Introduction

Regmon is an application that monitors and displays all Registry activity on a system. It has advanced filtering and search capabilities that make it a powerful tool for exploring the way Windows works, seeing how applications use the Registry, or tracking down problems in system or application configurations.

Regmon works on NT 4.0, Windows 2000, Windows 95, Windows 98 and Windows ME.

Starting Regmon

Simply run the *Regmon* GUI (Regmon.exe). *Windows NT/2000 note: You must have administrative privilege to run Regmont*. Menus, hot-keys, or toolbar buttons can be used to clear the window, save the monitored data to a file, and to filter and search output.

As events are printed to the output, they are tagged with a sequence number. If *Regmon's* internal buffers are overflowed during extremely heavy activity, this will be reflected with gaps in the sequence number.

Each time you exit *Regmon* it remembers the position of the window and the widths of the output columns.

Filtering Output

Use the Edit|Filter/Highlight dialog to select what data will be shown in the list view. The filters are processed against the text in all the output columns except the sequence number and time. The '*' wildcard matches arbitrary strings, filters are case-insensitive. Only matches shown in the include filter, but that are not excluded with the exclude filter, are displayed. Use ';' to separate multiple filter component strings (e.g. "CurrentControl;Software").

For example, if the include filter is "HKLM\", and the exclude filter is "HKLM\System*", all references to keys and values under HLM\, except to those under HKLM\System would be monitored.

Wildcards allow for complex pattern matching, making it possible to match specific Registry accesses by specific applications, for example. The include filter "Winword*Windows" would have *Regmon* only show accesses by Microsoft Word to keys and values that include the word "Windows".

Use the highlight filter specify output that you want to have highlighted in the listview output. Select highlighting colors with Edit|Highlight Colors.

Limiting Output

The History Depth dialog, accessed via toolbar button or the Edit|History menu item, allows you to specify the maximum number of lines that will be remembered in the output window. A depth of 0 is used to signify no limit.

Searching the Output

You can search the output window for strings using the Find menu item (or the find toolbar button). Once you have opened a Find dialog and hit the FindNext button, you can repeat the search without changing the focus back to the Find dialog by hitting the F3 key.

To start a search at a particular line in the output, select the desired line by clicking it. If no line is selected a new search starts at the first entry in searching down, and at the last entry for searching up.

Options

Regmon can either timestamp events or show the time elapsed since you last cleared the output window or started *Regmon*. The Options menu and the clock toolbar button let you toggle between the two modes. The button on the toolbar shows the current mode with a clock or a stopwatch. When showing duration the Time field in the output shows the number of seconds it took for the underlying file system to service particular requests. The Options|Show Milliseconds menu entry lets you add millisecond resolution to times presented when *Regmon* shows clock times.

You can toggle *Regmon* to always remain a top window with the Options|Always On Top menu item. In addition, you can toggle *Regmon* not to scroll the listview via the Options|Auto Scroll menu item or corresponding toolbar button.

Font Selection

Use the Edit|Font menu item to change the font used in the listview.

Jumping to a Key or Value in *Regedit*

If you come across a key or value name in the output that you want to modify or view in *Regedit*, you can do so simply by double-clicking on the line containing the name or pressing the *Regedit* toolbar button. *Regmon* will launch *Regedit* (if it hasn't been launched already) and navigate directly to the value or key. Note that if you select a non-existent value or key *Regmon* will take *Regedit* to a position as close as possible to where the value or key would be located.

Monitoring Boot-Time Registry Access (Windows NT/2K only)

To use *Regmon's* boot logging feature simply select the "Log Boot" menu entry. *Regmon* will indicate that starting the next time the system boots Registry activity will be monitored and recorded to a log file named REGMON.LOG in your system root directory. When you make this selection *Regmon* configures itself as the very first driver to initialize in the system, enabling it to capture the Registry startup activity of all other device drivers and services, including critical boot drivers such as SCSI miniport drivers and boot file system drivers.

Regmon stops recording to the log file when you start the *Regmon* GUI, and it will only log a single boot. Logging is therefore also stopped when the system shuts down, unless you have re-enabled boot-time logging for the subsequent boot. The format of the log file is the same tab-delineated text as a standard *Regmon* output file that can be viewed with any editor.

Before you use the boot-logging feature you should ensure that there is ample free space on your system drive. Capturing Registry activity from startup to shutdown on an NT 4.0 system will generate a log file with 90,000-120,000 records (7-10 MB in size), whereas an identically configured NT 5.0 system (Beta 2) will generate 140,000-160,000 records (15-25 MB's of log data). If *Regmon* fills the disk while writing to the log it will truncate the log file and leave a message in it indicating that the disk did not have enough free space. *Regmon* aborts logging and cleans up the log in such cases so that lack of disk space will not prevent a successful boot.

Reporting Bugs and Feedback

If you encounter a problem while running *Regmon*, please visit www.sysinternals.com to obtain the latest version. If you still have problems, please record all the information in the top few lines of a Blue Screen (if you encounter one), as well as the section of addresses and driver names just above the administrative message. Determine if the problem is reproducible, and if so, how, and send this information to:

> mark@sysinternals.com and
> cogswell@winternals.com

Licensing

If you want to license *Regmon* for redistribution, or license *Regmon* source code, please contact licensing@sysinternals.com.