

Using the Debug Diagnostic Tool

FaultWire

Background

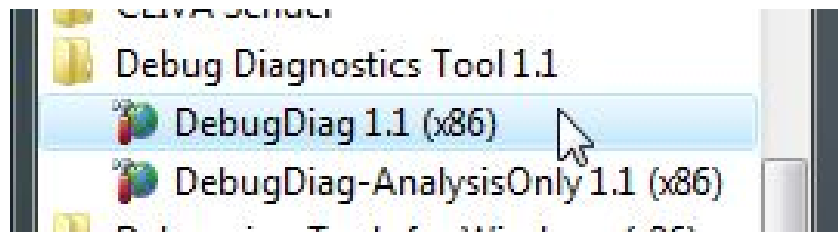
Windows has a tool to confirm a process or driver is faulty. Used mostly by developers, it could be used by anyone. It functions best when you know what the faulty process or service is first, so if you have no idea where to look, this is NOT the right tool to use.

It works by attaching itself to the designated process and watching for problems. If a fatal problem occurs, it places information into a dump file. Later using the Analysis tool, you can view the results.

Setting up Debug Analysis

We'll assume you've already downloaded and installed the Debug Diagnostic tool.

To launch Debug Diagnostic, use Start, All Programs, and find the Debug Diagnostics Tool folder. Select the choice DebugDiag (the version and processor type may be different than shown).

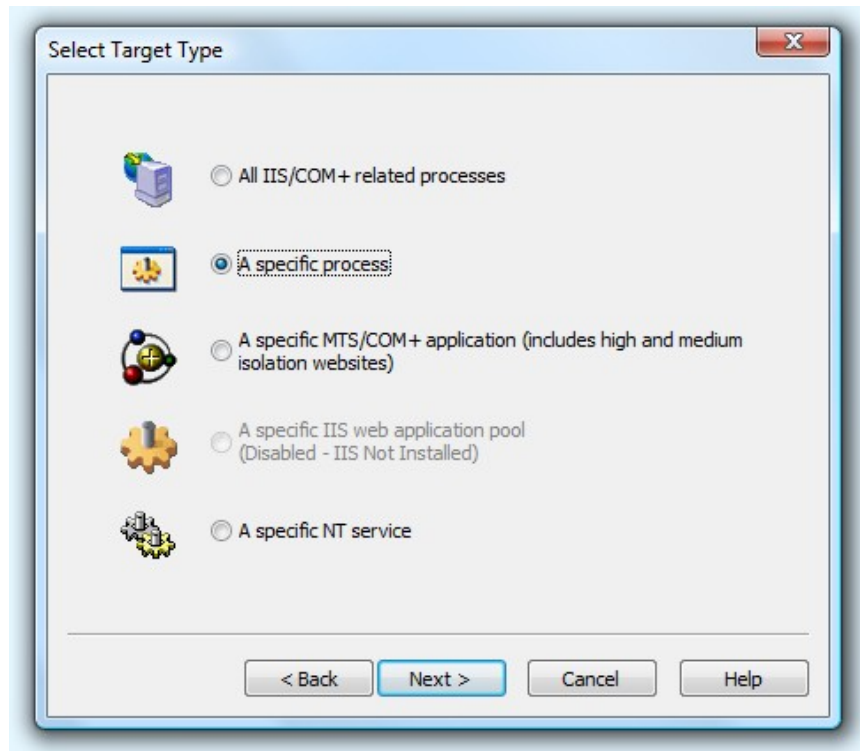


The Select Rule Type Dialog Appears (you can also select this from the main dialog Tools menu).

