



Comodo Cleaning Essentials

Software Version 1.6

User Guide Guide Version 1.6.042111

> Comodo Security Solutions 525 Washington Blvd. Jersey City, NJ 07310

Table of Contents

1. Introduction to Comodo Cleaning Essentials	4
1.1.System Requirements	5
1.2.Downloading Comodo Cleaning Essentials	5
1.3.Starting Comodo Cleaning Essentials	
1.4.The Main Interface	6
2.Scanning Your System	7
2.1.Full Scan	8
2.2.Custom Scan	14
3.Introduction to KillSwitch	25
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	
3.1.3.Replacing Windows Task Manager with KillSwitch	27
3.2.The Main Interface	
3.2.1.The System Tray Icons	
3.3.Viewing and Handling Processes and Services	
3.3.1.Processes	
3.3.1.1.Stopping, Starting and Handling the Processes	
3.3.1.2.Viewing Properties of a Process	40
3.3.1.3.Searching for Handles or DLLs	56
3.3.2.Services	
3.3.2.1.Stopping, Starting and Deleting the Services	
3.3.2.2.Viewing the Properties of a Service	59
3.3.3.Network Connections	
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	
3.4.5.Scanning Your System for Hidden Processes	
3.4.6.Viewing the Page Files in Your System	
3.4.7.Verifying Authenticity of Applications	
3.4.8.Repairing Windows Settings and Features	86
3.5.Managing Currently Logged-in Users	87
3.6.Help and About Details	
3.6.1.1.Help	
3.6.1.2.About	
4.Configuring Comodo Cleaning Essentials	91

COMODO Creating Trust Online*

4.1.Quarantined Items	
4.2.Manage Trusted Vendors	
4.3.0ptions	
5.Help and About Details	
5.1.Help	
5.2.About	
About Comodo	

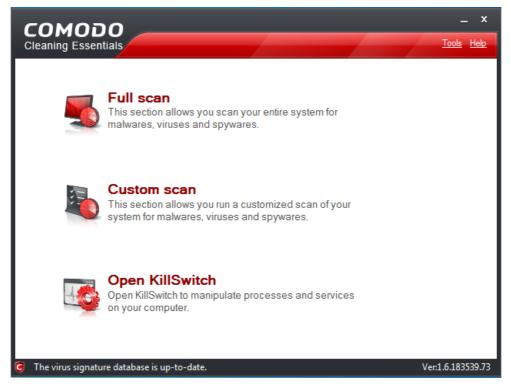
1. Introduction to Comodo Cleaning Essentials

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

64 Bit Operating Systems:

http://download.com/doc/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.

Ģ	COMODO	Cleaning Essentials License Agreement	×
		END USER LICENSE AND SUBSCRIBER AGREEMENT COMODO CLEANING ESSENTIALS	A III
	DOWNLOA ("PRODUCT BY CLICKIN READ THIS BE BOUND NOT DOWN	T - PLEASE READ THESE TERMS CAREFULLY BEFORE DING, INSTALLING, OR USING COMODO'S CLEANING ESSENTIALS TS"). BY DOWNLOADING, INSTALLING, OR USING THE PRODUCTS, OR IG ON "I ACCEPT" BELOW, YOU ACKNOWLEDGE THAT YOU HAVE AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO BY ITS TERMS. IF YOU DO NOT AGREE TO THE TERMS HEREIN, DO ILOAD OR USE THE SOFTWARE, SUBSCRIBE TO OR USE THE , OR CLICK ON "I ACCEPT".	
		er license and subscriber agreement is between you ("you" or "Subscriber"), individual or as a business entity, and either:	
	a.	if you are not located in China, Comodo Security Solutions, Inc., which has its principal place of business at 525 Washington Blvd., Suite 1400, Jersey City, New Jersey 07310, or	
	b.	if you are located in China, Beijing Comodo Software Development Co. Ltd.,	¥
(Print	Accept Decline	•

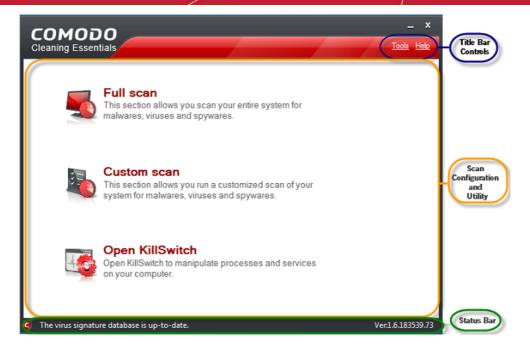
• Read the agreement and click 'Accept'. If you do not want to use the application, click 'Decline'.

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.

COMODO Creating Trust Online*



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.

COMODO Creating Trust Online*

Refer to the following sections for more details on:

- Full Scan
- Custom Scan

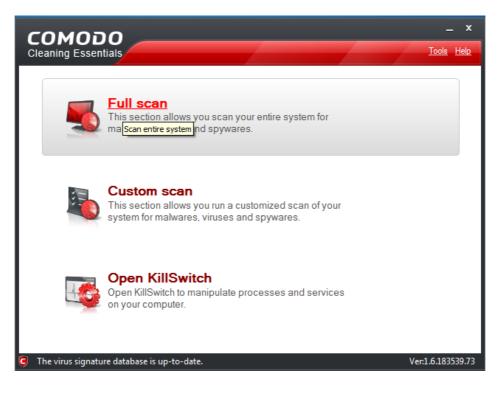
2.1. Full Scan

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.

COMODO Cleaning Essentials(21)
As the part of the scanning process, your computer will now be restarted in order to perform the rootkit scanning. Would you like to restart it now?
Yes No

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.

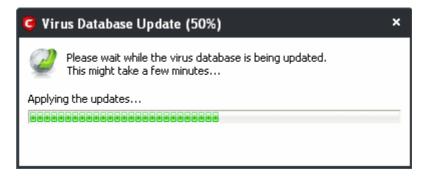


The restart dialog window will start a count down from 30 and if you do not choose either 'Yes' or 'No' option, the system will automatically restart when the count down reaches 0.

- 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.

🧯 COMODO Cleaning Essentials - Scanning 🛛 🛛 🗕 🗆 🗙									
	Scanning: Status:	Memory C:\Program Files\COMODO\Unite\ThinVn	c.exe						
 Objects Scanned Threats Found: 	d: 36 O	Start Time: Duration:	2/10/2011 2:08:54 PM 00:00:17						
🗹 Show on top		🕕 Pause	🚺 Stop Scan						

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

🤤 COMODO Cleaning Essentials - Scan Finished 🛛 🗕 🗖 🗙							
	Scanning: Full scan Status: Scan Finished						
Objects Scanned Threats Found:	d: 268136 26	Start Time: Duration:	2/10/2011 2:08:54 PM 00:57:52				
🗹 Show on top			Results				

• 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).

🤤 сом	0D0 Cleaning Essentials- Scan Results			×
	Threat Name	Risk		-
	Application.Win32.LeakTest.~TMZ@1	Low		
	C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\Extracte			
	C:\RECYCLER\5-1-5-21-2052111302-602609370-1801674531-500\Dc4.dll			≡
	Application.Win32.LeakTest.dmc@1	Low	_	3
	— I C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\cpil_suite			
	— I C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\Extracte			
	C:\System Volume Information_restore{90A369D4-5FDD-4749-B5CB-E3A515			
	Application.Win32.LeakText.~TMY@1	Low	-	3
	—			
	C:\RECYCLER\S-1-5-21-2052111302-602609370-1801674531-500\Dc1.exe			
	Application.Win32.LeakTest.~dmd@1	Low	-	
	— I C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\Extracte			
	—			
	— C:\RECYCLER\S-1-5-21-2052111302-602609370-1801674531-500\Dc2.dll			
	C:\RECYCLER\S-1-5-21-2052111302-602609370-1801674531-500\Dc3.dll			
	C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\FPR.zip	Low	-	
	Application.Win32.LeakTest.~FPR@(9460415, 8073497, 9458817,)	Low	_	
	Clea	n •	Ignore	•

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'.

	Threat Name	Risk		-
	Application.Win32.LeakTest.~TMZ@1	Low 😑		
Z	C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\Extracte			
	C:\RECYCLER\5-1-5-21-2052111302-602609370-1801674531-500\Dc4.dll			Ξ
	Application.Win32.LeakTest.dmc@1	Low 🗧		
M	- 📄 C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\cpil_suite			
M	— C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\Extracte			1
	C:\System Volume Information_restore{90A369D4-5FDD-4749-B5CB-E3A515			
	Application.Win32.LeakText.~TMY@1	Low 🗧		1
	— C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\Extracte			-
	C:\RECYCLER\5-1-5-21-2052111302-602609370-1801674531-500\Dc1.exe			
	Application.Win32.LeakTest.~dmd@1	Low 🗧		Ē.
	— C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\Extracte			
M	— C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\Extracte			
M	– 📄 C:\RECYCLER\5-1-5-21-2052111302-602609370-1801674531-500\Dc2.dll			
	C:\RECYCLER\5-1-5-21-2052111302-602609370-1801674531-500\Dc3.dll			
	C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\FPR.zip	Low 🗧		1
	Application.Win32.LeakTest.~FPR@(9460415, 8073497, 9458817,)	Low 🗧		
	Clear	1 🔻	Ignore	+

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'.

~	Threat Name R	lisk		٢.,
	Application.Win32.LeakTest.~TMZ@1	ow 😑		
	– 📄 C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\Extracte			
	C:\RECYCLER\S-1-5-21-2052111302-602609370-1801674531-500\Dc4.dll			
	Application.Win32.LeakTest.dmc@1	ow 😑	_	3
M	— I C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\cpil_suite			
M	— I C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\Extracte			1
M	C:\System Volume Information_restore{90A369D4-5FDD-4749-B5CB-E3A515			
	Application.Win32.LeakText.~TMY@1	ow 📒	_	5
M	— I C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\Extracte			
M	C:\RECYCLER\S-1-5-21-2052111302-602609370-1801674531-500\Dc1.exe			
	Application.Win32.LeakTest.~dmd@1	ow 📒	_	3
M	— I C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\Extracte			
	— I C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\Extracte			
	—			
	└ 📄 C:\RECYCLER\S-1-5-21-2052111302-602609370-1801674531-500\Dc3.dll			
	C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\FPR.zip	ow 📒	_	5
	LeakTest.~FPR@(9460415, 8073497, 9458817,)	ow 📒	_	۶P

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.

	Threat Name	Risk		
	Application.Win32.LeakTest.~TMZ@1	Low		
	 C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\Extracte 			
	└ 📄 C:\RECYCLER\5-1-5-21-2052111302-602609370-1801674531-500\Dc4.dll			E
	Application.Win32.LeakTest.dmc@1	Low	_	
	—			
	— I C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\Extracte			
	C:\System Volume Information_restore{90A369D4-5FDD-4749-B5CB-E3A515			
	Application.Win32.LeakText.~TMY@1	Low	_	
	— I C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\Extracte			
	C:\RECYCLER\S-1-5-21-2052111302-602609370-1801674531-500\Dc1.exe			
	Application.Win32.LeakTest.~dmd@1	Low	_	
	— C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\Extracte			
	— C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\Extracte			
	— C:\RECYCLER\S-1-5-21-2052111302-602609370-1801674531-500\Dc2.dll			
M	C:\RECYCLER\5-1-5-21-2052111302-602609370-1801674531-500\Dc3.dll			
M	C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\FPR.zip	Low	_	
	🖵 Application.Win32.LeakTest.~FPR@(9460415, 8073497, 9458817,)	Low	_	

The selected applications will be deleted from your system.

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

Т	hreat Name	Risk		
	Application.Win32.LeakTest.~TMZ@1	Low	_	_
	— C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\Extracte			
	└ 📄 C:\RECYCLER\5-1-5-21-2052111302-602609370-1801674531-500\Dc4.dll			=
	Application.Win32.LeakTest.dmc@(117030777, 1)	Low	_	-
	— C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\Extracte			
	C:\System Volume Information_restore{90A369D4-5FDD-4749-B5CB-E3A515			
	C:\System Volume Information_restore{90A369D4-5FDD-4749-B5CB-E3A515			
1	📙 C:\System Volume Information_restore{90A369D4-5FDD-4749-B5CB-E3A515			
	Application.Win32.LeakText.~TMY@(117030909, 1)	Low	_	
	C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\Extracte			
	C:\RECYCLER\5-1-5-21-2052111302-602609370-1801674531-500\Dc1.exe			
1	C:\System Volume Information_restore{90A369D4-5FDD-4749-B5CB-E3A515			
1	📙 C:\System Volume Information_restore{90A369D4-5FDD-4749-B5CB-E3A515			
	Application.Win32.LeakTest.~dmd@(117030827, 1)	Low	_	
	C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\Extracte			
	— C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\Extracte			
1	C:\RECYCLER\5-1-5-21-2052111302-602609370-1801674531-500\Dc2.dll			-

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.

COMODO Cleaning Esse	entials(23)
threats are removed or q services.	e restarted in order to verify that all selected quarantined, and continue to scan for hidden Yes No

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

•

Restart system and continue scan
Exit
🔨 🖨 🔨 📣 🚳 🖽 11140 MM

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.

뎍 Cleanup results - (3 Threats)			×
Threat Name	Operation	Status	
Application.Win32.LeakTest.dmc@1 (1)			
C:\System Volume Information_restore{90A369D4-5FDD-4749-B5CB-E3A5	Disinfect	OK	
Application.Win32.LeakTest.dmc@117030777 (1)			
C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\Extract	Ignore and report	OK	
Application.Win32.LeakTest.~TMZ@1 (1)			
C:\RECYCLER\5-1-5-21-2052111302-602609370-1801674531-500\Dc4.dll	Disinfect	OK	
		Close	

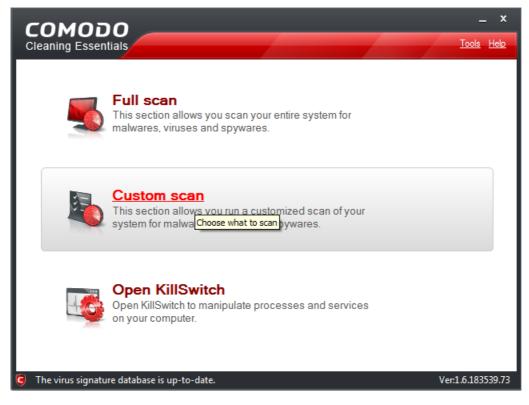
• Click the 'Close' button and the application will be closed.

