

Instructions

HD Observer from Process Leader Software

How to supervise the installation of a software? This article treats the various manners of supervising an installation of software on your computer.....3

How to supervise the Windows Registry? This article informs you how to extract useful information from the Windows Registry.....4

How to know the source of suspect files? Your antivirus discovered a suspect file, how to find, using HD Observer, which installation of program brought this virus, or from which Internet website a virus comes.....5

What to do, so that HD Observer ignores the contents of certain directories during complete analyses of a disk? Certain programs run in background on your computer and write data all times... If you do not want that HD Observer observe them, you can parameterize it.....6

How to prohibit certain files on your hard disks? Files are installed regularly on your computer, or each time you go on certain websites... You can prohibit them on all your disks or certain directories.....7

How to carry out a Internet monitoring? How to supervise your hard disks when you go on Internet. How to parameterize HD Observer so that it associates the address of Internet websites and the files which are placed on your hard disk when you open a Web page?8

How to use the HD Observer-method monitoring? This article treats possibilities of the events monitoring when you use the HD Observer method.....9

Which methods for which events? This article helps you to make the best choice of the method to be used... There are two methods of monitoring, the events-method and the scan-method.....10

How to supervise the programs which launch out at the starting of Windows? HD Observer supervises the starting of Windows... This article explains you how to disable or cancel the order of automatic launching of a program at the starting of Windows.....11

How to supervise the start page of your browser? This article explains you how to supervise your Internet start page and to restore it automatically by HD Observer so necessary.....12

How to use HD Observer during the monitoring of a download? HD Observer proposes you a principle of control.....12

How to supervise the installation of a software? This article treats the various manners of supervising an installation of software on your computer...

To supervise the installation of a software :

1. Open HD Observer
2. Choose the monitoring for installation
3. Activate monitoring
4. Choose the mode of installation which is appropriate for the software that you want to install
5. Install software
6. Stop the monitoring once the installation finished*

* an installation is finished when :

- the installation of software is finished
 - the computer was started again (if the installation requires it)
 - the program was opened a first time
-

How to supervise the Windows Registry? This article informs you how to extract useful information from the Windows Registry...

To supervise the Registry of Windows :

1. Configure HD Observer for the monitoring of the Registry in the tab "Scan" of the options panel
2. Select the level of monitoring of Registry :
 - Monitoring of the keys (sufficient when one installs a program for the first time on a computer)
 - Monitoring the values of the keys (If you made a reinstallation of a program)
 - Monitoring the data (if you want to see the modifications which events causes on the data of Registry)
3. Select the principal keys which you want to monitor, (tab "Scan")
 - HKey_Class_Root (H CR): for associations and extensions of files
 - HKey_Current_User (H CU): for the configuration and the parameters of the current user
 - HKey_Local_Machine (H LM): for the pilots, the hardware and software configurations of your computer
 - HKey_Users (H US): for the configuration and the parameters of all users of the PC
 - HKey_Current_Config (H CF): for the current configuration of the material

You can consult the keys and added values on the Registry in the tab "uninstallation" of the monitoring panel. In the tab "uninstall", click on "Read" button, then choose a view in the drop-down menu:

- select the view "Keys and Values of the Registry" for the added keys and values
 - the view "the data of Registry" for the data modifications
 - the green lines are the lines where modifications took place
 - in this view you can click on "Extract" button, to see the data modifications in red
-

How to know the source of suspect files? Your antivirus discovered a suspect file, how to find, using HD Observer, which installation of program brought this virus, or from which Internet website a virus comes...

Your antivirus discovered that the file "xxx.exe" is a virus or a spyware :

1. Note the exact name of the file and its extension, for example, "xxx.exe"
2. Open HD Observer and choose the panel "Options"
3. Select the tab "Search files"
4. Select in which kind of image HD Observer must search
5. Enter the file name to search
6. Click on "Search" button, once the file found, you can consult information about it :
 - o file path
 - o name of the image which contains the file
 - o date of the image
 - o date of the file
 - o kind of the image

By making a right-click on the concerned file, you can launch the following actions :

- Prohibition of the file on the computer
- Directory to be ignored
- Remove from the list
- Properties

You can then charge the data in the panel corresponding to the image, containing the file. Once the image charged, you will have access to following information :

- file path
 - exists (if the file exists always on the disk)
 - definition (if it is a file or a directory)
 - CreationTime
 - Internet website (Internet website from which the file comes, if Internet monitoring)
 - event (if it is a monitoring with the HD Observer method)
 - size (for monitoring with the HD Observer method)
-

What to do, so that HD Observer ignores the contents of certain directories during complete analyses of a disk? Certain programs run in background on your computer and write data at all times... If you do not want that HD Observer observe them, you can parameterize it...

To ignore the contents of certain directories during the HD Observer analyses :

1. Select the panel "Options"
2. Select the tab "Drives and directories"
3. Choose the monitoring (Installations, downloads, Internet, HD Observer)
4. Develop the TreeView and choose the directories to be ignored

When you want to ignore a directory which is in an image, you can directly select the file in the list, make a right-click, and choose "Directory to be ignored".

The names of directories which are in the "Directories to be ignored" will be on the images, but not their contents!

It is this method which you must use, so that HD Observer does not register in its images the writings of the programs which turn in background on your computer.

How to prohibit certain files on your hard disks? Files are installed regularly on your computer, or each time you go on certain websites... You can prohibit them on all your disks or certain directories...