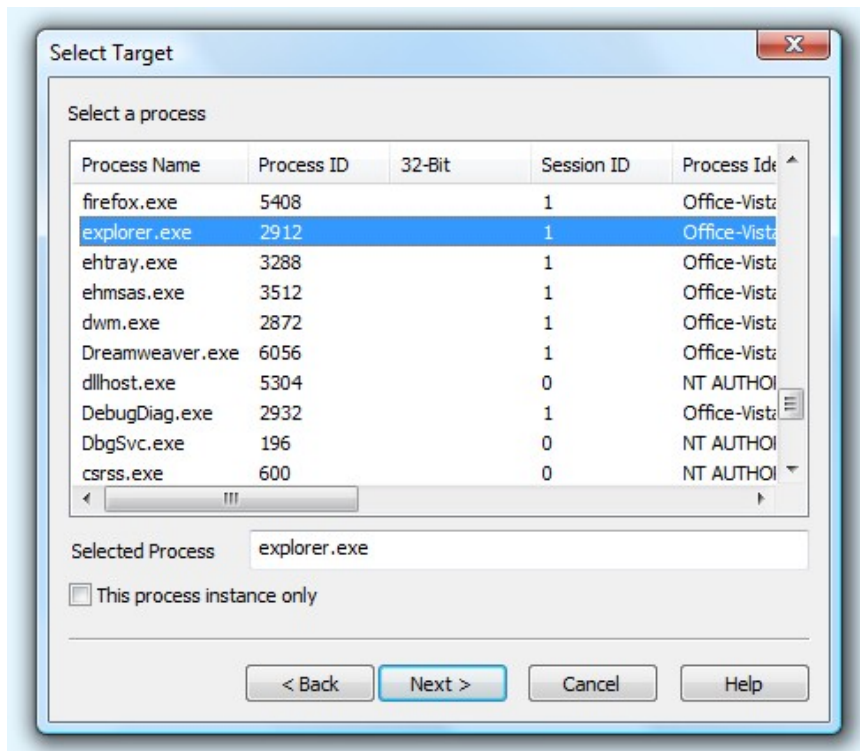


Using the Debug Diagnostic Tool FaultWire

Select the rule type, typically Crash and select Next.

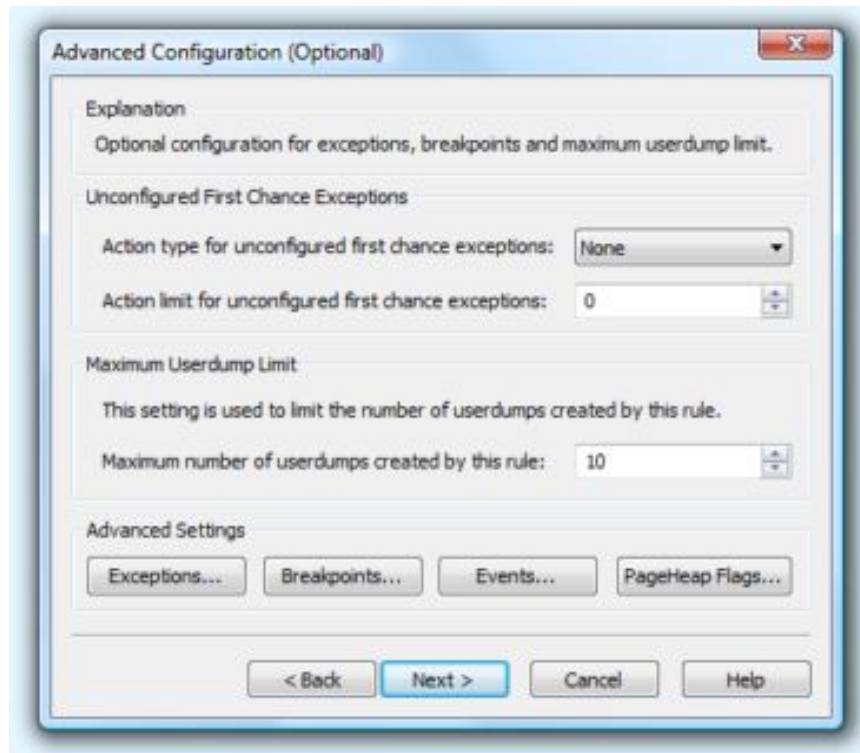


Select the target type. We'll pick A specific program (but you could also pick a service), and select Next.

