



# Comodo Cleaning Essentials

Software Version 1.6

## User Guide

Guide Version 1.6.091911

## Table of Contents

<b>1.Introduction to Comodo Cleaning Essentials</b> .....	<b>4</b>
1.1.System Requirements .....	5
1.2.Downloading Comodo Cleaning Essentials.....	5
1.3.Starting Comodo Cleaning Essentials.....	6
1.4.The Main Interface.....	6
<b>2.Scanning Your System.....</b>	<b>7</b>
2.1.Full Scan.....	8
2.2.Custom Scan.....	14
<b>3.Introduction to KillSwitch.....</b>	<b>25</b>
3.1.Starting KillSwitch.....	25
3.1.1.From the Comodo Cleaning Essentials Interface.....	26
3.1.2.From the Folder Containing Comodo Cleaning Essentials Files.....	26
3.1.3.Replacing Windows Task Manager with KillSwitch.....	27
3.2.The Main Interface.....	28
3.2.1.The System Tray Icons.....	33
3.3.Viewing and Handling Processes and Services.....	35
3.3.1.Processes.....	35
3.3.1.1.Stopping, Starting and Handling the Processes.....	37
3.3.1.2.Viewing Properties of a Process.....	40
3.3.1.3.Searching for Handles or DLLs.....	56
3.3.2.Services.....	58
3.3.2.1.Stopping, Starting and Deleting the Services.....	59
3.3.2.2.Viewing the Properties of a Service.....	59
3.3.3.Network Connections.....	62
3.3.3.1.Inspecting and Closing Network Connections.....	64
3.3.4.Browser Helper Objects.....	66
3.3.4.1.Deleting Unused BHOs.....	67
3.3.5.Layered Service Providers.....	67
3.3.5.1.Deleting Unused LSPs.....	68
3.4.The Tools Menu.....	69
3.4.1.Viewing System Information.....	69
3.4.2.Configuring KillSwitch.....	71
3.4.2.1.General Settings.....	71
3.4.2.2.Advanced Settings.....	73
3.4.2.3.Symbols.....	74
3.4.2.4.Graphs.....	75
3.4.3.Managing Plug-ins.....	77
3.4.4.Creating a Service.....	78
3.4.5.Scanning Your System for Hidden Processes.....	81
3.4.6.Viewing the Page Files in Your System.....	82
3.4.7.Verifying Authenticity of Applications.....	83
3.4.8.Repairing Windows Settings and Features.....	86
3.5.Managing Currently Logged-in Users.....	87
3.6.Help and About Details.....	89

3.6.1.1.Help.....	90
3.6.1.2.About.....	90
<b>4.Configuring Comodo Cleaning Essentials.....</b>	<b>91</b>
4.1.Quarantined Items.....	91
4.2.Manage Trusted Vendors.....	92
4.3.Options.....	96
<b>5.Help and About Details.....</b>	<b>98</b>
5.1.Help.....	99
5.2.About.....	99
<b>About Comodo.....</b>	<b>100</b>

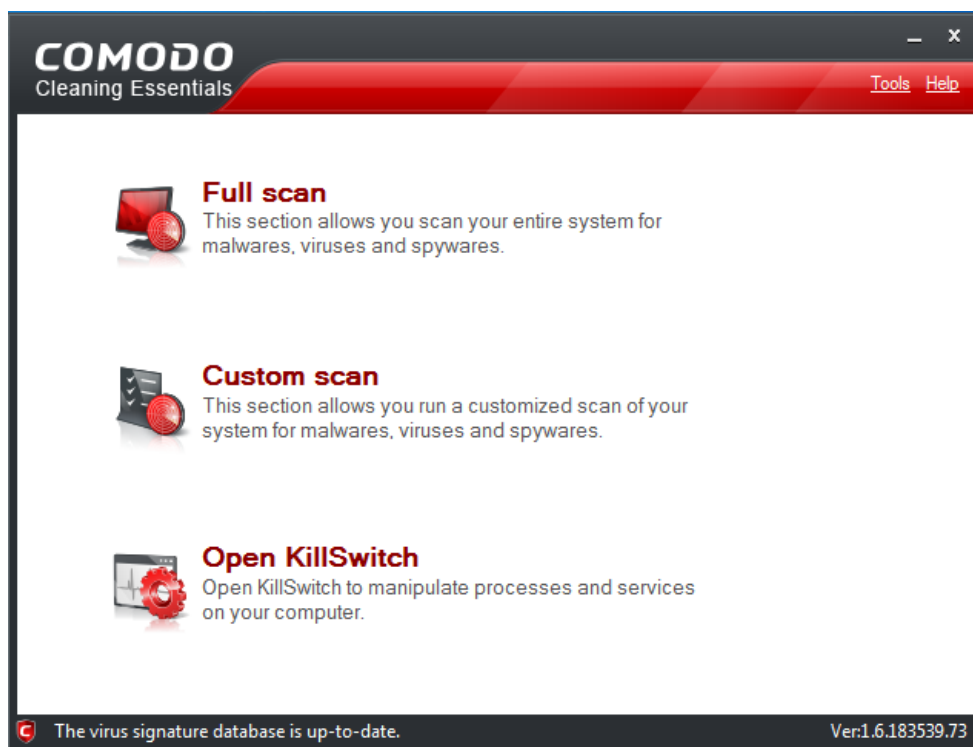
# 1. Introduction to Comodo Cleaning Essentials

Comodo Cleaning Essentials (CCE) is a set of computer security tools designed to help users identify and remove malware and unsafe processes from infected computers.

Major features include:

- **KillSwitch** - an advanced system monitoring tool that allows users to identify, monitor and stop any unsafe processes that are running on their system.
- **Malware scanner** - Fully customizable scanner capable of unearthing and removing viruses, rootkits, hidden files and malicious registry keys hidden deep in your system.

CCE is a lightweight, portable application which requires no installation and can be run directly from removable media such as a USB key. Home users can quickly and easily run scans and operate the software with the minimum of fuss. More experienced users will enjoy the high levels of visibility and control over system processes and the ability to configure customized scans from the granular options menu.



## Guide Structure

This guide is intended to take you through the step-by-step process of organization, configuration and use of Comodo Cleaning Essentials application.

- Section 1, **Introduction to Comodo Cleaning Essentials**, is a high level overview of the solution and serves as an introduction to the main themes and concepts that are discussed in more detail later in the guide.
  - **System Requirement** - Minimum required hardware and software for the application.
  - **Downloading Comodo Cleaning Essentials** - A brief outline of the download procedure.
  - **Starting Comodo Cleaning Essentials** - How to run the application.
  - **The Main Interface** - Description of menus and options in the main interface.
- Section 2, **Scanning your System**, explains the various methods of running a scan.

- **Full Scan** - Explains how to run a full scan of your system.
- **Custom Scan** - How to customize your scan.
- Section 3, **Introduction to KillSwitch** - is a high level overview of KillSwitch, a powerful built-in system monitoring tool and serves as an introduction to the main themes and concepts of KillSwitch.
  - **Starting KillSwitch** - How to start the tool.
  - **The Main Interface** - Description of menus and options in the main interface.
  - **Viewing and Handling Processes and Services** - explains the various features and how to use them.
    - **Processes**
    - **Services**
    - **Network Connections**
    - **Browser Helper Objects**
    - **Layered Service Providers**
  - **The Tools Menu** - Explains how to configure the tool and to access additional functionality
    - **Viewing System Information**
    - **Configuring KillSwitch**
    - **Managing Plug-ins**
    - **Creating a new Windows service**
    - **Scanning Your System for Hidden Processes**
    - **Viewing the Page Files in Your System**
    - **Verifying authenticity of Applications**
    - **Repairing Windows Settings and Features**
  - **Managing Currently Logged-in Users** - Explains management of users through KillSwitch.
  - **Help and About Details** - How to open the online help guide and find the version number and other miscellaneous details about the application.
- Section 4, **Configuring Comodo Cleanin Essentials** - Explains how to configure the application.
  - **Quarantined Items** - How to quarantine and restore suspicious files.
  - **Manage Trusted Vendors** - Adding and removing vendors to the Trusted Vendor List.
  - **Options** - How to configure the overall behavior of the application.
- Section 5, **Help and About** - How to open the online help guide and find the version number and other miscellaneous details about the application.

## 1.1. System Requirements

To ensure optimal performance of Comodo Cleaning Essentials, please ensure that your PC complies with the minimum system requirements as stated below:

- Windows 7 (Both 32-bit and 64-bit versions), Windows Vista (Both 32-bit and 64-bit versions) or Windows XP (Both 32-bit and 64-bit versions)
- 128 MB available RAM
- 210 MB hard disk space for both 32-bit and 64-bit versions

## 1.2. Downloading Comodo Cleaning Essentials

Comodo Cleaning Essentials is available for 32bit and 64 bit versions of Windows XP, Vista or Windows 7 and can be downloaded from the following locations:

32 Bit Operating Systems:

[http://download.comodo.com/cce/download/setups/cce\\_1.6.183539.73\\_x32.zip](http://download.comodo.com/cce/download/setups/cce_1.6.183539.73_x32.zip)

64 Bit Operating Systems:

[http://download.comodo.com/cce/download/setups/cce\\_1.6.183539.73\\_x64.zip](http://download.comodo.com/cce/download/setups/cce_1.6.183539.73_x64.zip)

After downloading the Comodo Cleaning Essentials setup files, simply double click on CCE.exe to start using the application. No

installation is required to use CCE, but the latest virus definitions will be downloaded upon first startup.

## 1.3. Starting Comodo Cleaning Essentials

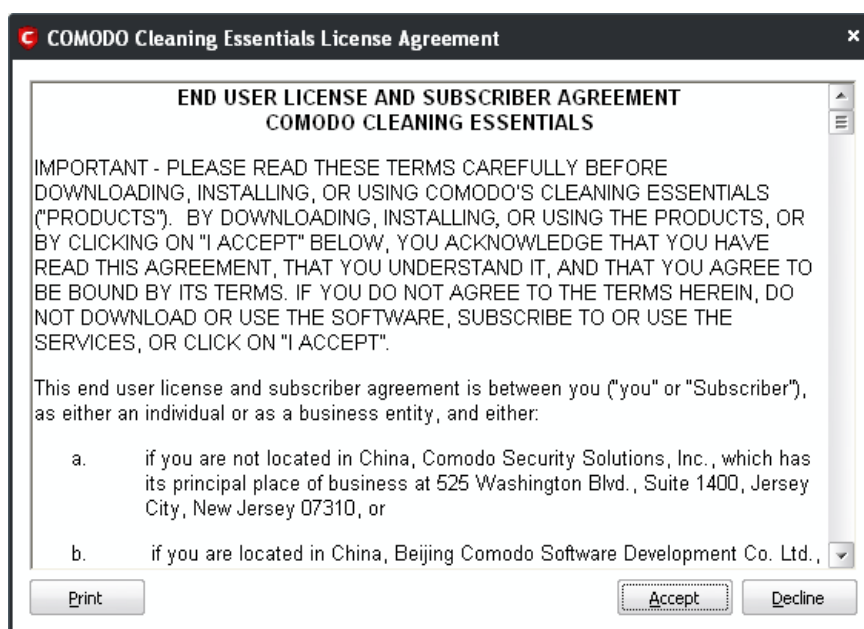
CCE is a lightweight, portable application which requires no installation and can be run directly from removable media such as a USB key.

### To start the CCE application

- Navigate to the CCE folder containing the files.

- Double-click on the  CCE.exe file.

When you are starting the application for the first time, you will be asked to accept the End-User License Agreement (EULA). It is mandatory for you to read and accept the EULA to continue using the application.

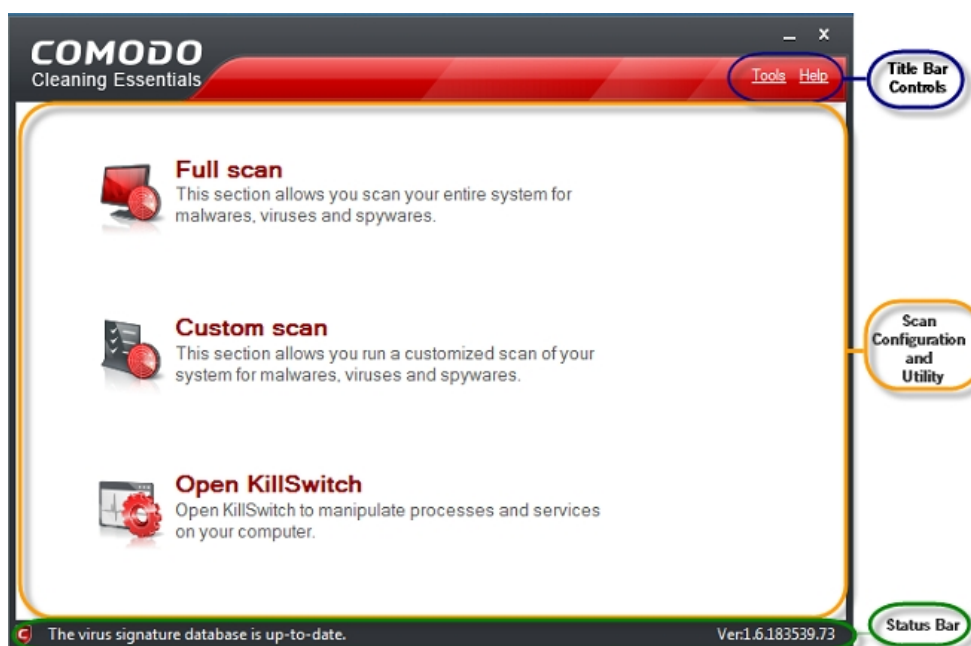


- Read the agreement and click 'Accept'. If you do not want to use the application, click 'Decline'.

You need to accept the EULA only when you are starting the application in your computer for the first time. From the next time onwards, the EULA will not be displayed.

## 1.4. The Main Interface

Comodo Cleaning Essentials' streamlined interface provides fingertip access and control over all functional areas of the software.



The main interface of the application has the following areas:

- **Scan Configuration and Utility Area;**
- **Title Bar Controls;**
- **Status Bar.**

## Scan Configuration and Utility Area

The Scan Configuration and Utility Area contains links that allow you to start scanning your system for potential malware and also contains the KillSwitch utility.

**Full Scan** - This section allows you to run a full scan of your system for malwares, viruses and spywares.

**Custom Scan** - This section allows you to customize your scan for malwares, viruses and spywares in your system.

**Open KillSwitch** - Launches the KillSwitch, an advanced system monitoring tool that allows you to identify, monitor and stop any unsafe processes that are running in your system.

## Title Bar Controls

The top right corner of the main interface contains the links 'Options' and 'Help' that allow you to configure the application and launch the online help guide.

**Options** - You can configure various settings in the application through this link.

**Help** - Launches the online help guide

## Status Bar

At the bottom of the main interface, the status of the virus signature database and version information of the software are displayed.

# 2. Scanning Your System

Comodo Cleaning Essentials allows you to perform a full system scan or a custom scan as per your requirements. Customized scanning is very useful if you want to scan only a particular file/folder/drive or if you have installed a program and suspect it may be infected.

Refer to the following sections for more details on:

- **Full Scan**
- **Custom Scan**

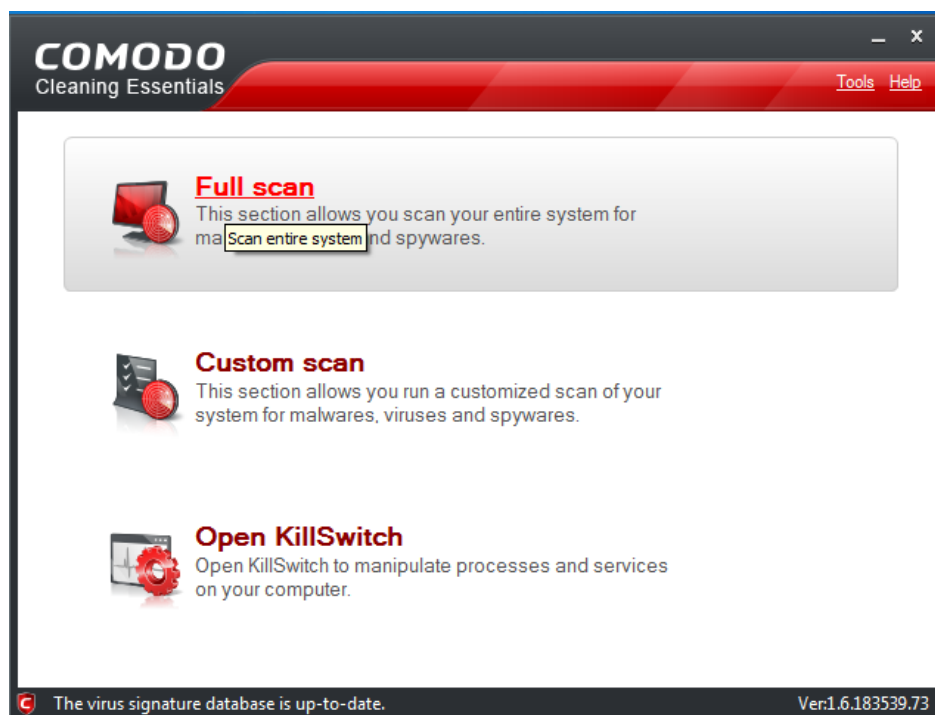
## 2.1.Full Scan

It is essential to run a full scan of your system periodically to detect any malware or viruses. After scanning is complete, the results panel will allow you to:

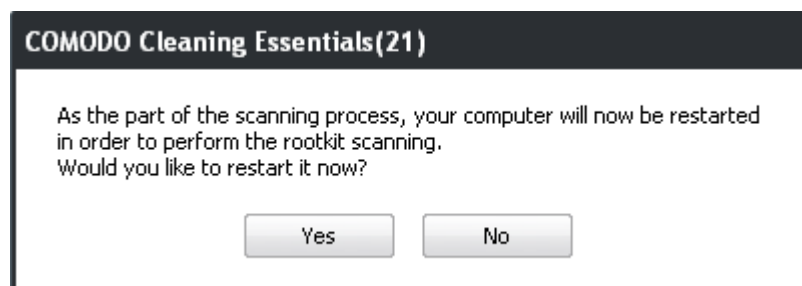
- **Move any threats identified by the scan into quarantine**
- **Disinfect the selected file/application if an exclusive disinfection routine is available**
- **Delete any infected files, folders or applications**
- **Exclude an application you consider as safe from the threat list**

### To run a full scan of your system

- Click the 'Full Scan' option in the main interface.



When you select this option, the application will ask your permission to restart the computer to perform rootkit scanning.



A rootkit is a type of malware that is designed to conceal the fact that the user's system has been compromised. Once installed, they camouflage themselves as (for example) standard operating system files, security tools and APIs used for diagnosis, scanning, and monitoring. Rootkits are usually not detectable by normal virus scanners because of this camouflage. However, CCE features a dedicated scanner that is capable of identifying rootkits and, if any, the hidden files and the registry keys stored by them.

The restart dialog window will start a count down from 30 and if you do not choose either 'Yes' or 'No' option, the system will

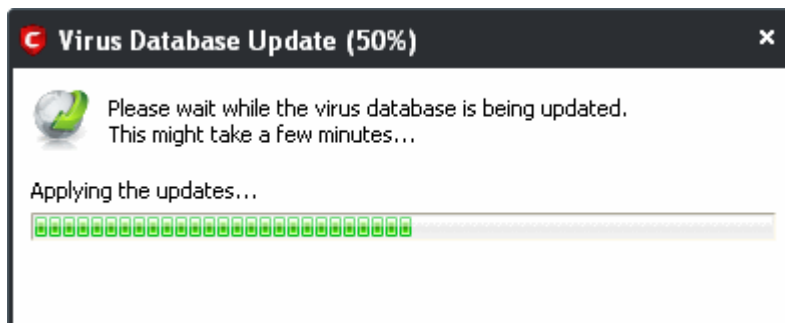


automatically restart when the count down reaches 0.

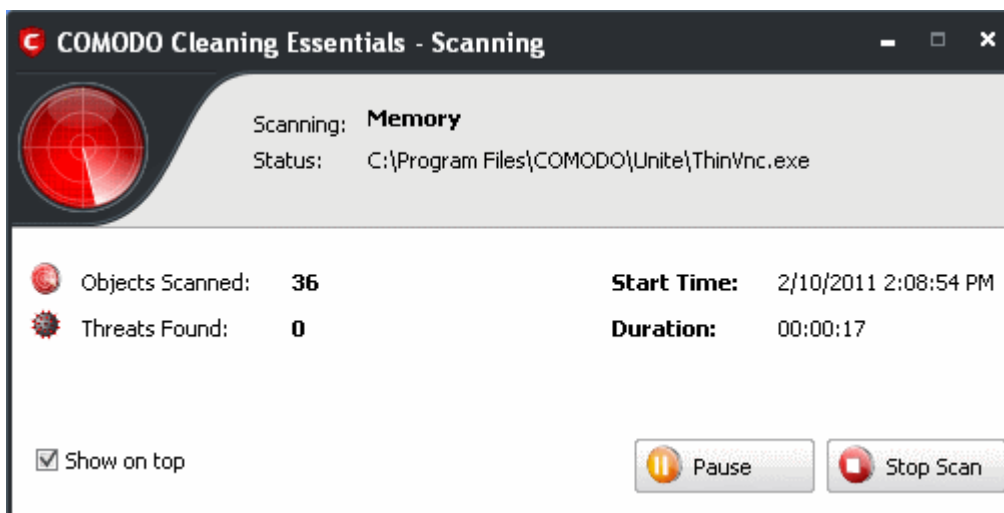
- Click Yes to restart the system to perform the rootkit scanning.
- If you click No, the full scan function will not be performed.

**Note:** The full scan will be performed only if you select Yes to restart the system to perform rootkit scanning.

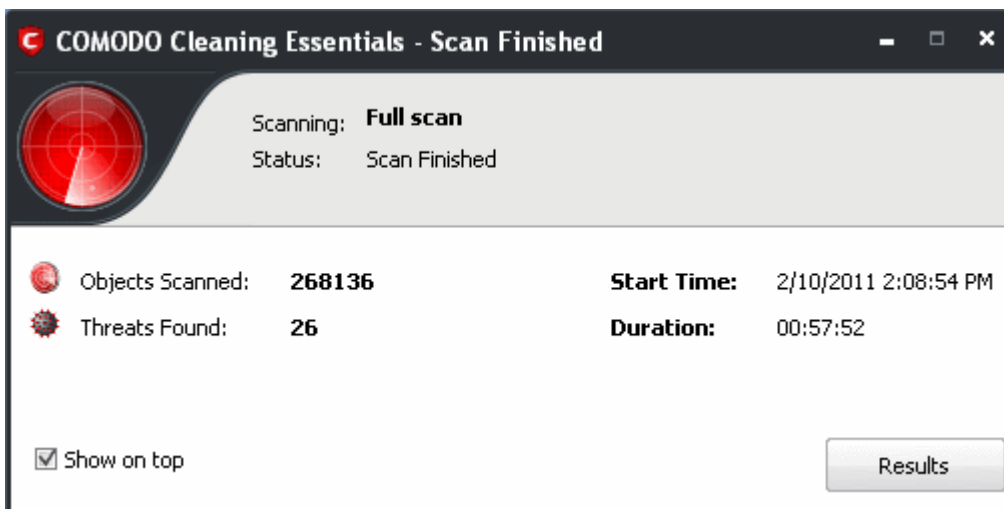
After the system has restarted, the virus database will be updated ...



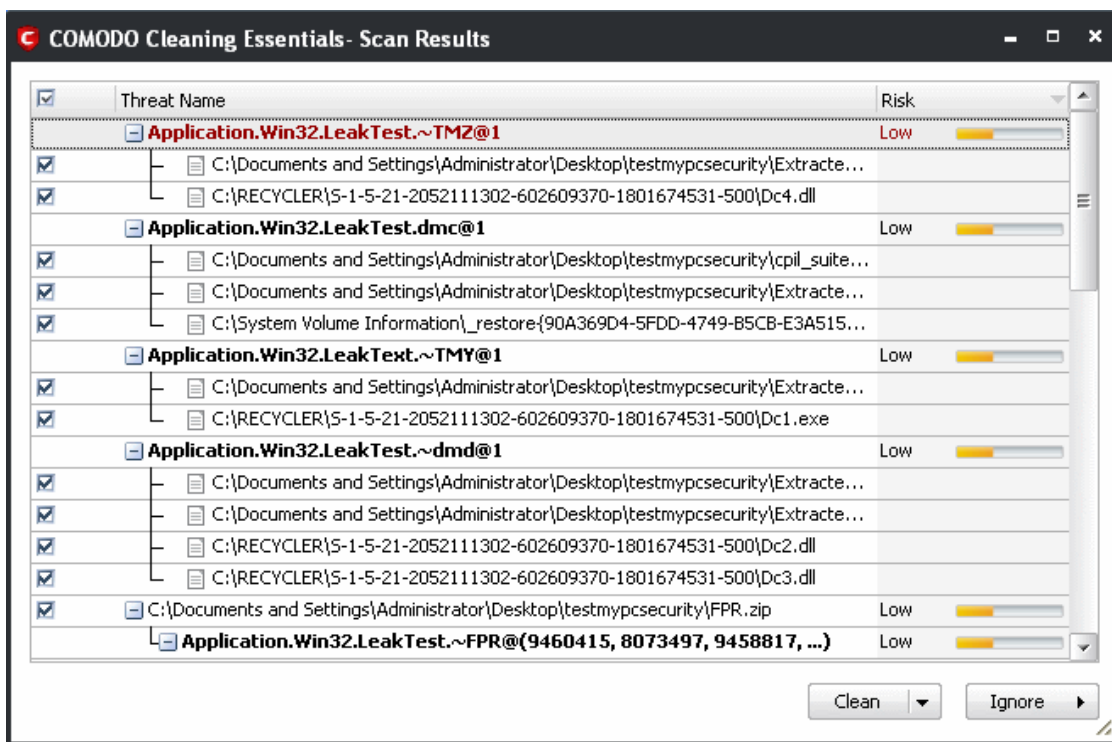
... and full scanning of your computer will start.



On completion of scanning, the 'Scan Finished' dialog will be displayed.



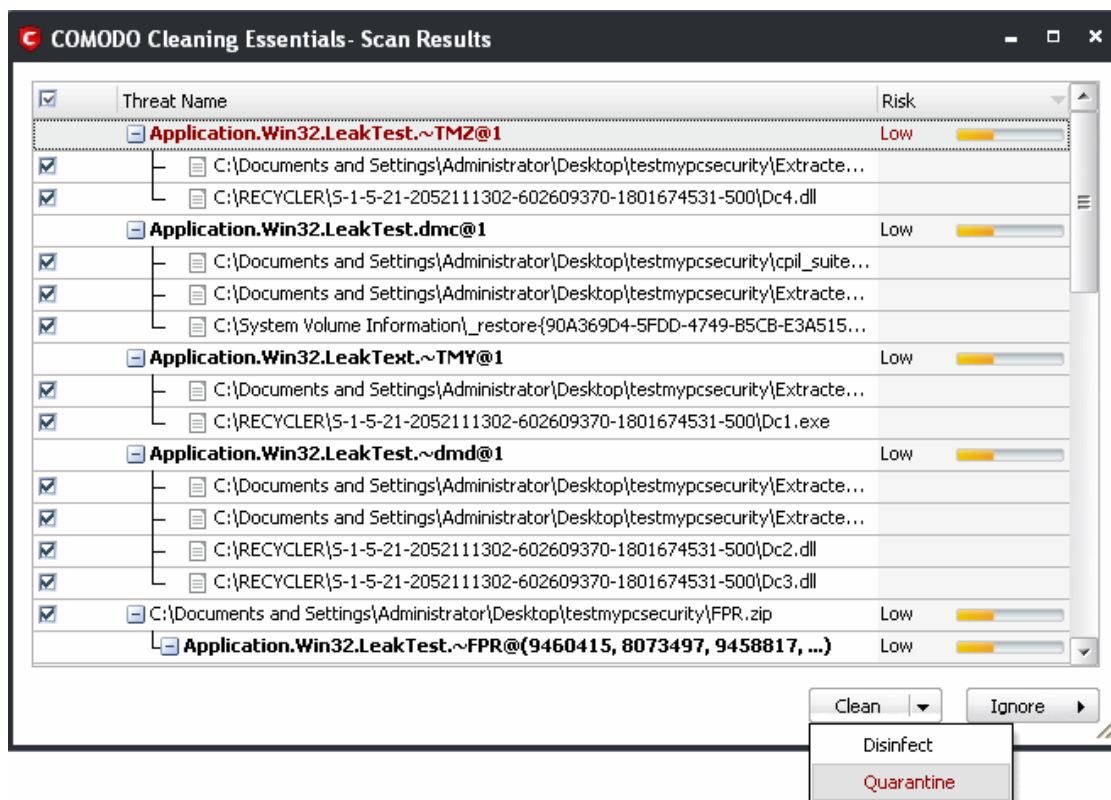
- Click 'Results' to view the Scan Results window. If malicious executables are discovered on your system, the scan results window displays the number of objects scanned and the number of threats (Viruses, Rootkits, Malware and so on).



**Tip:** You can sort the scan results by alphabetical order by clicking the 'Threat Name' column header. Similarly you can sort the scan results based on the risk level by clicking the 'Risk' column header. To select all the entries for actions such as moving them to quarantine or disinfect, select the check box beside the 'Threat name'.

## To move selected executables detected with threats to Quarantined Items

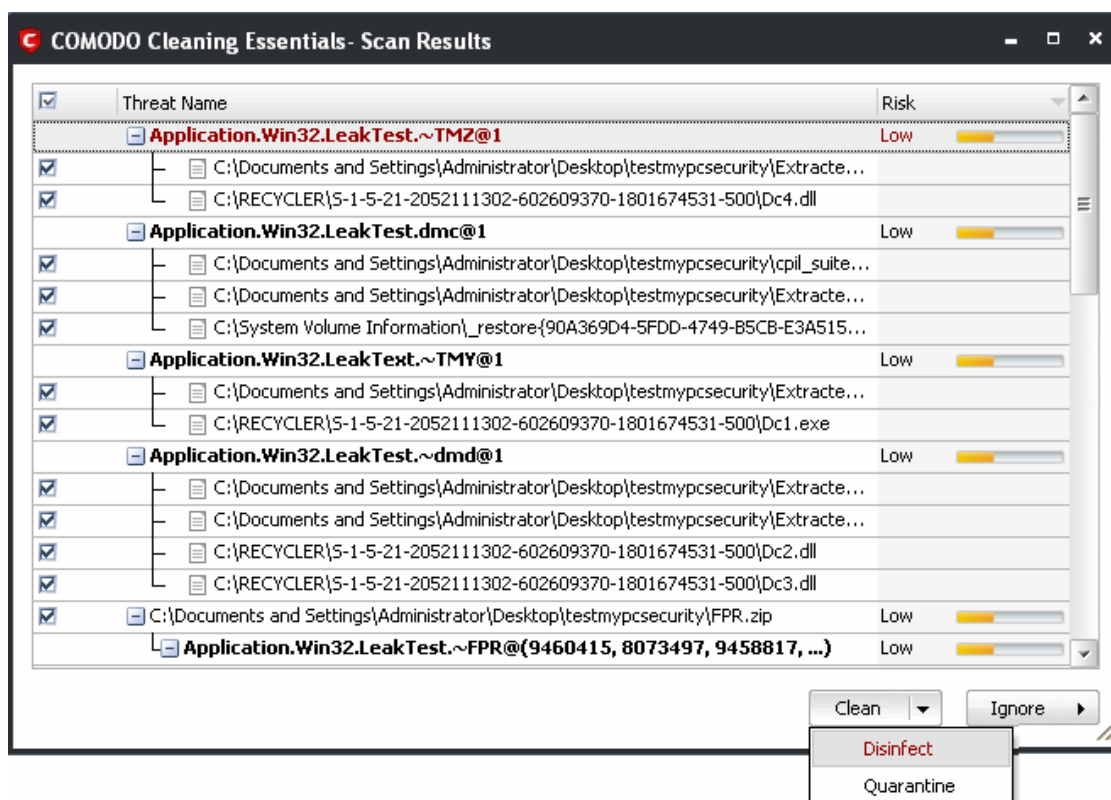
- Select the application from the results, click the drop-down button beside 'Clean' and select 'Quarantine'.



The selected items in the results window will be moved into quarantine. Click **'Options' > 'Quarantined Items'** to view quarantined applications, files/folders.

## To disinfect the file / application detected with a threat

- Select the application from the results, click the drop-down button beside the 'Clean' button and select 'Disinfect'.

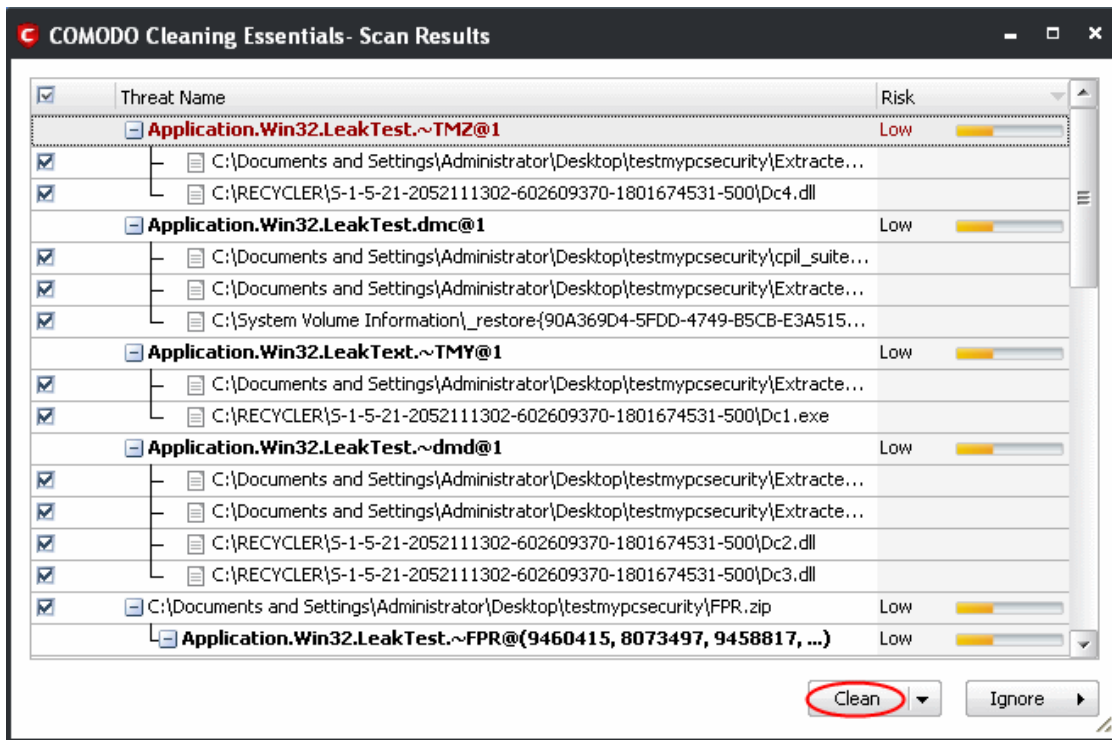


The antivirus disinfects the file if there exists a disinfection routine defined for the file and the file is recovered to its pre-viral

state. If no any disinfection routine is available, the file is deleted permanently from your system.

## To delete an application detected with a threat

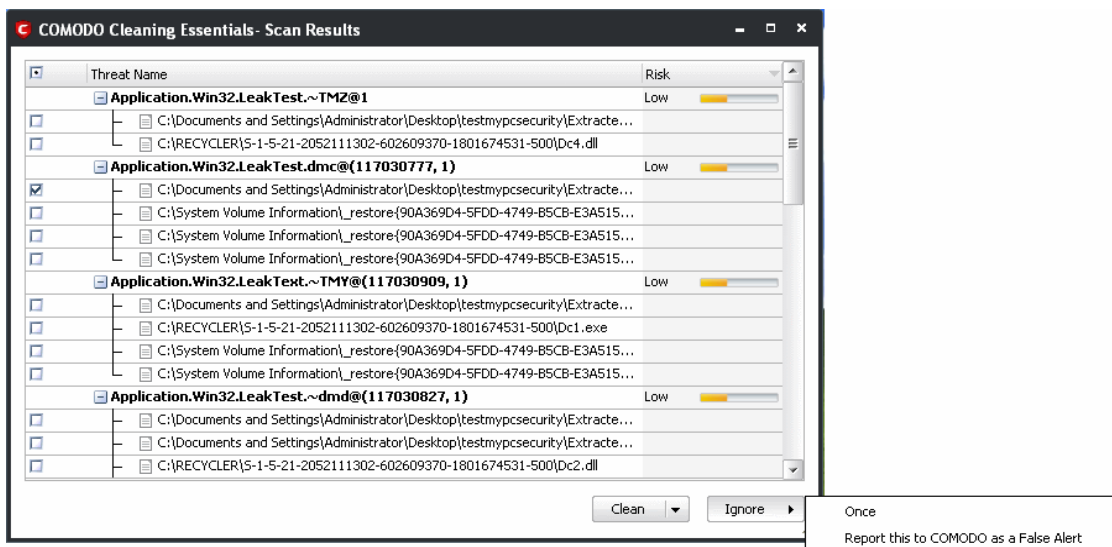
- Select the applications from the results, click the 'Clean' button.



The selected applications will be deleted from your system.

## To ignore an application / file you consider as safe from the threat list

- Click the 'Ignore' button



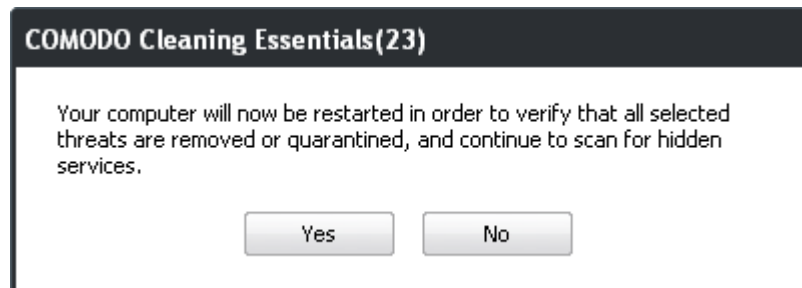
Selecting Ignore provides you with two options.

- **Once** - If you click 'Once', the virus is ignored only at that time only. If the same application invokes again, an Antivirus alert is displayed.
- **Report this to COMODO as a False Alert** - If you are sure that the file is safe, select 'Report this to COMODO as a False Alert'. The CCE sends the file to Comodo for analysis. If the file is trustworthy, it is added to the Comodo safelist.

When you close the results window after you have exercised your option to delete, disinfect or quarantine, CCE will ask your permission to restart the system to ascertain that the selected threats are indeed acted upon as opted. The restart dialog

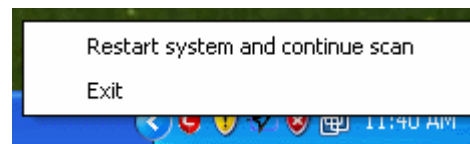
window will start a count down from 30 and if you do not choose either 'Yes' or 'No' option, the system will automatically restart when the count down reaches 0.

- Click 'Yes' to restart the system and to verify that the selected threats are removed or quarantined and to continue scanning for hidden services.



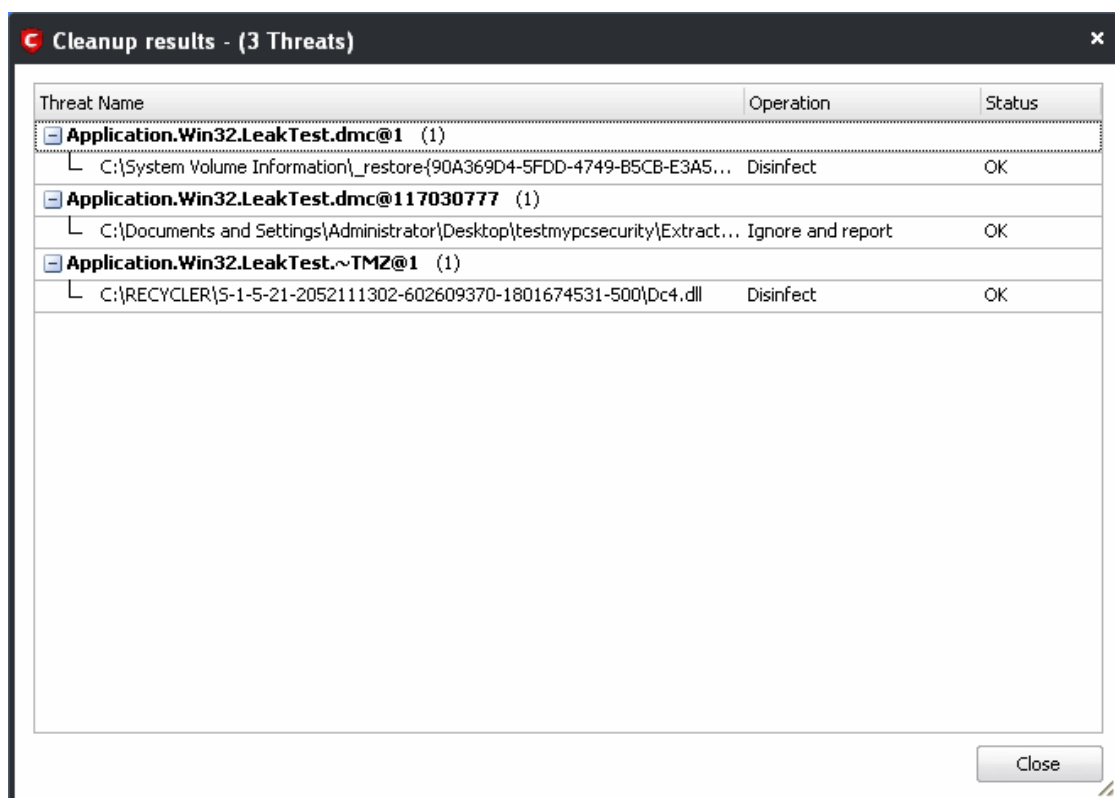
If you click 'No' the system will not restart. However, right-clicking the CCE system tray icon will provide you with two options:

- Restart system and continue scan
- Exit



- Click "Restart system and continue scan" to display the cleanup results or 'Exit' to exit the application.

