COMODO
Creating Trust Online®

# Comodo
# Cleaning Essentials

Software Version 2.5

# User Guide

Guide Version 2.5.071712

Comodo Security Solutions
1255 Broad Street
STE 100
Clifton, NJ 07013

# Table of Contents

**1.Introduction to Comodo Cleaning Essentials ... 4**

1.1.System Requirements ... 6

1.2.Downloading Comodo Cleaning Essentials ... 6

1.3.Starting Comodo Cleaning Essentials ... 6

1.4.The Main Interface ... 7

**2.Scanning Your System ... 9**

2.1.Smart Scan ... 9

2.2.Full Scan ... 14

2.3.Custom Scan ... 20

2.4.Comparison of Scan Types ... 30

**3.Configuring Comodo Cleaning Essentials ... 31**

**4.The Tools Menu ... 34**

4.1.Managing Quarantined Items ... 35

4.2.Managing Trusted Vendors ... 37

4.3.Importing Antivirus Database ... 41

4.4.Checking for Software Updates ... 42

**5.Introduction to KillSwitch ... 45**

5.1.Starting KillSwitch ... 46

5.1.1.From the Comodo Cleaning Essentials Interface ... 46

5.1.2.From the Folder Containing Comodo Cleaning Essentials Files ... 47

5.1.3.Replacing Windows Task Manager with KillSwitch ... 47

5.2.The Main Interface ... 48

5.2.1.The System Tray Icon ... 52

5.3.Viewing and Handling Processes, Applications and Services ... 54

5.3.1.Processes ... 54

5.3.1.1.Stopping, Starting and Handling the Processes ... 61

5.3.1.2.Viewing Properties of a Process ... 64

5.3.2.Applications ... 79

5.3.2.1.Handling the Applications ... 80

5.3.3.Services ... 81

5.3.3.1.Stopping, Starting and Deleting the Services ... 84

5.4.Viewing and Handling Network Connections and Usage ... 85

5.4.1.Network Connections ... 86

5.4.1.1.Inspecting and Closing Network Connections ... 88

5.4.2.Network Utilization ... 88

5.5.Configuring KillSwitch ... 89

5.6.KillSwitch Tools ... 93

5.6.1.Viewing System Information ... 95

5.6.2.Repairing Windows Settings and Features ... 97

5.6.3.Analyzing Program Usage ... 99

5.6.4.Searching for Handles or DLLs ... 101

5.6.5.Verifying Authenticity of Applications ... 102

5.6.6.Boot Logging and Handling Loaded Modules ... 106

5.6.7.Running Programs from Command Line Interface.......... 110
5.6.8.Viewing KillSwitch Logs.......... 112
5.6.9.Finding Process of the Active Window.......... 113
5.7.Managing Currently Logged-in Users.......... 114
5.8.Help and About Details.......... 116
5.8.1.Help.......... 116
5.8.2.About.......... 117
**6.Introduction to Autorun Analyzer.......... 118**
6.1.Starting Autorun Analyzer.......... 118
6.1.1.From the Comodo Cleaning Essentials Interface.......... 118
6.1.2.From the KillSwitch Interface.......... 119
6.1.3.From the Folder Containing Comodo Cleaning Essentials Files.......... 120
6.2.The Main Interface.......... 121
6.3.Viewing and Handling Autorun Items.......... 123
6.3.1.Handling Autorun Items.......... 124
6.3.2.Filtering Entries based on Categories.......... 125
6.3.3.Viewing Autorun Items for other User Accounts.......... 127
6.4.Help and About Details.......... 127
6.4.1.Help.......... 128
6.4.2.About Autorun Analyzer.......... 129
**7.Help and About Details.......... 129**
7.1.Help.......... 130
7.2.About.......... 130
**8.Using the Command Line Interface.......... 131**
8.1.Running a Smart Scan from the Command Line Interface.......... 131
8.2.Running a Custom Scan from the Command Line Interface.......... 132
8.3.Running a Virus Database Update Task from the Command Line Interface.......... 134
8.4.Viewing Help.......... 134
**About Comodo.......... 135**

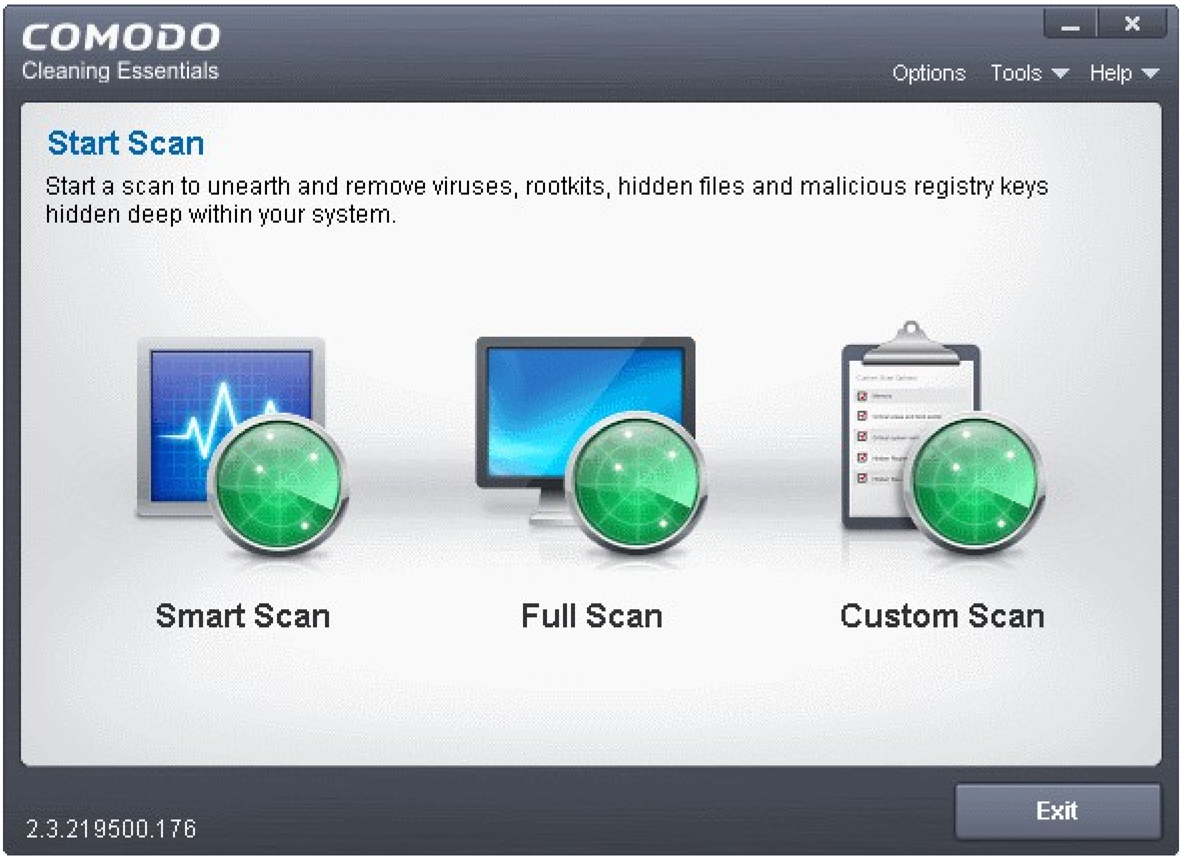
# 1. Introduction to Comodo Cleaning Essentials

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.
- **Autorun Analyzer** - An advanced utility to view and handle services and programs that were loaded when your system booted-up.

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.



Start Scan

Start a scan to unearth and remove viruses, rootkits, hidden files and malicious registry keys hidden deep within your system.

When started in aggressive mode, CCE forcibly terminates all the running applications and processes created by currently logged-in user for fast and efficient scanning.

## 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 Requirements** - 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 scanning your computer.
  - **Smart Scan** - Explains how to run a scan on critical areas of your system.
  - **Full Scan** - Explains how to run a full scan of your system.
  - **Custom Scan** - Explains how to scan on selected items.
  - **Comparison of Scan Types** – Provides details on scanners used and the scan sequences followed for different types of scans in CCE.
- Section 3, **Configuring Comodo Cleaning Essentials** - Explains how to configure the overall behavior of the CCE.
- Section 4, **The Tools Menu** – Explains how to use the tools in CCE.
  - **Managing Quarantined Items** - How to manage and restore quarantined files.
  - **Managing Trusted Vendors** – How to add or remove vendors to/from the Trusted Vendor List.
  - **Importing Antivirus Database** – How to import virus database from local storage or from network computer.
  - **Checking for Software Updates** - How to manually check for program updates.
- Section 5, **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 KillSwitch tool.
  - **The Main Interface** - Description of menus and options in the main interface.
  - **Viewing and Handling Processes, Applications and Services** - explains how to view the list of currently running processes, applications and services and handle them.
    - **Processes**
    - **Applications**
    - **Services**
  - **Viewing and Handling Network Connections and Usage** - explains how to view the details of currently active network connection and handle it.
    - **Network Connections**
    - **Network Utilization**
  - **Configuring KillSwitch** - Explains how to configure the overall behavior of KillSwitch
  - **KillSwitch Tools** – Explains how to use the tools in KillSwitch.
    - **Viewing System Information**
    - **Repairing Windows Settings and Features**
    - **Analyzing Program Usage**
    - **Searching for handles or DLLs**
    - **Verifying Authenticity of Applications**
    - **Bootlogging and Handling Modules**
    - **Running Programs from Command Line Interface**
    - **Viewing KillSwitch Logs**
    - **Finding Process of Active Window**
  - **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 6, **Introduction to Autorun Analyzer** - is a high level overview of Autorun Analyzer, a powerful tool to analyze and handle services and programs that were loaded when your system booted-up and serves as an introduction to the main themes and concepts of Autorun Analyzer.
  - **Starting Autorun Analyzer** - How to start the Autorun Analyzer tool.
  - **The Main Interface** - Description of menus and options in the main interface.
  - **Viewing and Handling Autorun Items** - Explains how to view the details of services and programs that were

loaded when your system booted-up.

  - **Help and About** – Explains how to view the online help and the About dialog of Autorun Analyzer.

- Section 7, **Help and About** - How to open the online help guide and find the version number and other miscellaneous details about the CCE application.
- Section 8, **Using the Command Line Interface** – Explanation on how to run various tasks of CCE application from Windows command line interface
  - **Running a Smart Scan from the Command Line Interface** – How to run a Smart Scan
  - **Running a Custom Scan from the Command Line Interface** – How to run a Custom Scan
  - **Running a Virus Database Update Task from the Command Line Interface** – How to update local virus database
  - **Viewing Help** – How to view online help guide of CCE 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_2.3.219500.176_x32.zip**

**64 Bit Operating Systems**:

**http://download.comodo.com/cce/download/setups/cce_2.3.219500.176_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

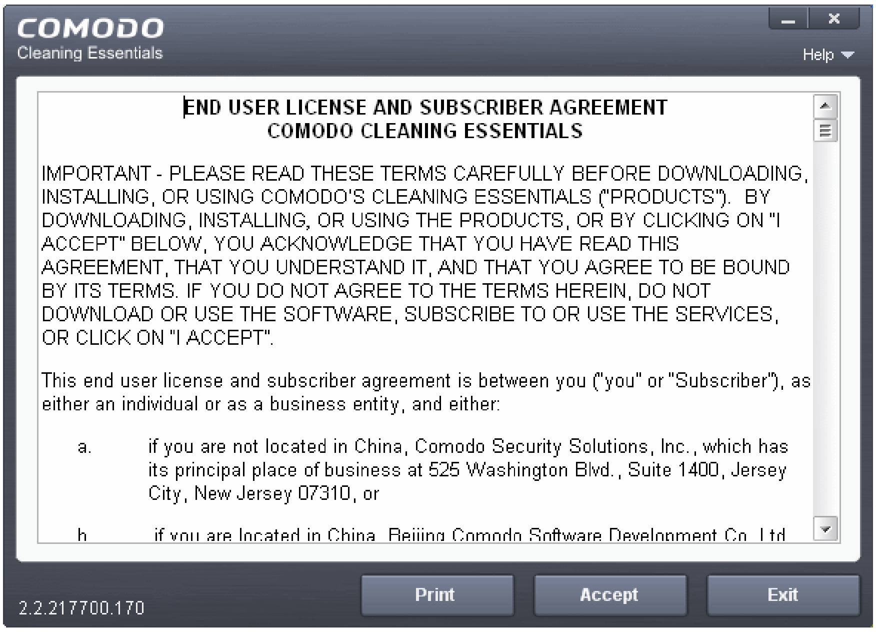
CCE is a lightweight, portable application which requires no installation and can be run directly from removable media such as a USB key.

### To start the CCE application

- Navigate to the CCE folder containing the files.
- Double-click on the CCE.exe file.
- To start CCE in aggressive mode, press and hold 'Shift' key and double click on the file 'CCE.exe'.

In aggressive mode, CCE forcibly terminates all the running applications and processes created by currently logged-in user before it starts, for fast and efficient scanning.

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.



END USER LICENSE AND SUBSCRIBER AGREEMENT
COMODO CLEANING ESSENTIALS

IMPORTANT - PLEASE READ THESE TERMS CAREFULLY BEFORE DOWNLOADING, INSTALLING, OR USING COMODO'S CLEANING ESSENTIALS ("PRODUCTS"). BY DOWNLOADING, INSTALLING, OR USING THE PRODUCTS, OR BY CLICKING ON "I ACCEPT" BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO BE BOUND BY ITS TERMS. IF YOU DO NOT AGREE TO THE TERMS HEREIN, DO NOT DOWNLOAD OR USE THE SOFTWARE, SUBSCRIBE TO OR USE THE SERVICES, OR CLICK ON "I ACCEPT".

This end user license and subscriber agreement is between you ("you" or "Subscriber"), as either an 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

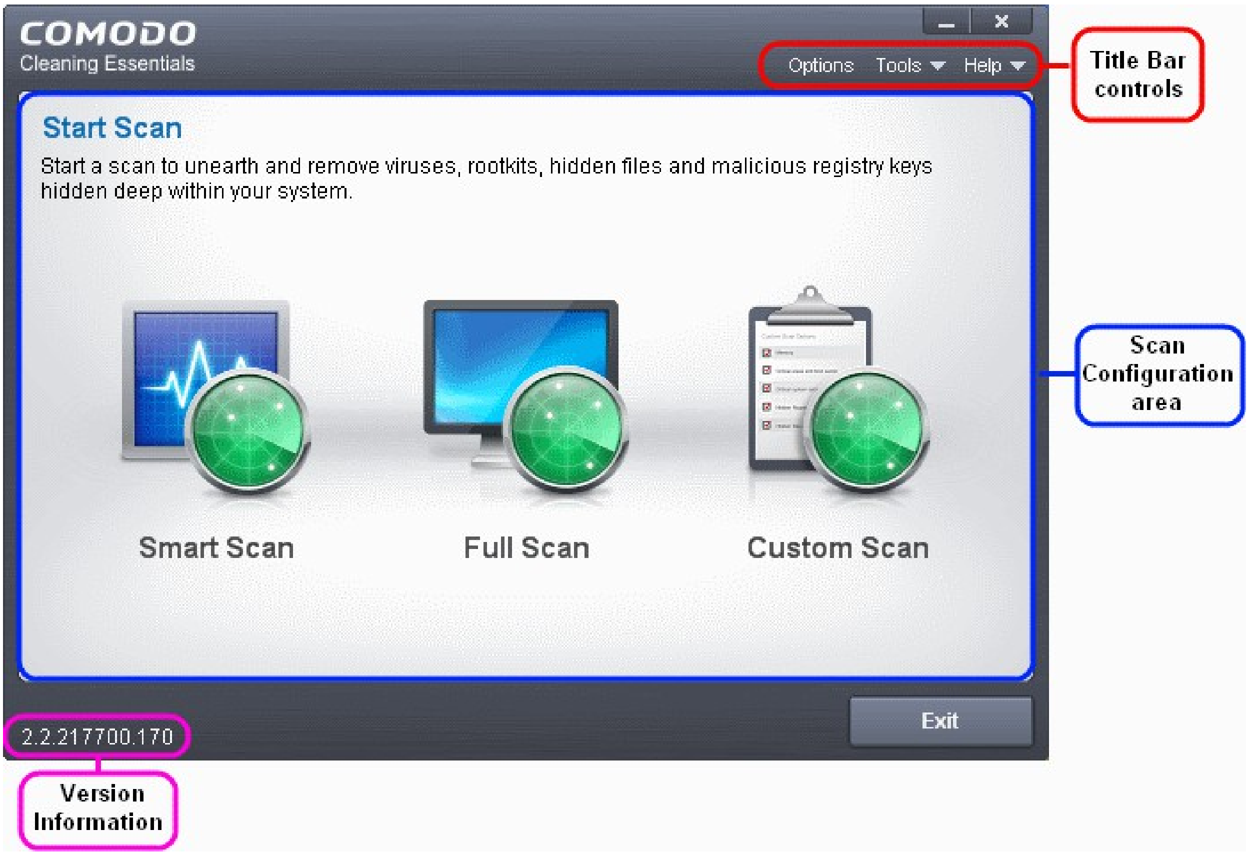
b. if you are located in China, Beijing Comodo Software Development Co. Ltd

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

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

# 1.4. The Main Interface

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



The main interface of the application has the following areas:

- **Scan Configuration Area**;
- **Title Bar Controls**;
- **Version Information**.

## Scan Configuration Area

The Scan Configuration Area allows you to start scanning your system for potential malware.

- **Smart Scan** - Run scan on memory, autorun entries, hidden services, critical areas like critical registry keys, system files, system configuration and boot sectors for possible infection by malware, viruses and spyware.
- **Full Scan** - Run a full scan on your system for malware, viruses and spyware.
- **Custom Scan** - Run a scan on areas that you wish for malwares, viruses and spywares in your system.

## Title Bar Controls

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

- **Options** - Allows you to configure various settings in the application.
- **Tools** - Allows you to manage Quarantined items, Trusted Vendor list and virus database. Also contains shortcuts to open KillSwitch and Autorun Analyzer.
- **Help** - Launches the online help guide

## Version Information

At the bottom of the main interface, the version information of the software is displayed.

# 2. Scanning Your System

Comodo Cleaning Essentials allows you to perform a quick scan of critical areas in your computer,  full system scan or a custom scan as per your requirements. The Quick Scan a.k.a Smart Scan, checks  the critical areas like Windows Registry, system Files, system memory, autorun entries, hidden services, and boot sectors for possible infection.

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. You can also scan an individual folder or a file you just downloaded from Internet or copied into your system instantly by dragging and dropping it over the CCE interface.

Refer to the following sections for more details on:

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

## 2.1. Smart Scan

Smart Scan in Comodo Cleaning Essentials allows you to run a quick scan on the critical areas in your system which are highly prone to infection from viruses, rootkits and other malware. Smart scan scans and cleans the system memory, autorun entries, hidden services, boot sectors and other critical areas like crucial registry keys in Windows registry, system files and system configuration. These areas are responsible for the stability of your computer and keeping them clean and sanitized is essential to keep you healthy and running.

Scanning  the critical areas of your system can be executed instantly, but  scanning for hidden services and drivers can be executed only after a system restart.

Hidden services are executed by  malicious attempts like a spyware through key logger, rootkits, buffer overflow or Denial of Service (DoS) attacks. These attacks will be running silently in the computer and enable hackers to steal your identity and confidential information like your credit card details.

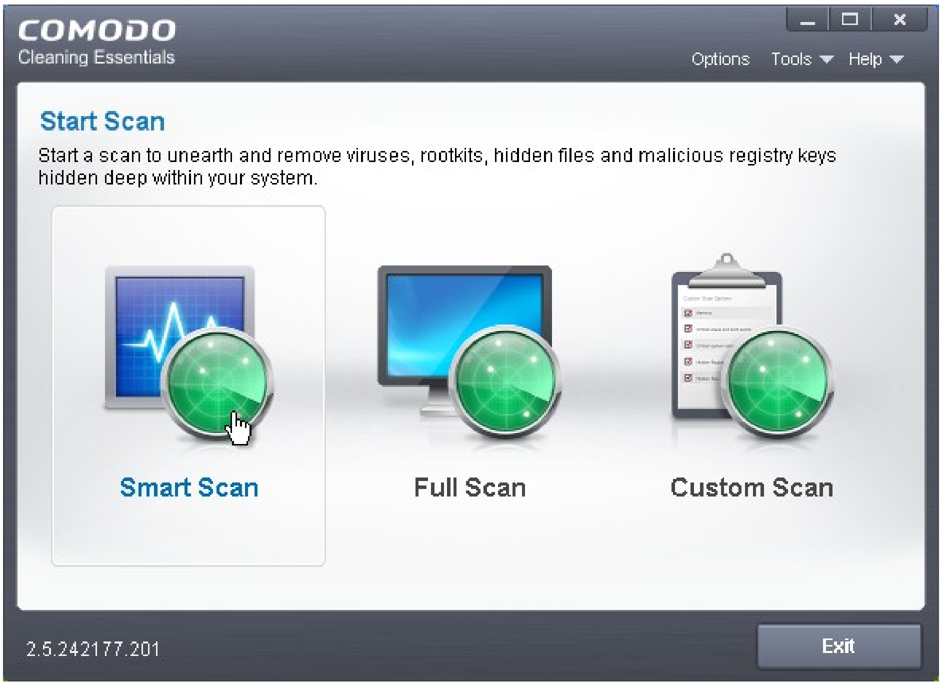
Hence, on completion of a Smart scan, CCE will require a system restart to scan for hidden services.

On completion of scanning, you can:

- Clean the detected threats or move them to Quarantine and later remove them;
- Exclude an application you consider as safe from the threat list;
- Report the threat as a False Positive to Comodo.

To start a Smart scan

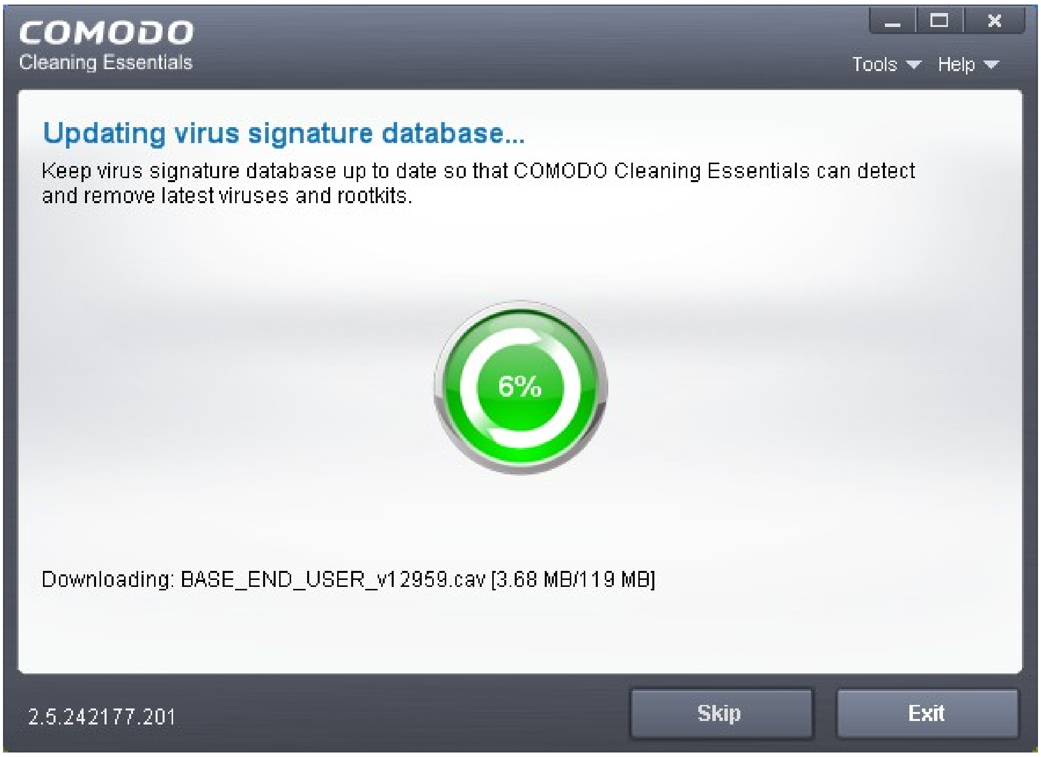
1. Click the 'Smart Scan' from the CCE main interface.



Start Scan

Start a scan to unearth and remove viruses, rootkits, hidden files and malicious registry keys hidden deep within your system.

The application will check whether any updates are available for the virus database before commencing the scan. If available, it will first update the local virus database.



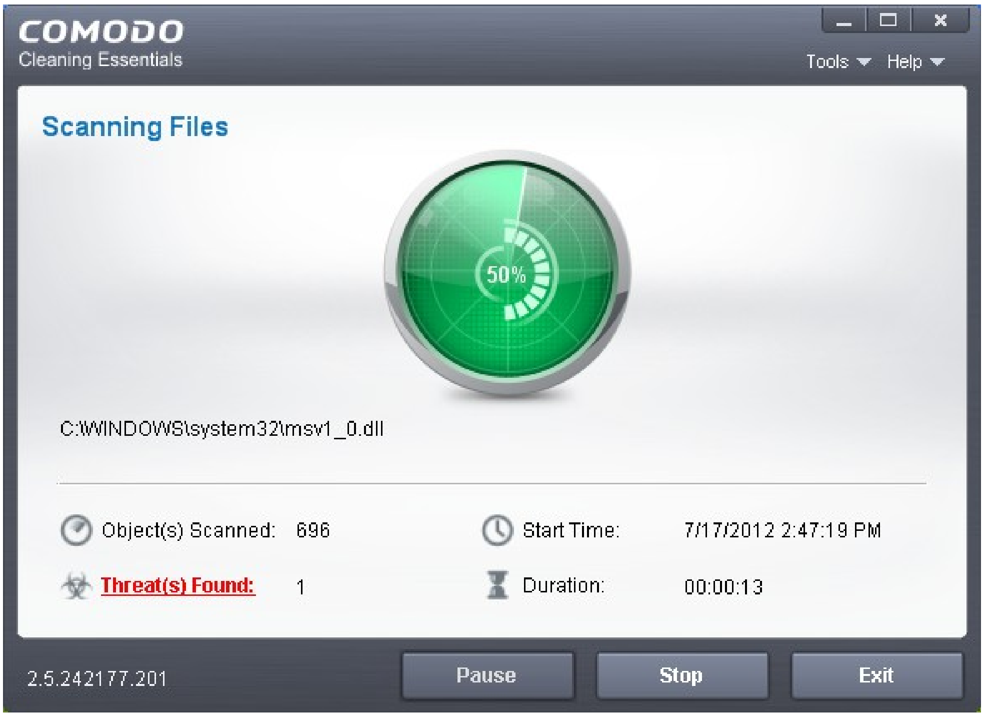
Updating virus signature database...

Keep virus signature database up to date so that COMODO Cleaning Essentials can detect and remove latest viruses and rootkits.

Downloading: BASE_END_USER_v12959.cav [3.68 MB/119 MB]

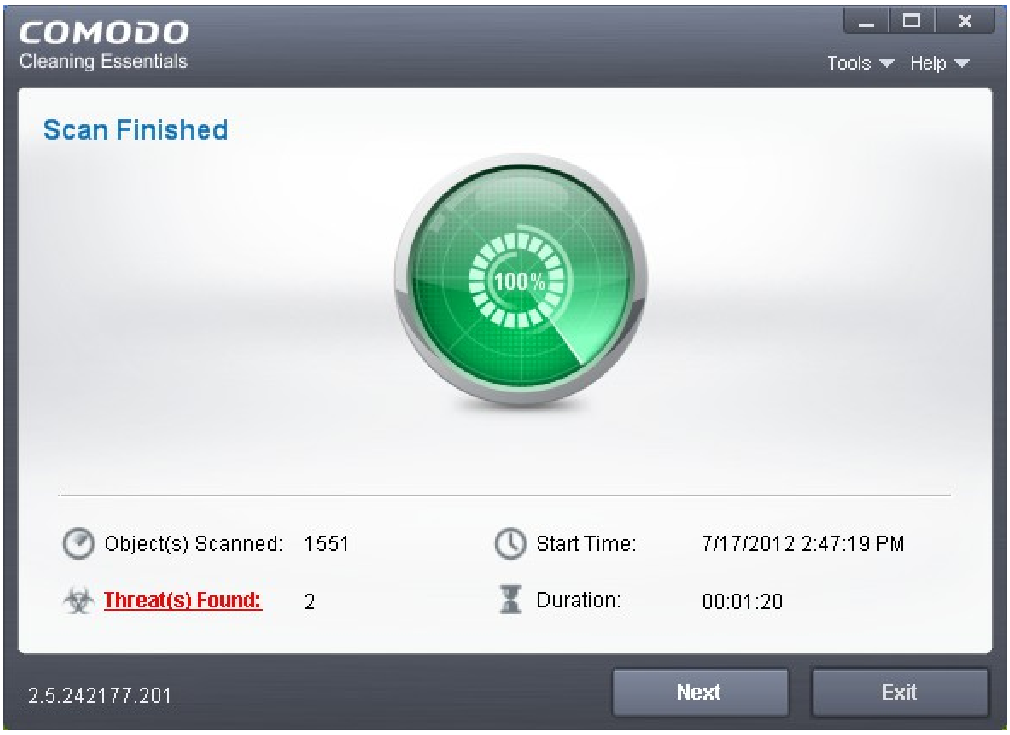
It is advised that you always let the application to update the database as  scanning with your virus database up-to-date detects even the zero-hour threats. However, if you do not want the database update at this moment, you can skip this step by clicking 'Skip'.

The application will start scanning the critical areas of your system and the progress will be displayed.

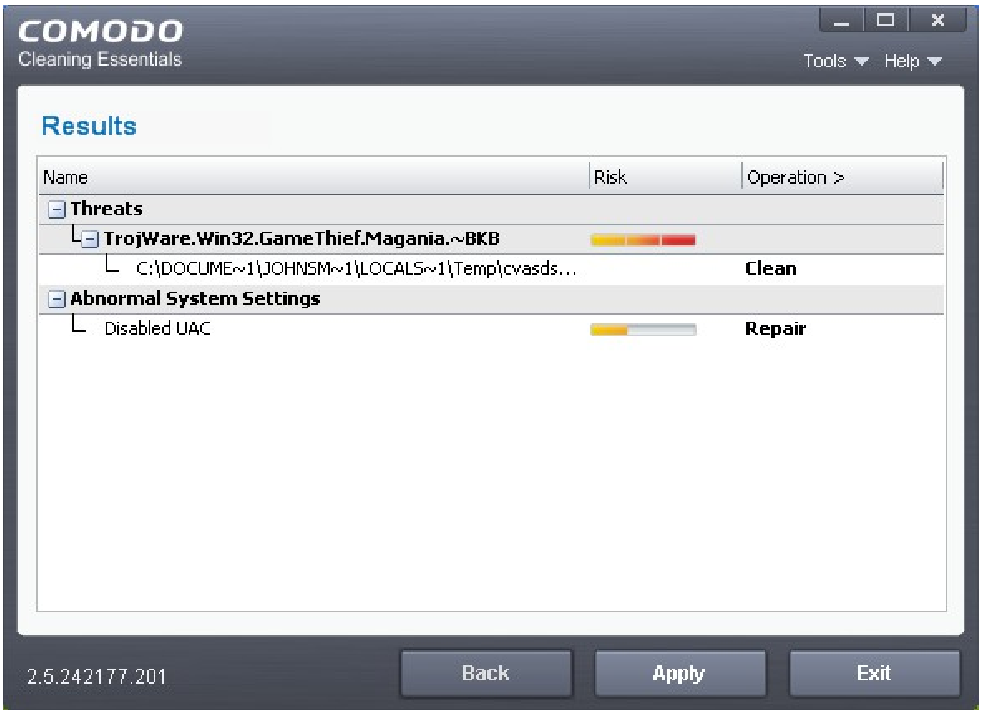


During the course of scanning, if you want to see details on the threats detected so far, click Threats Found link. A results window with the threats identified thus far will be displayed.

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



2. Click 'Next' to view the results.



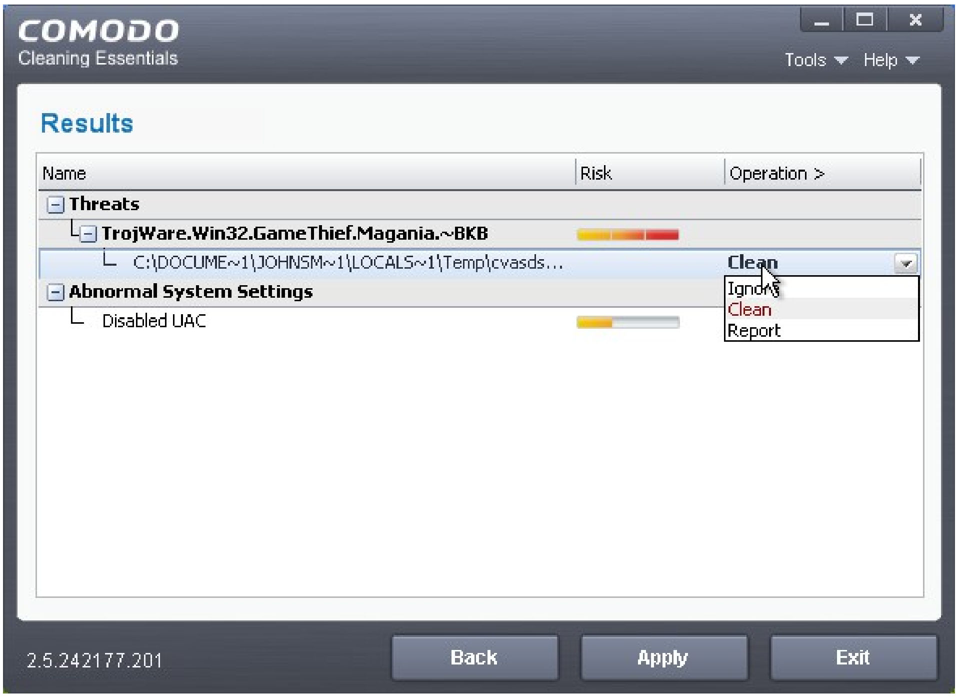
Results

| Name | Risk | Operation > |
|---|---|---|
| Threats | | |
| TrojWare.Win32.GameThief.Magania.~BKB | | |
| C:\DOCUME~1\JOHNSM~1\LOCALS~1\Temp\cvasds... | | Clean |
| Abnormal System Settings | | |
| Disabled UAC | | Repair |

- If malicious executables are discovered on your system, the 'Results' window displays the list of those items (Viruses, Malware and so on).

**Tip:** You can sort the scan results by alphabetical order by clicking the 'Threat Name' column header. Similarly you can sort the scan results based on the risk level by clicking the 'Risk' column header.

The 'Results' window allows you to quarantine and later remove, ignore the threat if it is a safe file or to submit it as a false positive to Comodo if you are sure about the authenticity of the file. The default operation is 'Clean', that means CCE will clean the threat if a disinfection routine is available for it, else, will move it to quarantine.



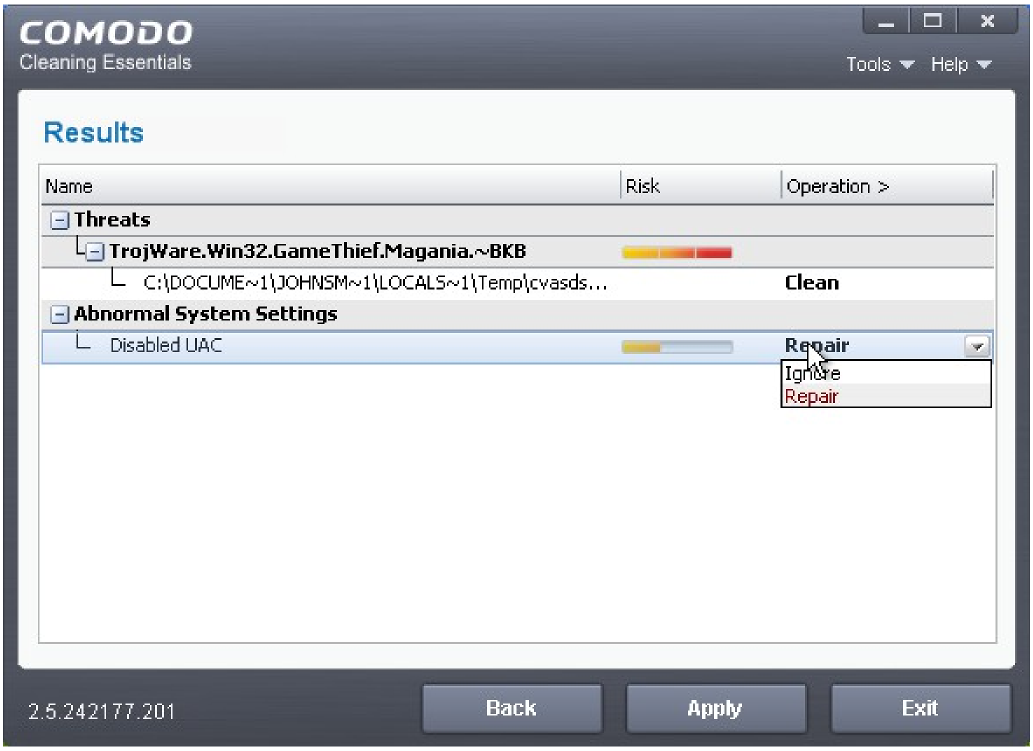
Results

| Name | Risk | Operation > |
|---|---|---|
| Threats | | |
| TrojWare.Win32.GameThief.Magania.~BKB | | |
| C:\DOCUME~1\JOHNSM~1\LOCALS~1\Temp\cvasds... | | Clean |
| Abnormal System Settings | | |
| Disabled UAC | | |

- To clean a  threat, click on the entry under the Operations column and select 'Clean'. The file will be disinfected or moved to quarantine upon applying the operation. You can later remove the file from your system from the 'Quarantined Items' interface. Refer to **Managing Quarantined Items** for more details.
- To ignore a threat if you consider the file is safe, click on the entry under the Operations column and select

'Ignore'.

- To report threat as a false-positive result, click on the entry under the Operations column and select 'Report'. The file will be sent to Comodo. Experts in Comodo will analyze the file and add it to whitelist, if found safe.
- To apply a common operation to all the entries in the list, click on the Operations column header and select the required action.

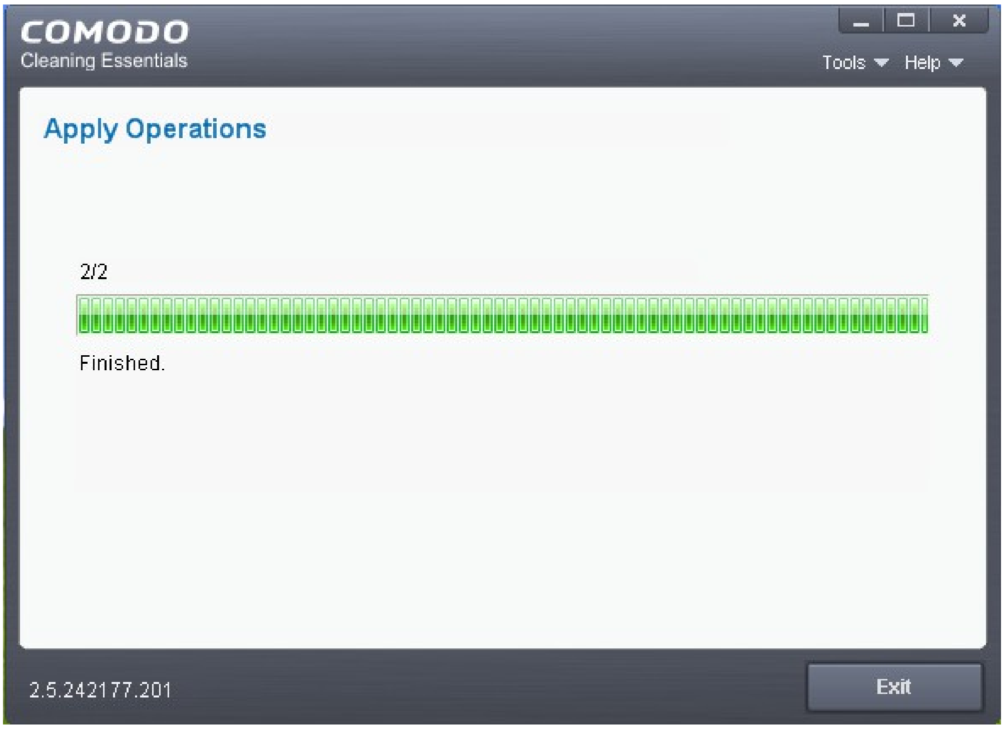


Results

| Name | Risk | Operation > |
|---|---|---|
| Threats | | |
| TrojWare.Win32.GameThief.Magania.~BKB | | |
| C:\DOCUME~1\JOHNSM~1\LOCALS~1\Temp\cvasds... | | Clean |
| Abnormal System Settings | | |
| Disabled UAC | | Repair<br>Ignore<br>Repair |

2.5.242177.201

3. Click 'Apply' to apply the selected operations to the threats. The selected operations will be applied...



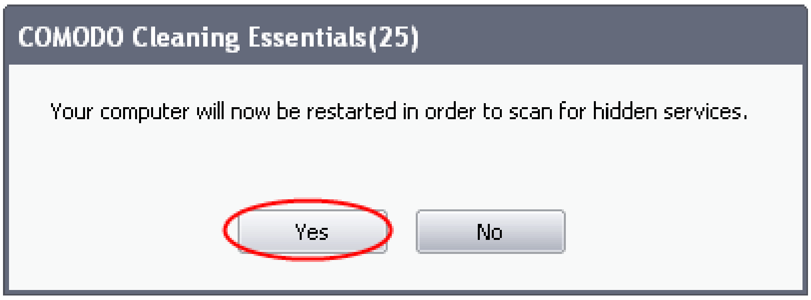
Apply Operations

2/2

Finished.

2.5.242177.201

... and your system will restart to check whether the operations are applied correctly and start scanning your system for hidden services and drivers.

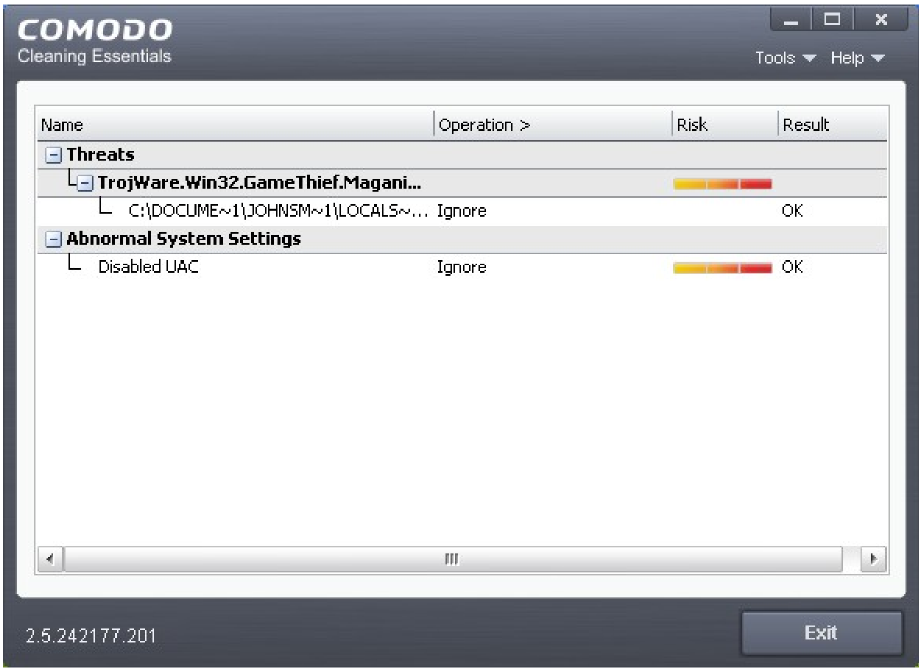


COMODO Cleaning Essentials(25)

Your computer will now be restarted in order to scan for hidden services.

4. Save all your work in the other windows and click Yes to restart your computer. If you plan to apply the operations at a later time, click No. The clean operations will be executed on the next restart of the computer.