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.

COMODO Creating Trust Online*

Comodo Cleaning Essentials - User Guide

Custom Scan Setting	×
Scan options	
Scan memory on start	
Scan critical areas	
Scan critical system settings	
Scan hidden registry objects	
Scan selected drives for hidden files/folders	
Don't scan for viruses	
Scan Target	
■ My Computer	Add Files
└────────────────────────────────────	Add Folder
	Remove
ОК	Cancel

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.

COMODO Creating Trust Online*

- 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.

Scan Target	
My Computer	Add Files
Local Disk(C:\)	Add Folder
	Remove
	OK Cancel
	14

To add files and run a custom scan

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

Scan Target	
My Computer	Add Files
	Add Folder
	Remove
	OK Cancel

Browse to the required file and click Open

.

Open								? 🛛
Look in:	🚞 cpil_suite		*	G	ø	ø	•	
My Recent Documents Desktop My Documents	CPIL2.dll							
My Computer	File name:	CPILSuite				*		Open
My Network	Files of type:	All Files(*.*) Open as read-only				*		Cancel

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

Scan Target	Add Files
	Add Folder
Custom C:\Documents and Settings\Administrator\Deskt	
4 III •	Remove
ОК	Cancel

• 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...

COMODO Creating Trust Online*

🤤 COMODO Clean	ing Essen	tials - Scanning	- • ×
	Scanning: Status:	Infected Files C:\Documents and Settings\Administrato	r\Desk\CPILSuite.exe
 Objects Scanned Threats Found: 	d: 1 O	Start Time: Duration:	2/11/2011 2:59:40 PM 00:00:03
🗹 Show on top		🕕 Pause	🔾 Stop Scan

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

🤤 COMODO Clean	ing Essen	tials - Scan Finished		- • ×
	Scanning: Status:	Custom scan Scan Finished		
 Objects Scanned Threats Found: 	d: 1 1		art Time: uration:	2/11/2011 2:59:40 PM 00:00:09
Show on top				Results

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

COMODO Creating Trust Online

🤤 сом	10D0 Cleaning Essentials- Scan Results		-	- x
	Threat Name	Risk		-
	Application.Win32.LeakTest.dmc@1	Low		
	🖵 📄 C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\Extracted fil			
	Clean	-	Ignore	
				/

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

Scan Target My Computer Scan Target My Computer Scan Disk(C:\) New Volume(D:\)	Add Files Add Folder
	Remove OK Cancel

Browse to required folder and click 'OK'

I.

COMODO Creating Trust Online

Browse For Folder	?×
Select and add a folder for custom scan.	
🞯 Desktop	
🕀 🛅 My Documents	
표 😼 My Computer	
표 🧐 My Network Places	
🥑 Recycle Bin	
🗷 🚞 CCE	
표 🚞 CIS 5.1	
🚞 EasyVPN	
C ProcessHacker	
🗄 🧰 testmypcsecurity	
,	
Make New Folder OK Car	ncel

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

Scan Target	
🗄 🔲 😼 My Computer	Add Files
	Add Folder
Local Disk(C:\)	Add Folder
C:\Documents and Settings\Administrator\Desktop'	
	Remove
ОК	Cancel
	14

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...

🕻 COMODO Cleaning Essentials - Scanning 🛛 🛛 🗕 🗖 🗙			
	Scanning: Status:	Infected Files C:\Documents and Settings\Administrato	r\Desktop\t\CPIL2.dll
 Objects Scanned Threats Found: 	d: 18 7	Start Time: Duration:	2/11/2011 4:11:23 PM 00:00:04
🗹 Show on top		U Pause	Stop Scan

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

COMODO Cleaning Essentials - Scan Finished			- • ×
	Scanning: Status:	Custom scan Scan Finished	
 Objects Scanned Threats Found: 	d: 58 19	Start Time Duration:	2/11/2011 4:11:23 PM 00:00:15
🗹 Show on top			Results

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

COMODO Creating Trust Online

Threat Name	Risk	
Application.Win32.LeakTest.~TMZ@1	Low 🗾	
📙 🔄 C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\Extracte		
Application.Win32.LeakTest.dmc@1	Low 🗾	
📙 🔲 C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\Extracte		
Application.Win32.LeakText.~TMY@1	Low 🗾	
📙 🔲 C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\Extracte		
Application.Win32.LeakTest.~dmd@1	Low 🗾	
— I C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\Extracte		
 🗀 📄 C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\Extracte		
 C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\FPR.zip	Low 🗾	
Application.Win32.LeakTest.~FPR@(9460415, 8073497, 9458817,)	Low 🗾	
– 📄 FPR/lt-fpr-b.exe		
- 🗐 FPR/lt-fpr.exe		
– 📄 FPR/surfload.exe		
🖵 📄 FPR/tlsdll.dll		
C:\Documents and Settings\Administrator\Desktop\testmypcsecurity\FireHole.zip	Low 🗾	
ApplicUnsaf.Win32.DemoLeakTest@114161	Low 🗾	

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

Scan Target	
🖃 🛄 😼 My Computer	Add Files
A:\	Add Folder
□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	Add Folder
C:\Documents and Settings\Administrator\Deskti	
C:\Documents and Settings\Administrator\Deskti	
	Remove
OK	Cancel

• Click the 'Remove' button

COMODO Creating Trust Online*

Comodo Cleaning Essentials - User Guide

Scan Target	
🖃 🛄 🈼 My Computer	Add Files
└───────── Local Disk(C:\)	Add Folder
🖻 🫅 Custom	
C:\Documents and Settings\Administrator\Deskti C:\Documents and Settings\Administrator\Deskti	
	Remove
ОК	Cancel

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

Scan Target	
🖃 🛄 😼 My Computer	Add Files
□ → A:\ □ → Local Disk(C:\) □ → ☐ Custom ↓ ↓ C:\Documents and Settings\Administrator\Deskto	Add Folder
	Remove
ОК	Cancel

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:

•

COMODO Creating Trust Online*

Scan Type				'Custom' Scan	
		Note/Description	'Full' Scan	'Don't Scan for Viruses' not selected	'Don't Scan for Viruses' selected
	Basic	File scanner of local AV engine	~	~	×
		Cloud based File Lookup Scanner	✓	~	×
Scanner	FLS	Cloud based verification of a file's digital signature	~	~	×
		Local check that the creator of the file is on the trusted vendor list	~	~	×
	CAMAS	File is uploaded to Comodo Automated Malware Analysis System (CAMAS) for inspection	~	~	×
	Scan Memory on start	Requires restart	~	Optional	×
	Scan Critical Areas	-	✓	Optional	×
	Scan Critical System Settings	-	~	Optional	×
Options	Scan hidden registry objects	-	~	Optional	Optional
	Scan hidden registry objects	-	✓	Optional	Optional
	Scan selected drives for hidden files/folders	-	~	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:

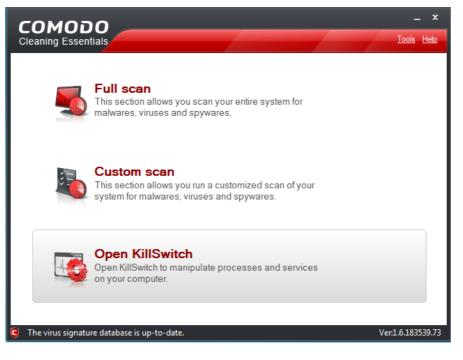
• From the Comodo Cleaning Essentials interface

COMODO Creating Trust Online*

- 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

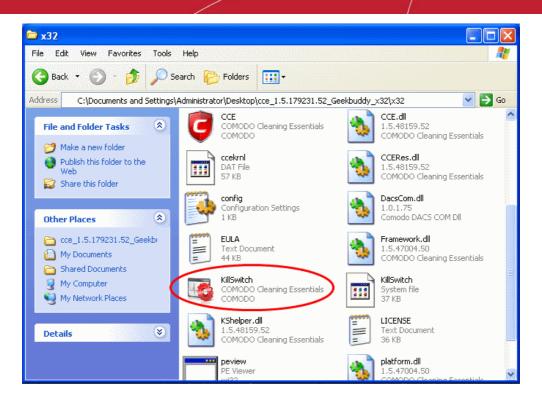


The KillSwitch main interface will be opened.

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.

COMODO Creating Trust Online



The KillSwitch main interface will be opened.

3.1.3. Replacing Windows Task Manager with KillSwitch

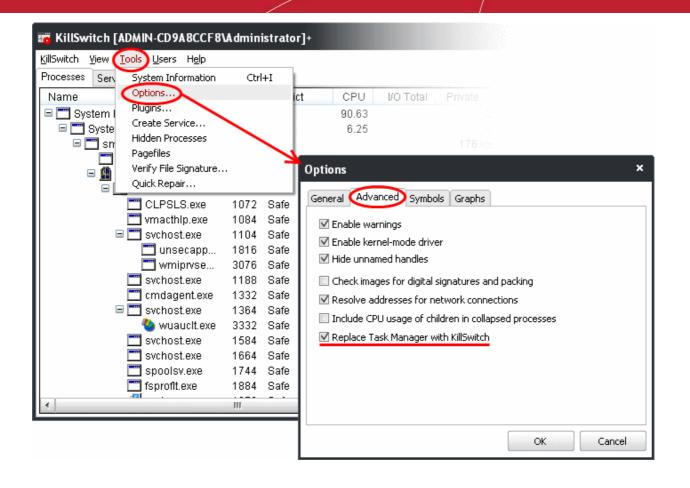
KillSwitch can be configured to replace Windows Task Manager. Doing so will mean that KillSwitch can be opened by:

- 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'.

COMODO Creating Trust Online*

Comodo Cleaning Essentials - User Guide



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.

Title Bar - Displays currently logged-in user name KillSwitch [ADMIN-CD9A8CCF8\Administrator]+ File Menu Bar KillSwitch View Iools Users Help Shortcut Icons Tab Processes Services Network BHD LSP Structure Name PID Verdict CPU I/O Total Private User Nam 🛅 System Idle Process 0 98.44 0 NT AUTHC 😑 🛅 System 4 Safe 0 NT AUTHO 🖃 🛅 smss.exe 168 kB NT AUTHO 540 Safe 🚞 osrsslexe 604 Safe 1.54 MB INT AUTHO 📓 winlogon.exe 628 Safe 6.11 MB NT AUTHO services.exe 1.65 MB NT AUTHO € 672 Safe 1.56 Main 568 kB NT AUTHO 📩 vmacthip.exe 840 Safe Display 🗂 svchost.exe 852 Safe 2.62 MB NT AUTHO Pane 🗂 svchost.exe 936 Safe 1.73 MB NT AUTHO 11.43 MB NT AUTHO 🗏 🛅 svchost.exe 1032 Safe 🌯 wuaucit.exe 5.42 MB ADMIN-CD 1844 Safe 🛅 svchost.exe 1080 Safe 1.13 MB NT AUTHO svchost.exe 1144 Safe 1.6 MB NT AUTHO 🛅 spoolsv.exe 1380 Safe 3.36 MB NT AUTHO 1.65 MB NT AUTHO 📵 VMwareServi... 1612 Safe 🗂 alg.exe 1976 Safe 1.07 MB NT AUTHC 🗂 Isass.exe 684 Safe 3.5 MB NT AUTHO ÷ CPU Usage: 1.56% Physical Memory: 65.91% Processes: 23 (Status Bar)

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.
		Note : 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

COMODO Creating Trust Online

COMODO Creating Trust Online*

		process.
	Rename All Unsafe Objects	Renames data and files that have been identified as unsafe by KillSwitch.
	Unload All Unsafe DIIs	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 Searching for Handles or DLLs 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:
		• Log-off;
		Sleep;Hibernate;
		Restart;
		Shutdown;
		• Power-off.
	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:
		CPU History
		CPU Usage
		I/O History
		Commit History
		Physical Memory History
		Right clicking the tray icons opens a panel containing shortcuts for executing various tasks. For more details, refer to the next section System Tray Icon .
	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 ' The Tools Menu ' 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 'Viewing System Information' for more details.
	Options	Opens the 'Options' dialog that enables you to configure the overall behavior of the application. Refer to the section 'Configuring KillSwitch' 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 'Managing Plug-ins' 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 ' Creating a Windows Service ' 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 'Scanning Your System for Hidden Processes' 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 'Viewing Page Files in Your System' 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 'Verifying Authenticity of Applications' for more details.
	Quick Repair	Provides a shortcut to troubleshoot and and repair important Windows settings and features. Refer Repairing Windows Settings and Features for more details.

Users		Enables to manage the status of user(s) that have currently logged- on to the system. Refer to 'Managing Currently Logged-in Users' for more details.
Help		Contains options to get help and support on usage of the product and to view the 'About' dialog. Refer to Help and About Details 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.

lcon	Task Executed
2	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 'Configuring KillSwitch' for more details.
譜	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 Searching for Handles or DLLs 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 'Viewing System Information' for more details.
	Shows the application window corresponding to the process/service selected from the main display pane until you keep the icon clicked.
	Note: 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 ' Properties ' dialog of the selected process with the ' Threads ' 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			
Processes	Displays the currently running processes in your system			
Services	Displays the Windows Services started along with your system			
Network	Displays the currently running processes that are involved in network connection activities.			
вно	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.			
LSP	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.

