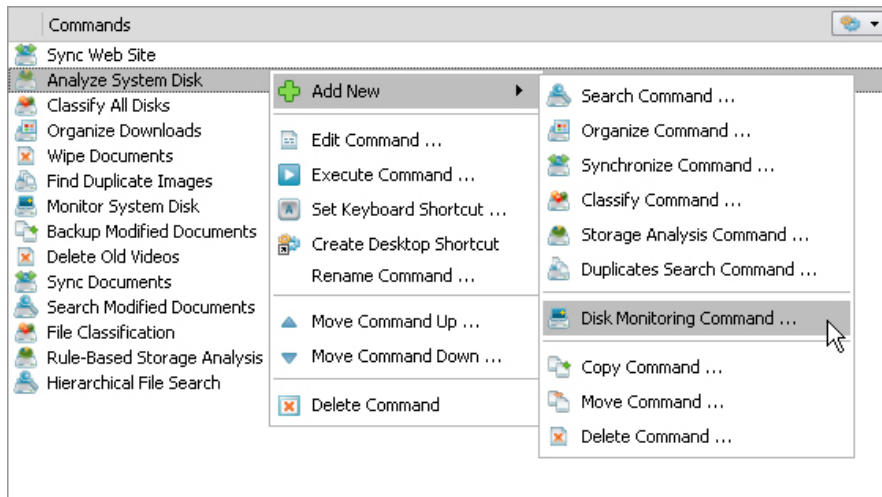
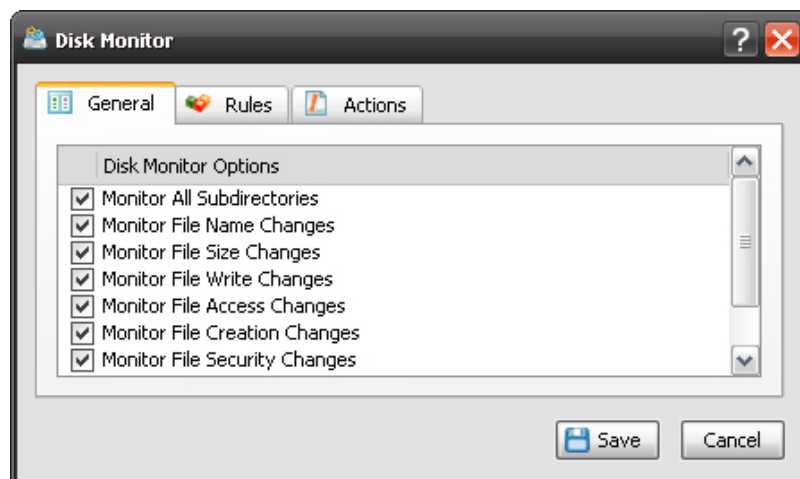


Real-Time Disk Change Monitoring Using FlexTk Ultimate

One of the biggest advantages of today's global Internet environment is an abundant availability of various types of freeware software products. Unfortunately, freeware software applications frequently contain malware, spyware or other kinds of harming software components requiring users to carefully evaluate and check each software product. In addition to the danger of installing a spyware application, IT professionals need to deal with applications compatibility making it absolutely necessary to validate each software product and to ensure that changes a software application makes in a desktop computer or server will not harm the operating system or other installed applications.