Upon the restart, the application will scan for hidden processes and if it detects any,  will clean them and display the results.



| Name | Operation > | Risk | Result |
|---|---|---|---|
| ⊟ **Threats** | | | |
| ⊟ **TrojWare.Win32.GameThief.Magani...** | | 🟥 | |
| C:\DOCUME~1\JOHNSM~1\LOCALS~... | Ignore | | OK |
| ⊟ **Abnormal System Settings** | | | |
| Disabled UAC | Ignore | 🟥 | OK |

2.5.242177.201

## 2.2. Full Scan

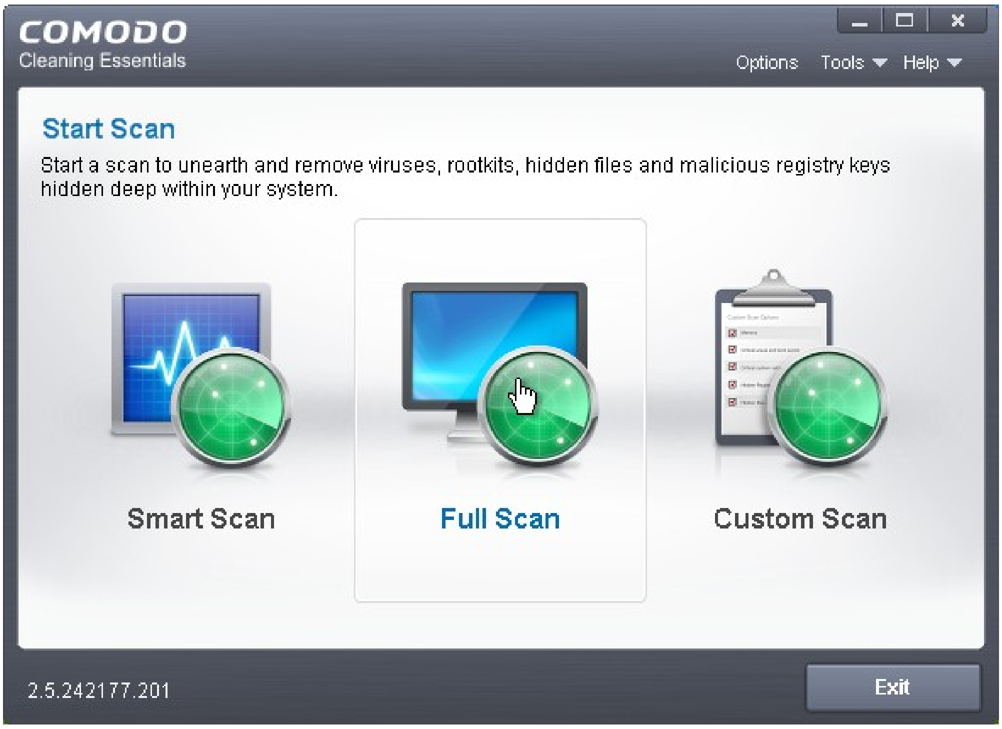
It is essential to run a full scan of your system periodically to detect any malware or viruses. During a full scan, CCE scans all areas including all partitions of hard disk drive, system memory of your computer to identify threats from viruses, malware, spyware and so on. Before commencing the scan, the application will restart your system in order to identify any hidden services or drivers created by rootkits, key loggers and so on.  Hence before starting  a full scan, save all your work and close all the other programs.

On completion of scanning, you can:

- Clean the detected threats or move them to Quarantine and later remove them;
- Exclude an application you consider as safe from the threat list;
- Report the threat as a False Positive to Comodo.

To start a Full scan

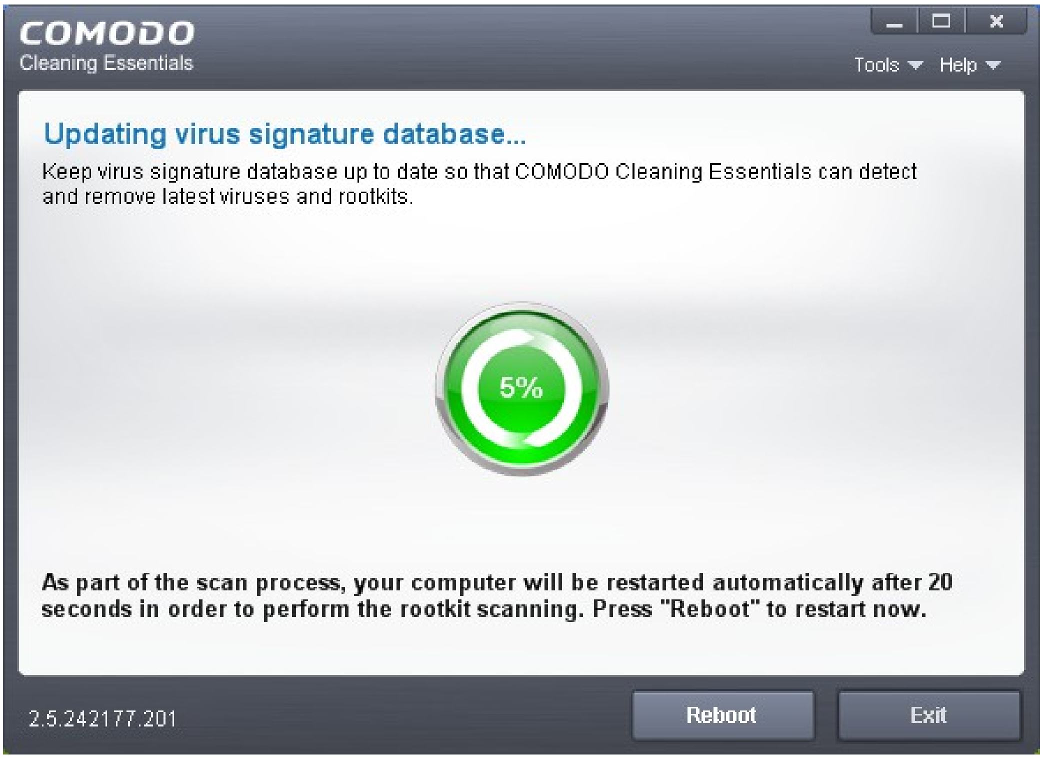
1. Click the 'Full Scan' from the CCE main interface.



Start Scan

Start a scan to unearth and remove viruses, rootkits, hidden files and malicious registry keys hidden deep within your system.

The application will ask your permission to restart the computer to perform rootkit scanning.



Updating virus signature database...

Keep virus signature database up to date so that COMODO Cleaning Essentials can detect and remove latest viruses and rootkits.

As part of the scan process, your computer will be restarted automatically after 20 seconds in order to perform the rootkit scanning. Press "Reboot" to restart now.

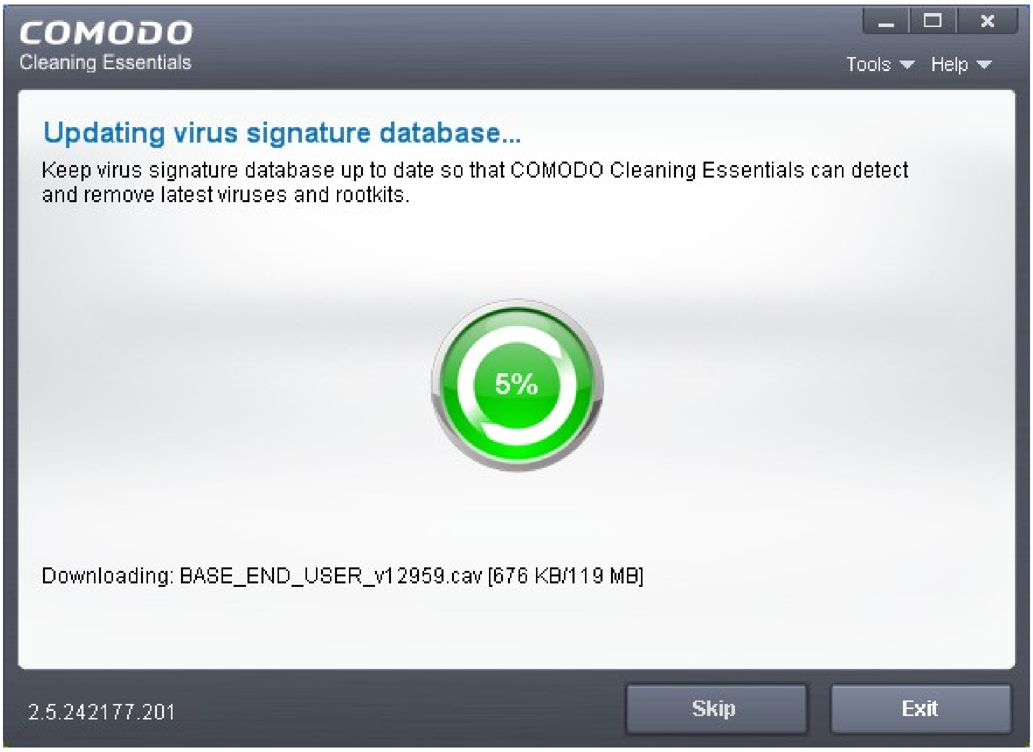
A rootkit is a type of malware that is designed to conceal the fact that the user's system has been compromised. Once installed, they camouflage themselves as (for example) standard operating system files, security tools and APIs used for diagnosis, scanning, and monitoring. Rootkits are usually not 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 restart, the application will check whether any updates are available for the virus database before commencing the scan. If available, it will first update the local virus database.



Updating virus signature database...

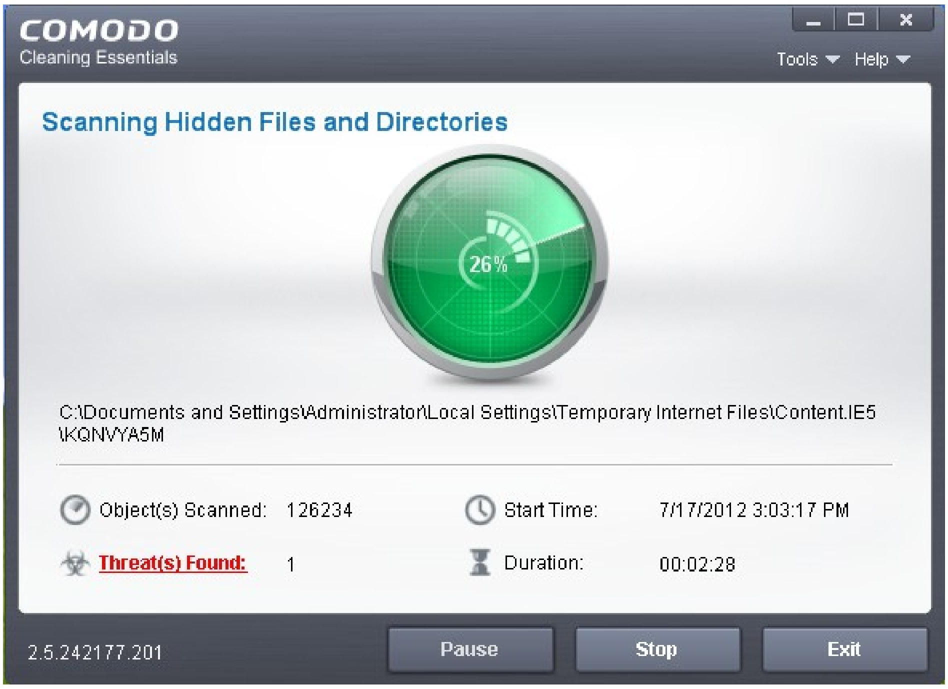
Keep virus signature database up to date so that COMODO Cleaning Essentials can detect and remove latest viruses and rootkits.

Downloading: BASE_END_USER_v12959.cav [676 KB/119 MB]

2.5.242177.201

It is advised that you always let the application to update the database as  scanning with your virus database up-to-date detects even the zero-hour threats. How ever, if you do not want the database update at this moment, you can skip this step by clicking 'Skip'.

The application will start scanning  your system and the progress will be displayed.



Scanning Hidden Files and Directories

C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5 \KQNVYA5M

Object(s) Scanned: 126234

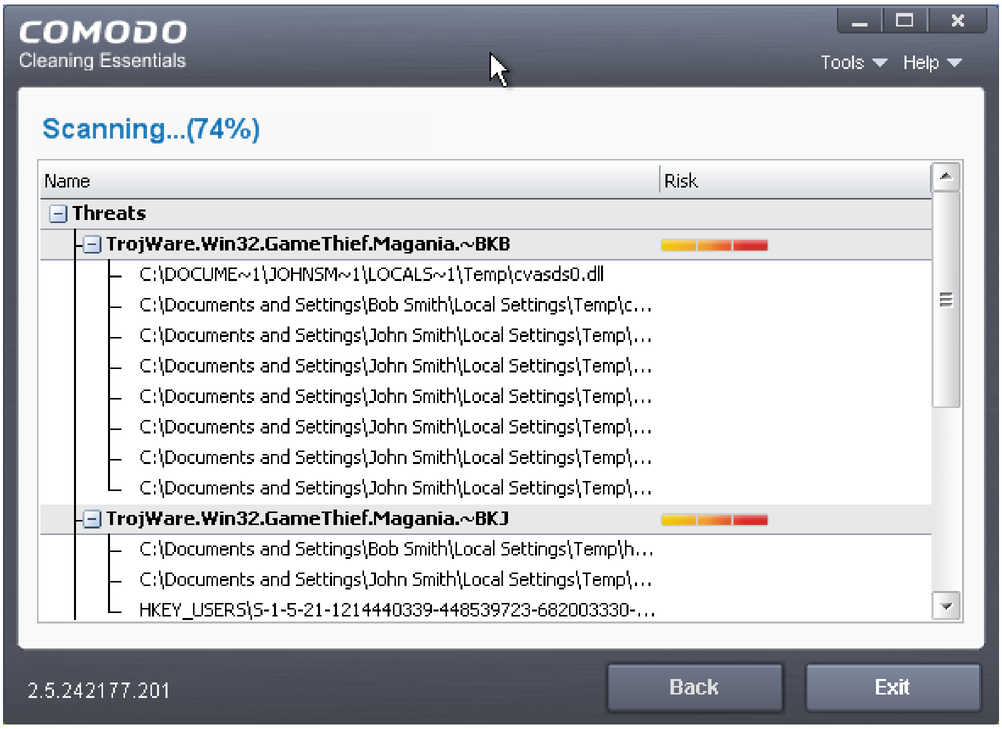
Start Time: 7/17/2012 3:03:17 PM

Threat(s) Found: 1

Duration: 00:02:28

2.5.242177.201

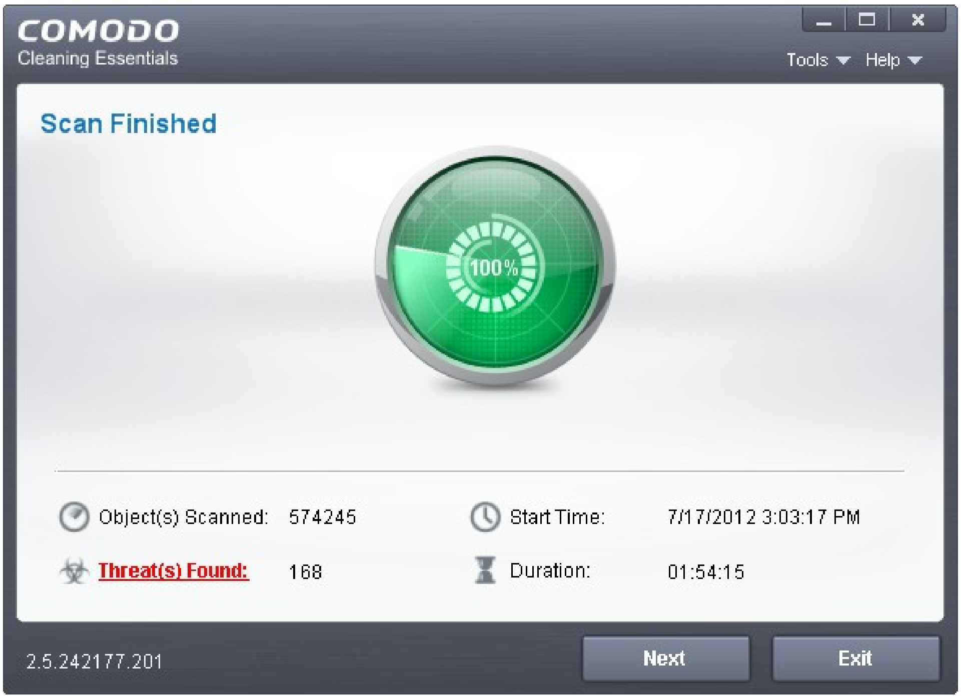
During the course of scanning, if you want to see details on the threats detected so far, click Threats Found link. A results window with the threats identified thus far will be displayed.



Scanning...(74%)

| Name | Risk |
|---|---|
| Threats | |
| TrojWare.Win32.GameThief.Magania.~BKB | 🟥 |
| C:\DOCUME~1\JOHNSM~1\LOCALS~1\Temp\cvasds0.dll | |
| C:\Documents and Settings\Bob Smith\Local Settings\Temp\c... | |
| C:\Documents and Settings\John Smith\Local Settings\Temp\... | |
| C:\Documents and Settings\John Smith\Local Settings\Temp\... | |
| C:\Documents and Settings\John Smith\Local Settings\Temp\... | |
| C:\Documents and Settings\John Smith\Local Settings\Temp\... | |
| C:\Documents and Settings\John Smith\Local Settings\Temp\... | |
| C:\Documents and Settings\John Smith\Local Settings\Temp\... | |
| TrojWare.Win32.GameThief.Magania.~BKJ | 🟥 |
| C:\Documents and Settings\Bob Smith\Local Settings\Temp\h... | |
| C:\Documents and Settings\John Smith\Local Settings\Temp\... | |
| HKEY_USERS\S-1-5-21-1214440339-448539723-682003330-... | |

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



Scan Finished

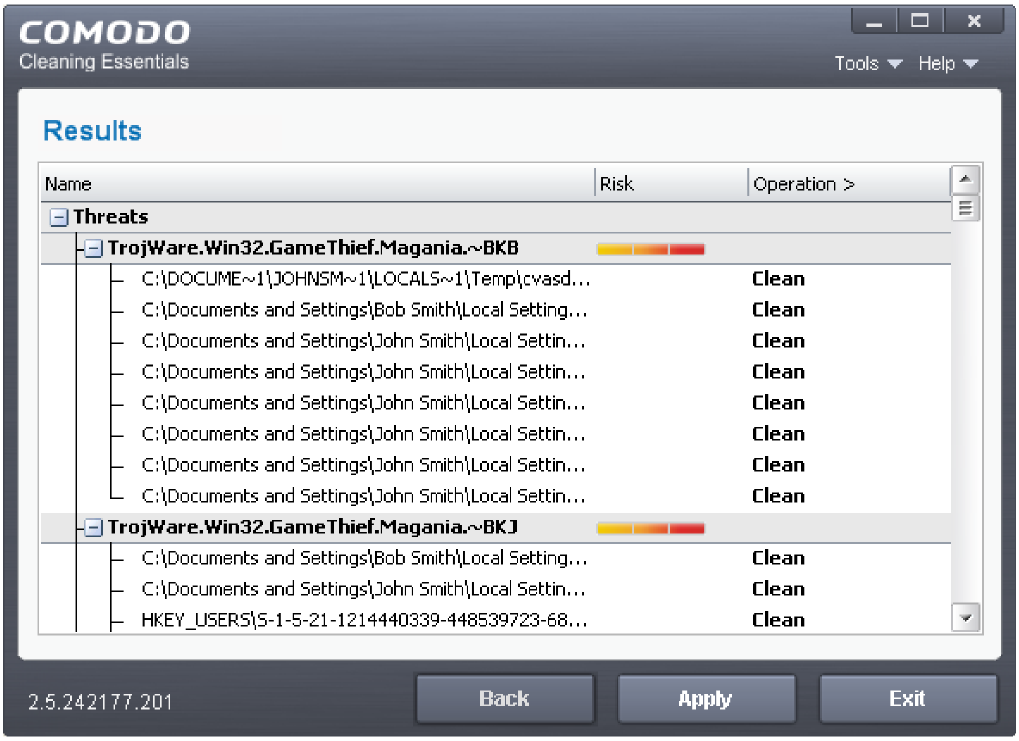
Object(s) Scanned: 574245

Start Time: 7/17/2012 3:03:17 PM

Threat(s) Found: 168

Duration: 01:54:15

2. Click 'Next' to view the results.

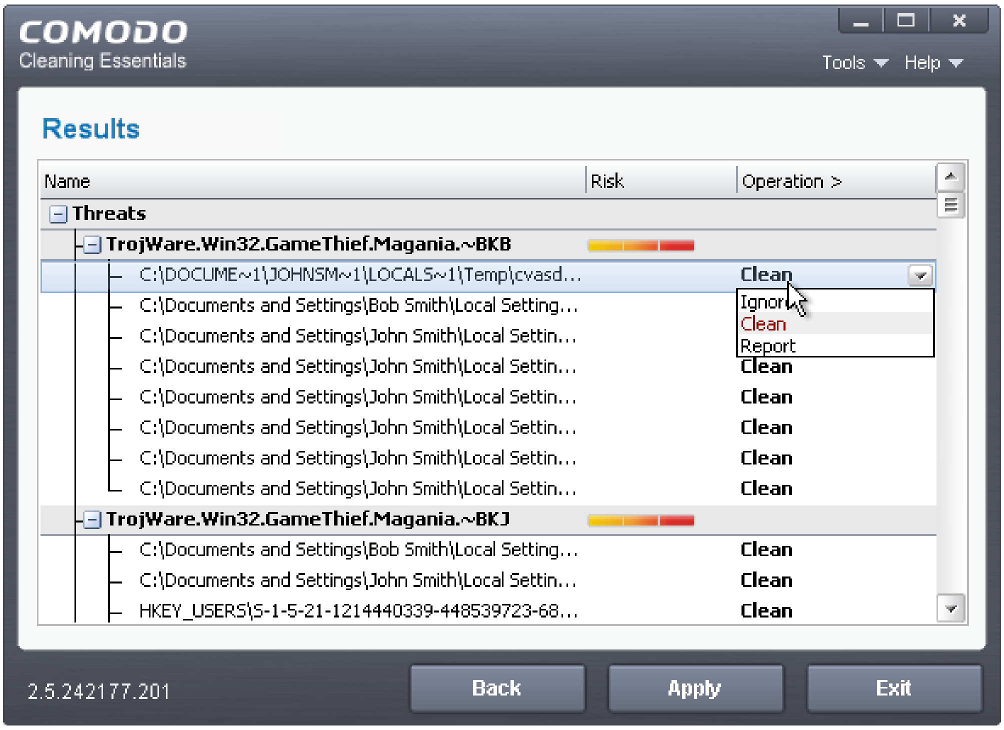


| Name | Risk | Operation > |
|---|---|---|
| Threats | | |
| TrojWare.Win32.GameThief.Magania.~BKB | | |
| C:\DOCUME~1\JOHNSM~1\LOCALS~1\Temp\cvasd... | | Clean |
| C:\Documents and Settings\Bob Smith\Local Setting... | | Clean |
| C:\Documents and Settings\John Smith\Local Settin... | | Clean |
| C:\Documents and Settings\John Smith\Local Settin... | | Clean |
| C:\Documents and Settings\John Smith\Local Settin... | | Clean |
| C:\Documents and Settings\John Smith\Local Settin... | | Clean |
| C:\Documents and Settings\John Smith\Local Settin... | | Clean |
| C:\Documents and Settings\John Smith\Local Settin... | | Clean |
| TrojWare.Win32.GameThief.Magania.~BKJ | | |
| C:\Documents and Settings\Bob Smith\Local Setting... | | Clean |
| C:\Documents and Settings\John Smith\Local Settin... | | Clean |
| HKEY_USERS\S-1-5-21-1214440339-448539723-68... | | Clean |

- If malicious executables are discovered on your system, the 'Results' window displays the list of those items (Viruses, Malware and so on).

**Tip:** You can sort the scan results by alphabetical order by clicking the 'Threat Name' column header. Similarly you can sort the scan results based on the risk level by clicking the 'Risk' column header.

The 'Results' window allows you to quarantine and later remove, ignore the threat if it is a safe file or to submit it as a false positive to Comodo if you are sure about the authenticity of the file. The default operation is 'Clean', that means CCE will clean the threat if a disinfection routine is available for it, else, will move it to quarantine.

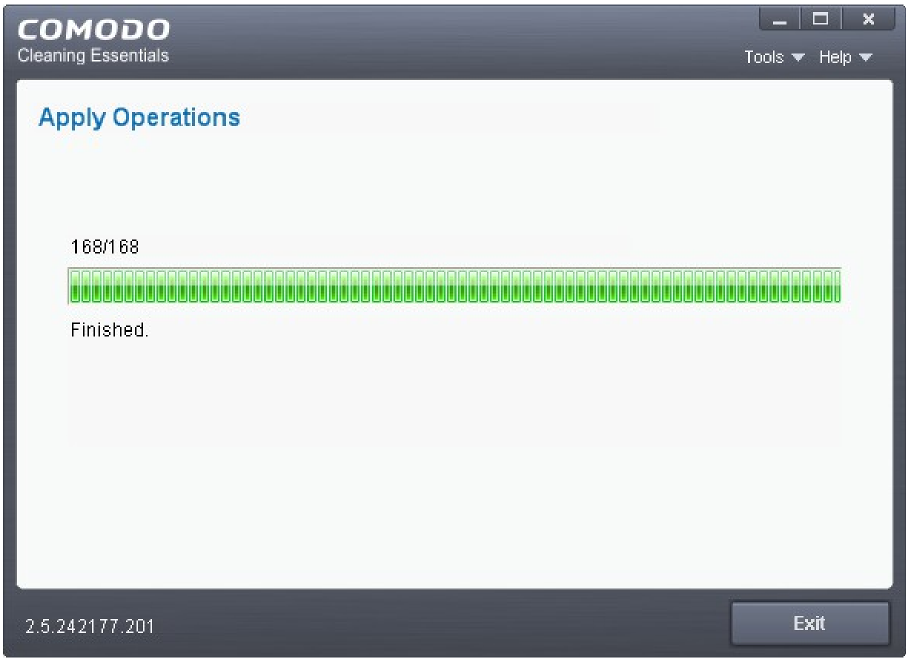


| Name | Risk | Operation > |
|---|---|---|
| Threats | | |
| TrojWare.Win32.GameThief.Magania.~BKB | | |
| C:\DOCUME~1\JOHNSM~1\LOCALS~1\Temp\cvasd... | | Clean |
| C:\Documents and Settings\Bob Smith\Local Setting... | | |
| C:\Documents and Settings\John Smith\Local Settin... | | |
| C:\Documents and Settings\John Smith\Local Settin... | | Clean |
| C:\Documents and Settings\John Smith\Local Settin... | | Clean |
| C:\Documents and Settings\John Smith\Local Settin... | | Clean |
| C:\Documents and Settings\John Smith\Local Settin... | | Clean |
| C:\Documents and Settings\John Smith\Local Settin... | | Clean |
| TrojWare.Win32.GameThief.Magania.~BKJ | | |
| C:\Documents and Settings\Bob Smith\Local Setting... | | Clean |
| C:\Documents and Settings\John Smith\Local Settin... | | Clean |
| HKEY_USERS\S-1-5-21-1214440339-448539723-68... | | Clean |

- To clean a  threat, click on the entry under the Operations column and select 'Clean'. The file will be disinfected or moved to quarantine upon applying the operation. You can later remove the file from your system from the 'Quarantined Items' interface. Refer to **Managing Quarantined Items** for more details.

- To ignore a threat if you consider the file is safe, click on the entry under the Operations column and select 'Ignore'.
- To report threat as a false-positive result, click on the entry under the Operations column and select 'Report'. The file will be sent to Comodo. Experts in Comodo will analyze the file and add it to whitelist, if found safe.
- To apply a common operation to all the entries in the list, click on the Operations column header and select the required action.

3. Click 'Apply' to apply the selected operations to the threats. The selected operations will be applied...



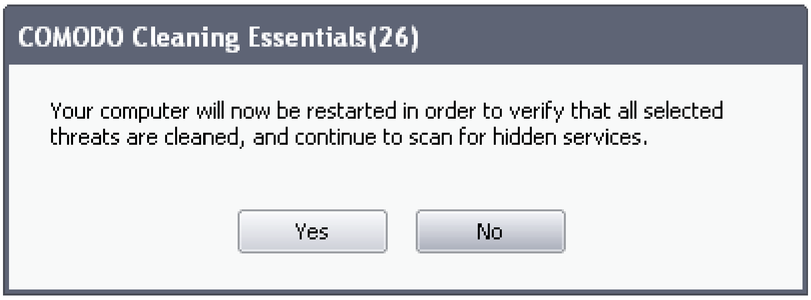
Apply Operations

168/168

Finished.

2.5.242177.201

... and your system will restart to check whether the operations are applied correctly and start scanning your system for  hidden services and drivers.



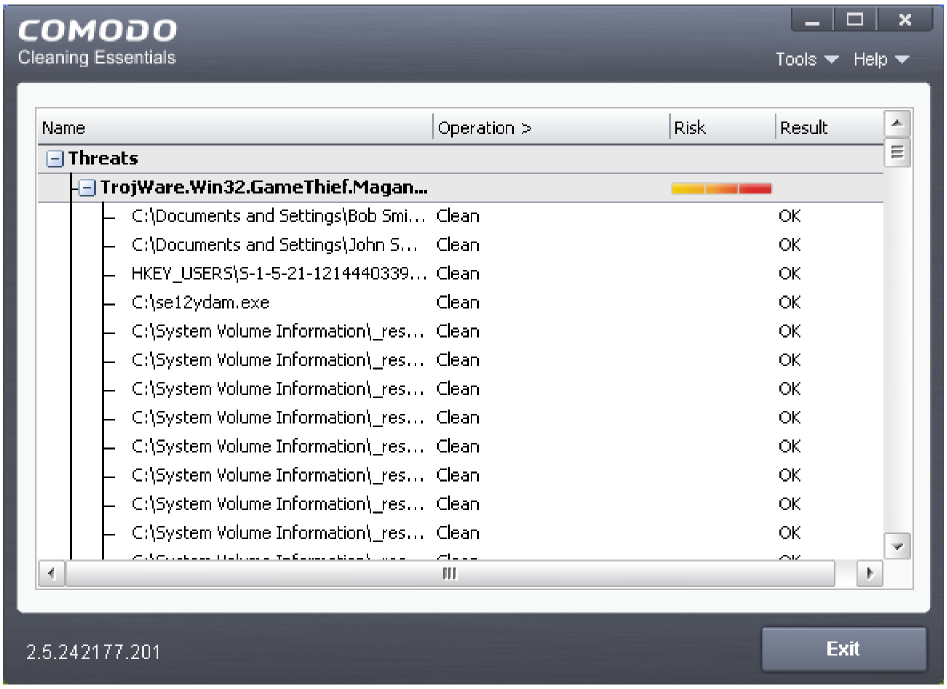
COMODO Cleaning Essentials(26)

Your computer will now be restarted in order to verify that all selected threats are cleaned, and continue to scan for hidden services.

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 your computer.
- If you plan to apply the operations at a later time, click No. The clean operations  will be checked and scan for hidden services will be resumed on the next restart of the computer.

The results will be displayed.



| Name | Operation > | Risk | Result |
|---|---|---|---|
| Threats | | | |
| TrojWare.Win32.GameThief.Magan... | | 🟥 | |
| C:\Documents and Settings\Bob Smi... | Clean | | OK |
| C:\Documents and Settings\John S... | Clean | | OK |
| HKEY_USERS\S-1-5-21-1214440339... | Clean | | OK |
| C:\se12ydam.exe | Clean | | OK |
| C:\System Volume Information_res... | Clean | | OK |
| C:\System Volume Information_res... | Clean | | OK |
| C:\System Volume Information_res... | Clean | | OK |
| C:\System Volume Information_res... | Clean | | OK |
| C:\System Volume Information_res... | Clean | | OK |
| C:\System Volume Information_res... | Clean | | OK |
| C:\System Volume Information_res... | Clean | | OK |
| C:\System Volume Information_res... | Clean | | OK |

2.5.242177.201

## 2.3. 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 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.

The system will require a restart to scan for hidden services and  drivers only if you choose to scan memory, critical areas, scan for hidden registry objects and services and hidden files and folders. Else no restart is required.

On completion of scanning, you can:

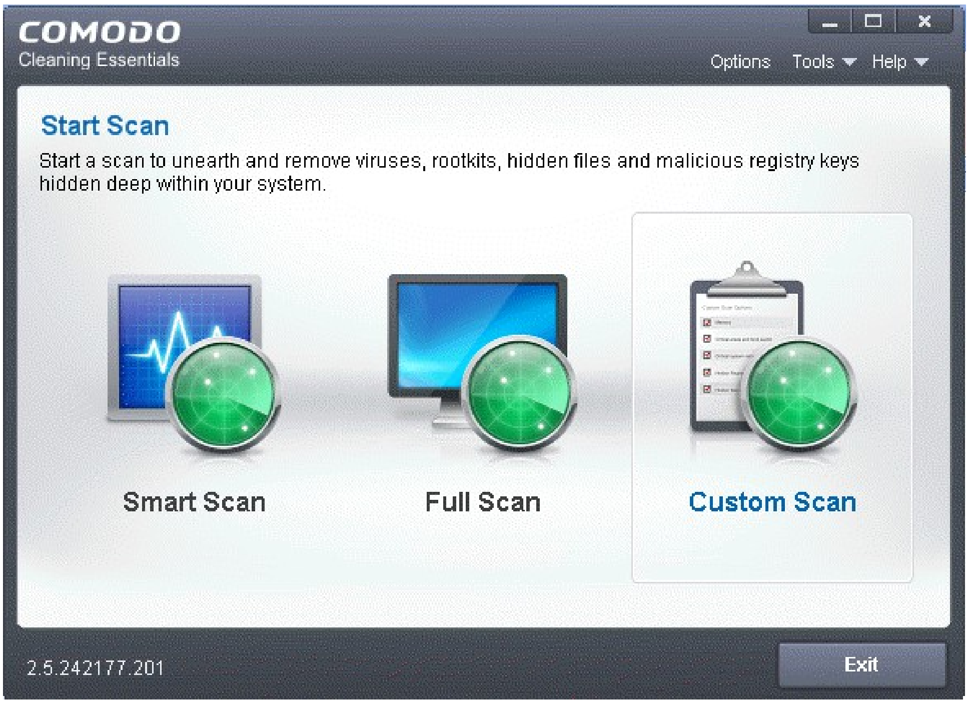
- Clean the detected threats or move them  to Quarantine and later remove them;
- Exclude an application you consider as safe from the threat list;
- Report the threat as a False Positive to Comodo.

Comodo Cleaning Essentials allows you to:

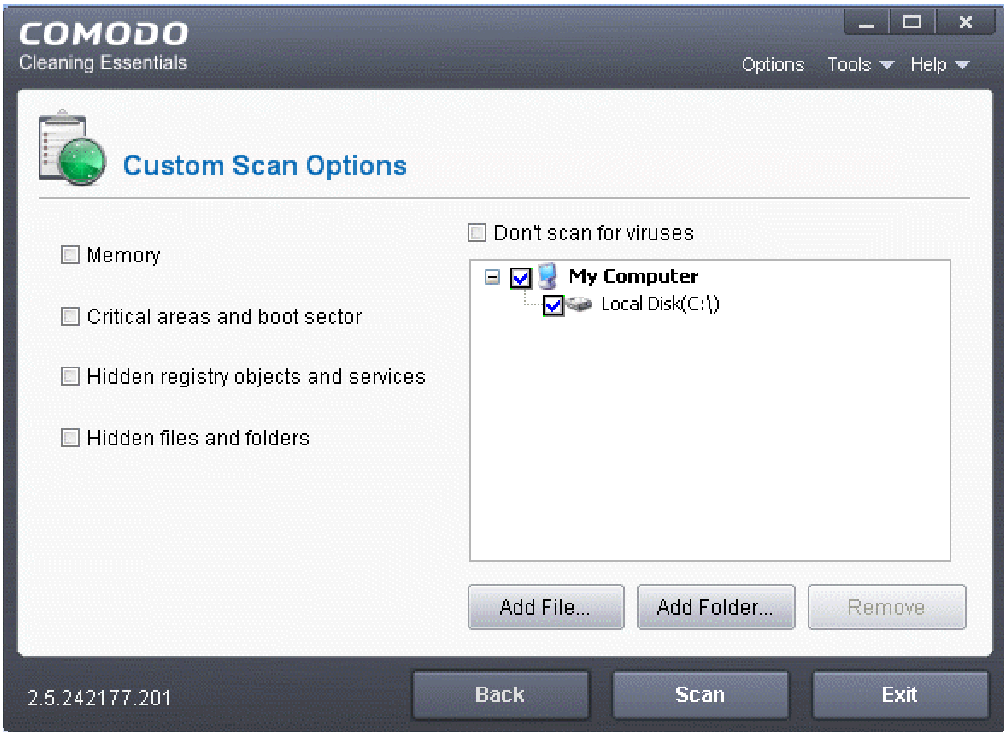
- **Start a Custom Scan on selected  folder(s)/file(s) with configuration of scan options**
- **Instantly scan a file or folder**

### Starting a Custom Scan

1. Click the 'Custom  Scan' from the CCE main interface.


COMODO
Cleaning Essentials
Options
Tools
Help
Start Scan
Start a scan to unearth and remove viruses, rootkits, hidden files and malicious registry keys hidden deep within your system.
Smart Scan
Full Scan
Custom Scan
2.5.242177.201
Exit

The Custom Scan Setting dialog window will be displayed.



□ Memory

□ Critical areas and boot sector

□ Hidden registry objects and services

□ Hidden files and folders

□ Don't scan for viruses

☑ My Computer
- ☑ Local Disk(C:\)

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.

2. Choose the Scan Options

- **Memory -** When selected, CCE scans the system memory during the start of any custom scan.
- **Critical areas and Boot Sector** - When selected, CCE scans the Program Files folder and WINDOWS folder of the Operating System of your computer and the Boot Sector of your hard disk drive during the start of any custom scan.
- **Hidden registry objects and Services -** When selected, all the hidden registry objects will be scanned by CCE during the start of any custom scan.
- **Hidden files and 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 as specified by the above options. This option is only for scanning the above said areas and not on any target areas in your hard disk drive. Hence, the target selection area will become inactive and grayed out.

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

- CCE won't invoke AV engine entirely.
- You must choose at least one of other options:

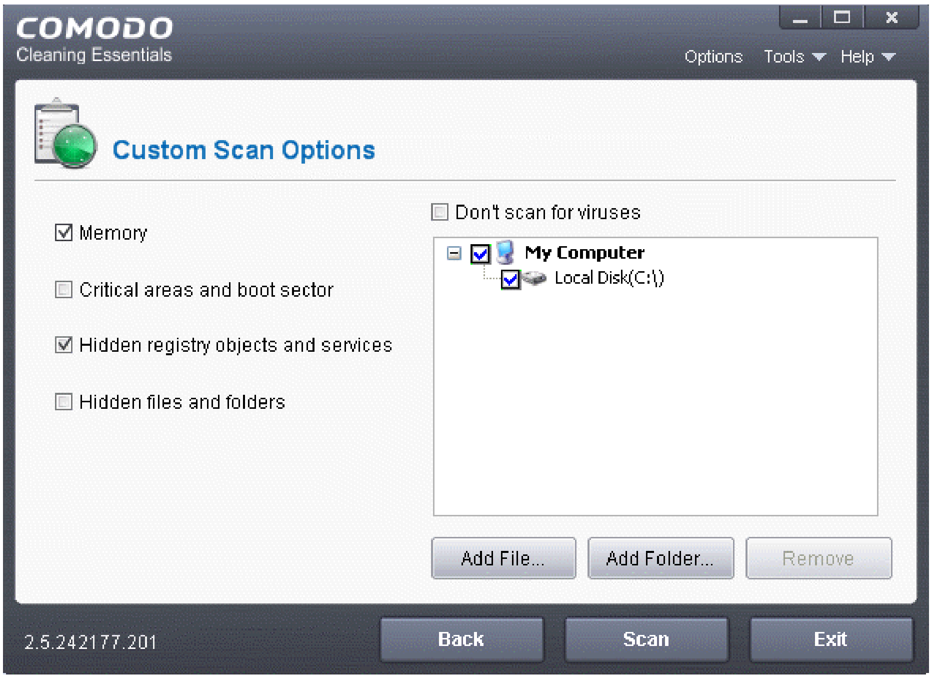
i. Memory

ii. Critical areas and Boot Sector

iii. Hidden registry objects and Services

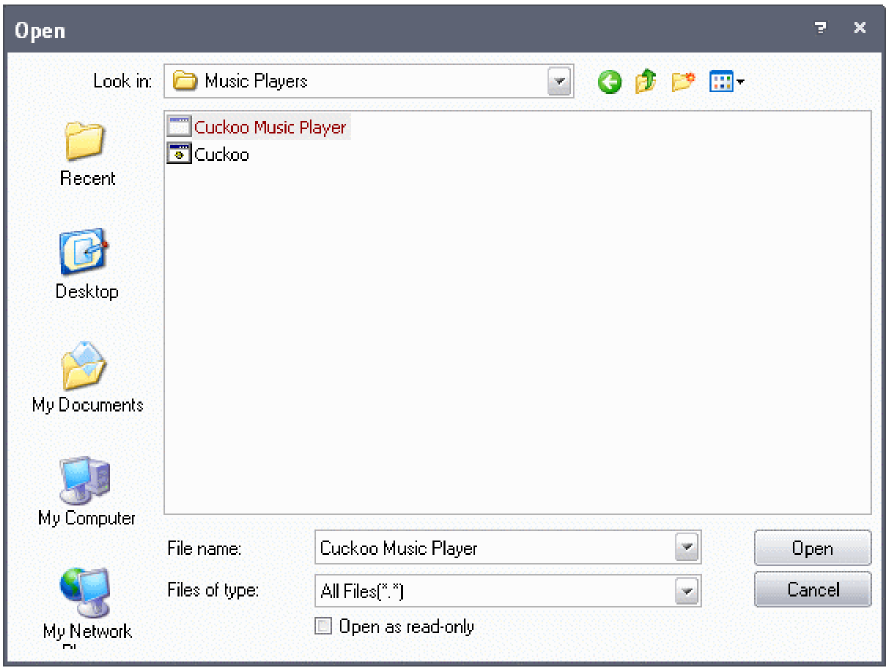
iv. Hidden files and folders

3. Choose the scan target area(s). By default, all the drives in your system will be selected for custom scan.



To add file(s)

- Click the ' Add Files'.
- Browse to the required file and click 'Open'



Look in: Music Players

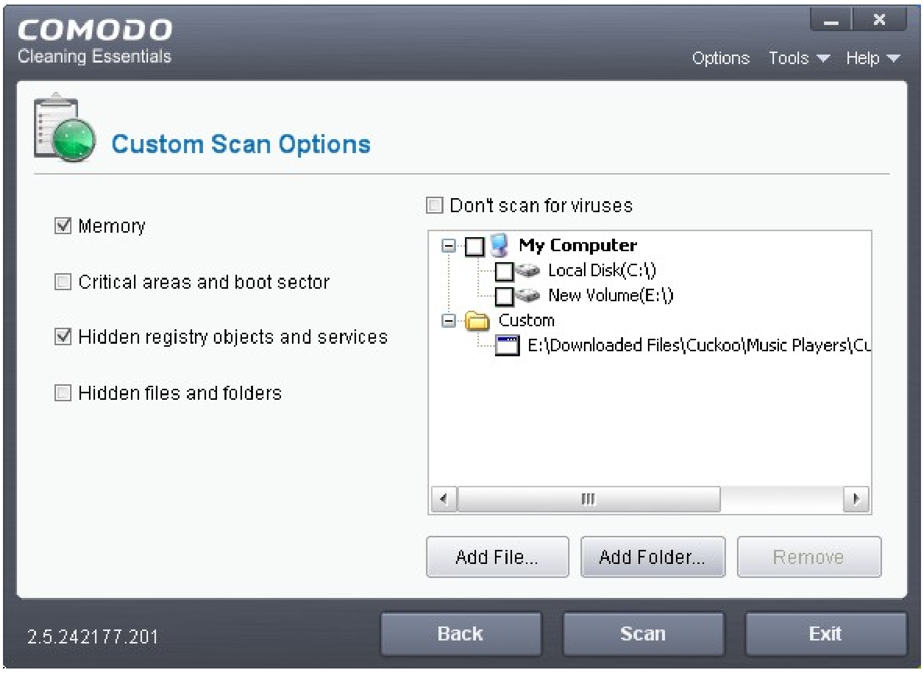
Cuckoo Music Player
Cuckoo

File name: Cuckoo Music Player

Files of type: All Files(*.*)

□ Open as read-only

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



Custom Scan Options

☑ Memory

□ Critical areas and boot sector

☑ Hidden registry objects and services

□ Hidden files and folders

□ Don't scan for viruses

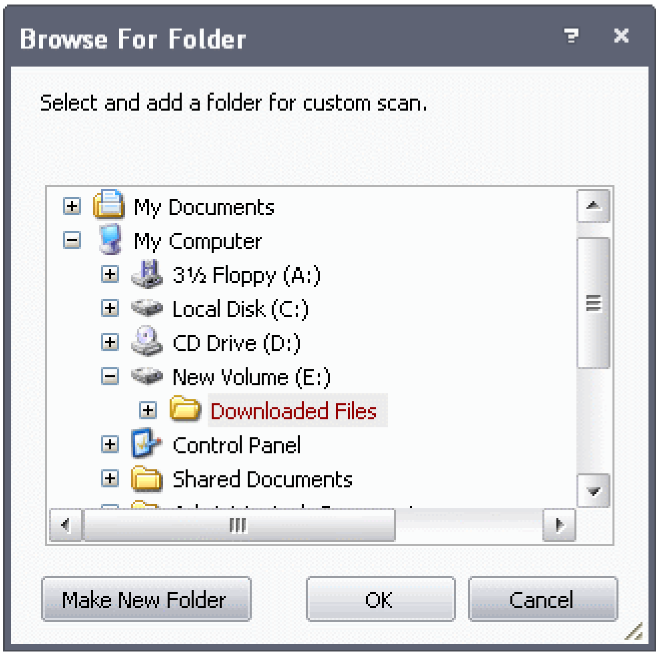
□ My Computer
□ Local Disk(C:\)
□ New Volume(E:\)
Custom
E:\Downloaded Files\Cuckoo\Music Players\Cu

2.5.242177.201

- You can add more files and folders for a simultaneous custom scan. Repeat the process to add more files.

