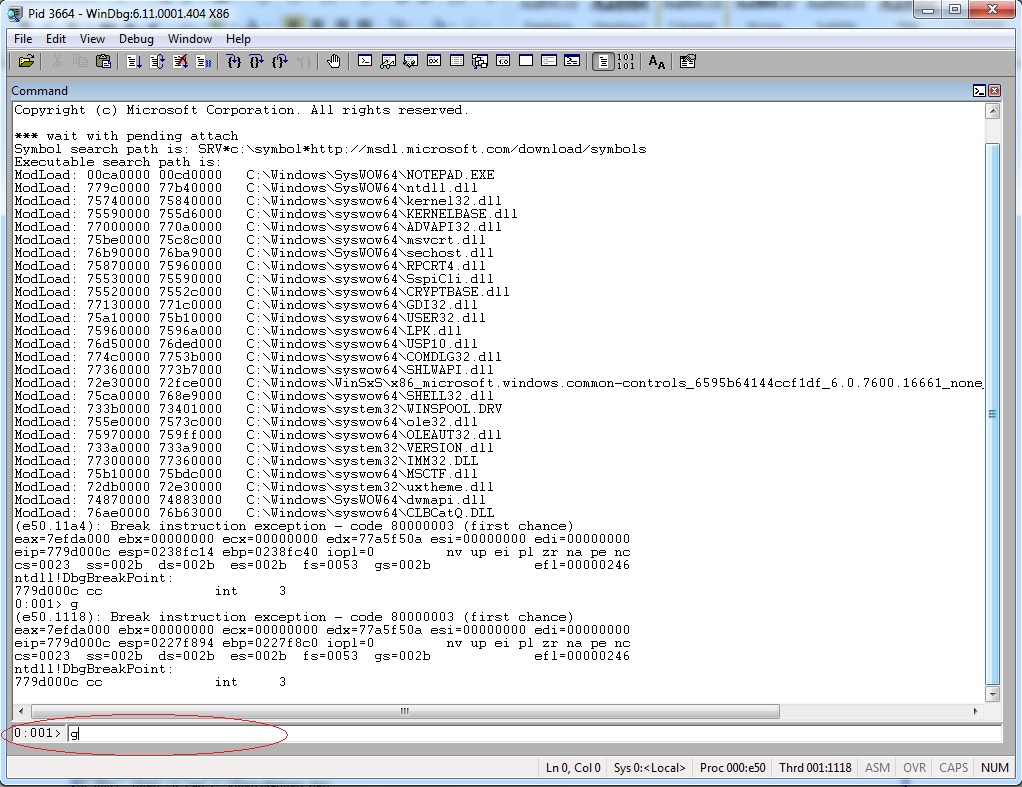
<http://msdl.microsoft.com/download/symbols/debuggers/dbg_x86_6.11.1.404.msi>

1. **Install Debugging tools for Windows**

First we install it. Accept all the defaults.

1. **Collect Crash dump**

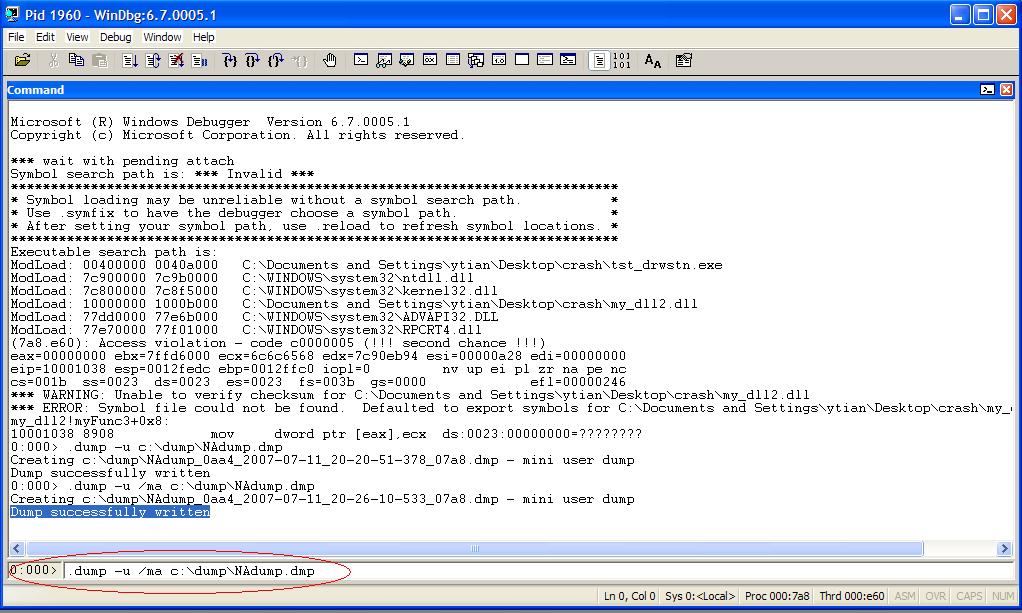
Open Windbg, on “File” menu, click “Attach to a Process”, then in the process list window, choose the process to be diagnosed and click “OK”. In the Windbg command input window, type “g” and hit Enter, as shown below:



