

Änderungen und Erweiterungen in (der Hilfe von) Elwiz 4.0



<http://www.heysoft.de/>

Elwiz läuft unter folgenden Betriebssystemen:

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

Elwiz läuft nicht unter Windows Version 6 (Vista, Longhorn).

Sie können mit Elwiz jedoch auch die wichtigsten Ereignisprotokolle Anwendung, Sicherheit und System von Clients mit Windows 6 überwachen und formatiert anzeigen. Das gelingt den eingebauten Ereignisanzeigen älterer Windows-Versionen bisher nicht. Warum die Anzeige weiterer Vista-Protokolle gegenwärtig nicht möglich ist, lesen Sie in http://heysoft.de/Frames/Vista_Remarks1_de.htm

Elwiz 4.0 benötigt auch die Version 4.0 von EventWatcher- und Ereignissammeldienst.

Die Deinstallation des alten und Installation des neuen EventWatcher-Dienstes auf allen Clients kann jetzt wahlweise auch mit dem neuen Tool **EventWatcherInstaller** durchgeführt werden. Nähere Informationen finden Sie in der Datei **Install.hlp**.

Ab Windows Version 6 (Vista, Longhorn) gibt es zahlreiche Neuerungen im Ereignisprotokoll. Eine der wohl von vielen Anwendern als überflüssig betrachteten Änderungen ist die Änderung sämtlicher Ereignis-IDs des Sicherheitsprotokolls – zu den altbekannten Nummern wurde jeweils die Konstante 4096 hinzugezählt. Aus dem Anmeldeereignis mit der sicher gut bekannten ID 528 wurde so das Ereignis mit der ID 4624.

Falls Sie sich lieber die alten Ereignis-IDs anzeigen lassen möchten, so können Sie dies tun, indem Sie die Checkbox **Alte Ereignis-IDs im Sicherheitsprotokoll von Vista anzeigen** (unter **Einstellungen – Konfiguration – Verschiedenes**) markieren.

Diese Einstellung steuert nur die Anzeige in Elwiz, die Filterregeln arbeiten immer mit den tatsächlichen IDs. Das hat den Vorteil, dass Sie jederzeit die Anzeige umschalten können. Außerdem ist es die Erklärung dafür, dass z.B.

Sicherheitsereignis 538 von Vista-Rechnern auch dann angezeigt wird, wenn Sie eine Regel definiert haben, die alle Ereignisse 538 ausfiltert, denn bei Vista handelt es sich ja hierbei tatsächlich um Ereignisse mit der ID 4634, bei denen sich noch dazu der Name der Ereignisquelle geändert hat. Das ist auch der zweite Grund, warum Sie für das Sicherheitsprotokoll von Vista alle Filterregeln neu anlegen müssen.

Wenn neue Alarme eintreffen, während Sie sich ein Protokoll ansehen, springt Elwiz sofort zu dem neuen Alarm. Um zurück zu dem zuvor betrachteten Protokoll zu gelangen, können Sie **F4** auf der Tastatur drücken oder **Zurück zum vorherigen Protokoll** im Kontextmenü des Protokollbaumes wählen.

Sobald Sie in Ihrer Domäne auch Rechner mit Windows Version 6 (Vista) betreiben, sollten Sie die Option **Verschieben von Ereignissen aus "Aktuellen Ereignisprotokollen" beim Öffnen** (unter **Einstellungen – Konfiguration – Ereignisprotokolldateien**) deaktivieren.

Der Grund ist folgender:

Seit Windows 6 gibt es ein neues Ereignisprotokollformat. Die Ereignisse befinden sich dort jetzt in evtx-Dateien. Es besteht die Möglichkeit, die Ereignisse trotzdem in evt-Dateien zu sichern, jedoch gehen dabei Informationen verloren. Das sind z.B. Angaben zum Zeitpunkt des Ereignisses (evt-Dateien speichern es mit einer Genauigkeit von einer Sekunde, evtx-Dateien aber mit einer Genauigkeit von einer Millisekunde) oder zu Prozess- und Thread-ID des verursachenden Programms.

Wenn Sie also Elwiz dazu verwenden, auch die Ereignisse eines Vista-Rechners einzusammeln und zu löschen, verlieren Sie bei der Konvertierung in evt-Dateien einen Teil der Informationen, die anschließend nicht mehr wiederhergestellt werden können.

Die beiden Navigations-Schaltflächen **ID <** und **ID >** ändern ihr Verhalten, wenn die Alt-Taste gedrückt ist, während sie angeklickt werden. Statt zum vorigen beziehungsweise nächsten Ereignis mit der selben ID springt man dann zum vorigen beziehungsweise nächsten Ereignis mit einer anderen ID. Das kann besonders nützlich sein, wenn man eine Protokolldatei schnell nach allen vorkommenden Ereignis-IDs durchsuchen möchte. Man sortiert sie dann zuerst nach der Ereignis-ID und blättert dann mit **Alt** und **ID >** durch alle vorkommenden verschiedenen Ereignisse.