When the system has restarted, CCE will display the cleanup results.



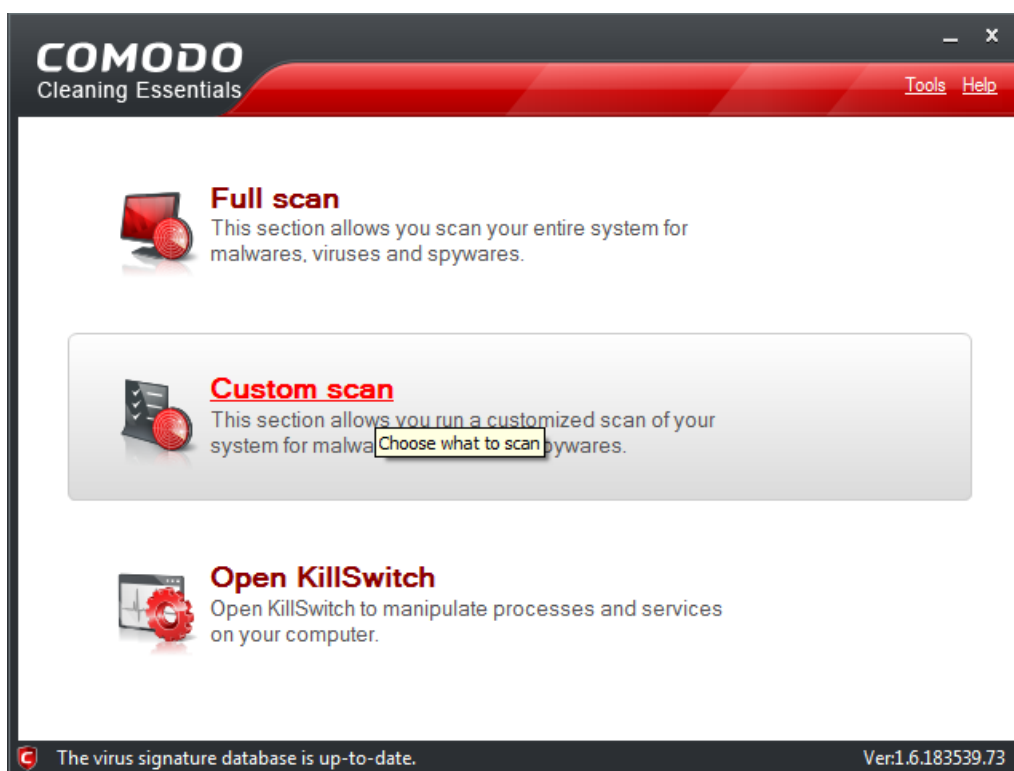
- Click the 'Close' button and the application will be closed.

## 2.2. Custom Scan

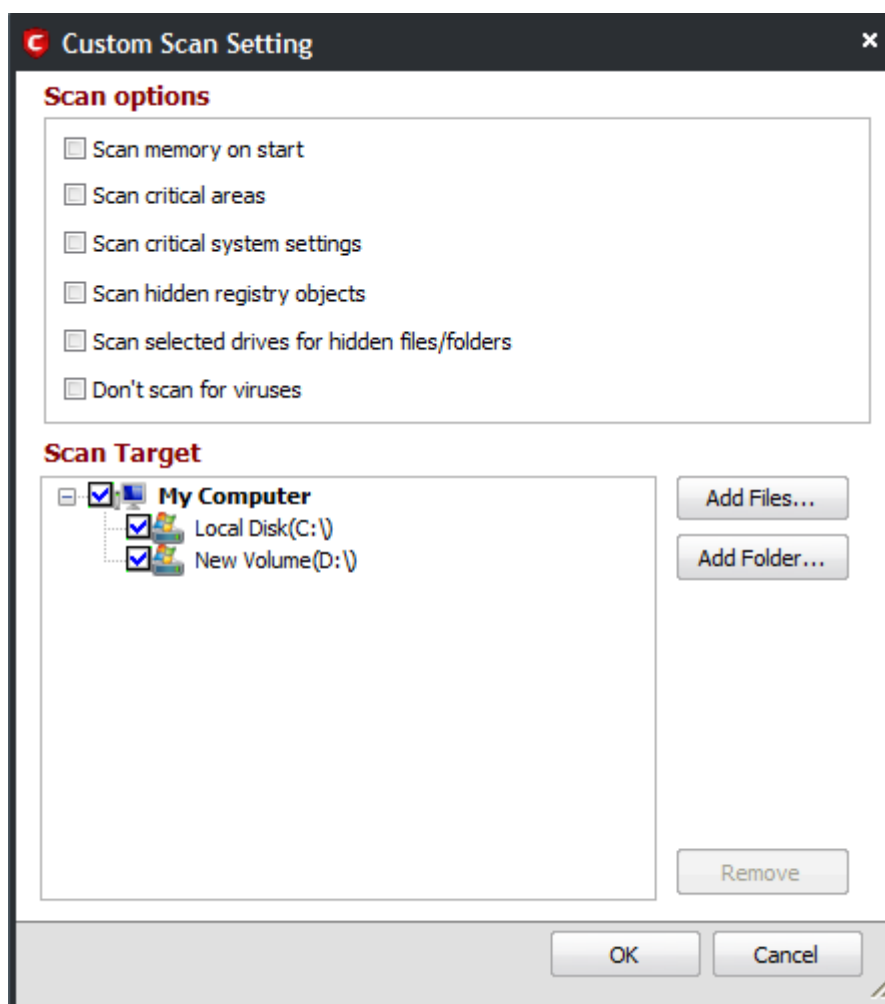
The custom scan feature allows you to check for viruses in any particular file/folder or drive. You may have just downloaded some files from the internet and not sure whether it is free from malware or not. The custom scan feature in CCE allows you to select a file or folder to check for malware or viruses. The custom scan feature is a useful and flexible complement to periodically running a 'regular' full scan of your system.

Custom Scan is relatively agile scan method. You can choose what would you want to scan, and where would you want to scan. Also, it doesn't need restart before scan. Accordingly, you have no way to do the extra scanning during startup.

- Click the Custom Scan feature in the main interface.



The Custom Scan Setting dialog window will be displayed.



You can select which options you prefer for the custom scan and also choose which specific files, folders or drives are to be included in the scan in the Scan Target area..

### Scan Options

- **Scan memory on start** - When selected, CCE scans the system memory during the start of any custom scan.
- **Scan critical areas** - When selected, CCE scans the Program Files folder and WINDOWS folder of the Operating System of your computer during the start of any custom scan.
- **Scan critical system settings** - When selected, CCE scans the system settings during the start of any custom scan.

**Note:** If this option is selected:

- CCE scans important registry keys and operating system settings. If any of these have been modified from their defaults then these will be listed in the results. Selecting 'Cleanup/Disinfect' will revert the settings back to their original values

- **Scan hidden registry objects** - When selected, all the hidden registry objects will be scanned by CCE during the start of any custom scan.
- **Scan selected drives for hidden files/folders** - When selected, CCE scans hidden files and folders in the drives that are selected in the Scan Target area.
- **Don't scan for viruses** - When selected, CCE will not check for viruses in the target areas.

**Note:** If this option is selected:

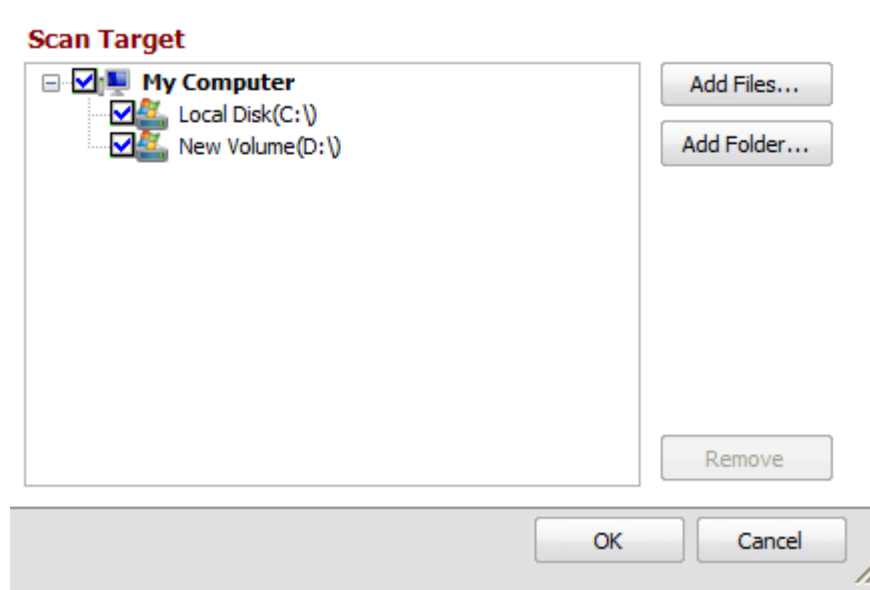
- CCE won't invoke AV engine entirely.
- 'Scan Memory on start' and 'Scan critical areas' will become greyed out and unavailable.

- You must choose at least one of the remaining options:
  - i. Scan critical system settings
  - ii. Scan for hidden registry objects
  - iii. Scan selected drives for hidden files/folders

You will not be able to run a scan on any targets unless one of the above is chosen.

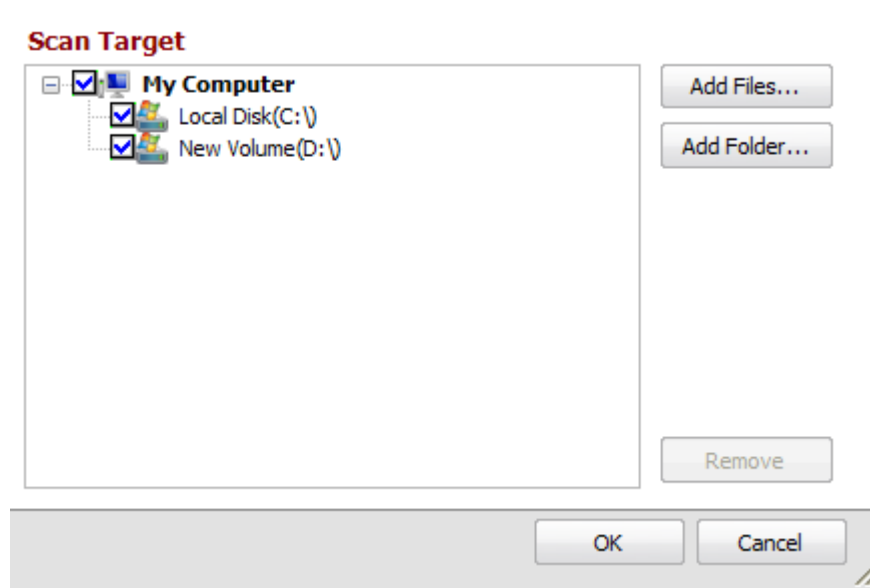
## Scan Target

By default, all the drives in your system will be selected for custom scan.



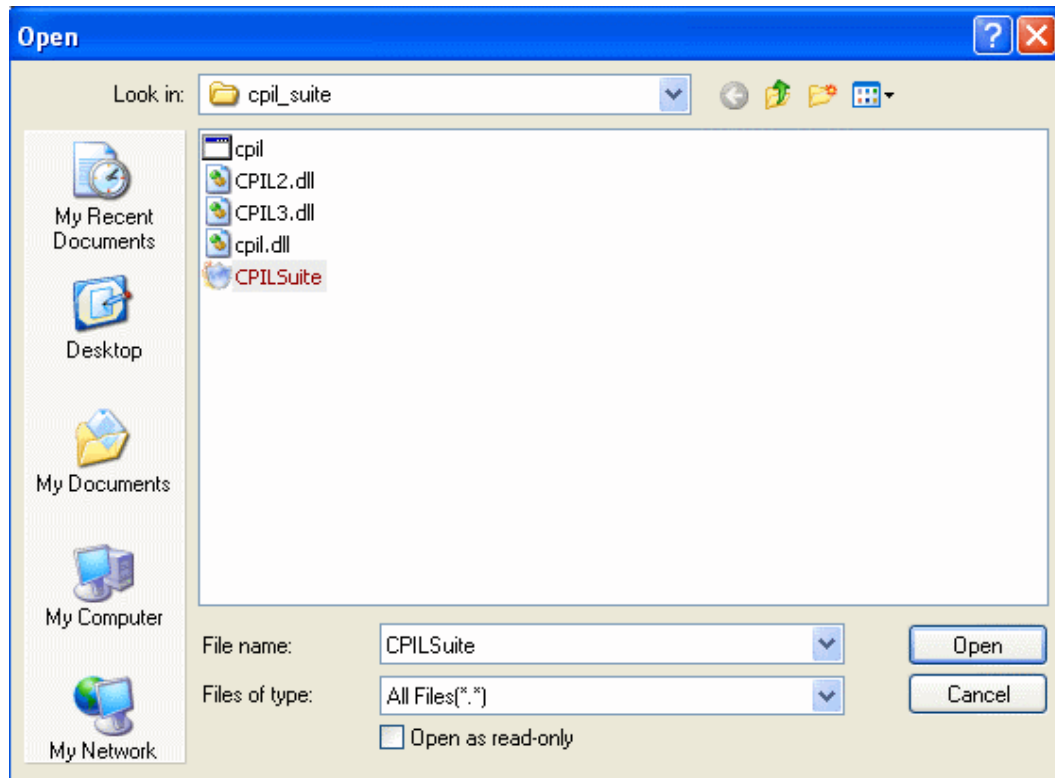
### To add files and run a custom scan

- Click the 'Add Files' button in the Scan Target area

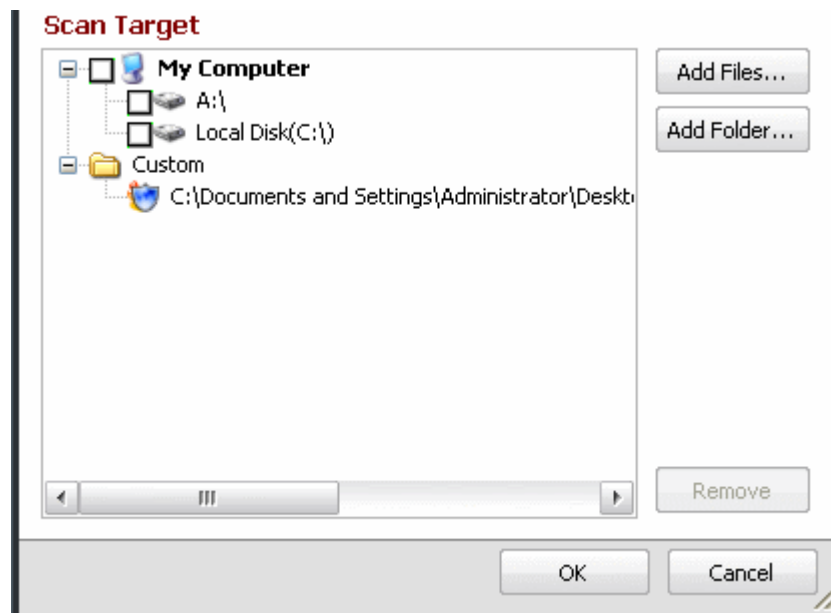




- Browse to the required file and click Open



The selected file will be added to the custom Scan Target area.

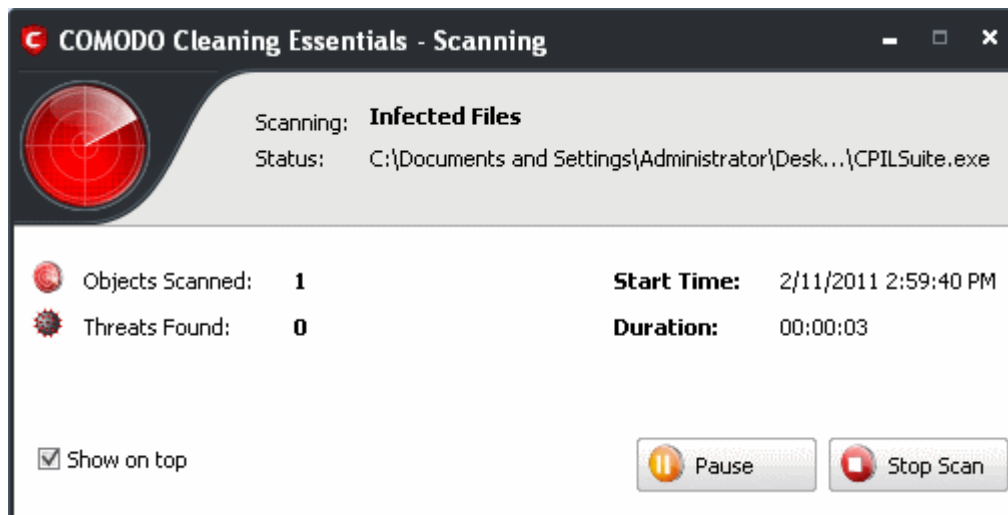


- Click 'Add Files' to add another file

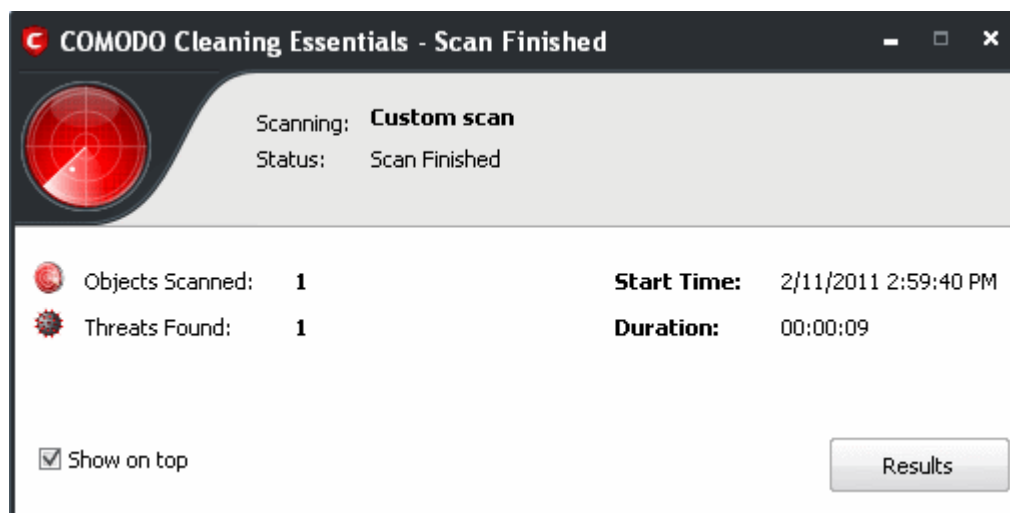
**Note:** You can add files and folders simultaneously for a custom scan.

- Click 'OK' to run the custom scan

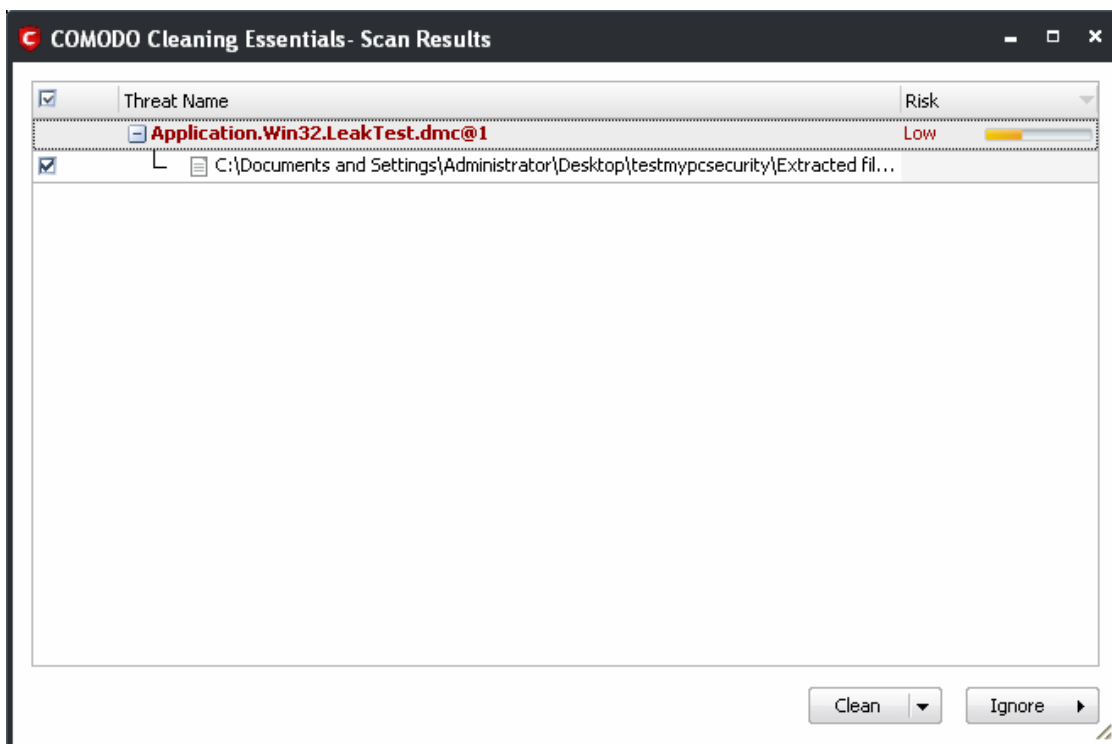
The custom scan for the added file will be performed...



...and when the custom scan for the selected file is completed, the Scan Finished dialog will be displayed.



- Click the 'Results' button to open the Scan Results window.

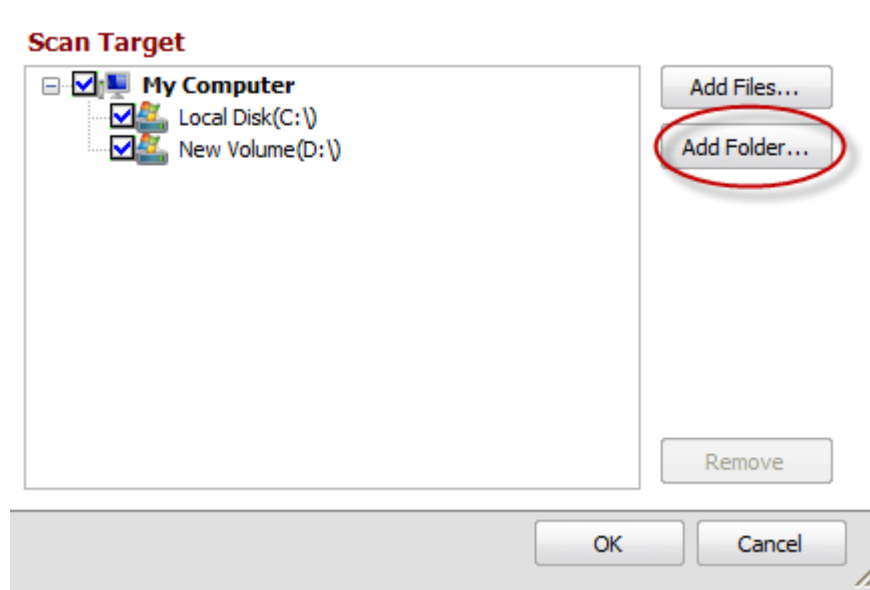


Click the following links to find out how to:

- [Clean the infected file/application](#)
- [Disinfect the file/application](#)
- [Quarantine the file/application](#)
- [Ignore the affected file/application](#)

## To add folders and run a custom scan

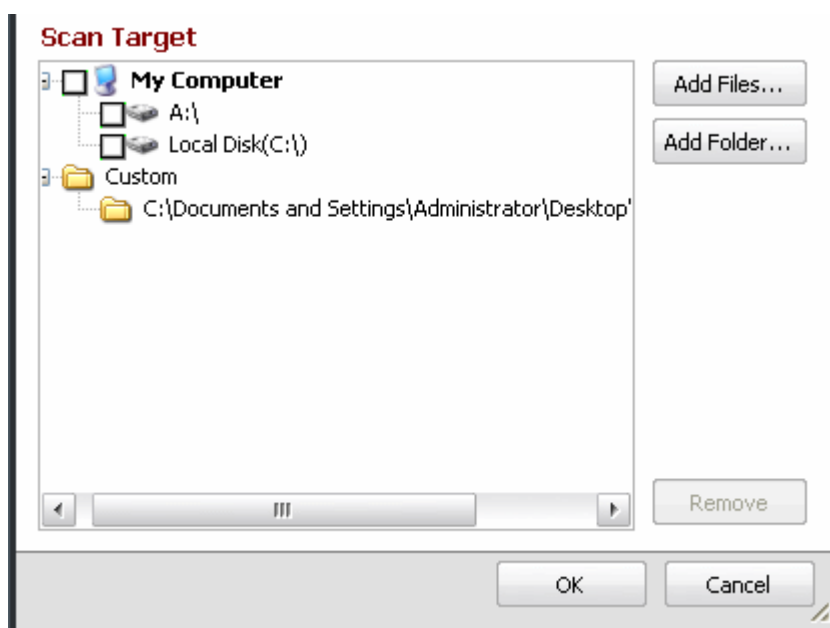
- Click the 'Add Folder' button in the Scan Target area



- Browse to required folder and click 'OK'



The selected folder will be added to the custom Scan Target area.

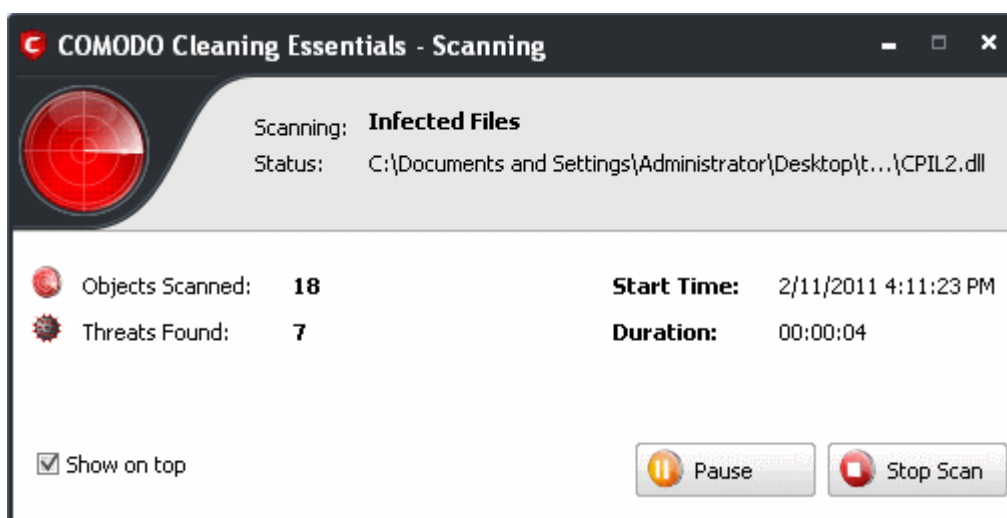


- Click 'Add Folder' to add another folder

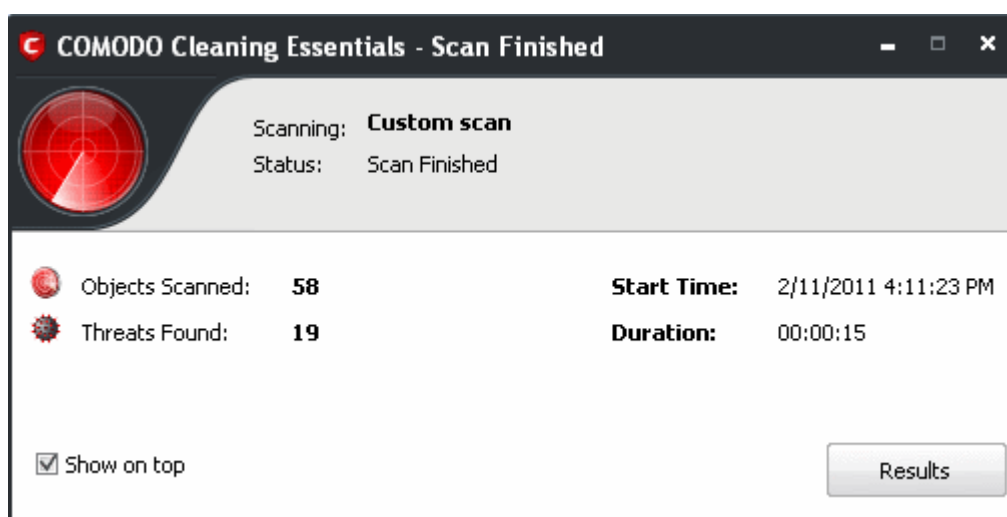
**Note:** You can add files and folders simultaneously for a custom scan.

- Click 'OK' to run the custom scan

The custom scan for the added folder will be performed...



...and when the custom scan for the selected folder is completed, the Scan Finished dialog will be displayed.



- Click the 'Results' button to open the Scan Results window.

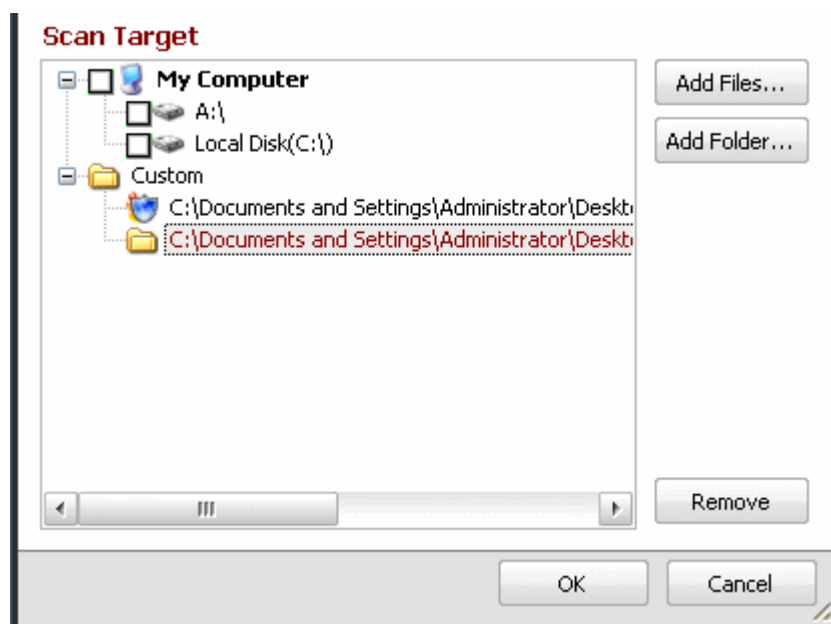


Click the following links to find out how to:

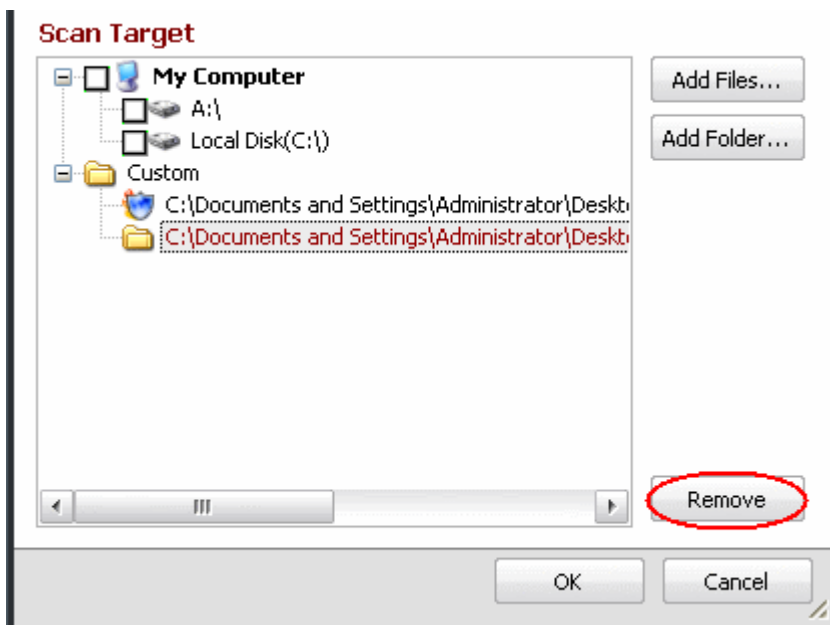
- [Clean the infected file/application](#)
- [Disinfect the file/application](#)
- [Quarantine the file/application](#)
- [Ignore the affected file/application](#)

## To remove files/folder from the Scan Target area

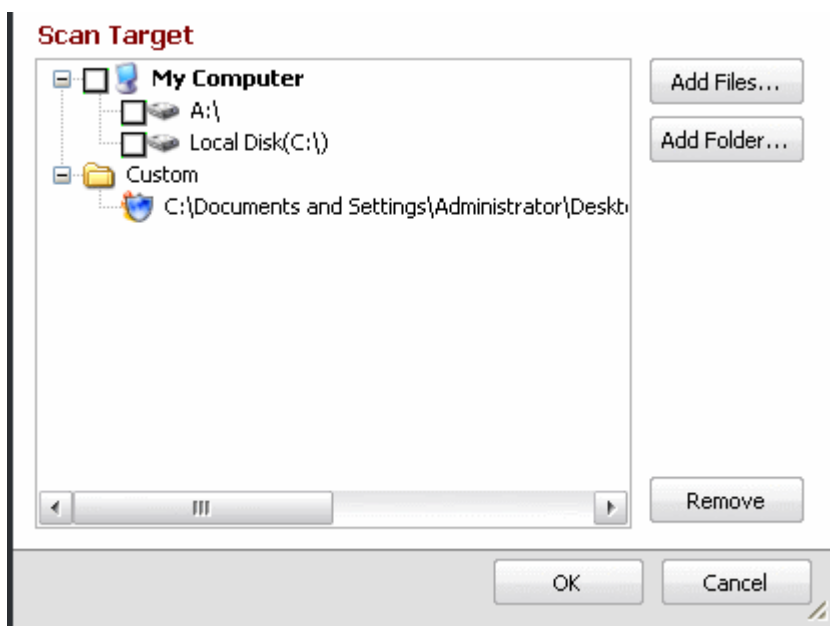
- Select the file/folder that you do not want for a custom scan



- Click the 'Remove' button



The selected file/folder will be removed from the custom scan area.



- Click 'OK' to proceed with the custom scan of the remaining files/folders.

The differences between a full and custom scan can be summarized as follows:

Scan Type		Note/Description	'Full' Scan	'Custom' Scan	
				'Don't Scan for Viruses' not selected	'Don't Scan for Viruses' selected
Scanner	Basic	File scanner of local AV	☑	☑	☒

Scan Type	Note/Description engine	'Full' Scan	'Custom' Scan		
	FLS	Cloud based File Lookup Scanner	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		Cloud based verification of a file's digital signature	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		Local check that the creator of the file is on the trusted vendor list	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	CAMAS	File is uploaded to Comodo Automated Malware Analysis System (CAMAS) for inspection	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Options</b>	Scan Memory on start	Requires restart	<input type="checkbox"/>	Optional	<input type="checkbox"/>
	Scan Critical Areas	-	<input type="checkbox"/>	Optional	<input type="checkbox"/>
	Scan Critical System Settings	-	<input type="checkbox"/>	Optional	<input type="checkbox"/>
	Scan hidden registry objects	-	<input type="checkbox"/>	Optional	Optional
	Scan hidden registry objects	-	<input type="checkbox"/>	Optional	Optional
	Scan selected drives for hidden files/folders	-	<input type="checkbox"/>	Optional	Optional



## 3. Introduction to KillSwitch

KillSwitch is an advanced system monitoring tool that allows users to quickly identify, monitor and terminate any unsafe processes that are running on their system. Apart from offering unparalleled insight and control over computer processes, KillSwitch provides you with yet another powerful layer of protection for Windows computers.

The unsafe processes addressed by KillSwitch are often triggered by malware that has been introduced onto your system. These harmful programs can gain entry onto your system in many different ways. For example, you may encounter malware by visiting a malicious website, by double clicking an attachment in a unsolicited e-mail message or on clicking on a deceptive pop-up window. Once installed, most malware will embed itself into your system as a resident program then attempt to initiate an attack. These attacks can take a variety of forms and include operating system exploits and scripts that could turn your computer into a zombie PC or allow the easy theft of your private data. Worst still, many of these processes are so well hidden they are completely invisible to the average user. This is where KillSwitch comes in.

KillSwitch can show ALL running processes - exposing even those that were invisible or very deeply hidden. It allows you to identify which of those running processes are unsafe and to shut them all down with a single click. You can also use KillSwitch to trace back to the malware that generated the process.

The KillSwitch section of this guide is broken down into the following sections:

- **Starting KillSwitch**
- **The Main Interface**
- **Viewing and Handling Processes and Services**
  - **Processes**
    - **Stopping, Starting and Handling the Processes**
    - **Viewing Properties of a Process**
    - **Searching for Handles or DLLs**
  - **Services**
    - **Stopping, Starting and Deleting the Services**
    - **Viewing the Properties of a Service**
  - **Network Connections**
    - **Inspecting and Closing Network Connections**
  - **Browser Helper Objects**
  - **Layered Service Providers**
- **The Tools Menu**
  - **Viewing System Information**
  - **Configuring KillSwitch**
  - **Managing Plug-ins**
  - **Creating a new Windows service**
  - **Scanning Your System for Hidden Processes**
  - **Viewing the Page Files in Your System**
  - **Verifying authenticity of Applications**
  - **Repairing Windows Settings and Features**
- **Managing Currently Logged-in Users**
- **Help and About Details**

### 3.1. Starting KillSwitch

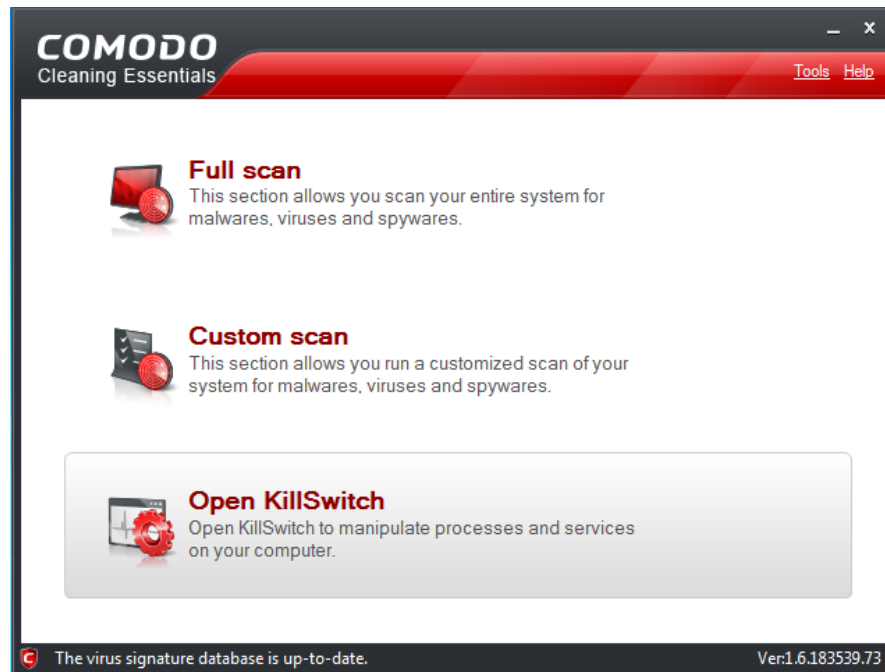
KillSwitch can be started by the following ways:

- **From the Comodo Cleaning Essentials interface**

- From the folder containing Comodo Cleaning Essentials files
- By replacing Windows Task Manager with KillSwitch

## 3.1.1. From the Comodo Cleaning Essentials Interface

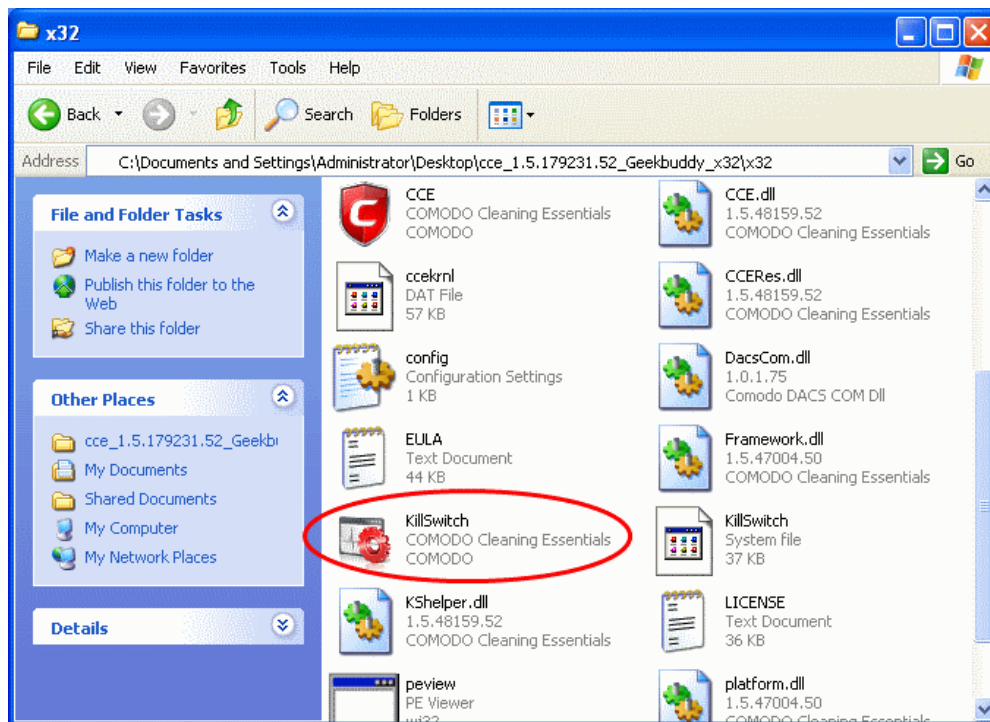
- Click on 'Open KillSwitch' option from the main interface of Comodo Cleaning Essentials



The KillSwitch main interface will be opened.