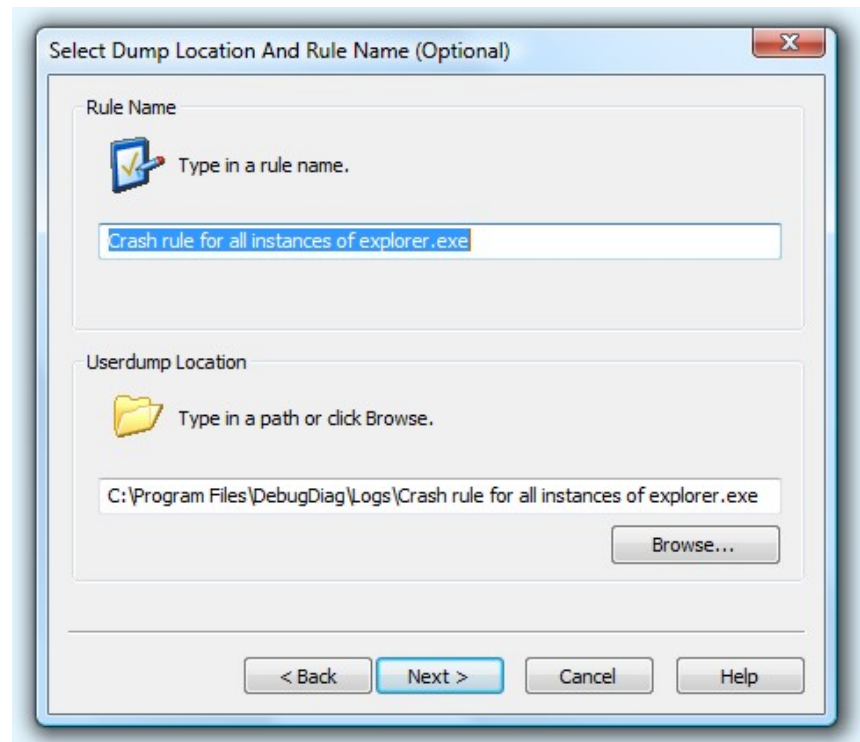


Using the Debug Diagnostic Tool FaultWire

Pick the process you want to monitor and select **Next**

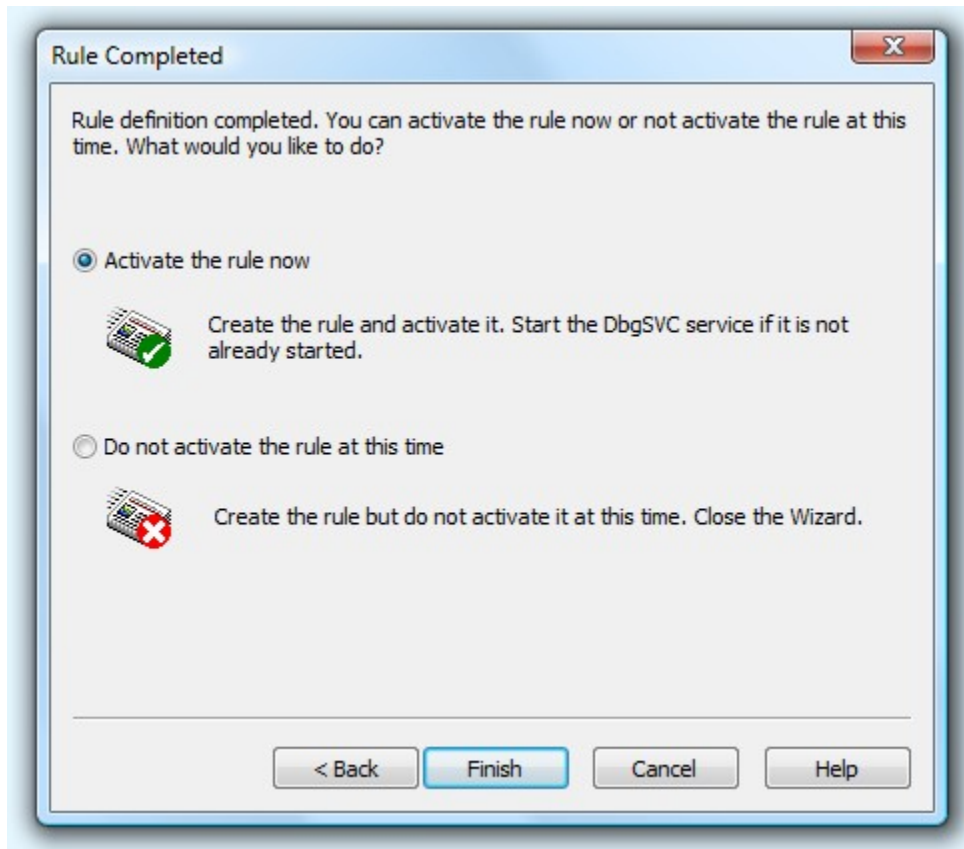


Select any advanced options you want. The defaults should be fine for most users. Select **Next**