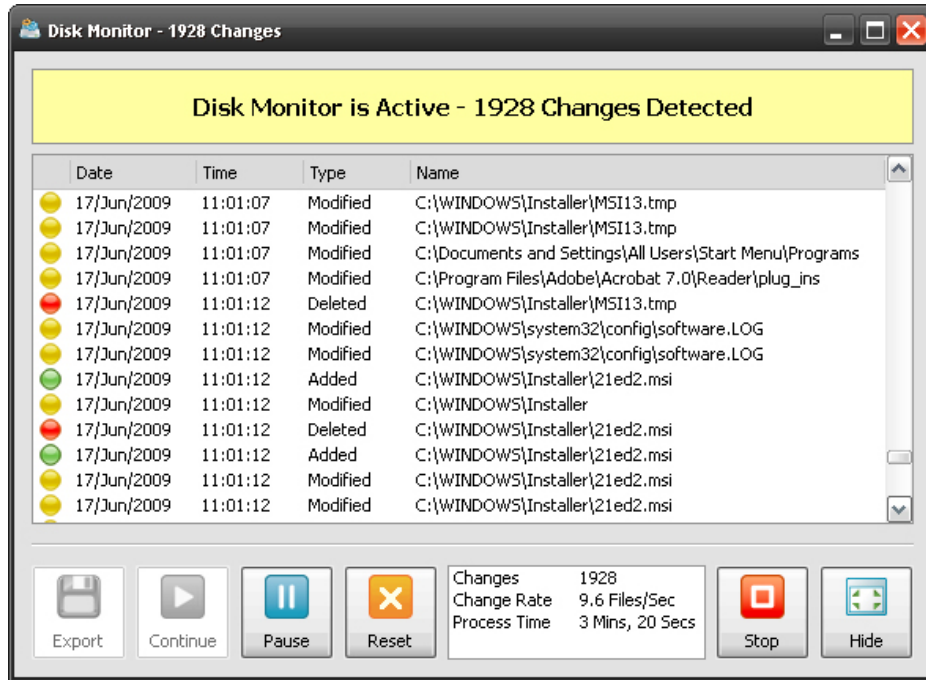


One potential way to validate an unknown software application is to install the application in a test environment and to monitor all changes that the application makes on the system disk during the installation procedure. FlexTk Ultimate, FlexTk Agent and FlexTk Server provide power computer users and IT professionals with an advanced, real-time disk monitor allowing one to monitor one or more disks or directories and see all the added, changed or deleted files in real-time.

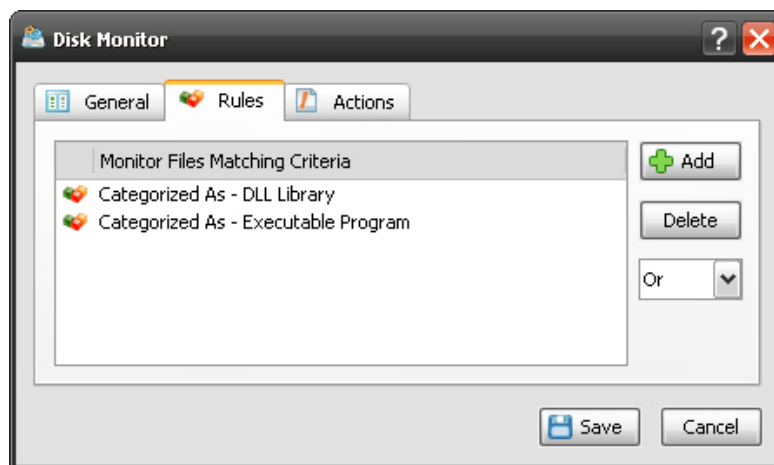


For example, let's create a user-defined disk monitoring command that will monitor changes made on the system disk during installation of such a well known application as the Adobe Acrobat PDF reader. In order to add a new disk monitoring operation, select the 'User-Defined Commands' view on one of the tool panes, press the right mouse button and select the 'Add New - Disk Monitoring Command' menu item. On the command inputs dialog, add the system disk and press the 'Next' button. On the 'Event Types' dialog, selected all types of changes and press the 'Save' button.

In order to start the monitoring command, click on the command item in the user-defined commands tool pane. Now, let's start the installation procedure. As soon as the installer begins the installation process, FlexTk's disk monitor starts to report about all the added, changed and deleted files. The reporting process occurs in real-time and all file system changes are reported at the same time as they are performed on the disk.



Surprisingly, such a relatively small and simple application has made almost 2,000 changes on the system disk making it quite difficult to review changes that were made. In general, when testing an application for a potentially dangerous behavior, there is no need to review all the changes that the application makes on the disk, but only ones that are made in executables and DLL libraries.



Any disk monitoring operation may be configured to show changes that are made in specific types of files according to one or more user-specified file matching rules. Now, let's add two file matching rules that will limit the disk monitoring operation to show all changes that were made in executables and DLL libraries. In order to do that, open the disk monitoring command, select the 'Rules' tab, add file matching rules to monitor files categorized as 'Executable Programs' and 'DLL Libraries', select the 'OR' rules logic and press the 'Save' button.

During the second installation, the disk monitoring command reported about 149 changes in executable files and DLL libraries making it very easy to review each change and see that this specific application modifies no system components, adds PDF plugins for Mozilla FireFox and Internet Explorer and puts all other files into the application specific directory.