## 3.1.2. From the Folder Containing Comodo Cleaning Essentials Files

- Navigate to the folder containing the Comodo Cleaning Essentials files
- Double click on the file 'KillSwitch.exe' from the Windows Explorer window.



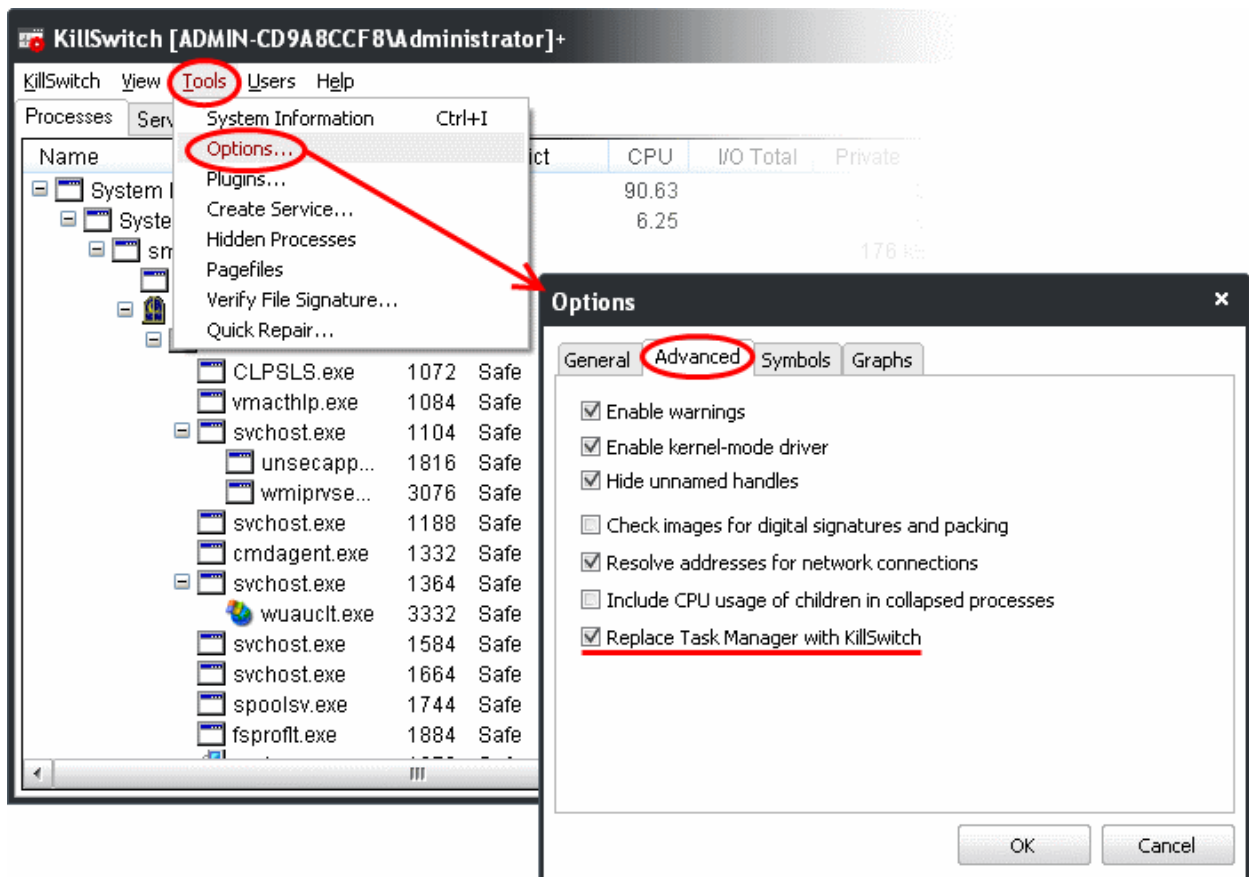
The KillSwitch main interface will be opened.

### 3.1.3. Replacing Windows Task Manager with KillSwitch

KillSwitch can be configured to replace Windows Task Manager. Doing so will mean that KillSwitch can be opened by:

- Pressing Ctrl + Alt + Del and clicking Task Manager;
- Right-clicking on the Task Bar and selecting 'Task Manager' from the pop-up menu;
- Pressing Ctrl + Shift + Esc;
- Clicking 'Start' > 'Run' and typing the command 'taskmgr'.

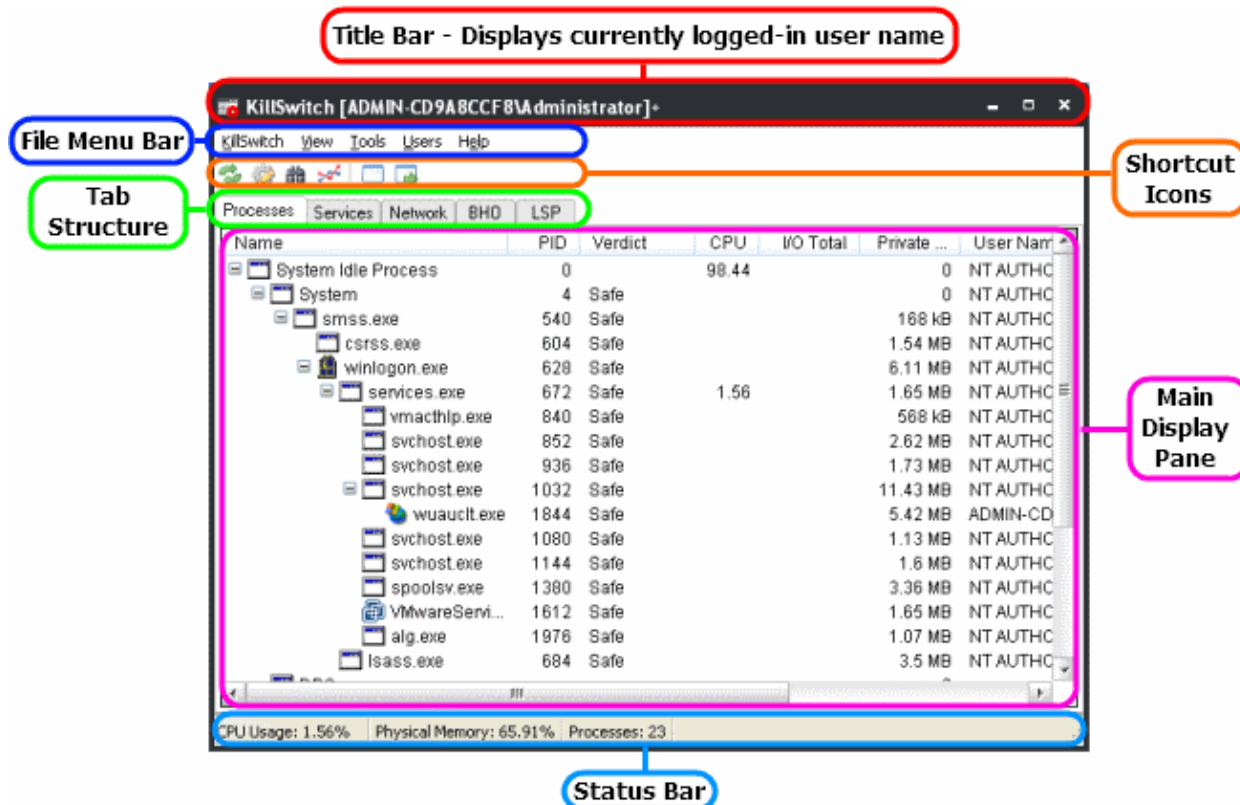
To replace Task Manager with KillSwitch, you first need to start the application by one of the methods explained **above**, click 'Tools' > 'Options' > 'Advanced' and enable 'Replace Task Manager with KillSwitch'.



For more details, refer to the description of '**Replace Task Manager with KillSwitch**' in the section '**Tools**' > '**Options**' > '**Advanced Settings**'.

## 3.2. The Main Interface

KillSwitch's streamlined interface provides access to all important features and options of the application at finger tips.



The interface is divided into four main areas:

- **The File Menu bar;**
- **Shortcut Icons;**
- **Tab Structure;**
- **Main display Pane;**
- **Status Bar.**

## The File Menu Bar

The file menu bar displays the controls for executing various tasks and configuring the overall behavior of the application.

Menu	Option	Description
KillSwitch		Contains options related to handling processes, objects and dll files collectively, shortcuts for running command line interface programs and switching power state of your system.
	Terminate All Unsafe Processes	Stops all the currently running processes that are identified as unsafe by KillSwitch. <b>Note:</b> By stopping a running process you will lose any unsaved data being used by the application that generated the process. Save data in all running applications before selecting this option.
	Suspend All Unsafe Process	Temporarily halts all the currently running processes that are identified as unsafe by KillSwitch in their current states. Suspended processes can be resumed by right clicking on the process in the process tab and selecting 'Resume' from the context sensitive menu.
	Delete All Unsafe Objects	Deletes data and files that have been identified as unsafe by KillSwitch. An 'object' is a process or library that has been loaded into memory. Every process is an object but not every object is a process.

	Rename All Unsafe Objects	Renames data and files that have been identified as unsafe by KillSwitch.
	Unload All Unsafe DLLs	Removes all the dll files that are identified as unsafe by KillSwitch, from the system memory.
	Run	Opens the Windows 'Run' dialog for executing command line interface programs with administrative privileges.
	Run as Limited User	Opens the Windows 'Run' dialog for executing command line interface programs with default limited user privileges.
	Run As	Opens the Windows 'Run' dialog for executing command line interface programs with privileges granted to a specified user of the computer.
	Save	Opens the 'Save as' dialog to save the currently displayed list in the main display area as a .txt file or .csv file.
	Find handles or DLLs	Opens a 'Filter' dialog that enables you to make a quick search to identify the Handles, DLLS that are triggered or loaded to system memory or mapped files , by entering the name of the object. Refer to the section <b>Searching for Handles or DLLs</b> for more details.
	Computer	Enables you to switch the power state of your computer. Hovering the mouse cursor options opens a sub-menu containing the following options: <ul style="list-style-type: none"> <li>• Lock;</li> <li>• Log-off;</li> <li>• Sleep;</li> <li>• Hibernate;</li> <li>• Restart;</li> <li>• Shutdown;</li> <li>• Power-off.</li> </ul>
	Exit	Closes the KillSwitch application.
View		Contains options related to display nature of the application.
	Tray Icons	Enables you to select the tray icons displayed in the system tray at the bottom right corner of the screen. The icons are displayed as usage/history indicators of various system hardware resources. The choices available are: <ul style="list-style-type: none"> <li>• CPU History</li> <li>• CPU Usage</li> <li>• I/O History</li> <li>• Commit History</li> <li>• Physical Memory History</li> </ul> Right clicking the tray icons opens a panel containing shortcuts for executing various tasks. For more details, refer to the next section <b>System Tray Icon</b> .
	Show Only the Unsafe Images in Memory	Displays only the program images identified as unsafe by KillSwitch currently loaded to system memory in the main display area.
	Hide Safe Objects	Displays only the items identified as unsafe by KillSwitch in the main display area, relevant to the tab selected. This is useful to identify the unsafe objects just at-a-glance.







	Always on Top	Selecting this makes the KillSwitch window to displayed on top of all the windows that are currently open in your system.
	Opacity	Enables you to set the transparency of KillSwitch window. The choices range from 10% to full opaque, in the intervals of 10.
	Refresh	Updates and refreshes the KillSwitch window.
	Update Interval	Enables you to set the interval at which KillSwitch automatically refreshes itself and updates the details in the main display area. The choices range from fast (0.5 seconds) to Very Slow (10 seconds)
	Update Automatically	KillSwitch automatically refreshes and updates the details displayed in the main display area only if this option is selected. If you want to view the details fetched at a specific moment and wish to keep it without updates for some time e.g. for analysis purposes, you can temporarily disable this option.
Tools		Contains options for viewing graphical representations of usage/history of your system resources, configuring overall behavior of the application and accessing additional utilities. Refer to the section ' <b>The Tools Menu</b> ' for more details.
	System Information	Opens the System Information panel that shows the graphical representations and statistics of the usage/history of your system resources. Refer to the section ' <b>Viewing System Information</b> ' for more details.
	Options	Opens the 'Options' dialog that enables you to configure the overall behavior of the application. Refer to the section ' <b>Configuring KillSwitch</b> ' for more details.
	Plug-ins	Opens the 'Plug-ins' dialog that enables you to configure various plug-ins added to KillSwitch application for executing tasks like raising notifications, controlling Windows Services etc. Refer to the section ' <b>Managing Plug-ins</b> ' for more details.
	Create Service	Enables you to create your own user-defined Windows Service for Windows applications and some 16-bit applications. Creating a service for applications allows them to be started along with Windows irrespective of the user that logs-in to the system. Refer to the section ' <b>Creating a Windows Service</b> ' for more details.
	Hidden Processes	Enables you to initiate a scan for hidden processes running currently in your system. Most of the malware/spyware trigger their process and run them concealed, so that they would not be visible in the list of processes. The 'Hidden Processes' feature enables you to scan your system for such processes and to check whether any malware/spyware is currently running in your system. Refer to the section ' <b>Scanning Your System for Hidden Processes</b> ' for more details.
	Page files	Opens the 'Pagefiles' dialog that displays a list of page files that are currently stored on secondary storage, e.g. different drive partitions of your hard disk drive. Refer to the section ' <b>Viewing Page Files in Your System</b> ' for more details.
	Verify File Signature	Enables you to check whether applications/programs installed and files stored in your system are trusted and digitally signed to confirm the authenticity of them. Refer to ' <b>Verifying Authenticity of Applications</b> ' for more details.
	Quick Repair	Provides a shortcut to troubleshoot and and repair important Windows settings and features. Refer <b>Repairing Windows Settings and Features</b> for more details.



Users		Enables to manage the status of user(s) that have currently logged-on to the system. Refer to ' <b>Managing Currently Logged-in Users</b> ' for more details.
Help		Contains options to get help and support on usage of the product and to view the 'About' dialog. Refer to <b>Help and About Details</b> for more details.
	Search	Opens online Comodo Cleaning Essentials help guide.
	About	Opens KillSwitch 'About' dialog that contains the version, license and copyright information and an option to diagnose the KillSwitch installation in your system.

## Shortcut Icons

This area displays several shortcuts. The icons enable you to directly execute certain tasks, which can otherwise be executed from the menus and options in the file menu bar.

Icon	Task Executed
	Updates and refreshes the KillSwitch window.
	Opens the 'Options' dialog that enables you to configure the overall behavior of the application. Refer to the section ' <b>Configuring KillSwitch</b> ' for more details.
	Opens a 'Filter' dialog that enables you to make a quick search to identify the Handles, DLLS that are triggered or loaded to system memory or mapped files , by entering the name of the object. Refer to the section <b>Searching for Handles or DLLs</b> for more details.
	Opens the System Information panel that shows the graphical representations and statistics of the usage/history of your system resources. Refer to the section ' <b>Viewing System Information</b> ' for more details.
	Shows the application window corresponding to the process/service selected from the main display pane until you keep the icon clicked. <b>Note:</b> Clicking the 'Show Window' shows only the application window that is in open state and not the windows minimized to task bar.
	Shows the application window corresponding to the process/service selected from the main display pane until you keep the icon clicked and displays the ' <b>Properties</b> ' dialog of the selected process with the ' <b>Threads</b> ' tab opened to view the threads associated with the process.

## Tab Structure

The Tabs area contains a set of tabs for selecting the items you wish to view in the main display area and to control them through context sensitive menu.

Tab	Items Displayed
<b>Processes</b>	Displays the currently running processes in your system
<b>Services</b>	Displays the Windows Services started along with your system
<b>Network</b>	Displays the currently running processes that are involved in network connection activities.
<b>BHO</b>	Displays the list of plug-ins added to Internet Explorer. Examples include plug-ins that help in opening files of different formats in the browser window, plug-ins for displaying additional tool bars.
<b>LSP</b>	Displays a list of Layered Service Provider dll files which are currently installed in your system for regulating



Internet traffic from/to applications like web browser, email client that access Internet.

## Main Display Pane

The main display pane displays the list of items like Processes, Services etc. as per the selected tab with required details on each entry as a table. Right clicking on an entry opens the context sensitive menu with the options relevant to the items displayed.

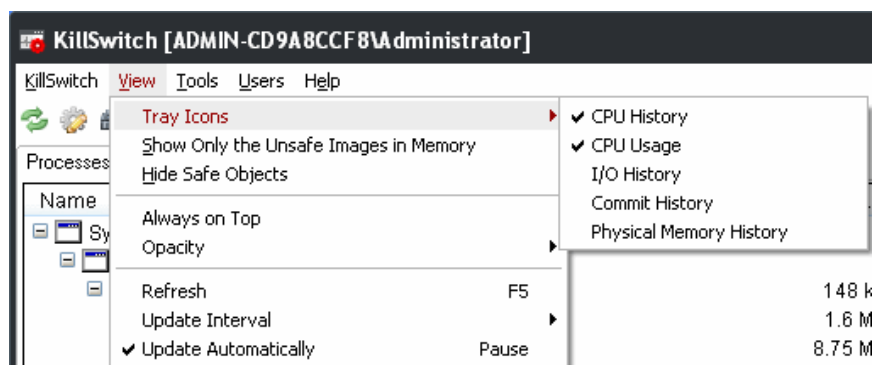
## The Status Bar

The status bar at the bottom of the interface displays the current CPU usage and the occupied volume of the system memory (in percentage) by the currently running processes and the total number of processes currently running in your system.

## 3.2.1. The System Tray Icons

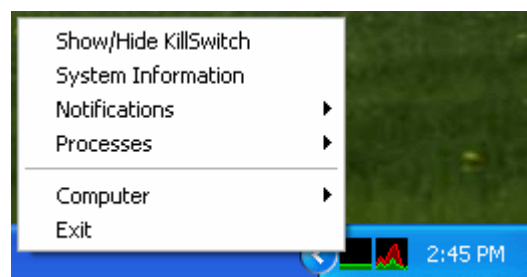
KillSwitch displays icons in the system tray at the bottom right corner of the screen as set through 'View' > 'Tray Icons' option. Each icon is displayed as a graphical representation of the history/usage of the respective hardware/software resource as chosen from the options given below:

- CPU History;
- CPU Usage;
- I/O History;
- Commit History;
- Physical Memory History.



Right clicking on any of the system tray icon opens a context sensitive menu that contains the following options:

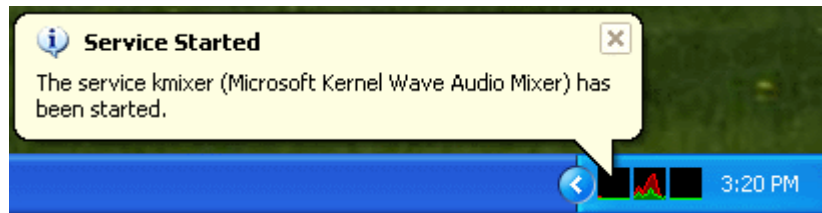
- **Show/Hide KillSwitch;**
- **System Information;**
- **Notifications;**
- **Processes;**
- **Computer;**
- **Exit;**



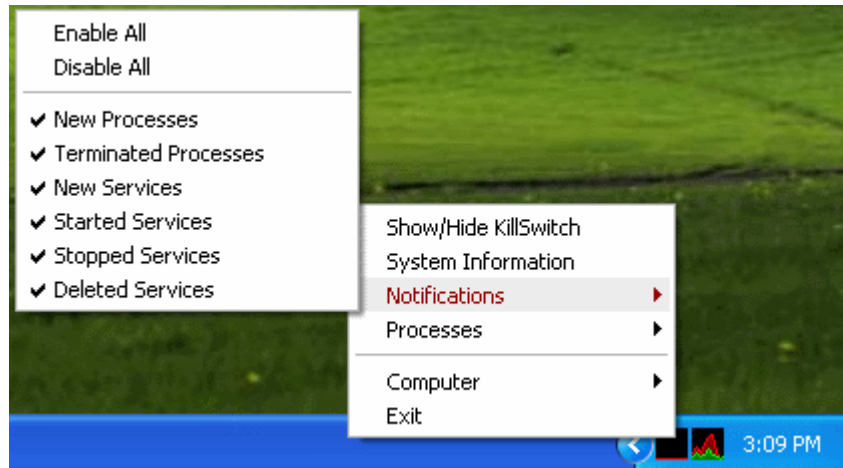
- **Show/Hide KillSwitch** - Enables you to switch between Show and Hide states of KillSwitch application window.

**Tip:** Double clicking on any of the system tray icon also allows you to switch the KillSwitch application window between Show and Hide states

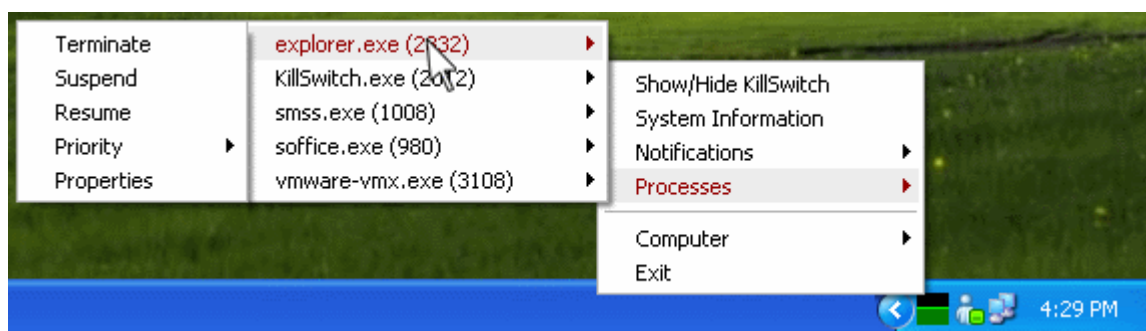
- **System Information** - Opens the System Information panel that shows the graphical representations and statistics of the usage/history of your system resources. Refer to the section '**Viewing System Information**' for more details.
- **Notifications** - KillSwitch can instantly alert you with a balloon messages whenever certain events like start/stop of a process/service happen. The balloon messages pop-out from the right corner of the screen.



The notification option in the context sensitive menu allows you to configure precisely which events will trigger a notification.

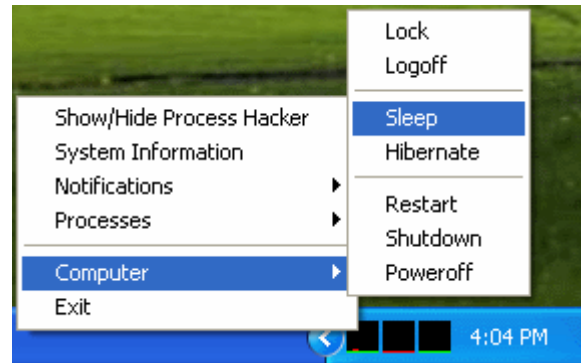


- **Enable All** - Raises an alert on all the events.
- **Disable All** - Switches alerts off.
- **New Processes** - Raises an alert whenever a new process is created/started by the system or when the user starts certain applications.
- **Terminated Processes** - Raises an alert whenever a running process is stopped/killed by the system or when the user closes certain applications.
- **New Services** - Raises an alert whenever a new service is created by the system or when the user starts certain applications.
- **Started Services** - Raises an alert whenever a stopped service is restarted by the system or when the user starts certain applications.
- **Stopped Services** - Raises an alert whenever a running service is stopped.
- **Deleted Services** - Raises an alert whenever a running/stopped service is deleted by the user.
- **Processes** - Displays a list of the processes running in your system and allows you to stop, suspend, resume, set priority and view the **Properties** dialog of any process by hovering the mouse cursor over it and selecting the option from the mouse-over options.



**Tip:** By default, five processes are displayed in the 'Processes' sub-menu pane. You can change the number of processes to be displayed by setting the value of '**Icon Processes**' field under 'General' tab of 'options' dialog. Refer to '**Tools**' > '**Configuring KillSwitch**' > '**General Settings**' for more details.

- **Computer** - Enables you to switch the power state of your computer. Hovering the mouse cursor options opens a sub-menu containing the following options:
  - Lock;
  - Log-off;
  - Sleep;
  - Hibernate;
  - Restart;
  - Shutdown;
  - Power-off.



- **Exit** - Closes the KillSwitch application.

### 3.3. Viewing and Handling Processes and Services

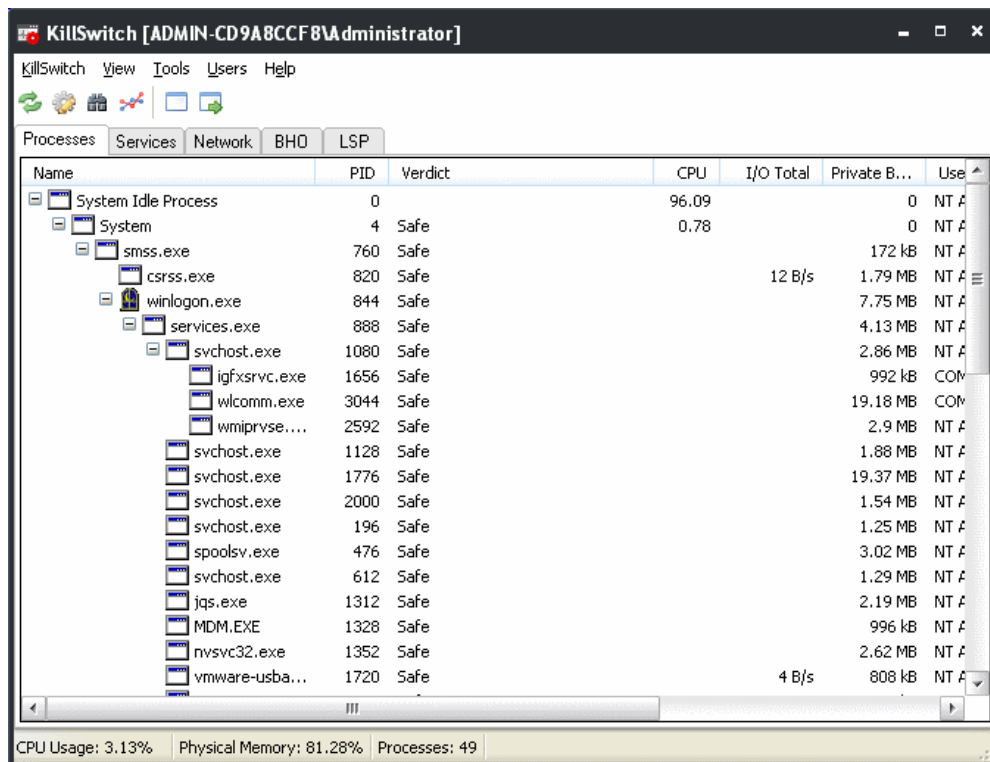
The main display pane of the application window displays the list of currently running processes, services etc., based on the tab selected from the tab structure. Right-clicking on each entry opens context sensitive menu that enables starting/stopping the processes/services, viewing properties of the processes etc. The tab structure contains the following tabs:

- **Processes;**
- **Services;**
- **Network Connections;**
- **Browser Help Objects (BHO);**
- **Layered Service Providers (LSP).**

#### 3.3.1. Processes

The Processes tab displays all the processes that are currently running in your system as a table in the main display pane.

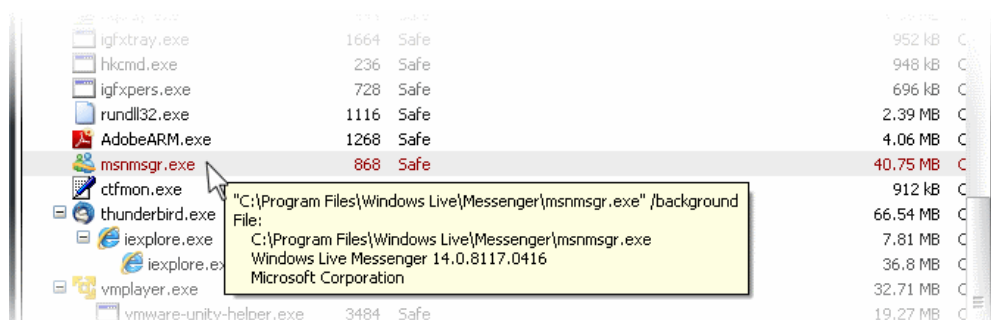
- The processes can be viewed in tree view or as a list.
- The new processes started and the processes that are stopped are highlighted.
- Right clicking on a process opens a context sensitive menu that enables you to perform various operations like stop, restart, set priority, view properties, etc, on the process. You can even select multiple process (by holding the 'Ctrl' key while selecting the processes) to execute these actions.



**Process Table - Descriptions of Columns**

Column	Description
Name	Displays the name of the processes. Clicking on the column header enables sorting the entries in tree structure, ascending or descending alphabetical order of the processes names.
PID	Displays the Process Identification number. Clicking on the column header enables sorting the entries in ascending or descending order of the PID numbers.
Verdict	Displays the result of analysis on each process by KillSwitch using different scanners such as <b>CAMAS</b> . Processes are indicated as 'Safe' or 'Unsafe' as per the analysis.
CPU	Displays the CPU usage of the process as a portion of overall CPU usage by the process in percentage. <b>Note:</b> For the processes which are collapsed in the display, the shown CPU usage will include the usage by the child processes only if the option ' <b>Include usage of children in collapsed processes</b> ' is enabled under the ' <b>Advanced</b> ' tab of ' <b>Tools</b> ' > ' <b>Options</b> ' dialog. Else, only the usage by the parent process will be displayed.
I/O total	Shows the speed at which data is input to/output from the process.
Private Bytes	Shows the current size of system memory allocated to the process that cannot be shared with other processes.
User Name	Displays the user that has initiated the process.
Description	Describes the nature of the processes.

- Placing the mouse cursor over a process displays a tool-tip that contains the details of the process.

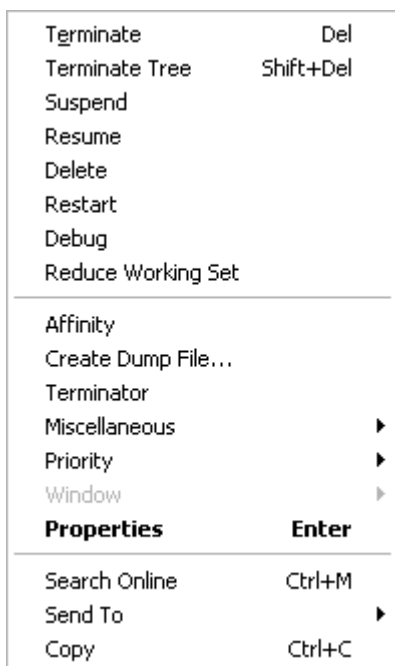


### 3.3.1.1. Stopping, Starting and Handling the Processes

The 'Processes' tab allows you to stop, suspend, restart, set priority, view properties etc. of individual processes, by right clicking on the processes and selecting the option from the context sensitive menu.

**Tip:** KillSwitch can identify all unsafe processes and objects and then, according to your preference, Terminate, Suspend, Delete, Rename or Unload them all at once. To do this, click '**KillSwitch**' from the **file menu bar** and select the required option.

- Right click on a process to open the context sensitive menu.



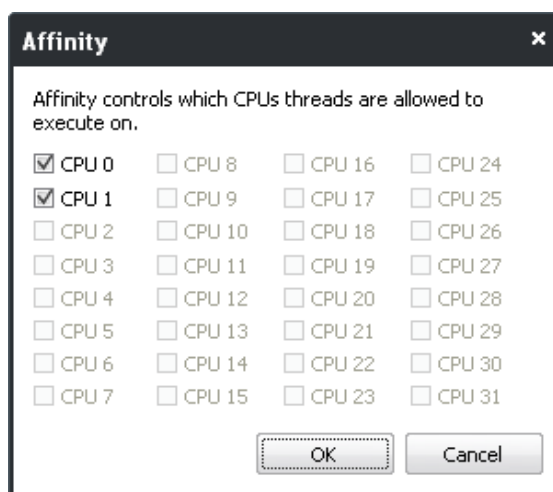
- **Terminate** - Terminates the selected process(es). KillSwitch can, except under extraordinary circumstances, be able to terminate any process, including ones protected by rootkits or security software.
- **Terminate Tree** - Terminates the selected process and its descendants (child processes).
- **Suspend** - Suspends the selected process(es). KillSwitch can suspend any process, including ones protected by rootkits or security software.
- **Resume** - Resumes the selected (suspended) process(es). KillSwitch can resume any process, including ones protected by rootkits or security software.
- **Delete** - Deletes the selected (running or suspended) process(es) from the disk. KillSwitch can delete any process, including ones protected by rootkits or security software. You will be asked for confirmation before deleting a process. Your computer will need a restart for this action to take effect.

**Warning:** Deleting a process will permanently remove the application that has triggered the process.

- **Restart** - Restarts the selected process with the same command line arguments and working directory.
- **Debug** - Starts the debugger, for the selected process. This is useful for the software developers and testers, to debug the applications that are newly installed in their systems.
- **Reduce Working Set** - Empties the working sets involved with the selected process(es). This is a safe function; the process will eventually reclaim most of its working set.

**Background Note:** The working set of a process is the collection of information referenced by the process periodically. This collections are stored as page files in the secondary memory, such as the portion of the hard disk partitions allotted as virtual memory.

- **Affinity** - Enables you to view and modify the process' processor affinity (the CPU to which the process is allocated) in a in a symmetric multiprocessing operating system e.g. to reduce cache related problems.

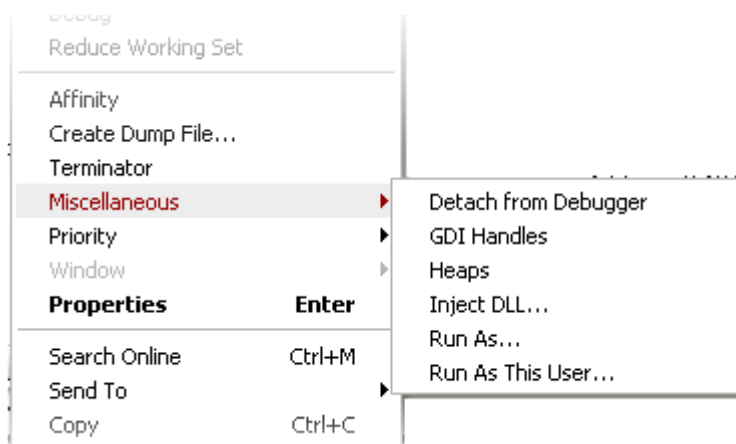


**Background Note:**

In a symmetric multiprocessing operating system, each task (process or thread) in the queue is assigned with a tag indicating its preferred processor so that it is allocated to the preferred processor during allocation time.

Some remnants of a process may remain in one processor's cache from the last execution. Scheduling the same process to run on the same processor next time will increase the efficiency of the process, when compared to running on another processor. For example, an application which does not use multiple threads, such as some graphics-rendering software is run on multiple instances, allocating it to the same processor will reduce the performance-degradation due to cache misses and increase the overall system efficiency.

- **Create Dump File** - Enables you to create a crash dump file for the process. This operation does not actually cause the process to crash or terminate.
- **Terminator** - Selecting this option initiates an in-built terminator tool that kills the selected process(es) using various techniques, if the process cannot be terminated directly by KillSwitch.
- **Miscellaneous** - Contains options to view miscellaneous details and to perform miscellaneous operations on the selected process.



- **Detach from Debugger** - Disassociates the process from any running debugger. This will cause any attached debuggers to stop working.
- **GDI Handles** - Displays the list of Graphics Device Interface (GDI) handles (brushes, pens, fonts, bitmaps, and others) associated with the selected process.
- **Heaps** - Shows the memory heaps created by the selected process.

**Warning:** A temporary thread will be created in the process for displaying the heaps.

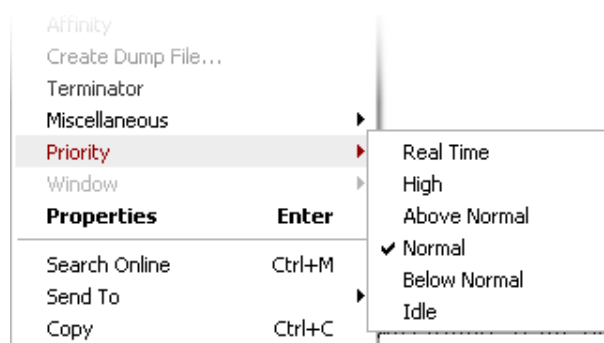
- **Inject DLL** - Enables you to select a DLL file (or any other PE image) for injecting into the selected process.

**Note:** On Windows XP, this option is only available for processes running in the same session as KillSwitch (usually processes in the same user account). On Windows Vista and above, there is no such restriction.

- **Run As** - Opens the 'Run As' dialog for executing the application associated with the process with the privileges granted to any user of the computer.
- **Run As This User** - Opens the 'Run As' dialog for executing the application associated with the process with the privileges granted to the currently logged-in user of the computer.

- **Priority** - Enables you to sets the priority for the process. The available options are:

- Real Time;
- High;
- Above Normal;
- Normal;
- Below Normal;
- Idle.

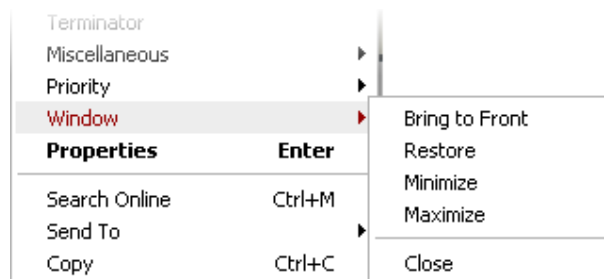


**Note:** This option is not available when multiple processes are selected.

- **Window** - Allows you to position/re-size the process' window, if one was found. If the process does not have any visible windows, the menu is disabled. The options available are:



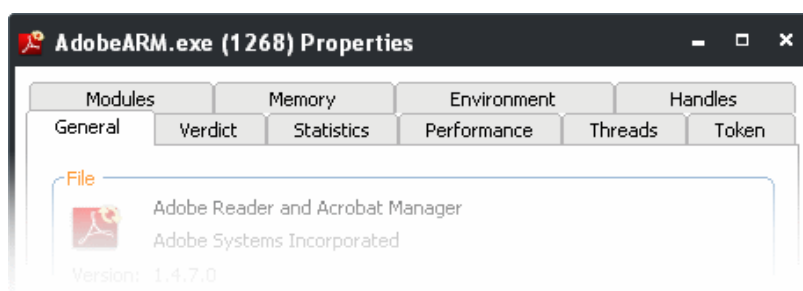
- Bring to Front;
- Restore;
- Minimize;
- Maximize;
- Close.



- **Properties** - Opens the properties dialog of the selected processes. Refer to the section **Viewing the Properties of a Process** for more details.
- **Search Online** - Opens the default web browser of your system with the search engine specified and searches for information on the process on the web. You can specify the search engine as per your choice by clicking **'Tools' > 'Options' > 'General' > 'Search Engine'**.
- **Send To** - Submits the application that has triggered the process for analysis to [virustotal.com](http://virustotal.com) or [virusscan.jotti.org](http://virusscan.jotti.org) as selected from the sub-menu. You can submit the files which you suspect to be a malware. The files will be analyzed by experts and added to white list or black list accordingly.
- **Copy** - Copies the row of the selected process from the list of processes into your clipboard.

### 3.3.1.2. Viewing Properties of a Process

To view the properties dialog, just double click on the process in the main display pane or right click on the process from the main display pane and select 'Properties' from the context sensitive menu. 'Properties' is used to cover the large amount of information that surrounds each process. Because the amount of data is so large, the 'Properties' interface is broken down into ten separate tabs, each containing important information and functionality related to the particular process.