To add Folder(s):

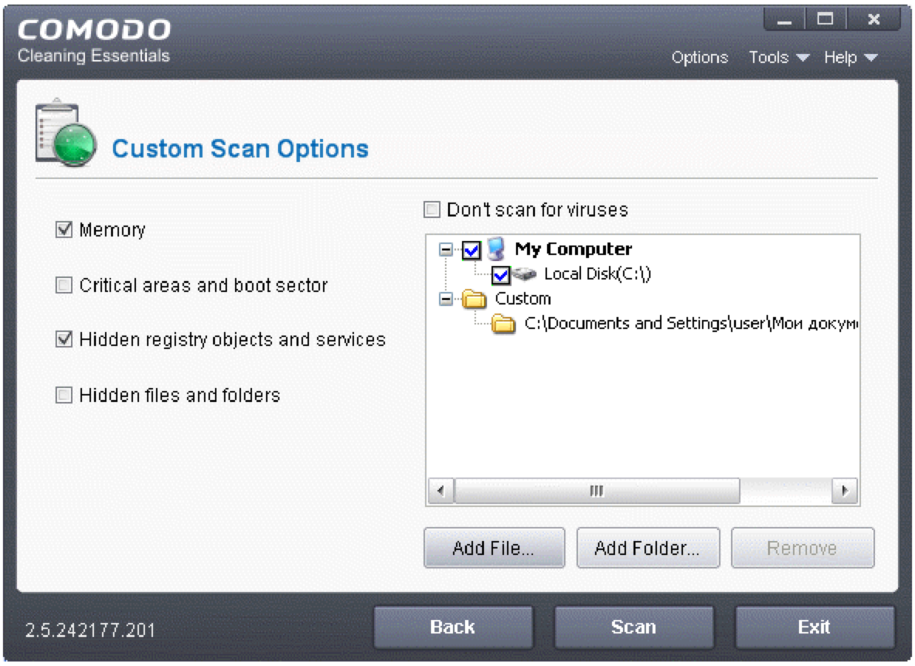
- Click the ' Add Folders'.
- Browse to the required folder and click 'OK'.



Browse For Folder

Select and add a folder for custom scan.

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



Custom Scan Options

☑ Memory

□ Critical areas and boot sector

☑ Hidden registry objects and services

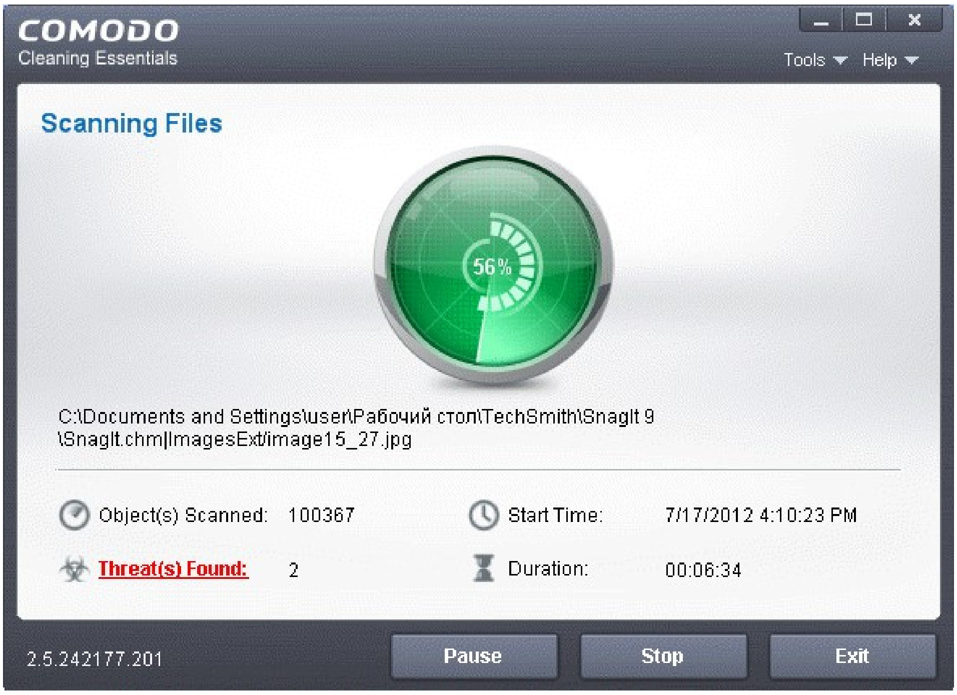
□ Hidden files and folders

□ Don't scan for viruses

2.5.242177.201

- You can add more files and folders for a simultaneous custom scan. Repeat the process to add more files.

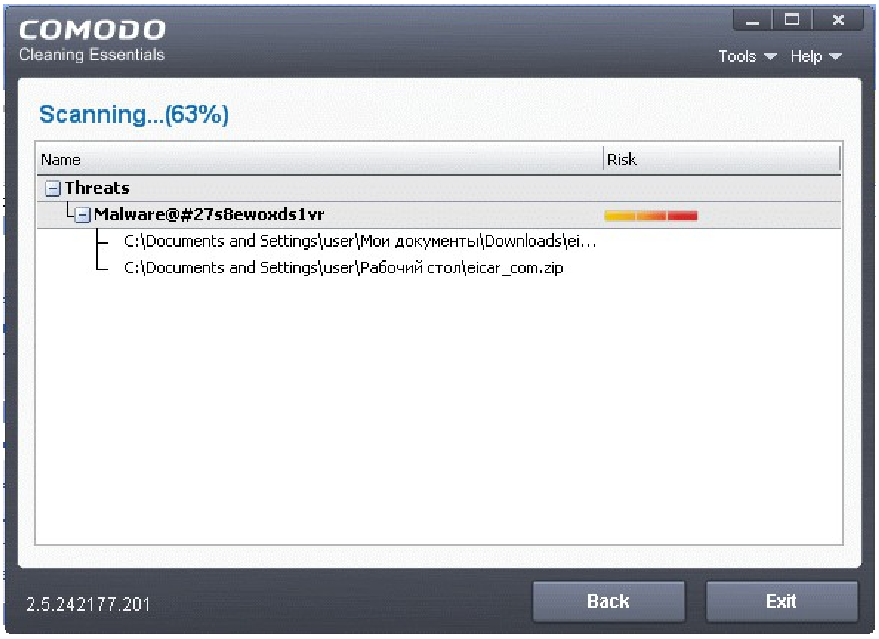
4. Click 'Scan' to run the custom scan. The selected file(s)/Folder(s) will be scanned with the scan options and the progress will be displayed.



C:\Documents and Settings\user\Рабочий стол\TechSmith\SnagIt 9\SnagIt.chm|ImagesExt/image15_27.jpg

Object(s) Scanned: 100367
Start Time: 7/17/2012 4:10:23 PM
Threat(s) Found: 2
Duration: 00:06:34

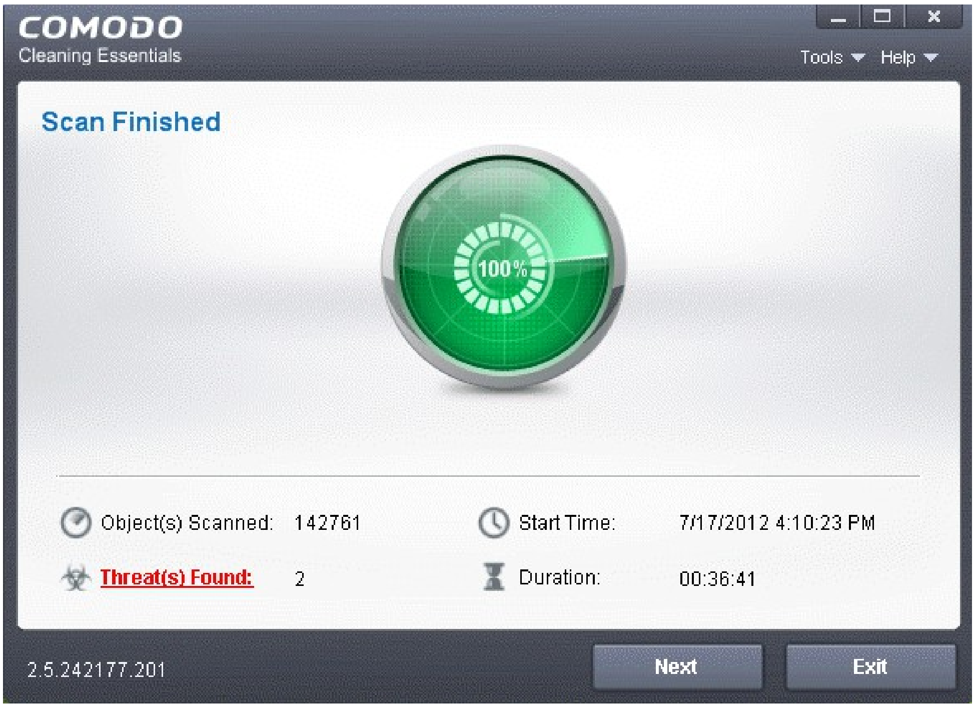
During the course of scanning, if you want to see details on the threats detected so far, click 'Threat(s) Found' link. A results window with the threats identified thus far will be displayed.



| Name | Risk |
|---|---|
| Threats | |
| Malware@#27s8ewoxds1vr | |
| C:\Documents and Settings\user\Мои документы\Downloads\ei... | |
| C:\Documents and Settings\user\Рабочий стол\eicar_com.zip | |

**The Results**

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



Scan Finished

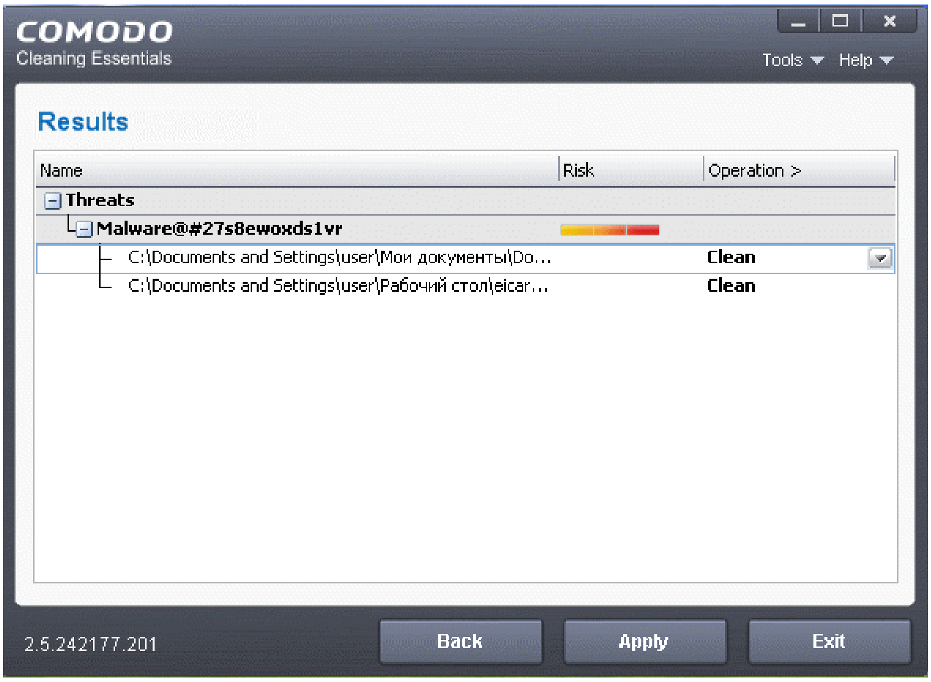
Object(s) Scanned: 142761

Threat(s) Found: 2

Start Time: 7/17/2012 4:10:23 PM

Duration: 00:36:41

5. Click 'Next' to view the results.



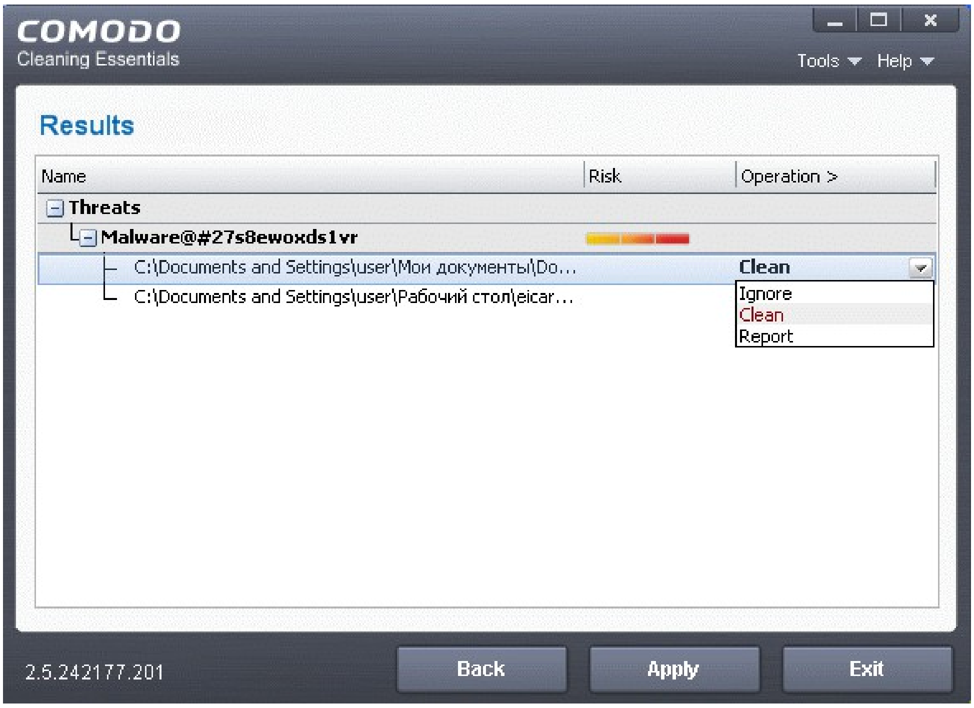
Results

| Name | Risk | Operation > |
|---|---|---|
| ⊟ Threats | | |
| ⊟ Malware@#27s8ewoxds1vr | 🟥 | |
| C:\Documents and Settings\user\Мои документы\Do… | | Clean |
| C:\Documents and Settings\user\Рабочий стол\eicar… | | Clean |

- If malicious executables are discovered on the scanned areas, the 'Results' window displays the list of those items (Viruses, Malware and so on).

**Tip:** You can sort the scan results by alphabetical order by clicking the 'Threat Name' column header. Similarly you can sort the scan results based on the risk level by clicking the 'Risk' column header.

The 'Results' window allows you to quarantine and later remove, ignore the threat if it is a safe file or to submit it as a false positive to Comodo if you are sure about the authenticity of the file. The default operation is 'Clean', that means CCE will clean the threat if a disinfection routine is available for it, else, will move it to quarantine.

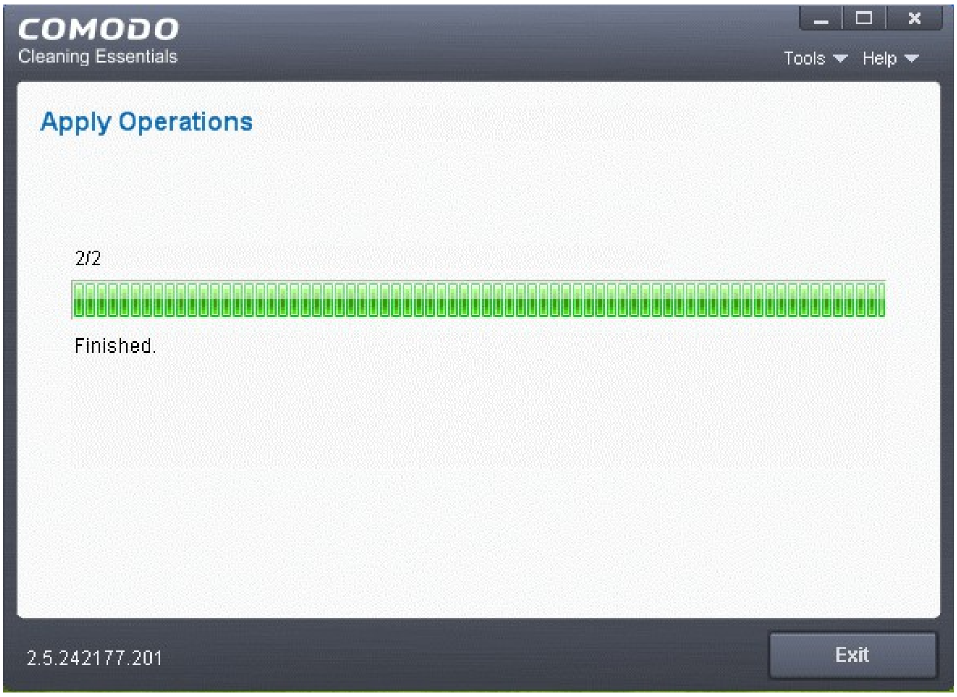


Results

| Name | Risk | Operation > |
|---|---|---|
| Threats | | |
| Malware@#27s8ewoxds1vr | | |
| C:\Documents and Settings\user\Мои документы\Do… | | Clean |
| C:\Documents and Settings\user\Рабочий стол\eicar… | | |

- To clean a  threat, click on the entry under the Operations column and select 'Clean'. The file will be disinfected or moved to quarantine upon applying the operation. You can later remove the file from your system from the 'Quarantined Items' interface. Refer to **Managing Quarantined Items** for more details.
- To ignore a threat if you consider the file is safe, click on the entry under the Operations column and select 'Ignore'.
- To report threat as a false-positive result, click on the entry under the Operations column and select 'Report'. The file will be sent to Comodo. Experts in Comodo will analyze the file and add it to whitelist, if found safe.
- To apply a common operation to all the entries in the list, click on the Operations column header and select the required action.

6. Click 'Apply' to apply the selected operations to the threats. The selected operations will be applied.



Apply Operations

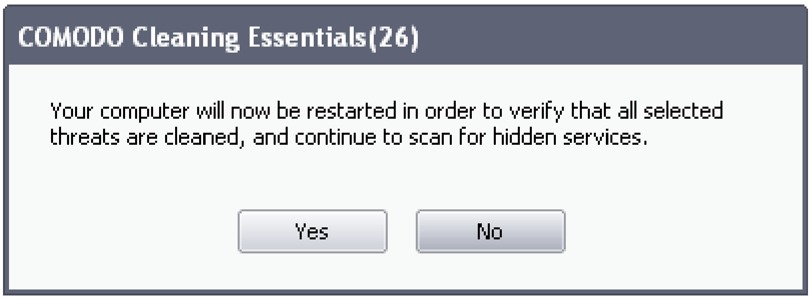
2/2

Finished.

If you have chosen at least anyone of the scan options from:

- Memory;
- Critical areas and Boot Sector;
- Hidden registry objects and Services;
- Hidden files and folders.

Your system will restart to check whether the operations are applied correctly and start scanning your system for hidden services and drivers.

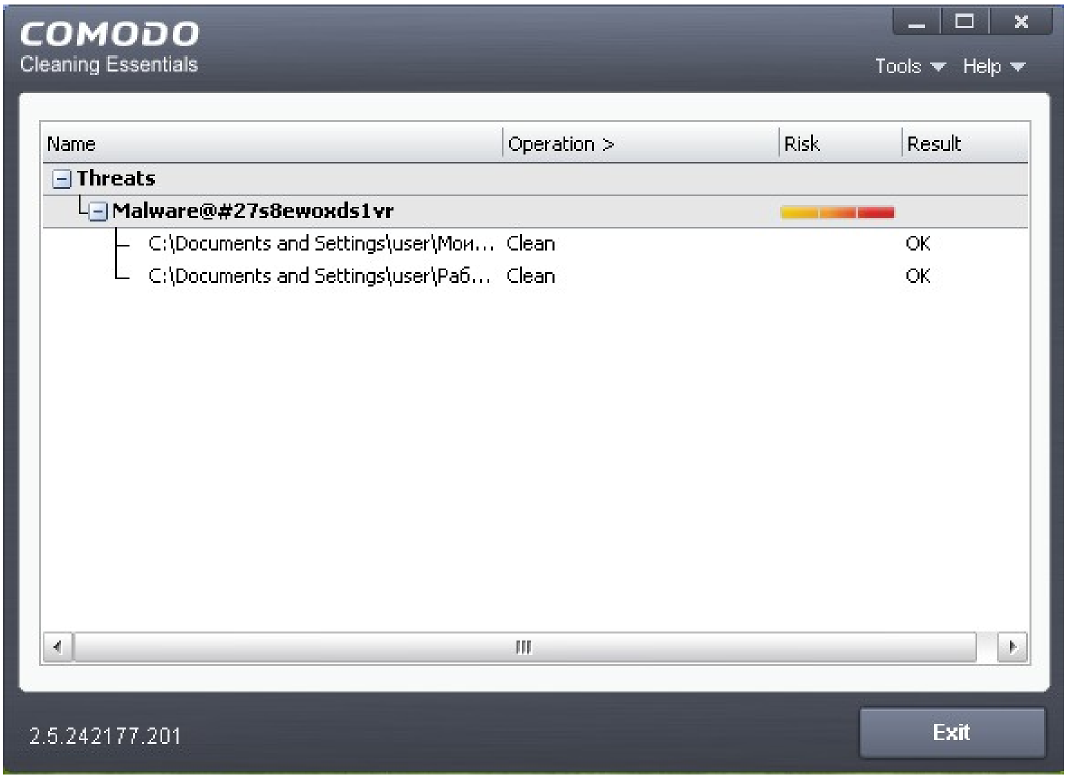

COMODO Cleaning Essentials(26)

Your computer will now be restarted in order to verify that all selected threats are cleaned, and continue to scan for hidden services.

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 your computer.
- If you plan to apply the operations at a later time, click No. The clean operations will be checked and scan for hidden services will be resumed on the next restart of the computer.

The results will be displayed.



| Name | Operation > | Risk | Result |
|---|---|---|---|
| Threats | | | |
| Malware@#27s8ewoxds1vr | | | |
| C:\Documents and Settings\user\Мои... | Clean | | OK |
| C:\Documents and Settings\user\Раб... | Clean | | OK |

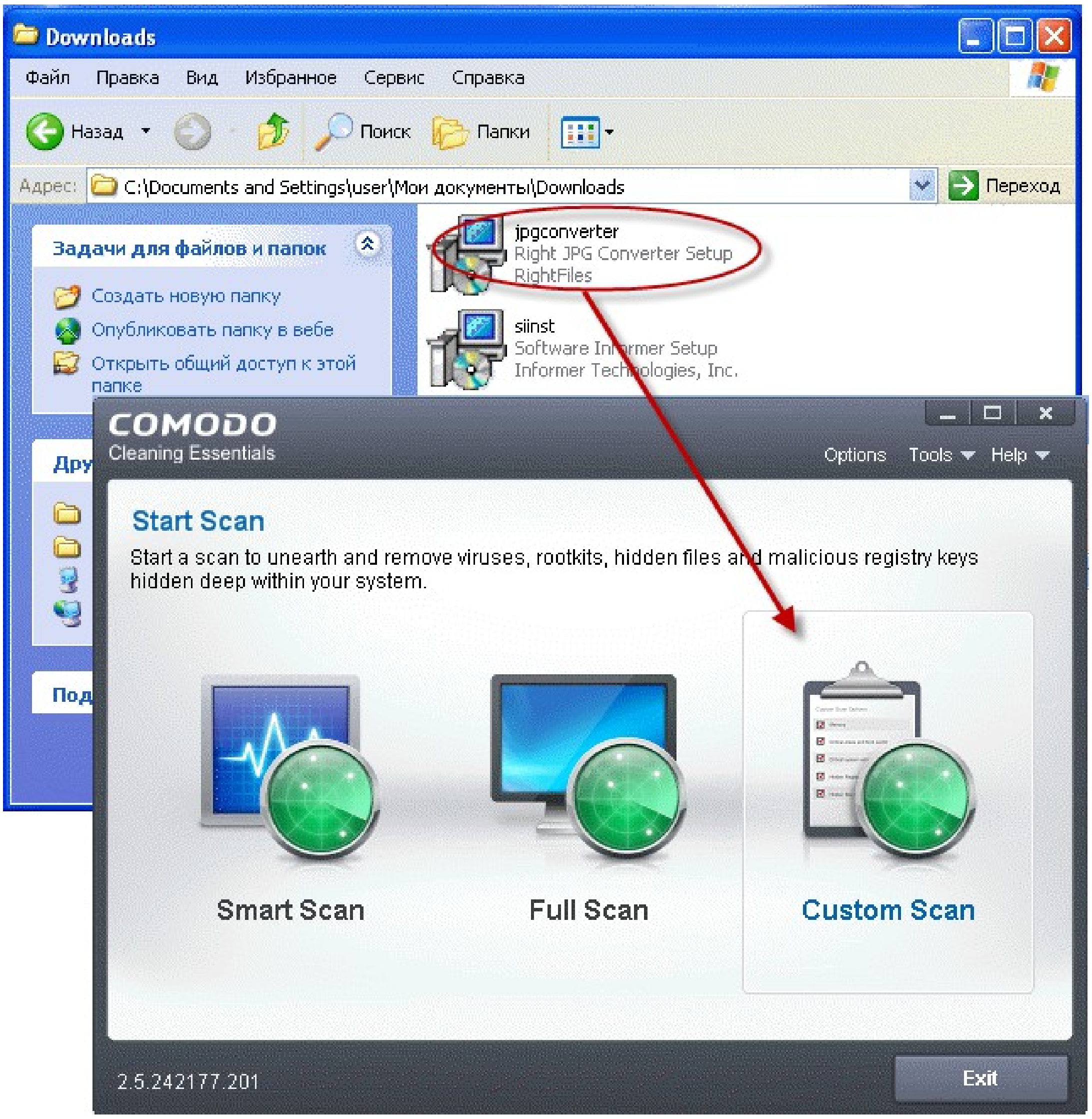
2.5.242177.201

## Instantly Scan Folder or File

You can scan a folder or file you just downloaded from Internet / copied in to your system of items in a removable storage device like a pen drive by dragging and dropping it on to the CCE interface.

**To instantly scan an item**

- Drag the item from its parent folder and drop it on to the CCE Interface

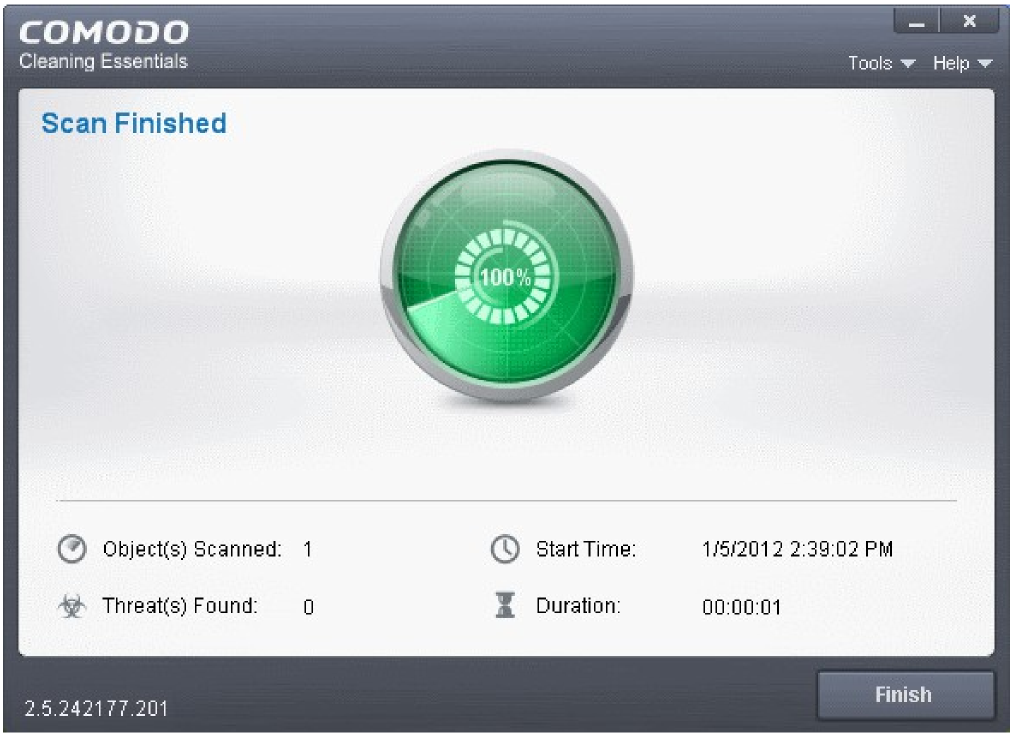


Downloads
Файл Правка Вид Избранное Сервис Справка
Назад
Поиск
Папки
Адрес: C:\Documents and Settings\user\Мои документы\Downloads
Переход
Задачи для файлов и папок
Создать новую папку
Опубликовать папку в вебе
Открыть общий доступ к этой папке
Дру
Под
jpgconverter
Right JPG Converter Setup
RightFiles
siinst
Software Informer Setup
Informer Technologies, Inc.
COMODO
Cleaning Essentials
Options
Tools
Help
Smart Scan
Full Scan
Custom Scan
2.5.242177.201
Exit

Start Scan

Start a scan to unearth and remove viruses, rootkits, hidden files and malicious registry keys hidden deep within your system.

The folder/file will be scanned immediately.



Scan Finished

Object(s) Scanned: 1

Threat(s) Found: 0

Start Time: 1/5/2012 2:39:02 PM

Duration: 00:00:01

2.5.242177.201

If any threats are found, the results will be displayed. Refer to **The Results** section for more details.

## 2.4. Comparison of Scan Types

### Scanners

The following table gives the descriptions of scanners used in Comodo Cleaning Essentials:

| Scanner | Description |
|---|---|
| Basic | Local Antivirus Scanner |
| FLS | File Lookup System. The FLS attempts to establish the trustworthiness of a file by running three sequential scans. First, a file is checked against the local Trusted Vendors List (TVL). If the file is not present on the TVL then it passes onto Cloud Vendor Verification (CVV). If the CVV test yields no results it passes onto Comodo's cloud based AV scanner. |
| CAMAS | Upload untrusted executables to COMODO Automated Malware Analysis System (CAMAS) for inspection (available if enabled in Options) |
| Memory | Scans running processes and modules |
| Hidden file | Scan for hidden files and directories |
| Hidden key | Scan for hidden keys and values |
| Hidden service | Scan for hidden services and drivers (requires restart) |
| Critical areas | Scan critical registry keys, system files and system configuration |
| MBR | Scan boot sector (Available if enabled in Options) |

### Scan Types

The following table gives the sequence of scanners employed while scanning various areas for different scan types. The symbol ' > ' indicates a sequential process. For example, 'Basic > FLS' means that the item is first checked using the Basic (local) AV scanner. Only if the file is not identified as malware by the Basic scan will the item pass onto the next type of scan – 'FLS'.

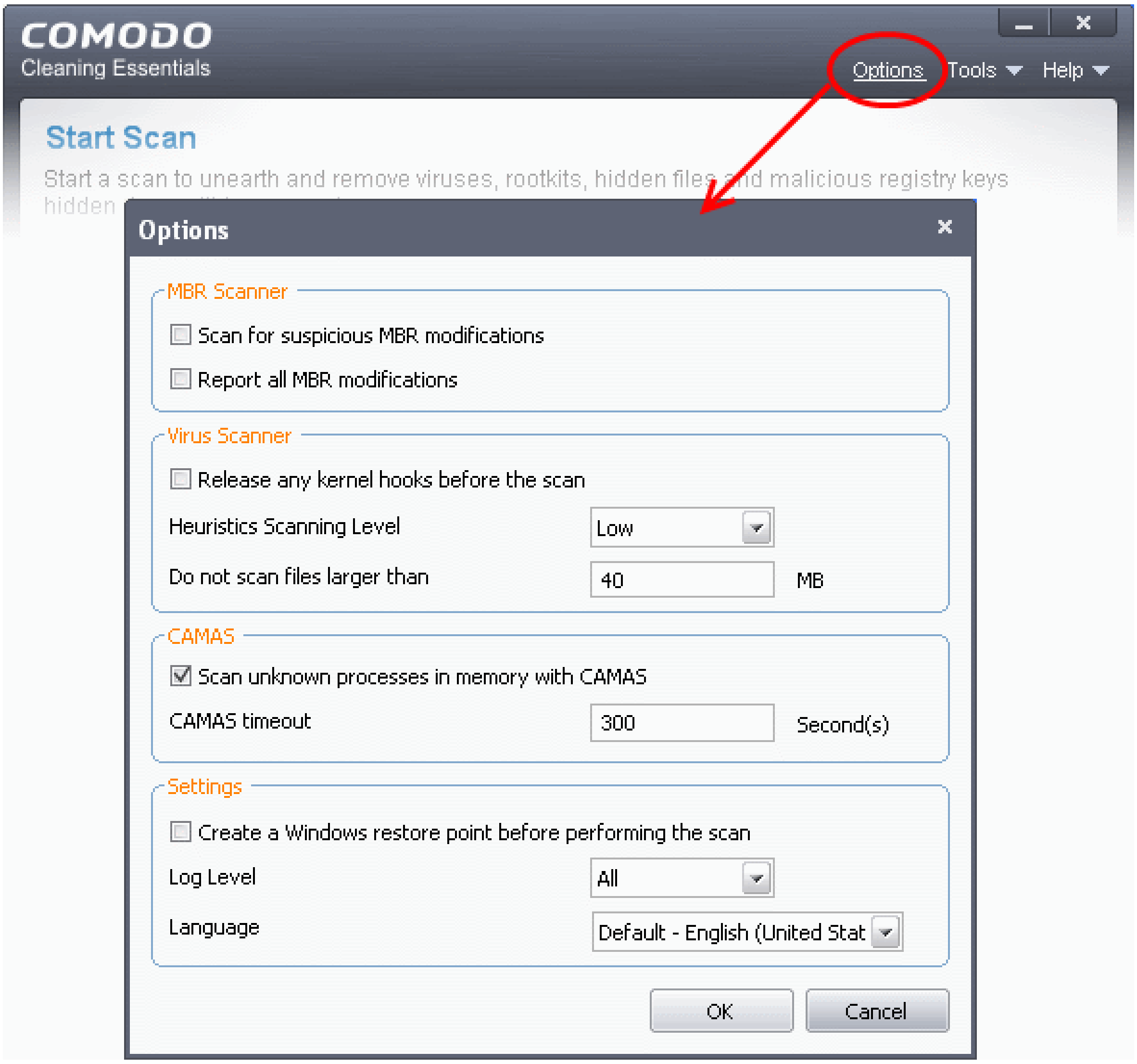
| Scan Options | Smart Scan | Full Scan | Custom Scan |
|---|---|---|---|

| | | | **(Scanners are the same as Full Scan)** |
|---|---|---|---|
| Memory | Basic>FLS<br>Scope: all running modules | Basic>FLS>CAMAS>Memory<br>Scope: all running modules | Optional. Scope: all running modules |
| Critical areas and boot sector | Critical areas>MBR<br>Scope: entire areas | Critical areas>MBR<br>Scope: entire areas | Optional. Scope: entire areas |
| Hidden registry objects and services | Hidden key>Hidden service<br>Scope: autorun registry entries | Hidden key>Hidden service<br>Scope: entire registry | Optional. Scope: entire registry |
| Hidden files and folders | Hidden file<br>Scope: autorun files | Hidden file<br>Scope: files in all drives | Optional. Scope: files in all drives |
| Virus | Basic>FLS<br>Scope: autorun files | Basic>FLS<br>Scope: files in all drives | Optional. Scope: Customizable |

# 3. Configuring Comodo Cleaning Essentials

CCE can be configured according to user preferences by clicking the 'Options' from the title bar. You can manage various functions such as scanning suspicious MBR entries, connection to CAMAS (Comodo Automated Malware Analysis System) for submitting suspicious files and more.

To access the Options interface, click 'Options' from the title bar controls.


COMODO
Cleaning Essentials
Options
Tools
Help
Start Scan
Start a scan to unearth and remove viruses, rootkits, hidden files and malicious registry keys
hidden
Options
OK
Cancel

MBR Scanner

□ Scan for suspicious MBR modifications

□ Report all MBR modifications

Virus Scanner

□ Release any kernel hooks before the scan

Heuristics Scanning Level: Low

Do not scan files larger than: 40 MB

CAMAS

☑ Scan unknown processes in memory with CAMAS

CAMAS timeout: 300 Second(s)

Settings

□ Create a Windows restore point before performing the scan

Log Level: All

Language: Default - English (United Stat

## MBR Options

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

## Virus Scanner Settings

- **Release any kernel hooks before the scan** - When selected, hooked kernel hooks will be released  before any scanning process. This option is for advanced users only.  Unhooking kernel hooks will deactivate any other security products installed in your system and may impair the stability of your system and/or can incur permanent data loss. Select this option only if you are an advanced user and have knowledge on the risks of the process.
- **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 recommends it for quarantine. Heuristics is about detecting virus-like behavior or attributes rather than looking for a precise virus signature that matches a signature on the virus blacklist.

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

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

  - **Off** - Selecting this option disables heuristic scanning. This means that virus scans only 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

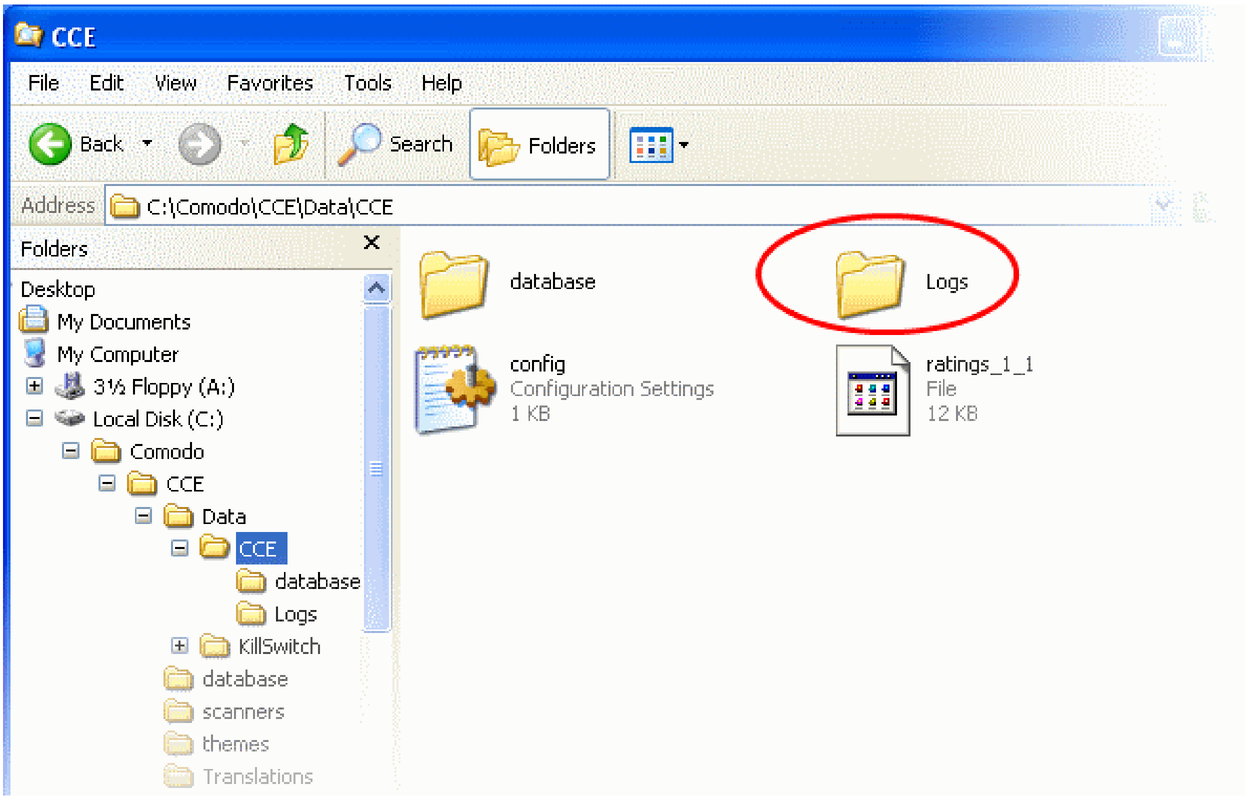
**CAMAS** - CAMAS (Comodo Automated Malware Analysis System) is a cloud based analysis system where the submitted files will undergo a thorough inspection by our cloud virus scanning and behavior monitoring systems to try to establish whether they contain malicious code. If the file exhibits malicious 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.
- **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

- **Create a Windows restore point before performing the scan** - When selected, CCE will create a Windows restore point before embarking on the scanning process. Should problems occur 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 folder <folder containing CCE files>\Data\CCE\Logs:



To view the logs:

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

  Or

- Click Tools > Browse Logs...

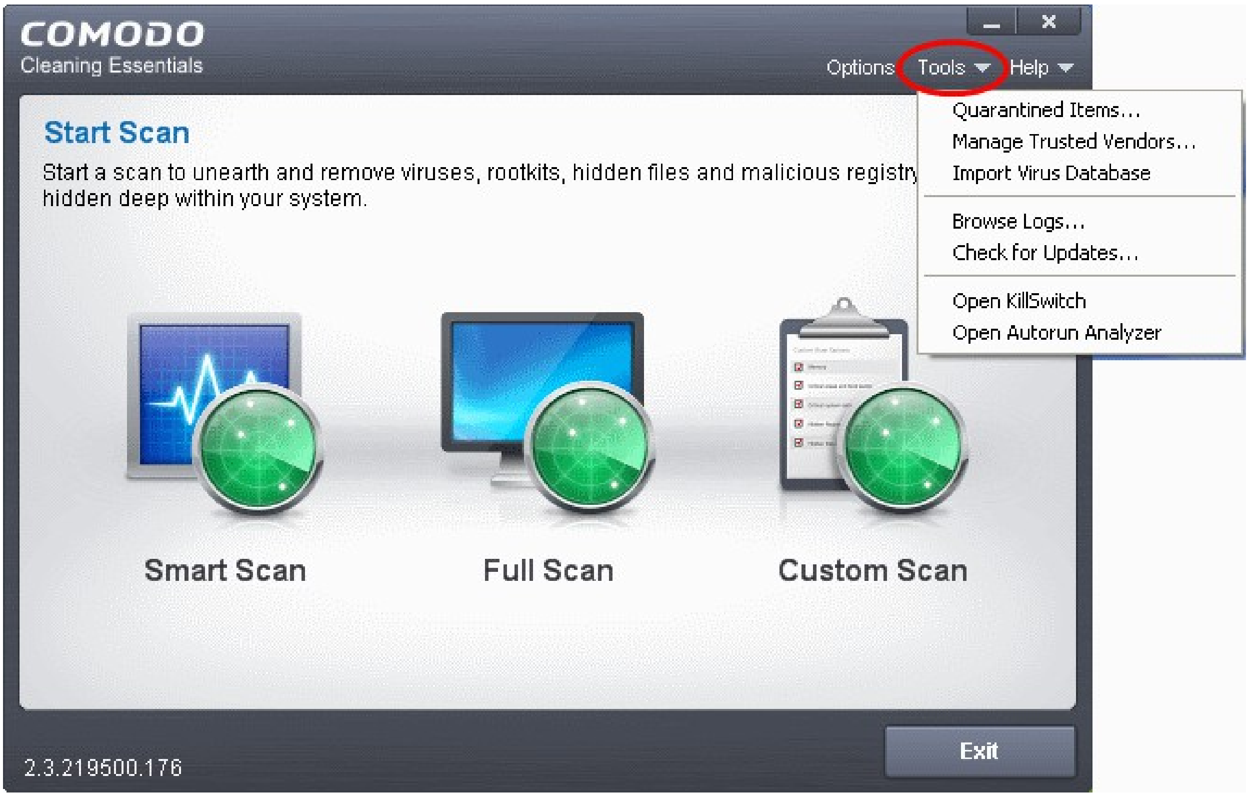
- **Select Language**- CCE is available in several languages and the default language is English (US). If you want to change the language, select your language from the drop-down menu.
- Click 'OK' for the settings to take effect .

# 4.The Tools Menu

The 'Tools' menu  enables you to manage quarantined items and local trusted vendors list and view logs. It also allows you to configure for importing virus database updates from a local storage or from other computer or a server in your network.