<u>K</u> illSwitch	<u>View</u> <u>T</u> ools <u>U</u> sers H <u>e</u> lp		
Processes Name	Tray Icons Show Only the Unsafe Images in Hide Safe Objects Always on Top Opacity	Memory V C	CPU History CPU Usage I/O History Commit History Physical Memory History
	Refresh Update Interval ✔ Update Automatically	F5 Pause	148 1.6 N 8.75 N

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;



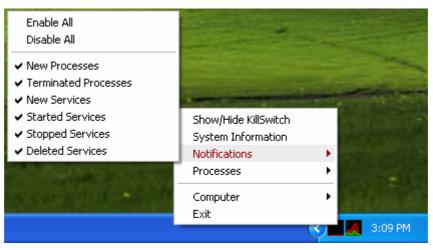
• Show/Hide KillSwitch - Enables you to switch between Show and Hide states of KillSwitch application window.

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.

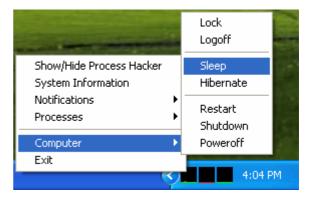
Exit	Suspend Resume Priority ► Properties	explorer.exe (2832) KillSwitch.exe (2012) smss.exe (1008) soffice.exe (980) vmware-vmx.exe (3108)	+ + + +	Show/Hide KillSwitch System Information Notifications Processes Computer Exit	
------	---	---	------------------	--	--

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:

COMODO Creating Trust Online*

- 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.

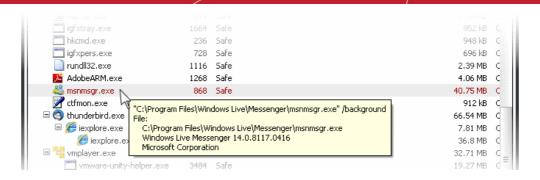
- The processes can be viewed in tree view or as a list.
- The new processes started and the processes that are stopped are highlighted.
- Right clicking on a process opens a context sensitive menu that enables you to perform various operations like stop, restart, set priority, view properties, etc,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

illSwitch <u>V</u> iew <u>T</u> ools <u>U</u> sers H <u>e</u> lp						
š 🌼 🛍 🛩 📄 🗔						
Processes Services Network BHO	LSP					
Name	PID	Verdict	CPU	I/O Total	Private B	Use
🗏 🛅 System Idle Process	0		96.09		0	NT A
🖃 🛅 System	4	Safe	0.78		0	NT A
🖃 🛅 smss.exe	760	Safe			172 kB	NT A
🛅 csrss.exe	820	Safe		12 B/s	1.79 MB	NT A
🖃 🏥 winlogon.exe	844	Safe			7.75 MB	NT A
🖃 🚞 services.exe	888	Safe			4.13 MB	NT A
🖃 📩 svchost.exe	1080	Safe			2.86 MB	NT A
🥅 igfxsrvc.exe	1656	Safe			992 kB	COM
📰 wicomm.exe	3044	Safe			19.18 MB	COM
📰 wmiprvse	2592	Safe			2.9 MB	NT A
📰 svchost.exe	1128	Safe			1.88 MB	NT A
📰 svchost.exe	1776	Safe			19.37 MB	NT A
📰 svchost.exe	2000	Safe			1.54 MB	NT A
📰 svchost.exe	196	Safe			1.25 MB	NT A
📰 spoolsv.exe	476	Safe			3.02 MB	NT A
📰 svchost.exe	612	Safe			1.29 MB	NT A
📰 jqs.exe	1312	Safe			2.19 MB	NT A
mdm.exe	1328	Safe			996 kB	NT A
📰 nvsvc32.exe	1352	Safe			2.62 MB	NT A
📩 vmware-usba	1720	Safe		4 B/s	808 kB	NT A
			1		•	Þ

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 CAMAS. 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.			
	Note : 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 'Include usage of children in collapsed processes' is enabled under the 'Advanced' tab of 'Tools' > 'Options' 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	rivate Bytes Shows the current size of system memory allocated to the process that cannot be shared wit 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.

T <u>e</u> rminate	Del	
Terminate Tree	Shift+Del	
Suspend		
Resume		
Delete		
Restart		
Debug		
Reduce Working Set		
Affinity		
Create Dump File		
Terminator		
Miscellaneous		•
Priority		•
Window		
Properties	Enter	
Search Online	Ctrl+M	
Send To		•
Сору	Ctrl+C	

- **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
- **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.

Affinity			×
Affinity con execute on		Us threads are a	allowed to
🗹 CPU 0	CPU 8	CPU 16	CPU 24
🗹 CPU 1	CPU 9	CPU 17	CPU 25
CPU 2	🗌 CPU 10	🗌 CPU 18	🗌 CPU 26
CPU 3	CPU 11	CPU 19	🗌 CPU 27
CPU 4	🗌 CPU 12	🗌 CPU 20	🗌 CPU 28
CPU 5	🗌 CPU 13	🗌 CPU 21	🗌 CPU 29
CPU 6	🗌 CPU 14	🗌 CPU 22	🗌 CPU 30
CPU 7	🗌 CPU 15	🗌 CPU 23	CPU 31
		ОК	Cancel

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.

Reduce Working Set			
Affinity Create Dump File Terminator			
Miscellaneous Priority Window		•	Detach from Debugger GDI Handles Heaps
Properties	Enter		Inject DLL
Search Online Send To Copy	Ctrl+M Ctrl+C	•	Run As Run As This User

- 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;	Affinity Create Dump File Terminator Miscellaneous	I	
Above Normal;	Priority	1	• Real Time
• Normal;	Window	1	High
Below Normal;	Properties	Enter	Above Normal
• Idle.	Search Online Send To Copy	Ctrl+M I Ctrl+C	Vormal 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;	Terminator		
•	Restore;	Miscellaneous Drieritu	+	
•	Minimize;	Priority Window	•	Bring to Front
•	Maximize;	Properties	Enter	Restore
•	Close.	Search Online Send To	Ctrl+M ▶	Minimize Maximize
		Сору	Ctrl+C	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 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.
- **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.

Module	s	Memory	Environment	н	andles
General	Verdict	Statistics	Performance	Threads	Token
File		er and Acrobat M ems Incorporated	-		

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.

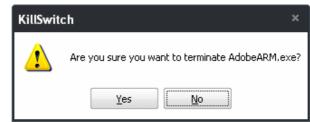
COMODO Creating Trust Online*

📌 AdobeARM.ex	e (12)	58) Propertie	es			×
Modules	<u> </u>	Memory	Environment		Handles	
General Ve	rdict	Statistics	Performance	Thread:	s Token	
File						γI
		r and Acrobat N ms Incorporated	2			
Version: 1.4.7	-	ns incorporated	1			
Image File Nam	e:					
C:\Program Fil	es\Com	mon Files\Adob	e\ARM\1.0\AdobeAF	RM.exe		
						7
Command Line:	"(:'Program Files'	Common Files\Adob	elARM\1.(1)AdobeAR	וו
Current Director			d Settings\Administr			
Started:			es ago (2/15/2011 9	:44:49 AM)	
PEB Address:	0x7ff	14000				
Parent:	explo	rer.exe (1448)				
DEP:	Disabl	ed				
Protection:	N/A					
			Permiss	ions	Terminate	
					Close	

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

iroup or user names:		
Administrator (ADMIN-C	D9A8UUF8VAdministral	orj
SYSTEM		
		Demous
	A <u>d</u> d	<u>R</u> emove
ermissions for Administrator	Allow	Deny
Full control	\checkmark	
	\checkmark	
Query information		
Query information Set information	\checkmark	
	\checkmark	
Set information		
Set information Set quotas		
Set information Set quotas Set session ID		

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.

soffice.ex	e (1612)	Properties			-	• •	×
Modules General	Verdict	Memory Statistics	Environment Performance	Threa		idles Token	
Scanner 4		Verdict]
Basic FLS CAMAS		Undetecte Unknown Error (FileT					
					ſ		1
						Close	

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	-

COMODO Creating Trust Online*

Scan Result	From	Note
	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: http://camas.comodo.com

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.

COMODO Creating Trust Online

Modules	Memory	Environment	Har	ndles
ieneral Verdici	: Statistics	Performance	Threads	Token
CPU		_I/O		1
Priority	8	Reads	178	
Cycles	N/A	Read Bytes	7.55 MB	
Kernel Time	00:00:00.140	Writes	18	
User Time	00:00:00.296	Write Bytes	146.2 kB	
Total Time	00:00:00.437	Other	668	
)	Other Bytes	11.43 kB	
Memory		I/O Priority	N/A	
Private Bytes	4.06 MB	- Other		
Peak Private Bytes		Handles	141	
Working Set	7.75 MB	Peak Handles	N/A	
Peak Working Set		GDI Handles	30	
Virtual Size Peak Virtual Size	53.71 MB	USER Handles	25	
Page Faults Page Priority	30,456 N/A	Details		
Page Prioricy	NVA J			(

• 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.

Handle Statistics		×
Туре 🔺	Count	*
Desktop Directory Event File IoCompletion Key KeyedEvent	1 3 93 26 7 56	E
Mutant Port Process Section Semaphore Thread Timer	21 5 1 14 33 12 2	
WindowStation	2	Close

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.

COMODO Creating Trust Online*

Comodo Cleaning Essentials - User Guide

Modules		Memory	Environment	Handles
General	Verdict	Statistics	Performance	Threads Toker
3.13% (K	: 3.13%, U: 0).00%)		
				<u> </u>
Private Byt	es			
Private B	ytes: 4.32 M	B		
			2/15/201	ytes: 4.06 MB
[¹ 0				
R+0: 0, \	w: 0			
		+ + + + + + + + + + + + + + + + + + +		



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.

COMODO Creating Trust Online*

<u>"</u>	AdobeARM	.exe (1268	8) Propertie	es		-	- ×
ſ	Modules	M	lemory	Environ	ment	Hand	es
ĺ	General	Verdict	Statistics	Performan	ce Th	reads	Token
		ontext 🔻				Priority	
	3980 3020			CreateThread exe+0x281b3		Normal Normal	
	2100 2096 1528 1400		USERENV.dl ntdll.dll!RtlD AdobeARM.	I!RegisterGPNo owncaseUnico exe+0x281b3 exe+0x2727a	otificat deStri	Normal Normal Normal Normal	
	Start Module:		•	n Files\Adobe\	ARM\1.0\A	dobeARM.e	
	Started:		2011 9:44:49	AM			
	State: Kernel Time:		JserRequest	Dud a sila si			
	Kernel Time: User Time:			Priority: Base Priority:	9 8		
	Context Switc			O Priority:	N/A		
	Cycles: N/A			Page Priority:	N/A		
							lose

Handling Threads

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

Inspect T <u>e</u> rminate Suspend Resume	Del	
Affinity Permissions Token Analyze Priority		• •
Сору	Ctrl+C	

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

🗖 s	ack - thread 3048	×
0 1 2 3 4 5 6	Name ntdll.dll!KiFastSystemCallRet kernel32.dll!WaitForSingleObject+0x12 AdobeARM.exe+0x567a AdobeARM.exe+0x5774d AdobeARM.exe+0x40079 AdobeARM.exe+0x2720f kernel32.dll!RegisterWaitForInputIdle+0x49	
	Copy Refresh Close	

- 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 in a symmetric multiprocessing operating system e.g. to reduce cache related problems.

Affinity				×
Affinity con execute on		Us threads are a	allowed to	
🗹 CPU 0	CPU 8	CPU 16	🗌 CPU 24	
🗹 CPU 1	CPU 9	CPU 17	🗌 CPU 25	
CPU 2	CPU 10	🗌 CPU 18	CPU 26	
CPU 3	CPU 11	CPU 19	🗌 CPU 27	
CPU 4	🗌 CPU 12	🗌 CPU 20	🗌 CPU 28	
CPU 5	CPU 13	🗌 CPU 21	CPU 29	
CPU 6	🗌 CPU 14	🗌 CPU 22	🗌 CPU 30	
CPU 7	CPU 15	🗌 CPU 23	CPU 31	
	[OK	Cancel	

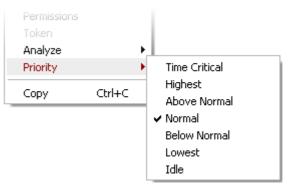
- Refer to the **Background note** in the section 'Stopping, Starting and Handling the Processes' for more details.
- **Permissions** Opens the 'Permissions' dialog that enables you to configure the access rights for the thread to the registered users of the computer.

group or user names:		
🕵 Administrator (ADMIN-CD9) 🕵 SYSTEM	A8CCF8\Administra	tor)
	A <u>d</u> d	<u>R</u> emove
ermissions for Administrator	Allow	Deny
Full control	\checkmark	
Query information	\checkmark	
Set information	\checkmark	
Get context	\checkmark	
Set context	\checkmark	
	\checkmark	
Set token		

- 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.

Information	×
Thread is waiting (alertable, wait all) for: Handle 0x380 (Event): (unnamed object) Handle 0x384 (Event): \BaseNamedObjects\userenv: Machine Group Policy has been app Handle 0x388 (Event): \BaseNamedObjects\userenv: User Group Policy has been applied	4
Save Copy	•

- **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.

AdobeAlu	V.exe (1268) Prope	rties		
Modules		Memory	Environmen	t H	landles
General	Verdic	: Statistics	Performance	Threads	Token
User: User SID: Session: 0		O\Administrator -1708537768-7 Elevated: N/i	46137067-842925246 A Virtualize		
Name 🔺		FL	ags		
COMODO\ Everyone LOCAL NT AUTHO S-1-5-5-0-1	RITY\Aut RITY\INT	Ma Ma henticate Ma ERACTIVE Ma	ndatory (Default Ena ndatory (Default Ena ndatory (Default Ena ndatory (Default Ena ndatory (Default Enabl gon ID (Default Enabl	bled) bled) bled) bled)	
Name 🔺		Status	Description		
SeBackupP SeChangel SeCreateG	Notify IobalP	Disabled Default Enabled Default Enabled Disabled	d Create global of	e checking	=
SeCreateP SeDebugPr SeEnableD SeImperso SeIncrease SeIncrease SeLoadDriv SeMachine	rivilege elega nateP Base Quot rerPri	Disabled Disabled Default Enabled Disabled Disabled Enabled	Create a pagefi Debug program Enable compute d Impersonate a d Increase schedu Adjust memory Load and unload Add workstation	é s r and user acc :lient after aut uling priority quotas for a p d device drivers	
SeCreateP SeDebugPr SeEnableD SeImperso SeIncrease SeIncrease SeLoadDriv	rivilege elega nateP Base Quot rerPri	Disabled Disabled Default Enabled Disabled Disabled Enabled	Debug program Enable compute Impersonate a (Increase schedu Adjust memory Load and unload	ie s r and user acc client after aut Jling priority quotas for a p d device drivers is to domain	

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.