Using the Debug Diagnostic Tool FaultWire

Set a name for this rule (as you can have multiple rules) and set the dump location. Select **Next**

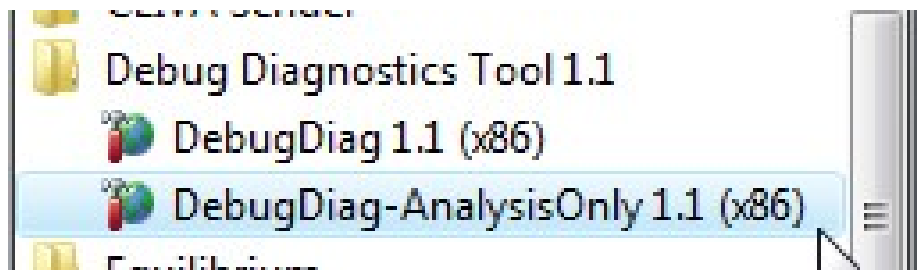


Confirm you want to activate the rule and select Finished. The rule will now appear in the main Debug Diagnostic Dialog. You're now ready for the next crash of your selected process or service!

Looking at the Results

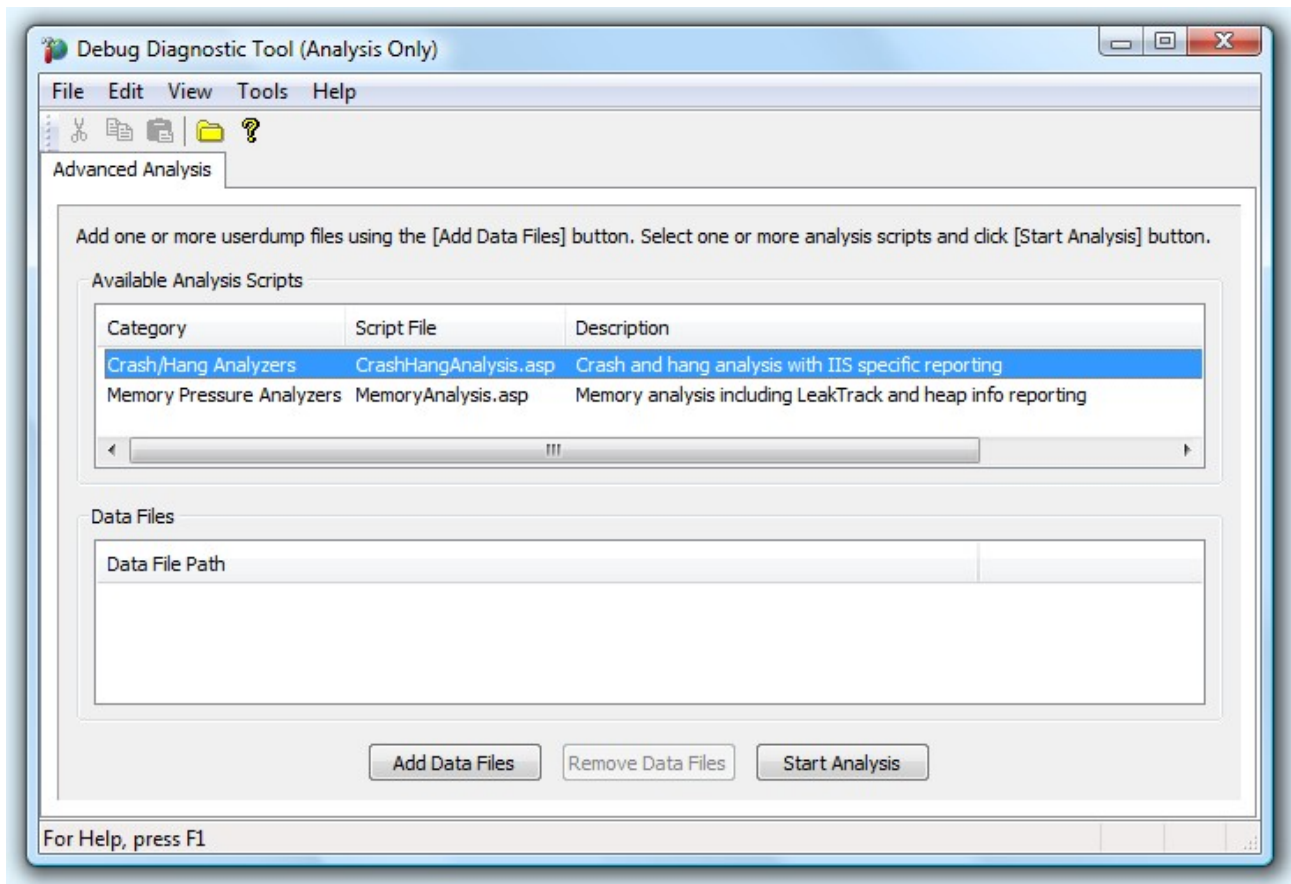
We'll assume you've already downloaded and installed the Debug Diagnostic tool.