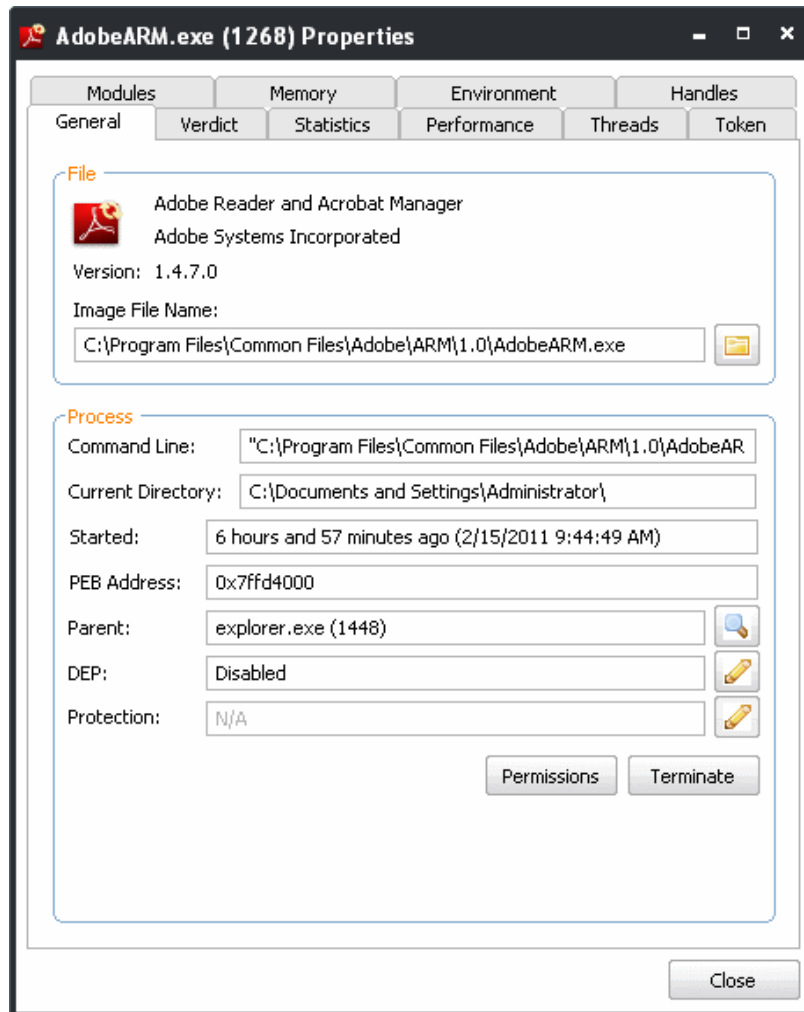
Further details are available on each tab by clicking the following links :

- **General;**
- **Verdict;**
- **Statistics;**
- **Performance;**
- **Threads;**
- **Token;**
- **Modules;**
- **Memory;**
- **Environment;**
- **Handles;**

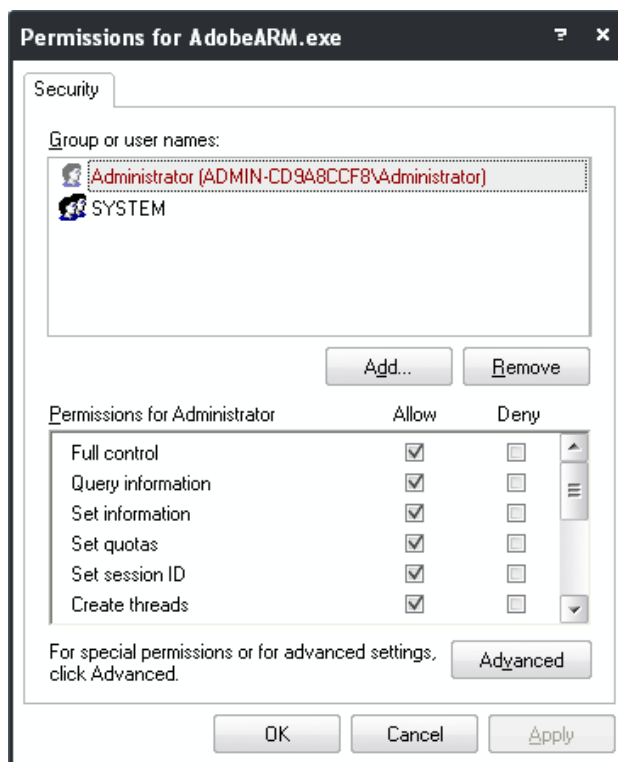
### General Properties

The 'General' tab displays the basic information about the process and its image file. You can also view/change its Data Execution Prevention (DEP) status etc You can also protect/unprotect the process if you are using Windows Vista and above.

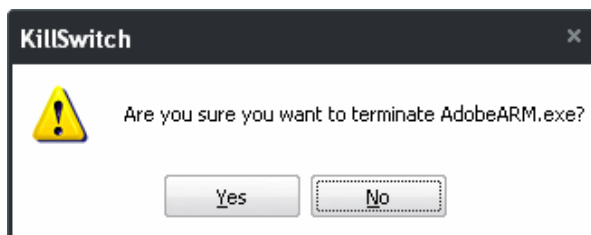




- **Permissions** - Clicking 'Permissions' enables you to configure the access rights of the application to the registered users of the computer.



- **Terminate** - Clicking 'Terminate' stops the process. You will be asked for confirmation before stopping the process.

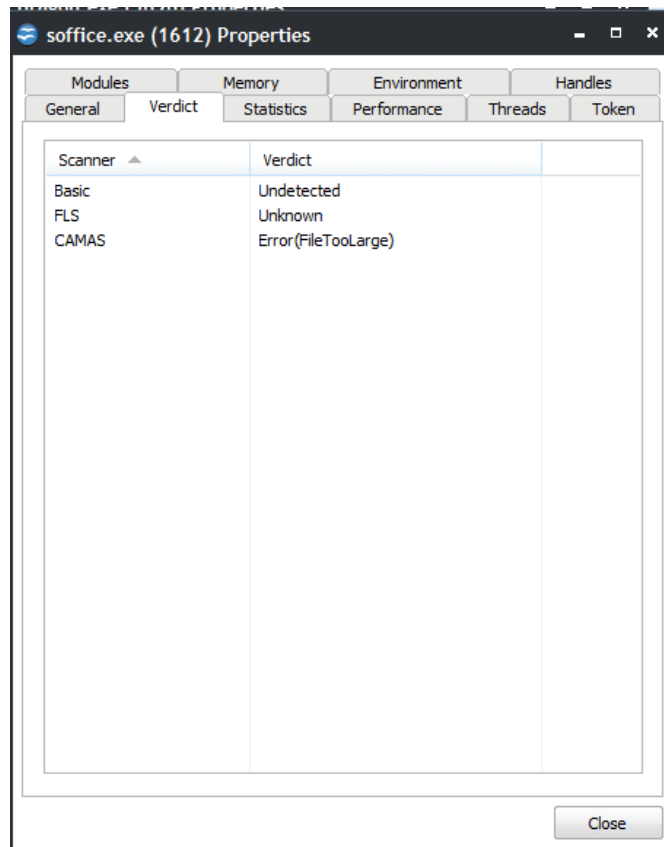


[Click here to go back to list of properties.](#)

## Verdict

The 'Verdict' tab displays list of scanning tests performed by KillSwitch on the process through its native scanner, **CAMAS** and the results pertaining to each scan.

To view the details of scan result, press Verdict tab.



See the following scan results:

Scan Result	From	Note
Basic	File scanner of local AV engine	To ensure the most accurate scan results, please update the AV database prior to running an AV scan.
FLS	Cloud based file scanner	-
	Cloud based verification of a file's digital signature	-
	Local verifier of trusted vender Local check that the creator of the file is on the trusted vendor list	Checks that the file has a digital signature. If it does, then checks this signature is in the trusted vendor list.
CAMAS	File is uploaded to Comodo Automated Malware Analysis System (CAMAS) for inspection	Use private communication protocol to send the file to CAMAS for analysis. Public CAMAS URL: <a href="http://camas.comodo.com">http://camas.comodo.com</a>

Verdict column shows the final verdict **only** according to the priorities.

The priority of scan result is following (High to low):

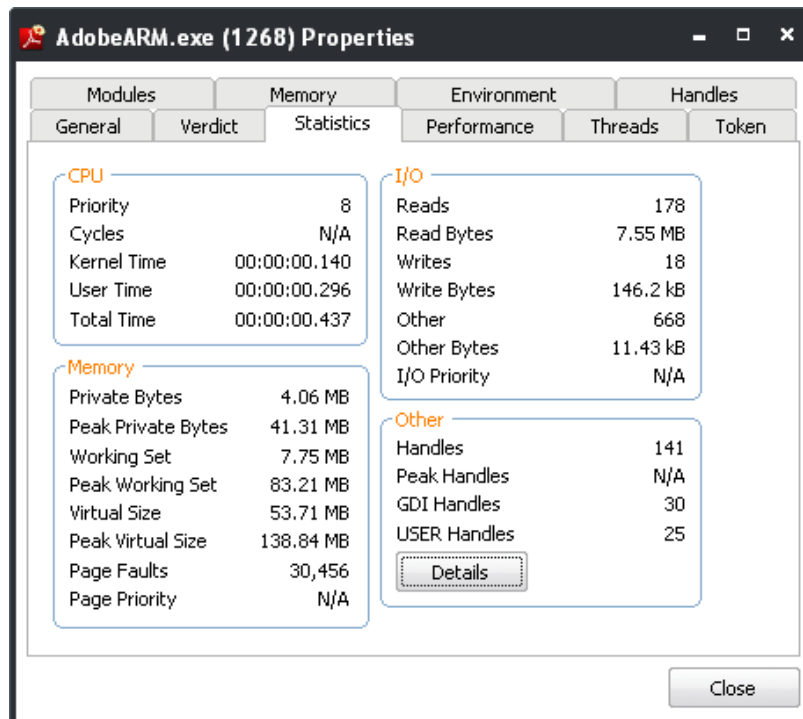
1. Basic.Malware
2. FLS.Malware

3. FLS.Safe
4. CAMAS.Detected
5. CAMAS.Malware
6. CAMAS.Suspicious
7. CAMAS.SuspiciousP
8. CAMAS.SuspiciousPP
9. FLS.Unknown
10. FLS.Absent

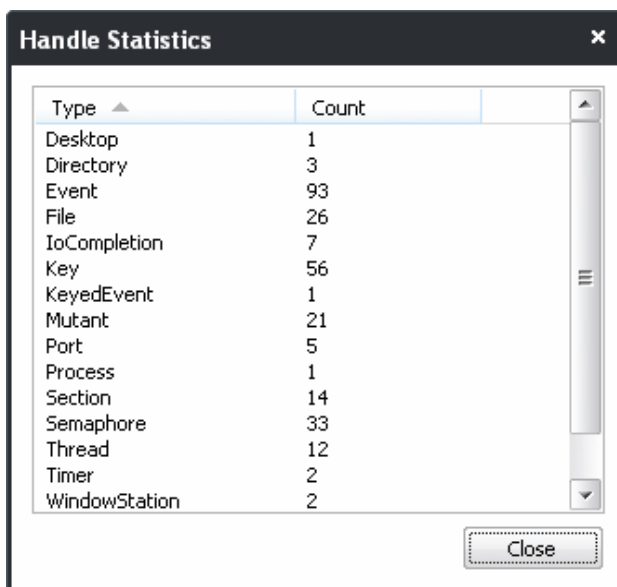
[Click here to go back to list of properties.](#)

## Statistics

The 'Statistics' tab displays the statistics and performance information like CPU usage, I/O activity, Memory usage etc. This data can help advanced users track the resource overhead of a process at a granular level.



- **Viewing Statistical Report on Handles** - Clicking Details in 'Others' area opens the 'Handle Statistics' dialog that displays a statistical report on the Handles currently running in your system.

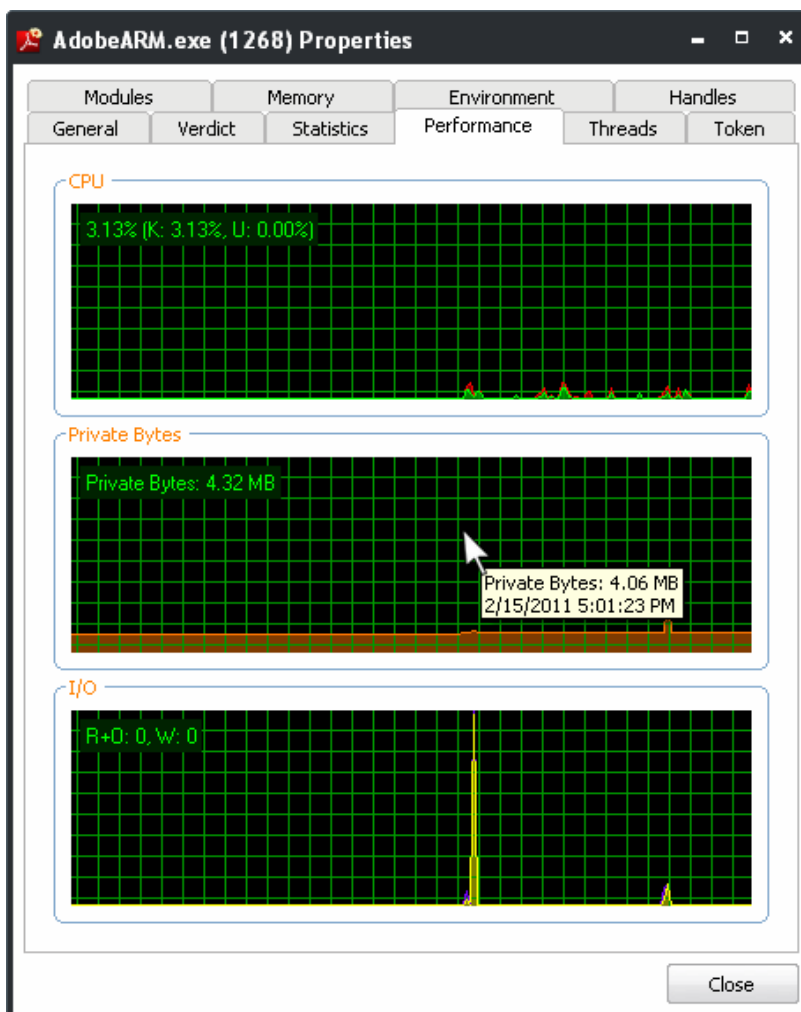


Type	Count
Desktop	1
Directory	3
Event	93
File	26
IoCompletion	7
Key	56
KeyedEvent	1
Mutant	21
Port	5
Process	1
Section	14
Semaphore	33
Thread	12
Timer	2
WindowStation	2

[Click here to go back to list of properties.](#)

## Performance

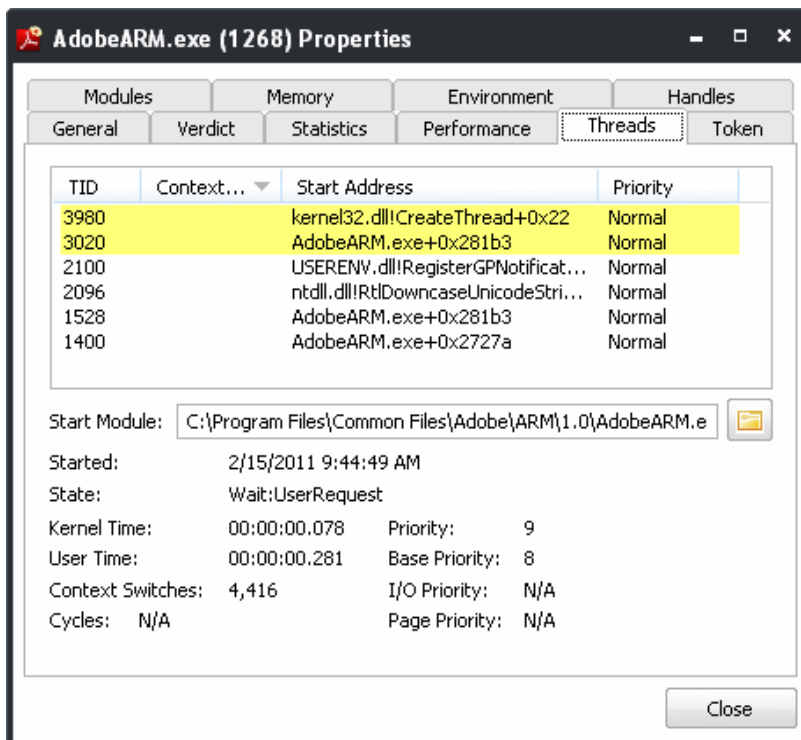
The 'Performance' tab displays three graphs relating to the process' performance - CPU Usage, Private Bytes, and I/O activity. This window helps the advanced users to track the resource overhead of a process pictorially. You can hover your mouse over the graphs to view details.



[Click here to go back to list of properties.](#)

## Threads

The 'Threads' tab displays a list of threads of the process, including their symbolic start addresses. You can click on a thread to view more information, or double-click a thread to view its call stack.

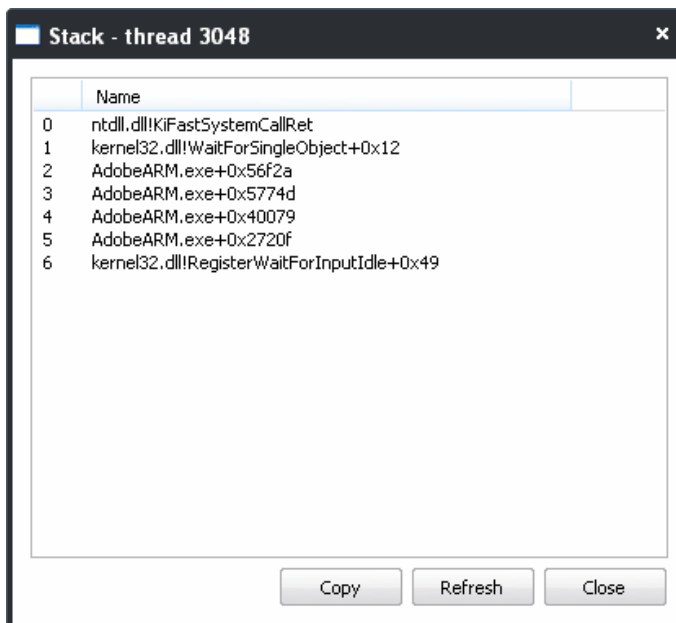


## Handling Threads

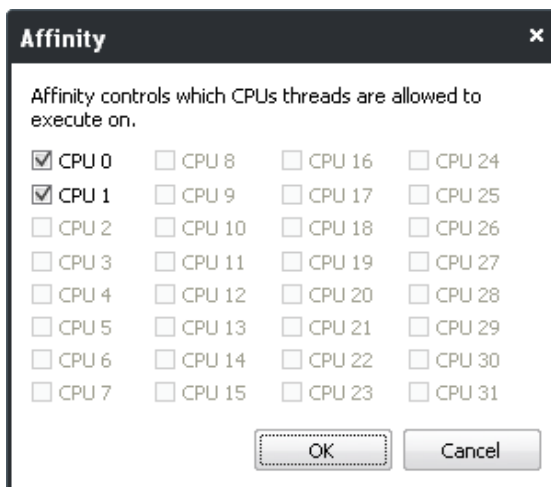
Right-clicking on a thread opens a context sensitive menu that enables you to perform various actions on the threads.



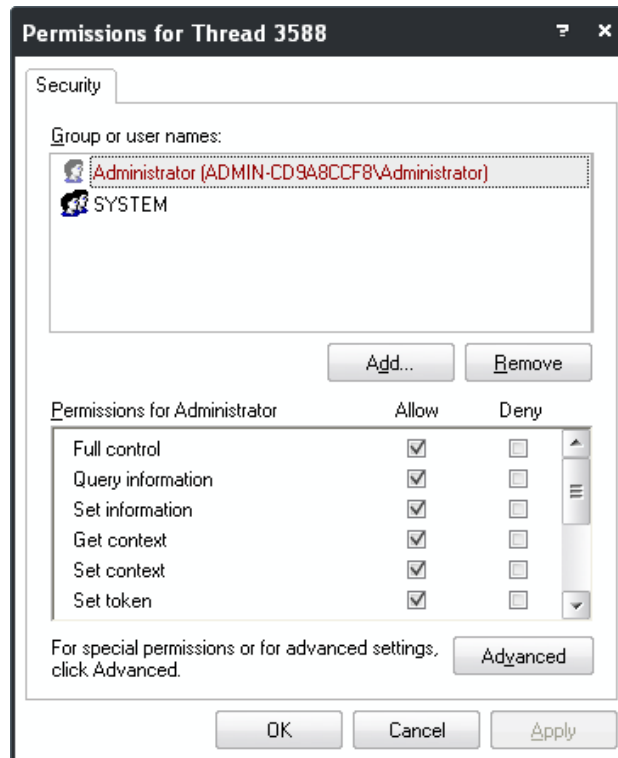
- **Inspect** - Analyzes the thread and displays a list of stacks in the thread.



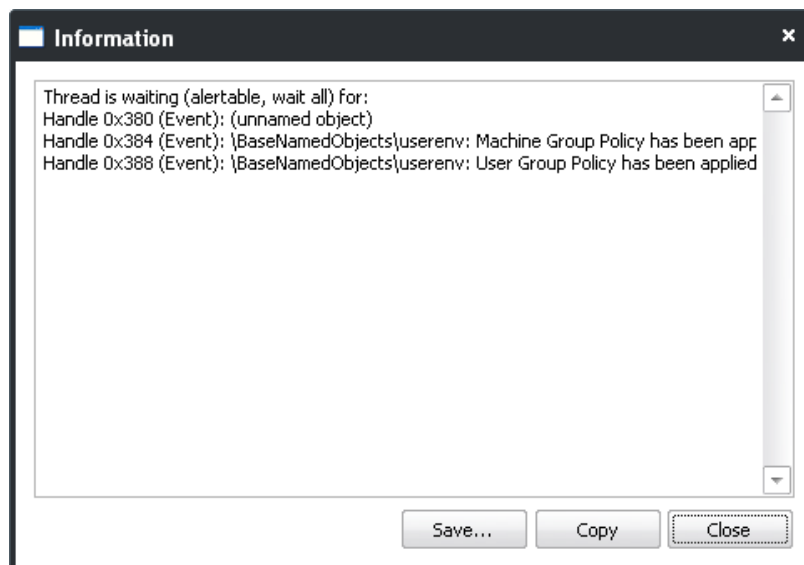
- **Terminate** - Stops the selected thread. You will be asked for confirmation before terminating the thread.
- **Suspend** - Temporarily stops the selected thread. You can resume the thread by clicking 'Resume' in the context sensitive menu.
- **Resume** - Resumes selected (suspended) thread.
- **Affinity** - Enables you to view and modify the selected thread's processor affinity (the CPU to which the thread is allocated) in a symmetric multiprocessing operating system e.g. to reduce cache related problems.



- Refer to the **Background note** in the section 'Stopping, Starting and Handling the Processes' for more details.
- **Permissions** - Opens the 'Permissions' dialog that enables you to configure the access rights for the thread to the registered users of the computer.

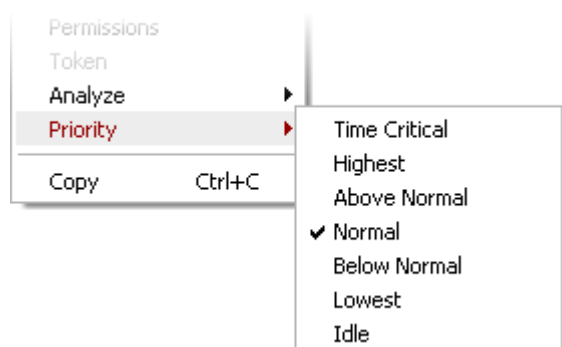


- **Token** - Displays a list of access tokens of the selected thread.
- **Analyze** - Analyzes the selected thread to check waiting status and provides a detailed report.



- **Priority** - Enables you to sets the priority for the selected thread. The available options are:

- Time Critical;
- Highest;
- Above Normal;
- Normal;
- Below Normal;
- Lowest;
- Idle.



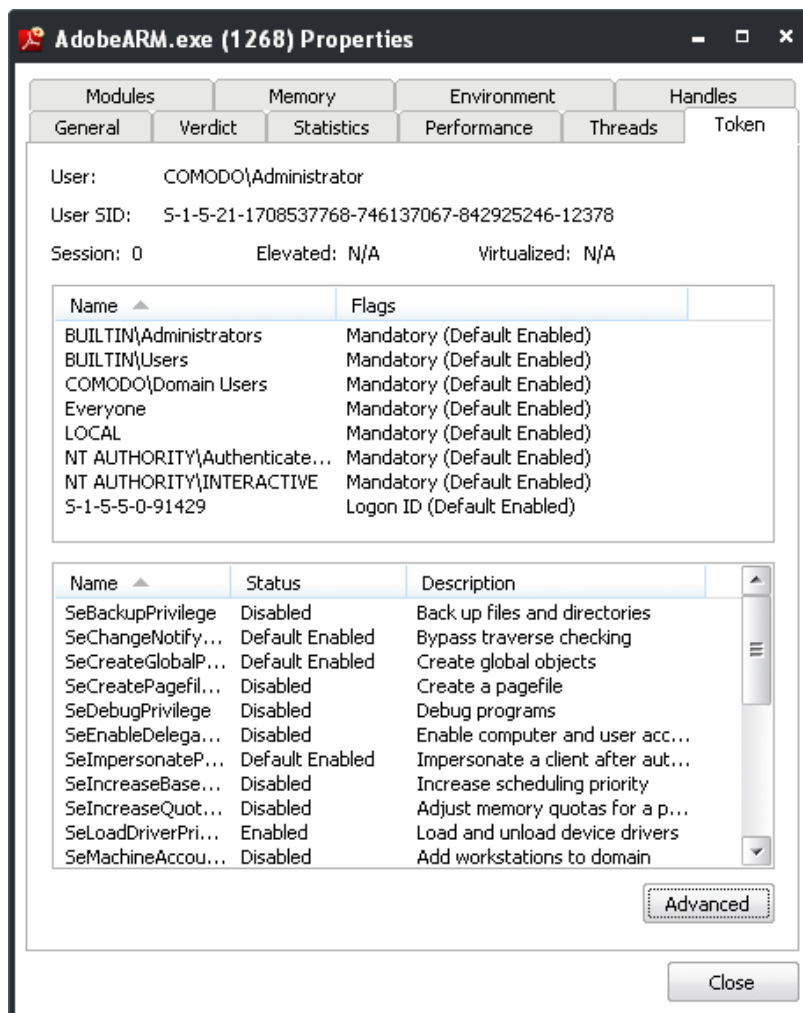


- **Copy** - Copies the row of the selected thread from the list of threads into your clipboard.

[Click here to go back to list of properties.](#)

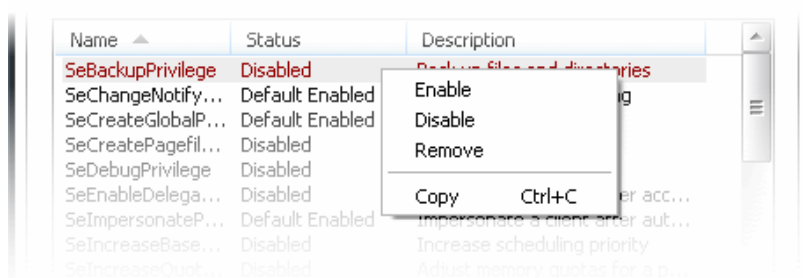
## Token

The Token tab displays the primary token of the process. The token of a process is an object which describes security attributes such as the user, groups and privileges.



## Enabling and Disabling Privileges to Tokens

Right-clicking on the token privileges displayed in the bottom pane opens a context sensitive menu that enables you to switch between enabled/disabled states of them.

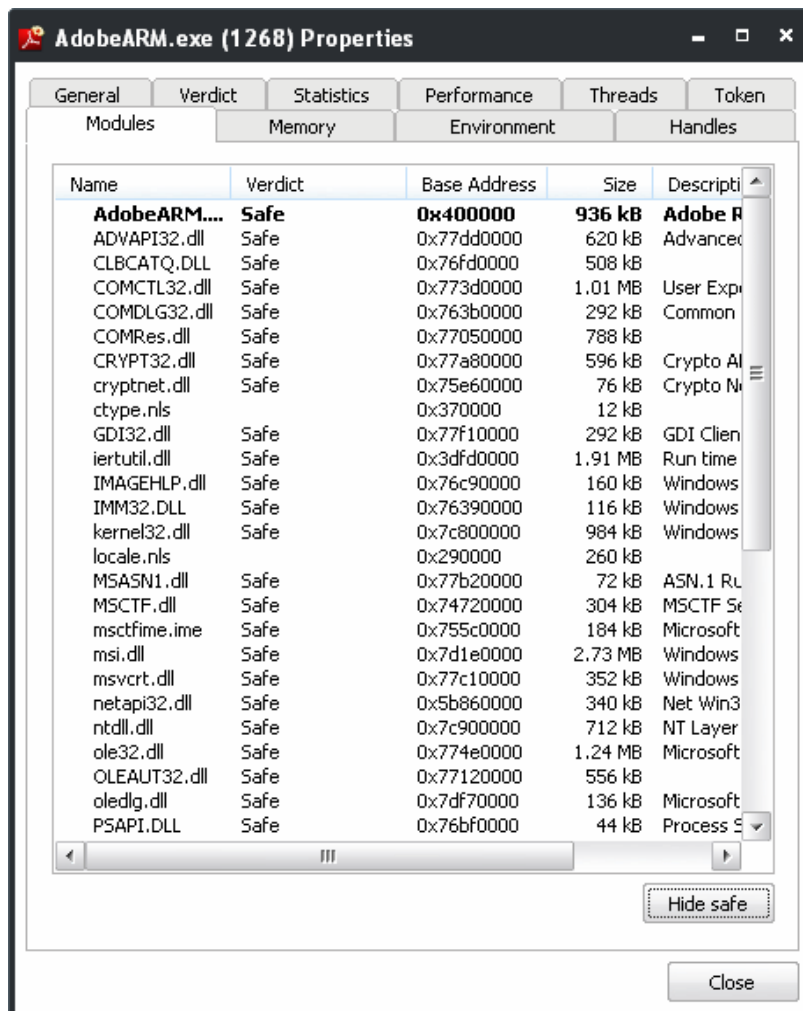


- **Enable** - Enables the selected privilege to the token.
- **Disable** - Disables the selected privilege to the token
- **Remove** - Removes the selected privilege for the token
- **Copy** - Copies the selected row to your clip-board.
- Clicking the 'Advanced' button opens the Token Properties dialog.

[Click here to go back to list of properties.](#)

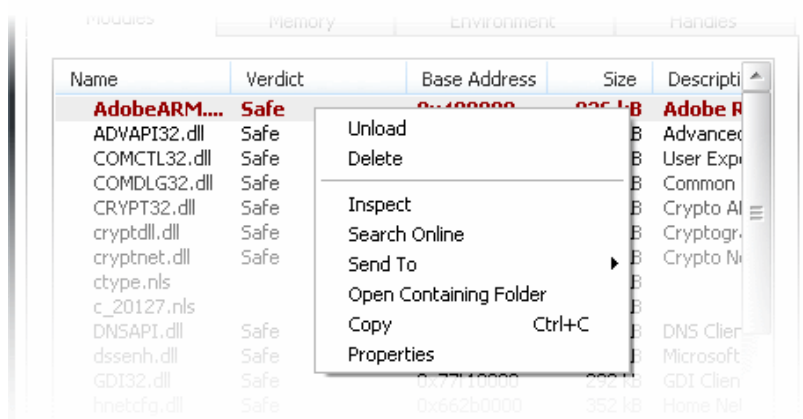
## Modules

The 'Modules' tab displays the modules loaded by the process. Modules are the dynamic link library (DLL) files that are loaded to the system memory by the selected process.



## Handling the Modules

Right-clicking on a module listed opens a context sensitive menu that enables you to perform various actions like unloading the module from the memory.

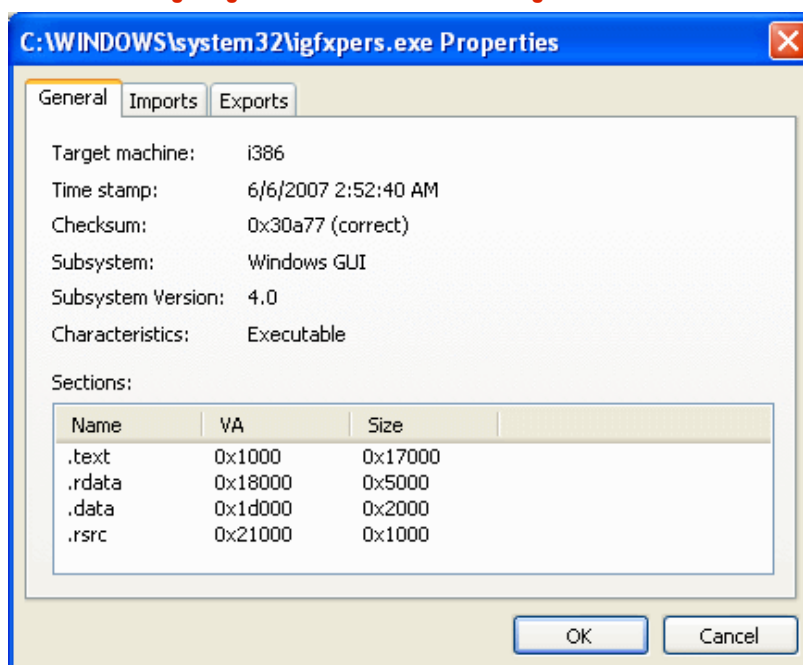


- **Unload** - Unloads the selected module from the system memory.
- **Delete** - Removes the selected module from your computer. You will be asked for confirmation before deleting the

module.

**Warning:** Deleting some critical modules of an application may render the application unusable.

- **Inspect** - Opens the Import and Export table of the module in the PE viewer. You can specify the PE viewer to display the properties dialog as per your choice in the PE Viewer field under the General tab of 'Options' dialog. Refer to '**Tools**' > '**Configuring KillSwitch**' > '**General Settings**' for more details.

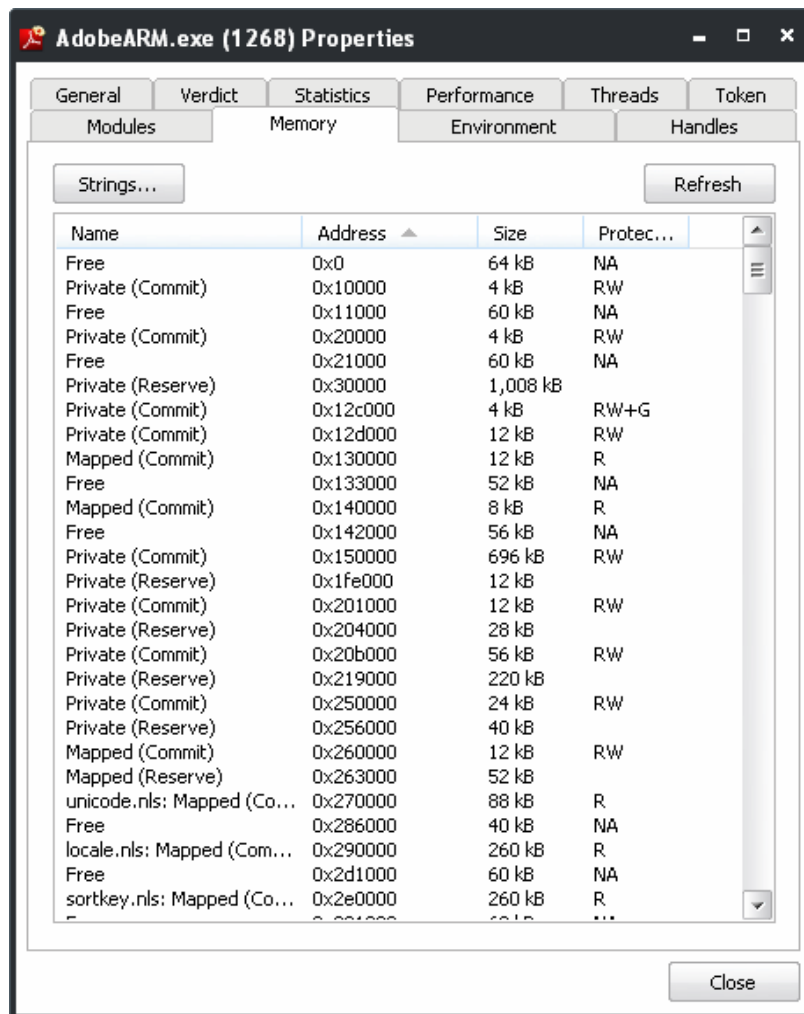


- **Search Online** - Opens the default web browser of your system with the search engine specified and searches for information on the module on the web. You can specify the search engine as per your choice by clicking '**Tools**' > '**Options**' > '**General**' > '**Search Engine**'.
- **Send To** - Submits the module for analysis to virustotal.com or virusscan.jotti.org as selected from the sub-menu. You can submit the files which you suspect to be a malware. The files will be analyzed by experts and added to white list or black list accordingly.
- **Open Containing Folder** - Opens the folder in which the module is stored, in Windows Explorer window.
- **Copy** - Copies the row of the selected module from the list of module into your clipboard.
- **Properties** - Opens the 'Properties' dialog of the module.
- Clicking 'Hide Safe' button conceals the processes identified as safe bt KillSwitch and displays only the unsafe processes

[Click here to go back to list of properties.](#)

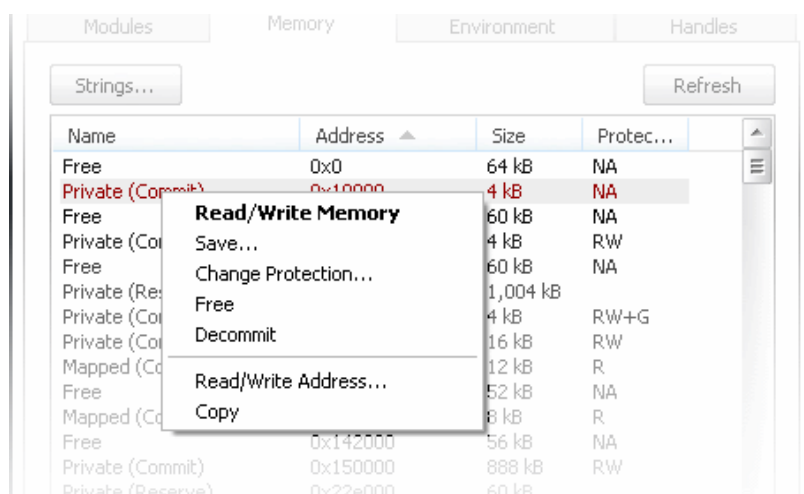
## Memory

The 'Memory' tab displays the virtual memory regions allocated to the process.

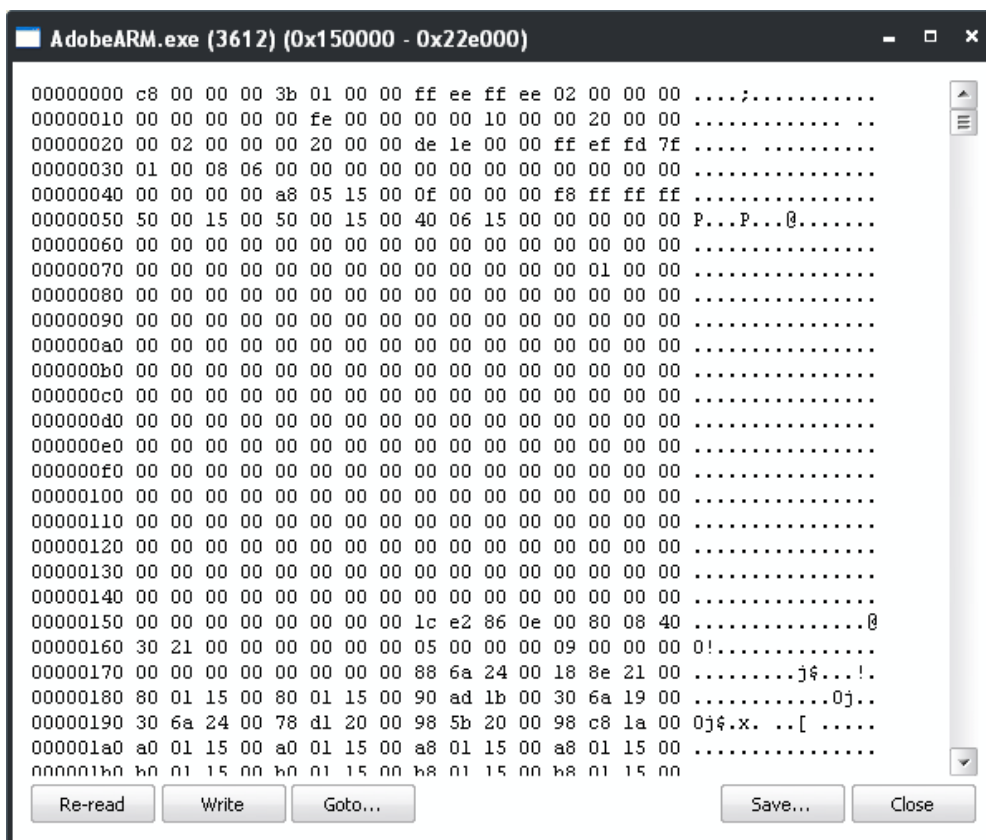


## View, Read/Write Memory Regions

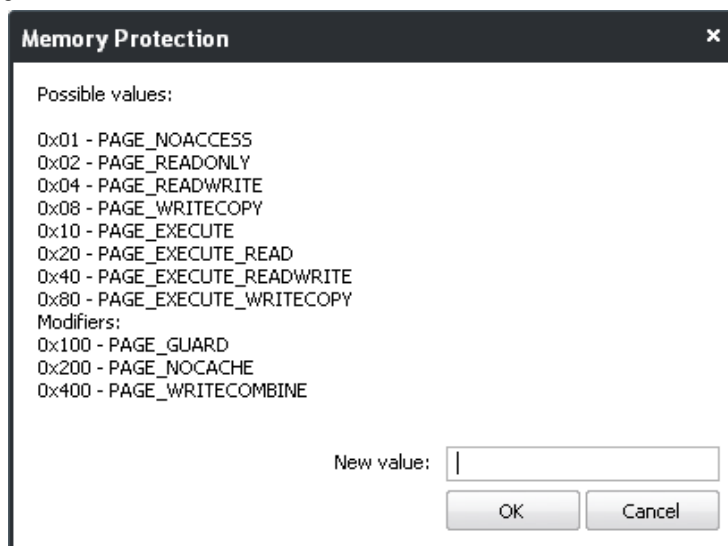
Right-clicking on a memory region opens a context sensitive menu that enables you to perform various actions like Read, Write data at required locations, and to perform other actions.



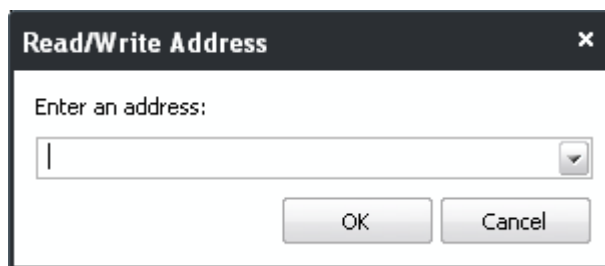
- **Read/Write Memory** - Opens the window that shows the bytes of data written in the memory locations of the virtual memory regions of the module. This window also enables you to alter the values at required memory addresses.



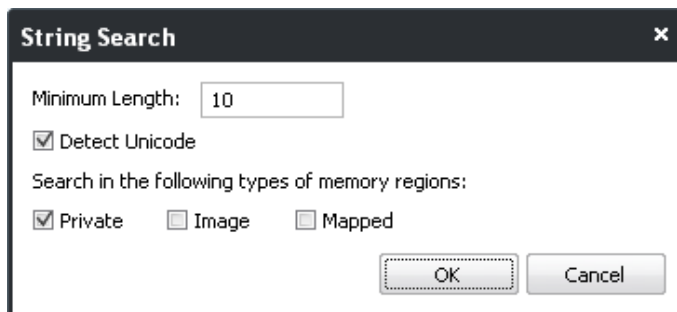
- **Save** - Saves the selected memory region as a binary file.
- **Change Protection** - Opens 'Memory Protection' dialog that enables you to configure the protection status of the memory region.