_
5

- 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.

AdobeARM	l.exe ('	1268) Propertie	25		- • ×
General	Verdict	: Statistics	Performance	Thread:	s Token
Modules		Memory	Environment		Handles
Name		Verdict	Base Address	Size	Descripti 📥
Adobe		Safe	0x400000	936 kB	Adobe R
ADVAPI:		Safe	0x77dd0000	620 kB	Advanced
CLBCAT		Safe	0×76fd0000	508 kB	
COMCTL		Safe	0x773d0000	1.01 MB	User Exp
COMDLO		Safe	0x763b0000	292 kB	Common
COMRes		Safe	0x77050000	788 kB	
CRYPT3	2.dll	Safe	0x77a80000	596 kB	Crypto Al =
cryptnel	t.dll	Safe	0x75e60000	76 kB	Crypto N 🗮
ctype.nl	s		0x370000	12 kB	
GDI32.d	III	Safe	0×77f10000	292 kB	GDI Clien
iertutil.d		Safe	0x3dfd0000	1.91 MB	Run time
IMAGEH	LP.dll	Safe	0x76c90000	160 kB	Windows
IMM32.0	DLL	Safe	0x76390000	116 kB	Windows
kernel32	2.dll	Safe	0x7c800000	984 kB	Windows
locale.nl	s		0x290000	260 kB	
MSASN1	.dll	Safe	0x77b20000	72 kB	ASN.1 Ru
MSCTF.	dll	Safe	0x74720000	304 kB	MSCTF Se
msetfime	e.ime	Safe	0x755c0000	184 kB	Microsoft
msi.dll		Safe	0x7d1e0000	2.73 MB	Windows
msvcrt.o		Safe	0x77c10000	352 kB	Windows
netapi32		Safe	0x5b860000	340 kB	Net Win3
ntdll.dll		Safe	0x7c900000	712 kB	NT Laver
ole32.dl	I	Safe	0x774e0000	1.24 MB	Microsoft
OLEAUT	•	Safe	0x77120000	556 kB	
oledig.d		Safe	0x7df70000	136 kB	Microsoft
PSAPI.D		Safe	0x76bf0000	44 kB	Process S 🗸
< l		111			Þ
					Hide safe
					Close

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.

Name	Verdict		Base Address	Size	Descripti
AdobeARM ADVAPI32.dll COMCTL32.dll	Safe Safe Safe	Unload Delete	0400000	B B	Adobe R Advanced User Expl
COMDLG32.dll CRYPT32.dll cryptdll.dll	Safe Safe Safe	Inspect Search		—— В В В	Common Crypto Al Cryptogr
cryptnet.dll ctype.nls c_20127.nls	Safe	•	- Containing Folder	▶ B B B	Crypto Ni
DNSAPI.dll dssenh.dll	Safe Safe	Copy Propert		rl+⊂ B B	DNS Clier Microsoft
	Safe T Safe		0x7710000 0x662b0000	292 KB 352 kB	

- 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.

C:\WIND	OWS\sys	tem32\ig	fxpers.exe Pro	perties 🛛 🔀
General	Imports	Exports		
Time st Checks Subsys Subsys	um:	0x30a7 Window		
Section		VA	Size	
.text .rdata .data .rsrc	3	0×1000 0×18000 0×1d000 0×21000	0×17000 0×5000 0×2000 0×1000	
				OK Cancel

- 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 submenu. 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.

COMODO Creating Trust Online

General Verdict	Statistics	Performance	Threads	Token
	emory	Environment		landles
Strings			F	Refresh
Name	Address	Size	Protec	-
Free	0x0	64 kB	NA	Ξ
Private (Commit)	0×10000	4 kB	RW	_
Free	0×11000	60 kB	NA	
Private (Commit)	0x20000	4 kB	RW	
Free	0x21000	60 kB	NA	
Private (Reserve)	0x30000	1,008 kB		
Private (Commit)	0x12c000	4 kB	RW+G	
Private (Commit)	0x12d000	12 kB	RW	
Mapped (Commit)	0×130000	12 kB	R	
Free	0×133000	52 kB	NA	
Mapped (Commit)	0×140000	8 kB	R	
Free	0x142000	56 kB	NA	
Private (Commit)	0×150000	696 kB	RW	
Private (Reserve)	0x1fe000	12 kB		
Private (Commit)	0x201000	12 kB	RW	
Private (Reserve)	0x204000	28 kB		
Private (Commit)	0x20b000	56 kB	RW	
Private (Reserve)	0x219000	220 kB		
Private (Commit)	0x250000	24 kB	RW	
Private (Reserve)	0x256000	40 kB		
Mapped (Commit)	0x260000		RW	
Mapped (Reserve)	0x263000	52 kB		
unicode.nls: Mapped (Co	. 0x270000	88 kB	R	
Free	0x286000		NA	
locale.nls: Mapped (Com	. 0x290000		R	
Free	0x2d1000	60 kB	NA	
sortkey.nls: Mapped (Co		260 kB	R	*
-		2010	•••	

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.

Modules		Memory	Environment	Han	Handles	
Strings]			Refi	resh	
Name		Address 🔺	Size	Protec	*	
Free		0×0	64 kB	NA	≡	
Private (Corre	wiFA	0~10000		NA		
Free	Read	/Write Memory	60 kB	NA		
Private (Col	Save		4 kB	RW		
Free	Chang	e Protection	60 kB	NA		
Private (Re	Free	0110000001111	1,004 kB			
Private (Col			4 kB	RW+G		
Private (Col	Decom	imit	16 kB	RW		
Mapped (Cd	Deed	United Andreas	12 kB	R		
Free	•	Write Address	52 kB	NA		
Mapped (Co	Сору		8 kB	R		
Free		0x142000	56 kB	NA		
Private (Com	nit)	0x150000		RW		

• 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.

COMODO Creating Trust Online

🔲 AdobeA	RM.	exe	(30	612) (0	x15	500)O -	0x	22e	000	D)						×
00000000	c8	00	00	00	Зb	01	00	00	ff	ee	ff	ee	02	00	00	00	;	
00000010	00	00	00	00	00	fe	00	00	00	00	10	00	00	20	00	00		5 I.
00000020	00	02	00	00	00	20	00	00	de	le	00	00	ff	ef	fd	7£		
00000030	01	00	08	06	00	00	00	00	00	00	00	00	00	00	00	00		
00000040	00	00	00	00	a8	05	15	00	0f	00	00	00	f8	ff	ff	ff		
00000050	50	00	15	00	50	00	15	00	40	06	15	00	00	00	00	00	PP	
00000060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00000070	00	00	00	00	00	00	00	00	00	00	00	00	00	01	00	00		
00000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
000000a0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
000000Ъ0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
000000c0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
000000000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
000000e0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
000000£0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00000100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00000110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00000120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00000130		00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00000140	00	00	00	00	00	00	00	00	00	00	00	00	00		00			
00000150		00	00	00	00	00	00	00		e2	86		00		08	40		
00000160	30	21	00	00	00	00	00							00			0!	
00000170		00	00	00	00	00											j\$!.	
00000180				00	80	01											0j	
00000190					78												Oj\$.x[
																	••••••	
00000150	ъO	п1	15	ΠĤ	ъ0 ПС	п1	15	ΠĤ	h8.	п1	15	ΠĤ	h8	п1	15	ΠĤ		5
Re-read			Writ	e		G	oto	•									Save Close	

- 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.

Memory Protection		×
Possible values:		
0x01 - PAGE_NOACCESS 0x02 - PAGE_READONLY 0x04 - PAGE_READWRITE 0x08 - PAGE_WRITECOPY 0x10 - PAGE_EXECUTE 0x20 - PAGE_EXECUTE_READ 0x40 - PAGE_EXECUTE_READWRITE 0x80 - PAGE_EXECUTE_WRITECOPY Modifiers: 0x100 - PAGE_GUARD 0x200 - PAGE_NOCACHE 0x400 - PAGE_WRITECOMBINE		
New value:	1	
	OK Cancel	

- 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.

COMODO Creating Trust Online*

Read/Write Address		×
Enter an address:		
1		-
	ОК	Cancel

- 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.

String Search	×
Minimum Length: 10	
☑ Detect Unicode	
Search in the following types of memory regions:	
🗹 Private 🔲 Image 📄 Mapped	
OK Cancel	

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.

🧏 AdobeARM.exe (1268)	Properti	es		_ = ;	×
General Verdict S Modules Men	itatistics hory	Performance Environment	Threads	s Token Handles	
Name ALLUSERSPROFILE APPDATA CLIENTNAME CommonProgramFiles COMPUTERNAME ComSpec FP_NO_HOST_CHECK HOMEDRIVE HOMEDATH LOGONSERVER NUMBER_OF_PROCESS OS Path PATHEXT PROCESSOR_ARCHITEC PROCESSOR_IDENTIFIER PROCESSOR_IDENTIFIER PROCESSOR_LEVEL VISTOR DOMAIN USERDAME USERPROFILE WINDIR	C:\Docum Console C:\Progra CSW080 C:\WINDC NO C: UDocumen \\CHN-DC 2 Windows_ C:\WINDC .COM).EX x86 X86 Famil: 6 1706 C:\Progra Console C: C:\WINDC C:\DOCUI C:\DOCUI C:\DOCUI C:\DOCUI C:\DOCUI C:\DOCUI C:\DOCUI C:\DOCUI C:\DOCUI C:\DOCUI C:\DOCUI	DWS\system32\cmd. Its and Settings\Adm NT DWS\system32;C:\W E;.BAT;.CMD;.VBS;. y 6 Model 23 Steppin m Files DWS ME~1\ADMINI~1\LO ME~1\ADMINI~1\LO NET ator ients and Settings\Ad	dmini s exe inistrator /INDO VBE;.J g 6, G g 6, G CALS~	r	
				Close	

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.

General	Verdict	Statistics	Performance	Threads	Toker
Modules		Memory	Environment		Handles
🛛 Hide unna	med hand	les			
Туре 🔺		Name		Handle	-
Desktop	١	Default		0x30	
Directory	١	KnownDlls		0x8	
Directory	١	Windows		0×14	
Directory	١	BaseNamedObjec	ts	0x38	
Event	1	BaseNamedObjec	ts\crypt32LogoffE	0x6c	=
Event	1	BaseNamedObjec	ts\userenv: User	0x80	-
Event	1	BaseNamedObjec	ts\userenv: Machi	0xfc	
Event	1	BaseNamedObjec	ts\userenv: User	0×108	
File	(:\Documents and	Settings\Admini	0xc	
File	(:\WINDOWS\Win	SxS\x86_Microsof	0×10	
File	0	:\WINDOWS\Win	SxS\x86_Microsof	0×40	
File		,Device\KsecDD	0x44		
File	0	:\WINDOWS\Win	0x54		
File			MINI~1\LOCALS~	0×90	
File			e\144:0\JS□□Ä	0xc4	
File	(:\Documents and	Settings\Admini	0x264	
Кеу		HKLM		0x24	
Кеу		HKCU\Software\Cl		0x4c	
Кеу		HKCU\Software\Cl	asses\CLSID	0×50	
Кеу		HKCU		0×58	
Кеу			Microsoft\Interne	0x64	
Кеу	-	HKU		0×94	
Кеу			Microsoft\System	0×10c	
Кеу		HKCU		0×110	
Кеу			Microsoft\Enterpri	0×118	
Кеу		•	Microsoft\System	0x124	
Кеу		HKCU		0×128	
Kev	ł	HKCH'i Software'i Mi	crosoft\SvstemCe	0x12c	

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

Modules		Memory	Environmer	ht Ha	Handles		
🛙 Hide unn	amed handles	;					
Туре 🔺	Na	ame		Handle			
Desktop	\D(efau ^{is}		0x20			
Directory	١Kr	nowi Close	Del	0x8			
Directory	(W	indd Protecte	ed	0×14			
Directory	\Ba	^{asen} Inherit		0x3c			
File	C:1	WII		0xc			
File	\Fi	leSy Copy	Ctrl+C	0x30			
File	\D	evici Proper	ties	0x38			
Key				0x34			

- 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

COMODO Creating Trust Online*

Handle Properties	×
General Security	
Basic Information Name: VDefault Type: Desktop Object Address: 0x89b69ab8 Granted Access: 0xf01ff (Full control)	
References Quota Charges References: 3816 Handles: 30	
OK Can	cel

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

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

🔲 Find Handles or	DLLs			×
Filter:			F	ind
Process 🔺	Туре	Name	Handle	

- 2. 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
- 3. 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.

COMODO Creating Trust Online*

🔲 Find Handles o	or DLLs		×
Filter: FLTLIB			Find
Process 🔺	Туре	Name	Handle
fsprofit.exe (1320) hf.exe (1468)	DLL DLL	C:\WINDOW5\system32\FLTLIB.DLL C:\WINDOW5\system32\FLTLIB.DLL	0x4ffe0000 0x4ffe0000

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

🔲 Find Handle	s or DLLs					×
Filter: FLTLIB					Fine	F
Process 🔺	Туре	Name	•		Handle	
fsprofit.exe (13)	20) DLL	C-1940	NDOWS\eveta	m32\FLTLIB.DLL	0x4ffe0000	
hf.exe (1468)	DLL	Close	Del	32\FLTLIB.DLL	0x4ffe0000	
		Process Pro	perties	1		
		Prope <u>r</u> ties	5	1		
		Сору	Ctrl+C			

- 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.