The tools menu contains shortcuts to open KillSwitch and Autorun Analyzer, valuable tools for optimizing your system performance.

The tools menu can be accessed by clicking 'Tools' from the title bar.



The 'Tools' menu has the following options:

- **Managing Quarantined Items** - Enables to manage the items moved to quarantine by various scans.
- **Managing Trusted Vendors** - Enables you to add and manage the vendors in the local Trusted Vendor List
- **Importing Antivirus Database** - Enables you to import virus database from your local storage or a network location.
- **Browse Logs** - Enables you to view the log of events recorded by the application.
- **Check for Updates** – Enables you to check whether updated version of the application is available.
- **Open KillSwitch** - Starts the KillSwitch utility
- **Open Autorun Analyzer** - Starts the Autorun Analyzer utility.

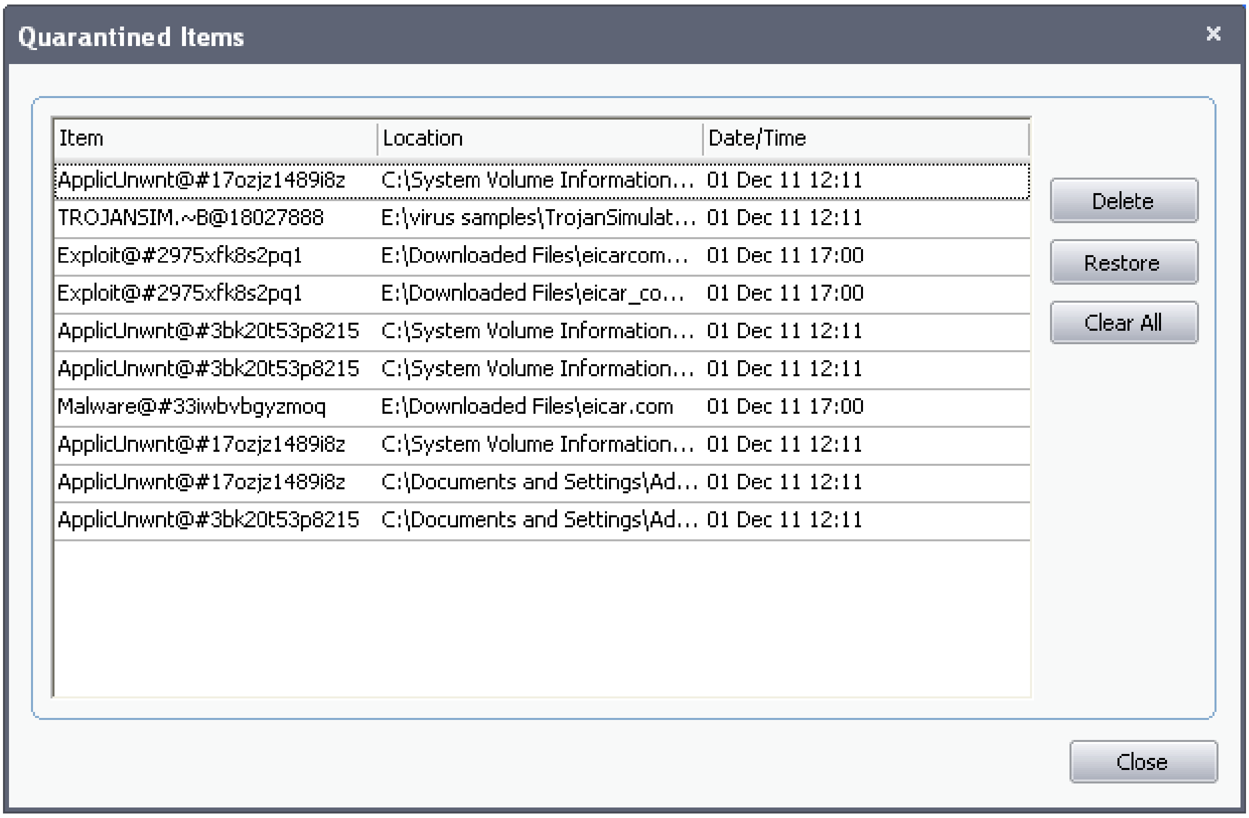
# 4.1.Managing Quarantined Items

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.

All the files cleaned using CCE are moved into Quarantine. You can later analyze these files and take the following measures:

- If the file could not be identified by you as safe, you can remove it from your system;
- If the file is safe and came from a trustworthy source, you can restore it to the original location.

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



| Item | Location | Date/Time |
|---|---|---|
| ApplicUnwnt@#17ozjz1489i8z | C:\System Volume Information... | 01 Dec 11 12:11 |
| TROJANSIM.~B@18027888 | E:\virus samples\TrojanSimulat... | 01 Dec 11 12:11 |
| Exploit@#2975xfk8s2pq1 | E:\Downloaded Files\eicarcom... | 01 Dec 11 17:00 |
| Exploit@#2975xfk8s2pq1 | E:\Downloaded Files\eicar_co... | 01 Dec 11 17:00 |
| ApplicUnwnt@#3bk20t53p8215 | C:\System Volume Information... | 01 Dec 11 12:11 |
| ApplicUnwnt@#3bk20t53p8215 | C:\System Volume Information... | 01 Dec 11 12:11 |
| Malware@#33iwbvbgyzmoq | E:\Downloaded Files\eicar.com | 01 Dec 11 17:00 |
| ApplicUnwnt@#17ozjz1489i8z | C:\System Volume Information... | 01 Dec 11 12:11 |
| ApplicUnwnt@#17ozjz1489i8z | C:\Documents and Settings\Ad... | 01 Dec 11 12:11 |
| ApplicUnwnt@#3bk20t53p8215 | C:\Documents and Settings\Ad... | 01 Dec 11 12:11 |

## 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.

From this interface you can:

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

### To delete a quarantined item from the system

- Select the item and Click 'Delete'.

This deletes the file from your system permanently.

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

- Select the item and click 'Restore'.

If the restored item does not contain a malware, it operates as usual. But if it contains a malware, it will be detected as a threat , during the next scan and moved to quarantine if you perform 'Clean' operation.

### To remove all the quarantined items permanently

- Click 'Clear All'.

This deletes all the quarantined items from your system permanently.

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

# 4.2. Managing Trusted Vendors

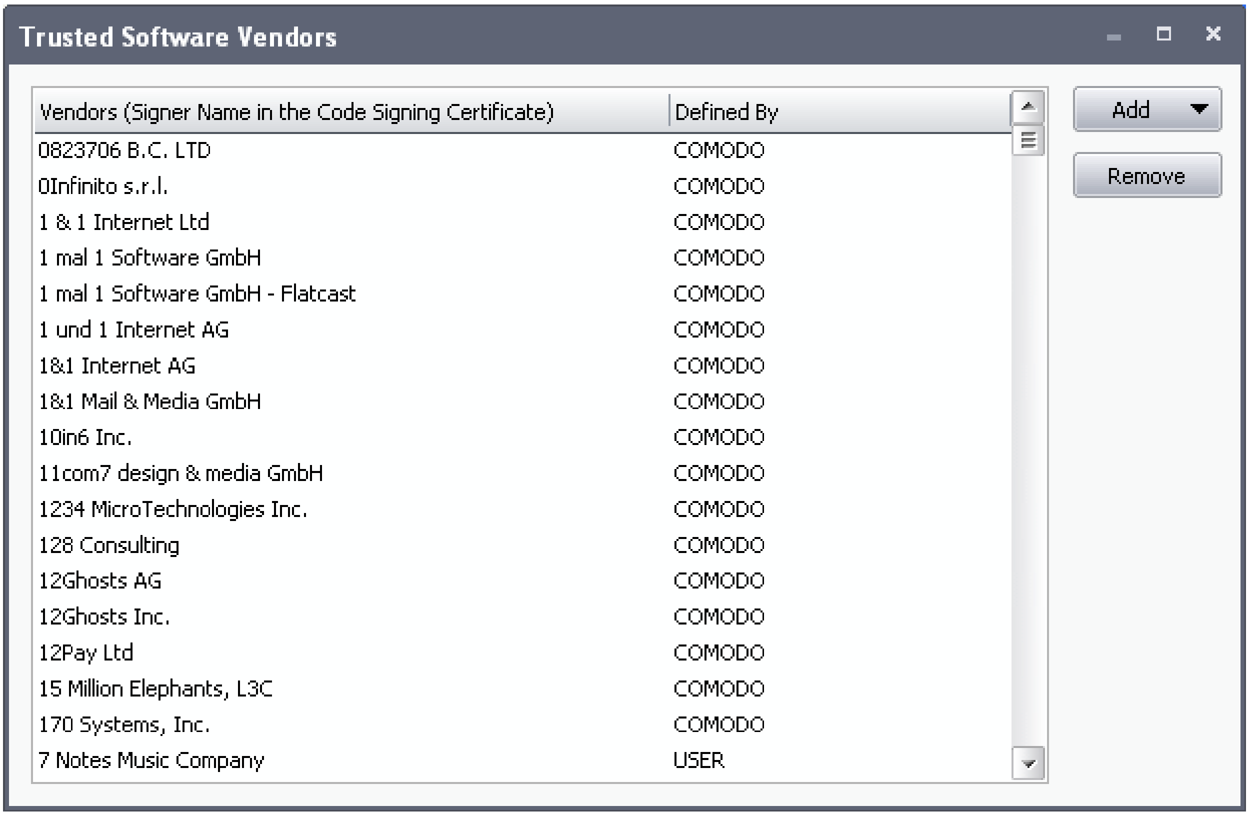
In Comodo Cleaning Essentials, there are two basic methods in which an application can be treated as safe. Either it has to be part of the 'Safe List' (of executables/software that is known to be safe) OR that application has to be signed by one of the vendors in the 'Trusted Software Vendor List'.

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'.



| Vendors (Signer Name in the Code Signing Certificate) | Defined By |
|---|---|
| 0823706 B.C. LTD | COMODO |
| 0Infinito s.r.l. | COMODO |
| 1 & 1 Internet Ltd | COMODO |
| 1 mal 1 Software GmbH | COMODO |
| 1 mal 1 Software GmbH - Flatcast | COMODO |
| 1 und 1 Internet AG | COMODO |
| 1&1 Internet AG | COMODO |
| 1&1 Mail & Media GmbH | COMODO |
| 10in6 Inc. | COMODO |
| 11com7 design & media GmbH | COMODO |
| 1234 MicroTechnologies Inc. | COMODO |
| 128 Consulting | COMODO |
| 12Ghosts AG | COMODO |
| 12Ghosts Inc. | COMODO |
| 12Pay Ltd | COMODO |
| 15 Million Elephants, L3C | COMODO |
| 170 Systems, Inc. | COMODO |
| 7 Notes Music Company | USER |

## Column Descriptions

- **Vendors** -1 The vendor that has signed the software;
- **Defined By** - Indicates whether the vendor was added to Trusted Software Vendor List by Comodo (as the vendor is globally whitelisted) or by the user.

- **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.

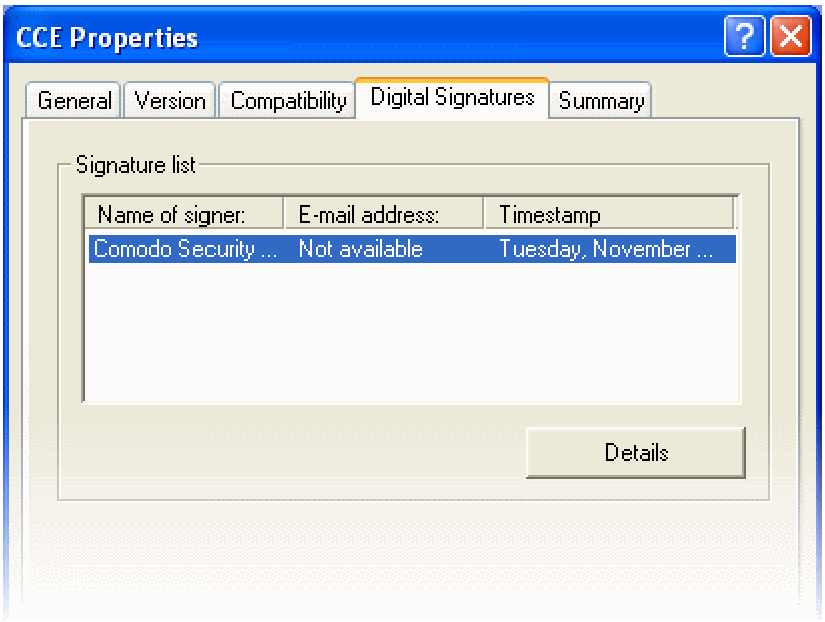
However, companies can't just 'sign' their own software and expect it to be trusted. This is why each code signing certificate is counter-signed by an organization called a 'Trusted Certificate Authority'. 'Comodo CA Limited' and 'Verisign' are two examples of a Trusted CA's and are authorized to counter-sign 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.

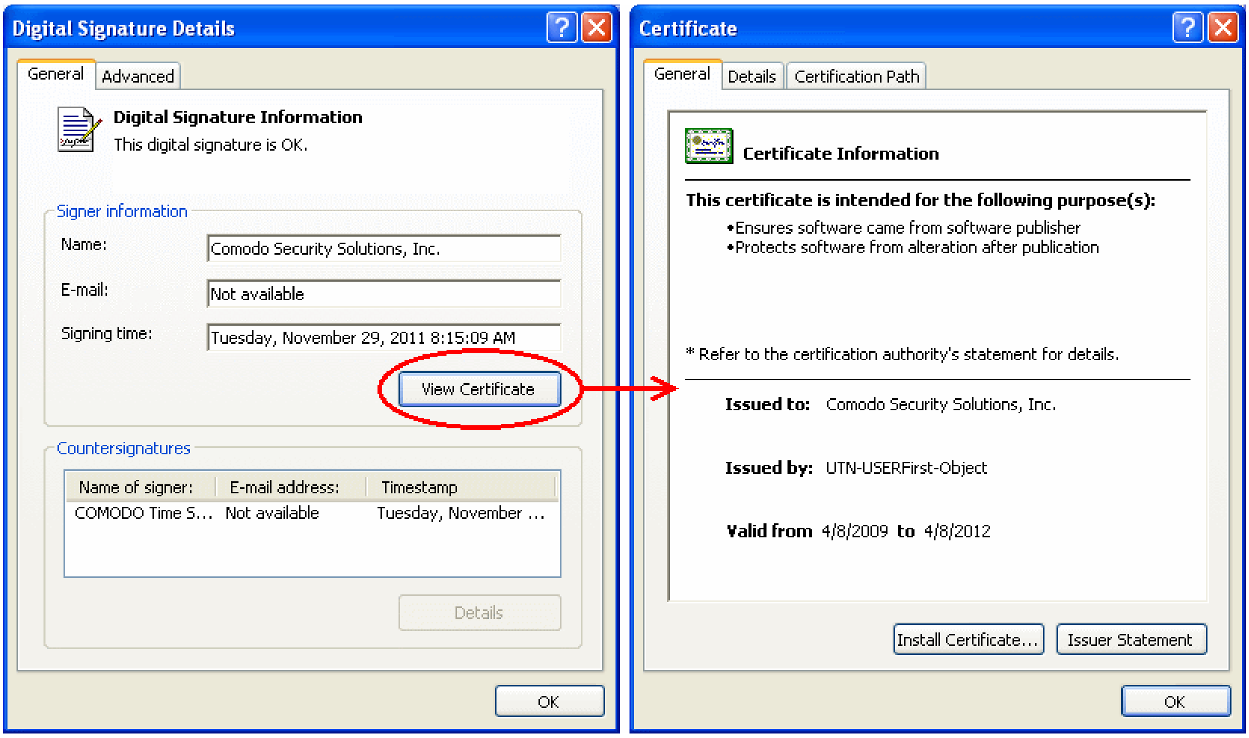
- Browse to the (default) installation directory of Comodo Cleaning Essentials.
- Right click on the file cce.exe.
- Select 'Properties' from the menu.
- Click the tab 'Digital Signatures (if there is no such tab then the software has not been signed).

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



| Name of signer: | E-mail address: | Timestamp |
|---|---|---|
| Comodo Security ... | Not available | Tuesday, November ... |

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



Digital Signature Details

General | Advanced

**Digital Signature Information**

This digital signature is OK.

Signer information

Name: Comodo Security Solutions, Inc.

E-mail: Not available

Signing time: Tuesday, November 29, 2011 8:15:09 AM

View Certificate

Countersignatures

| Name of signer: | E-mail address: | Timestamp |
|---|---|---|
| COMODO Time S... | Not available | Tuesday, November ... |

Details

OK

Certificate

General | Details | Certification Path

**Certificate Information**

**This certificate is intended for the following purpose(s):**

- Ensures software came from software publisher
- Protects software from alteration after publication

* Refer to the certification authority's statement for details.

**Issued to:** Comodo Security Solutions, Inc.

**Issued by:** UTN-USERFirst-Object

**Valid from** 4/8/2009 **to** 4/8/2012

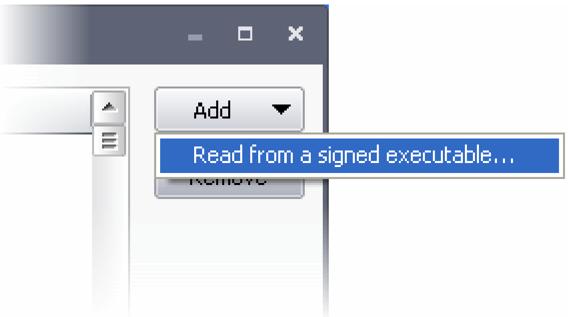
Install Certificate... | Issuer Statement

OK

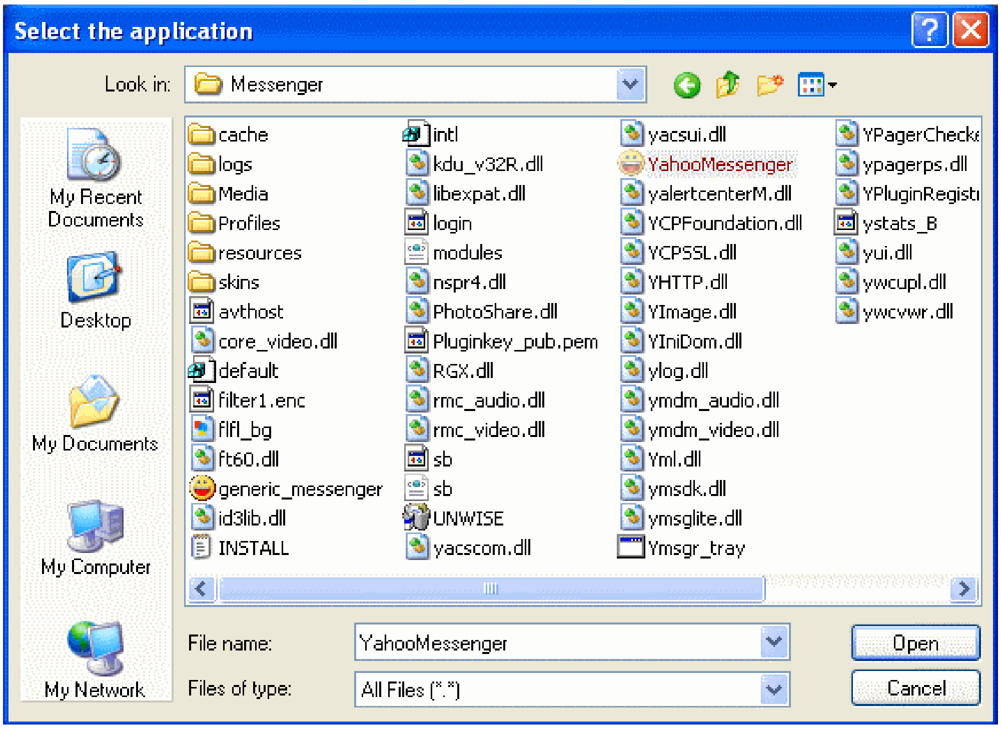
It should be noted that the example above is a special case in that Comodo, as creator of 'cce.exe', is both the signer of the software and, as a trusted CA, it is also the counter-signer (see the 'Countersignatures' box). In the vast majority of cases, the signer or the certificate (the vendor) and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

## Adding and Defining a User-Trusted Vendor

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



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



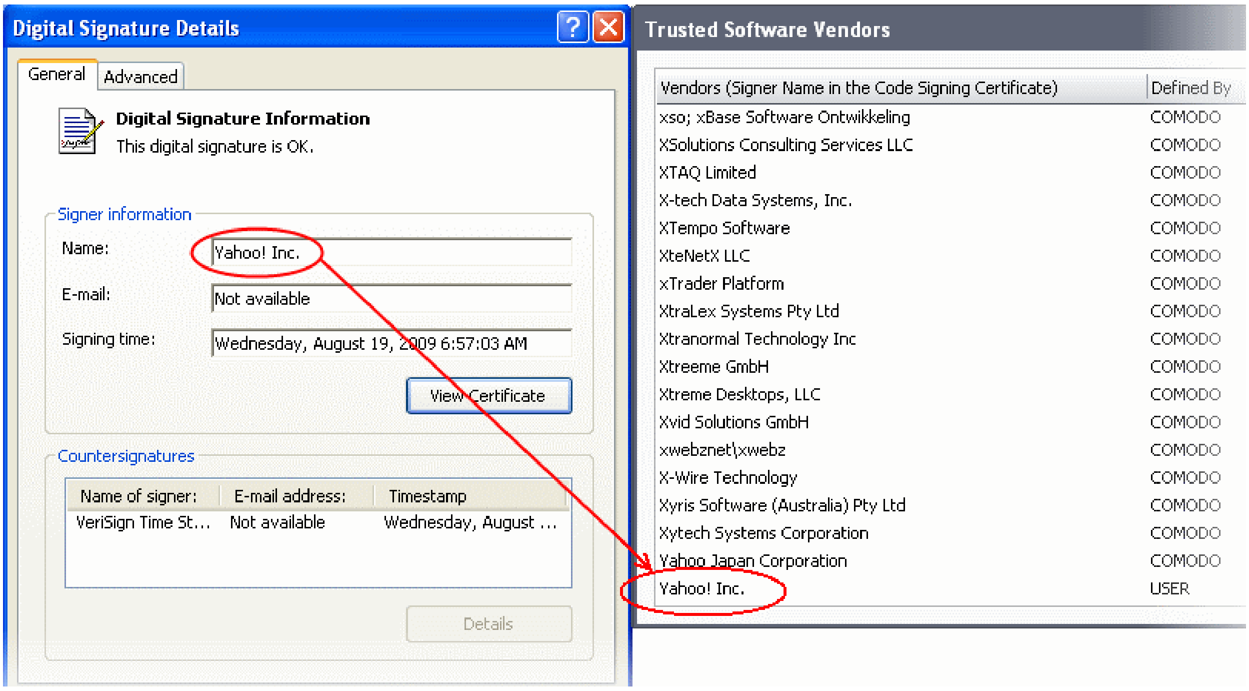
Select the application

Look in: Messenger

File name: YahooMessenger

Files of type: All Files (*.*)

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 Details

General | Advanced

**Digital Signature Information**

This digital signature is OK.

Signer information

Name: Yahoo! Inc.

E-mail: Not available

Signing time: Wednesday, August 19, 2009 6:57:03 AM

Countersignatures

| Name of signer: | E-mail address: | Timestamp |
|---|---|---|
| VeriSign Time St... | Not available | Wednesday, August ... |

Trusted Software Vendors

| Vendors (Signer Name in the Code Signing Certificate) | Defined By |
|---|---|
| xso; xBase Software Ontwikkeling | COMODO |
| XSolutions Consulting Services LLC | COMODO |
| XTAQ Limited | COMODO |
| X-tech Data Systems, Inc. | COMODO |
| XTempo Software | COMODO |
| XteNetX LLC | COMODO |
| xTrader Platform | COMODO |
| XtraLex Systems Pty Ltd | COMODO |
| Xtranormal Technology Inc | COMODO |
| Xtreeme GmbH | COMODO |
| Xtreme Desktops, LLC | COMODO |
| Xvid Solutions GmbH | COMODO |
| xwebznet\xwebz | COMODO |
| X-Wire Technology | COMODO |
| Xyris Software (Australia) Pty Ltd | COMODO |
| Xytech Systems Corporation | COMODO |
| Yahoo Japan Corporation | COMODO |
| Yahoo! Inc. | USER |

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. Importing Antivirus Database

CCE is configured to periodically check Comodo servers to see whether a virus database update is available for download.

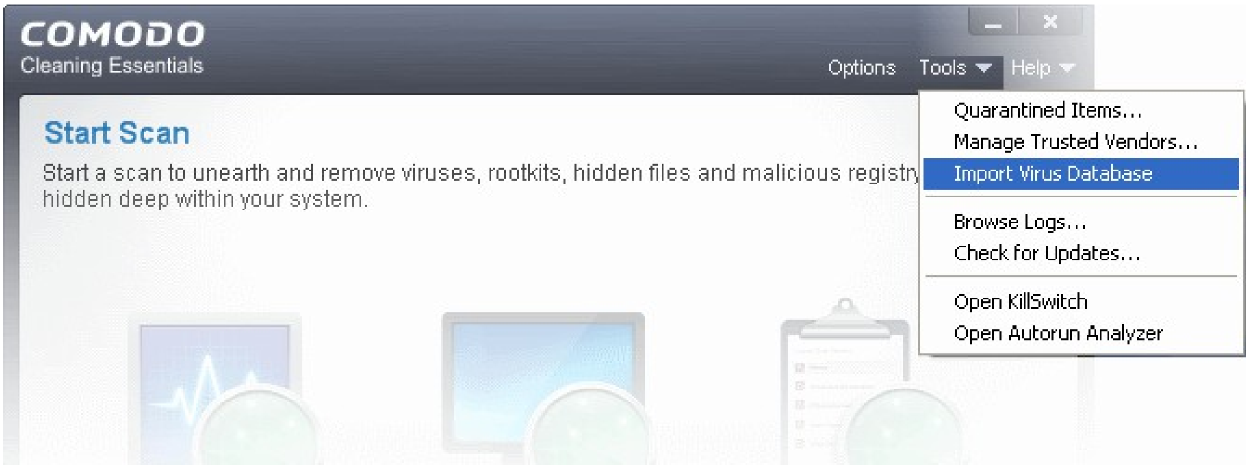
As an alternative to downloading from Comodo servers, you can import the virus database updates from local storage or from any of the other computers in your network that uses the same database. This can help accelerate update deployment across large networks of endpoints and reduce the bandwidth consumption.

**Example Scenarios:**

- If you also have Comodo Internet Security (CIS) installed and it is configured to regularly receive database updates then you can configure CCE to collect it's updates from your CIS folder. To do this, you just need to point CCE to the CIS folder that contains the (updated) bases.cav file. See instructions below.
- Similarly, if you are connected to a local network, you can import the updated database from any network folder that contains the latest bases.cav (for example, from another computer that has a (fully updated) CCE or CIS installed)).

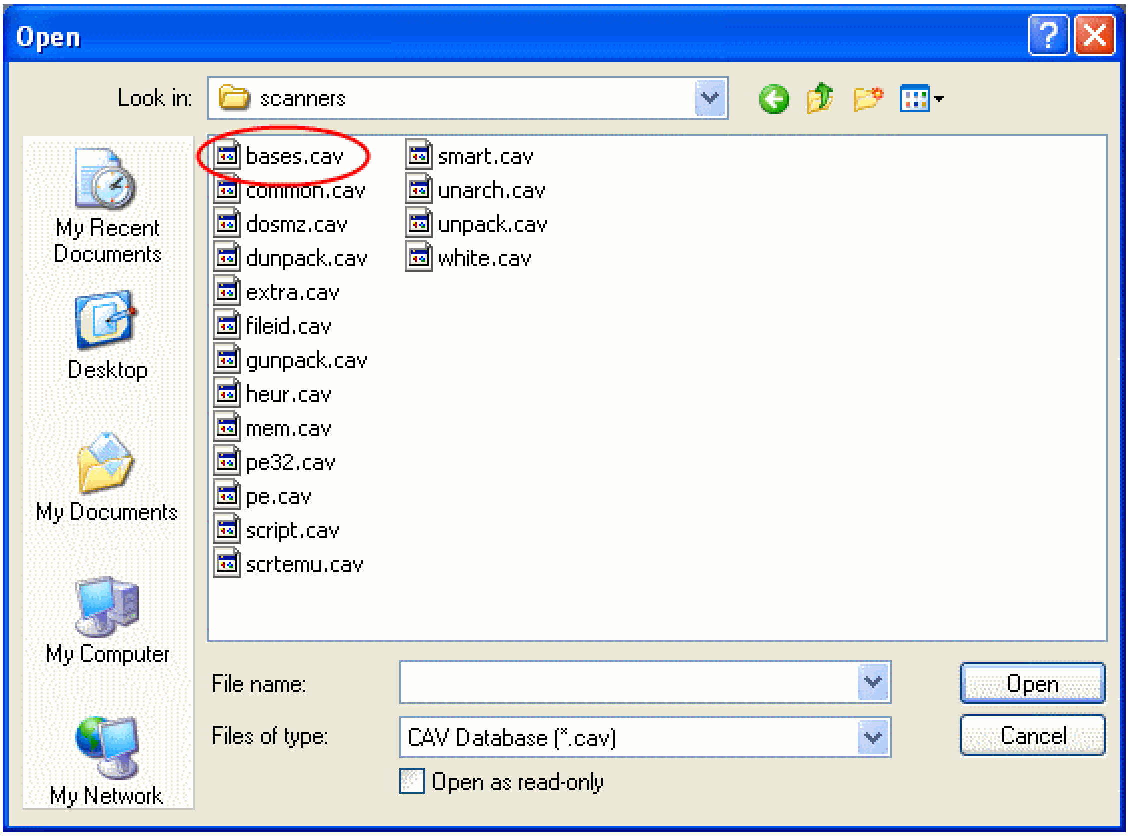
To import virus database

- Click Tools > Import Virus Database.



Start a scan to unearth and remove viruses, rootkits, hidden files and malicious registry hidden deep within your system.

The Windows  Open dialog will open.



- Navigate to the folder containing the virus database file like bases.cav and select the file

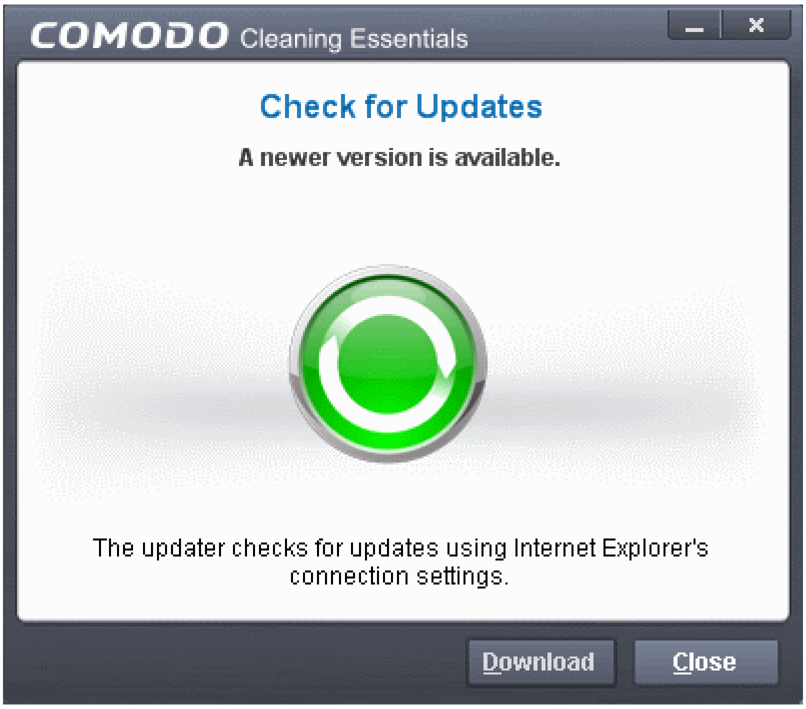
**Tip**: If you are importing the database from your CIS installation, the bases.cav will be available in the folder <installation drive>:\Program Files\COMODO\COMODO Internet Security\scanners.

- Click 'Open'.

The database file will be immediately imported to CCE.

## 4.4. Checking for Software Updates

CCE is configured for automatic periodic checking of availability of updated version of the software. If an updated version is available you will be prompted to download the new version.



Check for Updates

A newer version is available.

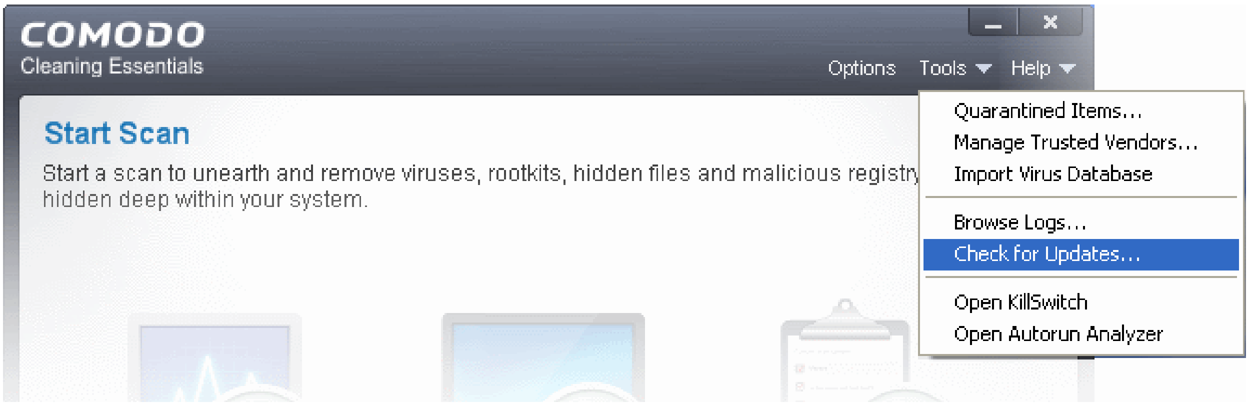
The updater checks for updates using Internet Explorer's connection settings.

- Clicking 'Download' will launch your default browser to download the latest version.

You can manually check whether any updates are available from the Tools menu of the application.

**To manually check for the software updates**

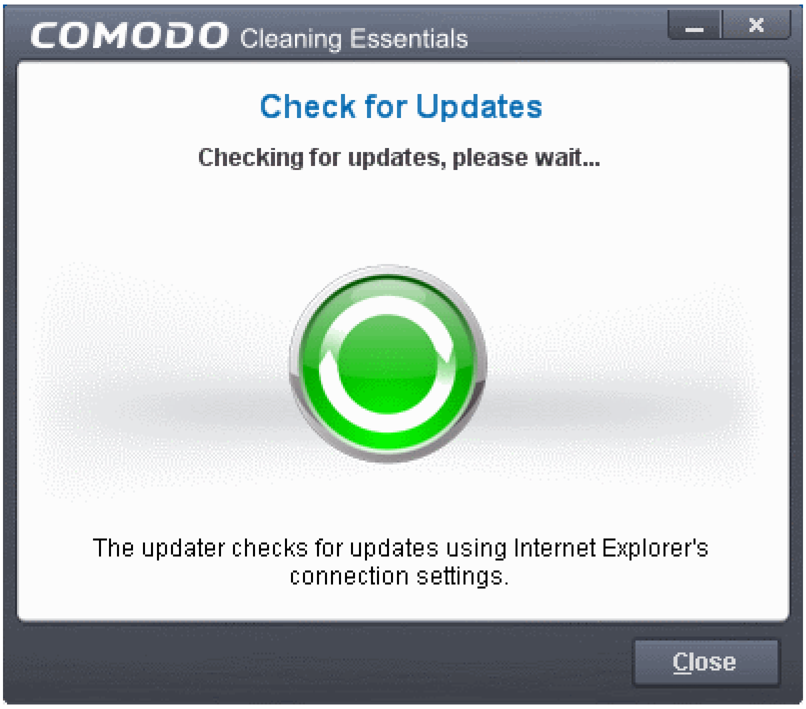
- Click 'Tools' > 'Check for Updates'



Start Scan

Start a scan to unearth and remove viruses, rootkits, hidden files and malicious registry hidden deep within your system.

The application will connect to Comodo servers and check for the availability of updates.



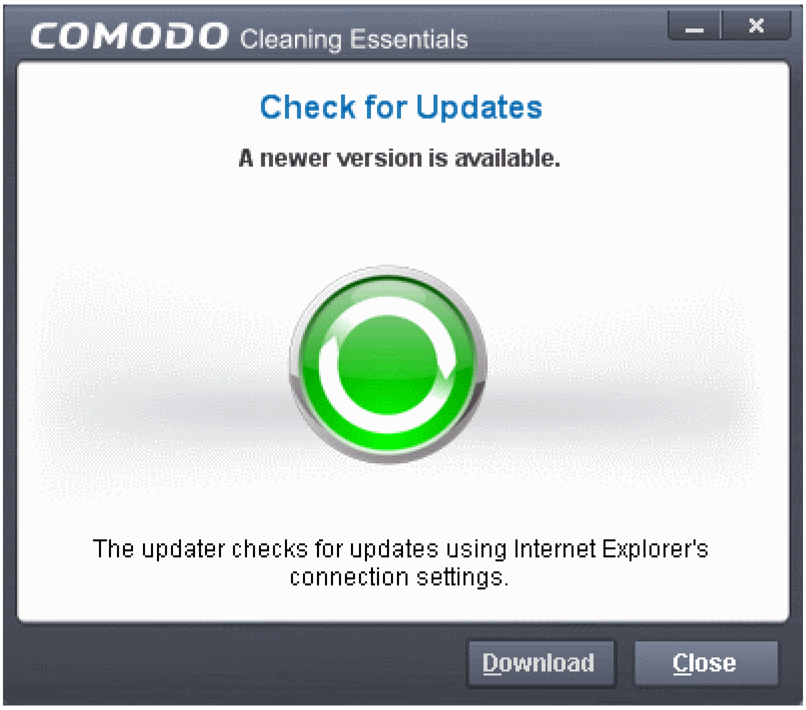
COMODO Cleaning Essentials

Check for Updates

Checking for updates, please wait...

The updater checks for updates using Internet Explorer's connection settings.

- If any updates are available, you will be prompted to download the latest version.



COMODO Cleaning Essentials

Check for Updates

A newer version is available.

The updater checks for updates using Internet Explorer's connection settings.

  - Clicking 'Download' will launch your default browser to download the latest version.
- If no updates are available, you will be notified on that.

Your product is currently up-to-date.

The updater checks for updates using Internet Explorer's connection settings.

# 5.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.

When started in aggressive mode, KillSwitch forcibly terminates all the running applications and processes created by currently logged-in user and enables the user to analyze the processes that were invoked automatically, in order to identify the harmful processes invoked by malware and hence to identify the malware.

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

- **Introduction to KillSwitch**
  - **Starting KillSwitch**
  - **The Main Interface**
- **Viewing and Handling Processes, Applications and Services**
  - **Processes**
    - **Stopping, Starting and Handling the Processes**
    - **Viewing Properties of a Process**
  - **Applications**
    - **Handling the Applications**
  - **Services**

        - Stopping, Starting and Deleting the Services
- Viewing and Handling Network Connections and Usage
    - Network Connections
        - Inspecting and Closing Network Connections
    - Network Utilization
- Configuring KillSwitch
- KillSwitch Tools
    - Viewing System Information
    - Repairing Windows Settings and Features
    - Analyzing Program Usage
    - Searching for Handles or DLLs
    - Verifying Authenticity of Applications
    - Boot Logging and Handling Loaded Modules
    - Running Programs from Command Line Interface
    - Viewing KillSwitch Logs
    - Finding Process of the Active Window
- Managing Currently Logged-in Users
- Help and About Details

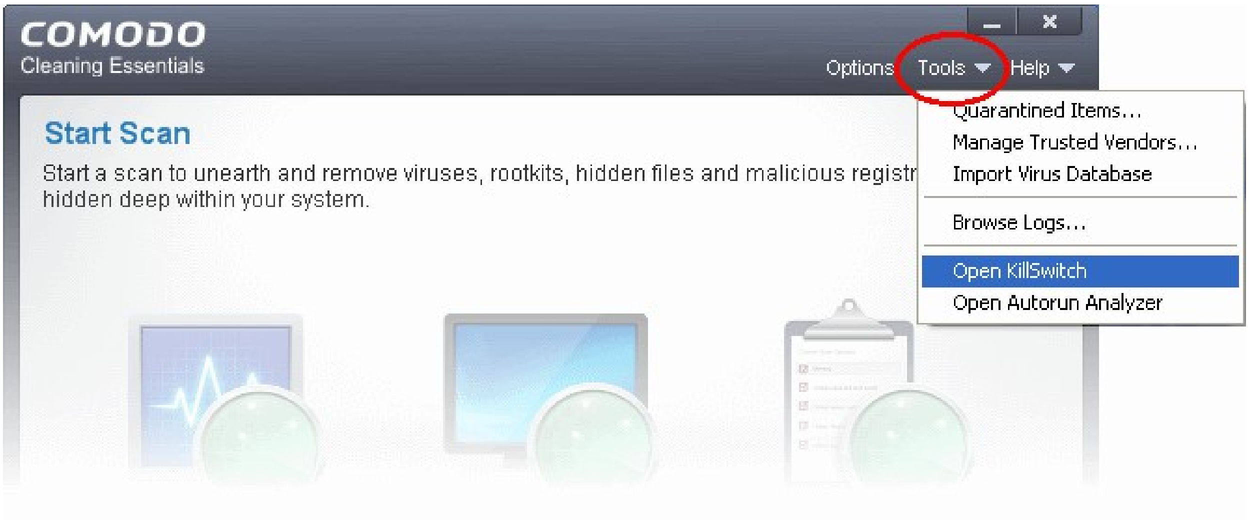
## 5.1. Starting KillSwitch

KillSwitch can be started by the following ways:

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

### 5.1.1. From the Comodo Cleaning Essentials Interface

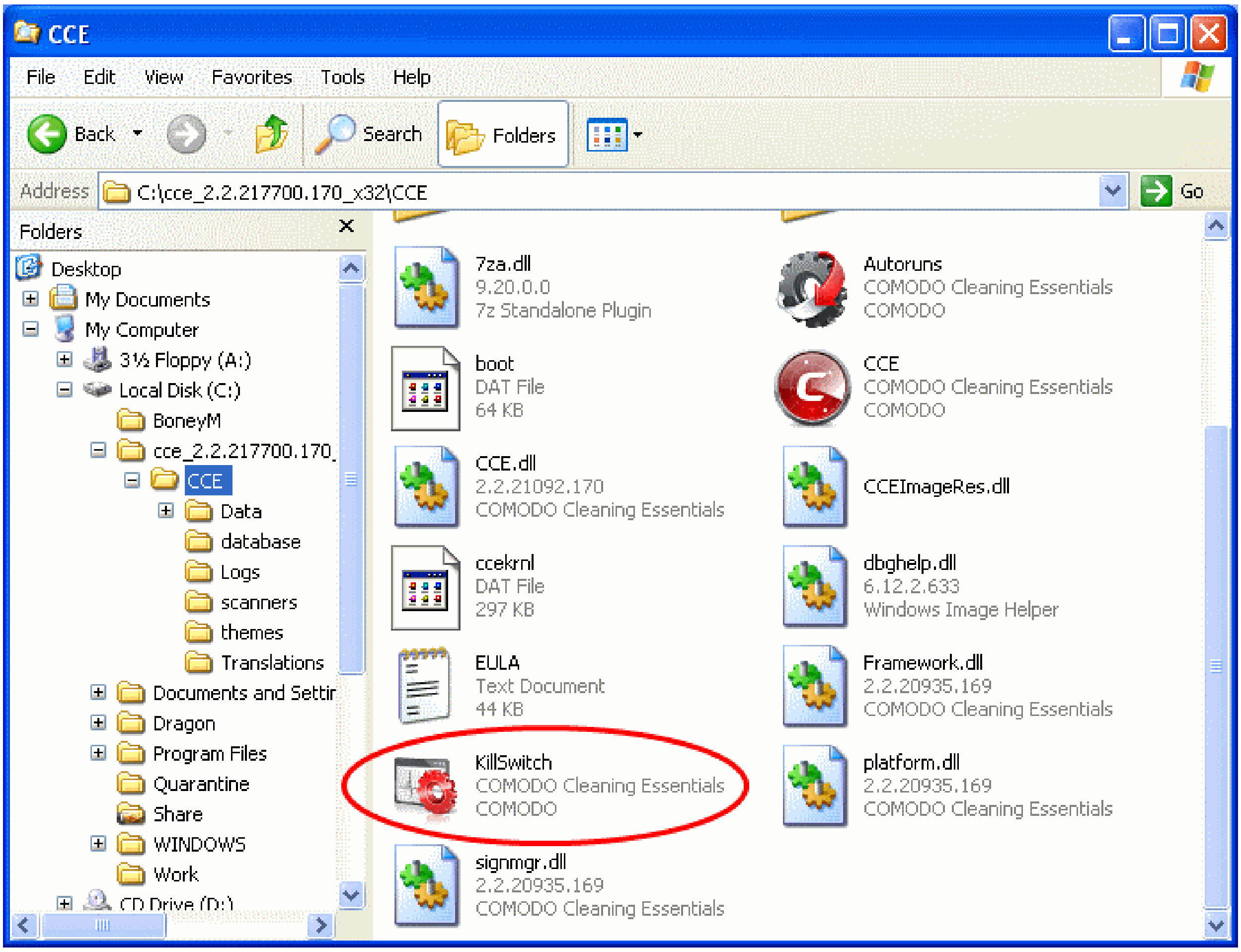
- Click Tools > Open KillSwitch from the title bar controls of the main interface of Comodo Cleaning Essentials.
- To open KillSwitch in **aggressive mode**, press and hold 'Shift' key and click Tools > Open KillSwitch


COMODO
Cleaning Essentials
Options
Tools
Help
Quarantined Items...
Manage Trusted Vendors...
Import Virus Database
Browse Logs...
Open KillSwitch
Open Autorun Analyzer
Start Scan
Start a scan to unearth and remove viruses, rootkits, hidden files and malicious registr
hidden deep within your system.