- **Free** - Unmaps the memory region and makes it free for use by other modules. You will be asked for confirmation before unmapping.
- **Decommit** - Uncommits the memory region from the module, so that the memory region can be used for other modules.
- **Read/Write Address** - Enables you to read the bytes of data from specific addresses within the selected memory region.



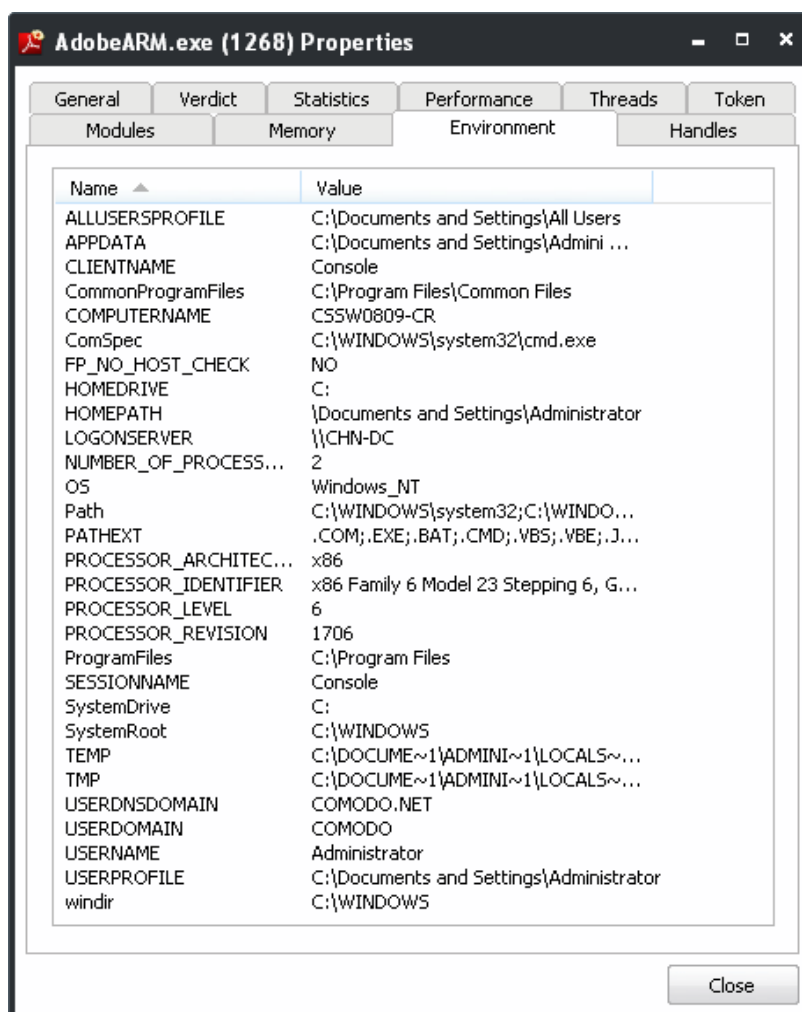
- **Copy** - Copies the row of the selected memory region from the list into your clipboard.
- Clicking the **'Strings...'** button enables you to start a scan for search for strings of specified size within the memory regions of the processes.



[Click here to go back to list of properties.](#)

## Environment

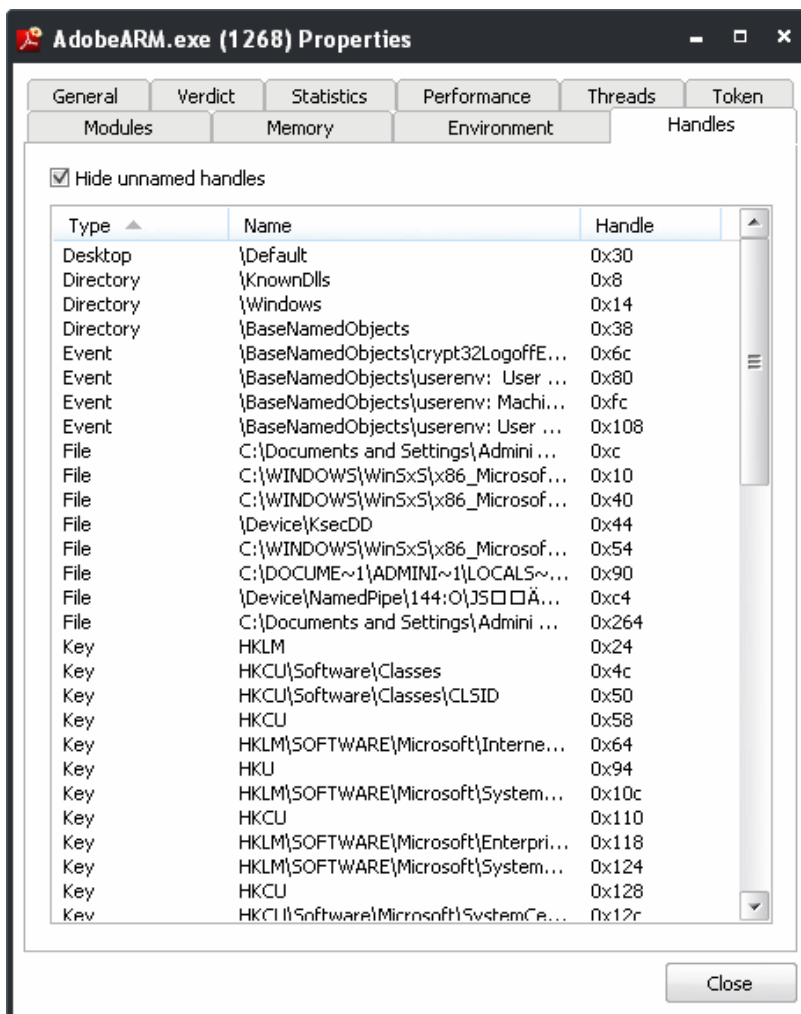
The 'Environment' tab displays the process' environment variables, which are the variables accessible to process describing the operating system environment. Environment variables are normally inherited by child processes.



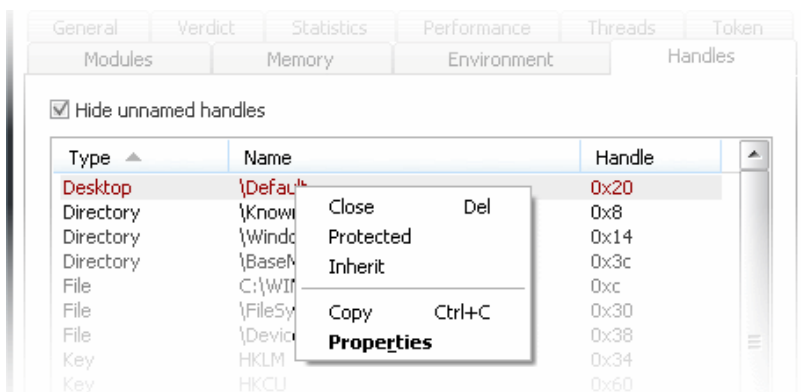
[Click here to go back to list of properties.](#)

## Handles

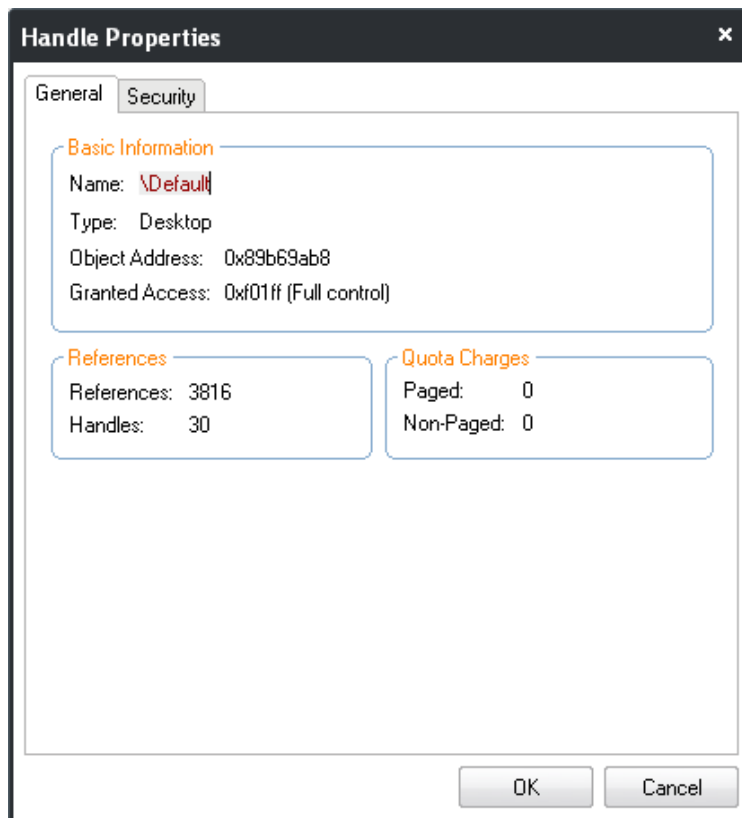
The 'Handles' tab displays the process' handles - resources it has opened. A handle refers to the value used to uniquely identify a resource, such as a file or a registry key, accessed by the process or the application.



- Right-clicking on an handle opens a context sensitive menu that enables to close view the properties of the handle.



- **Close** - Closes the Handle. Closing a process handle does not terminate the associated process or remove the process object.
- **Protected** - Protects the handle from changes
- **Inherit** - Enables the child processes of the Process associated with the handle to inherit it, so that the child processes will have the same value and access privileges for the handle as those of the parent process.
- **Copy** - Copies the row to your clip-board.
- **Properties** - Opens the 'Properties' dialog of the Handle



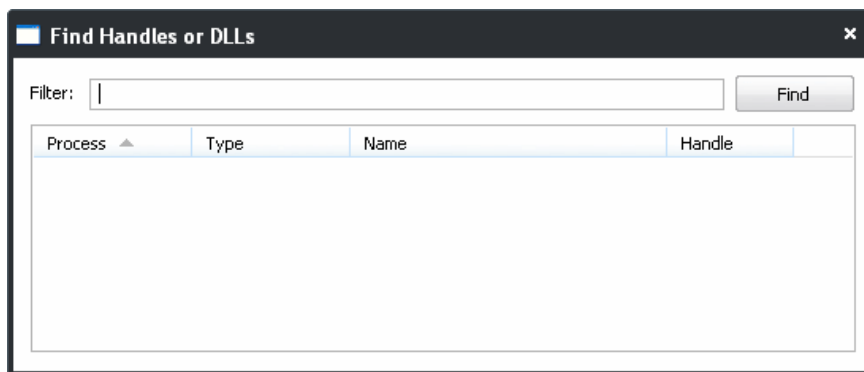
[Click here to go back to list of properties.](#)

### 3.3.1.3. Searching for Handles or DLLs

KillSwitch contains a built-in search tool to find specific handles, DLLs and mapped files of the currently running processes by entering their names.

**To search for a specific handles, DLLs and mapped files**

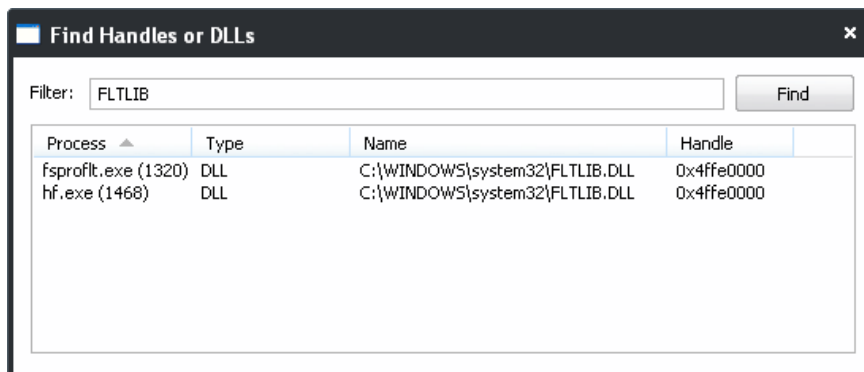
- Click 'KillSwitch' > 'Find Handles or DLLs' or click the  icon from the shortcut icons area. The 'Find Handles or DLLs' dialog will open.



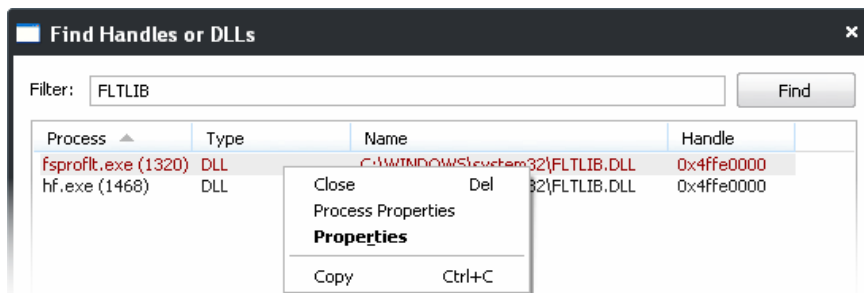
- Enter the name of the object you wish to search, in the Filter text box. The entered string can be a sub-string of the object name. The search key is not case-sensitive
- Click 'Find'.

The results window will contain the process(es) associated with the object, the type of the object and its handle as a table.

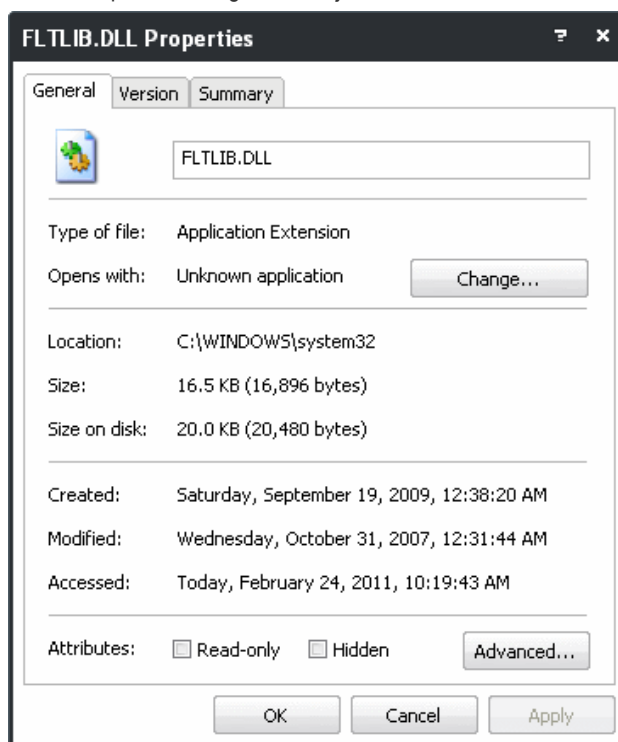




- Right clicking on the results open a context sensitive menu, that enables you to close the Handle and view the properties of the Handle.





- **Close** - Closes the selected Object. This option only allows you only to close the handles. Closing a process handle does not terminate the associated process or remove the process object. If you wish to "unlock" a file which is loaded as a DLL or mapped, you must open the Properties dialog for the relevant Process using the Process Properties option from the same menu, select the **Modules** tab, right-click the relevant item, and select 'Unload'.
- **Process Properties** - Opens the Properties dialog of the associated Process. Refer to **Viewing Properties of a Process** for more details.
- **Properties** - Opens the Properties dialog of the Object.

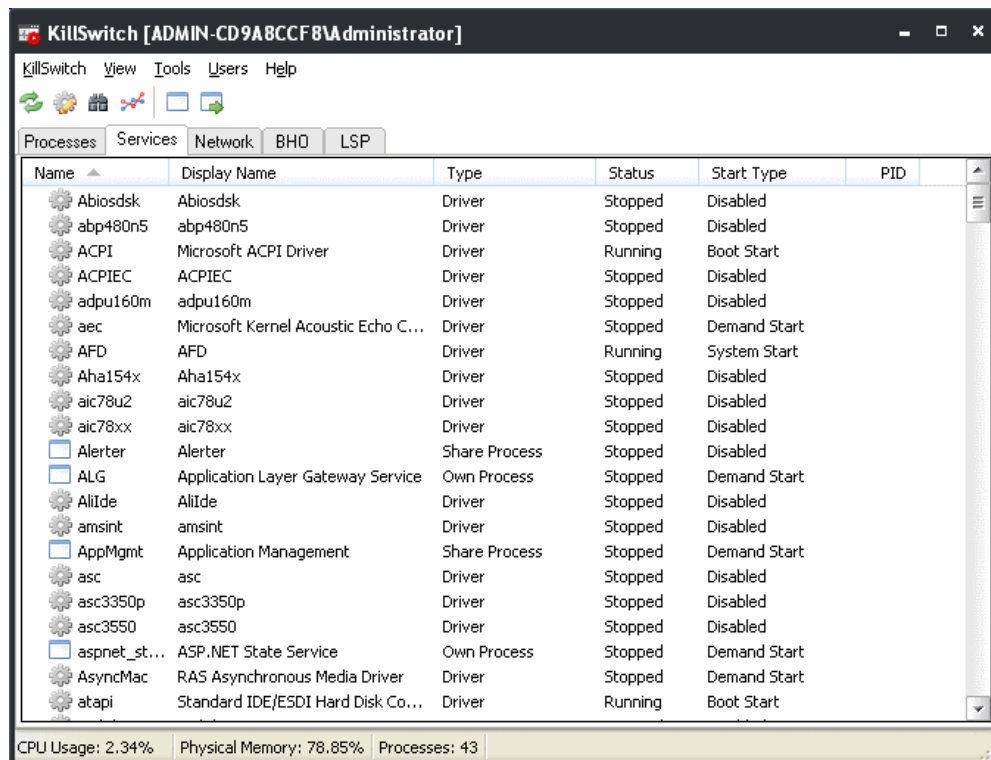


- **Copy** - Copies the row to your clip-board.

## 3.3.2. Services

The 'Services' tab displays all the Windows Services/drivers loaded in your system as a table in the main display pane. It also allows your to start, stop, restart or delete them as required.

- The services associated with the processes/applications are indicated by  icon.
- The drivers are are indicated by  icon.
- Right clicking on a Service opens a context sensitive menu that enables you start, stop, restart or delete it. You can even select multiple services (by holding the 'Ctrl' key while selecting the services) to execute these actions.



**Services Table - Descriptions of Columns**

Column	Description
Name	Displays the name of the processes. Clicking on the column header sorts the entries in ascending or descending alphabetical order of the names.
Display Name	Shows the name by which the service is indicated in the Windows System Configuration Utility. Clicking on the column header sorts the entries in ascending or descending alphabetical order of the display names.
Type	Displays the type of the service, viz. shared processes (in svchost.exe instances), separate processes (processes on their own), or drivers. Clicking on the column header sorts the entries in ascending or descending order of the types.
Status	Displays the status of the service, i.e. whether it is running, stopped or disabled. Clicking on the column header sorts the entries in based on their status.
Start Type	Indicates how the service can be started, i.e. whether it automatically starts with Windows, started on demand or disabled. Clicking on the column header sorts the entries in based on their start types.
PID	Displays the Process Identification number of the process associated to the service. Only the PIDs of the currently running services are displayed. Clicking on the column header enables sorting the entries in ascending or descending order of the PID numbers.

### 3.3.2.1. Stopping, Starting and Deleting the Services

The 'Services' tab allows you to start, stop and delete the services, by right clicking on the services and selecting the option from the context sensitive menu.

- Right click on a service to open the context sensitive menu.



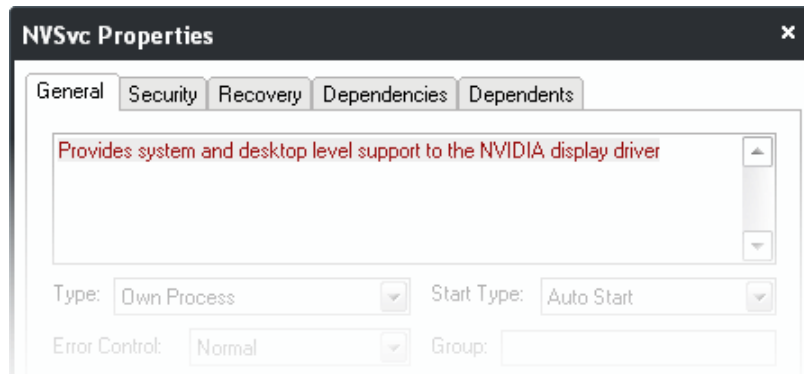
- **Go to Process** - Switches the display to the Processes tab and highlights the process associated with the service. This is useful when you want to terminate or suspend the process associated with the service.
- **Start** - Starts the selected service. This option is available only for the services with 'Stopped' status.
- **Continue** - Resumes the suspended/paused service. This option is available only for the services with 'Paused' status.
- **Pause** - Suspends the running service. This option is available only for the services with 'Running' status.
- **Stop** - Halts the running service. This option is available only for the services with 'Running' status.
- **Restart** - Restarts the running service. This option is available only for the services with 'Running' status.
- **Delete** - Deletes the selected (running, stopped, paused or disabled) service(s) from the disk. KillSwitch can delete any service, including ones protected by rootkits or security software. You will be asked for confirmation before deleting a service.

**Warning:** Deleting a critical service may render your computer unusable. Use this option only if you are an advanced user with thorough knowledge on services.

- **Copy** - Copies the row of the selected service(s) from the list of services into your clipboard.
- **Properties** - Opens the properties dialog of the selected service. Refer to the section [Viewing the Properties of a Service](#) for more details.

### 3.3.2.2. Viewing the Properties of a Service

To view the properties dialog, just double click on the service or right click on the service from the main display pane and select 'Properties' from the context sensitive menu. 'Properties' is used to cover the large amount of information that surrounds each service. Because the amount of data is so large, the 'Properties' interface is broken down into five separate tabs, each containing important information and functionality related to the particular process.

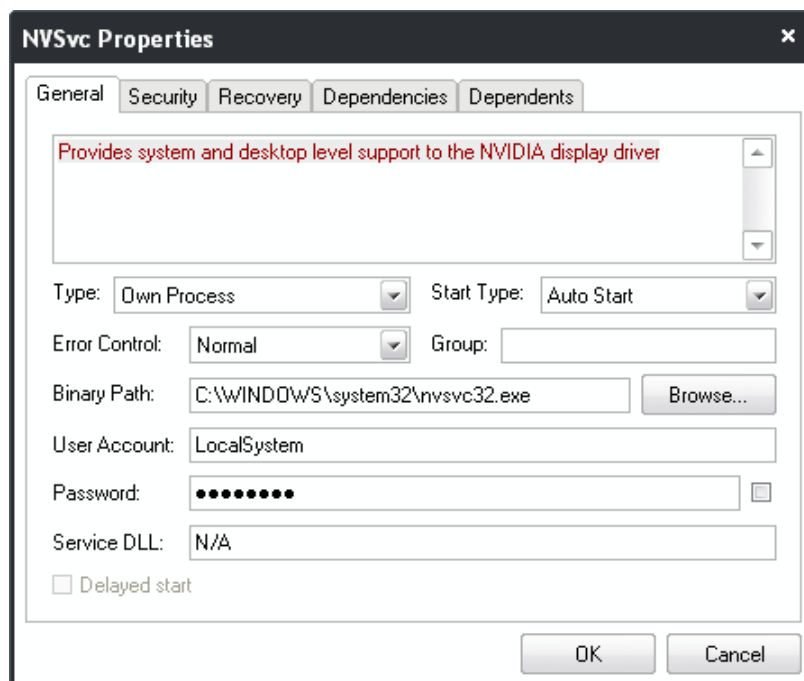


Further details are available on each tab by clicking the following links:

- **General;**
- **Security;**
- **Recovery;**
- **Dependencies;**
- **Dependents;**

## General Properties

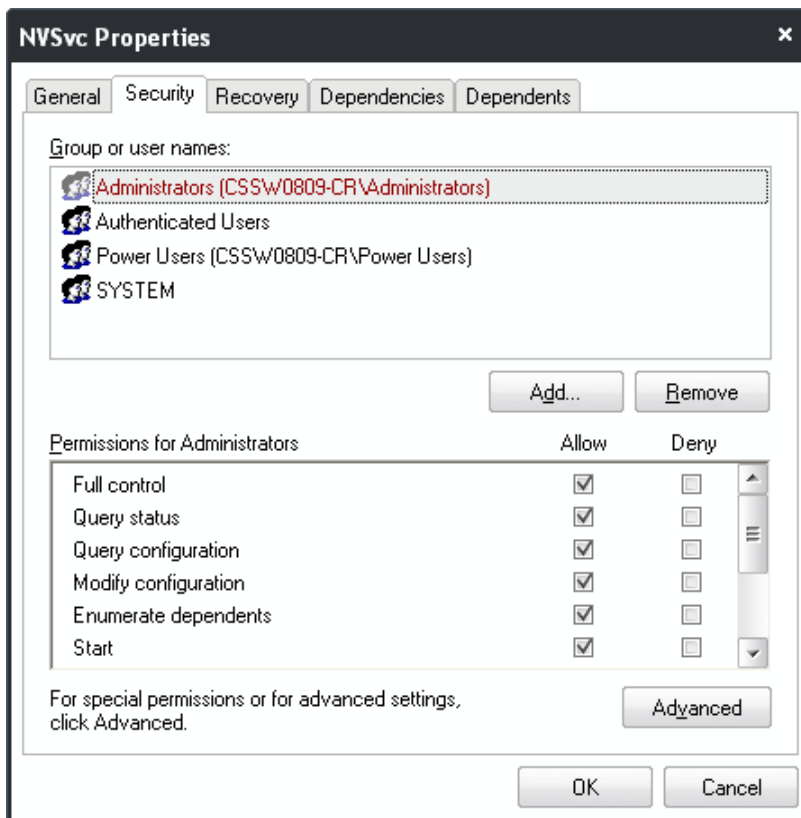
The General tab displays the basic information about the service and its type. You can also view/change its type, start type, Error Control type, Group, change the binary or executable file associated with the service from this interface.



[Click here to go back to list of properties.](#)

## Security

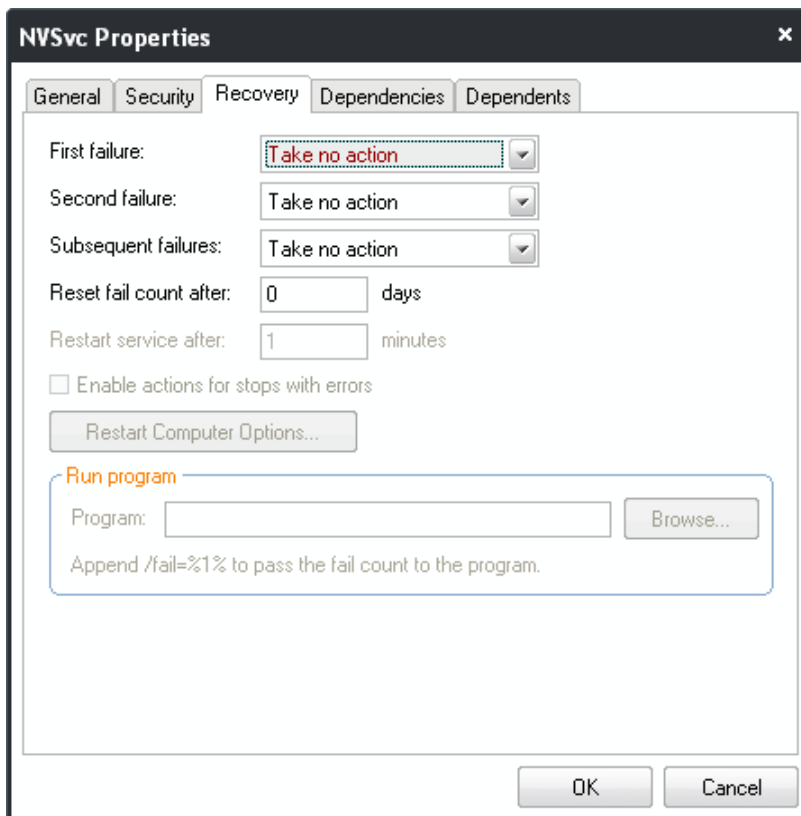
The 'Security' tab enables you to view and change the permissions granted to different users/user groups of your computer and other users/user groups on your network to access this service.



[Click here to go back to list of properties.](#)

## Recovery

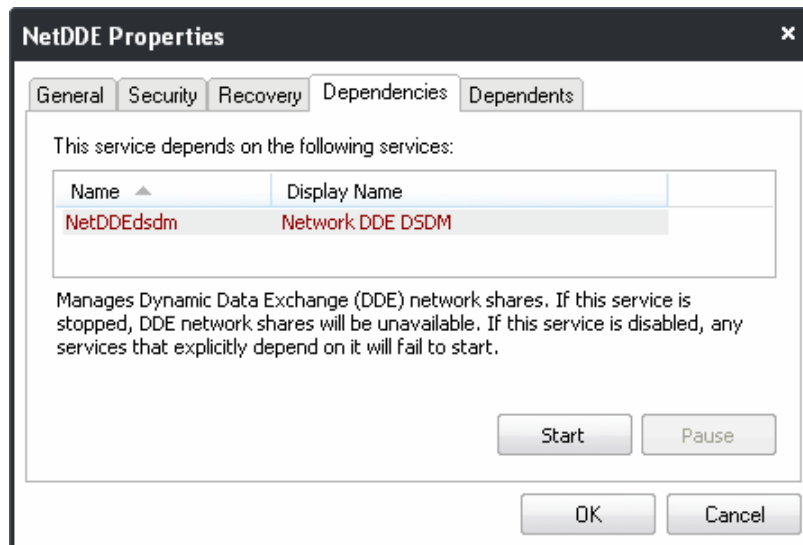
The 'Recovery' tab enables you for granular configuration for restarting the service in case of failures.



[Click here to go back to list of properties.](#)

## Dependencies

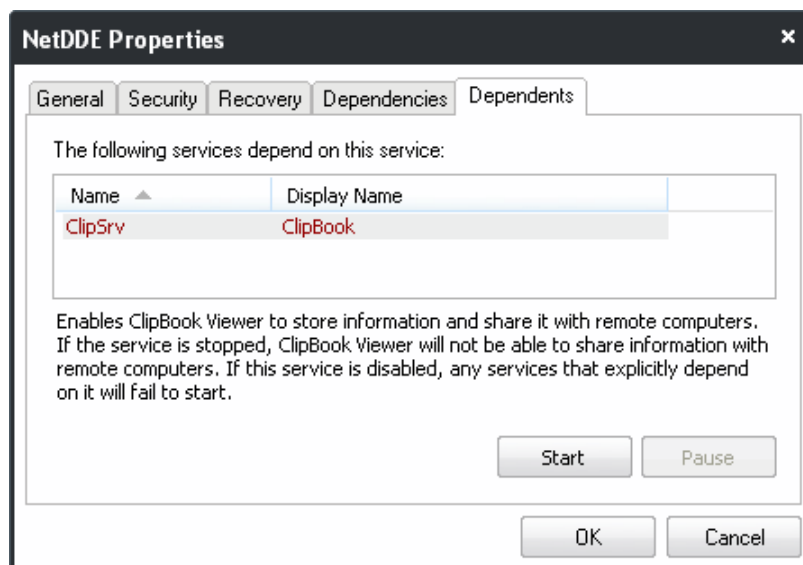
The 'Dependencies' tab shows a list of other services, upon which the selected service depends. Also you can start or pause the listed services from this interface.



[Click here to go back to list of properties.](#)

## Dependents

The 'Dependents' tab shows a list of other services, which the depend on selected service. Also you can start or pause the listed services from this interface.

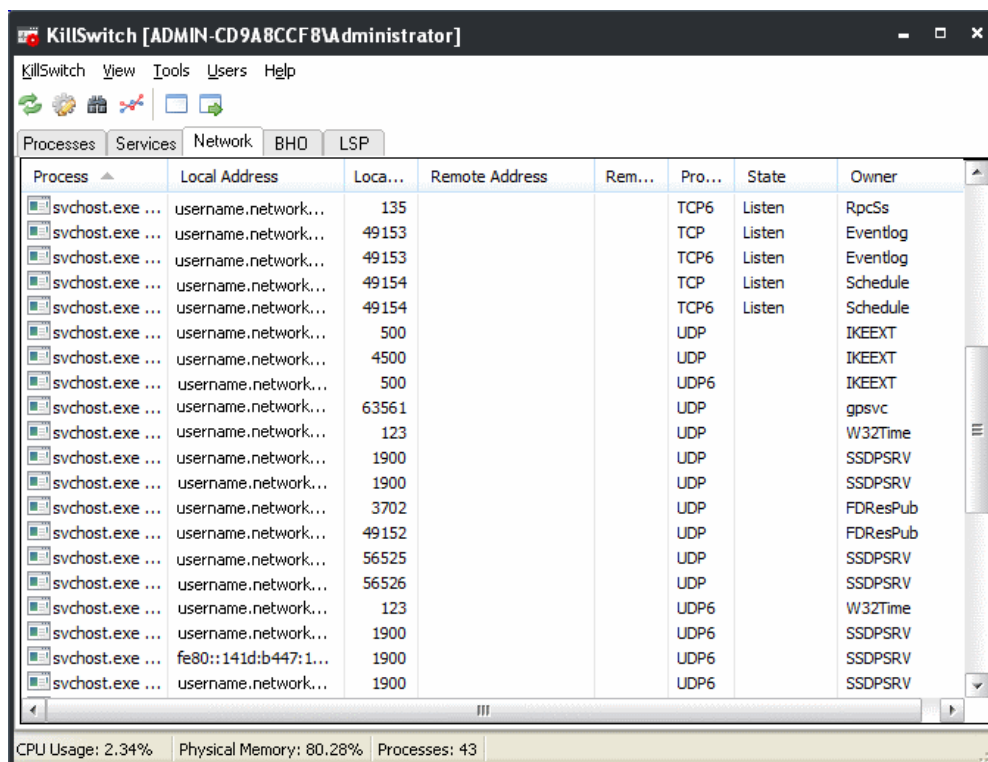


[Click here to go back to list of properties.](#)

## 3.3.3. Network Connections

The 'Network' tab displays all the network connections that are currently running in your system as a table in the main display pane.

- The new connections that are started and the connections that are stopped are highlighted.
- Right clicking on a connection opens a context sensitive menu that enables you to view the process associated with the connection, ping the remote host, trace the route to the remote host, perform Whois analysis and close the connection.



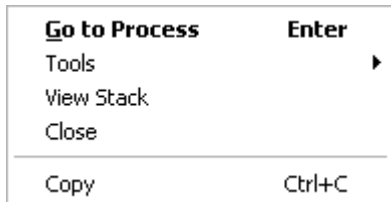
**Network Connections Table - Descriptions of Columns**

Column	Description
Process	Displays the process associated with the connection. Clicking on the column header sorts the entries in ascending or descending alphabetical order of the process names.
Local Address	Shows the local address of the connection. Clicking on the column header sorts the entries in ascending or descending numerical/alphabetical order of the addresses. <b>Note:</b> The host names are displayed only if the option ' <b>Resolve addresses for network connections</b> ' is enabled under the ' <b>Advanced</b> ' tab of ' <b>Tools</b> ' > ' <b>Options</b> ' dialog. Else only the IP addresses are displayed.
Local Port	Displays the local port number through which the connection is established. Clicking on the column header sorts the entries in ascending or descending order of the port numbers.
Remote Address	Shows the address of the remote host of the connection. Clicking on the column header sorts the entries in ascending or descending numerical/alphabetical order of the addresses. <b>Note:</b> The host names are displayed only if the option ' <b>Resolve addresses for network connections</b> ' is enabled under the ' <b>Advanced</b> ' tab of ' <b>Tools</b> ' > ' <b>Options</b> ' dialog. Else only the IP addresses are displayed.
Remote Port	Displays the port number of the remote host through which the connection is established. Clicking on the column header sorts the entries in ascending or descending order of the port numbers.
Protocol	Shows the connection protocol. Clicking on the column header sorts the entries in based on the protocols.
State	Shows the status of the connection. Clicking on the column header sorts the entries in based on the status of each connection.
Owner	Shows the service associated with the network connection. Clicking on the column header sorts the entries in based on the alphabetical order of the owner names. <b>Note:</b> The owner information is displayed only in Windows Vista, Windows 7 and Windows 2008.

## 3.3.3.1. Inspecting and Closing Network Connections

The 'Network' tab allows you to inspect a connection for trouble shooting and closing a connection if required, by right clicking on the connection and selecting the option from the context sensitive menu.

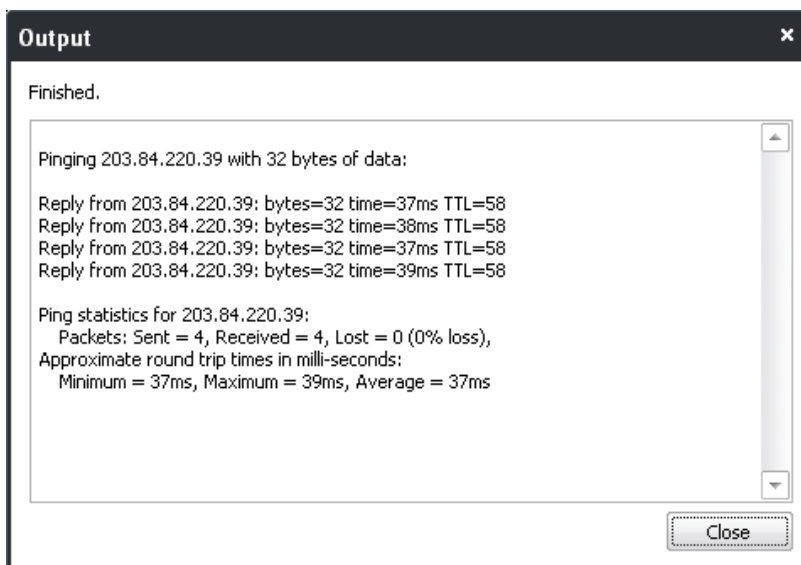
- Right click on a network connection to open the context sensitive menu.



- **Go to Process** - Switches the display to the **Processes** tab and highlights the process associated with the connection. This is useful when you want to terminate or suspend the process associated with the connection.
- **Tools** - Contains tools to inspect the connection with the remote host. This is useful for troubleshooting purposes.

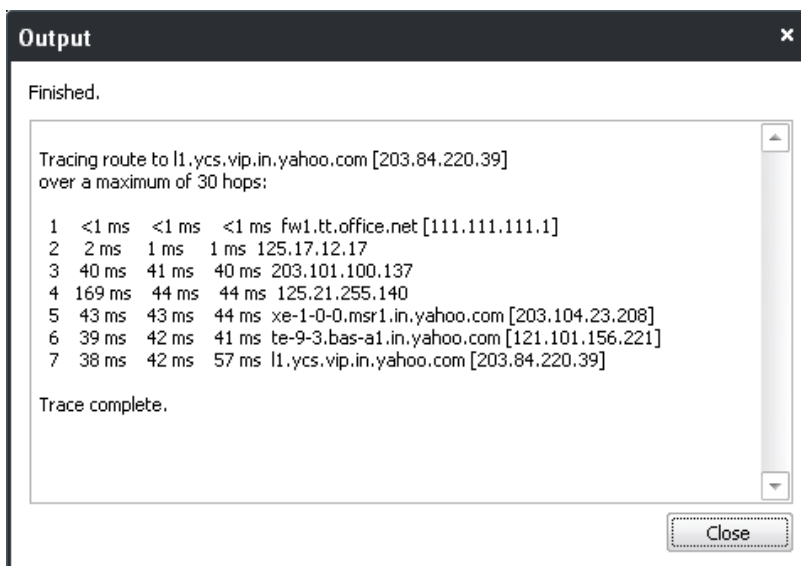


- **Ping** - Pings the remote host by sending Internet Control Message Protocol (ICMP) echo request packets to the remote host and provides the results as the round trip time, to analyze the ability to reach the remote host.