FLTLIB.DLL P	roperties 🭷 🗙
General Versi	on Summary
3	FLTLIB.DLL
Type of file:	Application Extension
Opens with:	Unknown application Change
Location:	C:\WINDOW5\system32
Size:	16.5 KB (16,896 bytes)
Size on disk:	20.0 KB (20,480 bytes)
Created:	Saturday, September 19, 2009, 12:38:20 AM
Modified:	Wednesday, October 31, 2007, 12:31:44 AM
Accessed:	Today, February 24, 2011, 10:19:43 AM
Attributes:	Read-only Hidden Advanced
	OK Cancel Apply

• **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 licon.
- 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.

illSwitch ⊻iew <u>T</u> o	ols <u>U</u> sers H <u>e</u> lp					
🍃 🌼 🛍 🛩 🛛						
Processes Services	Network BHO LSP					
Name 🔺	Display Name	Туре	Status	Start Type	PID	
🌼 Abiosdsk	Abiosdsk	Driver	Stopped	Disabled		
🔅 abp480n5	abp480n5	Driver	Stopped	Disabled		
🌼 ACPI	Microsoft ACPI Driver	Driver	Running	Boot Start		
🌼 ACPIEC	ACPIEC	Driver	Stopped	Disabled		
🌼 adpu160m	adpu160m	Driver	Stopped	Disabled		
🌼 aec	Microsoft Kernel Acoustic Echo C	Driver	Stopped	Demand Start		
🌼 AFD	AFD	Driver	Running	System Start		
🔅 Aha154x	Aha154x	Driver	Stopped	Disabled		
🐡 aic78u2	aic78u2	Driver	Stopped	Disabled		
💮 aic78xx	aic78xx	Driver	Stopped	Disabled		
🔄 Alerter	Alerter	Share Process	Stopped	Disabled		
🔄 ALG	Application Layer Gateway Service	Own Process	Stopped	Demand Start		
🔅 AliIde	AliIde	Driver	Stopped	Disabled		
🐡 amsint	amsint	Driver	Stopped	Disabled		
AppMgmt	Application Management	Share Process	Stopped	Demand Start		
🔅 asc	asc	Driver	Stopped	Disabled		
🐡 asc3350p	asc3350p	Driver	Stopped	Disabled		
🔅 asc3550	asc3550	Driver	Stopped	Disabled		
📃 aspnet_st	ASP.NET State Service	Own Process	Stopped	Demand Start		
🐡 AsyncMac	RAS Asynchronous Media Driver	Driver	Stopped	Demand Start		
🂮 atapi	Standard IDE/ESDI Hard Disk Co	Driver	Running	Boot Start		3

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.				
Туре	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.

<u>G</u> o to Process	
Start	
Continue	
Pause	
Stop	
Restart	
Delete	
Сору	Ctrl+C
	F-1
Properties	Enter

- **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.

NVSvc P	roperties					×
General	Security Rec	overy Depend	dencies D	ependents)	1	
Provide	es system and d	esktop level sup	port to the	NVIDIA dis	play driver	
						-
Туре:	Own Process		Start	Type: Aut	to Start	v
Error Co	ontrol: Norma					

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

COMODO Creating Trust Online*

- 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.

NVSvc P	roperti	es				×	
General	Securiț	y Recovery	Dependenci	es Depen	dents		
Provide	Provides system and desktop level support to the NVIDIA display driver						
Type:	Own Pro	ocess	-	Start Type:	Auto Start		
Error Co	ontrol:	Normal	-	Group:			
Binary F	^D ath:	C:\WINDOW	S\system32\n	vsvc32.exe		Browse	
User Ad	count:	LocalSystem					
Passwo	ord:	•••••					
Service	DLL:	N/A					
🗌 Dela	ayed star						
					OK	Cancel	

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.

COMODO Creating Trust Online*

NVSvc P	ropertie	5				×		
General	Security	Recovery	Dependencies	Dependents				
<u>G</u> roup (Group or user names:							
<u>, 58</u> A	dministrator	s (CSSW080	09-CRVAdministra	tors)				
🚮 🚮	uthenticate	d Users						
🖉 P	ower Users	(CSSW080	9-CR\Power Use	rs)				
🔰 🕵 S'	YSTEM							
				A <u>d</u> d	<u>R</u> emove			
<u>P</u> ermiss	sions for Ad	ministrators		Allo	w Deny			
Eully	control							
	control			\checkmark				
	control ry status			\checkmark				
Que		ation						
Que	ry status			\checkmark				
Que Que Mod	ry status ry configura	ation						
Que Que Mod	ry status ry configura ify configur merate dep	ation						
Que Que Mod Enur Start	ry status ry configura ify configur merate dep t	ation endents	dvanced settings					

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.

NVSvc Properties						×
General Security Rec	overy	Dependencies	Dependents			
First failure:	Take	no action	-			
Second failure:	Take	no action	-			
Subsequent failures:	Take	no action	-			
Reset fail count after:	0	days				
Restart service after:	1	minutes				
Enable actions for st	ops with					
Restart Computer C	ptions					
Run program						٦l
Program:					Browse	
Append /fail=%1% to	pass th	e fail count to the	e program.			
			(эк	Cancel	

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.

NetDDE Properties			×
General Security Reco	overy Dependencies	Dependents	
This service depends on	the following services:		
Name 🔺	Display Name		
NetDDEdsdm	Network DDE DSDM		
Manages Dynamic Data stopped, DDE network s services that explicitly o	shares will be unavailab	le. If this service is disa	
		ОК	Cancel

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.

NetDDE Propertie	5		×
General Security	Recovery Dependencies	Dependents	
The following servic	ces depend on this service:		
Name 🔺	Display Name		
ClipSrv	ClipBook		
If the service is sto	iewer to store information a opped, ClipBook Viewer will r . If this service is disabled, a t.	not be able to share info any services that explicit Start	rmation with ly depend Pause
		OK	Cancel

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.

COMODO Creating Trust Online*

(illSwitch <u>V</u> iew <u>T</u> ools <u>U</u> sers H <u>e</u> lp							
3 🔅 🛍 🛩 🗔 🗔							
Processes Services Network BHO	LSP						
Process A Local Address	Loca	Remote Address	Rem	Pro	State	Owner	-
svchost.exe username.network.	135			TCP6	Listen	RpcSs	
svchost.exe username.network.	49153			TCP	Listen	Eventlog	
svchost.exe username.network.	49153			TCP6	Listen	Eventlog	
svchost.exe username.network				TCP	Listen	Schedule	
svchost.exe username.network	49154			TCP6	Listen	Schedule	
svchost.exe username.network	500			UDP		IKEEXT	
svchost.exe username.network	4500			UDP		IKEEXT	
svchost.exe username.network	500			UDP6		IKEEXT	1
svchost.exe username.network	63561			UDP		gpsvc	
svchost.exe username.network	123			UDP		W32Time	=
🔜 svchost.exe username.network	1900			UDP		SSDPSRV	
svchost.exe username.network	1900			UDP		SSDPSRV	
svchost.exe username.network	3702			UDP		FDResPub	
svchost.exe username.network	49152			UDP		FDResPub	
svchost.exe username.network	56525			UDP		SSDPSRV	
🔜 svchost.exe 🛛 username.network	56526			UDP		SSDPSRV	
svchost.exe username.network	123			UDP6		W32Time	
svchost.exe username.network	1900			UDP6		SSDPSRV	
svchost.exe fe80::141d:b447:1	1900			UDP6		SSDPSRV	
svchost.exe username.network	1900			UDP6		SSDPSRV	
1							F

	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.						
	Note : The host names are displayed only if the option ' Resolve addresses for network connections ' is enabled under the ' Advanced ' tab of ' Tools ' > ' Options ' 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.						
	Note : The host names are displayed only if the option ' Resolve addresses for network connections ' is enabled under the ' Advanced ' tab of ' Tools ' > ' Options ' 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.						
	Note: 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.

<u>G</u> o to Process Tools	Enter 🕨
View Stack Close	
Сору	Ctrl+C

- **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.

<u>G</u> o to Process	Enter	
Tools	1	Ping
View Stack		Traceroute
Close		Whois
Copy	Ctrl+C	

• **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.

Output	×
Finished.	
Pinging 203.84.220.39 with 32 bytes of data: Reply from 203.84.220.39: bytes=32 time=37ms TTL=58 Reply from 203.84.220.39: bytes=32 time=38ms TTL=58 Reply from 203.84.220.39: bytes=32 time=37ms TTL=58 Deals from 203.84.220.39: bytes=32 time=37ms TTL=58	<u> </u>
Reply from 203.84.220.39: bytes=32 time=39ms TTL=58 Ping statistics for 203.84.220.39: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 37ms, Maximum = 39ms, Average = 37ms	
	Close

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

COMODO Creating Trust Online*

Output	×
Finished.	
Tracing route to l1.ycs.vip.in.yahoo.com [203.84.220.39] over a maximum of 30 hops:	
1 <1 ms <1 ms <1 ms fw1.tt.office.net[111.111.111.1] 2 ms 1 ms 1 ms 125.17.12.17 3 40 ms 41 ms 40 ms 203.101.100.137 4 169 ms 44 ms 145.21.255.140 5 43 ms 43 ms 44 ms xe-1-0-0.msr1.in.yahoo.com[203.104.23.208] 6 39 ms 42 ms 41 ms te-9-3.bas-a1.in.yahoo.com[121.101.156.221] 7 38 ms 42 ms 57 ms l1.ycs.vip.in.yahoo.com[203.84.220.39]	
Trace complete.	.
[Close

• 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.

NO. Au	e APNIC Whois Database - Wi		م
Z., N. (1993)			
Ele Edt Yew	Favorites Icols Help		
Favorites 👌 Al	PNIC - Query the APNIC Whois Datab	550 (m)	
		APNIC - Query the APNIC Whois Database	
	To assist you	with debugging problems, this whois query was received from IP Address	
	TO USUISE FOU		
	le la	[125 17 12 18]	
		Your web client may be behind a web proxy.	
	% (whois.apni	the following authoritative answer from: whois.apnic.net c.net node-5] copyright terms <u>http://www.apnic.net/db/dbcopyright.html</u>	
	inetnum:	202.86.4.0 - 202.86.7.255	
	netname:	yahoo-india	
	descr:	Yahoo! Web Services India Pvt Ltd, Internet Content Provider IN	
	country: admin-c:	YII7-AP	
	tech-c:	XII7-AP	
	mnt-routes:	MAINT-IN-Yahoo	The second second
	mnt-by;	APNIC-HM	
	status:	ASSIGNED FORTABLE	STATISTICS AND AND
	remarks:	-+	
	remarks:	This object can only be updated by APNIC hostmasters.	
	remarks:	To update this object, please contact APNIC	574.0.677
	remarks:	hostmasters and include your organisation's account	
	remarks:	name in the subject line.	
		-	
	remarks:	-*	NY AVAILABLE OF

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

COMODO Creating Trust Online*

Name			
nspr4.dll!PR_ xul.dll!XRE_rr xul.dll!gfxFor xul.dll!gfxFor sqlite3.dll!sql sqlite3.dll!sql firefox.exe+ xpcom.dll+0x sqlite3.dll!sql	0x542d onnect+0x53 DestroySocketPollFd+0xet ain+0x3508 atGroup::FontResolverProd itGroup::FontResolverProd ite3_result_text16le+0xad ite3_shutdown+0x1928 0x30308 :2eb7b6 ite3_result_text16le+0xad ite3_shutdown+0x1928 0x2a0d	:+0x69a :+0x595 36	

- 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 o 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.

COMODO Creating Trust Online

🕫 KillSwitch [ADMIN-CD9A8CCF8\Admini	strator] – 🗆 ×
<u>K</u> illSwitch <u>V</u> iew <u>T</u> ools <u>U</u> sers H <u>e</u> lp	
🤣 🎲 🛍 🛩 🗔 🗔	
Processes Services Network BHO LSP	
GUID 🔺	Path
{18DF081C-E8AD-4283-A596-FA578C2 {6EBF7485-159F-4bff-A14F-B9E3AAC4 {9030D464-4C02-4ABF-8ECC-5164760 {DBC80044-A445-435b-BC74-9C25C1C {E15A8DC0-8516-42A1-81EA-DC94EC {E7E6F031-17CE-4C07-BC86-EABFE5	C:\Program Files\Common Files\Adob C:\Program Files\Microsoft\Search En C:\Program Files\Java\jre6\bin\jp2ssv.dll C:\Program Files\Java\jre6\bin\jp2ssv.dll C:\Program Files\Java\jre6\lib\deploy\jq
CPU Usage: 3.91% Physical Memory: 79.93% Pr	rocesses: 48

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.