The KillSwitch main interface will be opened.

## 5.1.2. 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.
- To open KillSwitch in **aggressive mode**, press and hold 'Shift' key and double click on the file 'KillSwitch.exe'.



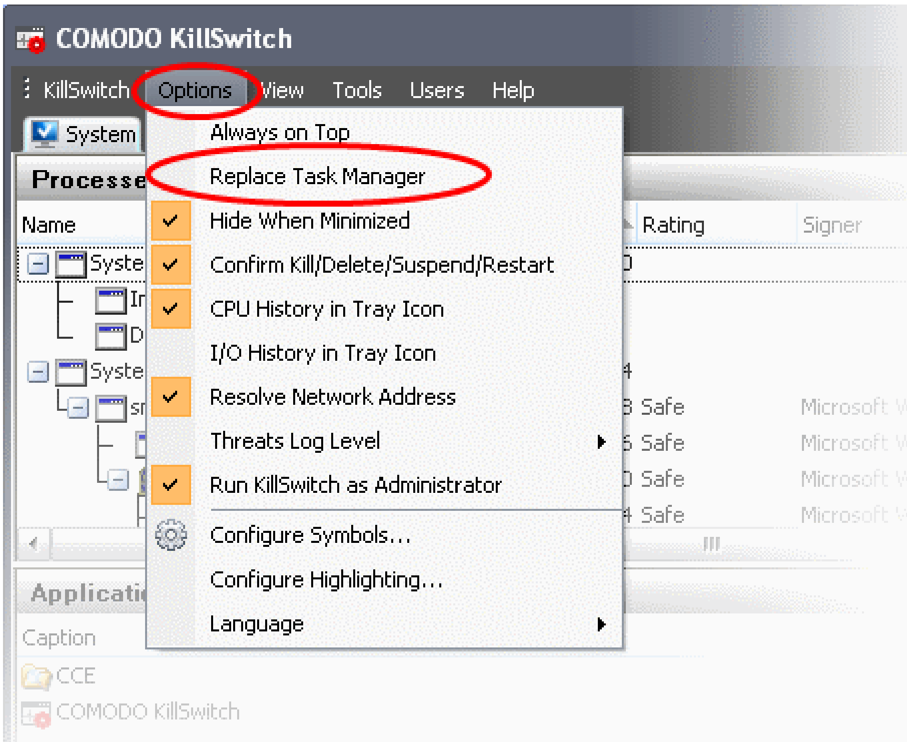
The KillSwitch main interface will be opened.

## 5.1.3. 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'.
- Pressing holding the 'Shift' key while opening KillSwitch in any of the above said methods will open KillSwitch in **aggressive mode**.

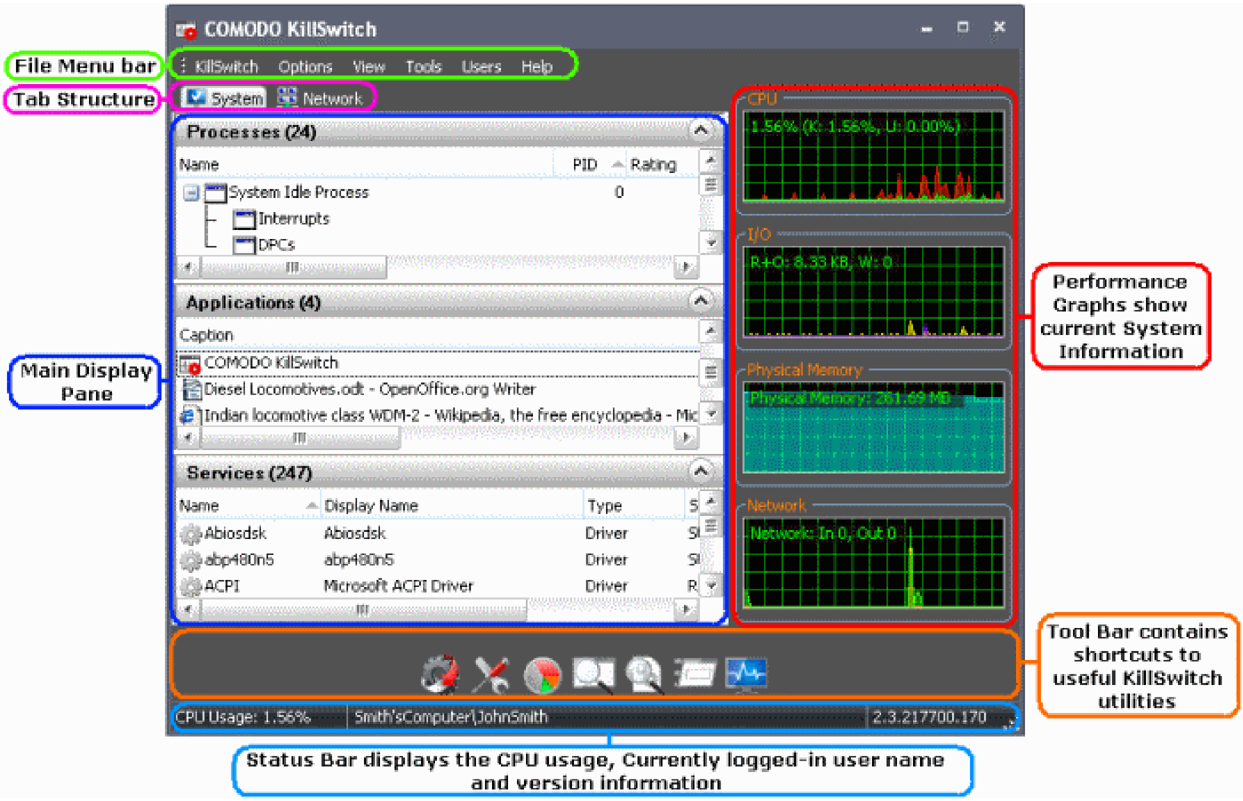
To replace Task Manager with KillSwitch, you first need to start the application by one of the methods explained **above**, click 'Options' from the title bar and enable 'Replace Task Manager'.



For more details, refer to the description of **'Replace Task Manager with KillSwitch'** in the section '**Configuring KillSwitch**'.

## 5.2. The Main Interface

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


COMODO KillSwitch
File Menu bar
Tab Structure
Main Display Pane
Performance Graphs show current System Information
Tool Bar contains shortcuts to useful KillSwitch utilities
Status Bar displays the CPU usage, Currently logged-in user name and version information
KillSwitch Options View Tools Users Help
System Network
Processes (24)
Applications (4)
Services (247)
CPU
I/O
Physical Memory
Network
CPU Usage: 1.56%
Smith'sComputer\JohnSmith
2.3.217700.170

The interface is divided into six main areas:

- **The File Menu bar;**

- **Tab Structure;**
- **Main display Pane;**
- **Graphical Reports Pane**;
- **Tool Bar**;
- **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 unsafe processes, saving current state and switching power state of your system. |
| | Kill All Unsafe Processes | Stops all the currently running processes that are identified as unsafe by KillSwitch.<br>**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. |
| | Save Current View | Opens the 'Save as' dialog to save the currently displayed list in the main display area as a .csv file. |
| | Save | Opens the 'Save as' dialog to save the data in all display panes as a .csv file. |
| | Shutdown | Enables you to switch the power state of your computer. Hovering the mouse cursor options opens a sub-menu containing the following options:<br>• Shutdown;<br>• Power-off;<br>• Restart;<br>• Sleep;<br>• Hibernate;<br>• Lock;<br>• Log-off; |
| | Exit | Closes the KillSwitch application. |
| Options | | Contains 'Options' that enable you to configure the overall behavior of the application. Refer to the section '**Configuring KillSwitch**'  for more details. |
| View | | Contains options related to display nature of the application. |
| | 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. |
| | Show Only the Unsafe Images in | Displays only the program images identified as unsafe by KillSwitch |

| | | |
|---|---|---|
| | Memory | currently loaded to system memory in the main display area. |
| | Hide Safe Processes | 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. |
| | Opacity | Enables you to set the transparency of KillSwitch window. The choices range from 10% to full opaque, in the intervals of 10. |
| | Refresh Now | Updates and refreshes the KillSwitch window. |
| | Update Speed | 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. |
| | Performance Graphs | Switches the display of the performance graphs at  the right hand side of the main interface. |
| | Toolbar | Switches the display of the tool bar containing shortcuts to utilities at the bottom of the interface. |
| | Select Columns | Opens Select Columns interface that enables you to configure the columns to be displayed in different screens of KillSwitch. Refer to the section '**Column Selection**' for more details. |
| Tools | | Contains shortcuts for important utilities and  options for handling processes, objects and dll files collectively, shortcuts for running command line interface programs and so on. Refer to the section '**The Tools Menu**' for more details. |
| | Autorun Analyzer | Opens the **Autorun Analyzer** utility to view and handle services and programs that were loaded when your system booted-up. |
| | Quick Repair | Opens the 'Quick Repair' interface  to troubleshoot and and repair important Windows settings and features. Refer to **Repairing Windows Settings and Features** for more details. |
| | Program Usage Analyzer | Open the 'Program Usage Analyzer' window that displays a summary of usage of all the programs installed in your computer by different users. Refer to **Analyzing Program Usage** for more details. |
| | 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. |
| | 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. |
| | Enable Boot Logging | Instructs KillSwitch to log all modules loaded from next boot onwards and show them in its window automatically. Refer to **Boot Logging and Handling Loaded Modules** for more details. |
| | Run | Opens the Windows 'Run' dialog for executing command line interface programs with default limited user privileges. Refer to **Running Programs from Command  Line Interface** for more details. |

| | | |
|---|---|---|
| | Run as Administrator | Opens the Windows 'Run' dialog for executing command line interface programs with administrative privileges. |
| | Browse Logs | Open the KillSwitch logs saved in Data\KillSwitch\KS Logs sub- folder inside the folder that contains the CCE files. Refer to **Viewing KillSwitch Logs** 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. |

## 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 |
|---|---|---|
| **System** | | Displays the currently running processes, Applications and services that are currently running in your system, under respective collapsible panes. |
| | **Processes** | Displays the currently running processes in your system |
| | **Applications** | Displays the currently running Applications in your system |
| | **Services** | Displays the Windows Services started along with your system |
| **Network** | | Displays the currently running processes involved in network connections and the network usage, under respective collapsible panes. |
| | **Network Connections** | Displays the currently running processes that are involved in network connection activities. |
| | **Network Utilization** | Displays a graphical representation of network traffic through the network adapters running on your computer. |

## Main Display Pane

The main display pane displays the list of items like Processes, application, Services and so on 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.

## Graphical Reports Pane

The pane displays dynamic graphical representations of your CPU usage, I/O activity and physical memory usage and network usage of your system. You can switch the display of this pane On and Off by selecting/deselecting the option 'Performance Graphs' under 'View' menu in the File Menu bar.

## The Tool Bar

The Tool bar displayed beneath the Main Display pane contains shortcut icons to important utilities of KillSwitch.

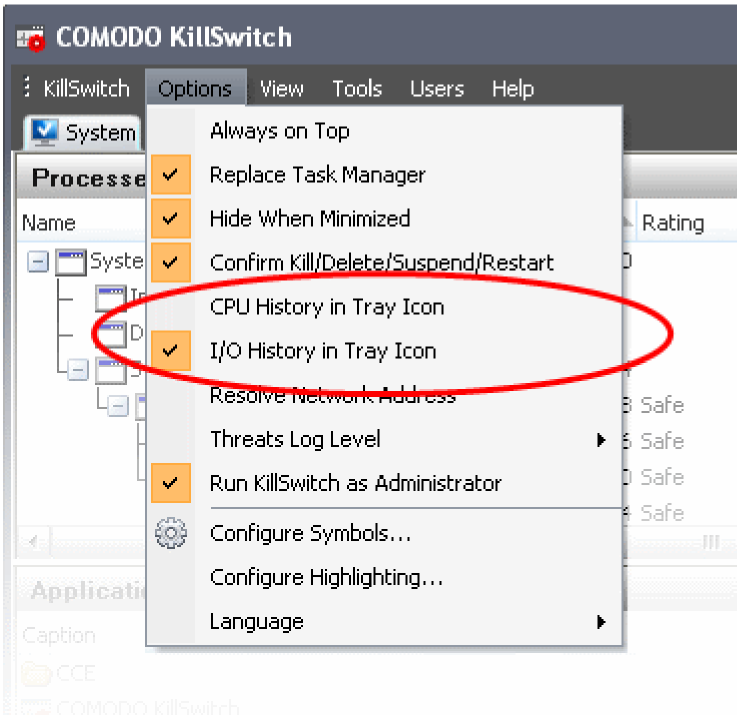
| Icon | Description |
|---|---|
| | Opens **Autorun Analyzer** utility to view and handle services and programs that were loaded when your system booted-up. |
| | Opens the 'Quick Repair' interface  to troubleshoot and and repair important Windows settings and features. Refer **Repairing Windows Settings and Features** for more details. |
| | Open the 'Program Usage Analyzer' window that displays a summary of usage of all the programs installed in your computer by different users. Refer to **Analyzing Program Usage** for more details. |
| | Starts the Find Window utility that allows the user to find process related to active application window or window components. Refer to **Finding Process of the Active Window** for more details. |
| | Opens a 'search' 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 Windows 'Run' dialog for executing command line interface programs with default limited user privileges. Refer to **Running Programs from Command Line Interface** 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. |

### The Status Bar

The status bar at the bottom of the interface displays the current CPU usage, currently logged-in user name and the version of KillSwitch that you are using.

## 5.2.1. The System Tray Icon

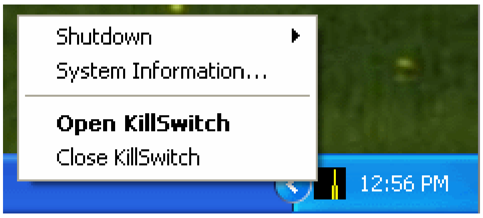
KillSwitch displays an icon in the system tray at the bottom right corner of the screen. The icon displays a dynamic graphical representation of the CPU usage history or IO activities as configured through Options > CPU History in tray Icon or Options > I/O History in Tray Icon, as shown below.



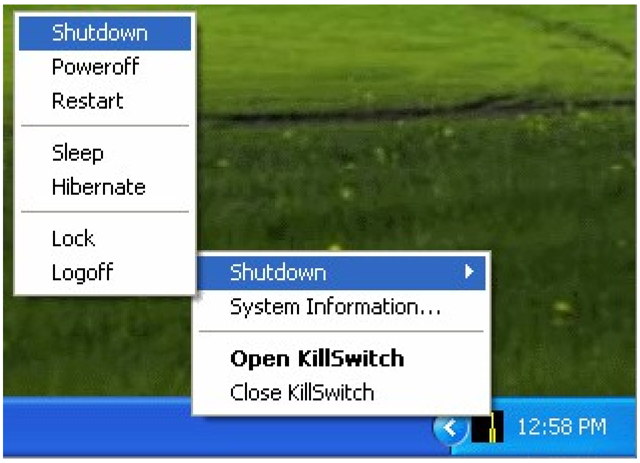
Refer to **Configuring KillSwitch** for more details.

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

- **Shutdown;**
- **System Information;**
- **Open KillSwitch**;
- **Close KillSwitch**.



- **Shutdown -** Enables you to switch the power state of your computer. Hovering the mouse cursor options opens a sub-menu containing the following options:



- Shutdown;
- Power-off;
- Restart;
- Sleep;
- Hibernate;
- Lock;
- Log-off.

- **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.
- **Open KillSwitch** - Opens the KillSwitch main interface window.
- **Close KillSwitch** - Exits the KillSwitch application.

## 5.3. Viewing and Handling Processes, Applications and Services

The main display pane of the application window displays the list of currently running processes, applications and services, on selecting the 'System' tab from the tab structure. The Processes, Applications and the Services are listed in their respective collapsible windows. Right-clicking on each entry opens context sensitive menu that enables various actions like starting/stopping the processes/services, viewing properties of the processes.

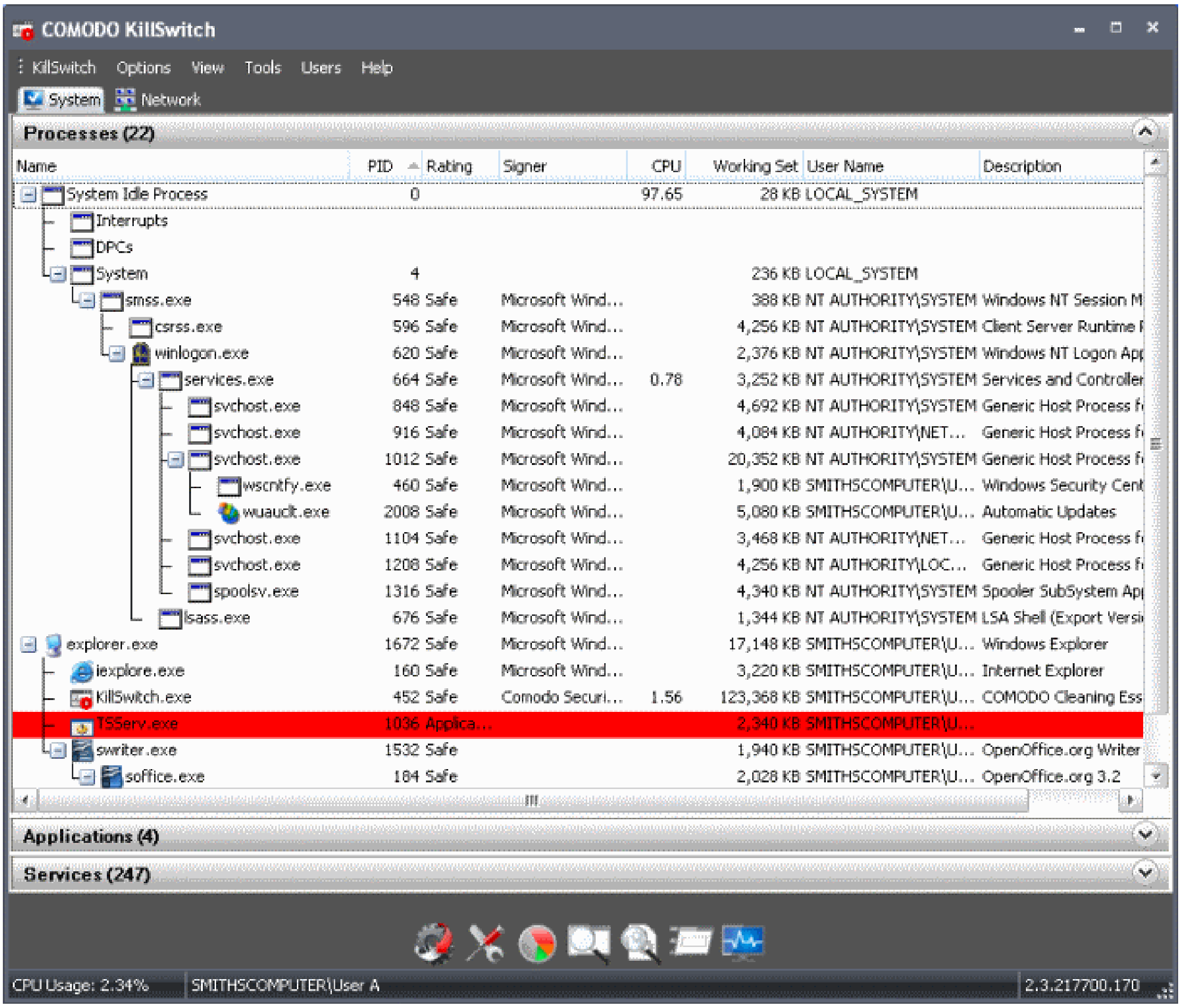
Click the links below for detailed explanations on the windows displayed under the System tab.

- **Processes**;
- **Applications**;
- **Services**.

### 5.3.1. Processes

The Processes window is displayed open by default and it shows all the processes that are currently running in your system as a table in the main display pane. To open the Processes window from closed state, click the down-arrow at the right of the 'Processes' stripe.

- The processes can be viewed in tree view or as a list.
- The new processes started and the processes that are stopped, processes identified as suspicious and hidden are highlighted with different colors. The highlighting colors can be set through **Configuring KillSwitch > Configure Highlighting**.
- 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.



| Name | PID | Rating | Signer | CPU | Working Set | User Name | Description |
|---|---|---|---|---|---|---|---|
| System Idle Process | 0 | | | 97.65 | 28 KB | LOCAL_SYSTEM | |
| Interrupts | | | | | | | |
| DPCs | | | | | | | |
| System | 4 | | | | 236 KB | LOCAL_SYSTEM | |
| smss.exe | 548 | Safe | Microsoft Wind... | | 388 KB | NT AUTHORITY\SYSTEM | Windows NT Session M |
| csrss.exe | 596 | Safe | Microsoft Wind... | | 4,256 KB | NT AUTHORITY\SYSTEM | Client Server Runtime F |
| winlogon.exe | 620 | Safe | Microsoft Wind... | | 2,376 KB | NT AUTHORITY\SYSTEM | Windows NT Logon App |
| services.exe | 664 | Safe | Microsoft Wind... | 0.78 | 3,252 KB | NT AUTHORITY\SYSTEM | Services and Controller |
| svchost.exe | 848 | Safe | Microsoft Wind... | | 4,692 KB | NT AUTHORITY\SYSTEM | Generic Host Process fo |
| svchost.exe | 916 | Safe | Microsoft Wind... | | 4,084 KB | NT AUTHORITY\NET... | Generic Host Process fo |
| svchost.exe | 1012 | Safe | Microsoft Wind... | | 20,352 KB | NT AUTHORITY\SYSTEM | Generic Host Process fo |
| wscntfy.exe | 460 | Safe | Microsoft Wind... | | 1,900 KB | SMITHSCOMPUTER\U... | Windows Security Cent |
| wuauclt.exe | 2008 | Safe | Microsoft Wind... | | 5,080 KB | SMITHSCOMPUTER\U... | Automatic Updates |
| svchost.exe | 1104 | Safe | Microsoft Wind... | | 3,468 KB | NT AUTHORITY\NET... | Generic Host Process fo |
| svchost.exe | 1208 | Safe | Microsoft Wind... | | 4,256 KB | NT AUTHORITY\LOC... | Generic Host Process fo |
| spoolsv.exe | 1316 | Safe | Microsoft Wind... | | 4,340 KB | NT AUTHORITY\SYSTEM | Spooler SubSystem App |
| lsass.exe | 676 | Safe | Microsoft Wind... | | 1,344 KB | NT AUTHORITY\SYSTEM | LSA Shell (Export Versi |
| explorer.exe | 1672 | Safe | Microsoft Wind... | | 17,148 KB | SMITHSCOMPUTER\U... | Windows Explorer |
| iexplore.exe | 160 | Safe | Microsoft Wind... | | 3,220 KB | SMITHSCOMPUTER\U... | Internet Explorer |
| KillSwitch.exe | 452 | Safe | Comodo Securi... | 1.56 | 123,368 KB | SMITHSCOMPUTER\U... | COMODO Cleaning Ess |
| TSServ.exe | 1036 | Applica... | | | 2,340 KB | SMITHSCOMPUTER\U... | |
| swriter.exe | 1532 | Safe | | | 1,940 KB | SMITHSCOMPUTER\U... | OpenOffice.org Writer |
| soffice.exe | 184 | Safe | | | 2,028 KB | SMITHSCOMPUTER\U... | OpenOffice.org 3.2 |

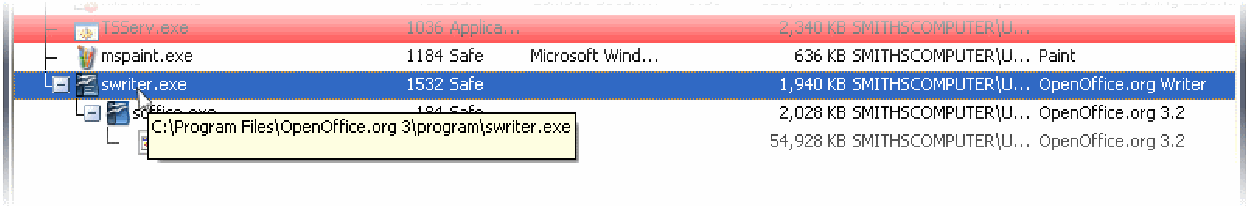
CPU Usage: 2.34% SMITHSCOMPUTER\User A 2.3.217700.170

The table below describes the columns that are displayed by default. You can add or remove the columns as per your requirement. Refer to **Column Selection** for more detailed explanation on this.

**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. |
| Rating | 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. Clicking on the column header enables sorting the entries based on the rating. |
| Signer | Displays the name of the Software vendor that has signed the software, which invoked the process. Clicking on the column header enables sorting the entries based on the ascending or descending alphabetical order of the names of the signers. |
| CPU | Displays the CPU usage of the process as a portion of overall CPU usage by the process in percentage. Clicking on the column header enables sorting the entries based on the CPU usage. |
| Working Set | Shows the number of page files in the virtual memory, referenced by the process. Clicking on the column header enables sorting the entries based on working set.<br>**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. |
| 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.



|  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|
| TSServ.exe | 1036 | Applica... |  |  | 2,340 KB | SMITHSCOMPUTER\U... |  |
| mspaint.exe | 1184 | Safe | Microsoft Wind... |  | 636 KB | SMITHSCOMPUTER\U... | Paint |
| swriter.exe | 1532 | Safe |  |  | 1,940 KB | SMITHSCOMPUTER\U... | OpenOffice.org Writer |
| soffice.exe |  |  |  |  | 2,028 KB | SMITHSCOMPUTER\U... | OpenOffice.org 3.2 |
|  |  |  |  |  | 54,928 KB | SMITHSCOMPUTER\U... | OpenOffice.org 3.2 |

C:\Program Files\OpenOffice.org 3\program\swriter.exe

## Column Selection

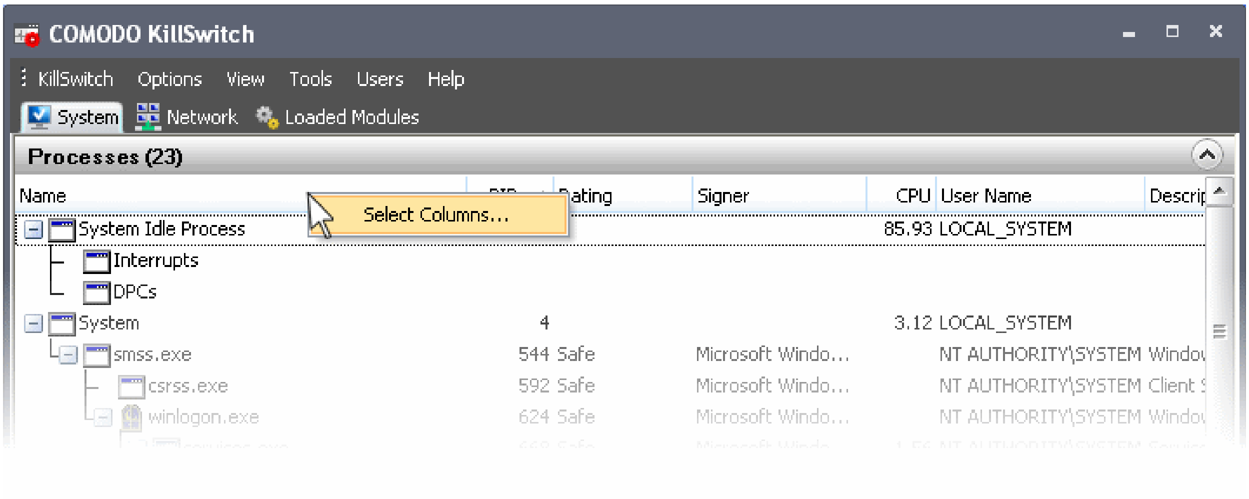
The Processes window displays the details on each process under eight columns. If you are an advanced user and wish to view more details on each process, you can configure the columns by adding or removing them.

To add or remove columns in Processes window:

- Click View > Select Columns

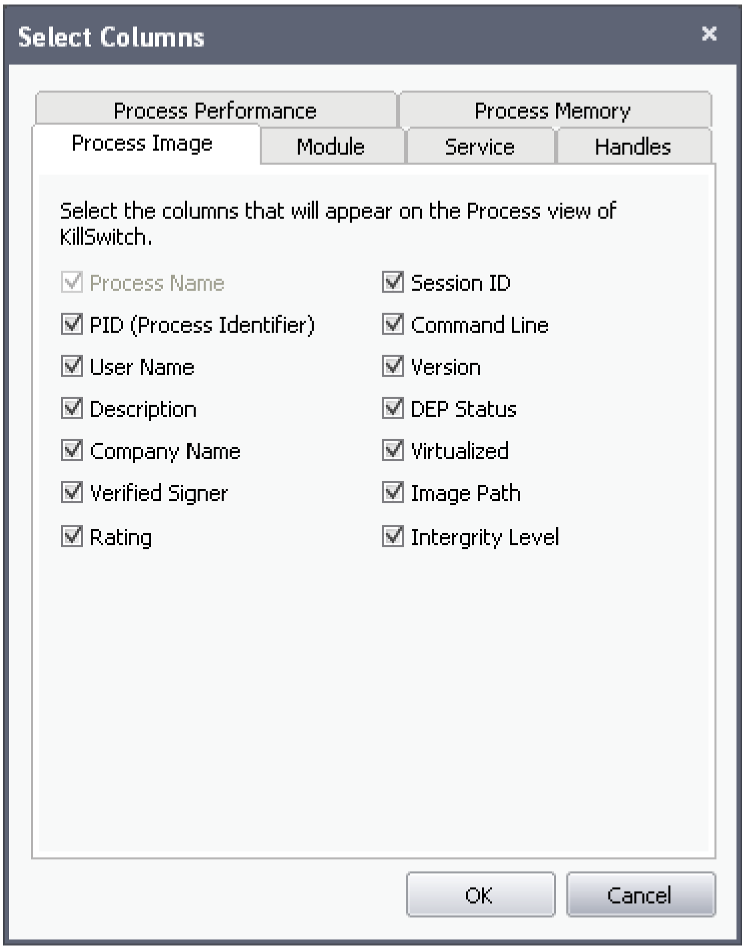
  Or

- Right click on the table header and select 'Select Columns' from the context sensitive menu.



| Name | PID | Rating | Signer | CPU | User Name | Descrip |
|---|---|---|---|---|---|---|
| System Idle Process | | | | 85.93 | LOCAL_SYSTEM | |
| Interrupts | | | | | | |
| DPCs | | | | | | |
| System | 4 | | | 3.12 | LOCAL_SYSTEM | |
| smss.exe | 544 | Safe | Microsoft Windo... | | NT AUTHORITY\SYSTEM | Windov |
| csrss.exe | 592 | Safe | Microsoft Windo... | | NT AUTHORITY\SYSTEM | Client S |
| winlogon.exe | 624 | Safe | Microsoft Windo... | | NT AUTHORITY\SYSTEM | Windov |

The 'Select Columns' dialog will appear. The dialog contains six tabs to configure the columns to be displayed for different categories of information on each process.



Select the columns that will appear on the Process view of KillSwitch.

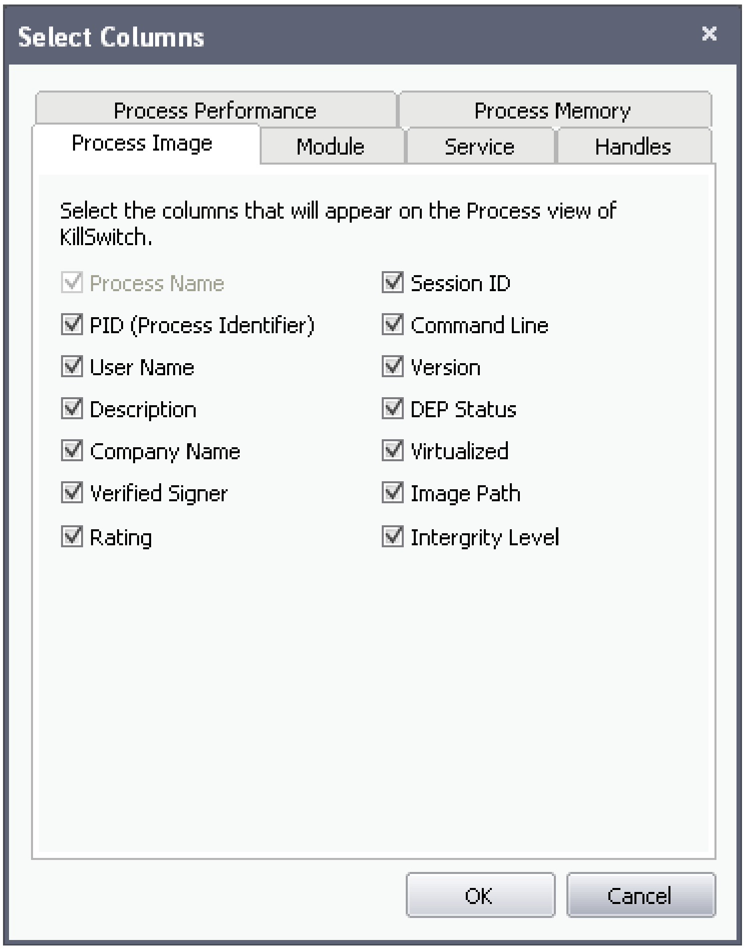
- ☑ Process Name
- ☑ PID (Process Identifier)
- ☑ User Name
- ☑ Description
- ☑ Company Name
- ☑ Verified Signer
- ☑ Rating
- ☑ Session ID
- ☑ Command Line
- ☑ Version
- ☑ DEP Status
- ☑ Virtualized
- ☑ Image Path
- ☑ Intergrity Level

Refer to the sections below for more details on each tab:

- **Process Image**
- **Process Performance**
- **Process Memory**
- **Module**
- **Service**
- **handles**

### Process Image

The Process Image tab allows you to select the columns to be displayed in the Process window,  to provide the basic information about the process and its image file. You can also configure to display the command line, Data Execution Prevention (DEP) status and so on of the image file.



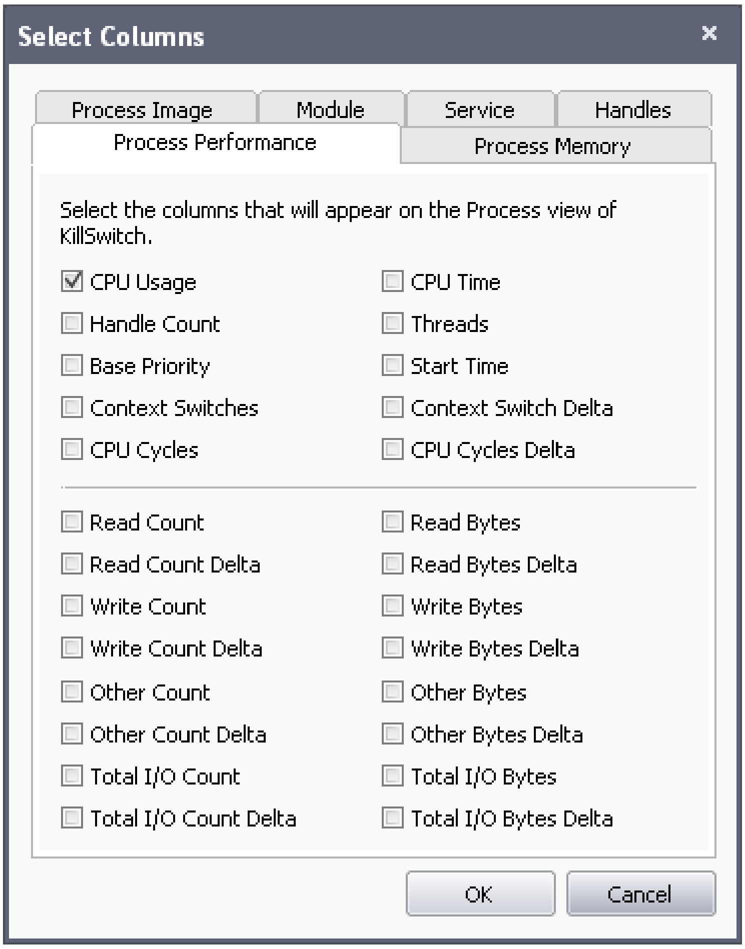
Select the columns that will appear on the Process view of KillSwitch.

☑ Process Name
☑ PID (Process Identifier)
☑ User Name
☑ Description
☑ Company Name
☑ Verified Signer
☑ Rating
☑ Session ID
☑ Command Line
☑ Version
☑ DEP Status
☑ Virtualized
☑ Image Path
☑ Intergrity Level

- Select the columns to be displayed by selecting the respective checkboxes
- Click OK for your configuration to take effect.

### Process Performance

The Process Performance tab allows you to select the columns to be displayed in the Process window,  to provide the detailed statistics and performance information like CPU usage, I/O activity and so on. This data will be useful to track the resource overhead of a process at a granular level.



Select Columns

Select the columns that will appear on the Process view of KillSwitch.

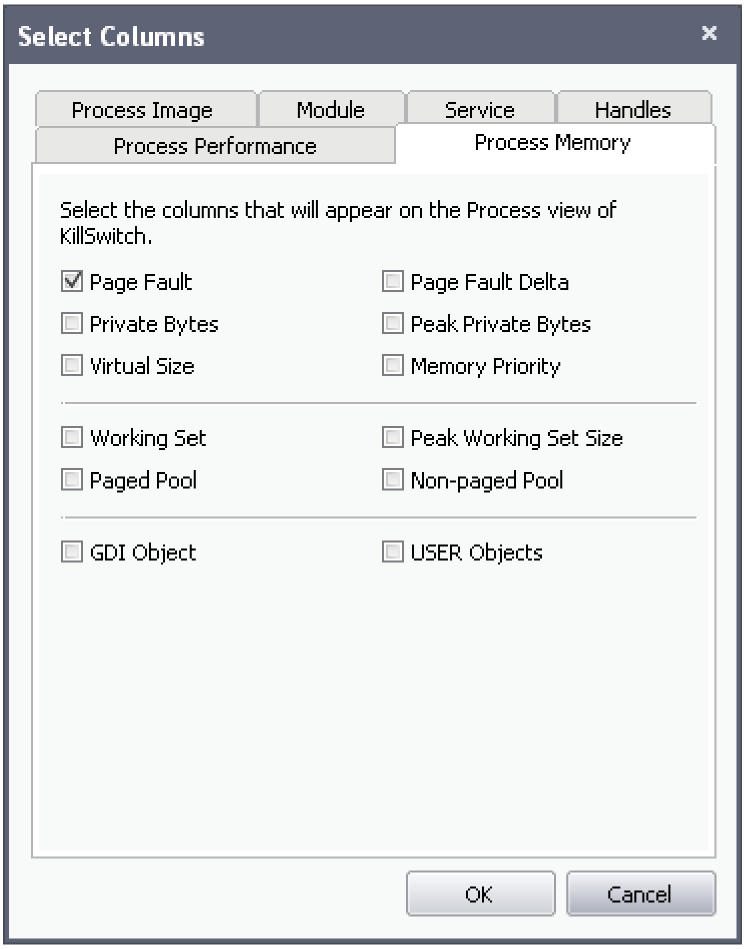
☑ CPU Usage
□ CPU Time
□ Handle Count
□ Threads
□ Base Priority
□ Start Time
□ Context Switches
□ Context Switch Delta
□ CPU Cycles
□ CPU Cycles Delta

□ Read Count
□ Read Bytes
□ Read Count Delta
□ Read Bytes Delta
□ Write Count
□ Write Bytes
□ Write Count Delta
□ Write Bytes Delta
□ Other Count
□ Other Bytes
□ Other Count Delta
□ Other Bytes Delta
□ Total I/O Count
□ Total I/O Bytes
□ Total I/O Count Delta
□ Total I/O Bytes Delta

- Select the columns to be displayed by selecting the respective checkboxes
- Click OK for your configuration to take effect.

### Process Memory

The Process Memory  tab allows you to select the columns to be displayed in the Process window,  to provide granular details on memory usage of each process.


Select Columns

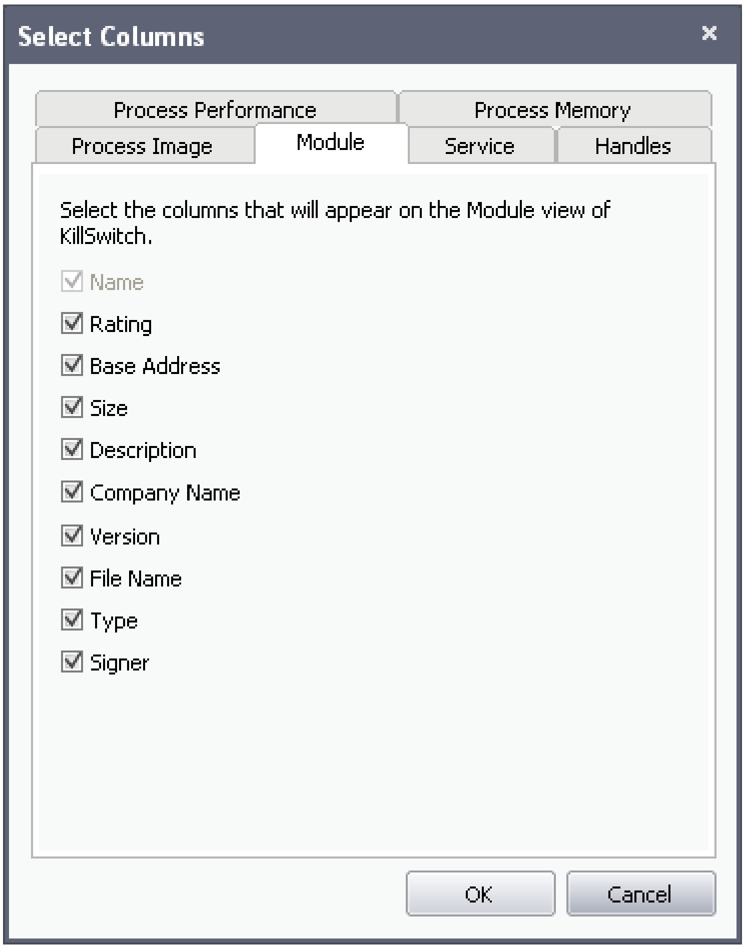
Select the columns that will appear on the Process view of KillSwitch.

☑ Page Fault
□ Page Fault Delta
□ Private Bytes
□ Peak Private Bytes
□ Virtual Size
□ Memory Priority
□ Working Set
□ Peak Working Set Size
□ Paged Pool
□ Non-paged Pool
□ GDI Object
□ USER Objects

- Select the columns to be displayed by selecting the respective checkboxes
- Click OK for your configuration to take effect.

### Module

The Module  tab allows you to configure the columns to be displayed under the 'Modules' tab in the 'Properties' dialog of a process.  For more details on the Properties dialog and the Modules tab, refer to the section **Viewing Properties of a Process** > **Modules**.



Select the columns that will appear on the Module view of KillSwitch.

