

Changes and Improvements in (the help of) Elwiz 4.0

Elwiz does run under the following operating systems:

- Windows NT 4
- Windows 2000
- Windows XP Professional
- Windows 2003

Elwiz does not run under Windows Version 6 (Vista, Longhorn).

You can watch and view the most important event logs Application, Security and System of clients running Windows 6 now. Even the native Event Viewer of Windows 5 is unable to show those events well formatted, but Elwiz does. http://heysoft.de/Frames/Vista_Remarks1_en.htm provides information why it is currently impossible to view more Vista logs from earlier versions of Windows.

Elwiz 4.0 needs version 4.0 of the EventWatcher and EventCollector services.

It is now possible to use the new tool **EventWatcherInstaller** for the deinstallation of the old and the installation of the new EventWatcher service on all clients. For more information see **Install.hlp**.

Starting with Windows version 6 (Vista, Longhorn) there are many improvements in the event log service.

One of the changes considered unnecessary by many users is the new meaning of all event IDs of the Security log – all well known IDs have been incremented by the constant value of 4096. The probably well known logon event with the ID 528 changed to 4624, for instance.

If it happens that you prefer to view the events with their old IDs, you can check the option **Show old Security event IDs for Vista logs** (under **Settings – Configuration – Misc**).

This setting does only control the view of the events. Filter rules always work with the real event IDs. This has the advantage that you can switch the view at any time. And it explains, for instance, why Security events 538 of Vista machines create alerts even when you did define a rule which filters out all events 538 – because the real ID for this event is 4634 on Vista. By the way, the name of the Security event source did change as well, which is the other reason that you need to define new filter rules for the Security log of Vista.

When new alerts arrive whilst you are viewing a log, Elwiz always jumps to the new alerts. To go back to the log you viewed previously, you can either press the key **F4** or choose **Back to previous log** in the context menu of the eventlog tree.

As soon as you add machines running Windows version 6 (Vista) to your domain, you should disable the option **Save “Current log” on touch ...** (unter **Settings – Configuration – Eventlog files**).

The reason for this suggestion is:

With Windows 6 the eventlog format changed. The events are gathered in evtx files now. It is still possible to backup the events to evt files, but you loose information if you do so. This is, for example, the exact time when the event occurred (evt files save time with an accuracy of 1 second, but evtx files save time with an accuracy of 1 millisecond) or the IDs of the process and even thread of the program which created the event.

If you enforce Elwiz to collect and clear events from machines running Windows version 6 or above (Vista and later), you will loose part of the information of the events, which can not be restored later!

The buttons **ID <** and **ID >** change their behaviour when you press the <Alt> key while clicking the button. Instead to jump to the previous or next event with the same ID, you will previous or next event with another ID. This might be especially useful when searching an eventlog file for all different event IDs it contains. Just sort the table by event ID and than browse through with **Alt** and **ID >**.