To launch Debug Diagnostic, use Start, All Programs, and find the Debug Diagnostics Tool folder. Select the choice DebugDiag-AnalysisOnly (the version and processor type may be different than shown).



The main dialog appears:

Using the Debug Diagnostic Tool FaultWire



The default, Crash/Hang Analyzers, should be selected. Click on the Start Analysis button. You will be prompted with an Open dialog. The first time it defaults to a documents directory, so you'll have to switch it to where the dump files are stored, typically at c:\Windows\Minidump or other directory or files you set in the prior step.

Pick the file you want to analyze and select Ok.

After a few seconds (or longer) it opens your browser to a page about the Crash dump. You'll have to allow ActiveX for the page script to complete it's analysis.

In some cases it may return a Warning "DebugDiag failed to locate the PEB...". At this point you can ignore the rest of the page as it has nothing useful. This error occurs if picked a file that was not previously set up to be monitored. Return to Setting Up Debug Analysis.

Getting the Debug Diagnostic Tool

To get and install Debug Diagnostic (used for all Windows 2000 and later).

1. Download Debug Diagnostic from Microsoft.
2. Install the Debug Diagnostic by running the downloaded Microsoft file.

Using the Debug Diagnostic Tool FaultWire



3. Follow the instructions from the installer.

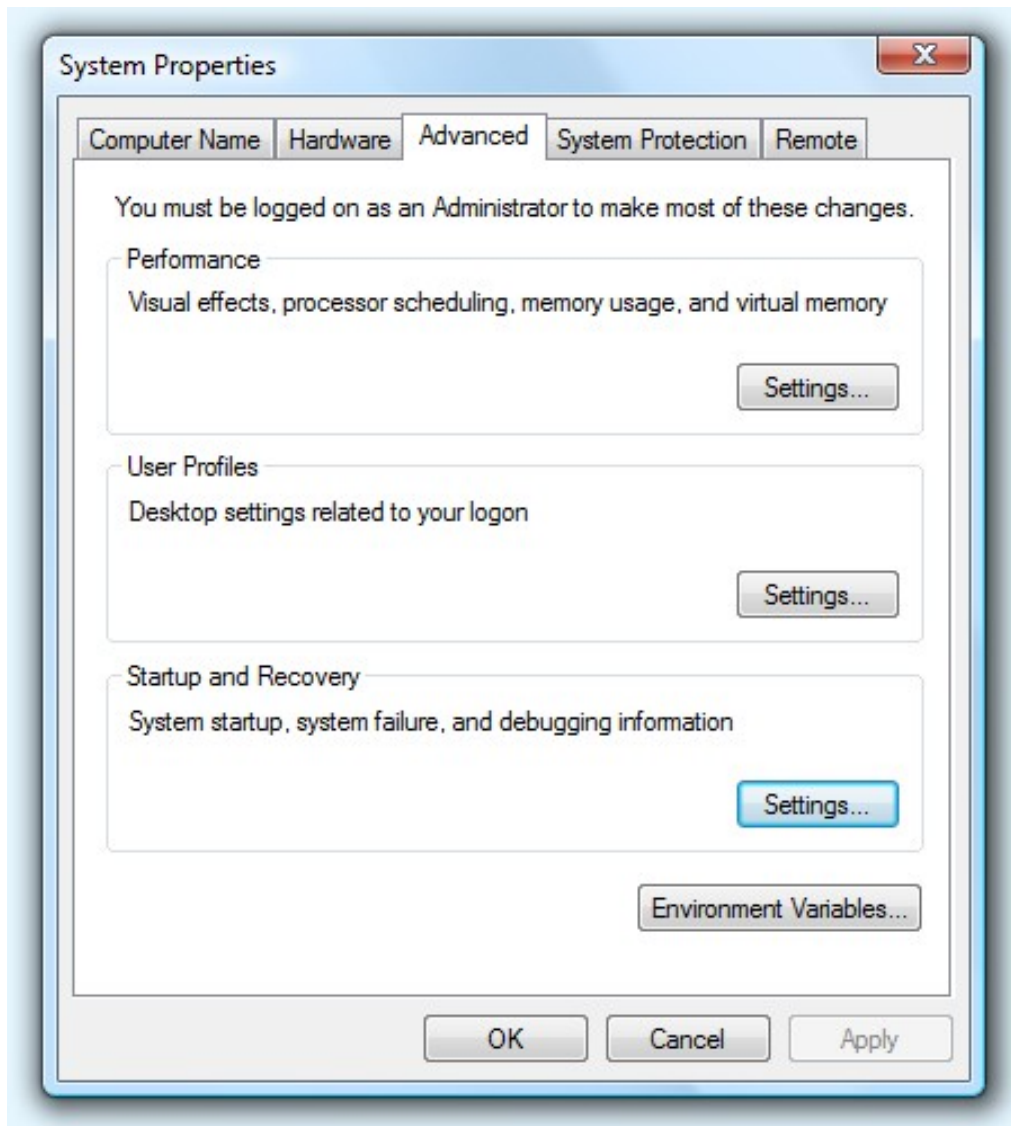
Turn on the Creation of Dump Files

Normally these are set on by default, but you can turn the ability to save dump files on or off and set where the crash dump directory will be written.

For Windows 7, Vista and Server 2008:

1. Select Start, then right-click on Computer, and select Properties.
2. Select Advanced system settings (on the left).
3. In System Properties, select the Advanced Tab, and under Startup and Settings, select the Settings button.