- ☑ Name
- ☑ Rating
- ☑ Base Address
- ☑ Size
- ☑ Description
- ☑ Company Name
- ☑ Version
- ☑ File Name
- ☑ Type
- ☑ Signer

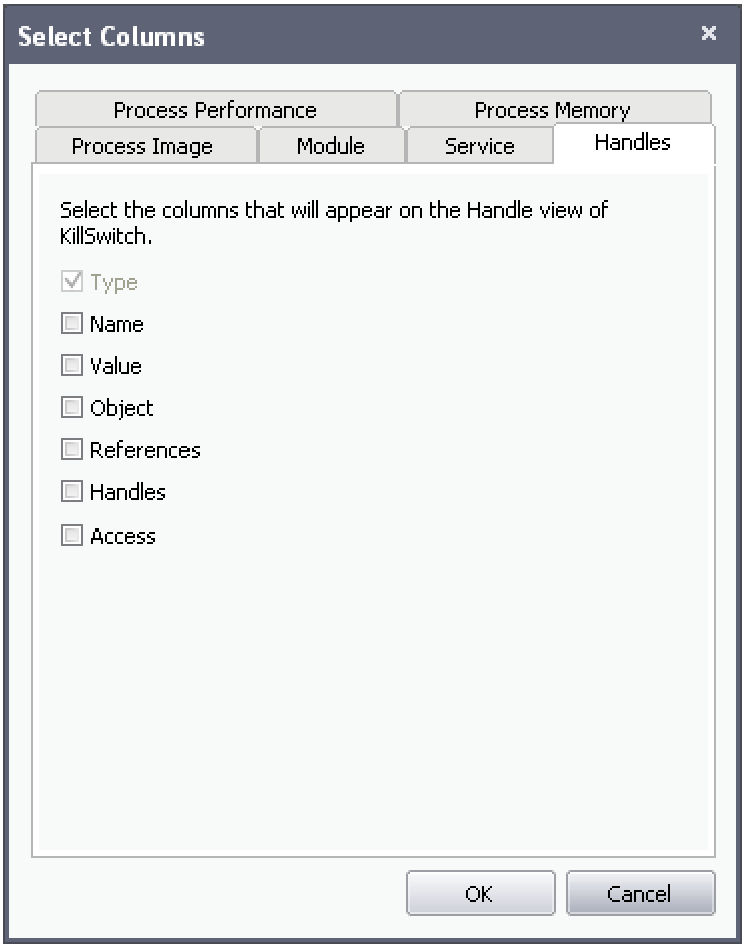
- Select the columns to be displayed by selecting the respective checkboxes
- Click OK for your configuration to take effect.

### Service

The Service tab allows you to configure the columns to be displayed in the Services window. Refer to the section **Services > Select Columns** for more details.

### Handles

The Handles tab allows you to configure the columns to be displayed under the 'Handles' tab in the 'Properties' dialog of a process. For more details on the Properties dialog and the 'Handles' tab, refer to the section **Viewing Properties of a Process** > **Handles**.



Select Columns

Select the columns that will appear on the Handle view of KillSwitch.

☑ Type
□ Name
□ Value
□ Object
□ References
□ Handles
□ Access

- Select the columns to be displayed by selecting the respective checkboxes
- Click OK for your configuration to take effect.

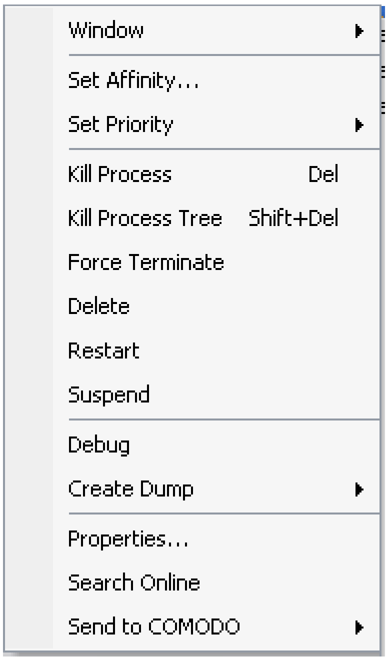
Next: **Stopping, Starting and Handling the Processes**

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

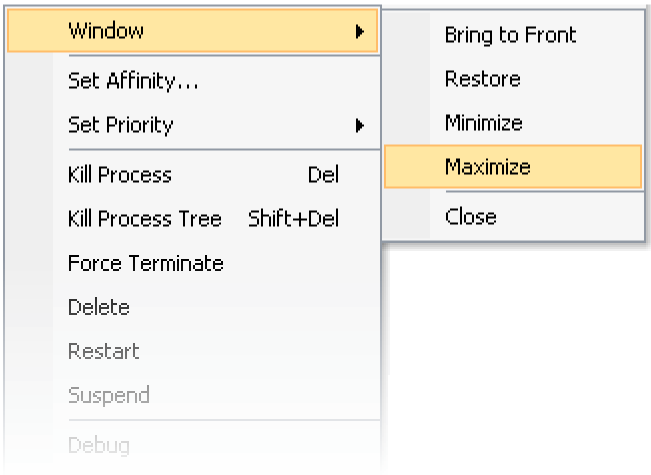
The 'Processes' window allows you to stop, suspend, restart, set priority, view properties and so on  of individual processes, by right clicking on the processes and selecting the option from the context sensitive menu.

**Tip**: KillSwitch can identify all unsafe processes and objects and then, according to your preference, Kill or Suspend 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.

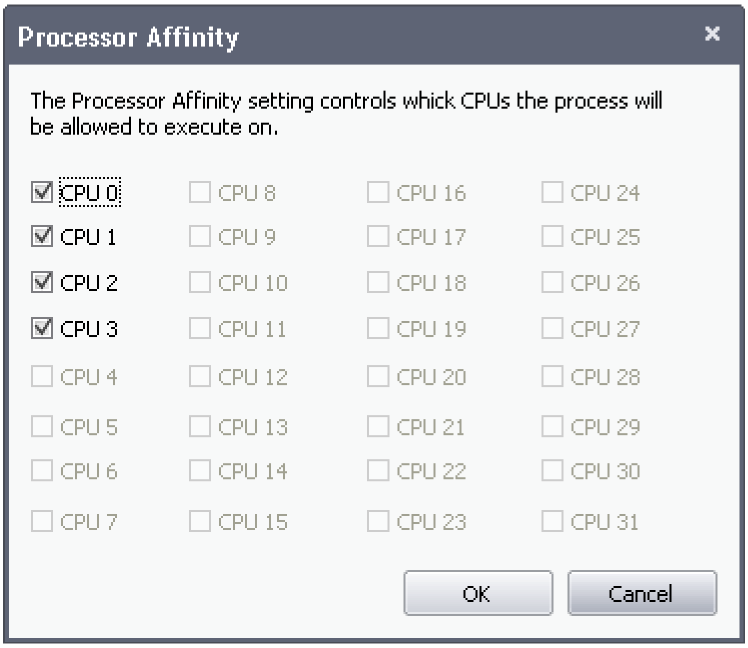


- **Window** - Allows you to position/re-size the process' window, if one was found. If the process does not have any visible windows, the menu is disabled. The options available are:



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

- **Set 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.



Processor Affinity

The Processor Affinity setting controls which CPUs the process will be allowed to execute on.

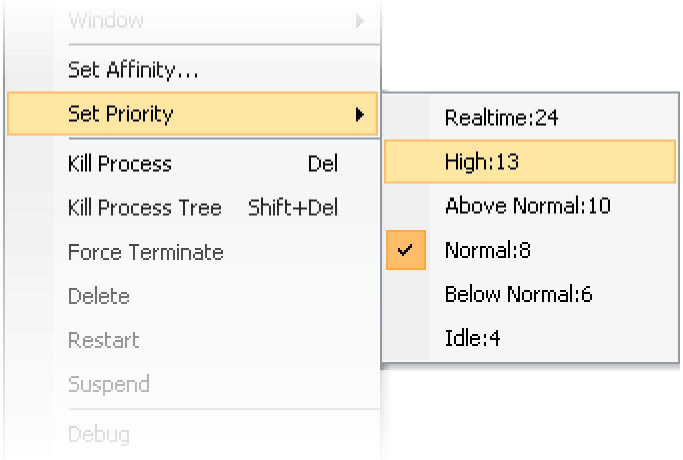
| | | | |
|---|---|---|---|
| ☑ CPU 0 | □ CPU 8 | □ CPU 16 | □ CPU 24 |
| ☑ CPU 1 | □ CPU 9 | □ CPU 17 | □ CPU 25 |
| ☑ CPU 2 | □ CPU 10 | □ CPU 18 | □ CPU 26 |
| ☑ CPU 3 | □ CPU 11 | □ CPU 19 | □ CPU 27 |
| □ CPU 4 | □ CPU 12 | □ CPU 20 | □ CPU 28 |
| □ CPU 5 | □ CPU 13 | □ CPU 21 | □ CPU 29 |
| □ CPU 6 | □ CPU 14 | □ CPU 22 | □ CPU 30 |
| □ CPU 7 | □ CPU 15 | □ CPU 23 | □ CPU 31 |

**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.

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

- **Priority** - Enables you to sets the priority for the process. The available options are:
  - Real Time;
  - High;
  - Above Normal;
  - Normal;
  - Below Normal;
  - Idle.

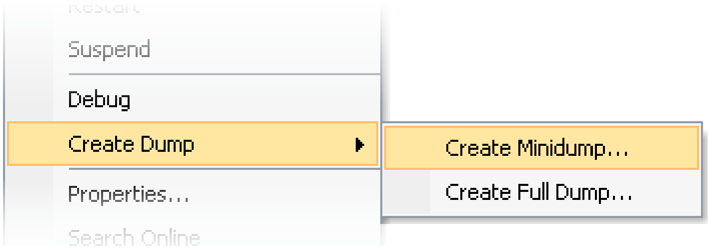


- **Kill Process** - Terminates the selected process(es). KillSwitch can, except under extraordinary circumstances, be able to terminate any process, including ones protected by rootkits or security software.
- **Kill Process Tree** - Terminates the selected process and its descendants (child processes).
- **Force Terminate** - Terminates the selected process(es) forcibly. This option suits for closing any programs that are under 'Not Responding' status.
- **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.

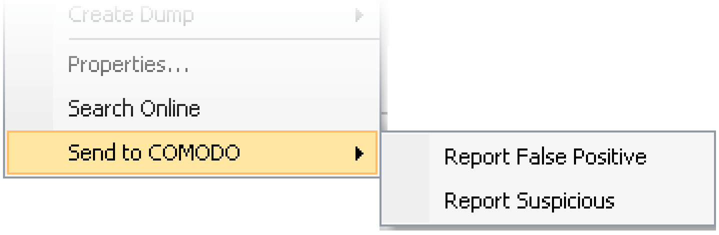
**Warning**: Deleting a process will permanently remove the application that has triggered the process.

- **Restart** - Restarts the selected process with the same command line arguments and working directory.
- **Suspend** - Suspends the selected process(es). KillSwitch can suspend any process, including ones protected by rootkits or security
- **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.
- **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. The available options are:



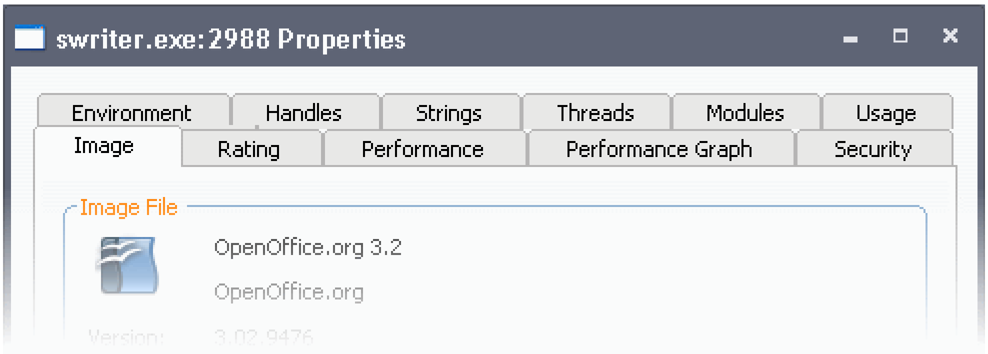
- Create Minidump... - Creates a small dump file containing only essential data.
- Create Fulldump... - Creates a full dump containing all the data.

- **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.
- **Send to COMODO** - Submits the application that has triggered the process for analysis to Comodo, as False Positive (if identified as suspicious by KillSwitch) or as Suspicious file 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 global white list or black list accordingly in order to benefit all the users of Comodo security products world wide.



## 5.3.1.2. 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 11 separate tabs, each containing important information and functionality related to the particular process.



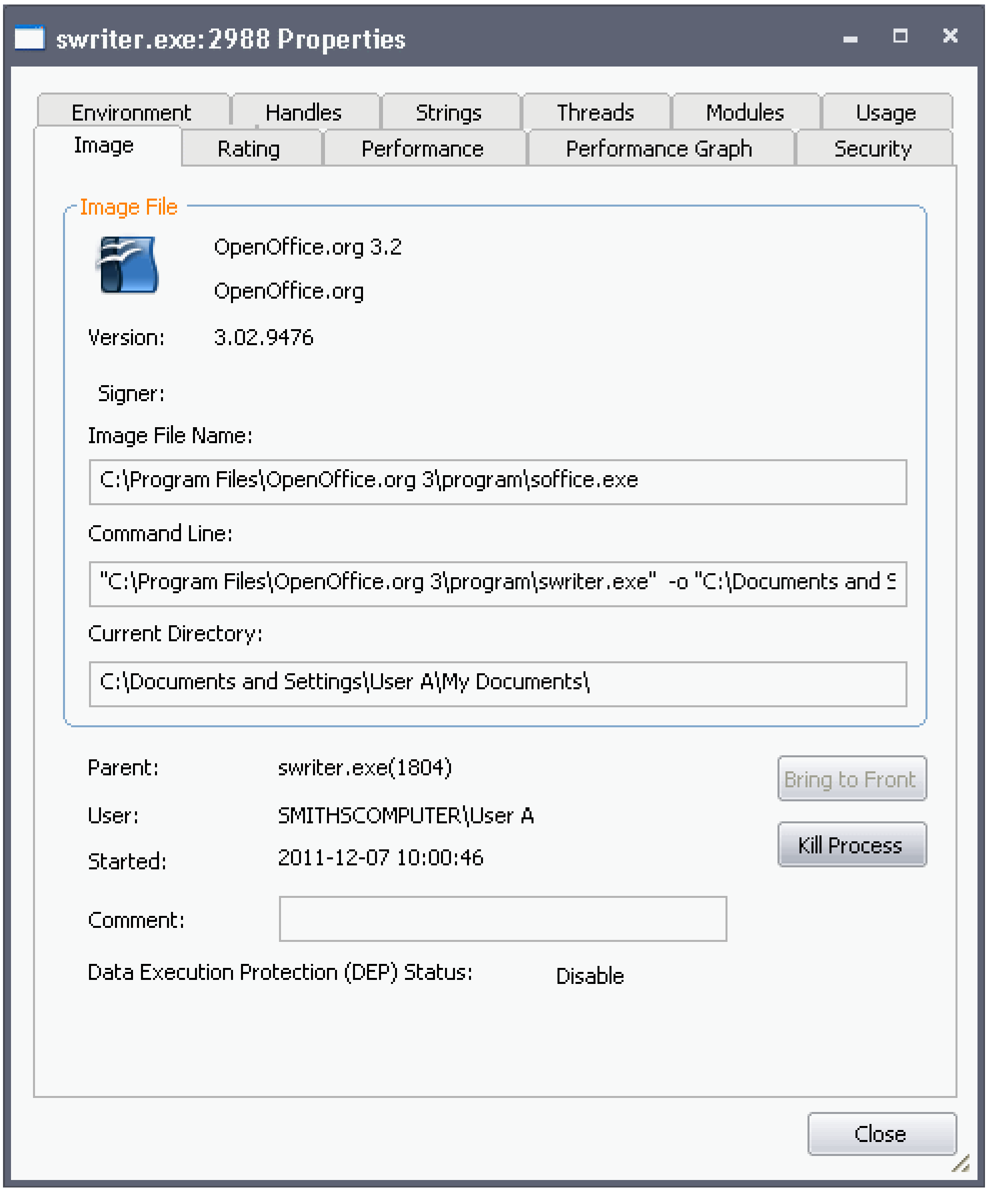
Further details are available on each tab by clicking the following links :

- **Image;**
- **Rating;**
- **Performance;**
- **Performance Graph;**
- **Security**;
- **Environment;**
- **Handles;**
- **Strings;**
- **Threads;**
- **Modules;**
- **Usage**.

**Note**: The 'Usage' tab will be displayed only for the processes at the first level of the process hierarchy. For the branch processes in the process tree, the 'Usage' tab will not be displayed and hence the 'Properties' dialog will contain only 10 tabs.

## Image

The 'Image' tab displays the basic information about the process and its image file. You can also view its command line, Data Execution Prevention (DEP) status, terminate the process and so on. The dialog also allows you to make the Window of the parent application of the process active and to terminate the process.



swriter.exe:2988 Properties

Image File

OpenOffice.org 3.2

OpenOffice.org

Version: 3.02.9476

Signer:

Image File Name:

C:\Program Files\OpenOffice.org 3\program\soffice.exe

Command Line:

"C:\Program Files\OpenOffice.org 3\program\swriter.exe" -o "C:\Documents and S

Current Directory:

C:\Documents and Settings\User A\My Documents\

Parent: swriter.exe(1804)

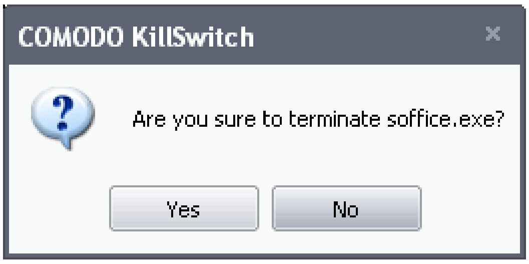
User: SMITHSCOMPUTER\User A

Started: 2011-12-07 10:00:46

Comment:

Data Execution Protection (DEP) Status: Disable

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



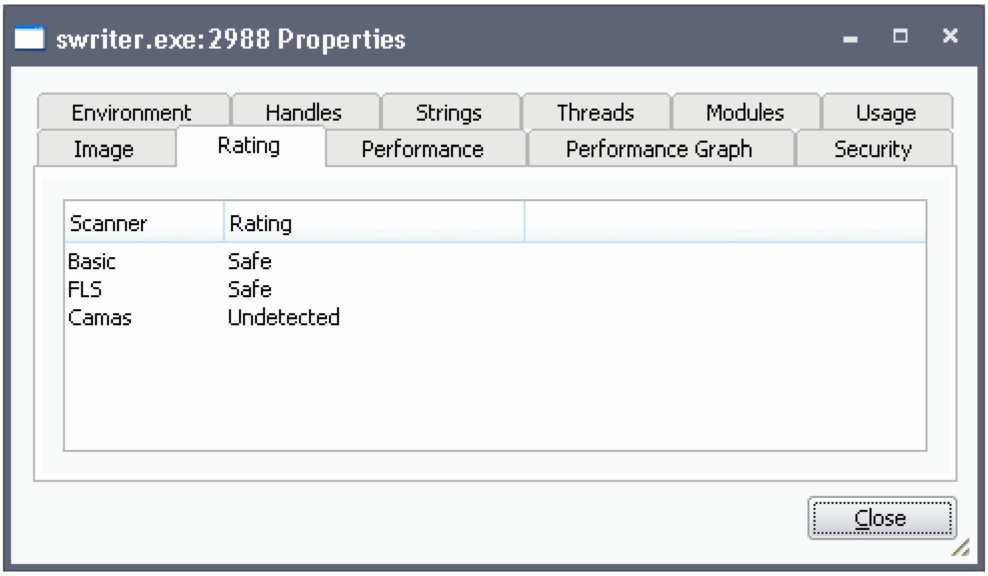
COMODO KillSwitch

Are you sure to terminate soffice.exe?

Click here to go back to list of properties.

## Rating

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



| Scanner | Rating |
|---|---|
| Basic | Safe |
| FLS | Safe |
| Camas | Undetected |

You can see the following scan results:

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

The Rating list shows the final rating **only** according to the priorities. The priority of scan results are the following (High to low):

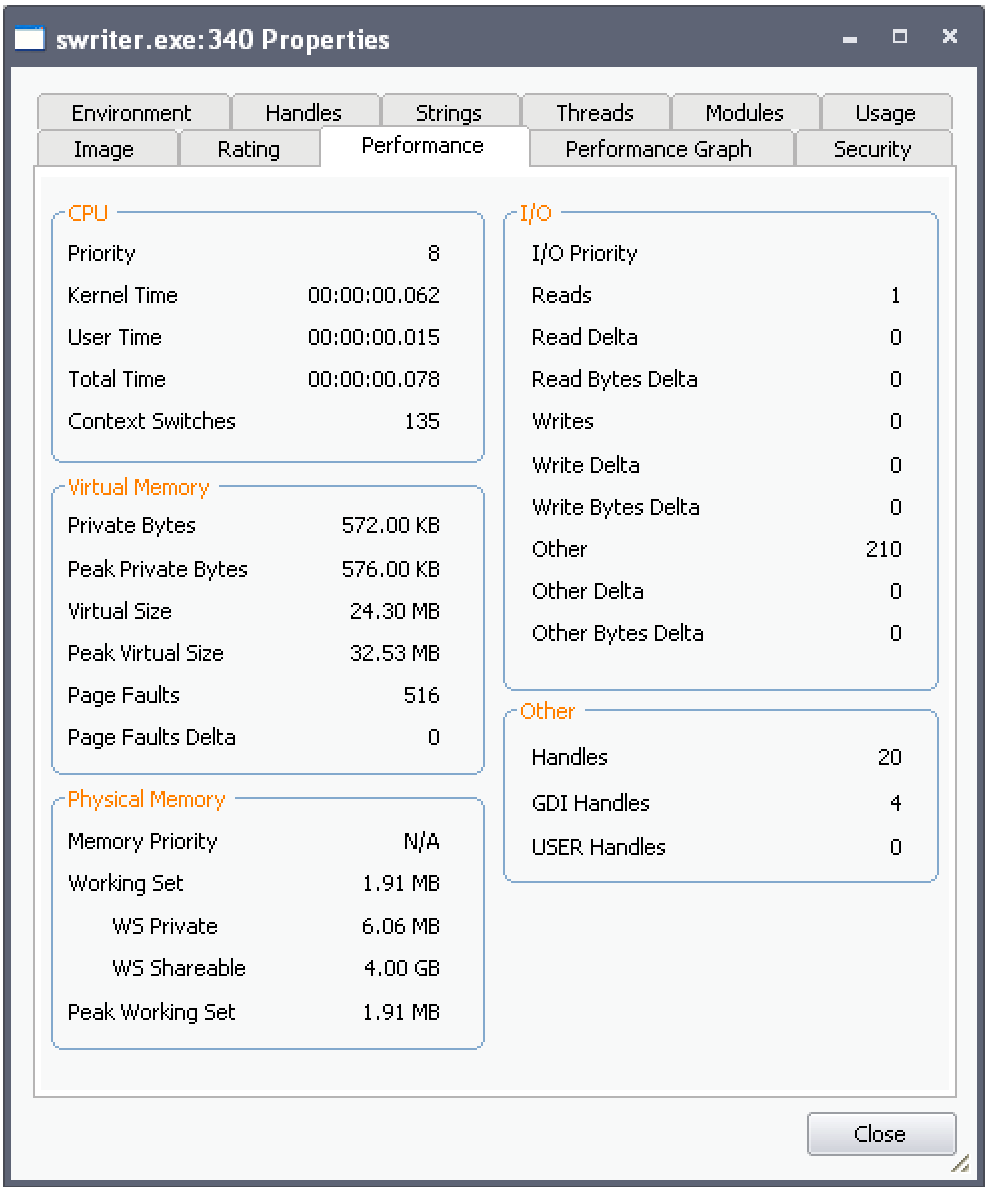
1. Basic.Malware
2. FLS.Malware
3. FLS.Safe
4. CAMAS.Detected
5. CAMAS.Malware
6. CAMAS.Suspicious
7. CAMAS.SuspiciousP
8. CAMAS.SuspiciousPP
9. FLS.Unknown

10. FLS.Absent

Click here to go back to list of properties.

## Performance

The 'Performance' 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.



CPU

| | |
|---|---|
| Priority | 8 |
| Kernel Time | 00:00:00.062 |
| User Time | 00:00:00.015 |
| Total Time | 00:00:00.078 |
| Context Switches | 135 |

Virtual Memory

| | |
|---|---|
| Private Bytes | 572.00 KB |
| Peak Private Bytes | 576.00 KB |
| Virtual Size | 24.30 MB |
| Peak Virtual Size | 32.53 MB |
| Page Faults | 516 |
| Page Faults Delta | 0 |

Physical Memory

| | |
|---|---|
| Memory Priority | N/A |
| Working Set | 1.91 MB |
| WS Private | 6.06 MB |
| WS Shareable | 4.00 GB |
| Peak Working Set | 1.91 MB |

I/O

| | |
|---|---|
| I/O Priority | |
| Reads | 1 |
| Read Delta | 0 |
| Read Bytes Delta | 0 |
| Writes | 0 |
| Write Delta | 0 |
| Write Bytes Delta | 0 |
| Other | 210 |
| Other Delta | 0 |
| Other Bytes Delta | 0 |

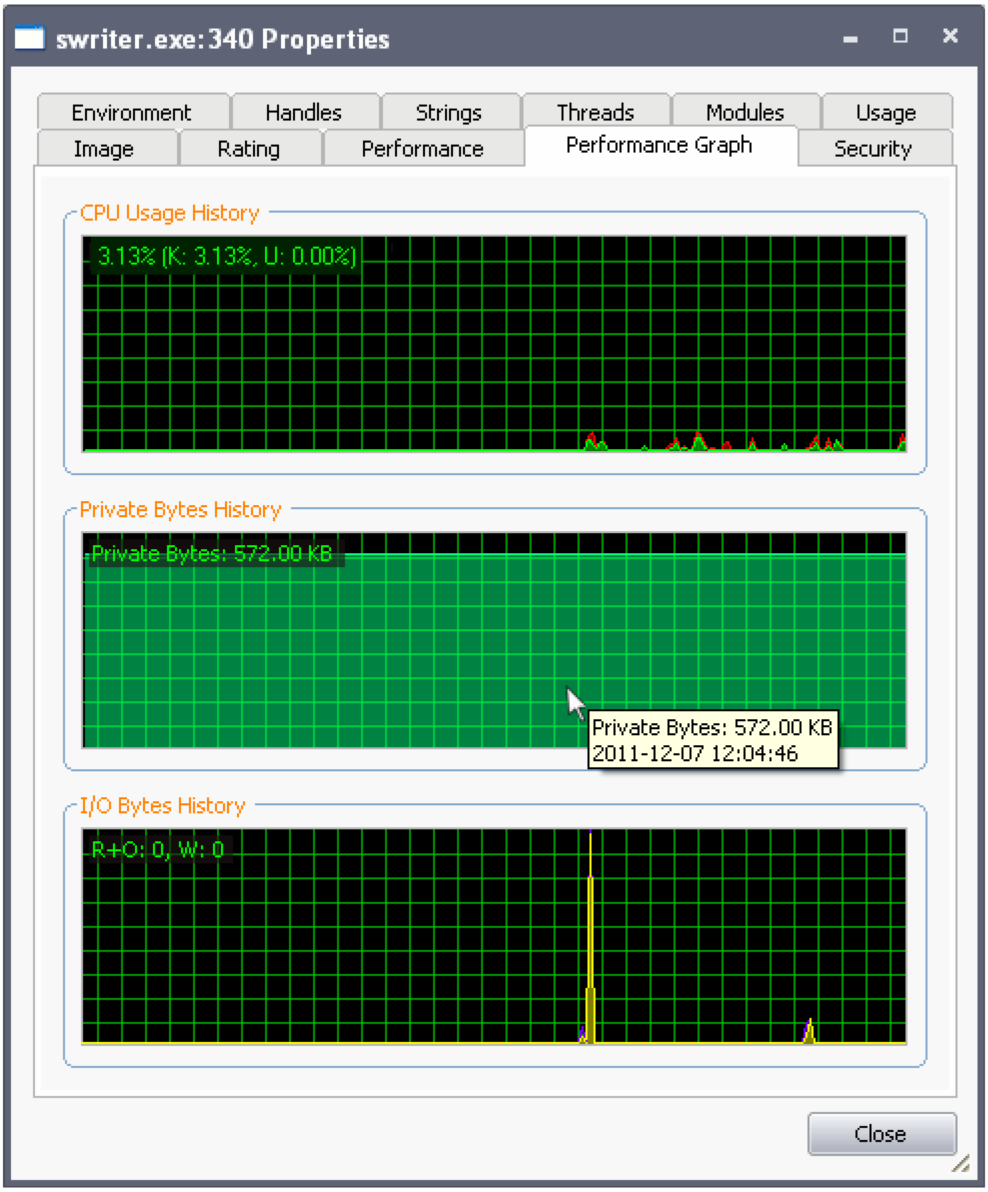
Other

| | |
|---|---|
| Handles | 20 |
| GDI Handles | 4 |
| USER Handles | 0 |

Click here to go back to list of properties.

## Performance Graph

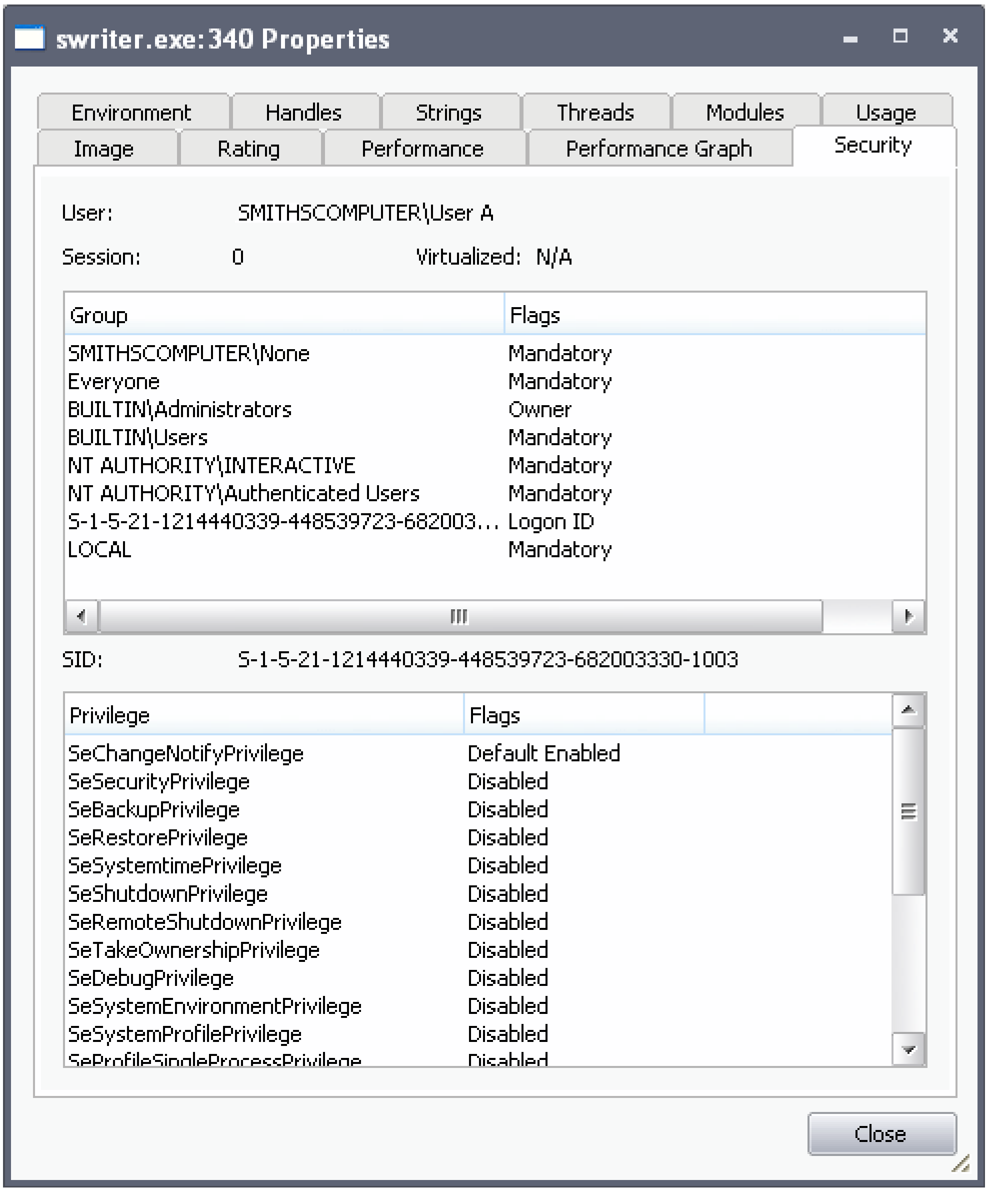
The 'Performance Graph' tab displays three graphs relating to the process' performance - CPU Usage, Private Bytes, and I/O activity. This window helps the advanced users to track the resource overhead of a process pictorially. You can hover your mouse over the graphs to view details.



**Click here to go back to list of properties**.

## Security

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



User: SMITHSCOMPUTER\User A

Session: 0 Virtualized: N/A

| Group | Flags |
|---|---|
| SMITHSCOMPUTER\None | Mandatory |
| Everyone | Mandatory |
| BUILTIN\Administrators | Owner |
| BUILTIN\Users | Mandatory |
| NT AUTHORITY\INTERACTIVE | Mandatory |
| NT AUTHORITY\Authenticated Users | Mandatory |
| S-1-5-21-1214440339-448539723-682003... | Logon ID |
| LOCAL | Mandatory |

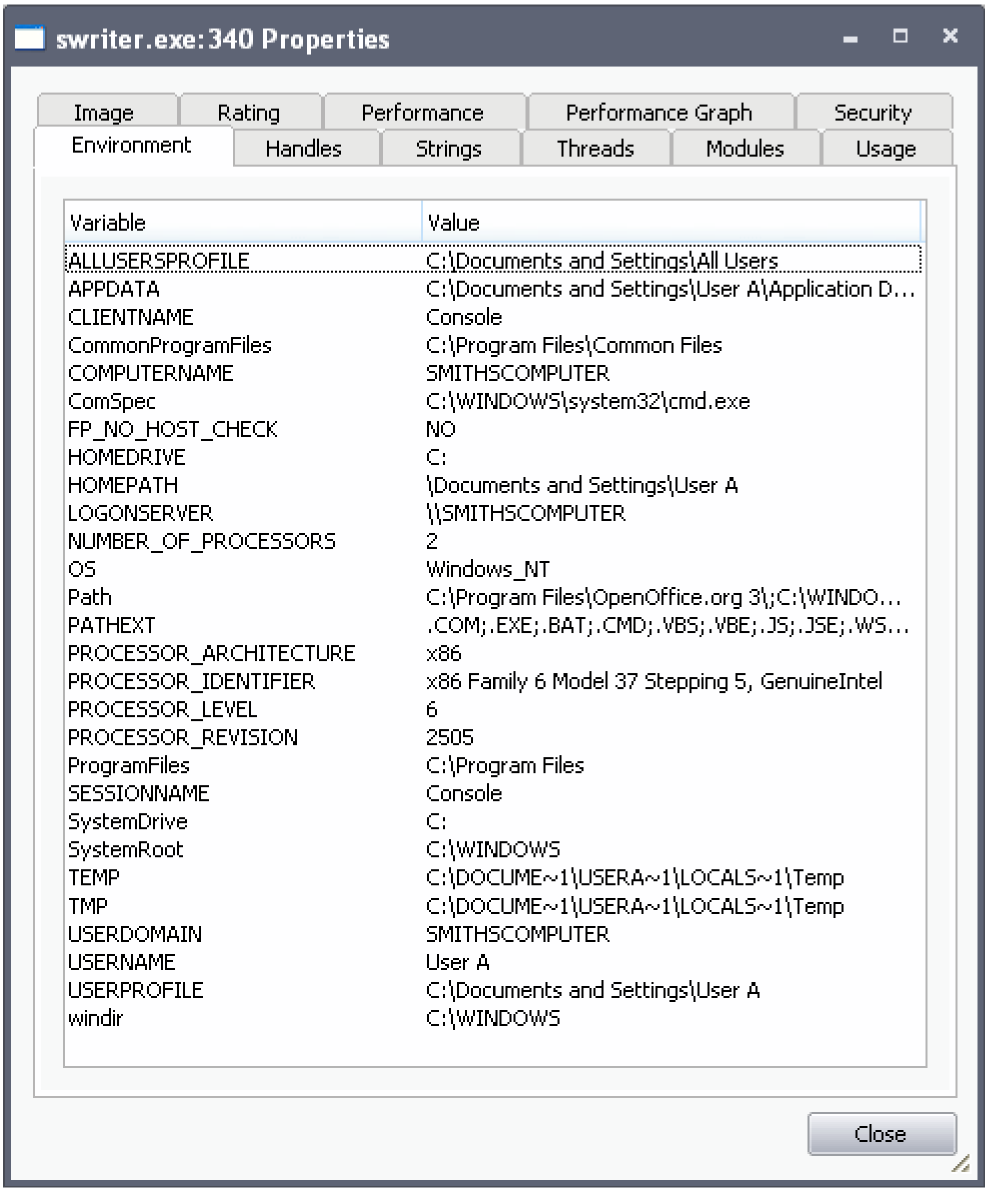
SID: S-1-5-21-1214440339-448539723-682003330-1003

| Privilege | Flags |
|---|---|
| SeChangeNotifyPrivilege | Default Enabled |
| SeSecurityPrivilege | Disabled |
| SeBackupPrivilege | Disabled |
| SeRestorePrivilege | Disabled |
| SeSystemtimePrivilege | Disabled |
| SeShutdownPrivilege | Disabled |
| SeRemoteShutdownPrivilege | Disabled |
| SeTakeOwnershipPrivilege | Disabled |
| SeDebugPrivilege | Disabled |
| SeSystemEnvironmentPrivilege | Disabled |
| SeSystemProfilePrivilege | Disabled |
| SeProfileSingleProcessPrivilege | Disabled |

**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.

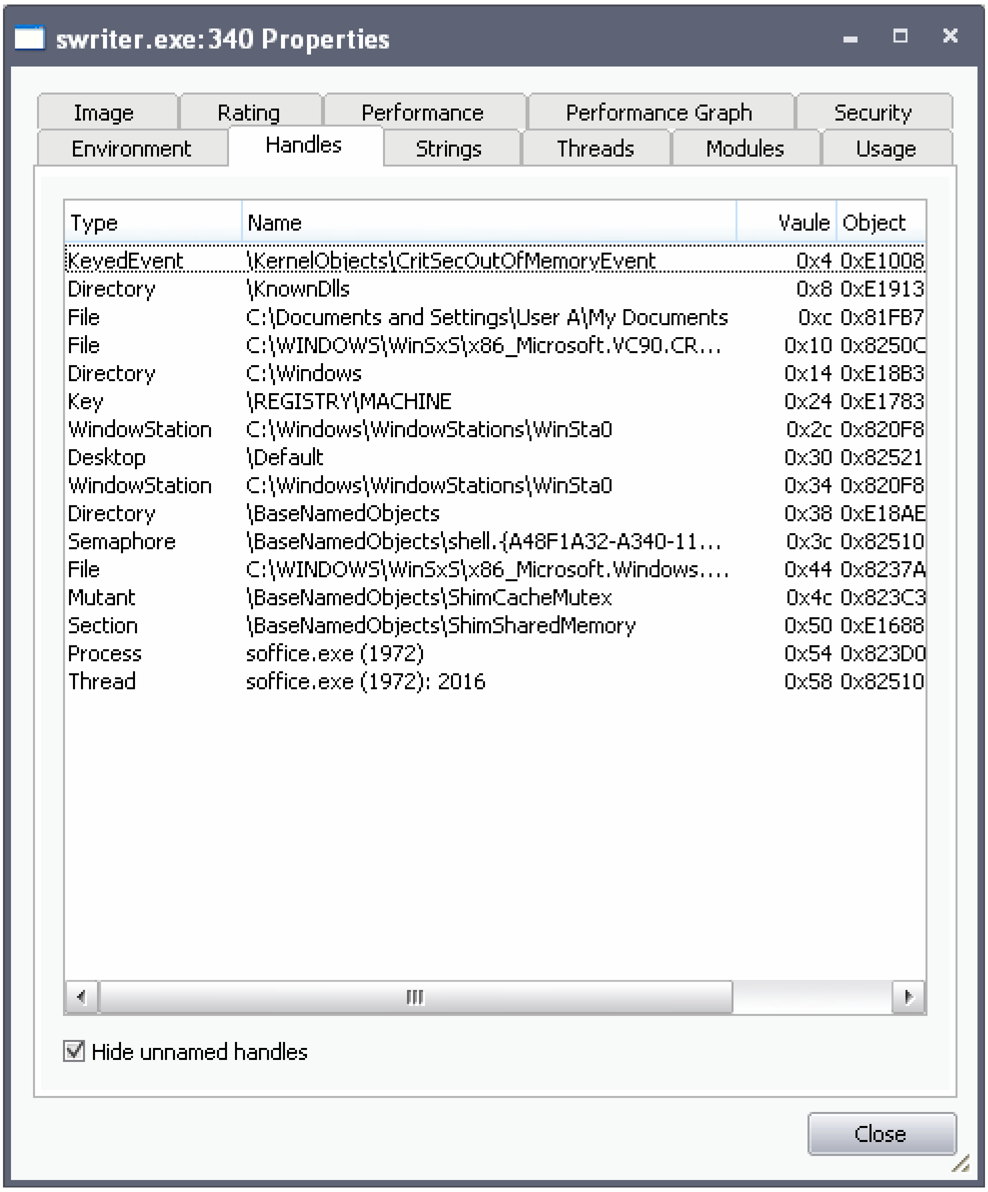


| Variable | Value |
|---|---|
| ALLUSERSPROFILE | C:\Documents and Settings\All Users |
| APPDATA | C:\Documents and Settings\User A\Application D... |
| CLIENTNAME | Console |
| CommonProgramFiles | C:\Program Files\Common Files |
| COMPUTERNAME | SMITHSCOMPUTER |
| ComSpec | C:\WINDOWS\system32\cmd.exe |
| FP_NO_HOST_CHECK | NO |
| HOMEDRIVE | C: |
| HOMEPATH | \Documents and Settings\User A |
| LOGONSERVER | \\SMITHSCOMPUTER |
| NUMBER_OF_PROCESSORS | 2 |
| OS | Windows_NT |
| Path | C:\Program Files\OpenOffice.org 3\;C:\WINDO... |
| PATHEXT | .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WS... |
| PROCESSOR_ARCHITECTURE | x86 |
| PROCESSOR_IDENTIFIER | x86 Family 6 Model 37 Stepping 5, GenuineIntel |
| PROCESSOR_LEVEL | 6 |
| PROCESSOR_REVISION | 2505 |
| ProgramFiles | C:\Program Files |
| SESSIONNAME | Console |
| SystemDrive | C: |
| SystemRoot | C:\WINDOWS |
| TEMP | C:\DOCUME~1\USERA~1\LOCALS~1\Temp |
| TMP | C:\DOCUME~1\USERA~1\LOCALS~1\Temp |
| USERDOMAIN | SMITHSCOMPUTER |
| USERNAME | User A |
| USERPROFILE | C:\Documents and Settings\User A |
| windir | C:\WINDOWS |

**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.

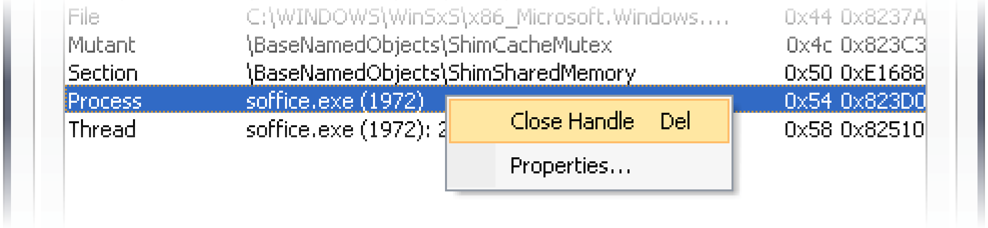


| Type | Name | Vaule | Object |
|---|---|---|---|
| KeyedEvent | \KernelObjects\CritSecOutOfMemoryEvent | 0x4 | 0xE1008 |
| Directory | \KnownDlls | 0x8 | 0xE1913 |
| File | C:\Documents and Settings\User A\My Documents | 0xc | 0x81FB7 |
| File | C:\WINDOWS\WinSxS\x86_Microsoft.VC90.CR... | 0x10 | 0x8250C |
| Directory | C:\Windows | 0x14 | 0xE18B3 |
| Key | \REGISTRY\MACHINE | 0x24 | 0xE1783 |
| WindowStation | C:\Windows\WindowStations\WinSta0 | 0x2c | 0x820F8 |
| Desktop | \Default | 0x30 | 0x82521 |
| WindowStation | C:\Windows\WindowStations\WinSta0 | 0x34 | 0x820F8 |
| Directory | \BaseNamedObjects | 0x38 | 0xE18AE |
| Semaphore | \BaseNamedObjects\shell.{A48F1A32-A340-11... | 0x3c | 0x82510 |
| File | C:\WINDOWS\WinSxS\x86_Microsoft.Windows.... | 0x44 | 0x8237A |
| Mutant | \BaseNamedObjects\ShimCacheMutex | 0x4c | 0x823C3 |
| Section | \BaseNamedObjects\ShimSharedMemory | 0x50 | 0xE1688 |
| Process | soffice.exe (1972) | 0x54 | 0x823D0 |
| Thread | soffice.exe (1972): 2016 | 0x58 | 0x82510 |

☑ Hide unnamed handles

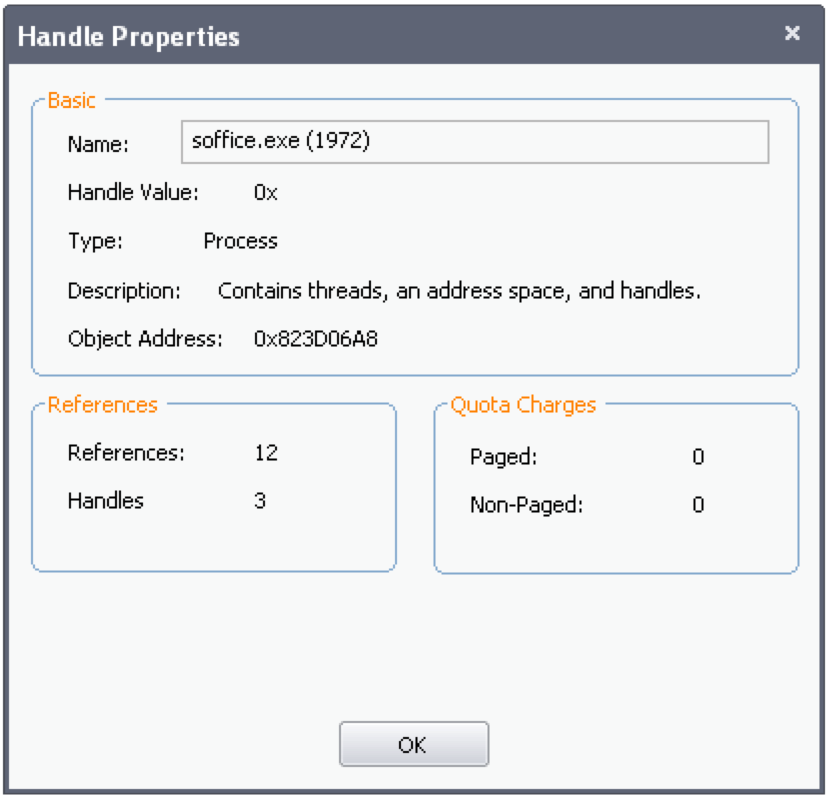
**Tip**: The columns displayed in Handles interface can be configured to display the details as required. Refer to **Column Selection** > **Handles** for more details.