To prohibit files on your hard disk :

1. Select the panel "Options"
2. Select the tab "Banned files"
3. Choose the kind of monitoring (installations, downloads, Internet, HD Observer)
4. Develop the TreeView and select the files to be prohibited

When you want to prohibit a file which is in a HD Observer image, you can directly select the file in the list, make a right-click, and choose "Forbid a file".

The file names which are in "Banned files" will be refused on your hard disk.

You can parameterize these prohibitions :

- you can choose the directory of prohibition
 - if HD Observer must require the authorization before refusing the file
 - if the sub-directories of the prohibited directory must also be monitored
-

How to carry out a Internet monitoring? How to supervise your hard disks when you go on Internet. How to parameterize HD Observer so that it associates the address of Internet websites and the files which are placed on your hard disk when you open a Web page?

To parameterize a monitoring Internet efficiently :

So that HD Observer associates the Internet website and the file which was copied on your computer, you must choose the events-method monitoring. For this :

1. Select the panel "Options"
2. Select the tab "Scan"
3. Choose the monitoring with events-method

To monitor the start page of your browser :

1. Select the panel "Options"
2. Select the tab "Parameters"
3. Check the option "Internet surfs"

To supervise the programs which launch out at the starting of Windows :

1. Select the panel "Options"
2. Select the tab "Windows start"
3. Check the option "Internet surfs"

You can launch a monitoring Internet from the panel " Internet Monitoring" of the HD Observer interface, but you can do that more quickly.

1. Make a right-click on the HD Observer icon in systray
 2. Select "Activate monitoring", then one of the two following options :
 - Internet (if your browser is already open)
 - Internet and to open the browser (if your browser is not yet open)
-

How to use the HD Observer-method monitoring? This article treats possibilities of the events monitoring when you use the HD Observer method...

To use efficiently the monitoring of HD Observer-method :

1. Select the panel "Options"
2. Select the tab "HD Observer"
3. Check at least one of the following options in the events report, so that the event is carried to the report
 - Files and Directories created
 - Files and Directories removed
 - Files and Directories renamed
 - Files and Directories modified
4. If you checked the monitoring of the modified files and directories, check at least one of the following options in the available filters, so that the event is carried to the report
 - Attributs
 - LastAccessWrite
 - CreationTime
 - LastAcces

The HD Observer monitoring has a greater sensitivity. You can consult the files which are installed on your computer in real time, on the tab "Monitoring" of the panel "HD Observer"

Which methods for which events? This article helps you to make the best choice of the method to be used... There are two methods of monitoring, the events-method and the scan-method...

For an installation of program having a large file volume, the method "Scan" is safer:

- with the method "Scan", even in the event of temporary blocking of the system, or overload of the memory, the data remain intact
- in the event of complete blocking of the computer during an installation, the data of the events-method will be lost, which is not the case with the method "Scan". After complete blocking of the system, then restarting the computer, the method "Scan" will find the files which were copied on the hard disk until the operating system blocking

For a light installation of program, the events-method is recommended :

- the events-method is fast to implement

For the monitoring of a download, the two methods are effective, if however you download files in great quantity, in "small packages" which will have to be reconstituted later, the events-method is recommended.

For monitoring Internet-surfs, the events-method is strongly recommended for the following reasons :

- the files (cookies, temporary, or others) which you prohibited on your hard disk will be removed more quickly and more effectively
- the events-method gives the Internet website and associates it to the files which are installed on your hard disk

The HD Observer-method monitoring is useful to observe any event on your computer. You can visualize the writing of the files on your hard disk in real time in a clear and concise interface. The events to be supervised can be of any kind :

- opening of a program
 - restarting of the computer
 - updating of a program
 - program working in background on your computer
 - CD-ROM with automatic launching
 - special events occurring during the activation of a Web page
 - or all other events...
-

**How to supervise the programs which launch out at the starting of Windows?
HD Observer supervises the starting of Windows... This article explains you how
to disable or cancel the order of automatic launching of a program at the
starting of Windows...**

To activate the monitoring of the new programs which launch out at starting of your computer :

1. Select the panel "Options"
2. Select the tab "Windows start"
3. Choose in which kind of monitoring control must be active

To modify the orders of starting :

1. Select the panel "Options"
2. Select the tab "Windows start"
3. Click on the "Refresh" button
4. Choose the view "All users" or "Current User"
 - You can definitively remove an order of launching a program at starting
 - Disable the order of launching
 - Enable the order of launching

To remove the order of launching definitively :

1. Select the order of launching
2. Click on the red button which is above the list
 - Warning : final removal!

To disable the order of launching :

1. Select the order of launching
 2. Check the box of the selected line
 - launching will not be done anymore, but can be reactivated; to reactivate the order, it is enough to uncheck the selected order
-

How to supervise the start page of your browser? This article explains you how to supervise your Internet start page and to restore it automatically by HD Observer so necessary...

To supervise the start page of your browser :

1. Select the panel "Options"
2. Select the tab "Parameters"
3. Choose in which kind of monitoring control must be active

If your start page is changed during the monitoring, HD Observer will ask you whether you accept the change, or if you refuse it.

How to use HD Observer during the monitoring of a download? HD Observer proposes you a principle of control...

To supervise a download, HD Observer makes the difference between the files which are installed on your computer in the "target directory" that you determined, and those which spread elsewhere. To activate the monitoring :

1. Select the panel "Downloads"
2. Select the tab "Downloads"
3. Indicate the directory in which the downloaded files must be copied
4. Activate the download monitoring

After the download monitoring, you can select a view which shows you the files which were copied in the "target directory" or spread elsewhere.