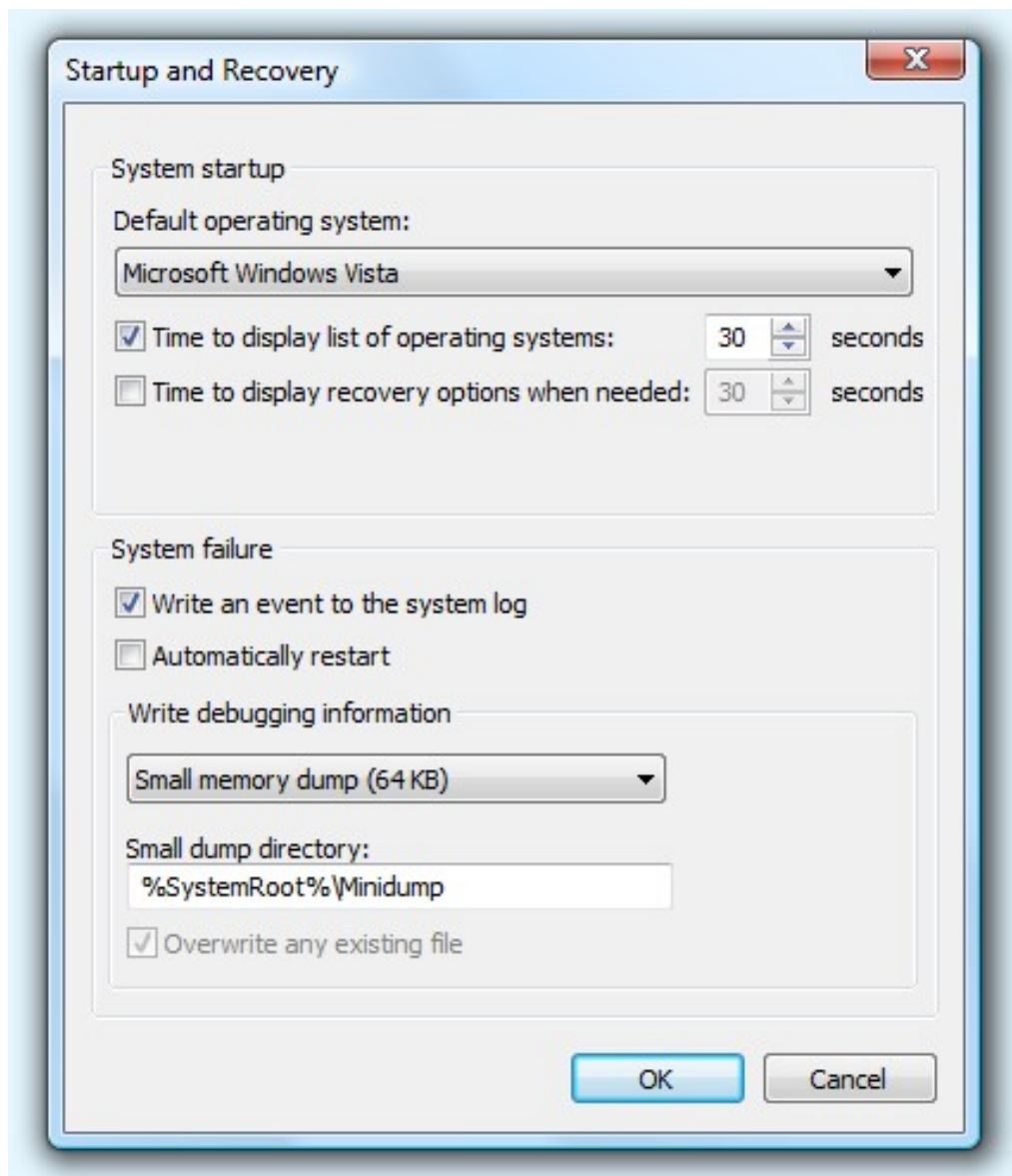
Using the Debug Diagnostic Tool FaultWire



4. In Startup and Recovery, under System failure, set Write an event to the system log as checked. Write debugging information should be set to Small memory dump so it will record each occurrence. You could use the Kernel Memory Dump option as well, but this is much larger in size and is primarily of use only for a device driver developer.

You can also change the default directory where these are written. We suggest using the default directory.

Using the Debug Diagnostic Tool FaultWire



5. After the changes are made, click on Ok, then Ok again, and then close the System Control Panel.

For Windows XP and Server 2003:

1. Select Start, then right-click on My Computer, and select Properties.
2. In System Properties, select the Advanced Tab, and under Startup and Settings, select the Settings button.
3. In Startup and Recovery, under System failure, set Write an event to the system log as checked. Write debugging information should be set to Small memory dump so it will record each occurrence. You could use the Kernel Memory Dump option as well, but this is much larger in size and would only be of use to a device driver developer.

Using the Debug Diagnostic Tool

FaultWire

You can also change the default directory where these are written. We suggest using the default directory.

4. After the changes are made, click on Ok, then Ok again.