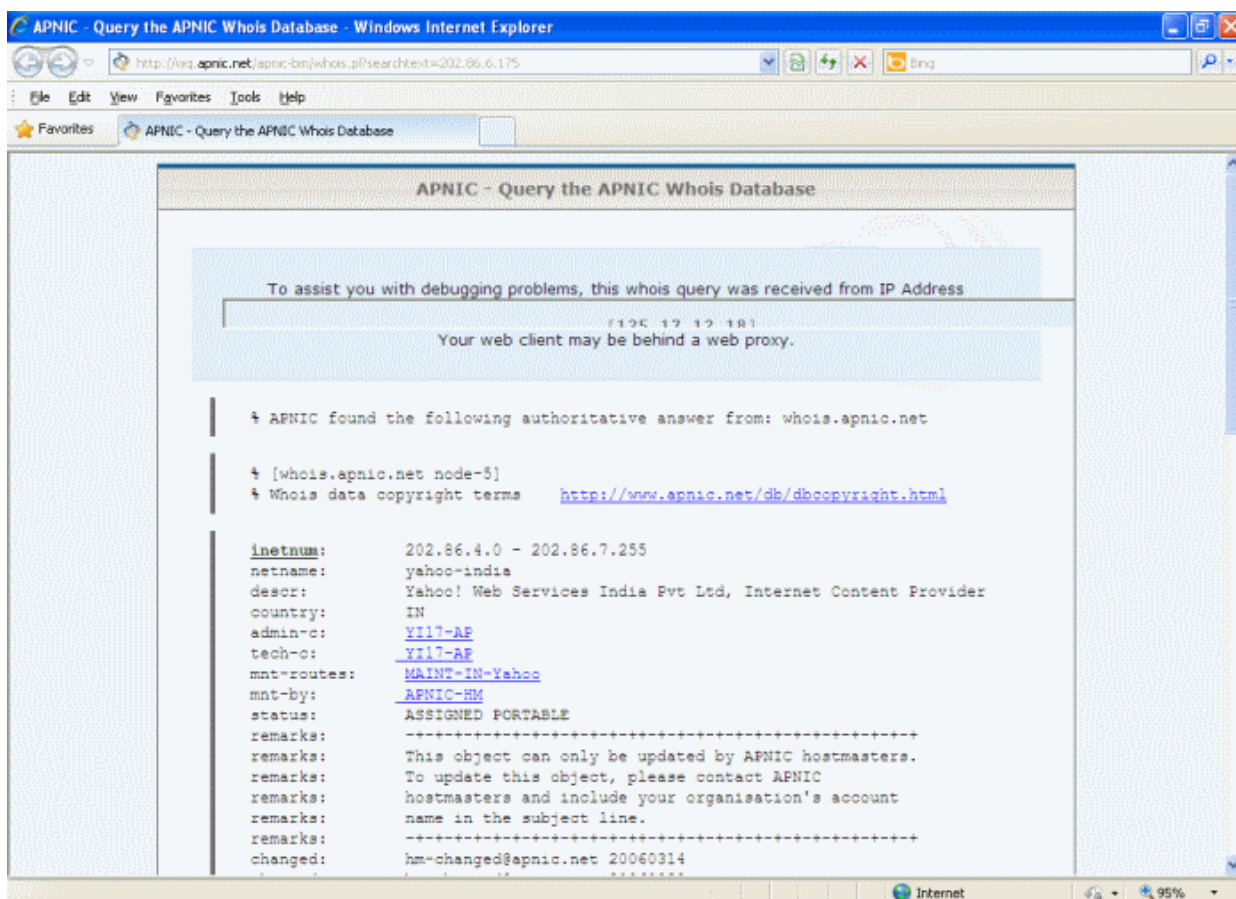


- **Trace Route** - Sends a sequence of Internet Control Message Protocol (ICMP) packets to the remote host and measures the route path and transit times of packets across the network

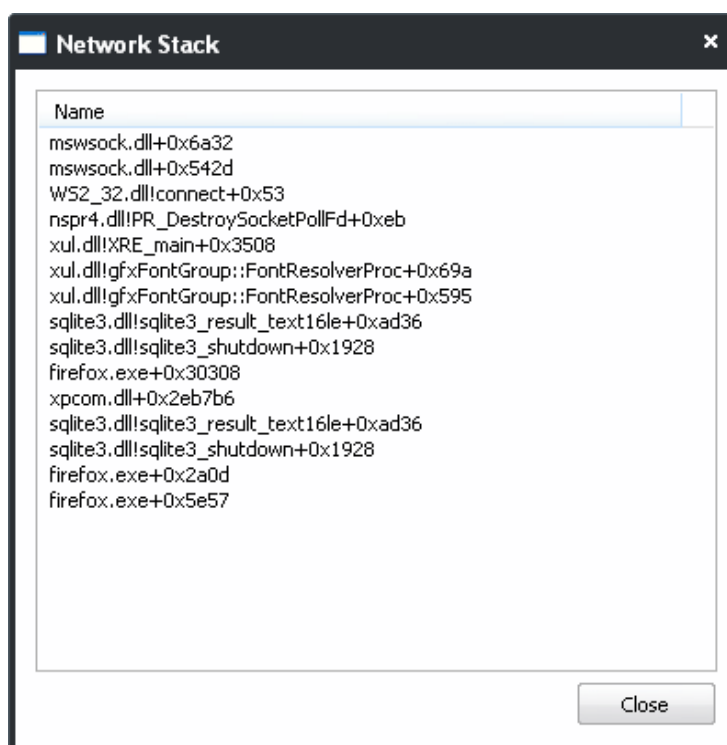




- **Whois** - Opens the default browser of the system, takes you to the Whois database and enables you to obtain contact information of the remote host connected. This is very much useful in law enforcement and business applications.



- **View Stack** - Opens the Network Stack dialog that displays a list of protocols in the stack.



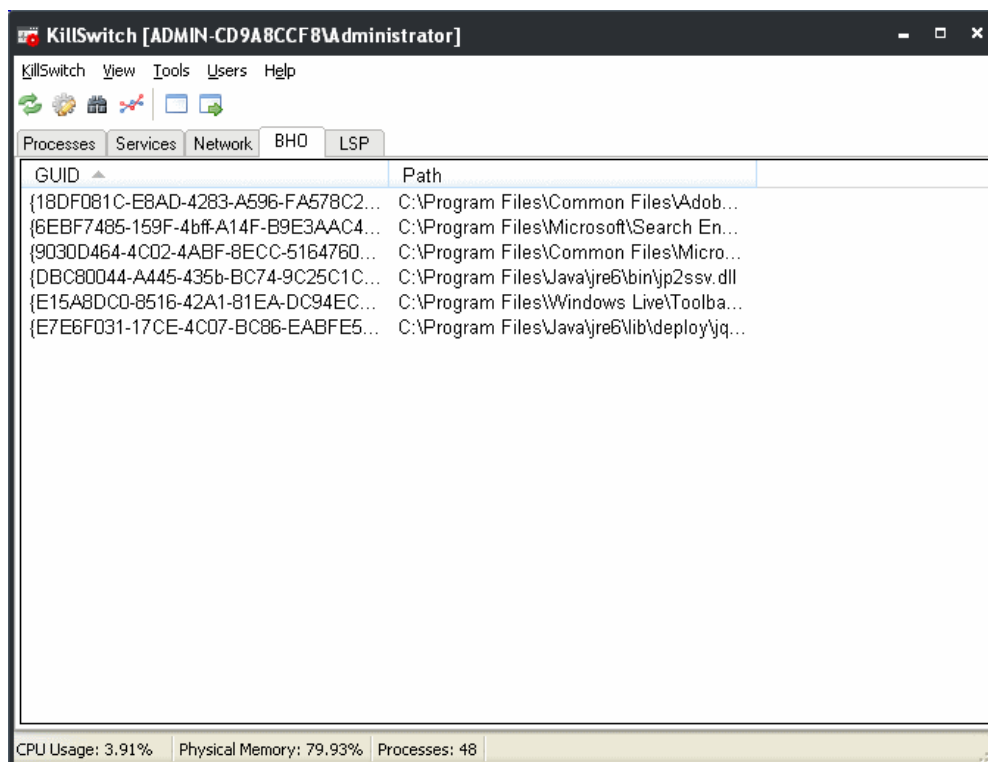
- **Close** - Closes the network Connection.
- **Copy** - Copies the row of the selected connection from the list of connections into your clipboard.

### 3.3.4. Browser Helper Objects

The 'BHO' tab displays all the Browser Helper Objects (BHO) that are currently installed in your system as a table in the main display pane. It also allows you to delete the BHOs which are of no use, from your system

**Background Note:** A Browser Helper Object (BHO) is a DLL module added as a plug-in for Microsoft's Internet Explorer web browser to provide added functionality. BHOs are of different types corresponding to the additional functionality they provide to IE. Some examples are given below:

- BHOs for enabling the display of different file formats which are not the native file formats supported by the browser. For example, for opening the pdf files in the IE window, it needs an Adobe Acrobat plug-in installed.
- BHOs for displaying toolbars in IE window. For example, to display the Google toolbar in IE, it needs a Google toolbar plug-in to be installed.

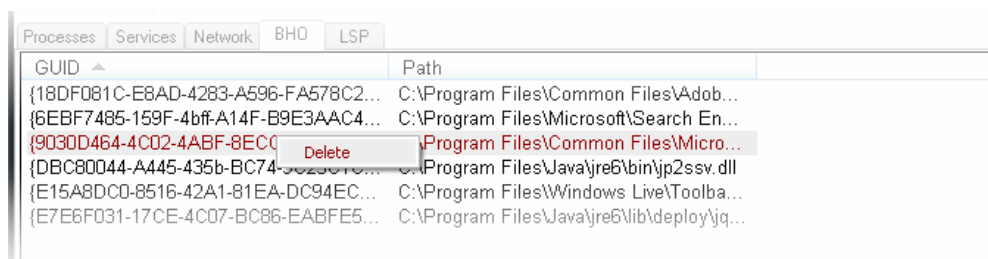


**LSP Table - Descriptions of Columns**

Column	Description
GUID	Displays the globally unique identifier (GUID) of the BHO. Clicking on the column header sorts the entries in ascending or descending order of the GUIDs.
Path	Displays the location at which the DLL is stored in your computer. Clicking on the column header sorts the entries in ascending or descending order of the paths.

### 3.3.4.1. Deleting Unused BHOs

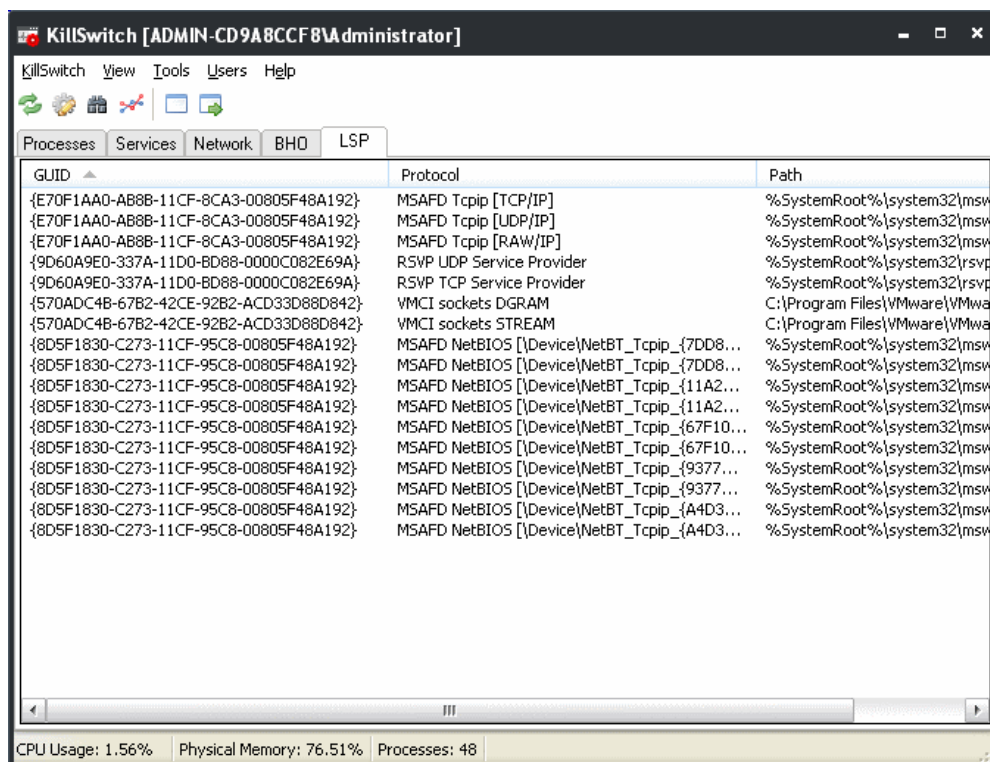
Just right click on the BHO and click 'Delete' from the context sensitive menu.



### 3.3.5. Layered Service Providers

The 'LSP' tab displays all the Layered Service Providers (LSP) that are currently installed in your system as a table in the main display pane. It also allows you to delete the LSPs which are of no use, from your system

**Background Note:** A layered Service provider is a DLL that intercepts and modifies the Internet traffic for the processing requirements of the applications/programs (such as a web browser, the email client, etc) that access Internet. For example the LSP associated with a security program will analyze the traffic for searching for viruses or other threats before passing the traffic to the application that requires it.

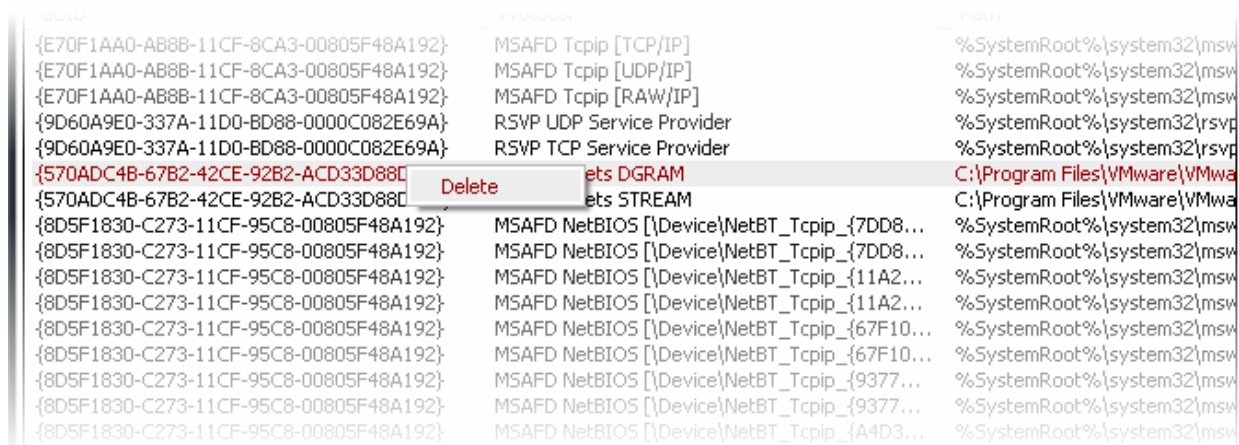


**LSP Table - Descriptions of Columns**

Column	Description
GUID	Displays the globally unique identifier (GUID) of the LSP. Clicking on the column header sorts the entries in ascending or descending order of the GUIDs.
Protocol	Shows the connection protocol of the LPC. Clicking on the column header sorts the entries in ascending or descending alphabetical order of the protocols.
Path	Displays the location at which the DLL is stored in your computer. Clicking on the column header sorts the entries in ascending or descending order of the paths.

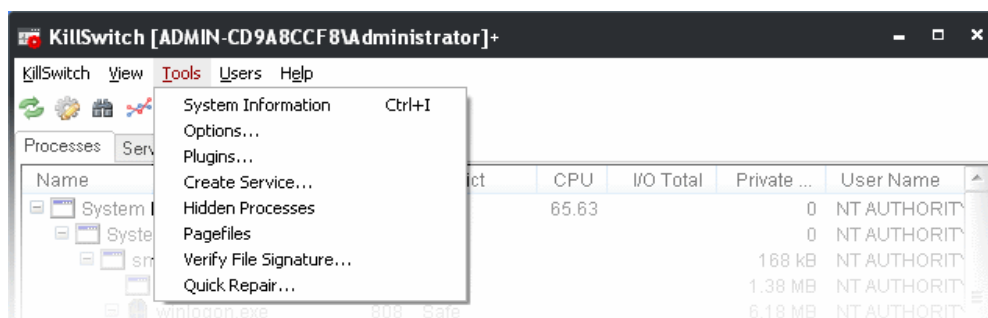
### 3.3.5.1. Deleting Unused LSPs

Just right click on the LSP and click 'Delete' from the context sensitive menu.



## 3.4. The Tools Menu

The Tools menu in the file menu bar caters options for viewing various critical information of your system and for granular configuration of the overall behavior of the application.




The options available are:

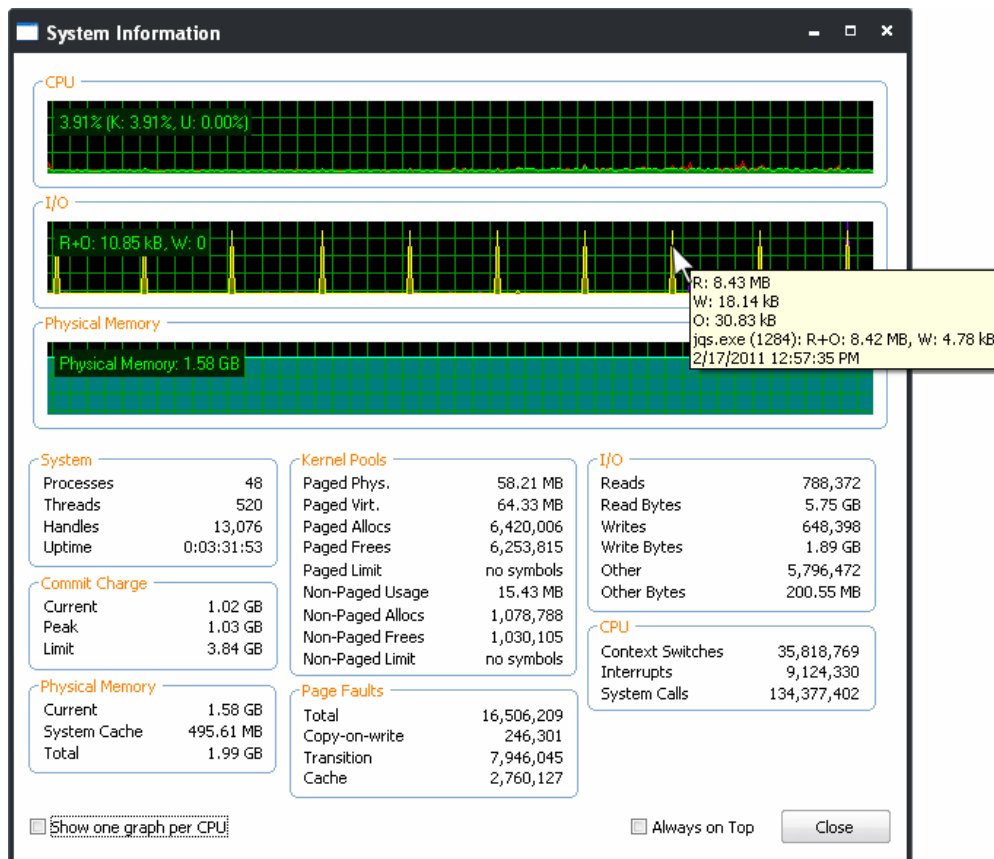
- **Viewing System Information;**
- **Configuring the Application;**
- **Managing plug-ins;**
- **Creating a new service;**
- **Scanning Your System for Hidden Processes;**
- **Viewing the Page Files in Your System;**
- **Verifying authenticity of Applications;**
- **Repairing Windows Settings and Features.**

### 3.4.1. Viewing System Information

The system information pane displays the dynamic graphical representations of your CPU usage, I/O activity and physical memory usage of your system, along with the detailed statistics on current usage of various system resources.

- To view the System Information pane, click 'Tools' > 'System Information'.

**Tip:** You can also open the System Information pane by clicking the  icon from the shortcut icons area.



## Graphical Reports

- **CPU** - Shows a dynamic graphical representation of the usage of CPU over time. You can hover your mouse over the graph to view details. In multiprocessor operating system, you can make the pane to display individual graph for each CPU by selecting the check box 'Show one graph per CPU' at the bottom left of the interface.
- **I/O** - Shows a dynamic graphical representation of Input/Output activities of the computer over time. You can hover your mouse over the graph to view details.
- **Physical Memory** - Shows a dynamic graphical representation of the usage of physical system memory over time. You can hover your mouse over the graph to view details.

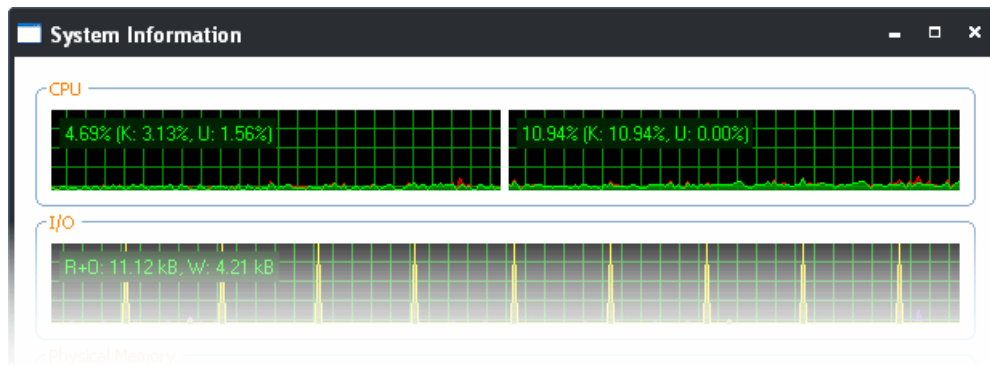
## Statistical Reports

- **System** - Displays a detailed statistics on the number of processes, threads and handles running on the computer.
- **Commit Charge**- Displays a statistics on virtual memory allocated to programs and the operating system. As the memory is copied to the paging file(s) in you hard disk drive , the value listed under Peak may exceed the maximum physical memory.
- **Physical Memory** - Displays a statistics on the total physical memory, also called RAM, installed on your computer.
  - Available - Represents the amount of free memory that is available for use.
  - System Cache - Shows the current physical memory used to map pages of open files.
- **Kernel Pools** - Shows a statistical report on memory used by the operating system kernel and device drivers.
  - Paged memory types - Memory that can be copied to the paging file, thereby freeing the physical memory. The physical memory can then be used by the operating system.
  - Non-paged memory types - Memory that remains resident in physical memory and will not be copied out to the paging file.
- **Page Faults** - Shows a statistical report on the page faults, The page fault is the direct access to the page that is mapped in the virtual memory but not loaded in the physical memory.
- **I/O** - Shows a statistical report on the Input/Out put activities of your computer.

- **CPU** - Shows a statistical report on the activities on the CPU.

## Check Boxes

- **Show one graph per CPU** - Displays individual graphs for each processor in a multiprocessor operating system. Hence this option will be enabled only in multiprocessor operating system environment.

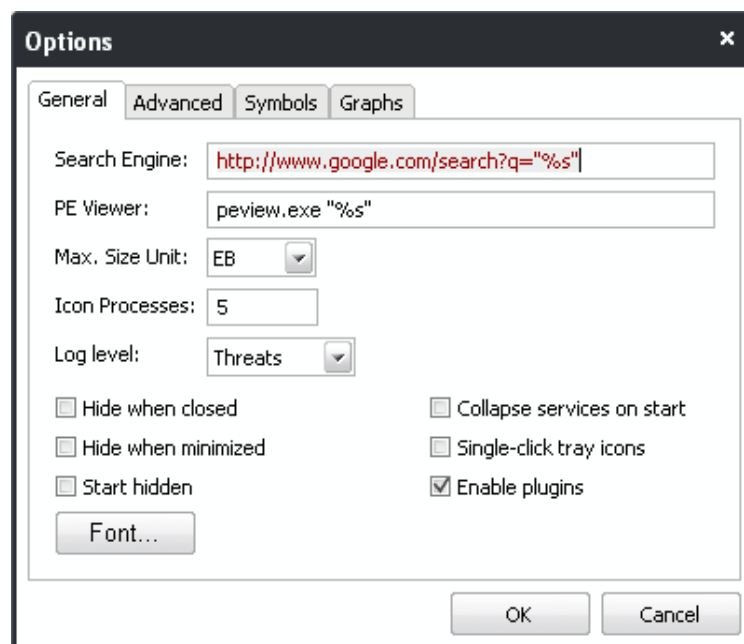


- **Always on Top** - Always Positions the System Information pane above all the other open windows on the display.

## 3.4.2. Configuring KillSwitch

The overall behavior of the KillSwitch application can be configured through the 'Options' dialog.

- To open the Options dialog, click 'Tools' > 'Options'.



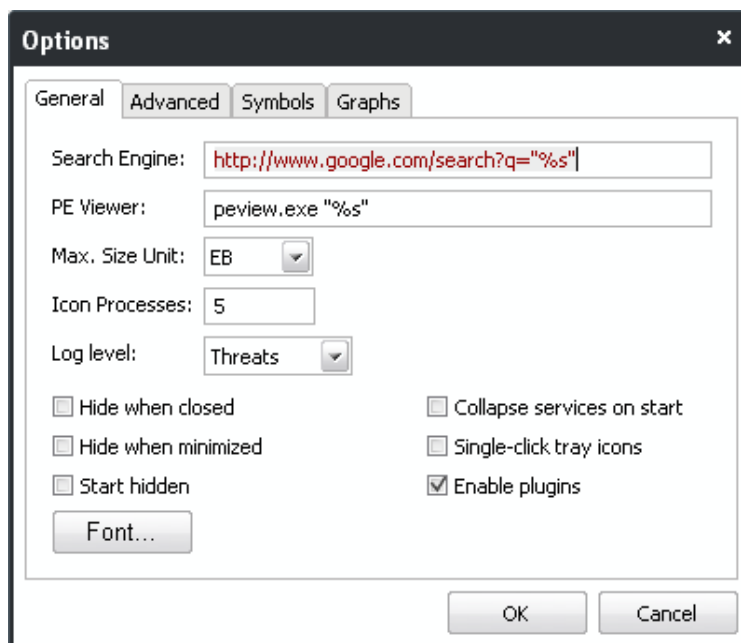
The 'Options' dialog enables granular configuration of the application under four tabs:

- **General**
- **Advanced**
- **Symbols**
- **Graphs**

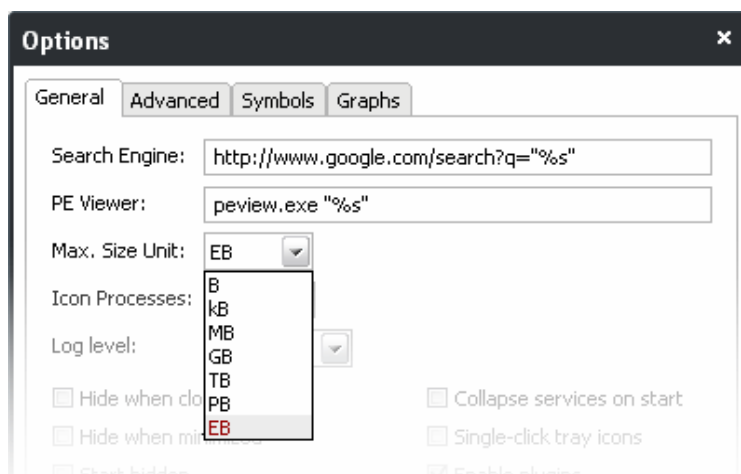
### 3.4.2.1. General Settings

The 'General' tab allows you to configure the general properties and look and appearance of the application interfaces.





- **Search Engine** - Enables you to set the default search engine for use by the 'Search Online...' option in the context sensitive menu of the process tab. You need to alter the address by only replacing the portion of http://www.domain.com and retain the other portions. %s will be replaced by the name of the selected process.
- **PE Viewer** - Enables you to set the PE viewer for use in displaying the Import/Export tables of Modules, on clicking Inspect from the context sensitive menu under **Modules** tab of **Process Properties** dialog. You need to specify only the executable file name of the PE viewer. %s will be replaced by the name of the selected module.
- **Max. Size Unit** - Enables you to specify the maximum data size unit for displaying the statistical reports in the interfaces of KillSwitch. Data of sizes which can be displayed as 1024 or less in a smaller unit will be displayed in that smaller unit, while sizes requiring a larger unit will use units up to the maximum unit specified here.



- **Icon Processes** - Enables you to set the maximum number of processes that can be displayed in the sub-menu pane on right clicking the **KillSwitch system tray icon** and hovering the mouse cursor over 'Processes' option.
- **Log level** - Allows you to select the option for creating log reports.



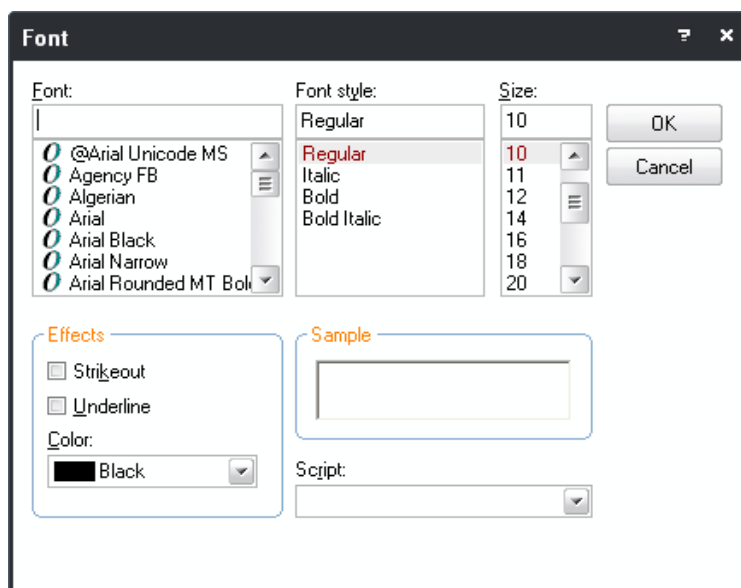


You have three options from the drop down box:

- **Disable** - Instructs KillSwitch to not to generate log reports for the scans completed.
- **Threats** - Instructs KillSwitch to generate log reports containing files that it has detected as threats.
- **All** - Instructs KillSwitch to generate log reports for all the files that it has scanned.

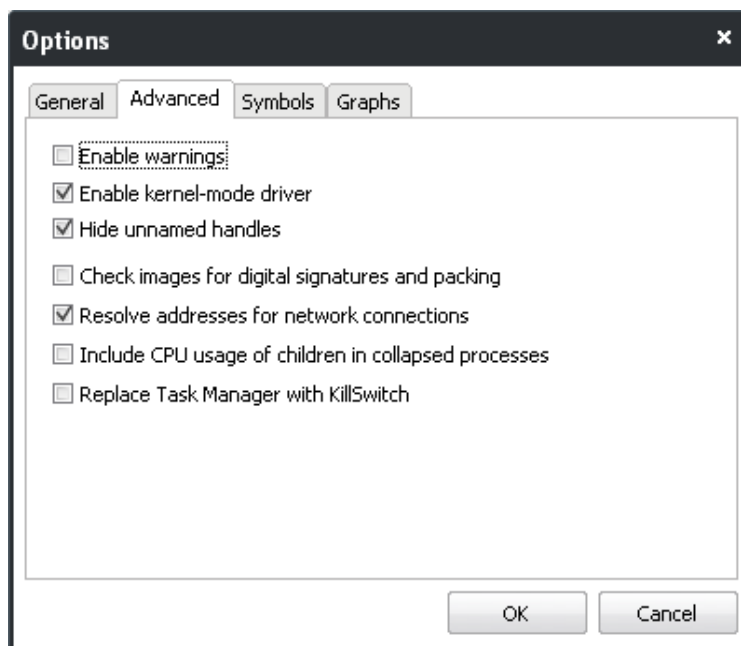
Refer to the section **Logs** for more details on how to view the logs generated.

- **Hide when closed** - If enabled, KillSwitch will automatically hide itself when it is closed. You can double-click on the system tray icon to reopen the application.
- **Hide when minimized** - If enabled, KillSwitch will automatically hide itself when it is minimized. You can double-click on the system tray icon to reopen the application.
- **Start hidden** - If enabled, KillSwitch will start hidden. You can double-click on the system tray icon to show KillSwitch window.
- **Collapse services on start** - If enabled, KillSwitch will collapse the services.exe tree, hiding all services at startup.
- **Single-click tray icons** - If enabled, KillSwitch will show/hide itself with just a single click on its system tray icon(s). Else, a double-click is needed to start the application from the system tray icon.
- **Enable plugins** - KillSwitch uses several plug-ins for various additional functions. These plug-ins will be enabled only if this option is selected. This option allows you to enable or disable plug-ins on the whole. For more details on granular management of plug-ins refer to the section **Managing Plug-ins**.
- **Font Settings** - Clicking the Font button opens the Font dialog that enables you to set the fonts types, sizes and styles for the information displayed in all of the KillSwitch interfaces.



## 3.4.2.2. Advanced Settings

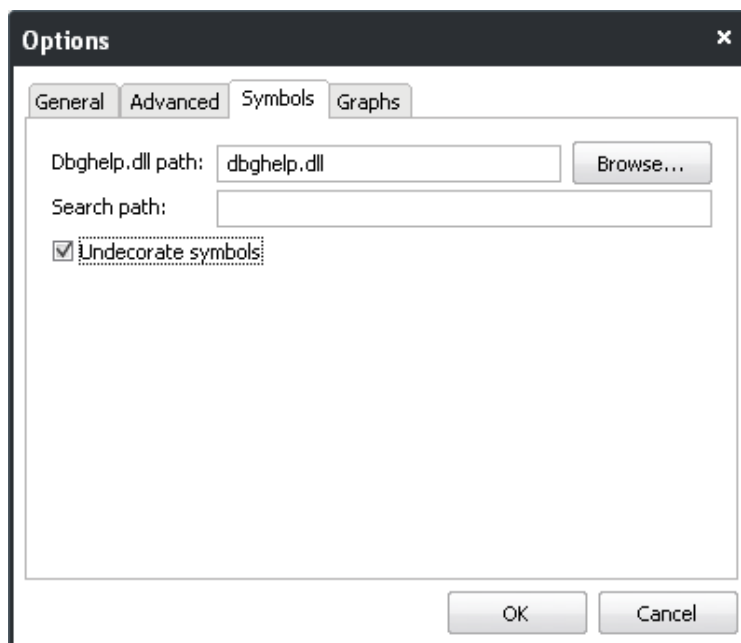
The 'Advanced' tab allows you to configure the application for advanced level options.



- **Enable Warnings** - The confirmation dialogs displayed on execution of critical actions, e.g. terminating a process, will appear only if this option is selected.
- **Enable kernel-mode driver** - Some **handles** cannot be displayed by a user-mode program like KillSwitch. Enabling this option starts a built-in tool that allows KillSwitch to display all handles and bypass rootkits/security software in limited ways. If enabled, it will be loaded the next time KillSwitch is started.
- **Hide unnamed handles** - If enabled, unnamed handles will be hidden by default under the 'Handles' tab of Process Properties window. This can be changed ad hoc in the '**Process Properties window**' > '**Handles**' tab when required.
- **Check images for digital signatures and packing** - If enabled, Kill will check process images for digital signatures and determine whether they are packed. This features requires Internet connection.
- **Resolve addresses for network connections** - If enabled, KillSwitch retrieves the host names for all the network connections for display in the 'Local Address' and 'Remote Address' columns under the '**Network**' tab of the main interface. If not enabled, only the IP addresses of the local host and the remote host are displayed in the interface.
- **Include CPU usage of children in collapsed processes** - If enabled, the 'CPU Usage' shown for processes which are collapsed under the '**Processes**' tab, will include the sum the usages both by the parent process and the child processes.
- **Replace Task Manager with KillSwitch** - If enabled, any attempt to start Windows Task Manager, (e.g. press Ctrl + Alt + Del > Click 'Task Manager' or right-click on the Task Bar and select 'Task Manager' from the pop-up menu) will start KillSwitch instead. To re-enable Windows Task Manager when Ctrl + Alt + Del is pressed (or 'Task Manager' is selected by another method), simply disable this setting and click 'OK'.

### 3.4.2.3. Symbols

The 'Symbols' tab enables you to configure for the images that are displayed in the KillSwitch interfaces.



- **Dbghelp.dll path** - Enables you to change the path of the dbghelp.dll file stored in your computer if you have replaced it from the standard version.

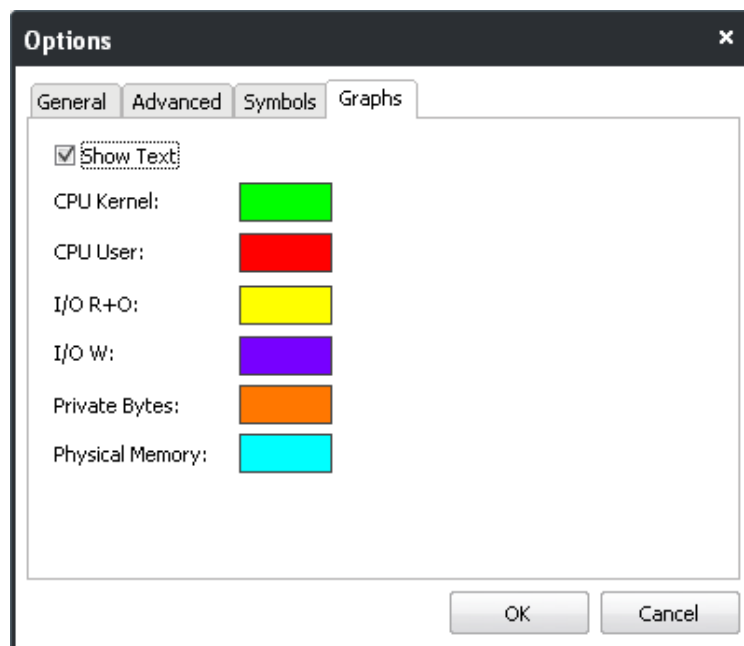
**Background Note:** dbghelp.dll is a Windows Image Helper. It is a system process module that contains functions used for the symbol engine and for the symbol and module enumeration. The module is needed for your Windows system to work properly. If the module has got corrupted, you may be having trouble with your Windows image viewing and editing programs. In that case you should replace your existing version with a new one.

- **Search Path** - Enables you to specify the path of the symbol server of your choice. Most users wish to use the following: SRV\*C:\Users\USERNAME\Symbols\*http://msdl.microsoft.com/download/symbols. This will have any needed symbols downloaded from Microsoft's symbol server to the specified directory.
- **Undecorate Symbols** - If enabled, C++ symbol names will be undecorated (unmangled). This is most useful for methods with complex signatures.

### 3.4.2.4. Graphs

The 'Graphs' tabs enables you to configure the look and feel of the graphs shown in:

- **'Process Properties'** dialog > **'Performance'** tab;
- **'Tools Menu'** > **'System Information'**.



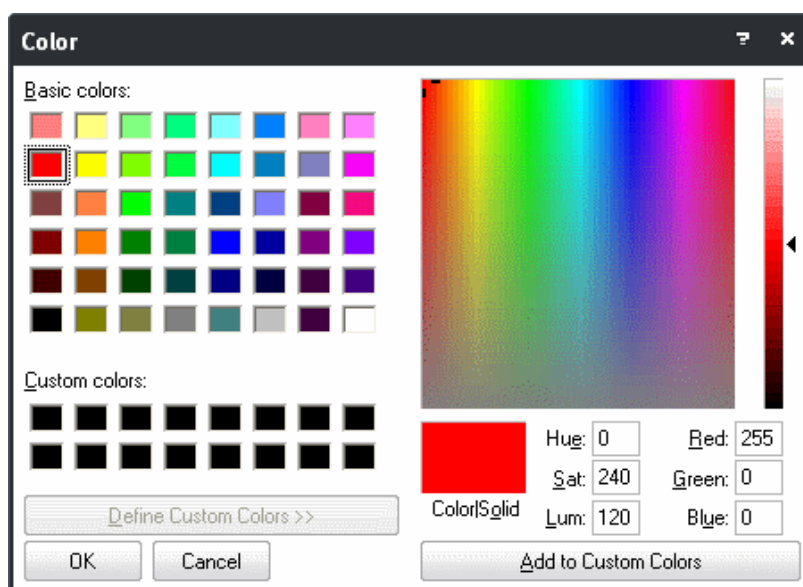
- **Show Text** - The text representing the current usage will be displayed on each graph under '**Process Properties**' dialog > '**Performance**' tab and '**Tools**' > '**System Information**' window, only if this option is enabled.

This interface also enables you to select the color of the line in the graphs indicating the history/usage information of:

- CPU Kernel;
- CPU User;
- I/O R+O;
- I/O W;
- Private Bytes;
- Physical Memory.

### To change the color of a desired line

1. Click on the color patch beside the required parameter. The 'Color' window will be displayed with the default color selected.



2. Choose the color in which you wish the parameter to be indicated in the graph. You can do this by two ways:
  - Directly choose the color from the palette; or
  - Type the RGB or Hue, Saturation and Luminance values in the respective fields to create a custom color,

then click 'Add to Custom Colors' to add the color to the palate.

3. Click OK.

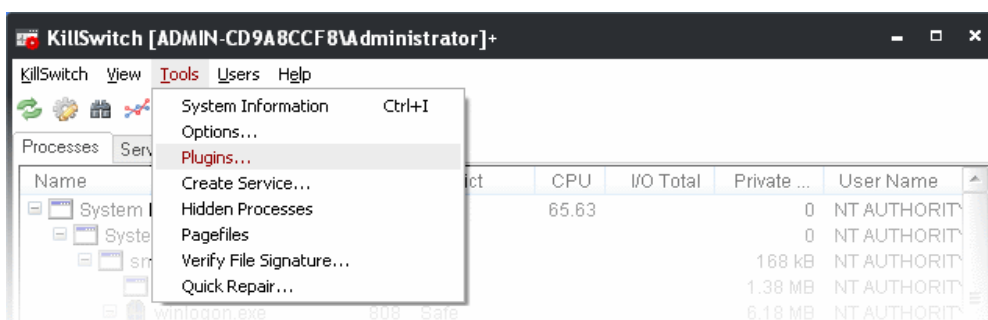
The graphs will be displayed with the colors you have chosen.

## 3.4.3. Managing Plug-ins

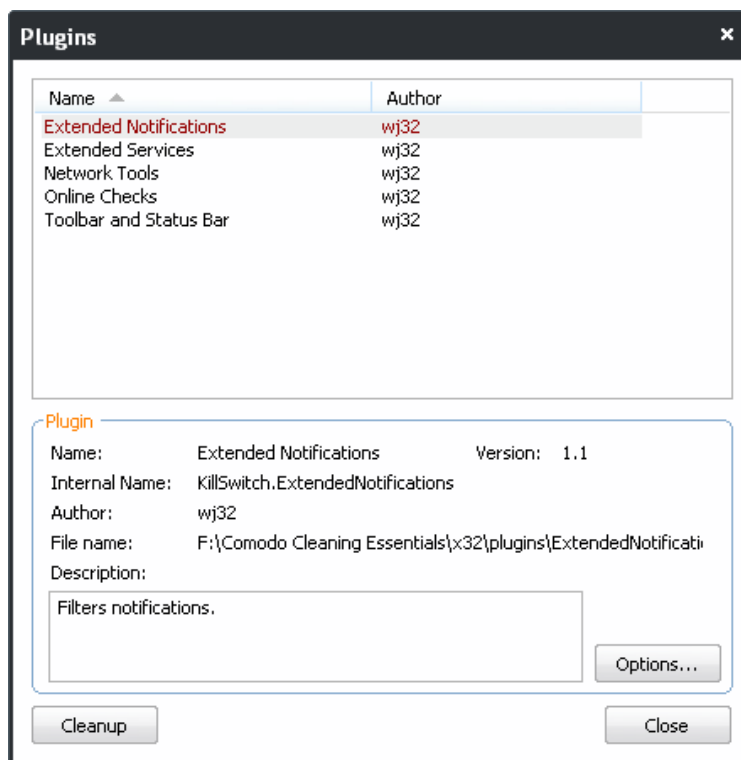
KillSwitch is shipped with a set of plug-ins that provide additional functionality to it. Comodo keeps on developing the plug-ins which will be added to KillSwitch in user computers upon updates to the program which will in-turn keep on adding new functionality to the product.