Processes	Services	Network	BHO	LSP			
GUID 🔺					Path		
{18DF08 {6EBF74		-4283-A59 4bff-A14F			· · · ·	Files\Commo Files\Micros	
(9030D48 (DBC800		<mark>(ABF-8E</mark> (435b-BC7	D	elete		Files\Commo Files\Java\jre	
1.5		42A1-81E 4C07-BC			0	Files\Windov Files\Java\jre	

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

COMODO Creating Trust Online*

before passing the traffic to the application that requires it.

jillSwitch <u>Vi</u> ew <u>T</u> ools <u>U</u> sers H <u>e</u> lp ≱ 🎲 📸 🛩 │ 🗔 📮		
Processes Services Network BHO LSP GUID {70F1AA0-AB8B-11CF-8CA3-00805F48A192}	Protocol MSAFD Tcpip [TCP/IP]	Path %SystemRoot%\system32\m:
[270F1AA0-AB8B-11CF-8CA3-00805F48A192] [270F1AA0-AB8B-11CF-8CA3-00805F48A192] [9D60A9E0-337A-11D0-8D88-0000C082E69A] [9D60A9E0-337A-11D0-8D88-0000C082E69A] [970ADC4B-67B2-42CE-92B2-ACD33D88D842] [570ADC4B-67B2-42CE-92B2-ACD33D88D842] [8D5F1830-C273-11CF-95C8-00805F48A192] [8D5F1830-C273-11CF-95C8-00805F48A192] [8D5F1830-C273-11CF-95C8-00805F48A192] [8D5F1830-C273-11CF-95C8-00805F48A192] [8D5F1830-C273-11CF-95C8-00805F48A192] [8D5F1830-C273-11CF-95C8-00805F48A192] [8D5F1830-C273-11CF-95C8-00805F48A192] [8D5F1830-C273-11CF-95C8-00805F48A192] [8D5F1830-C273-11CF-95C8-00805F48A192] [8D5F1830-C273-11CF-95C8-00805F48A192] [8D5F1830-C273-11CF-95C8-00805F48A192] [8D5F1830-C273-11CF-95C8-00805F48A192] [8D5F1830-C273-11CF-95C8-00805F48A192] [8D5F1830-C273-11CF-95C8-00805F48A192] [8D5F1830-C273-11CF-95C8-00805F48A192]	MSAFD Tcpip [UDP/IP] MSAFD Tcpip [UDP/IP] RSVP UDP Service Provider RSVP UDP Service Provider VMCI sockets DGRAM VMCI sockets DGRAM VMCI sockets STREAM MSAFD NetBIOS [\Device\NetBT_Tcpip_{7DB MSAFD NetBIOS [\Device\NetBT_Tcpip_{7DB MSAFD NetBIOS [\Device\NetBT_Tcpip_{11A2 MSAFD NetBIOS [\Device\NetBT_Tcpip_{67F10 MSAFD NetBIOS [\Device\NetBT_Tcpip_{67F10 MSAFD NetBIOS [\Device\NetBT_Tcpip_{67F10 MSAFD NetBIOS [\Device\NetBT_Tcpip_{9377 MSAFD NetBIOS [\Device\NetBT_Tcpip_{9377 MSAFD NetBIOS [\Device\NetBT_Tcpip_{44D3 MSAFD NetBIOS [\Device\NetBT_Tcpip_{44D3} MSAFD NetBIOS [\Device\NetBT_Tcpip_{44D3}] MSAFD NetBIOS [\Device\NetBT_Tcpip_{44D3}] MSAFD NetBIOS [\Device\NetBT_Tcpip_{44D3}] MSAFD NetBIOS [\Device\NetBT_Tcpip_{44D3}] MSAFD NetBIOS [\Device\NetBT_Tcpip_{44D3]}]	%SystemRoot%(system32)m %SystemRoot%(system32)m %SystemRoot%(system32)m %SystemRoot%(system32)rs C:\Program Files\MMware\MMu %SystemRoot%(system32)m %SystemRoot%(system32)m %SystemRoot%(system32)m %SystemRoot%(system32)m %SystemRoot%(system32)m %SystemRoot%(system32)m %SystemRoot%(system32)m %SystemRoot%(system32)m %SystemRoot%(system32)m
VUusage: 1.56% Physical Memory: 76.51% P	III	

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.

COMODO Creating Trust Online

ł	{E70F1AA0-AB8B-11CF-8CA3-00805F48A192}	MSAFD Tcpip [TCP/IP]	%SystemRoot%\system32\msw
1	{E70F1AA0-AB8B-11CF-8CA3-00805F48A192}	MSAFD Tcpip [UDP/IP]	%SystemRoot%\system32\msw
1	{E70F1AA0-AB8B-11CF-8CA3-00805F48A192}	MSAFD Tcpip [RAW/IP]	%SystemRoot%\system32\msw
1	{9D60A9E0-337A-11D0-BD88-0000C082E69A}	RSVP UDP Service Provider	%SystemRoot%\system32\rsvp
I	{9D60A9E0-337A-11D0-BD88-0000C082E69A}	RSVP TCP Service Provider	%SystemRoot%\system32\rsvp
	{570ADC4B-67B2-42CE-92B2-ACD33D88E Dele	ets DGRAM	C:\Program Files\VMware\VMwa
	{570ADC4B-67B2-42CE-92B2-ACD33D88E	ets STREAM	C:\Program Files\VMware\VMwa
	{8D5F1830-C273-11CF-95C8-00805F48A192}	MSAFD NetBIOS [\Device\NetBT_Tcpip_{7DD8	%SystemRoot%\system32\msw
	{8D5F1830-C273-11CF-95C8-00805F48A192}	MSAFD NetBIOS [\Device\NetBT_Tcpip_{7DD8	%SystemRoot%\system32\msw
I	{8D5F1830-C273-11CF-95C8-00805F48A192}	MSAFD NetBIOS [\Device\NetBT_Tcpip_{11A2	%SystemRoot%\system32\msw
	{8D5F1830-C273-11CF-95C8-00805F48A192}	MSAFD NetBIOS [\Device\NetBT_Tcpip_{11A2	%SystemRoot%\system32\msw
	{8D5F1830-C273-11CF-95C8-00805F48A192}	MSAFD NetBIOS [\Device\NetBT_Tcpip_{67F10	%SystemRoot%\system32\msw
	{8D5F1830-C273-11CF-95C8-00805F48A192}	MSAFD NetBIOS [\Device\NetBT_Tcpip_{67F10	%SystemRoot%\system32\msw
	{8D5F1830-C273-11CF-95C8-00805F48A192}	MSAFD NetBIOS [\Device\NetBT_Tcpip_{9377	%SystemRoot%\system32\msw
	{8D5F1830-C273-11CF-95C8-00805F48A192}	MSAFD NetBIOS [\Device\NetBT_Tcpip_{9377	%SystemRoot%\system32\msw
	{8D5F1830-C273-11CF-95C8-00805F48A192}	MSAFD NetBIOS [\Device\NetBT_Tcpip_{A4D3	

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.

📷 KillSwitch	👼 KillSwitch [ADMIN-CD9A8CCF8\Administrator]+ 🛛 🗧 🗖 🗙					×		
<u>K</u> illSwitch <u>V</u> iew	<u>T</u> ools <u>U</u> sers H <u>e</u> lp							
😒 🎲 🋗 🛩	System Information	Ctrl+I						
Processes Serv	Options							
	Plugins	ł						
Name	Create Service	i	t CPU	I/O Total	Private	User Na	me	_
📔 🖃 System I	Hidden Processes		65.63		0	NT AUTH	IORIT	
😑 🚞 Syste	Pagefiles				0	NT AUTH	IORIT	
😑 🚞 sn	Verify File Signature				168 kB	NT AUTH	IORIT	1
	Quick Repair							
📔 🗆 🕒 🖌	winlogon.exe	808 Safe						

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.

COMODO Creating Trust Online*

System Info	rmation				×	
CPU 3.91% (K: 3.9 1/0 B+0: 10.85 k	1%, U: 0.00%)					
Physical Memory Physical Mem	,				.14 kB), W: 4.7
System Processes Threads Handles	48 520 13,076	Kernel Pools Paged Phys. Paged Virt. Paged Allocs	58.21 MB 64.33 MB 6,420,006	I/O Reads Read Bytes Writes	788,372 5.75 GB 648,398	
Commit Charge Current Peak Limit	0:03:31:53	Paged Frees Paged Limit Non-Paged Usage Non-Paged Allocs Non-Paged Frees Non-Paged Limit	6,253,815 no symbols 15.43 MB 1,078,788 1,030,105 no symbols	Write Bytes Other Other Bytes CPU Context Switches	1.89 GB 5,796,472 200.55 MB 35,818,769	
Physical Memory Current System Cache Total	1.58 GB 495.61 MB 1.99 GB	Page Faults Total Copy-on-write Transition Cache	16,506,209 246,301 7,946,045 2,760,127	Interrupts System Calls	9,124,330 134,377,402	
Show one grap	h a su CDU	·		Always on T	OD Close	

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

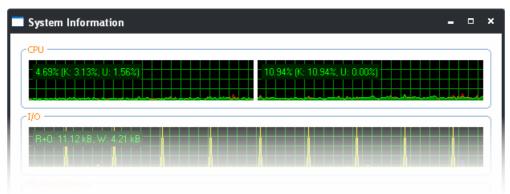
- System Displays a detailed statistics on the number of processes, threads and handles running on the computer.
- **Commit Charge** Displays a statistics on virtual memory allocated to programs and the operating system. As the memory is copied to the paging file(s) in you hard disk drive , the value 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'.

Options		×
General Advanc	ed Symbols Graph	s
Search Engine:	http://www.google	.com/search?q="%s"
PE Viewer:	peview.exe "%s"	
Max. Size Unit:	EB 💌	
Icon Processes:	5	
Log level:	Threats 💽	
🔲 Hide when clo	osed	Collapse services on start
🔲 Hide when mi	nimized	Single-click tray icons
🔲 Start hidden		🗹 Enable plugins
Font		
		OK Cancel

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.

Options			×
General Advanc	ed Symbols Graphs		
Search Engine:	http://www.google.co	pm/search?q="%s"	
PE Viewer:	peview.exe "%s"		
Max. Size Unit:	EB		
Icon Processes:	5		
Log level:	Threats		
🔲 Hide when cla	osed	Collapse services on start	
📃 Hide when mi	nimized	Single-click tray icons	
📃 Start hidden		🗹 Enable plugins	
Font			
		OK Cancel	

- 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.

Options		×
General Advanc	ed Symbols Graphs	
Search Engine:	http://www.google.com/	/search?q="%s"
PE Viewer:	peview.exe "%s"	
Max. Size Unit:	EB 💌	
Icon Processes:	B kB	
Log level:	MB GB	
Hide when clo	TB	Collapse services on start
	EB	Single-click tray icons

- 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.

	EB 🗾	
Icon Processes:	5	
Log level:	Threats	
🔲 Hide when clo	Disable Threats	Collapse services on start
🔲 Hide when mir	All	Single-click tray icons

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 doubleclick 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.

Font			?	×
Eont: O @Arial Unicode MS O Agency FB O Algerian O Arial O Arial Black O Arial Narrow O Arial Rounded MT Bol	Font style: Regular Regular Italic Bold Bold Italic	Size: 10 10 11 12 14 16 18 20 ▼	OK Cancel	
Effects Strikeout Underline Color: Black	Seript:			

3.4.2.2. Advanced Settings

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

COMODO Creating Trust Online*

Options	×
General Advanced Symbols Graphs	
Enable warnings	
🗹 Enable kernel-mode driver	
I Hide unnamed handles	
Check images for digital signatures and packing	
Resolve addresses for network connections	
Include CPU usage of children in collapsed processes	
Replace Task Manager with KillSwitch	
OK Cancel	

- 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.

COMODO Creating Trust Online*

Options	×
General Advanced Symbols Graphs	
Dbghelp.dll path: dbghelp.dll Search path:	Browse
✓ Undecorate symbols	
ОК	Cancel

• **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'.

Options	×	
General Advanced Symbols	s Graphs	1
Show Text		
CPU Kernel:		
CPU User:		
I/O R+O:		
I/O W:		
Private Bytes:		
Physical Memory:		
	OK Cancel]

• 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.

Color	₹ X
<u>B</u> asic colors:	
	Hu <u>e</u> : 0 <u>R</u> ed: 255
	<u>S</u> at: 240 <u>G</u> reen: 0
Define Custom Colors >>	Color(Solid Lum: 120 Blue: 0
OK Cancel	Add to Custom Colors

- 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 palate; 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 plugins 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.

🃷 KillSwitch	ADMIN-CD9A8CCF8\A	dministrato	or]+			×
<u>K</u> illSwitch <u>V</u> iew	<u>Tools</u> <u>U</u> sers H <u>e</u> lp					
😒 🎲 曲 🛩	System Information	Ctrl+I	1			
Processes Serv	Options					
Processes Serv	Plugins					_
Name	Create Service		ict CPU I/O Total Priva	ate U	ser Name	-
🗧 🚞 System I	Hidden Processes		65.63	0 N1	r AUTHORI	r
😑 🚞 Syste	Pagefiles			0 N1	r AUTHORI	r
🖃 🚞 sn	Verify File Signature		16	58 kB - N1	FAUTHOR	r
	Quick Repair		1.3			
	winlogon.exe	808 Safe	6.1			

Plugins × Author Name Extended Notifications wj32 Extended Services wj32 Network Tools wj32 Online Checks wj32 Toolbar and Status Bar wj32 Pluain Extended Notifications Version: 1.1 Name: Internal Name: KillSwitch.ExtendedNotifications Author: wj32 File name: F:\Comodo Cleaning Essentials\x32\plugins\ExtendedNotificati Description: Filters notifications. Options... Cleanup Close

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.

COMODO Creating Trust Online

Extended Not	ifications Properties		×
Processes Ser	rvices		
You can config Wildcards can	gure processes for which notific be used, and ordering is consic	ations are disp lered.	layed.
[Include] *			Move Up
			Move Down
		 Include 	C Exclude
		Add/Update	Remove
Examples: note*.exe			
C:\Windows\s C:\Windows*	ystem32\cmd.exe		
		ОК	Cancel

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

	Filters notificati	ons.	
Ц			Options
	Cleanup		Close

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'.

📷 KillSwitch [ADMIN-CD9A8CCF8\A	dministra	tor]+		- • ×
<u>K</u> illSwitch ⊻iew	<u>Tools</u> <u>U</u> sers H <u>e</u> lp		_		
😎 🎲 📸 🛩 Processes Serv	System Information Options Plugins	Ctrl+I			
Name	Create Service		ict CPU I/O Tota	Private	User Name 🛛 📥
🖃 🚞 System I	Hidden Processes		65.63	0	NT AUTHORIT
😑 🚞 Syste	Pagefiles			0	NT AUTHORIT
🖃 🚞 sn	Verify File Signature			168 kB	NT AUTHORIT
	Quick Repair				
🛛 🕞 🗍 🖥	winlogon.exe	808 Safe			

COMODO Creating Trust Online

The 'Create Service' dialog will open.

Create Servic	e	×	
Name:	Test Service		
Display Name:	Test Service		
Туре:	Own Process		
Start Type:	Demand Start		
Error Control:	Ignore 💌		
Binary Path:		Browse	
		OK Cancel	

- 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.

