

16 October 2007

By: Marius Oiaga, Technology News Editor

System Maintenance
Microsoft

[Manage Windows Vista Event Log Files](#)

The conversion to the .evtx format

Windows Vista – as well as the predecessor Windows operating systems – comes with a complex infrastructure designed to log all the activity of the platform. The tool associated with logs in Windows Vista is Event Viewer. Users will be able to access this utility by entering Event Viewer in the Search box under the Start menu. Then simply right click the highlighted result and choose Run as Administrator from the contextual menu that pops up. Event viewer will keep track of a range of events including items related to Administrative tasks, Applications, Security, Setup, System, Applications and Services Logs and Forwarded Events. The simplest way to deal with event files in Windows Vista is to have them saved as under the new Event Log file format - .evtx. Vista users will notice that the operating system also offers the possibility to convert exported Event Log (.evt) files from Windows XP and Windows Server 2003 to the .evtx format. The conversion can be done via the Event Viewer MMC, just make your way to the saved even, right click it and choose Save As. Additionally, Windows Events Command Line Utility (WEVTUTIL.EXE) can also be used in order to perform the conversion. "This utility is very powerful when manipulating Event Log files. You can retrieve information about event logs and publishers, install and uninstall event manifests, export logs and more. For our purposes though we are going to use the utility to convert our log file. The syntax is as follows: wevtutil export-log .evt .evtx /f. With larger log files using this utility is quicker than having the MMC export and save the file," revealed [Steve Paruskiewicz](#), from the Enterprise Platforms Support Windows Server Performance team. Type "cmd" in the Search box under the Start menu and press Ctrl + Shift + Enter in order to launch command prompt with administrative privileges. Now write "wevtutil" and hit Enter in order to get an idea of the commands associated with this utility. Paruskiewicz additionally offers a script set up to add a context menu handler to .evt files.