**Note:** For the plug-ins to be operative the option '**Enable Plug-ins**' should have been selected under the '**General**' tab of '**Tools**' > '**Options**'.

The Plug-ins option in the Tools menu enables you to configure the plug-ins that are used with the application.



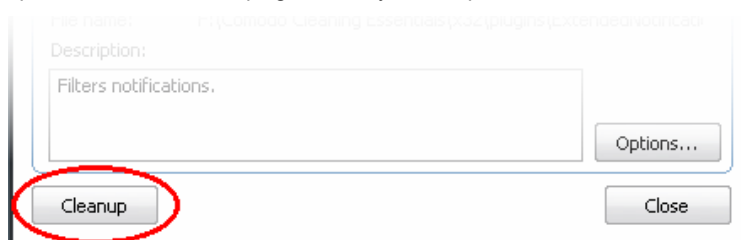
To configure the Plug-ins, click 'Plugins...' from the 'Tools' menu. The Plugins dialog will open.



The upper pane of the dialog displays a list of the KillSwitch plug-ins available in your computer. Clicking on a plug-in will display the details of the plug-in in the lower pane. Some of the plug-ins allow you to configure their usage with respect to processes and services, by clicking the 'Options' button.



Clicking 'Clean-up' removes the unused plug-ins from your computer.

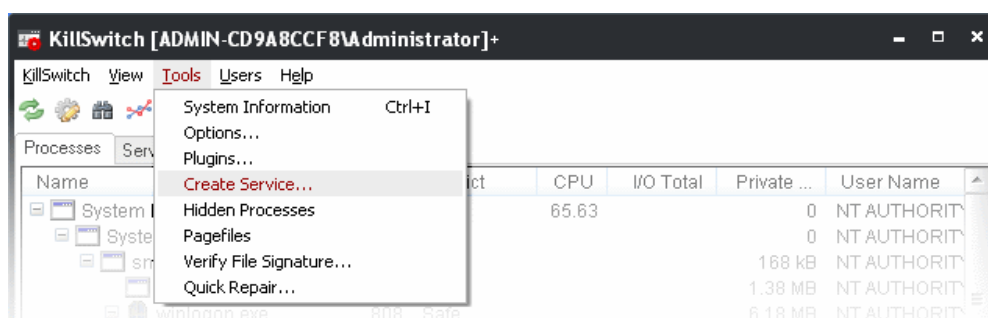


## 3.4.4. Creating a Service

KillSwitch enables you to create new services to start/run with Windows for drivers, applications, programs or any executable files. Once created as a service, the driver or the executable is loaded into system memory when Windows is started irrespective of the user that logs-in and started as you configure. One example of usage of this feature is configuring a self developed or user-defined security software or a driver for a third-party hardware to start along with Windows.

### To create a new service

1. From the Tools menu, select 'Create Service'.



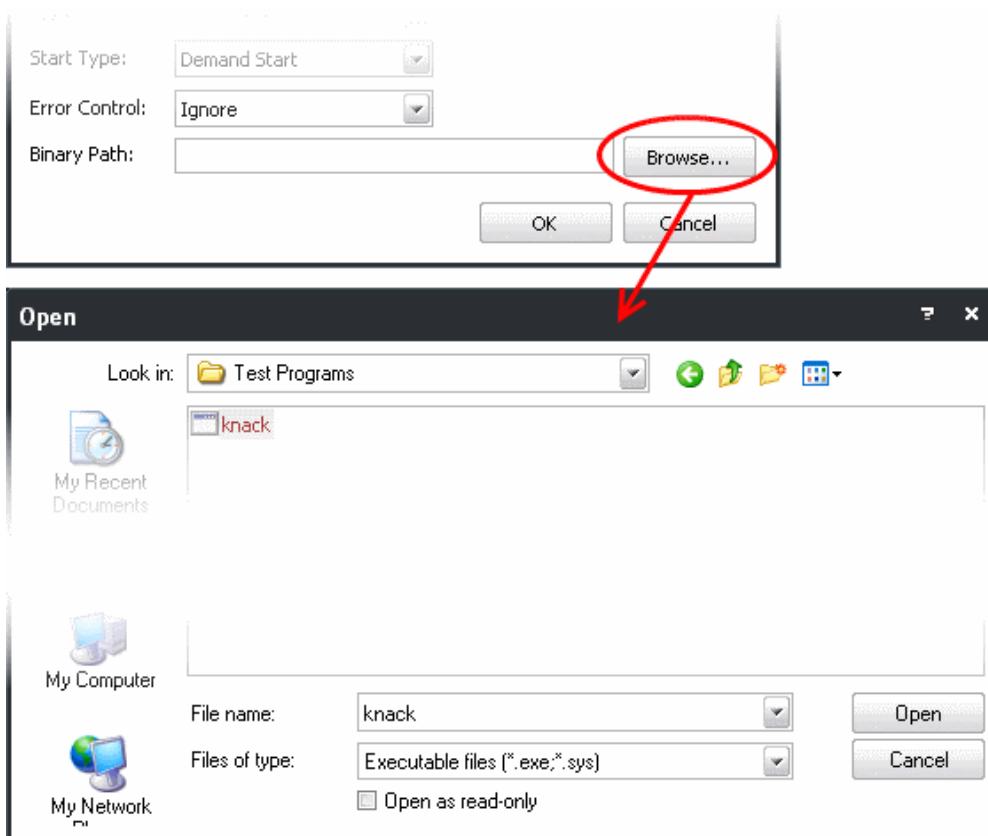
The 'Create Service' dialog will open.

2. Enter the name and display name of the new service to be created in the respective text boxes. The service will be identified with the names you are entering, under the **'Services'** tab of the main interface.
3. Select the type of the service from the 'Type' drop-down.

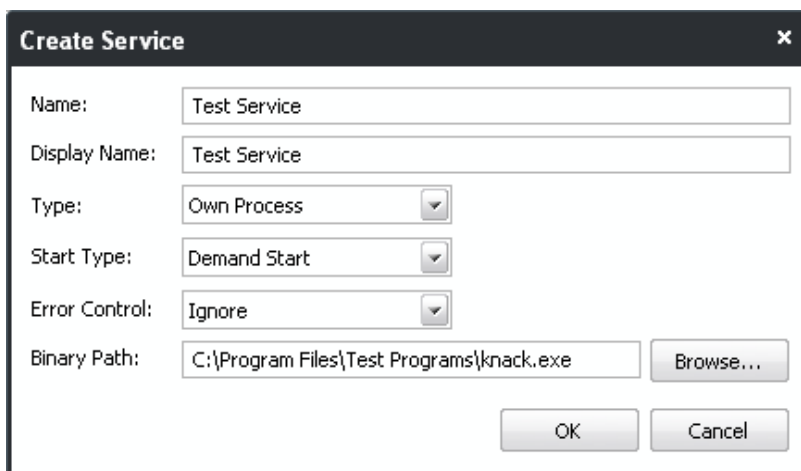
4. Select how the service should start from the 'Start Type' drop-down.

5. Select how the service should respond in case of an error in the 'Error Control' drop-down.

6. Enter the path of the driver or the executable file stored in your computer in the Binary Path text box. You can click the 'Browse' button and browse to the location where the executable is stored.

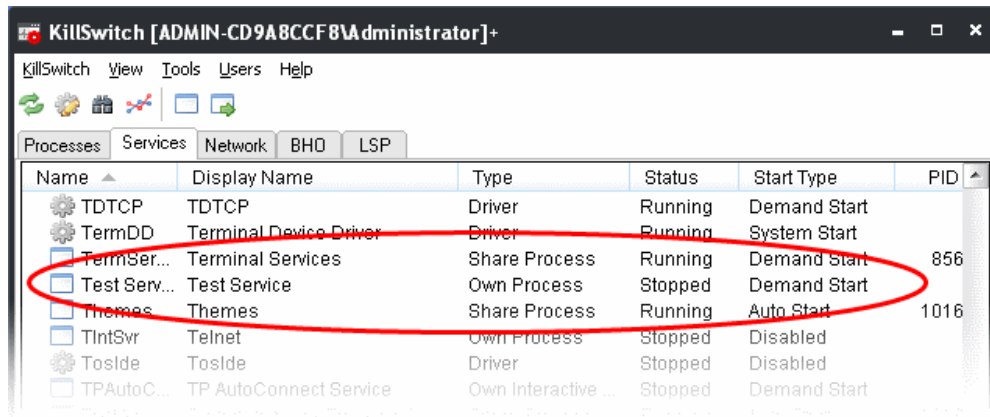


The selected file will be added.



7. Click OK. The service will be added to your computer and will start as you specified in the 'Start Type' option, from the next restart of the computer. You can view the service listed in the **'Services'** tab of the main interface.



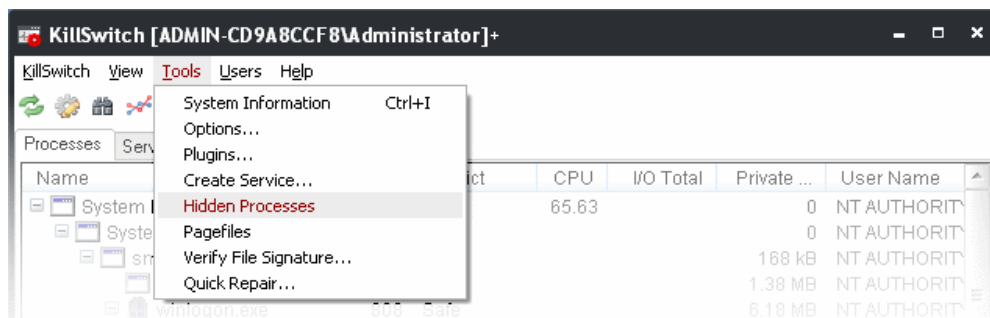


### 3.4.5. Scanning Your System for Hidden Processes

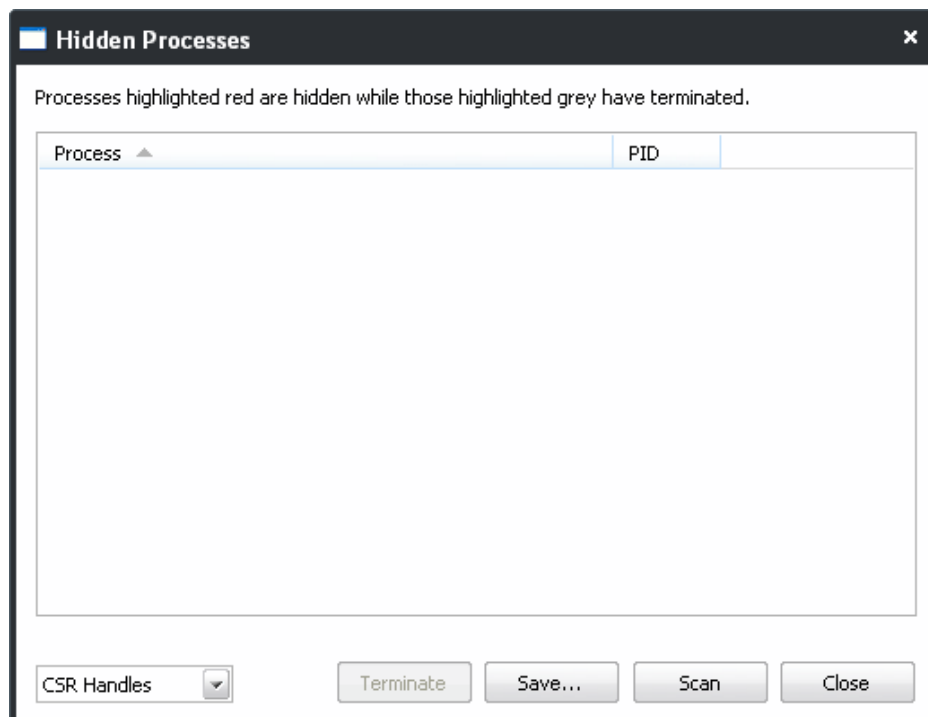
KillSwitch can scan your computer for the processes that run hidden and not visible under the 'Process' tab of the main interface. The users can find malicious attempts like a spyware through rootkits, buffer overflow or Denial of Service (DoS) attacks running silently in the computer and terminate them to safeguard their valuable and confidential data from being stolen or corrupted.

#### To scan your computer for hidden processes

1. From the 'Tools' menu, click 'Hidden Processes'

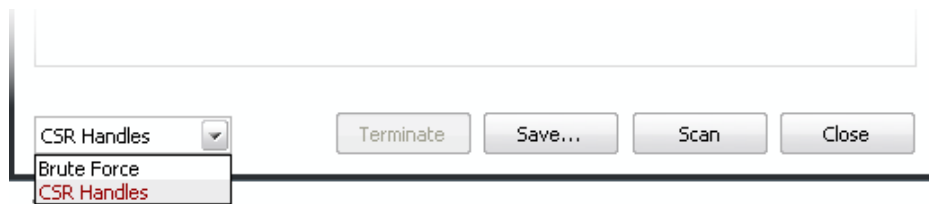


The hidden Processes dialog will open.

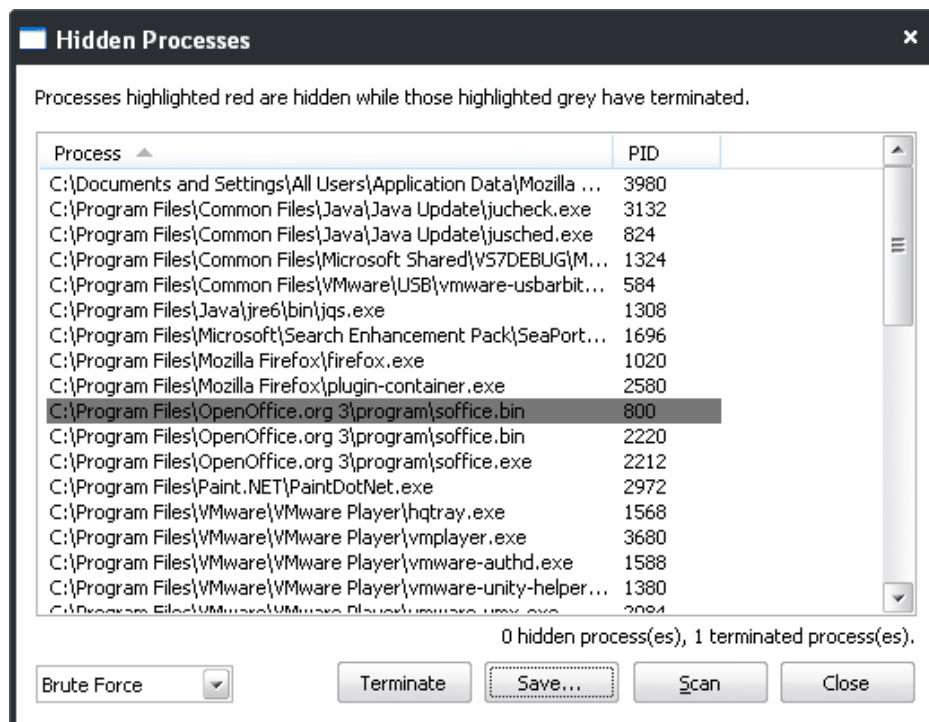


2. Select whether you want to scan your system for 'CSR Handles' or 'Brute Force' attacks from the drop-down at the

bottom left corner of the dialog.



- Click Scan. On completion of the scan, all the processes running in your system will be listed. The processes that are running hidden will be highlighted with red color and the processes that are found hidden and terminated automatically will be highlighted with gray color.



- To stop a processes, select the process and click 'Terminate'.
- To save the scan results as a .txt file, click 'Save'

### 3.4.6. Viewing the Page Files in Your System

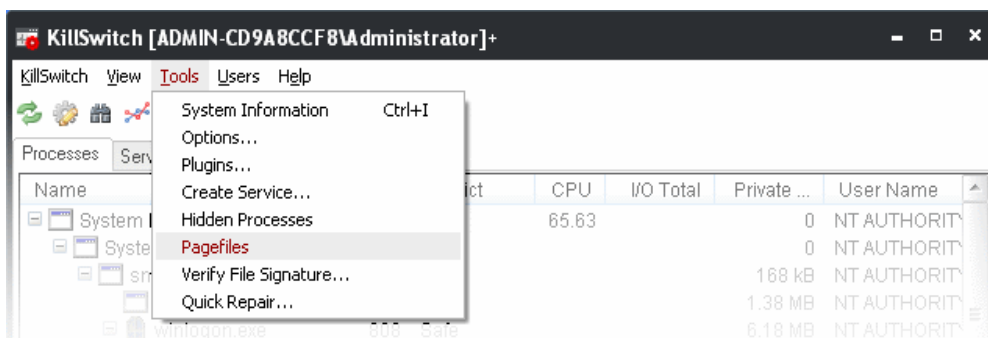
A page file is a reserved portion in the partition(s) of your hard disk drive, to acts as Virtual Memory - an extension for the system memory (RAM). A page file can be accessed as one contiguous chunk of data and enables faster access than accessing data from many different original locations. Windows automatically moves the least accessed data located in the system memory to the page file. As the user switches to other programs or files, this seamless process continues, using the page file as a container. Going back to a previous program will cause the system to swap contents in the page file for contents in RAM, thus increasing the efficiency and performance speed of the system.

Windows creates page files in your hard disk with size in proportion to the system memory capacity, during installation. Advanced users can reconfigure the system-provided default size value of the page file to meet their particular needs.

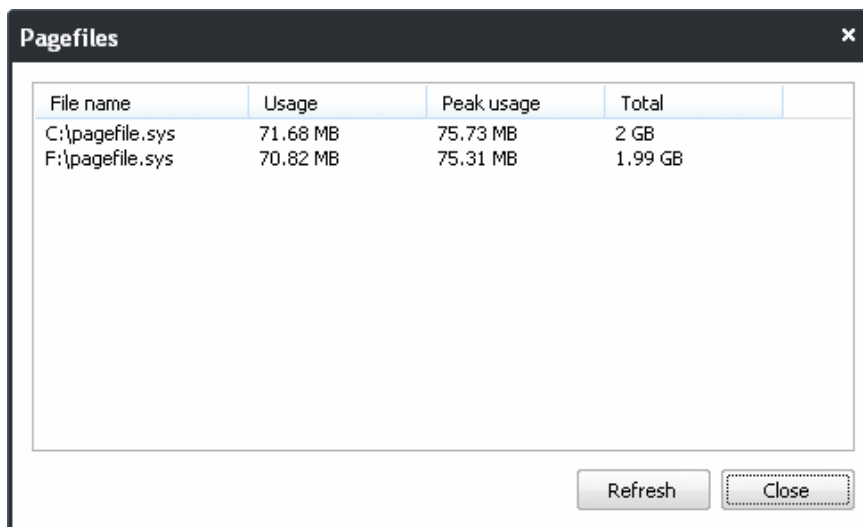
KillSwitch enables you to view the page file(s) created in your system.

#### To view the page files

- From the 'Tools' menu, click 'Pagefiles...'



The page files dialog will open. It contains a list of the page files created in different partitions of your hard disk drive.



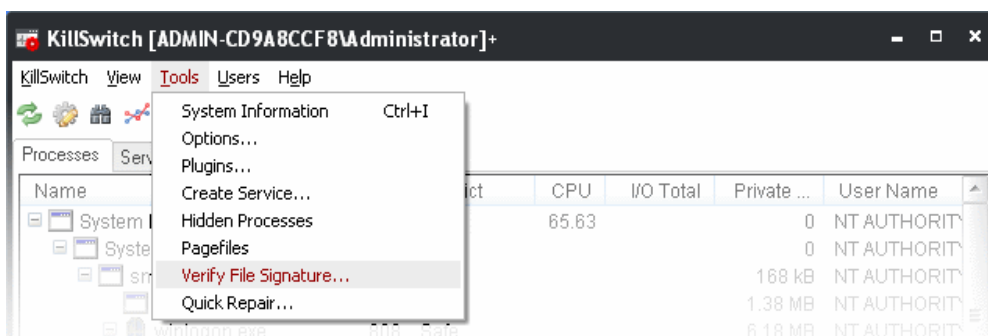
### 3.4.7. Verifying Authenticity of Applications

A software application can be treated as a 'Trusted' one if it is published by a Trusted Software publisher/vendor. To ensure the authenticity, the publisher/vendor digitally sign their software using a code signing certificate obtained from a Trusted Certificate Authority (CA). Ensuring whether a software/application is signed by a vendor ensures that the software is trusted. Refer to the **Background details** given below for more information.

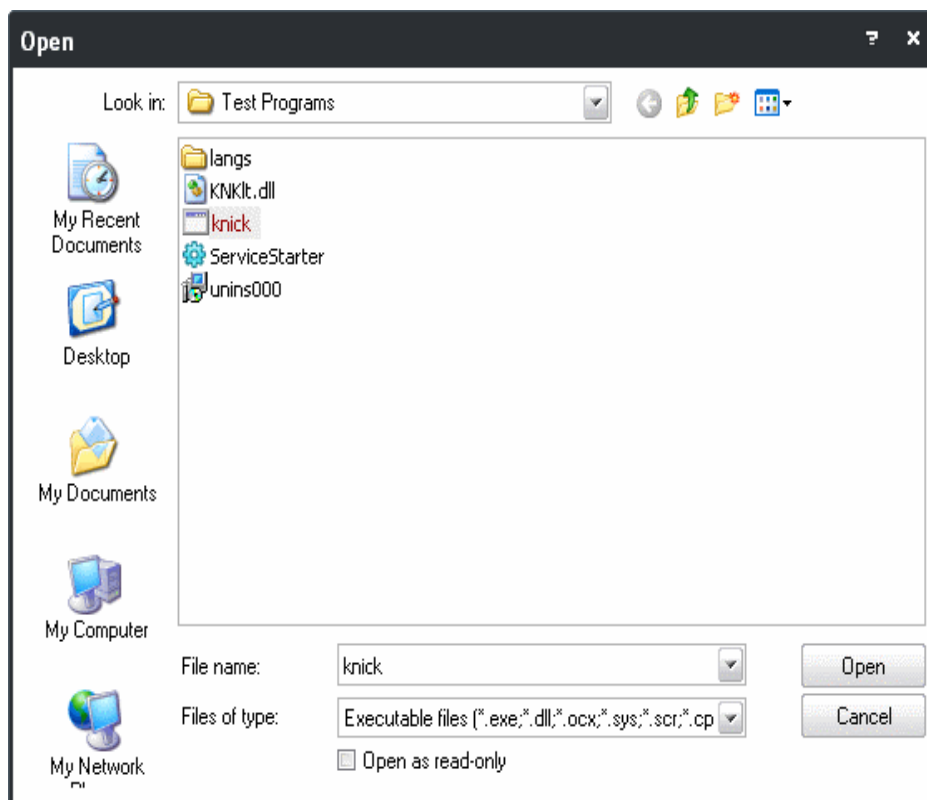
KillSwitch enables you check whether an application/program is digitally signed by the vendor and to ensure whether the program is trusted and free from malice.

To check whether an application/program installed in your computer is digitally signed

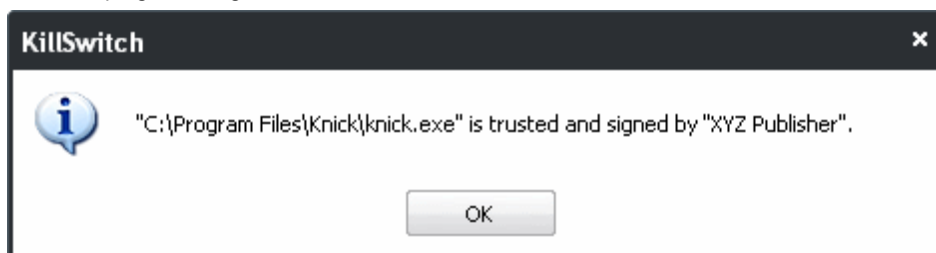
- From the 'Tools' menu, click 'Verify File Signature...'



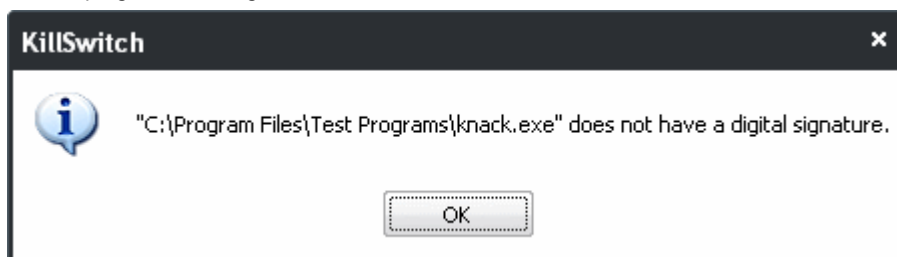
...and navigate to the folder containing the files of the program and select the binary/executable file.



- Click 'Open'. KillSwitch will immediately display the result which indicated whether the program is signed or not signed.
- If the program is signed:



- If the program is not signed:



## Background

Many software vendors digitally sign their software with a code signing certificate. This practice helps end-users to verify:

- **Content Source:** The software they are downloading and are about to install really comes from the publisher that signed it.
- **Content Integrity:** That the software they are downloading and are about to install has not be modified or corrupted since it was signed.

In short, users benefit if software is digitally signed because they know who published the software and that the code hasn't been tampered with - that are are downloading and installing the genuine software.

The 'Vendors' that digitally sign the software to attest to its probity are the software publishers. These are the company names you see listed in the first column in the graphic above.

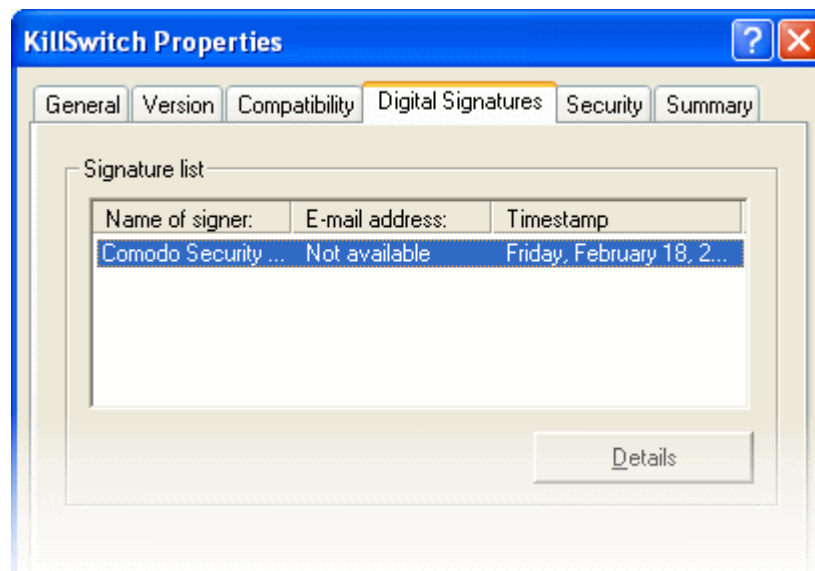
However, companies can't just 'sign' their own software and expect it to be trusted. This is why each code signing certificate is counter-signed by an organization called a 'Trusted Certificate Authority'. 'Comodo CA Limited' and 'Verisign' are two examples of a Trusted CA's and are authorized to counter-sign 3rd party software. This counter-signature is critical to the trust process and a Trusted CA only counter-signs a vendor's certificate after it has conducted detailed checks that the vendor is a legitimate company.

If a file is signed by a Trusted Software Vendor and the user has enabled 'Trust Applications that are digitally signed by Trusted Software Vendors' then it will be automatically trusted by Comodo Internet Security (if you would like to read more about code signing certificates, see <http://www.instantssl.com/code-signing/>).

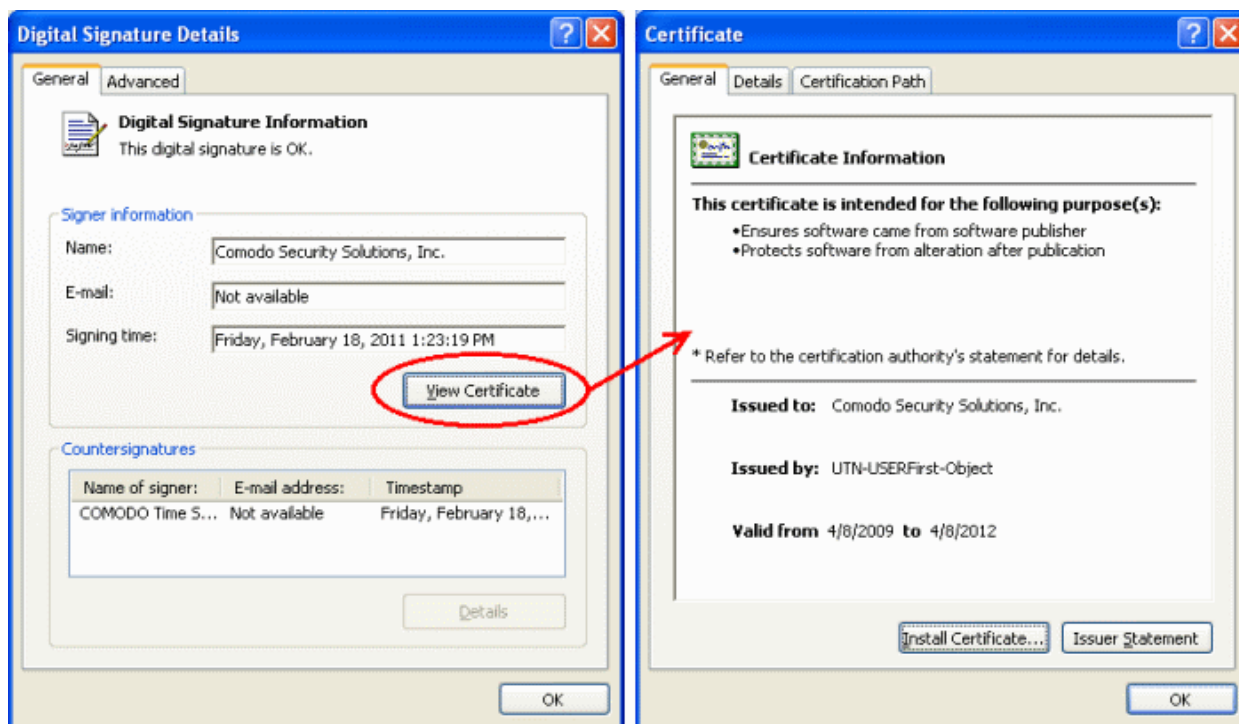
One way of telling whether an executable file has been digitally signed is checking the properties of the .exe file in question. For example, the main program executable for Comodo KillSwitch is called 'KillSwitch.exe' and has been digitally signed.

- Browse to the folder containing the Comodo Cleaning Essentials files
- Right click on the file KillSwitch.exe.
- Select 'Properties' from the menu.
- Click the tab 'Digital Signatures (if there is no such tab then the software has not been signed).

This displays the name of the CA that signed the software as shown below:



Select the certificate and click the 'Details' button to view digital signature information. Click 'View Certificate' to inspect the actual code signing certificate. (see below)



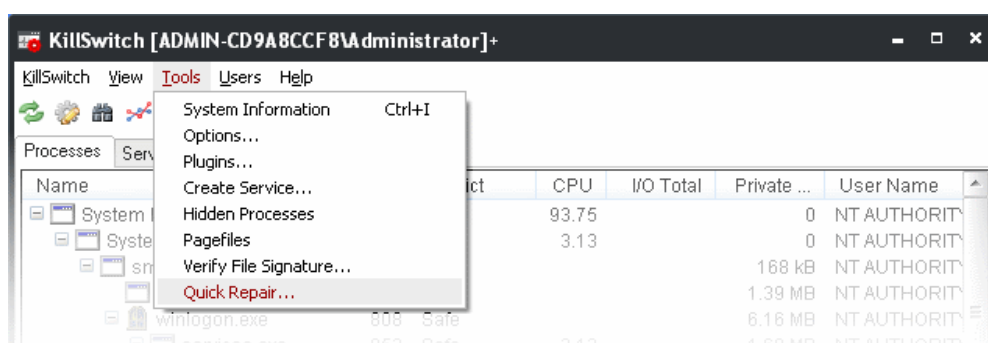
It should be noted that the example above is a special case in that Comodo, as creator of 'KillSwitch.exe', is both the signer of the software and, as a trusted CA, it is also the counter-signer (see the 'Countersignatures' box). In the vast majority of cases, the signer or the certificate (the vendor) and the counter-signer (the Trusted CA) are different.

## 3.4.8. Repairing Windows Settings and Features

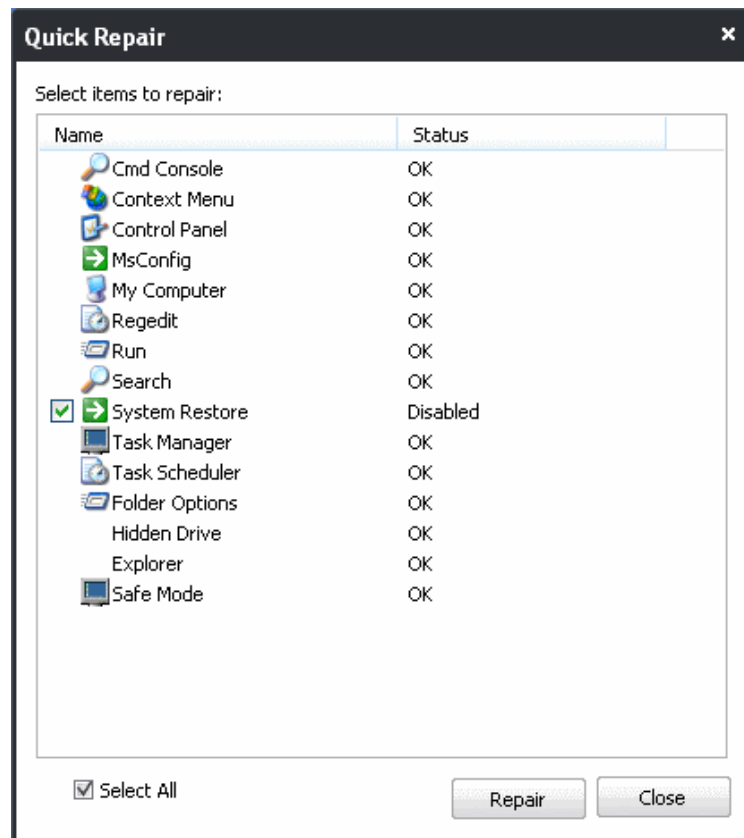
KillSwitch allows you to quickly troubleshoot and repair very important Windows settings and features which are other wise hard to reach. This feature greatly benefits users at beginner level. If crucial Windows settings go wrong, they can be fixed only experienced and skilled geeks. But with KillSwitch even inexperienced users can troubleshoot and fix those problems with a few clicks.

### To check start repairing the Windows settings and features

1. From the 'Tools' menu, click 'Quick Repair...'



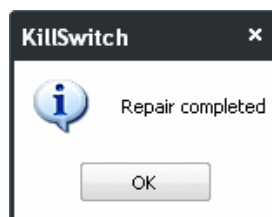
The Quick Repair dialog will appear with a list of features that can be repaired and their current status.



2. Select the checkboxes beside the items you wish to troubleshoot and repair.

**Note:** The checkboxes will appear only for the items that require fixing.

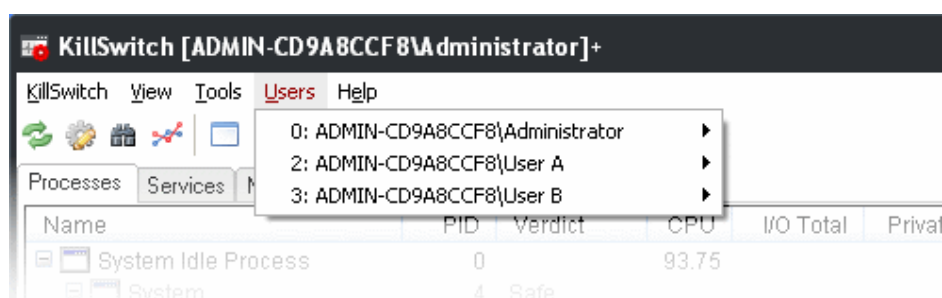
3. Click Repair. KillSwitch will automatically fix the errors in the settings of the selected item. A completion dialog will appear.



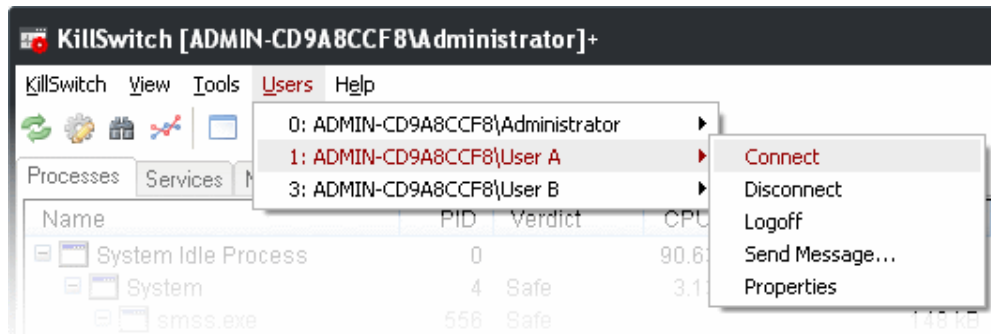
## 3.5. Managing Currently Logged-in Users

The 'Users' menu in the file menu bar lists the user(s) that have logged-in to the system either directly on to the desktop or through remote desktop connection. You can easily switch the user, log-off and communicate with a concurrently logged-in user (either locally or through remote desktop).

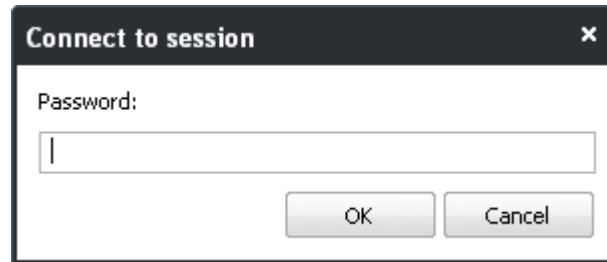
To view the the currently logged-in users, click the 'Users' menu from the file menu bar.



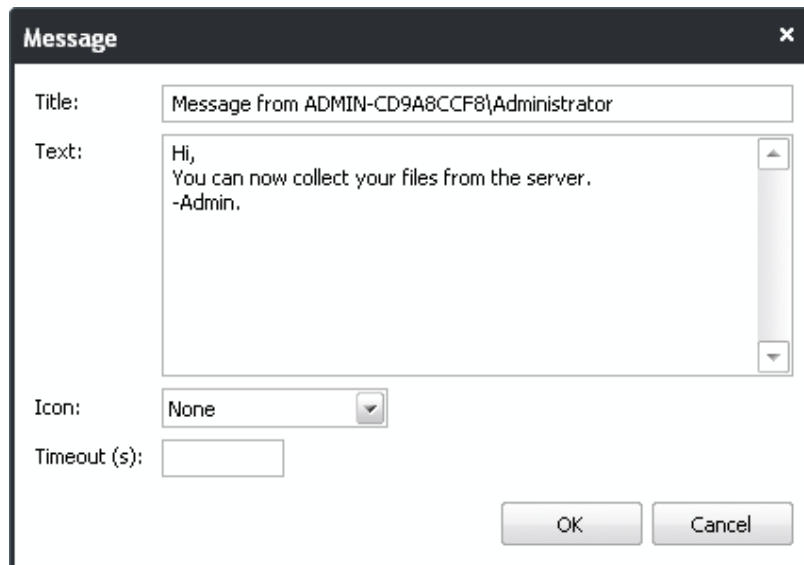
Hovering the mouse cursor over an user opens an options panel with the following options:



- **Connect** - Enables you to connect to the selected user's account to your Windows session and access the user's files, programs etc. You will be prompted to enter the password of the selected user to connect.

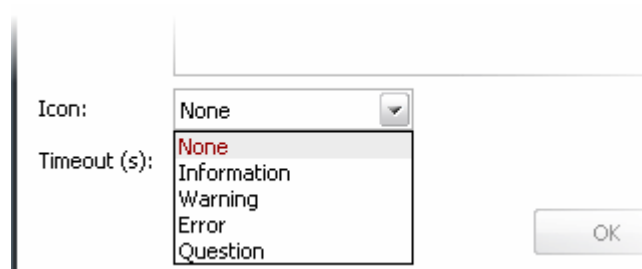


- **Disconnect** - Enables you to disconnect the connected user account from your Windows session.
- **Log off** - Forcedly log off the selected user from your computer.
- **Send Message** - Opens a message dialog that enables you to communicate your messages like information, warnings, questions etc. to the selected user.







### To send a message to a selected user

- Enter your message in the 'Text' field.
- Depending on the type of your message, select the icon to be displayed along side the message from the 'Icon' drop-down. The options available are given in the table below:

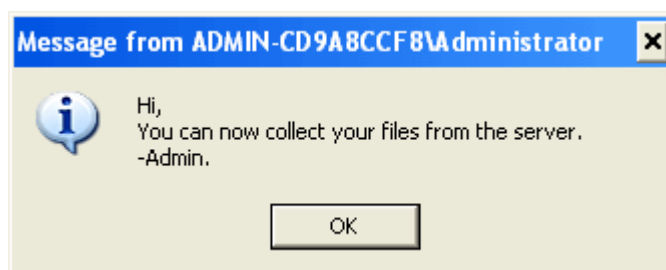




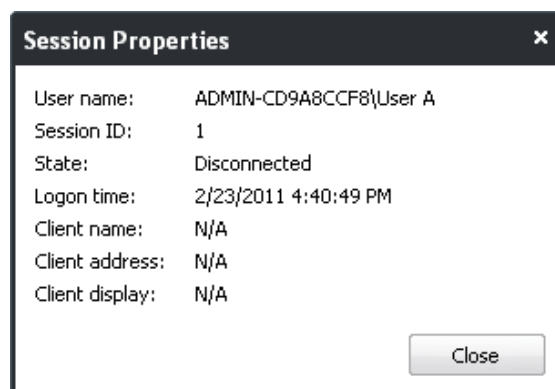
Option	Icon Displayed
None	No icon will be displayed
Information	
Warning	
Question	
Error	

- Enter the period (in seconds) till which the message has to be displayed in the user's desktop irrespective of whether the user views or not in the 'Timeout' text box. If you leave the box blank, the time out period is set infinite.
- Click OK.