Display Name:	Test Service	
Туре:	Own Process	
Start Type:	Driver FS Driver Own Process	
Error Control:	Share Process	
Binary Path:	Own Interactive Process Share Interactive Process Browse	

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

Туре:	Own Process	×	
Start Type:	Demand Start	-	
Error Control:	Disabled Boot Start		
Binary Path:	System Start Auto Start		Bro
	Demand Start		

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

Start Type:	Demand Start	V		
Error Control:	Ignore	v		
Binary Path:	<mark>Ignore</mark> Normal Severe			Browse
	Critical		OK	Cancel

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.

COMODO Creating Trust Online*

1.11		and the second
Start Type:	Demand Start	
Error Control:	Ignore	
Binary Path:		Browse
		OK Cancel
Open		🖌
Look in:	눱 Test Programs	🔽 🔇 🌶 📂 🎞-
My Recent Documents	knack	
My Computer		
	File name:	knack 🖸 Open
	Files of type:	Executable files (*.exe;*.sys)
My Network		Open as read-only

The selected file will be added.

Create Servic	e x
Name:	Test Service
Display Name:	Test Service
Туре:	Own Process
Start Type:	Demand Start
Error Control:	Ignore
Binary Path:	C:\Program Files\Test Programs\knack.exe Browse
	OK Cancel

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.

COMODO Creating Trust Online

📷 KillSwitch [Al	DMIN-CD9A8CCF8\Administr	ator]+			-	•	×
<u>K</u> illSwitch <u>V</u> iew <u>T</u> o	ools <u>U</u> sers H <u>e</u> lp						
🤹 🎲 📸 🛩 🛛							
Processes Service	S Network BHO LSP						
Name 🔺	Display Name	Туре	Status	Start Type		PID	~
🌼 TDTCP	TDTCP	Driver	Running	Demand Start			
🌼 TermDD	Terminal Device Driver	Driver	Running	System Start			
TermSer	Terminal Services	Share Process	Running	Demand Start	-	856	
Test Serv	Test Service	Own Process	Stopped	Demand Start		>	
Themes	Themes	Share Process	Running	Auto Start		1016	
🔄 TIntSvr	Telnet	Own Process	Stopped	Disabled			
🌼 Toside	Toside	Driver	Stopped	Disabled			
TPAutoC	TP AutoConnect Service	Own Interactive	Stopped	Demand Start			ŝ1

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'

🥫 KillSwitch [A	DMIN-CD9A8CCF8\A	dministrate	or]+		×
KillSwitch View]	<mark>ools U</mark> sers H <u>e</u> lp				
🕏 🌼 🋗 🛩 Processes Serv	System Information Options Plugins	Ctrl+I			
Name	Create Service		ict CPU I/O Tota	I Private	User Name [🔺
🖃 🚞 System I	Hidden Processes		65.63	0	NT AUTHORIT
🖃 🚞 Syste	Pagefiles			0	NT AUTHORIT
🖃 🚞 sn	Verify File Signature			168 kB	NT AUTHORIT
	Quick Repair				
V 🗋 🖂 🗸	/inlogon.exe	808 Safe	,		

The hidden Processes dialog will open.

Hidden Processes			×
Processes highlighted red are hide	den while those highlighte	d grey have terminal	ed.
Process 🔺		PID	
CSR Handles	Terminate Sa	ve Scar	Close

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.

COMODO Creating Trust Online

CSR Handles 💽	Terminate	Save	Scan	Close
Brute Force CSR Handles				

3. 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.

Process 🔺	PID	-
C:\Documents and Settings\All Users\Application Data\Mozilla	3980	
C:\Program Files\Common Files\Java\Java Update\jucheck.exe	3132	
C:\Program Files\Common Files\Java\Java Update\jusched.exe	824	=
C:\Program Files\Common Files\Microsoft Shared\VS7DEBUG\M	1324	-
C:\Program Files\Common Files\VMware\USB\vmware-usbarbit	584	
C:\Program Files\Java\jre6\bin\jqs.exe	1308	
C:\Program Files\Microsoft\Search Enhancement Pack\SeaPort	1696	
C:\Program Files\Mozilla Firefox\firefox.exe	1020	
C:\Program Files\Mozilla Firefox\plugin-container.exe	2580	
C:\Program Files\OpenOffice.org 3\program\soffice.bin	800	
C:\Program Files\OpenOffice.org 3\program\soffice.bin	2220	
C:\Program Files\OpenOffice.org 3\program\soffice.exe	2212	
C:\Program Files\Paint.NET\PaintDotNet.exe	2972	
C:\Program Files\VMware\VMware Player\hqtray.exe	1568	
C:\Program Files\VMware\VMware Player\vmplayer.exe	3680	
C:\Program Files\VMware\VMware Player\vmware-authd.exe	1588	
C:\Program Files\VMware\VMware Player\vmware-unity-helper	1380	
C/Drogram Eilad VMularal VMulara Diauarhumulara, umv. ava	2004	

- 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 potion 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...'

📷 KillSwitch [ADMIN-CD9A8CCF8\A	dministrat	or]+		_ = ×
<u>K</u> illSwitch <u>V</u> iew	<u>Tools</u> <u>U</u> sers H <u>e</u> lp		_		
😎 🌼 📸 🛩 Processes Serv	System Information Options Plugins	Ctrl+I			
Name	Create Service		ict CPU	I/O Total Private	User Name 🔺
🖃 🚞 System I	Hidden Processes		65.63		0 NT AUTHORITY
😑 🚞 Syste	Pagefiles				0 NT AUTHORIT
🖃 🚞 sn	Verify File Signature			168	KB INT AUTHORIT
	Quick Repair				
	winlogon.exe	808 Safe	-		

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

agefiles				×
File name	Usage	Peak usage	Total	
C:\pagefile.sys F:\pagefile.sys	71.68 MB 70.82 MB	75.73 MB 75.31 MB	2 GB 1.99 GB	
			Refresh	Close

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 soft ware 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...'

📷 KillSwitch [A	DMIN-CD9A8CCF8\A	dministrat	or]+			-	٥	×
KillSwitch View]	ools <u>U</u> sers H <u>e</u> lp		_					
🗇 🎲 📸 🛩 Processes Serv	System Information Options Plugins	Ctrl+I						
Name	Create Service		ict CPU	I/O Total Privat	e	User Na	ame	-
🖃 🚞 System I	Hidden Processes		65.63		0	NT AUTH	IORI	P
🖃 🚞 Syste	Pagefiles				0	NT AUTH	IORI	n ii
🖃 🚞 sn	Verify File Signature			16	3 kB	NT AUTH	IORI	n il
	Quick Repair				MB			
🗔 🗍 🕅	rinlogon.exe	808 Safe	-					

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

COMODO Creating Trust Online

Open			?	×
Look in:	눱 Test Programs	🔄 🕜 🤌 🔛 -		
My Recent Documents Desktop	Calangs KNKlt.dll KNKlt.dll ServiceStarter			
My Documents				
My Computer				
	File name:	knick	Open	
My Network	Files of type:	Executable files (*.exe;*.dll;*.ocx;*.sys;*.scr;*.cp 💌	Cancel	

• Click 'Open'. KillSwitch will immediately display the result which indicated whether the program id signed or not signed.

If the p	program is signed:	
KillSwit	ch	×
(į)	"C:\Program Files\Knick\knick.exe" is trusted and signed by "XYZ Publisher".	
	OK	

If the program is not signed:

KillSwit	ch ×	
(į)	"C:\Program Files\Test Programs\knack.exe" does not have a digital signature.	
	OK	

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 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:

CillSwitch Properties 🔹 💽 🔀				
Gene	eral Version Comp	atibility Digital Sign	atures Security Summary	
- 9	Signature list			
	Name of signer:	E-mail address:	Timestamp	
	Comodo Security	Not available	Friday, February 18, 2	
			<u>D</u> etails	

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)

COMODO Creating Trust Online

	Details	Certificate
ieneral Advanced		General Details Certification Path
	signature Information al signature is OK.	Certificate Information
Signer informatio Name: E-mail:	n Comodo Security Solutions, Inc. Not available	This certificate is intended for the following purpose(s): •Ensures software came from software publisher •Protects software from alteration after publication
Signing time:	Friday, February 18, 2011 1:23:19 F	* Refer to the certification authority's statement for details.
	<u>V</u> iew Co	Issued to: Comodo Security Solutions, Inc.
Countersignature	35	Issued to: Comodo Security Solutions, Inc. Issued by: UTN-USERFirst-Object
Name of signe	35	Issued to: Comodo Security Solutions, Inc. Issued by: UTN-USERFirst-Object
Name of signe	es rr: E-mail address: Timestamp e S Not available Friday, Febru	Issued to: Comodo Security Solutions, Inc. Issued by: UTN-USERFirst-Object

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...'.

📷 KillSwitch [ADMIN-CD9A8CCF8\A	dministrat	or]+		- • ×
<u>K</u> illSwitch <u>V</u> iew	<u>Tools U</u> sers H <u>e</u> lp		_		
🛸 🎲 📸 🛩 Processes Serv	System Information Options Plugins	Ctrl+I			
Name	Create Service		ict CPU I/O Total	Private	User Name 🛛 🔺
🖃 🛅 System I	Hidden Processes		93.75	0	NT AUTHORIT
🖃 🚞 Syste	Pagefiles		3.13	0	NT AUTHORIT
🖃 🚞 sn	Verify File Signature			168 kB	NT AUTHORIT
	Quick Repair			1.39 MB	NT AUTHORIT
- B 🖉 🖓	winlogon.exe	808 Safe	-		

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

lame	Status	
PCmd Console	ок	
🍓 Context Menu	ок	
🚱 Control Panel	ОК	
MsConfig	ок	
😼 My Computer	ок	
🙆 Regedit	ок	
🖅 Run	ок	
🔎 Search	ок	
🛛 🔁 System Restore	Disabled	
💻 Task Manager	ок	
🙆 Task Scheduler	ок	
Folder Options	ок	
Hidden Drive	ок	
Explorer	ок	
🛄 Safe Mode	ОК	

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.

📷 KillSwitch [ADMIN-CD9A8	CCF8\Administrator]+			
KillSwitch Yiew Tools Users H	<u>e</u> lp			
Processes Countries A	4IN-CD9A8CCF8\Administrator 4IN-CD9A8CCF8\User A 4IN-CD9A8CCF8\User B			
Name	PID Verdict	CPU	I/O Total	Privat
🗖 🖃 System Idle Process	0	93.75		

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

COMODO Creating Trust Online*

📅 KillSwitch [ADMIN-CD9A8CCF8\Administrator]+			
KillSwitch View Tools !	<u>U</u> sers H <u>e</u> lp		_
ල් 🔅 සි 🛩 🗔	0: ADMIN-CD9A8CCF8\	Administrator 🔹 🕨	1
	1: ADMIN-CD9A8CCF8\	User A 💦 🕨 🕨	Connect
Processes Services N	3: ADMIN-CD9A8CCF8\	User B 🕨 🕨	Disconnect
Name	PID	Verdict CPU	Logoff
🛛 🖃 🚞 System Idle Proc	ess O	90.6	Send Message
🖃 🚞 System	4	Safe 3.13	Properties
			148 kB

• **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.

Connect to session		×
Password:		
1		
	OK Cancel	

- **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.

Message	×
Title:	Message from ADMIN-CD9A8CCF8\Administrator
Text:	Hi, You can now collect your files from the server. -Admin.
Icon: Timeout (s):	None
	OK Cancel

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 'lcon' drop-down. The options available are given in the table below:

Icon:	None	
Timeout (s):	None Information Warning Error	
	Question	OK

Option	Icon Displayed
None	No icon will be displayed
Information	(i)
Warning	1
Question	?
Error	\bigotimes

- 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.

Message	from ADMIN-CD9A8CCF8\Administrator	×
į	Hi, You can now collect your files from the server. -Admin.	
	ОК	

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

Session Properties		
User name: Session ID: State: Logon time: Client name: Client address: Client display:	ADMIN-CD9A8CCF8\User A 1 Disconnected 2/23/2011 4:40:49 PM N/A N/A N/A Close	

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.

KillSwitch View Tools Users H	elp			
🤣 🍥 🏔 📈 🗔 🗔 👘	Search			
Processes Services Network	About			
Name	PID Verdict	CPU	I/O Total	Priva

Clicking on the Help menu has the two options:

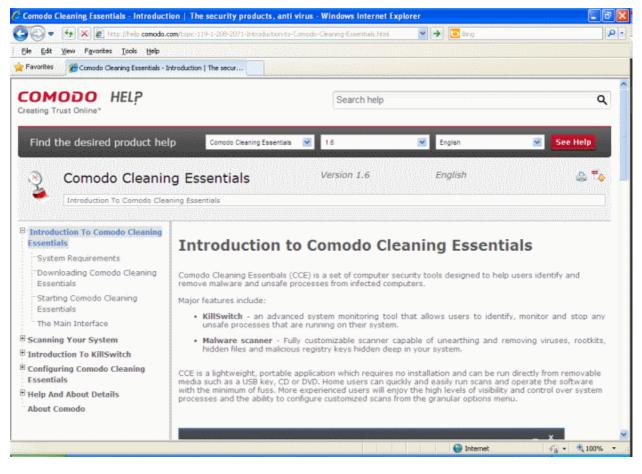
• Search

About

.

3.6.1.1. Help

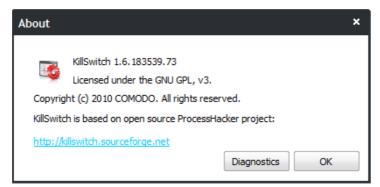
Selecting the 'Search' option from the Help menu opens the online help guide hosted at http://help.comodo.com/. Each area has its own dedicated page containing detailed descriptions of the application's functionality.



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.

Information		×
OBJECT INFORMATION PhObjectTypeObject: 23 objects PhStringType: 1381 objects PhAnsiStringType: 0 objects PhFullStringType: 0 objects PhDistType: 7088 objects PhPointerListType: 19 objects PhQueueType: 0 objects PhHashtableType: 5 objects PhFileStreamType: 0 objects PhSymbolProviderType: 0 objects PhServiceItemType: 274 objects PhNetworkItemType: 0 objects PhModuleProviderType: 0 objects PhModuleProviderType: 0 objects PhThreadProviderType: 0 objects PhThreadItemType: 0 objects		 الالله الله
	Save Copy Clos	

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'.