- **Hide unnamed handles** - Selecting this option removes the handles that do not have a name from the list of handles displayed.
- Right-clicking on an handle opens a context sensitive menu that enables to you to close or view the properties of the handle.



| | | | |
|---|---|---|---|
| File | C:\WINDOWS\WinSxS\x86_Microsoft.Windows.... | 0x44 | 0x8237A |
| Mutant | \BaseNamedObjects\ShimCacheMutex | 0x4c | 0x823C3 |
| Section | \BaseNamedObjects\ShimSharedMemory | 0x50 | 0xE1688 |
| Process | soffice.exe (1972) | 0x54 | 0x823D0 |
| Thread | soffice.exe (1972): 2 | 0x58 | 0x82510 |

- **Close Handle** - Closes the Handle. Closing a process handle does not terminate the associated process or remove the process object.
- **Properties** - Opens the 'Properties' dialog of the Handle. Also double clicking a handle opens its 'Properties' dialog.



Handle Properties

Basic

Name: soffice.exe (1972)

Handle Value: 0x

Type: Process

Description: Contains threads, an address space, and handles.

Object Address: 0x823D06A8

References

References: 12

Handles 3

Quota Charges

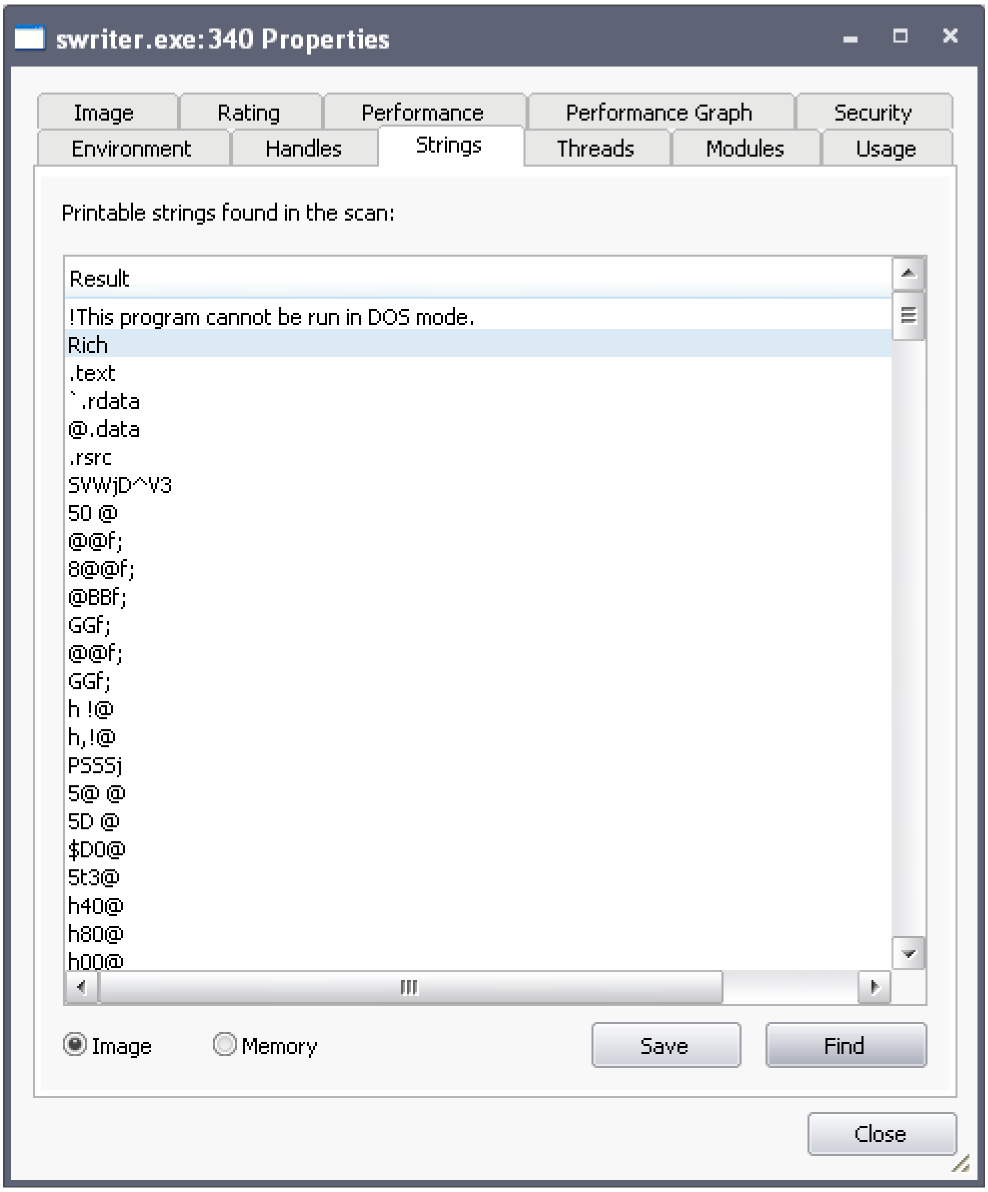
Paged: 0

Non-Paged: 0

**Click here to go back to list of properties**.

## Strings

The 'Strings' tab displays a list of ASCII and Unicode strings that are loaded to the process. You can choose to extract the threads loaded to Process image or Process memory.



Printable strings found in the scan:

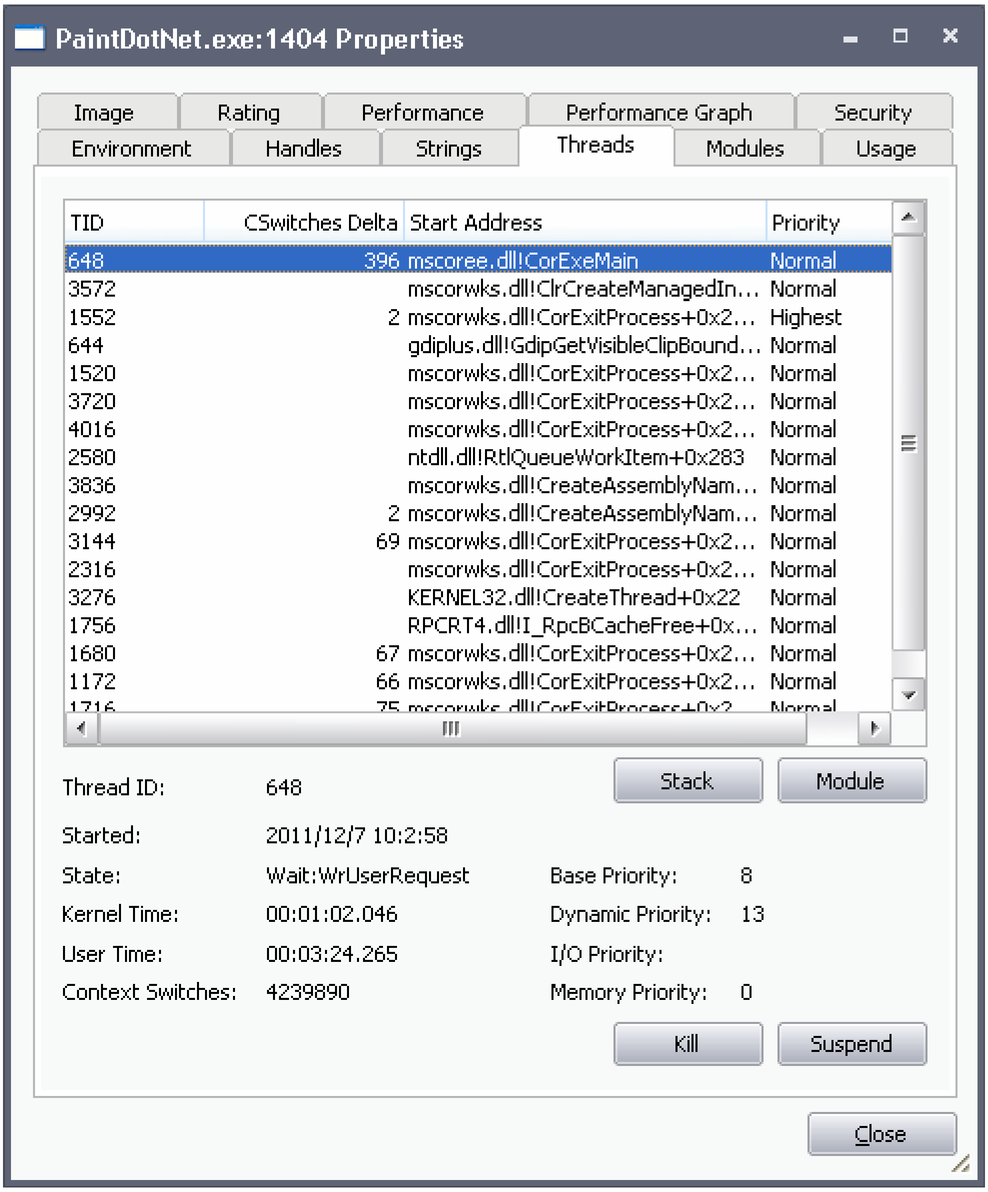
```
Result
!This program cannot be run in DOS mode.
Rich
.text
`.rdata
@.data
.rsrc
SVWjD^V3
50 @
@@f;
8@@f;
@BBf;
GGf;
@@f;
GGf;
h !@
h,!@
PSSSj
5@ @
5D @
$D0@
5t3@
h40@
h80@
h00@
```

● Image ○ Memory

- Select ‘Image’ or ‘Memory’ to extract and view the strings from Process Image or the Process Memory respectively.
- Click 'Save' to save the displayed list of strings as a text file.

## 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 and modules.



| TID | CSwitches Delta | Start Address | Priority |
|---|---|---|---|
| 648 | 396 | mscoree.dll!CorExeMain | Normal |
| 3572 | | mscorwks.dll!ClrCreateManagedIn... | Normal |
| 1552 | 2 | mscorwks.dll!CorExitProcess+0x2... | Highest |
| 644 | | gdiplus.dll!GdipGetVisibleClipBound... | Normal |
| 1520 | | mscorwks.dll!CorExitProcess+0x2... | Normal |
| 3720 | | mscorwks.dll!CorExitProcess+0x2... | Normal |
| 4016 | | mscorwks.dll!CorExitProcess+0x2... | Normal |
| 2580 | | ntdll.dll!RtlQueueWorkItem+0x283 | Normal |
| 3836 | | mscorwks.dll!CreateAssemblyNam... | Normal |
| 2992 | 2 | mscorwks.dll!CreateAssemblyNam... | Normal |
| 3144 | 69 | mscorwks.dll!CorExitProcess+0x2... | Normal |
| 2316 | | mscorwks.dll!CorExitProcess+0x2... | Normal |
| 3276 | | KERNEL32.dll!CreateThread+0x22 | Normal |
| 1756 | | RPCRT4.dll!I_RpcBCacheFree+0x... | Normal |
| 1680 | 67 | mscorwks.dll!CorExitProcess+0x2... | Normal |
| 1172 | 66 | mscorwks.dll!CorExitProcess+0x2... | Normal |
| 1716 | 75 | mscorwks.dll!CorExitProcess+0x2 | Normal |

Thread ID: 648

Started: 2011/12/7 10:2:58

State: Wait:WrUserRequest

Kernel Time: 00:01:02.046

User Time: 00:03:24.265

Context Switches: 4239890

Base Priority: 8

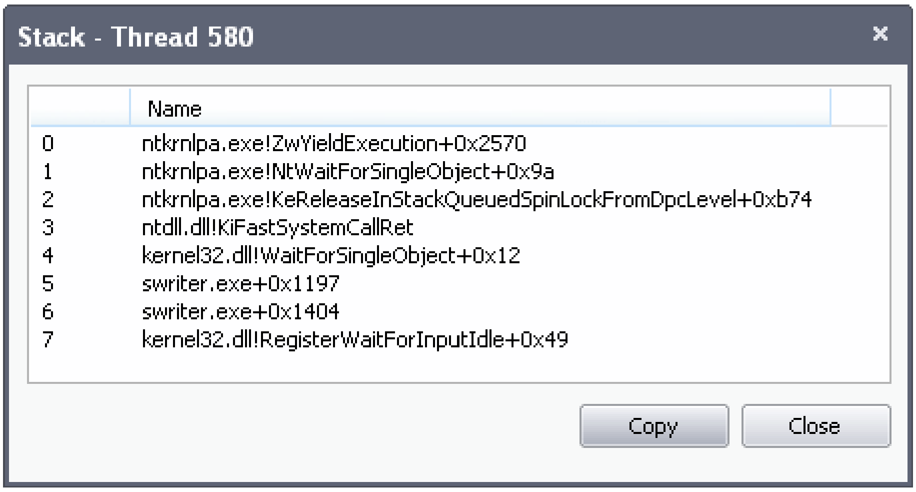
Dynamic Priority: 13

I/O Priority:

Memory Priority: 0

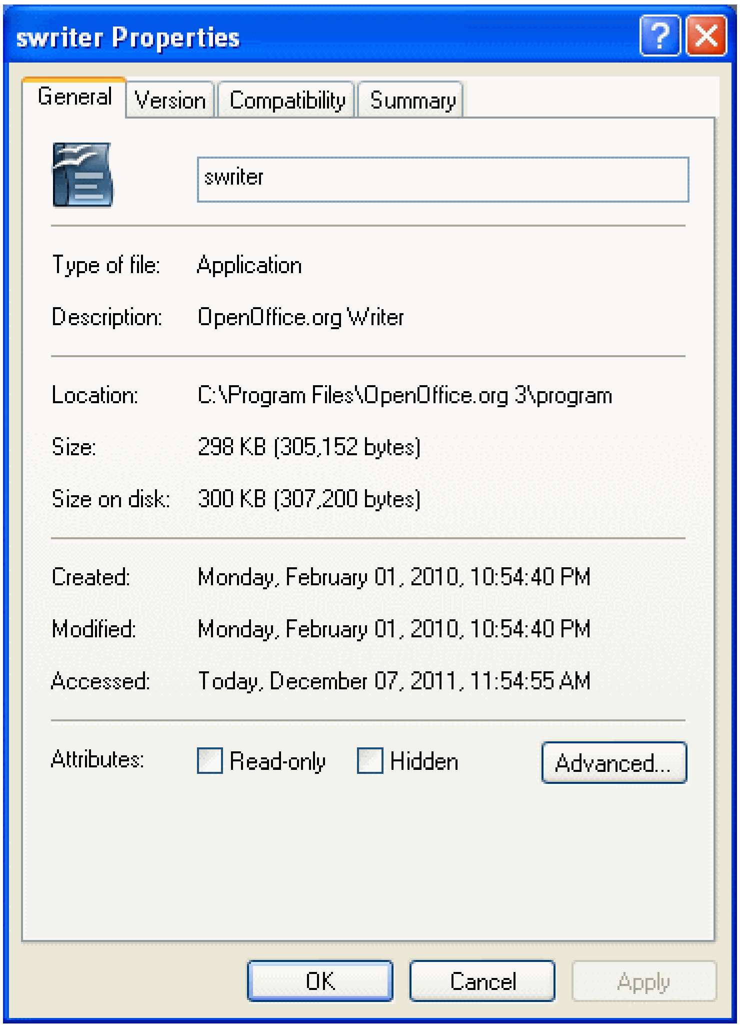
## Handling Threads

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



| | Name |
|---|---|
| 0 | ntkrnlpa.exe!ZwYieldExecution+0x2570 |
| 1 | ntkrnlpa.exe!NtWaitForSingleObject+0x9a |
| 2 | ntkrnlpa.exe!KeReleaseInStackQueuedSpinLockFromDpcLevel+0xb74 |
| 3 | ntdll.dll!KiFastSystemCallRet |
| 4 | kernel32.dll!WaitForSingleObject+0x12 |
| 5 | swriter.exe+0x1197 |
| 6 | swriter.exe+0x1404 |
| 7 | kernel32.dll!RegisterWaitForInputIdle+0x49 |

- **Module** - Opens the 'Properties' dialog of the module that has invoked the process.



swriter

Type of file: Application

Description: OpenOffice.org Writer

Location: C:\Program Files\OpenOffice.org 3\program

Size: 298 KB (305,152 bytes)

Size on disk: 300 KB (307,200 bytes)

Created: Monday, February 01, 2010, 10:54:40 PM

Modified: Monday, February 01, 2010, 10:54:40 PM

Accessed: Today, December 07, 2011, 11:54:55 AM

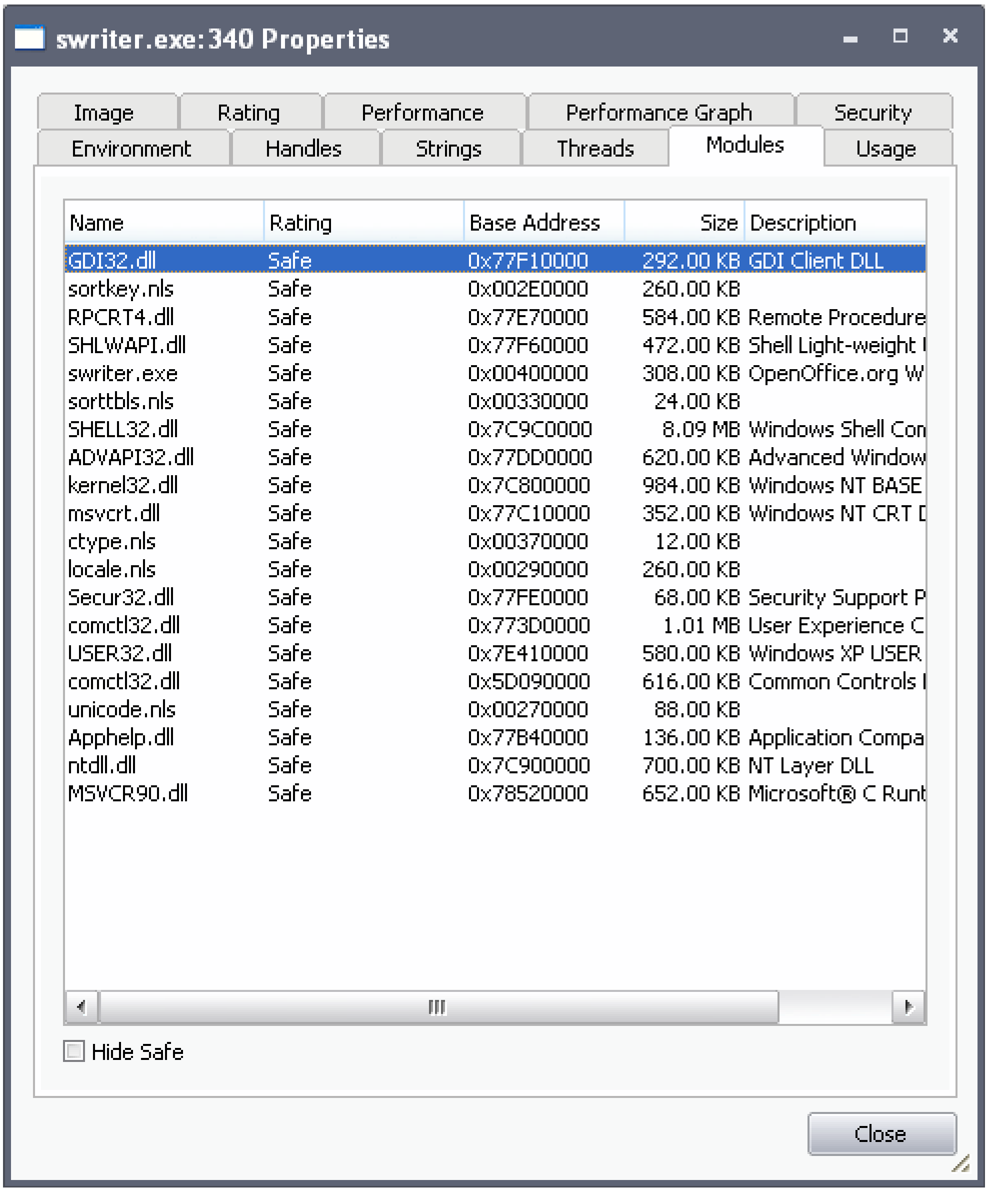
Attributes: □ Read-only □ Hidden

- **Kill** – Terminates the thread. Terminating the thread does not  terminate the associated process or remove the process object.
- **Suspend** – Suspends the thread.

**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.  Double clicking on a Module opens the 'Properties' dialog of it.



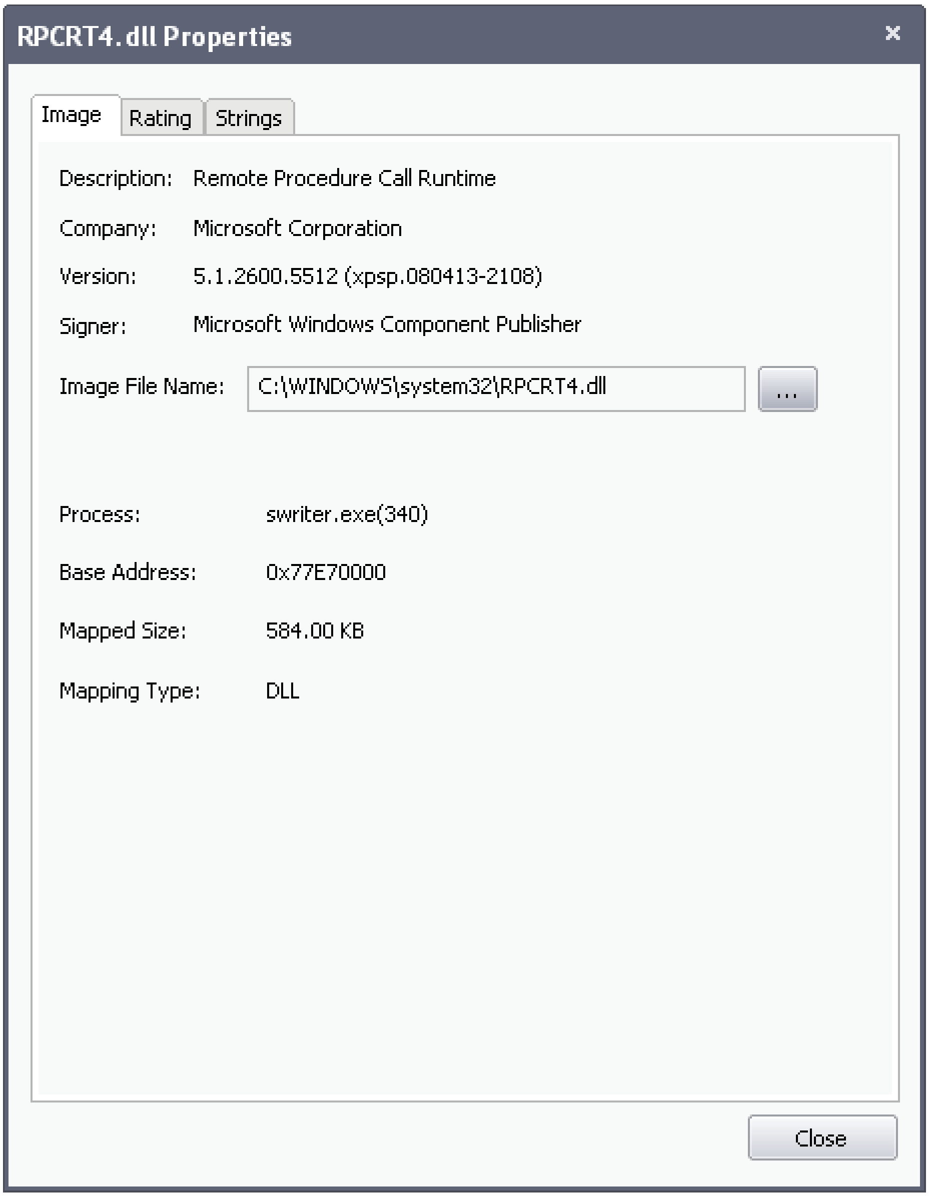
| Name | Rating | Base Address | Size | Description |
|---|---|---|---|---|
| GDI32.dll | Safe | 0x77F10000 | 292.00 KB | GDI Client DLL |
| sortkey.nls | Safe | 0x002E0000 | 260.00 KB | |
| RPCRT4.dll | Safe | 0x77E70000 | 584.00 KB | Remote Procedure |
| SHLWAPI.dll | Safe | 0x77F60000 | 472.00 KB | Shell Light-weight |
| swriter.exe | Safe | 0x00400000 | 308.00 KB | OpenOffice.org W |
| sorttbls.nls | Safe | 0x00330000 | 24.00 KB | |
| SHELL32.dll | Safe | 0x7C9C0000 | 8.09 MB | Windows Shell Con |
| ADVAPI32.dll | Safe | 0x77DD0000 | 620.00 KB | Advanced Window |
| kernel32.dll | Safe | 0x7C800000 | 984.00 KB | Windows NT BASE |
| msvcrt.dll | Safe | 0x77C10000 | 352.00 KB | Windows NT CRT D |
| ctype.nls | Safe | 0x00370000 | 12.00 KB | |
| locale.nls | Safe | 0x00290000 | 260.00 KB | |
| Secur32.dll | Safe | 0x77FE0000 | 68.00 KB | Security Support P |
| comctl32.dll | Safe | 0x773D0000 | 1.01 MB | User Experience C |
| USER32.dll | Safe | 0x7E410000 | 580.00 KB | Windows XP USER |
| comctl32.dll | Safe | 0x5D090000 | 616.00 KB | Common Controls I |
| unicode.nls | Safe | 0x00270000 | 88.00 KB | |
| Apphelp.dll | Safe | 0x77B40000 | 136.00 KB | Application Compa |
| ntdll.dll | Safe | 0x7C900000 | 700.00 KB | NT Layer DLL |
| MSVCR90.dll | Safe | 0x78520000 | 652.00 KB | Microsoft® C Runt |

**Tip**: The columns displayed in Handles interface can be configured to display the details as required. Refer to **Column Selection** > **Module** for more details.

- **Hide Safe** – Removes DLL modules identified as safe by KillSwitch and displays only unknown and unsafe modules.

### Handling the Modules

Double clicking on a Module name opens the Properties dialog of the module.



RPCRT4.dll Properties

Description: Remote Procedure Call Runtime

Company: Microsoft Corporation

Version: 5.1.2600.5512 (xpsp.080413-2108)

Signer: Microsoft Windows Component Publisher

Image File Name: C:\WINDOWS\system32\RPCRT4.dll

Process: swriter.exe(340)

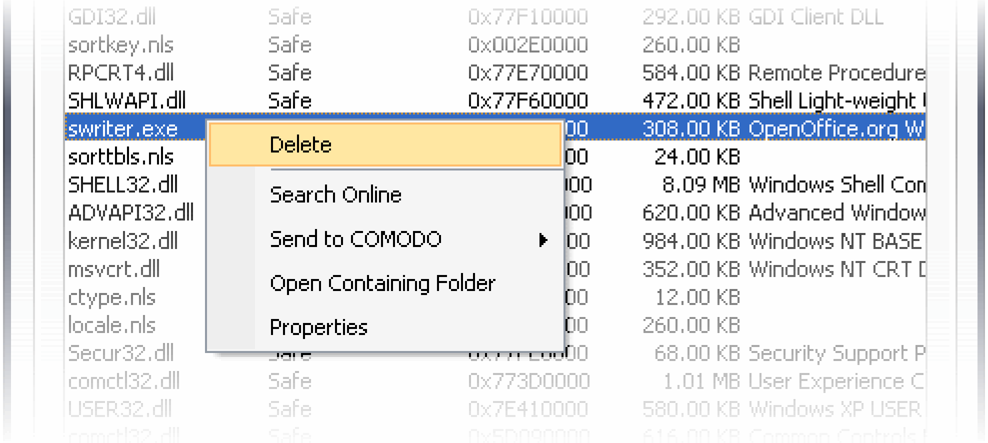
Base Address: 0x77E70000

Mapped Size: 584.00 KB

Mapping Type: DLL

The dialog provides complete details of the DLL module under the three tabs 'Image', 'Rating' and 'Strings' tabs.

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.



| | | | | |
|---|---|---|---|---|
| GDI32.dll | Safe | 0x77F10000 | 292.00 KB | GDI Client DLL |
| sortkey.nls | Safe | 0x002E0000 | 260.00 KB | |
| RPCRT4.dll | Safe | 0x77E70000 | 584.00 KB | Remote Procedure |
| SHLWAPI.dll | Safe | 0x77F60000 | 472.00 KB | Shell Light-weight |
| swriter.exe | | 00 | 308.00 KB | OpenOffice.org W |
| sorttbls.nls | | 00 | 24.00 KB | |
| SHELL32.dll | | 00 | 8.09 MB | Windows Shell Con |
| ADVAPI32.dll | | 00 | 620.00 KB | Advanced Window |
| kernel32.dll | | 00 | 984.00 KB | Windows NT BASE |
| msvcrt.dll | | 00 | 352.00 KB | Windows NT CRT D |
| ctype.nls | | 00 | 12.00 KB | |
| locale.nls | | 00 | 260.00 KB | |
| Secur32.dll | | 00 | 68.00 KB | Security Support P |
| comctl32.dll | Safe | 0x773D0000 | 1.01 MB | User Experience C |
| USER32.dll | Safe | 0x7E410000 | 580.00 KB | Windows XP USER |
| comctl32.dll | Safe | 0x5D090000 | 616.00 KB | Common Controls |

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

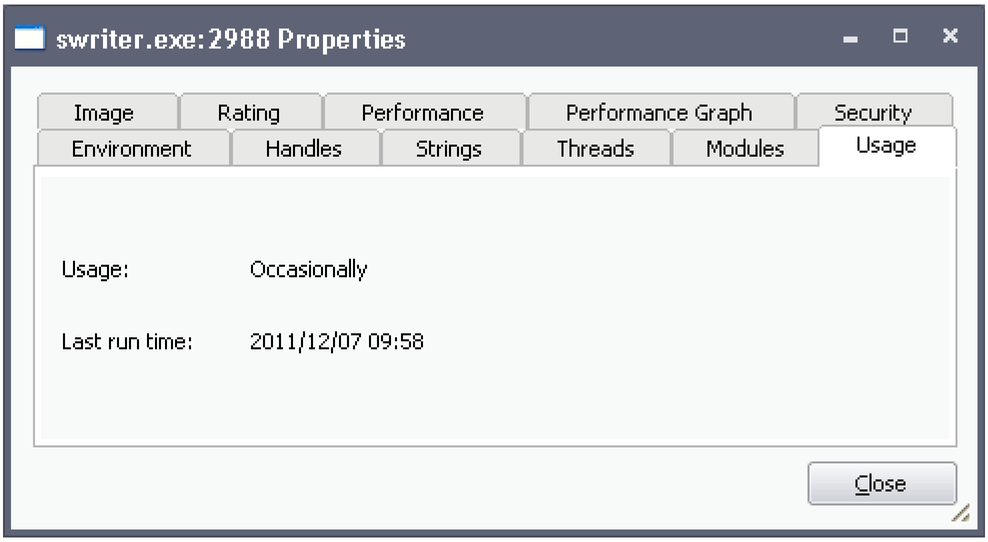
**Warning**: Deleting some critical modules of an application may render the application unusable.

- **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.
- **Send To Comodo** - Submits the module for analysis to Comodo as Suspicious or False Positive. 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.
- **Properties** - Opens the 'Properties' dialog of the module.

**Click here to go back to list of properties**.

### Usage

The 'Usage' tab displays how often the parent application of the process has been used by the user and its previous run time.



Usage: Occasionally

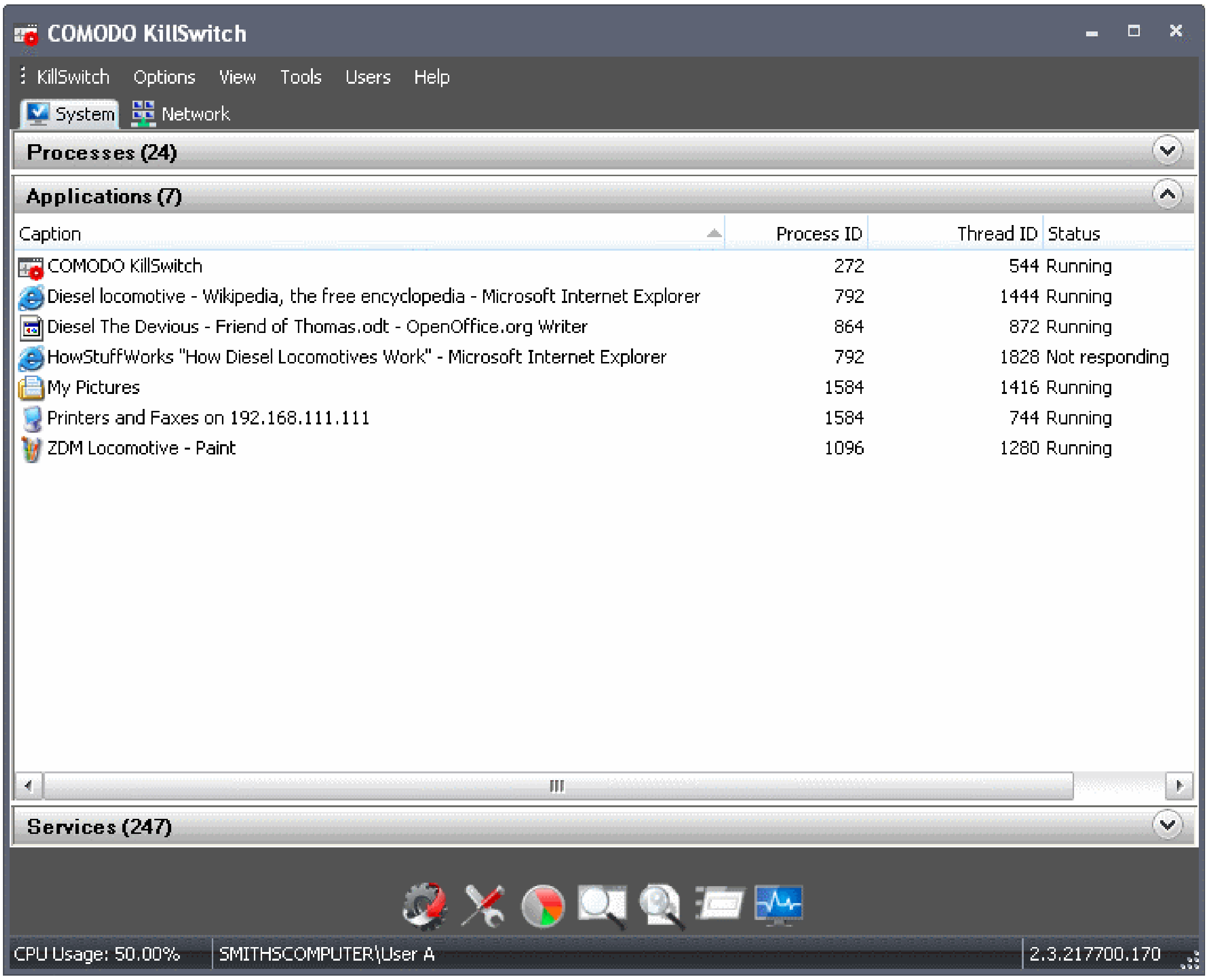
Last run time: 2011/12/07 09:58

**Click here to go back to list of properties**.

## 5.3.2. Applications

The 'Applications' window shows all the applications that are currently running in your system as a table in the main display pane. To open the 'Applications' window from closed state, click the down-arrow at the right of the 'Applications' stripe.

- The processes can be viewed as a list .
- The new applications started and the applications that are closed are highlighted with different colors. The highlighting colors can be set through **Configuring KillSwitch > Configure Highlighting**.
- Right clicking on an application opens a context sensitive menu that enables you to perform various operations like maximizing/minimizing application windows, close an application and access the process invoked by the application. You can even select multiple applications (by holding the 'Ctrl' key while selecting the processes) to execute these actions.



| Caption | Process ID | Thread ID | Status |
|---|---|---|---|
| COMODO KillSwitch | 272 | 544 | Running |
| Diesel locomotive - Wikipedia, the free encyclopedia - Microsoft Internet Explorer | 792 | 1444 | Running |
| Diesel The Devious - Friend of Thomas.odt - OpenOffice.org Writer | 864 | 872 | Running |
| HowStuffWorks "How Diesel Locomotives Work" - Microsoft Internet Explorer | 792 | 1828 | Not responding |
| My Pictures | 1584 | 1416 | Running |
| Printers and Faxes on 192.168.111.111 | 1584 | 744 | Running |
| ZDM Locomotive - Paint | 1096 | 1280 | Running |

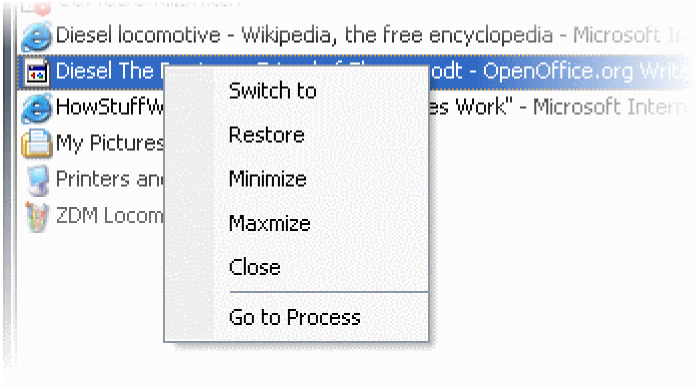
CPU Usage: 50.00% | SMITHSCOMPUTER\User A | 2.3.217700.170

| Applications Table - Descriptions of Columns | |
|---|---|
| **Column** | **Description** |
| Caption | Displays the names of the applications. Clicking on the column header enables sorting the entries in ascending or descending alphabetical order of the application names. |
| Process ID | Displays the Process Identification number of the process invoked by the application. Clicking on the column header enables sorting the entries in ascending or descending order of the PID numbers. |
| Thread ID | Displays the Thread Identification number of the process invoked by the application. Clicking on the column header enables sorting the entries in ascending or descending order of the Thread ID numbers. |
| Status | Displays the current execution status of the application. |

Next: **Handling the Applications**

## 5.3.2.1. Handling the Applications

The 'Applications' window allows you to bring the application window active, minimize/maximize the application window,  close the application and to access the process invoked by the application, by right clicking on the application and selecting the option from the context sensitive menu.

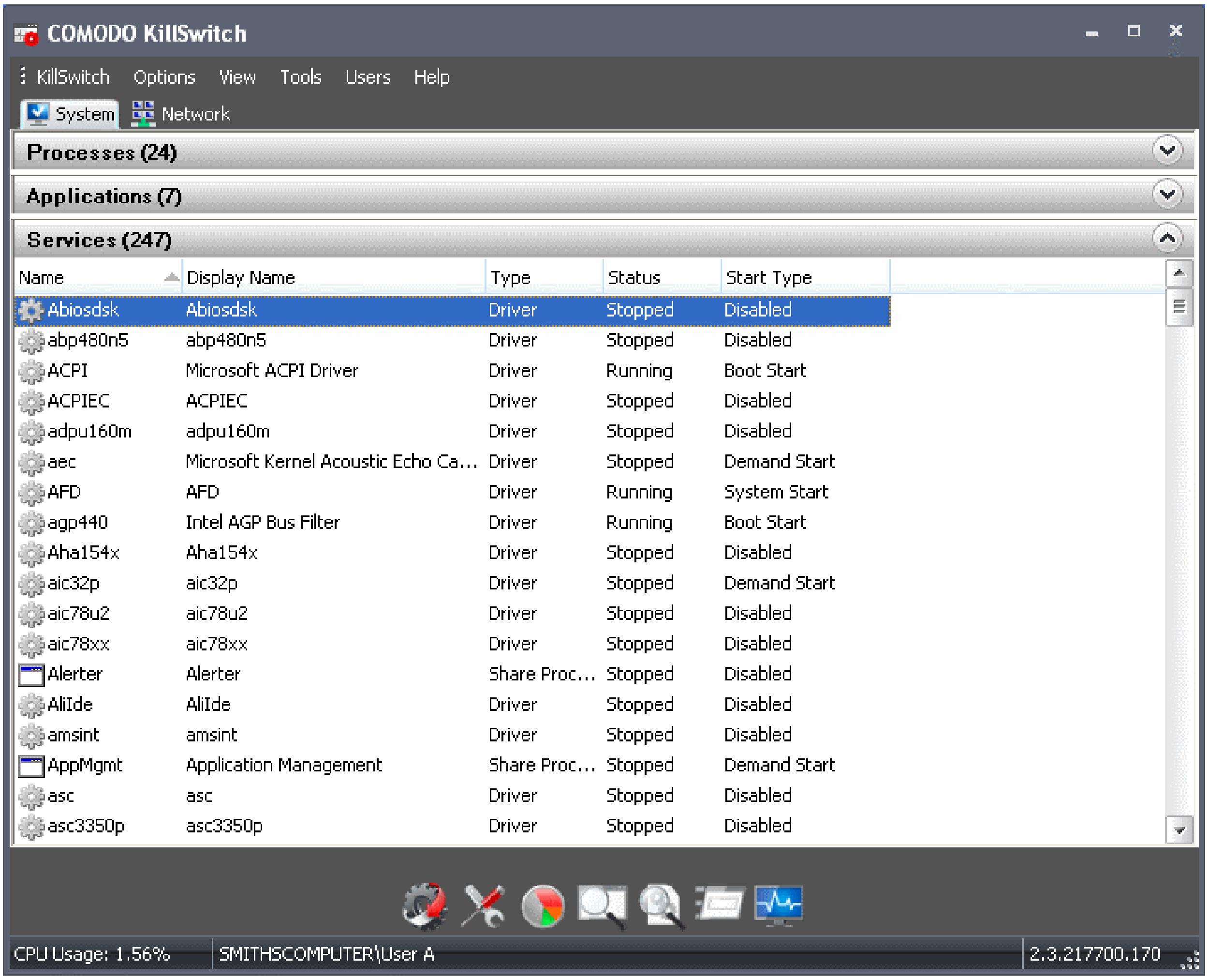

Diesel locomotive - Wikipedia, the free encyclopedia - Microsoft In
Diesel The
odt - OpenOffice.org Writ
HowStuffW
es Work" - Microsoft Intern
My Pictures
Printers an
ZDM Locom
Switch to
Restore
Minimize
Maxmize
Close
Go to Process

- **Switch to** - Brings the application active, minimizing the KillSwitch window.
- **Restore** - Restores the minimized application window from the Windows task bar to its last state.
- **Minimize** - Minimizes the application window to the Windows task bar.
- **Maximize** - Maximizes the application window.
- **Close** - Exits the application.
- **Go to Process** - Opens the 'Process' window with the process invoked by the application highlighted. This is useful when you want to terminate or suspend the process associated with the application. Refer to **Stopping, Starting and Handling Processes** for more details.