The message will be displayed in the user's desktop with the icon you selected.

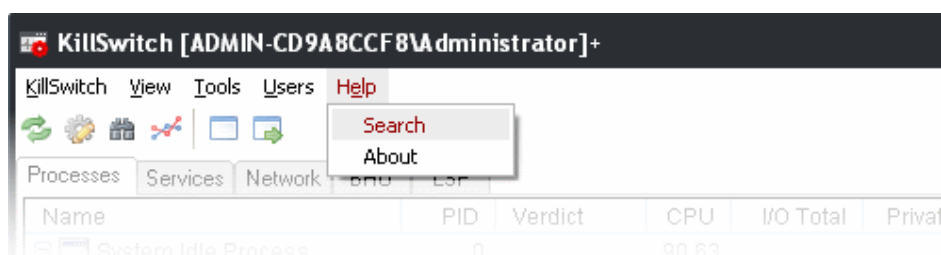


- **Properties** - Opens the 'Properties' dialog of the selected user, that displays the user's session properties.



## 3.6. Help and About Details

The 'Help' menu in the file menu bar enables you to access the online help guide and know about the version number of KillSwitch in your system.



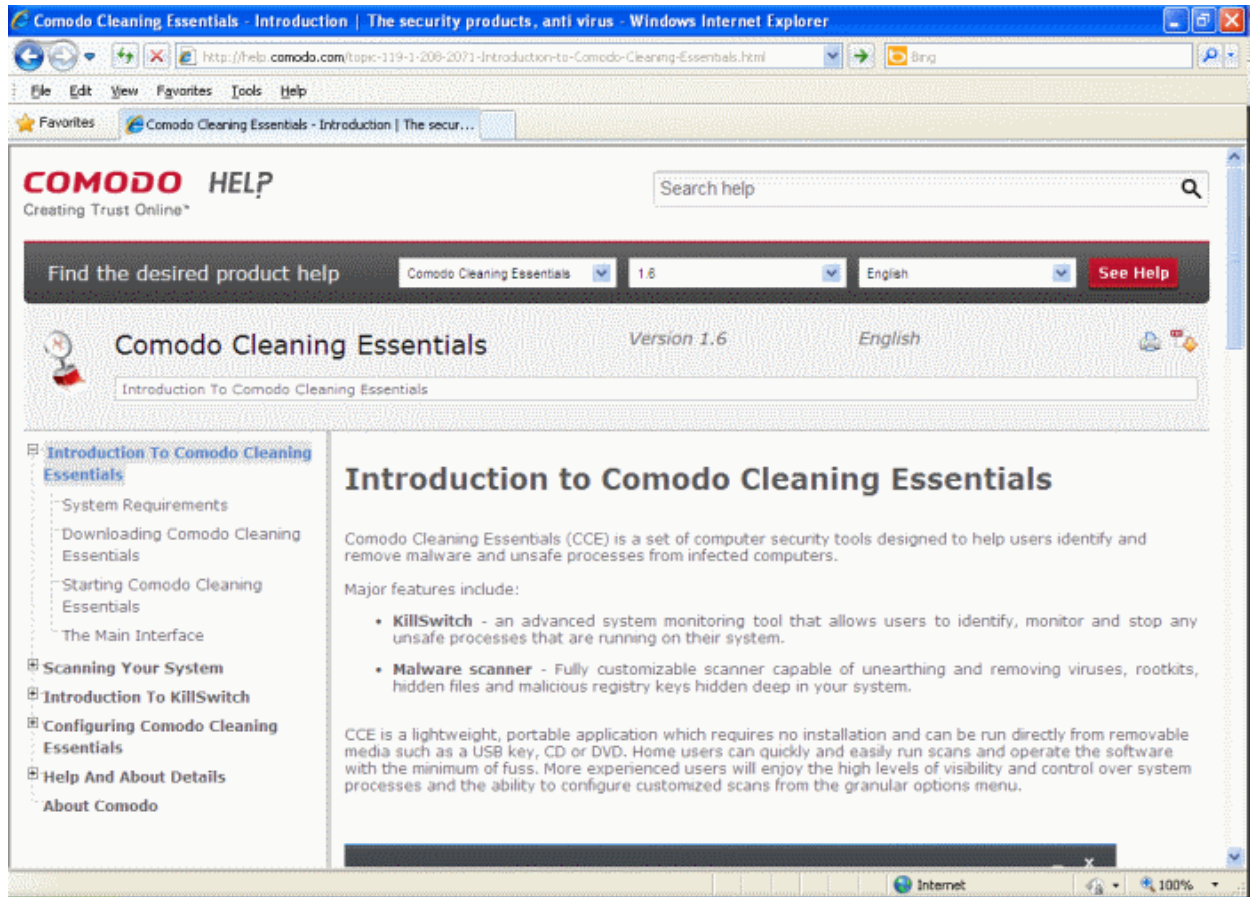
Clicking on the Help menu has the two options:

- **Search**

- **About**

## 3.6.1.1. Help

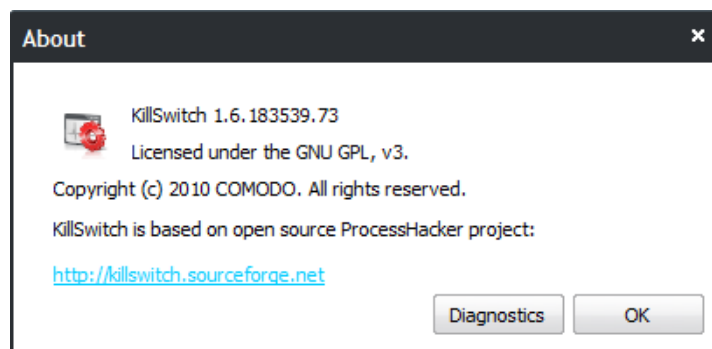
Selecting the 'Search' option from the Help menu opens the online help guide hosted at <http://help.comodo.com/>. Each area has its own dedicated page containing detailed descriptions of the application's functionality.



You can also print or download the help guide in pdf format from the webpage.

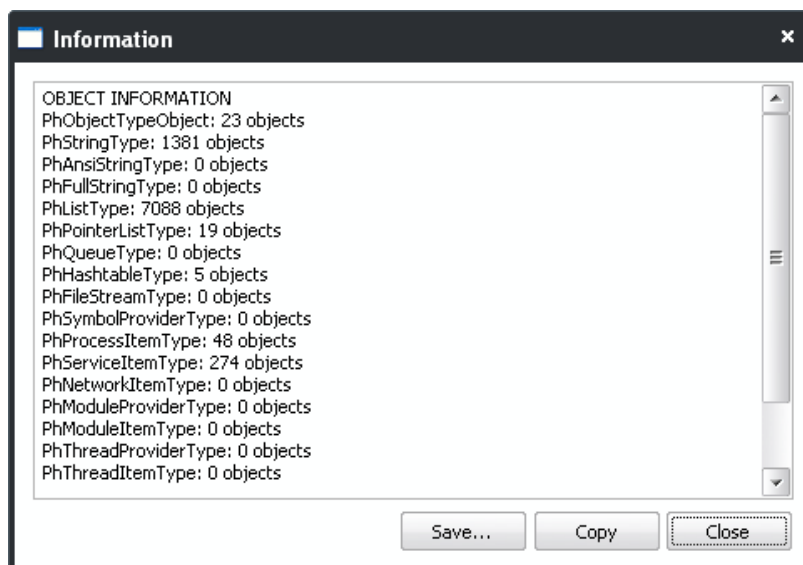
## 3.6.1.2. About

Clicking the 'About' option from the Help menu opens the 'About' information dialog of KillSwitch.



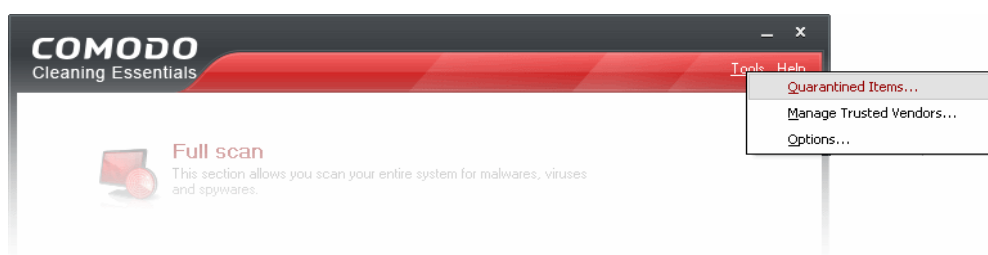
The About dialog displays the Version Number of KillSwitch, copyright information and a link to the project website.

Clicking the 'Diagnostics' button checks the integrity of the application in your system and outputs the report.



## 4. Configuring Comodo Cleaning Essentials

The 'Tools' menu at the top right enables configuring the application according to user preferences. You can manage various functions such as scanning suspicious MBR entries, automatic virus updates before, CAMAS (Comodo Automated Malware Analysis System) connection timeout and more. You will also be able to manage quarantined items and trusted vendors.



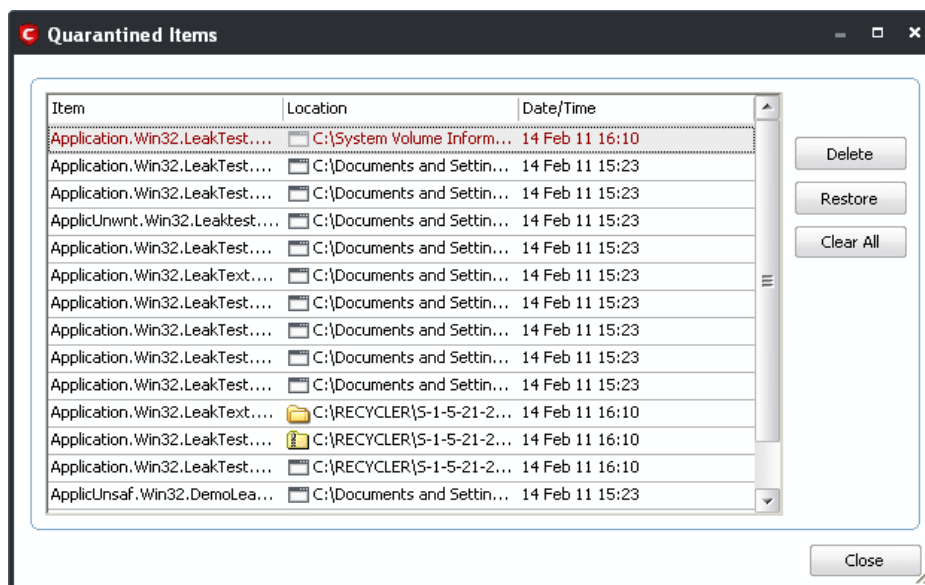
The 'Tools' menu has the following options:

- **Quarantined Items** - Enables to manage the items moved to quarantine after running scans.
- **Manage Trusted Vendors** - Enables you to add and manage the vendors as Trusted Vendor List
- **Options** - Enables you to configure the overall behavior of the application.

### 4.1. Quarantined Items

The quarantine facility removes and isolates suspicious files into a safe location before analyzing them for possible infection. Any files transferred in this fashion are encrypted- meaning they cannot be run or executed. This isolation prevents infected files from affecting the rest of your PC. If a file cannot be disinfected, then it provides a reliable safe-house until the virus database is updated- neutralizing the impact of any new virus.

To access the 'Quarantined Items' interface, Click 'Tools' > 'Quarantined Items'.



From this interface you can:

- **Delete a selected quarantined item from the system**
- **Restore a quarantined item**
- **Delete all quarantined items**

### Column Descriptions

- **Item** - Indicates which application or process propagated the event;
- **Location** - Indicates the location where the application or the file is stored;
- **Date/Time** - Indicates date and time, when the item is moved to quarantine.

### To delete a quarantined item from the system

- Select the item and Click 'Delete'.

This deletes the file from the system permanently.

### To restore a quarantined item to its original location

- Select the item and click 'Restore'.

### To remove all the quarantined items permanently

- Click 'Clear All'.

This deletes all the quarantined items from the system permanently.

**Note:** Quarantined files are stored using a special format and do not constitute any danger to your computer.

## 4.2. Manage Trusted Vendors

In Comodo Cleaning Essentials, there are two basic methods in which an application can be treated as safe. Either it has to be part of the 'Safe List' (of executables/software that is known to be safe) OR that application has to be signed by one of the vendors in the 'Trusted Software Vendor List'.

From this point:

- IF the vendor is on the 'Trusted Software Vendor' List, the application will be trusted and allowed to run.

Software publishers may be interested to know that they can have their signatures added, free of charge, to the 'master' Trusted Software Vendor List that ships to all users with CCE. Details about this can be found at the foot of this page.

To access the 'Trusted Software Vendors' interface, Click 'Tools' > 'Manage Trusted Vendors'.



[Click here to read background information on digitally signing software](#)

[Click here to learn how to Add / Define a user-trusted vendor](#)

[Software Vendors - click here to find out about getting your software added to the list](#)

## Background

Many software vendors digitally sign their software with a code signing certificate. This practice helps end-users to verify:

- Content Source:** The software they are downloading and are about to install really comes from the publisher that signed it.
- Content Integrity:** That the software they are downloading and are about to install has not be modified or corrupted since it was signed.

In short, users benefit if software is digitally signed because they know who published the software and that the code hasn't been tampered with - that are are downloading and installing the genuine software.

The 'Vendors' that digitally sign the software to attest to it's probity are the software publishers. These are the company names you see listed in the first column in the graphic above.

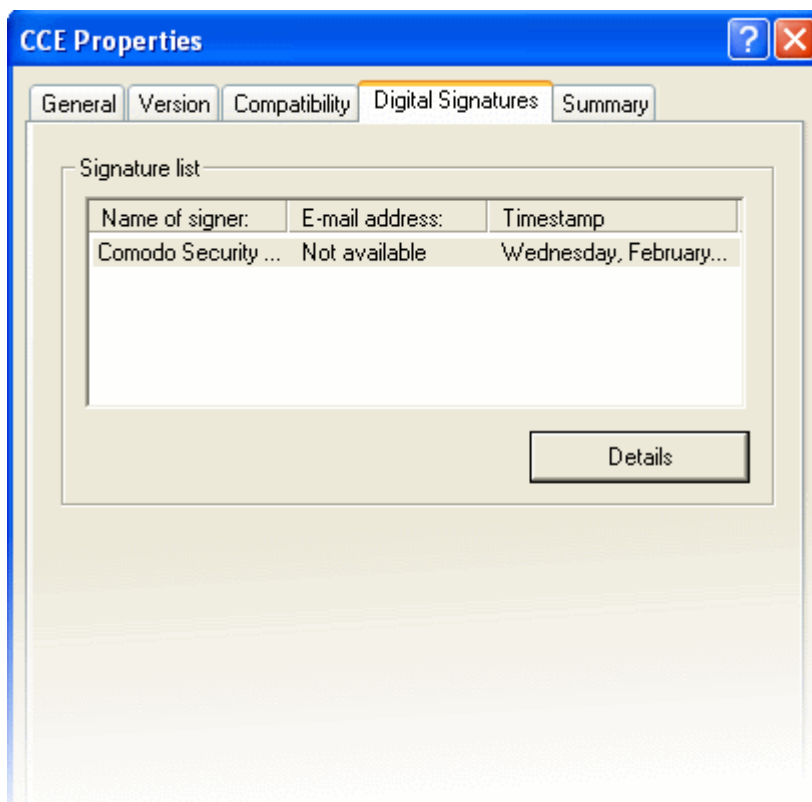
However, companies can't just 'sign' their own software and expect it to be trusted. This is why each code signing certificate is counter-signed by an organization called a 'Trusted Certificate Authority'. 'Comodo CA Limited' and 'Verisign' are two examples of a Trusted CA's and are authorized to counter-sign 3rd party software. This counter-signature is critical to the trust process and a Trusted CA only counter-signs a vendor's certificate after it has conducted detailed checks that the vendor is a legitimate company.

If a file is signed by a Trusted Software Vendor and the user has enabled 'Trust Applications that are digitally signed by Trusted Software Vendors' then it will be automatically trusted by CCE (if you would like to read more about code signing certificates, see <http://www.instantssl.com/code-signing/>).

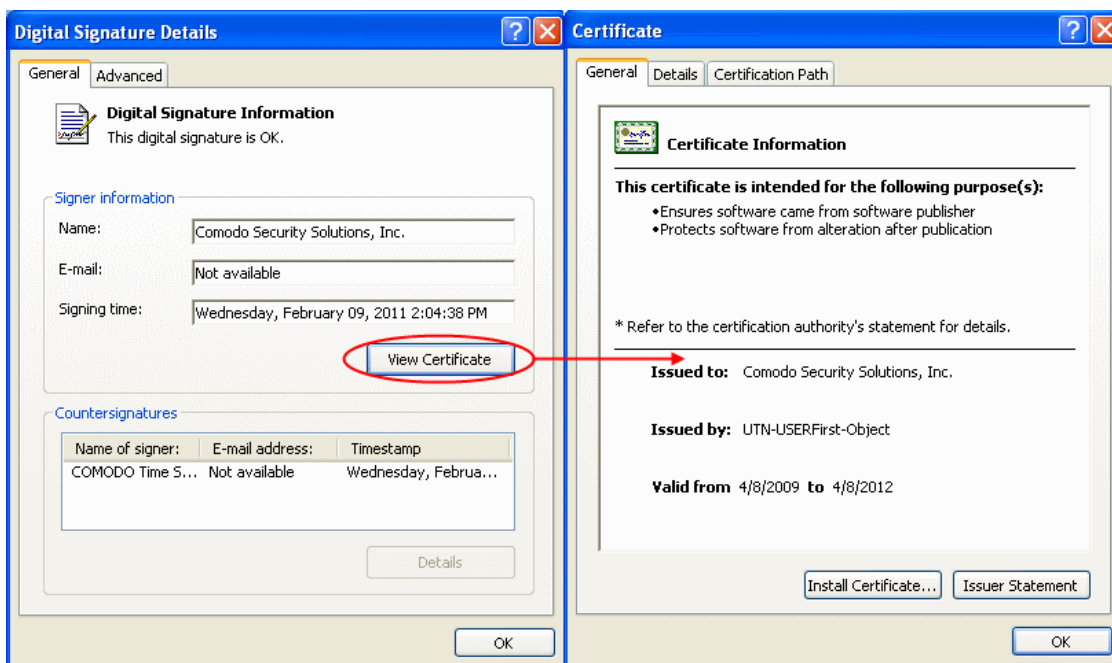
One way of telling whether an executable file has been digitally signed is checking the properties of the .exe file in question. For example, the main program executable for CCE is called 'cce.exe' and has been digitally signed.

- Browse to the (default) installation directory of Comodo Cleaning Essentials.
- Right click on the file cce.exe.
- Select 'Properties' from the menu.
- Click the tab 'Digital Signatures (if there is no such tab then the software has not been signed).

This displays the name of the CA that signed the software as shown below:



Click the 'Details' button to view digital signature information. Click 'View Certificate' to inspect the actual code signing certificate. (see below)



It should be noted that the example above is a special case in that Comodo, as creator of 'cce.exe', is both the signer of the software and, as a trusted CA, it is also the counter-signer (see the 'Countersignatures' box). In the vast majority of cases, the signer or the certificate (the vendor) and the counter-signer (the Trusted CA) are different. **See this example** for more details.

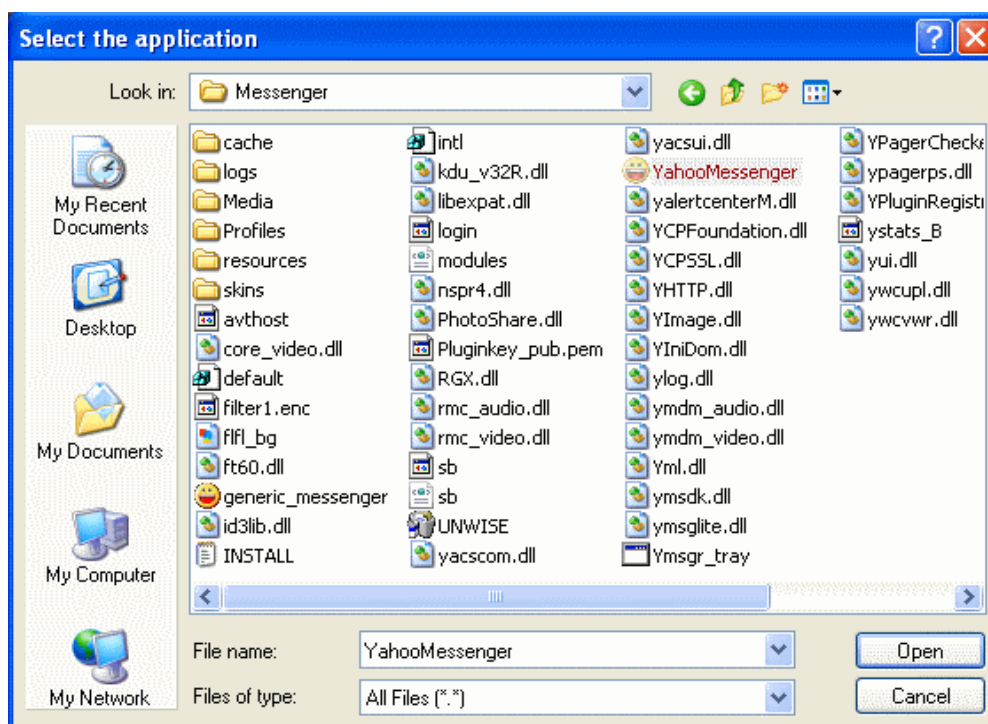
## Adding and Defining a User-Trusted Vendor

A software vendor can be added to the local 'Trusted Software Vendors' list by reading the vendor's signature from an executable file on your local drive.

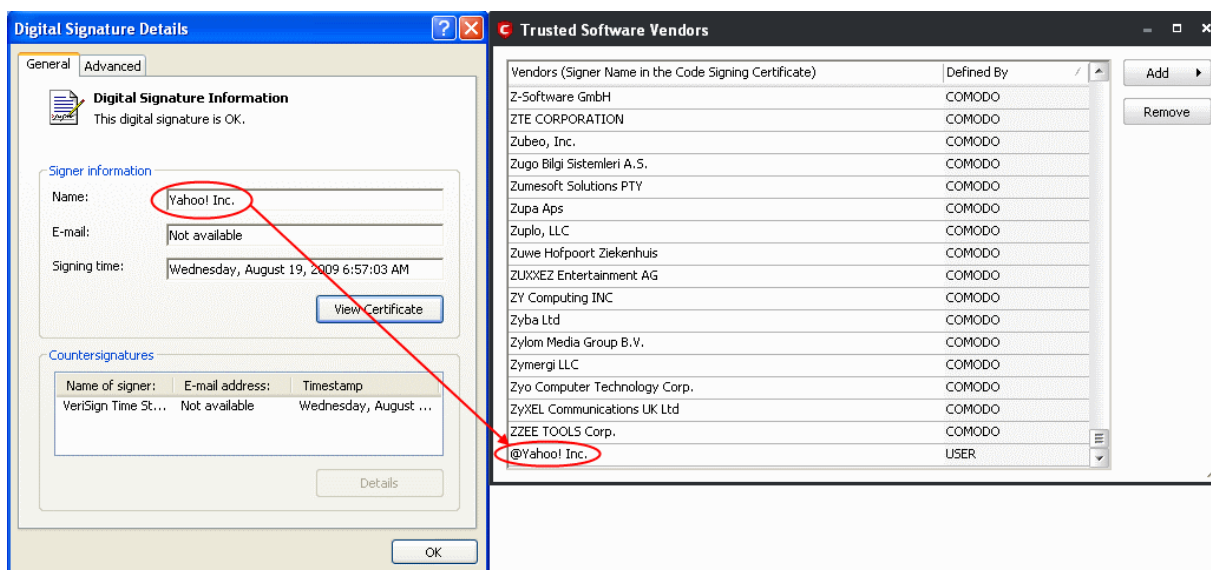




Click the add button on the right hand side and select 'Read from a signed executable...'. Browse to the location of the executable your local drive. In the example below, we are adding the executable 'YahooMessenger.exe'.



After clicking 'Open', CCE checks that the .exe file is signed by the vendor and counter-signed by a Trusted CA. If so, the vendor (software signer) is added to the Trusted Vendor list (TVL):



In the example above, CCE was able to verify and trust the vendor signature on YahooMessenger.exe because it had been counter-signed by the trusted CA 'Verisign'. The software signer 'Yahoo! Inc.' is now a Trusted Software Vendor and is added to

the list. All future software that is signed by the vendor 'Yahoo! Inc.' is automatically added to the Comodo Trusted Vendor list.

### The Trusted Vendor Program for Software Developers

Software vendors can have their software added to the default Trusted Vendor List that is shipped with CCE. This service is free of cost and is also open to vendors that have used code signing certificates from any Certificate Authority. Upon adding the software to the Trusted Vendor list, CCE automatically trusts the software and does not generate any warnings or alerts on installation or use of the software.

The vendors have to apply for inclusion in the Trusted Vendors list through the sign-up form at <http://internetsecurity.comodo.com/trustedvendor/signup.php> and make sure that the software can be downloaded by our technicians. Our technicians check whether:

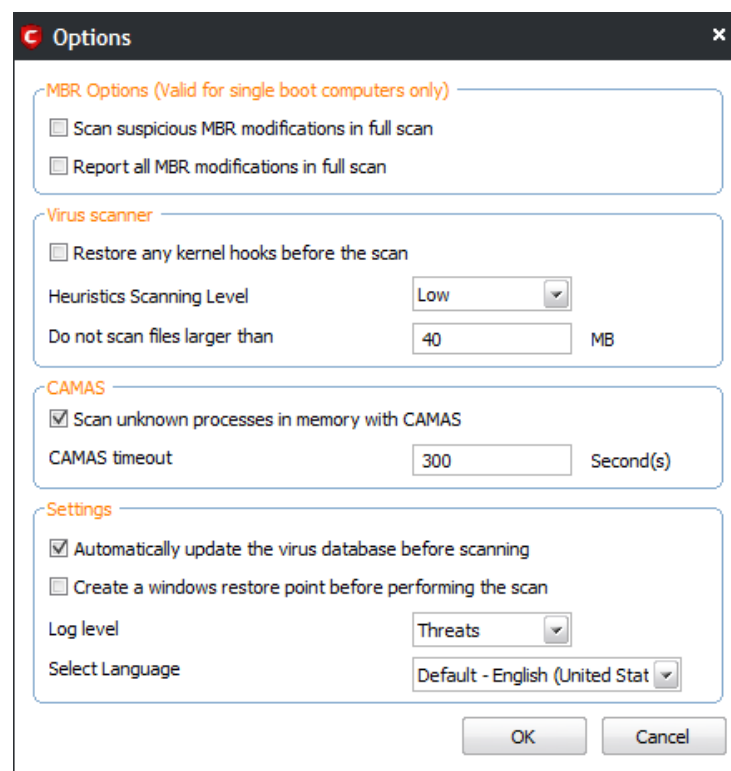
- The software is signed with a valid code signing certificate from a trusted CA;
- The software does not contain any threats that harm a user's PC;

before adding it to the default Trusted Vendor list of the next release of CCE.

More details are available at <http://internetsecurity.comodo.com/trustedvendor/overview.php>.

## 4.3. Options

The Options interface enables you to configure the overall behavior of the application. To access the Options interface, click 'Tools' > 'Options'.



### MBR Options

- **Scan for suspicious MBR entries in full scan** - When selected, CCE will automatically scan MBR (master boot record) for unknown or suspicious entries during full scan.
- **Report all MBR modifications in full scan** - When selected, CCE will record MBR modifications, if any, in the log file.

**Note:** The settings under MBR options are valid only for single boot computers and not applicable for multi-operating system computers.



## Virus Scanner Settings

- **Restore any kernel hooks before the scan** - When selected, kernel hooks that are unhooked will be restored before the scanning process. This option is for advanced users only and you will be warned when you modify this option.
- **Heuristics Scanning/Level** - CCE employs various heuristic techniques to identify previously unknown viruses and Trojan horses. 'Heuristics' describes the method of analyzing the code of a file to ascertain whether it contains code typical of a virus. If it is found to do so then the application deletes the file or recommends it for quarantine. Heuristics is about detecting virus-like behavior or attributes rather than looking for a precise virus signature that matches a signature on the virus blacklist.

This is a quantum leap in the battle against malicious scripts and programs as it allows the scan engine to 'predict' the existence of new viruses - even if it is not contained in the current virus database.

The drop-down menu allows you to select the level of Heuristic scanning from the four levels:

- **Off** - Selecting this option disables heuristic scanning. This means that virus scans only use the 'traditional' virus signature database to determine whether a file is malicious or not.
- **Low** - 'Lowest' sensitivity to detecting unknown threats but will also generate the fewest false positives. This setting combines an extremely high level of security and protection with a low rate of false positives. Comodo recommends this setting for most users.
- **Medium** - Detects unknown threats with greater sensitivity than the 'Low' setting but with a corresponding rise in the possibility of false positives.
- **High** - Highest sensitivity to detecting unknown threats but this also raises the possibility of more false positives too.
- **Do not scan files larger than** - This box allows you to set a maximum size (in MB) for the individual files to be scanned during manual scanning. Files larger than the size specified here, are not scanned. Default = 40 MB

## CAMAS Settings

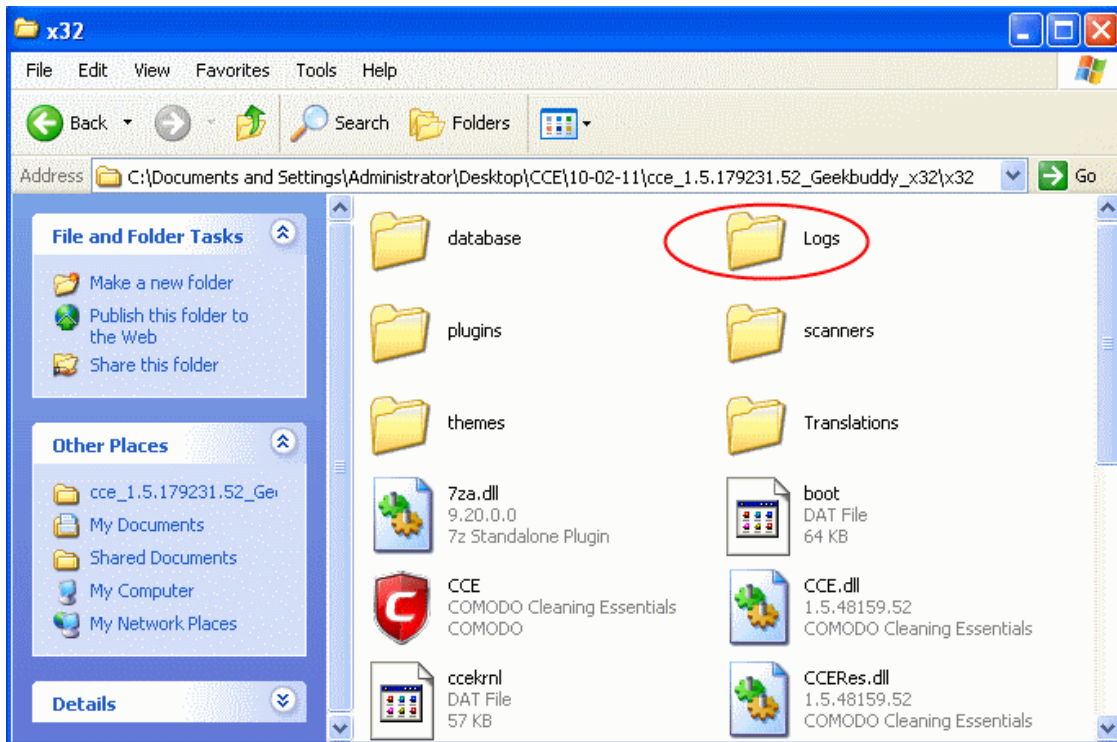
**CAMAS** - CAMAS (Comodo Automated Malware Analysis System) is a cloud based analysis system where the submitted files will undergo a thorough inspection by our cloud virus scanning and behavior monitoring systems to try to establish whether they contain malicious code. If the file exhibits malicious behavior, it will be added to the global blacklist. Once the global lists have been updated, any other users that have the same file on their machines will receive an almost instant verdict as to the file's safety.

- **Scan unknown processes in memory with CAMAS** - When this check box is selected, any unknown process or processes in memory will be automatically submitted to CAMAS (Comodo Automated Malware Analysis System).
- **CAMAS timeout** - This box allows you to set the time (in seconds) for which the files will be submitted to CAMAS. If the timeout is exceeded then CCE will stop attempting to contact the CAMAS servers and it is possible that no result will be returned to you.

## Miscellaneous Settings

- **Automatically update the virus database before scanning** - When selected, CCE checks for and downloads the latest virus updates from the Comodo website before scanning.
- **Create a Windows restore point before performing the scan** - When selected, CCE will create a Windows restore point before embarking on the scanning process. Should problems occur afterwards, you will be able to restore your system to the state just before you started the scan.
- **Log level** - This drop-down box allows you to select options for CCE event logs. There are two main types of log file - KillSwitch logs and CCE (scan) logs. The following options apply to both types of log:
  - **Disable** - If you select this option, CCE will not create any log files.
  - **Threats** - If this option is selected, CCE will generate log reports containing files that it has detected as threats.
  - **All** - If this option is selected, CCE will generate log reports for all files that have been scanned and will record all events. The log file will contain system information, cleanup results, details about the file path, whether it is malicious, the action taken and whether the action has been implemented.

Logs are saved in the 'Logs' sub-directory of the CCE folder:



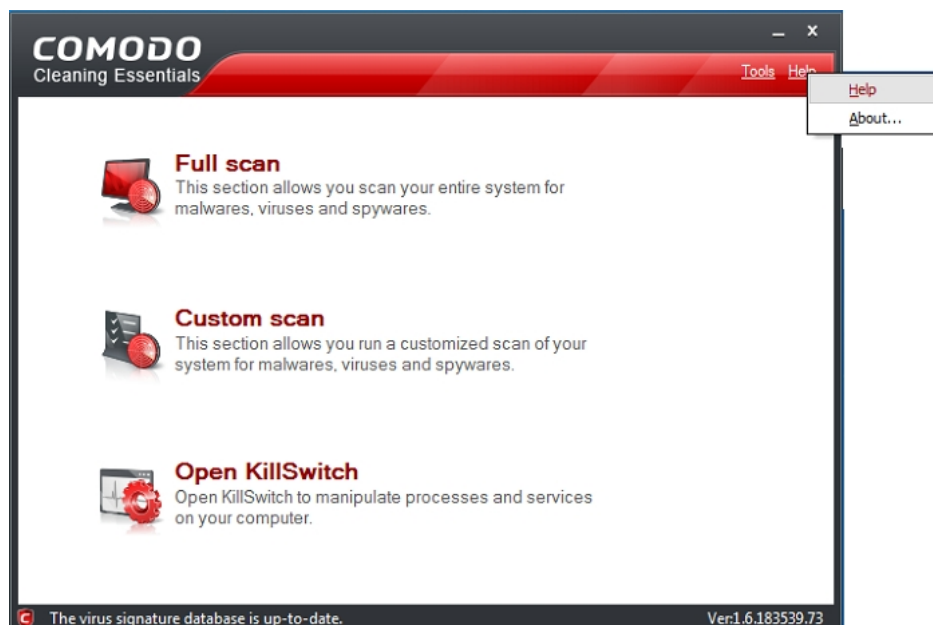
Double-click or right click and open the Logs folder. The folder will contain logs stored as time stamped text files.

**Select Language-** CCE is available in several languages and the default language is US English.

- Click 'OK' for the settings to take effect .

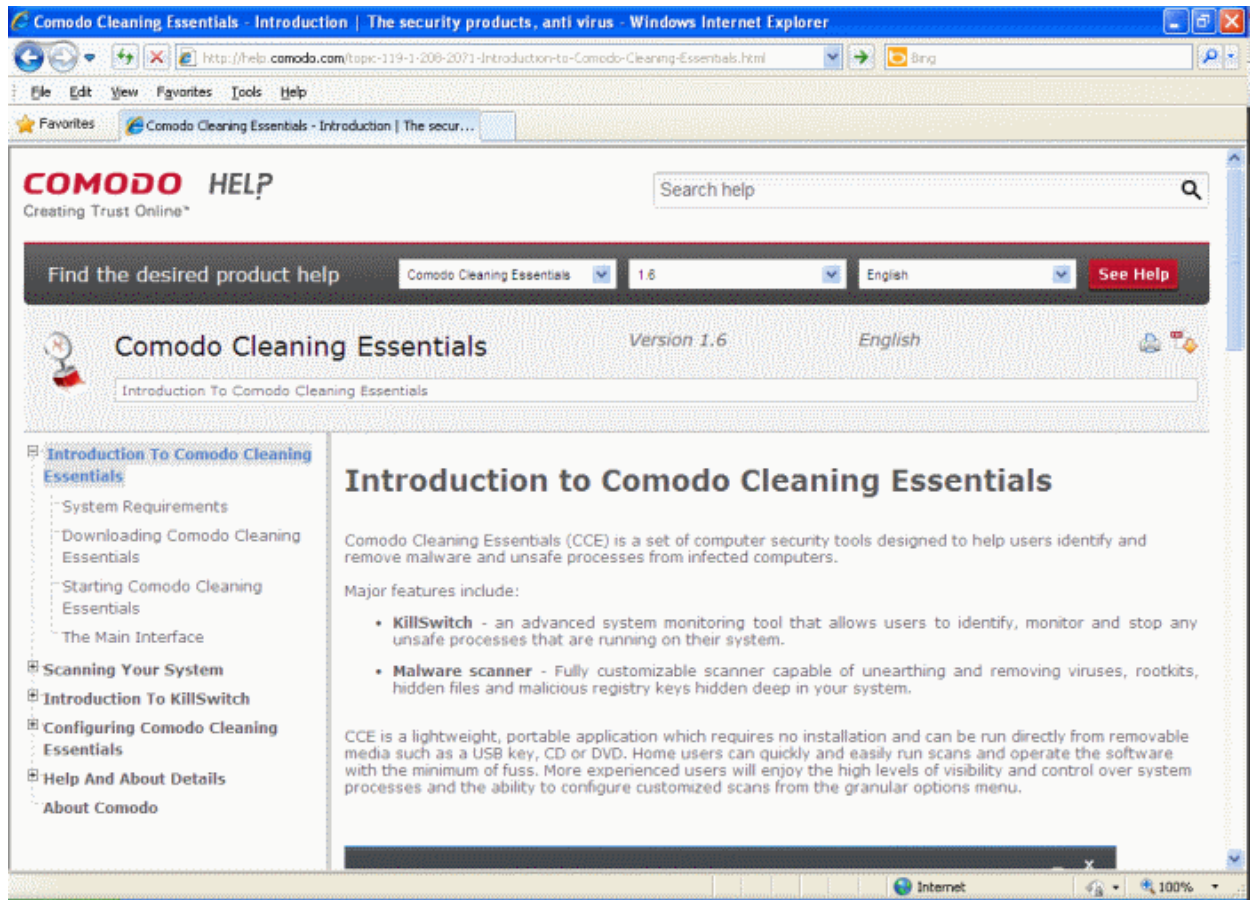
## 5.Help and About Details

The **Help** link at the top right corner of the main interface enables you to access the online help guide and know about the version number of CCE in your system.



## 5.1. Help

Click the Help link to open the online help guide hosted at <http://help.comodo.com/>. Each area has its own dedicated page containing detailed descriptions of the application's functionality.



You can also print or download the help guide in .pdf format from the webpage.

## 5.2. About

Click 'About' to view the 'About' information dialog.



You can view information about the Version Number of Comodo Cleaning Essentials and virus database that is in your computer and the unique serial number of the application. The serial number is used to identify the application currently used in your system and is necessary for support purposes.

## About Comodo

The Comodo companies are leading global providers of Security, Identity and Trust Assurance services on the Internet. Comodo CA offers a comprehensive array of PKI Digital Certificates and Management Services, Identity and Content Authentication (Two-Factor - Multi-Factor) software, and Network Vulnerability Scanning and PCI compliance solutions. In addition, with over 10,000,000 installations of its threat prevention products, Comodo Security Solutions maintains an extensive suite of endpoint security software and services for businesses and consumers.

Continual innovation, a core competence in PKI and a commitment to reversing the growth of Internet-crime distinguish the Comodo companies as vital players in the Internet's ongoing development. Comodo, with offices in the US, UK, China, India, Romania and the Ukraine, secures and authenticates the online transactions and communications for over 200,000 business customers and millions of consumers, providing the intelligent security, authentication and assurance services necessary for trust in on-line transactions.

### **Comodo Security Solutions, Inc.**

525 Washington Blvd. Jersey City,  
NJ 07310

United States

Tel: +1.888.256.2608

Tel: +1.703.637.9361

Email: [EnterpriseSolutions@Comodo.com](mailto:EnterpriseSolutions@Comodo.com)

### **Comodo CA Limited**

3rd Floor, 26 Office Village, Exchange Quay, Trafford Road,  
Salford, Greater Manchester M5 3EQ,

United Kingdom.

Tel : +44 (0) 161 874 7070

Fax : +44 (0) 161 877 1767

For additional information on Comodo - visit <http://www.comodo.com>.