COMODO Creating Trust Online

Item	Location	Date/Time		
Application.Win32.LeakTest	C:\System Volume Inform	14 Feb 11 16:10		D.L.
Application.Win32.LeakTest	🛅 C:\Documents and Settin	14 Feb 11 15:23		Delete
Application.Win32.LeakTest	🛅 C:\Documents and Settin	14 Feb 11 15:23		Restore
ApplicUnwnt.Win32.Leaktest	🛅 C:\Documents and Settin	14 Feb 11 15:23		
Application.Win32.LeakTest	🛅 C:\Documents and Settin	14 Feb 11 15:23		Clear All
Application.Win32.LeakText	🛅 C:\Documents and Settin	14 Feb 11 15:23	Ξ	
Application.Win32.LeakTest	🛅 C:\Documents and Settin	14 Feb 11 15:23		
Application.Win32.LeakTest	🛅 C:\Documents and Settin	14 Feb 11 15:23		
Application.Win32.LeakTest	🛅 C:\Documents and Settin	14 Feb 11 15:23		
Application.Win32.LeakTest	🛅 C:\Documents and Settin	14 Feb 11 15:23		
Application.Win32.LeakText	C:\RECYCLER\S-1-5-21-2	14 Feb 11 16:10		
Application.Win32.LeakTest	1 C:\RECYCLER\S-1-5-21-2	14 Feb 11 16:10		
Application.Win32.LeakTest	C:\RECYCLER\S-1-5-21-2	14 Feb 11 16:10		
ApplicUnsaf.Win32.DemoLea	C:\Documents and Settin	14 Feb 11 15:23	-	

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'.

Trusted Software Vendors			
Vendors (Signer Name in the Code Signing Certificate)	Defined By	/ 🔺	Add
0823706 B.C. LTD	COMODO	E	
OInfinito s.r.l.	COMODO		Remove
1 mal 1 Software GmbH	COMODO		
1 und 1 Internet AG	COMODO		
10in6 Inc.	COMODO		
11com7 design & media GmbH	COMODO		
1234 MicroTechnologies Inc.	COMODO		
128 Consulting	COMODO		
12Ghosts AG	COMODO		
12Ghosts Inc.	COMODO		
15 Million Elephants, L3C	COMODO		
1C Company	COMODO		
1media	COMODO		
2 PLAN LIMITED	COMODO		
20/20 INSIGHT PTY LTD	COMODO		
20-20 Technologies Inc.	COMODO		
2066562 Ontario Inc.	COMODO	v	

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:

- i. Content Source: The software they are downloading and are about to install *really comes from the publisher that signed it.*
- ii. 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:

CCE Properties	? 🛛
General Version Compatibility Digital Signa	atures Summary
Signature list	
Name of signer: E-mail address:	Timestamp
Comodo Security Not available	Wednesday, February
	Details

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

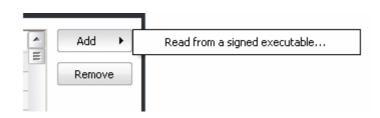
Digital Signature Details	? 🗙	Certificate
General Advanced		General Details Certification Path
Digital Signature Information This digital signature is OK.		Certificate Information
Cigner information Name: Comodo Security Solutions, Inc. E-mail: Not available		This certificate is intended for the following purpose(s): •Ensures software came from software publisher •Protects software from alteration after publication
Signing time: Wednesday, February 09, 2011 2:04:38 PM	\mathbb{P}^{-}	* Refer to the certification authority's statement for details. Issued to: Comodo Security Solutions, Inc.
Countersignatures Name of signer: E-mail address: Timestamp		Issued by: UTN-USERFirst-Object
COMODO Time S Not available Wednesday, Februa		Valid from 4/8/2009 to 4/8/2012
Details		Install Certificate) Issuer Statement
	ок	ОК

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.

COMODO Creating Trust Online



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'.

Select the appl	ication			? 🗙
Look in:	🚞 Messenger		👱 3 🕫 🖻 🗉	-
My Recent Documents Desktop	 cache logs Media Profiles resources skins avthost core_video.dll default filter1.enc 	 intl kdu_v32R.dll libexpat.dll login modules nspr4.dll PhotoShare.dll Pluginkey_pub.pem RGX.dll rmc_audio.dll 	 yacsui.dll YahooMessenger yalertcenterM.dll YCPFoundation.dll YCPSSL.dll YHTTP.dll YImage.dll YIniDom.dll ylog.dll ymdm audio.dll 	YPagerCheck: ypagerps.dll YPluginRegisti ystats_B yvi.dll ywcupl.dll
My Documents	 flfl_bg ft60.dll generic_messenger id3lib.dll INSTALL 	🔊 rmc_video.dll 💼 sb	ymdm_video.dll Yml.dll ymsdk.dll ymsglite.dll Tmyrr tray	
My Computer	<	hooMessenger		Open
My Network		Files (*.*)	~	Cancel

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):

Digital Signature Information 2:Software GinbH COMODO Signer information COMODO Zubeo, Inc. COMODO Signer information Vahool Inc. COMODO Zubeo, Inc. COMODO E-mail: Not available Comodo Zupo, LLC COMODO Signing time: Wednesday, August 19, 2009 6:57:03 AM Cueve Hofpoort Ziekenhuis COMODO ZUXXEZ Entertainment AG COMODO Zubed Entertainment AG COMODO Zyba Ltd Comodo Zyba Ltd COMODO Zyba Ltd Comodo Zyba Ltd COMODO Zyba Ltd Comodo Zymergi LLC COMODO Zyba Ltd Comodo Zymergi LLC COMODO Zyba Computer Technology Corp. COMODO Zymergi LLC COMODO Zyba Ltd Comodo Zymergi LLC COMODO Zymergi LLC COMODO Yey Elsign Time St Wednesday, August Computer Technology Corp. COMODO ZyWEL Communications UK Ltd COMODO	emove
Signer information Zubeo, Inc. COMODO Name: Vahool Inc. Zugo Bilgi Sistemleri A.S. COMODO E-mail: Not available Comodo Zupo, LLC Comodo Signing time: Wednesday, August 19, 2009 6:57:03 AM UWE extificate Comodo ZUXEZ Entertainment AG COMODO ZUXEZ Entertainment AG COMODO ZUXEZ Entertainment AG COMODO Zyba Ltd COMODO Zyba Ltd COMODO Zymer gi LLC Comodo Zymer gi LLC Zomodo Countersignatures Timestamp COMODO Zyo Computer Technology Corp. COMODO	emove
Signer information Yahool Inc. Zugo Bilgi Sistemleri A.S. COMODO Name: Yahool Inc. Yahool Inc. Yahool Inc. Comodo E-mail: Not available Zupio, LLC COMODO Signing time: Wednesday, August 19, 2009 6:57:03 AM Zuwe Hofpoort Ziekenhuis COMODO View Certificate View Certificate ZY Computing INC COMODO Zyba Ltd COMODO Zyba Utd COMODO Zyba Media Group B.V. COMODO Zymergi LLC COMODO Zyor Computer Technology Corp. COMODO Zyor Computer Technology Corp. COMODO	
Jugler minimization Name: Yahool Inc. E-mail: Not available Signing time: Wednesday, August 19, 2009 6:57:03 AM View Certificate View Certificate View Certificate Computing INC Countersignatures Combodie Name of signer: E-mail address: Timestamp Zive Computing IVC Zoord Computer Technology Corp. COMODO	
Name: Yahool Inc. Zumesoft Solutions PTY COMODO E-mail: Not available Zupa Aps COMODO Signing time: Wednesday, August 19, 2009 6:57:03 AM LLC COMODO ViewCertificate COMODO ZUXXEZ Entertainment AG COMODO Zyba Ltd COMODO Zyba Ltd COMODO Zyba Ltd COMODO Zyba Ltd COMODO Zybor media Group B.V. COMODO Zybor media Group B.V. Comodo Zyo Computer Technology Corp. COMODO Zyo Computer Technology Corp. Comodo	
E-mail: Not available Zupa Aps COMODO Signing time: Wednesday, August 19, 2009 6:57:03 AM Zupio, LLC COMODO View Certificate Zive Hofpoort Ziekenhuis COMODO ZVXEZ Entertainment AG COMODO Zive Hofpoort Ziekenhuis COMODO Zive Media Group B.V. COMODO Zylon Media Group B.V. COMODO Zymergi LLC COMODO Zivo Computer Technology Corp. COMODO	
Signing time: Wednesday, August 19, 2009 6:57:03 AM View Certificate Zuwe Hofpoort Ziekenhuis COMODO ZVXEZ Entertainment AG COMODO Zyba Ltd COMODO Zyba Ltd COMODO Zymergi LLC COMODO Zyo Computer Technology Corp. COMODO	
Signing time: Wednesday, August 19, 2009 6:57:03 AM View Certificate ZUXXEZ Entertainment AG COMODO ZY Computing INC COMODO Zyba Ltd COMODO Zylom Media Group B.V. COMODO Zymergi LLC COMODO Zyo Computer Technology Corp. COMODO	
Countersignatures LuxXe 2 Entertrainment A/s COMODO ViewCertificate ZY Computing INC COMODO Zyba Ltd COMODO Zyba Utd COMODO Zymergi LLC COMODO Zyo Computer Technology Corp. COMODO	
ViewCertificate Zyba Ltd COMODO Countersignatures Zylom Media Group B.V. COMODO Name of signer: E-mail address: Timestamp Zyo Computer Technology Corp. COMODO	
Countersignatures Zyba Ltd COMODO Countersignatures Zylom Media Group B.V. COMODO Zymergi LLC COMODO Zyo Computer Technology Corp. COMODO	
Countersignatures Zymergi LLC COMODO Name of signer: E-mail address: Timestamp Zyo Computer Technology Corp. COMODO	
Name of signer: E-mail address: Timestamp Zymergi LLC COMODO Zyo Computer Technology Corp. COMODO Comodo	
VeriSign Time St Not available Wednesday, August ZyXEL Communications UK Ltd COMODO	
ZZEE TOOLS Corp. COMODO	
ZZEE TOOLS Corp. COMODO	

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'.

🤤 Options	ж	2		
MBR Options (Valid for single boot computers) Scan suspicious MBR modifications in full s Report all MBR modifications in full scan				
Virus scanner	n			
Heuristics Scanning Level Do not scan files larger than	Low 40 MB			
CAMAS				
CAMAS timeout 300 Second(s)				
Automatically update the virus database Create a windows restore point before performed and the performance of the pe	_			
Log level Select Language	Threats			
	OK Cancel]		

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 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 recommend 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 uses 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 files safety.

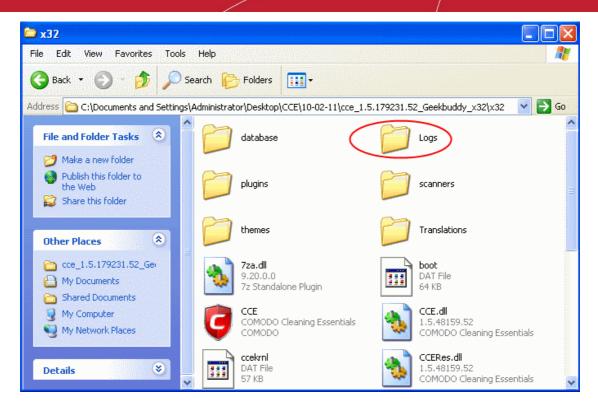
- Scan unknown processes in memory with CAMAS When this check box is selected, any unknown process or processes in memory will be automatically submitted to CAMAS (Comodo Automated Malware Analysis System).
- CAMAS timeout This box allows you to set the time (in seconds) for which the files will be submitted 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 creates a Windows restore point before embarking on the scanning process. Should problems occur after wards, you will be able to restore your system to the state just before your 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 it 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:

COMODO Creating Trust Online*



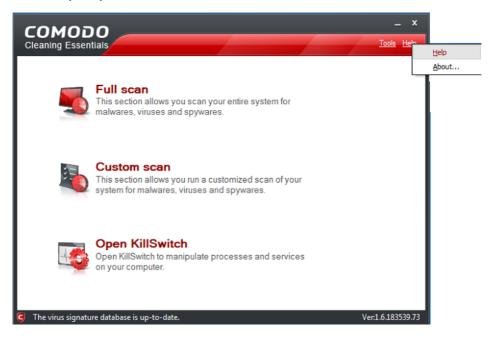
Double-click or right click and open the Logs folder. The folder will contain logs stored as time stamped text files.

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

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

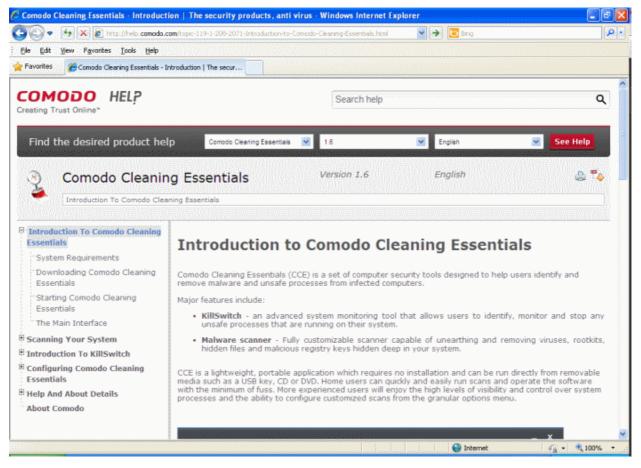
5. Help and About Details

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.

Comodo CA Limited

525 Washington Blvd. Jersey City,	3rd Floor, 26 Office Village, Exchange Quay, Trafford Road, Salford, Greater Manchester M5 3EQ,
NJ 07310	
United States	United Kingdom.
Tel: +1.888.256.2608	Tel : +44 (0) 161 874 7070
Tel: +1.703.637.9361	Fax : +44 (0) 161 877 1767
Email: EnterpriseSolutions@Comodo.com	

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