***Figure 1***

Then the windbg command input window will show “Debugger is running...”. Leave the system running, until the crash happens. When the crash happens, the Windbg command window will accept input again. Now enter the command:

.dump –u /ma [path name]

as shown in Figure 2(if it asks whether to save workspace information, click “Yes”):

***Figure 2***

Enter the following command in Windbg’s command window as shown in the red circle in *Figure 2*: .dump –u /ma c:\dump\NAdump.dmp

It tells Windbg to create a dump file; its path is designated as “c:\dump\NAdump.dmp”. Then it shows “Dump successfully written” as shown in Figure 2.

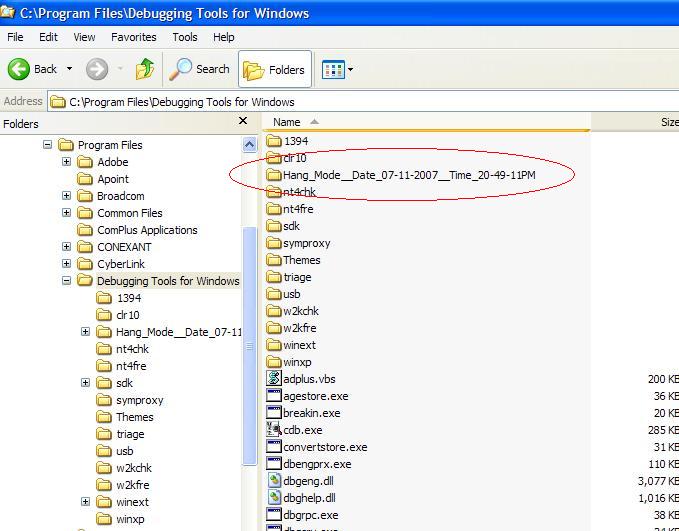
Now we can collect the dump file. Please note that Windbg appends the date/ time to the file name to make it unique.

Now you can close Windbg and restart the process. We also need to pay attention to if the customer has ‘auto restart service’ configured on the service. In the case that they have ‘auto restart’ configured, when the service crashes with windbg attached it, it won’t auto start because windbg is waiting for user input.

1. **Collect Hang mode dump:**

When our process (e.g. EIMserver.exe) goes into a hang situation, such as deadlock or the CPU reaches 100%, we open DOS command prompt window, go to Windbg installation directory, type in following command: Adplus –hang -quiet –pn EIMserver.exe

The adplus script instructs the debugger to take a memory snapshot of the process with name “EIMserver.exe”.

You may see that a “CDB debugger” command prompt window pops up and then disappears quickly. This means that the dump file is written to disk. You can find the dumps in the debugger’s installation folder. We need to collect the content of the whole folder suffixed with the date and time as shown in *Figure 3*:

***Figure 3***

# Kernel Mode dumps on Windows

On the BSOD (blue screen of death) machine, enable "Kernel mode dump" as followed:  
  
After rebooting:

1. Right click "My Computer" select "System Properties" and click the "Advanced" tab.
2. In the "Startup and Recovery" section, click "Settings".
3. In the "write debugging information" section select the drop down menu, select "Kernel Memory Dump" and click OK.

Now, the next time a blue screen happens, a kernel mode memory dump “MEMORY.DMP” will be created in %SystemRoot% folder. Please get the dump file.

# Dumps on Linux

1. Follow the KB to create crash dumps on Linux:

<https://emea.salesforce.com/articles/Knowledge_Article/Enabling-process-core-dumps-on-Linux-servers-and-V-Series-appliances>

1. Install gcore tool to create hang mode dumps when necessary
   1. First run the command ‘ps-e|grep [process name]’ to find the pid of the process to be diagnosed.
   2. Run the following command to get a core file for the process:

Gcore [pid].

* 1. Collect the core file with name core.pid