## 5.3.3. Services

The Services window is displayed open by default and it shows 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. To open the Services window from closed state, click the down-arrow at the right of the 'Services' stripe.

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



| Name | Display Name | Type | Status | Start Type |
|---|---|---|---|---|
| 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 Ca... | Driver | Stopped | Demand Start |
| AFD | AFD | Driver | Running | System Start |
| agp440 | Intel AGP Bus Filter | Driver | Running | Boot Start |
| Aha154x | Aha154x | Driver | Stopped | Disabled |
| aic32p | aic32p | Driver | Stopped | Demand Start |
| aic78u2 | aic78u2 | Driver | Stopped | Disabled |
| aic78xx | aic78xx | Driver | Stopped | Disabled |
| Alerter | Alerter | Share Proc... | Stopped | Disabled |
| AliIde | AliIde | Driver | Stopped | Disabled |
| amsint | amsint | Driver | Stopped | Disabled |
| AppMgmt | Application Management | Share Proc... | Stopped | Demand Start |
| asc | asc | Driver | Stopped | Disabled |
| asc3350p | asc3350p | Driver | Stopped | Disabled |

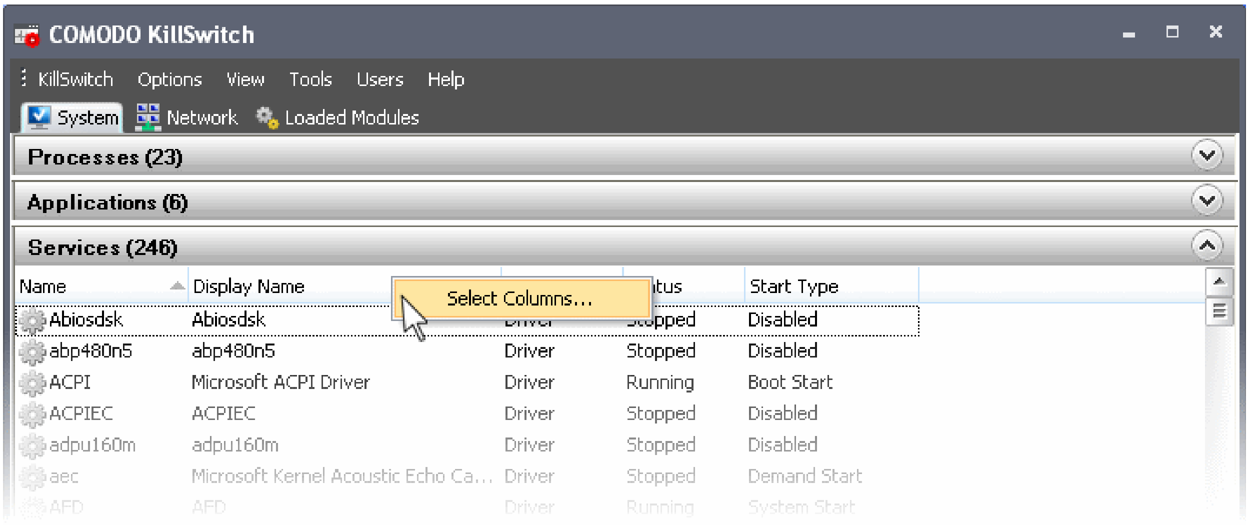
The table below describes the columns that are displayed by default. You can add or remove the columns as per your requirement. Refer to **Column Selection** for more detailed explanation on this.

| Services Table - Descriptions of Columns | |
|---|---|
| **Column** | **Description** |
| Name | Displays the name of the Service. Clicking on the column header sorts the entries in ascending or descending alphabetical order of the names. |
| Display Name | Shows the name by which the service is indicated in the Windows System Configuration Utility. Clicking on the column header sorts the entries in ascending or descending alphabetical order of the display names. |
| Type | Displays the type of the service, viz. shared processes (in svchost.exe instances), Own 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. |

## Column Selection

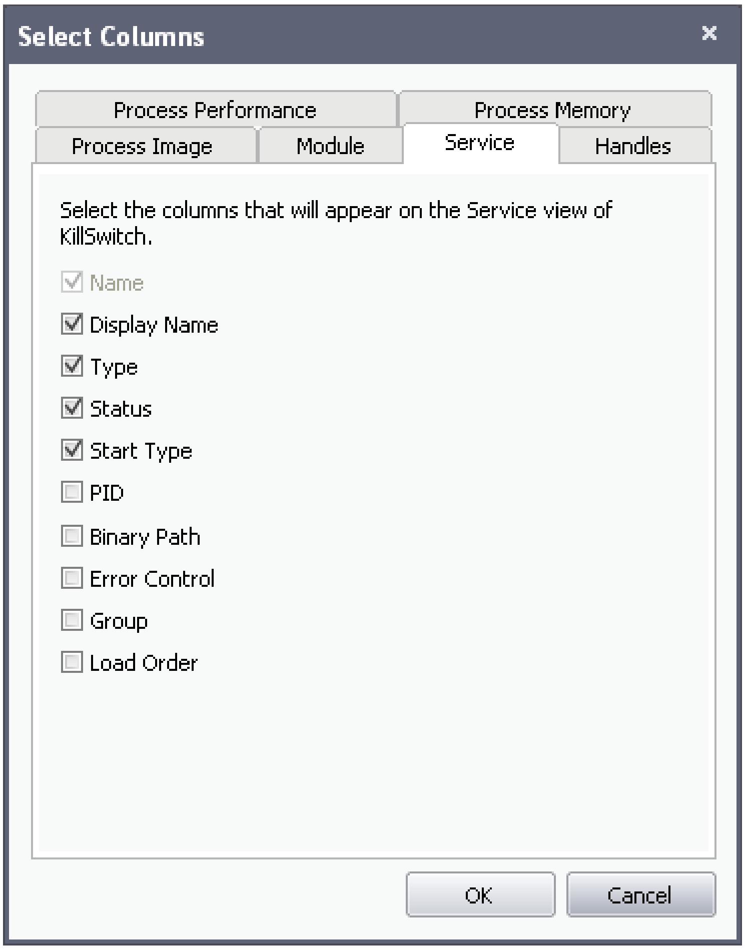
The Services window displays the details on each process under five columns. If you are an advanced user and wish to view more details on each service, you can configure the columns by adding or removing them.

To add or remove columns in Services window, right click on the table header and select 'Select Columns' from the context sensitive menu.



| Name | Display Name |  | tus | Start Type |
|---|---|---|---|---|
| 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 Ca... | Driver | Stopped | Demand Start |
| AFD | AFD | Driver | Running | System Start |

The 'Select Columns' dialog will be displayed with the 'Services' tab opened.



Select the columns that will appear on the Service view of KillSwitch.

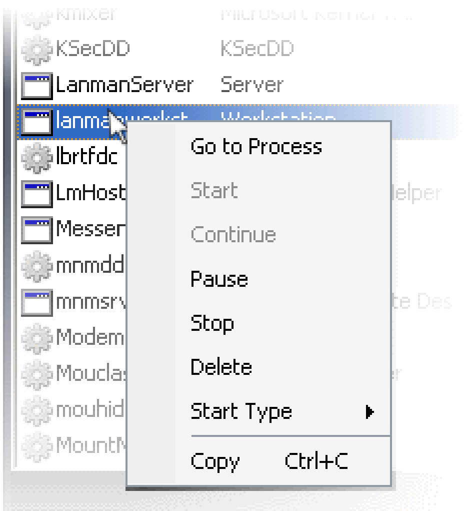
☑ Name
☑ Display Name
☑ Type
☑ Status
☑ Start Type
□ PID
□ Binary Path
□ Error Control
□ Group
□ Load Order

- Select the columns to be displayed by selecting the respective checkboxes
- Click OK for your configuration to take effect.

Next: Stopping, Starting and Deleting the Services

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

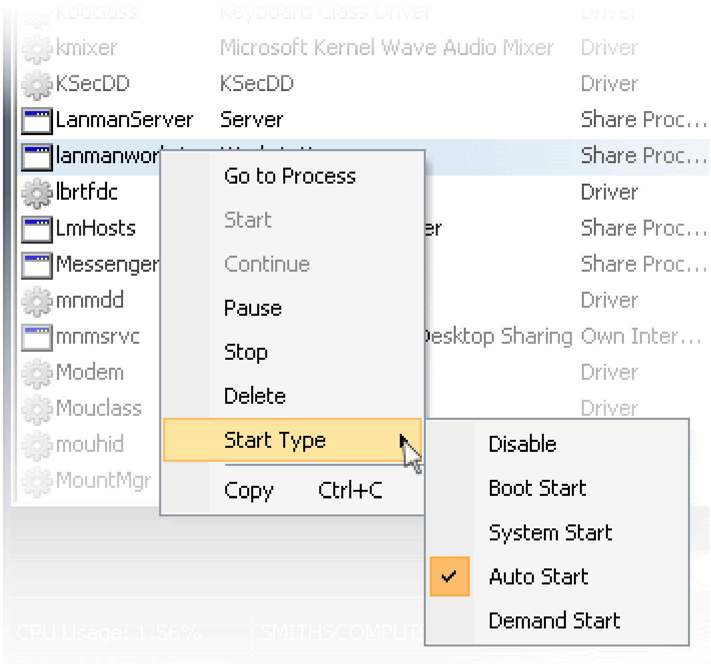
The 'Services' window you to start, stop and delete the services, by right clicking on the service and selecting the option from the context sensitive menu.



- **Go to Process** - Switches the display to the 'Processes' window and highlights the process associated with the service. This is useful when you want to terminate or suspend the process associated with the service. Refer to **Stopping, Starting and Handling Processes** for more details.
- **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.

- **Start Type** - Enables you to define when and how a particular service is to be started. Hovering the mouse cursor over Start Type will open a sub-menu with the options:



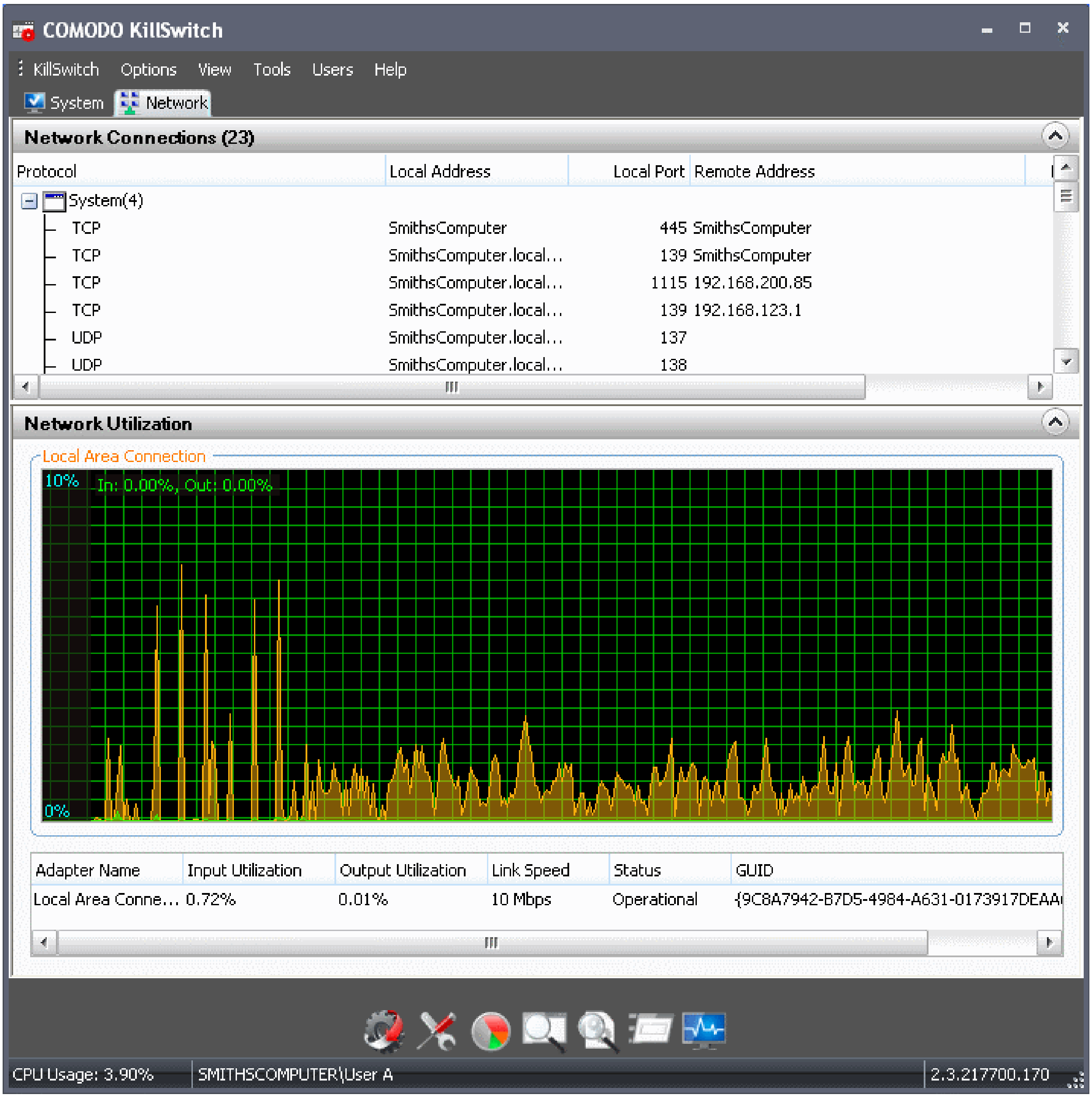
Hovering the mouse cursor over Start Type will open a sub-menu with the options:

- **Disable** – The service will be disabled from running.
- **Boot Start** – The service will be loaded by the boot loader and will started when the system is booted.
- **System Start** - The service will be started during kernel initialization automatically.
- **Auto Start** - The service will be started automatically upon each restart of the computer and will run even if the user is not logged-in.
- **Demand Start** - The service will be started only on demand by an application.

- **Copy** - Copies the row of the selected service(s) from the list of services into your clipboard.

## 5.4. Viewing and Handling Network Connections and Usage

The main display pane of the interface displays all the network connections that are currently running in your system as a table and a graphical representation of your network utilization, on selecting the 'Network' tab from the tab structure. The Network Connections and the Network Utilization are displayed in their respective collapsible windows. Right-clicking on each entry in the Network Connection opens context sensitive menu that enables you to access the process associated with the connection and to close the connection.



| Protocol | Local Address | Local Port | Remote Address |
|---|---|---|---|
| System(4) | | | |
| TCP | SmithsComputer | 445 | SmithsComputer |
| TCP | SmithsComputer.local... | 139 | SmithsComputer |
| TCP | SmithsComputer.local... | 1115 | 192.168.200.85 |
| TCP | SmithsComputer.local... | 139 | 192.168.123.1 |
| UDP | SmithsComputer.local... | 137 | |
| UDP | SmithsComputer.local... | 138 | |

| Adapter Name | Input Utilization | Output Utilization | Link Speed | Status | GUID |
|---|---|---|---|---|---|
| Local Area Conne... | 0.72% | 0.01% | 10 Mbps | Operational | {9C8A7942-B7D5-4984-A631-0173917DEAA |

CPU Usage: 3.90% | SMITHSCOMPUTER\User A | 2.3.217700.170

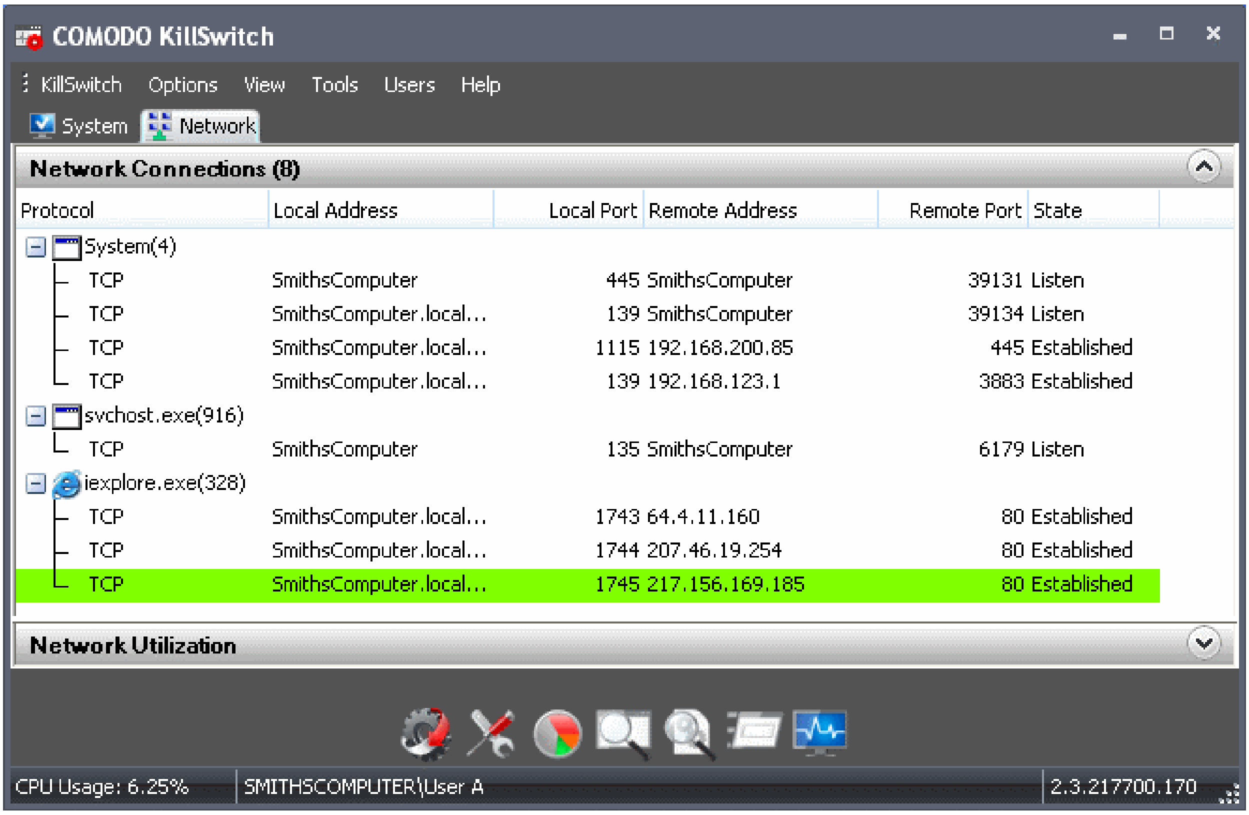
Click the links below for detailed explanations on the windows displayed under the 'Network' tab.

- **Network Connections**;
- **Network Utilization**.

## 5.4.1. Network Connections

The 'Network Connections' window is displayed open by default and it shows all the network connections that are currently running in your system as a table in the main display pane. It also allows you to inspect and close a connection from the right click options. To open the 'Network Connections' window from closed state, click the down-arrow at the right of the 'Network Connections' stripe.

- The new connections that are started and the connections that are stopped are highlighted with different colors. The highlighting colors can be set through **Options > Configure Highlighting**.
- Right clicking on a connection opens a context sensitive menu that enables you to view the process associated with the connection, and close the connection.



| Protocol | Local Address | Local Port | Remote Address | Remote Port | State |
|---|---|---|---|---|---|
| System(4) | | | | | |
| TCP | SmithsComputer | 445 | SmithsComputer | 39131 | Listen |
| TCP | SmithsComputer.local... | 139 | SmithsComputer | 39134 | Listen |
| TCP | SmithsComputer.local... | 1115 | 192.168.200.85 | 445 | Established |
| TCP | SmithsComputer.local... | 139 | 192.168.123.1 | 3883 | Established |
| svchost.exe(916) | | | | | |
| TCP | SmithsComputer | 135 | SmithsComputer | 6179 | Listen |
| iexplore.exe(328) | | | | | |
| TCP | SmithsComputer.local... | 1743 | 64.4.11.160 | 80 | Established |
| TCP | SmithsComputer.local... | 1744 | 207.46.19.254 | 80 | Established |
| TCP | SmithsComputer.local... | 1745 | 217.156.169.185 | 80 | Established |

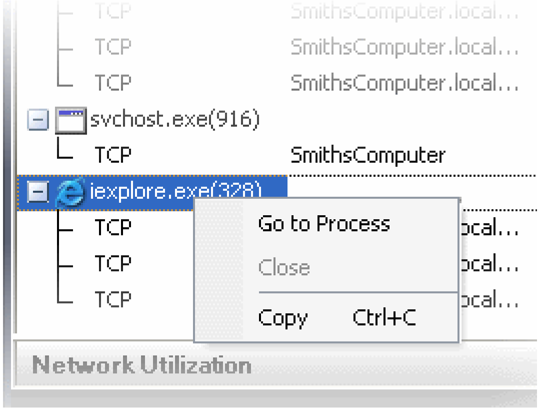
CPU Usage: 6.25% SMITHSCOMPUTER\User A 2.3.217700.170

| Network Connections Table - Descriptions of Columns | |
|---|---|
| **Column** | **Description** |
| Protocol | Shows the connection protocol. Clicking on the column header sorts the entries in based on the protocols. |
| 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.<br>**Note**: The host names are displayed only if the option '**Resolve addresses for Network Address**' is enabled under '**Options**' menu. 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.<br>**Note**: The host names are displayed only if the option '**Resolve addresses for Network Address**' is enabled under '**Options**' menu. 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. |
| State | Shows the status of the connection. Clicking on the column header sorts the entries in based on the status of each connection. |

Next: **Inspecting and Closing Network Connections**

### 5.4.1.1. Inspecting and Closing Network Connections

The 'Network Connections' window 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.



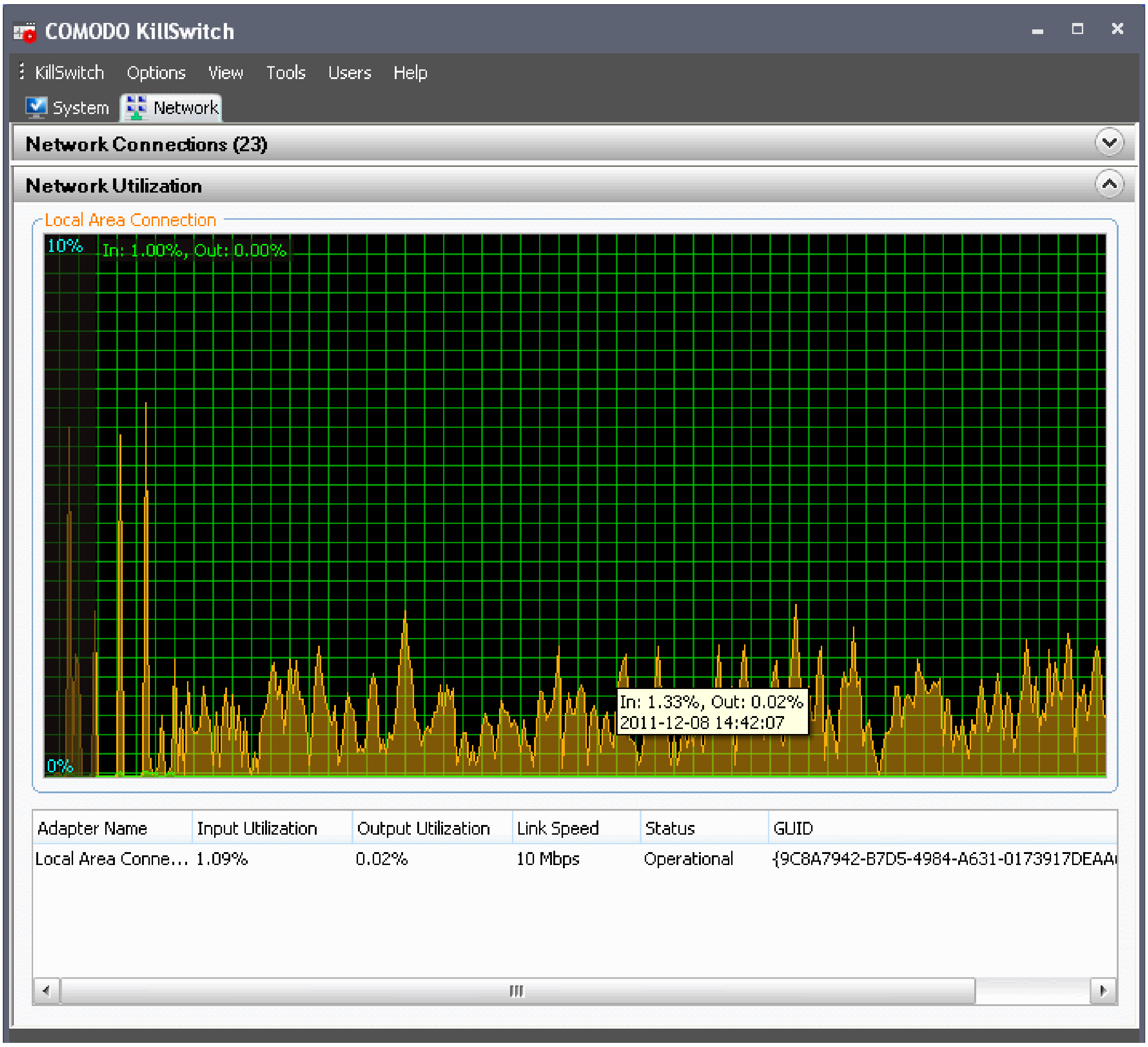
- **Go to Process** - Switches the display to the **Processes** window and highlights the process associated with the connection. This is useful when you want to terminate or suspend the process associated with the connection.
- **Close** - Closes the network Connection.
- **Copy** - Copies the row of the selected connection from the list of connections into your clipboard.

## 5.4.2. Network Utilization

The Network Utilization window provides a graphical overview of how much network traffic is being used over time by the network adapters running on your computer.  Placing the mouse cursor over the graph displays a tooltip with further details.

The window also displays the details of the network adapter beneath the graph.

To open the 'Network Utilization' window, click the down-arrow at the right of the 'Network Utilization' stripe.

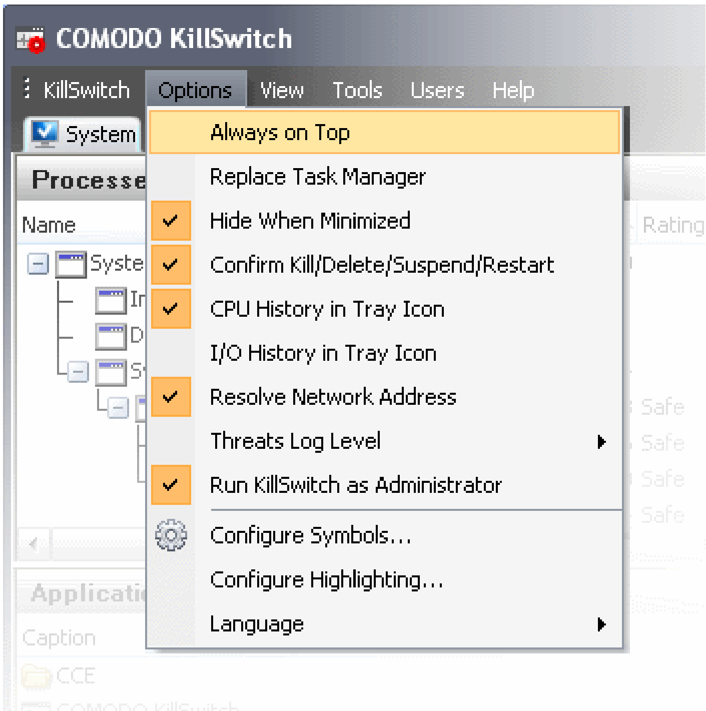


| Adapter Name | Input Utilization | Output Utilization | Link Speed | Status | GUID |
|---|---|---|---|---|---|
| Local Area Conne... | 1.09% | 0.02% | 10 Mbps | Operational | {9C8A7942-B7D5-4984-A631-0173917DEAA |

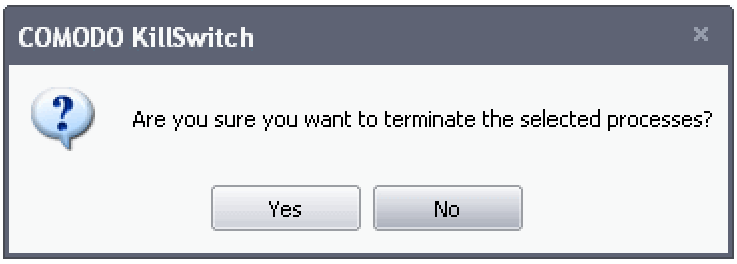
| Network Utilization Table - Descriptions of Columns | |
|---|---|
| **Column** | **Description** |
| Adapter Name | Shows the name of the network adapter. |
| Input Utilization | Shows the incoming traffic utilization in percentage. |
| Output Utilization | Shows the outgoing traffic utilization in percentage. |
| Link Speed | Shows the connection speed of you computer with the network. |
| Status | Displays the traffic flow operation status through the network connection. |
| GUID | Shows 32 character Globally Unique Identifier of the connection. |

## 5.5. Configuring KillSwitch

The 'Options' menu in the file menu bar enables granular configuration of the overall behavior of the KillSwitch application.

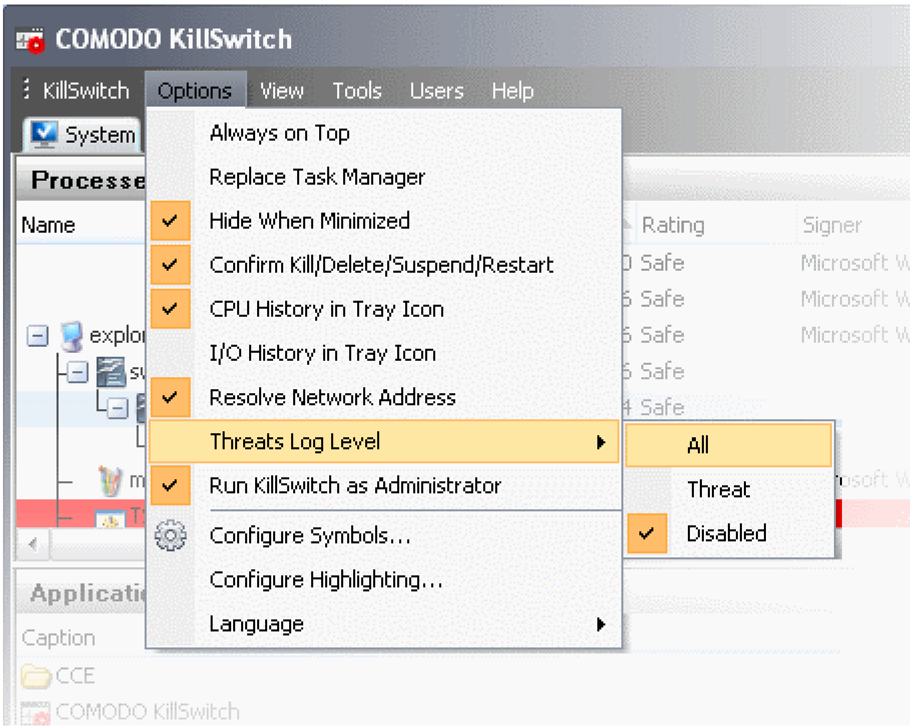


- **Always on Top** - If selected, KillSwitch application window is always maintained on top of all the other application windows on your computer display.
- **Replace Task Manager** - If selected, any attempt to start Windows Task Manager, (e.g. press Ctrl + Alt + Del > Click 'Task Manager' or right-click 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 deselect this option.
- **Hide When Minimized**- If selected, KillSwitch will automatically hide itself when it is minimized. You can double-click on the system tray icon to reopen the application.
- **Confirm Kill/Delete/Suspend/Restart** – Makes KillSwitch to display a confirmation dialog whenever you attempt to terminate, delete, suspend or restart a process, application, service or a network connection. An example is shown below.


COMODO KillSwitch

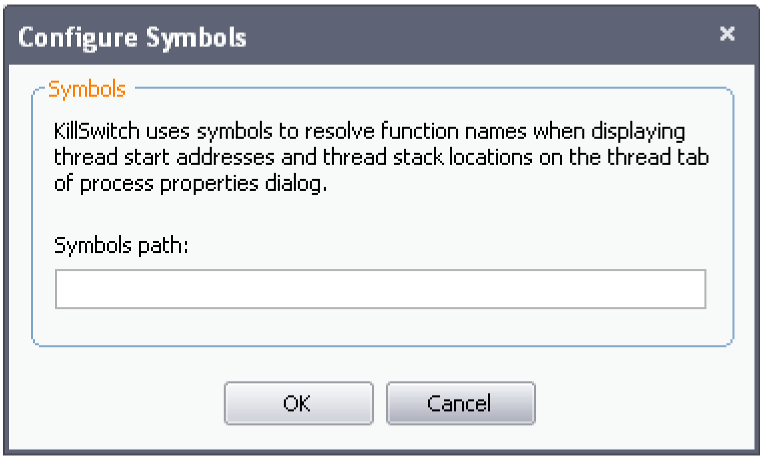
Are you sure you want to terminate the selected processes?

- **CPU History in Tray Icon** - KillSwitch displays a system tray icon at the bottom right corner of the screen. The icon enables to open or close the application, shutdown your system and so on. On selecting this option, the icon will display a dynamic graphical representation of the CPU usage history in your computer. Refer to the section 'The System Tray Icon' for more details.
- **I/O History in Tray Icon** – Makes the system tray icon to display a dynamic graphical representation of the input/output activities of your computer.
- **Resolve Network Address** - If enabled, KillSwitch retrieves the host names for all the network connections for display in the 'Local Address' and 'Remote Address' columns in the '**Network Connections**' window. If not enabled, only the IP addresses of the local host and the remote host will be displayed.
- **Threats Log Level** - Allows you to select the option for creating log reports. Hovering the mouse over 'Threats Log Level' displays a sub-menu with the three options:



- **Disable** - Instructs KillSwitch to not to generate log reports.
- **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.
- To view the logs, click Tools > Browse Logs...

- **Run KillSwitch as Administrator** - Irrespective of the privileges of the currently logged-in user account, all the operations of KillSwitch that require administrative privileges will be executed.
- **Configure Symbols** – KillSwitch uses the symbols from program database files to resolve the names of functions from running processes to find the start addresses and stack locations of threads, for displaying under the Threads tab of the Process – Properties dialog. If you have relocated the pdb files, you can specify the new path of the file through this option.



KillSwitch uses symbols to resolve function names when displaying thread start addresses and thread stack locations on the thread tab of process properties dialog.

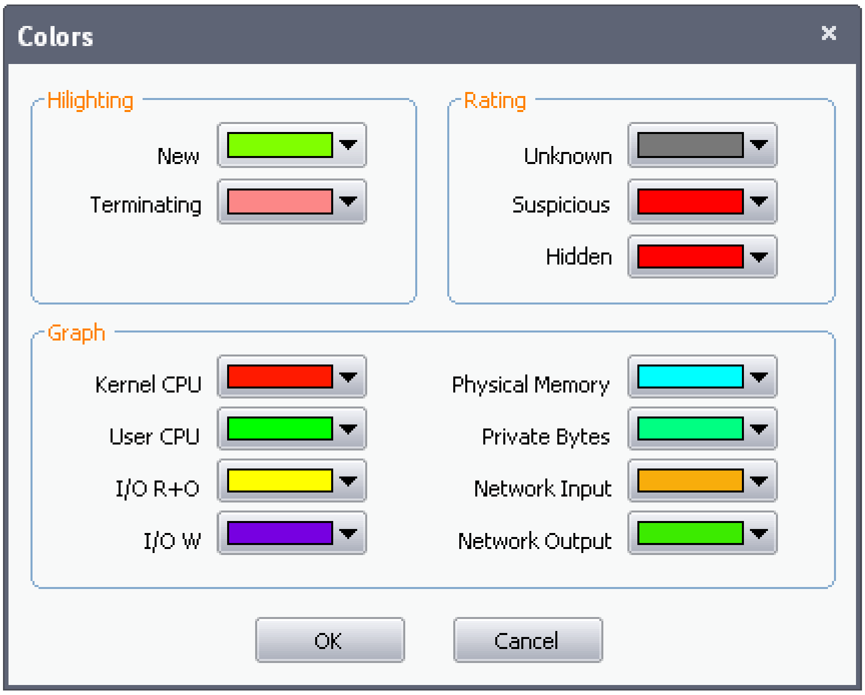
Symbols path:

- **Configure Highlighting** – KillSwitch highlights:
  - the processes that are started, stopped, identified as suspicious or hidden processes in the 'Process' window;
  - the applications that are started or closed in the 'Applications' window;
  - the services that are started and stopped in the 'Services' window;
  - the network connections that are started and stopped in the Network Connection window.

in different colors. The 'Configure Highlighting' option enables you to select the colors that are to be used for highlighting for different events. Also the option enables you to change the look and feel of the graphs such as

Performance Graphs in the Graphical Reports pane at the right hand side of the interface, Network Utilization graph under the Network tab of the main interface, Performance Graphs in the Process Properties dialog.

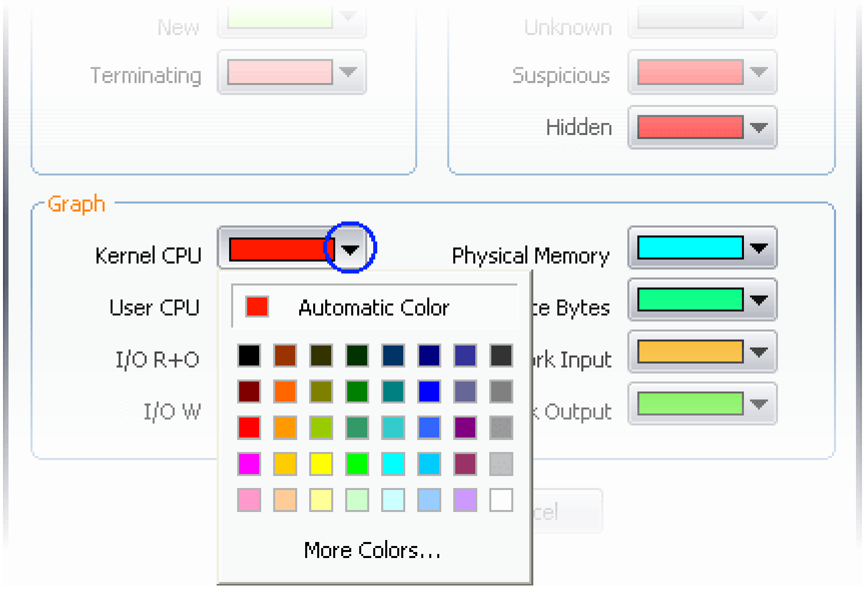
Clicking on the Configure Highlighting option will open a 'Colors' dialog.



- **Highlighting** – You can set the colors for highlighting the starting and terminating processes, services applications and network connections in the KillSwich interface from the 'Highlighting' area in the colors dialog.
- **Rating** – You can set the colors for highlighting the processes and services identified as suspicious, hidden or unknown from the 'Rating' area in the colors dialog.
- **Graph** – The Graphs area allows you to select the colors of the line in the graphs indicating the history/usage information on:
  - CPU usage by Kernel
  - CPU usage by User initiated applications and processes
  - I/O Read Only
  - I/O Write
  - Physical Memory Usage
  - Private Bytes
  - Network Input
  - Network Output

**To change the color of a desired line**

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



2. Choose the color for highlighting or the graph line. You can do this by two ways:
   - Directly choose the color from the palate; or
   - Click on 'More Colors...' to add a custom color to the palate and select it.
3. Click OK.

The highlighting and/or graph lines will be displayed with the colors you have chosen.

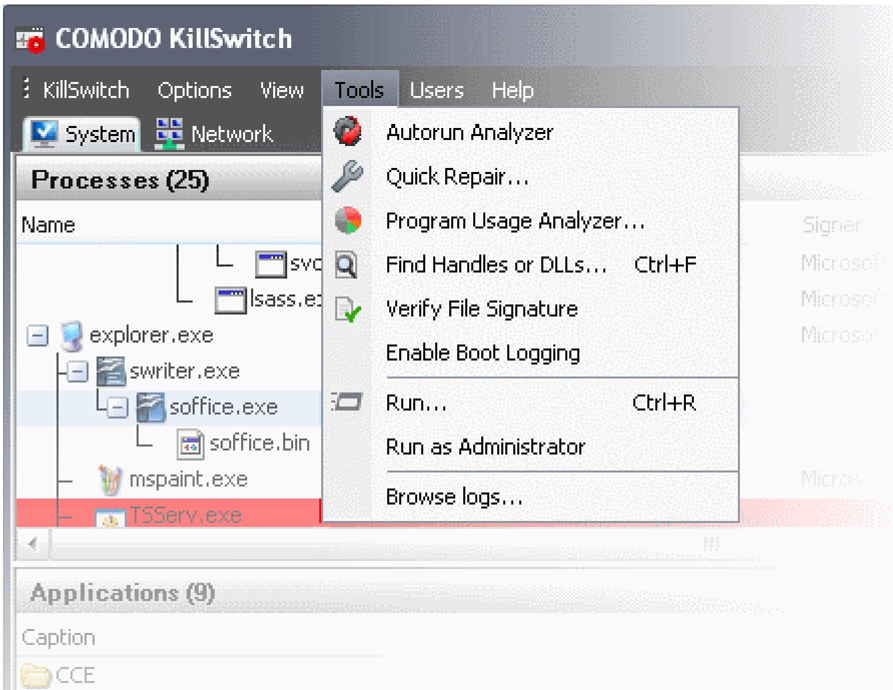
- **Language** - KillSwitch is available in several language. Hovering the mouse cursor over 'Language' in the 'Options' menu displays the list of languages. You can select the language for application from the list.

# 5.6. KillSwitch Tools

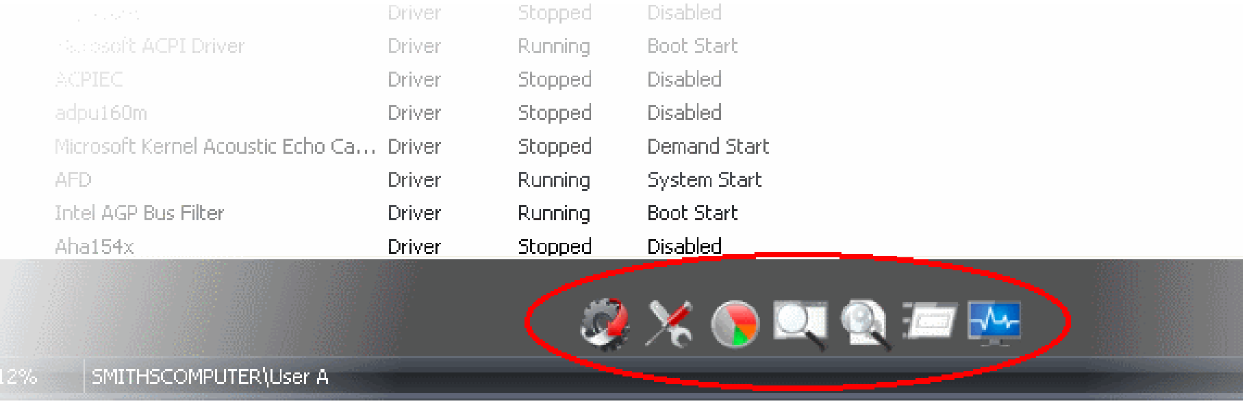
KillSwitch contains a set of utilities that help you in carrying out various activities like handling processes, objects and dll files collectively, troubleshooting and repairing important Windows settings, checking installed programs and their usages, verifying authenticity of installed programs and many more.

The utilities can be accesses from the Tools menu in the file menu bar and the shortcut in the tool bar beneath the main display pane.

- To access the utilities in the Tools menu, click on the Tool in the file menu bar.



- To access the utilities from the Tool bar, click on the respective icon in the tool bar.



| | | | |
|---|---|---|---|
| [illegible] | Driver | Stopped | Disabled |
| Microsoft ACPI Driver | Driver | Running | Boot Start |
| ACPIEC | Driver | Stopped | Disabled |
| adpu160m | Driver | Stopped | Disabled |
| Microsoft Kernel Acoustic Echo Ca... | Driver | Stopped | Demand Start |
| AFD | Driver | Running | System Start |
| Intel AGP Bus Filter | Driver | Running | Boot Start |
| Aha154x | Driver | Stopped | Disabled |

| Icon | Description |
|---|---|
| | Opens **Autorun Analyzer** utility to view and handle services and programs that were loaded when your system booted-up. |
| | Opens the 'Quick Repair' interface  to troubleshoot and and repair important Windows settings and features. Refer **Repairing Windows Settings and Features** for more details. |
| | Open the 'Program Usage Analyzer' window that displays a summary of usage of all the programs installed in your computer by different users. Refer to **Analyzing Program Usage** for more details. |
| | Starts the Find Window utility that allows the user to find process related to active application window or window components. Refer to **Finding Process of the Active Window** for more details. |
| | Opens a 'search' 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 Windows 'Run' dialog for executing command line interface programs with default limited user privileges. Refer to **Running Programs from Command Line Interface** 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. |

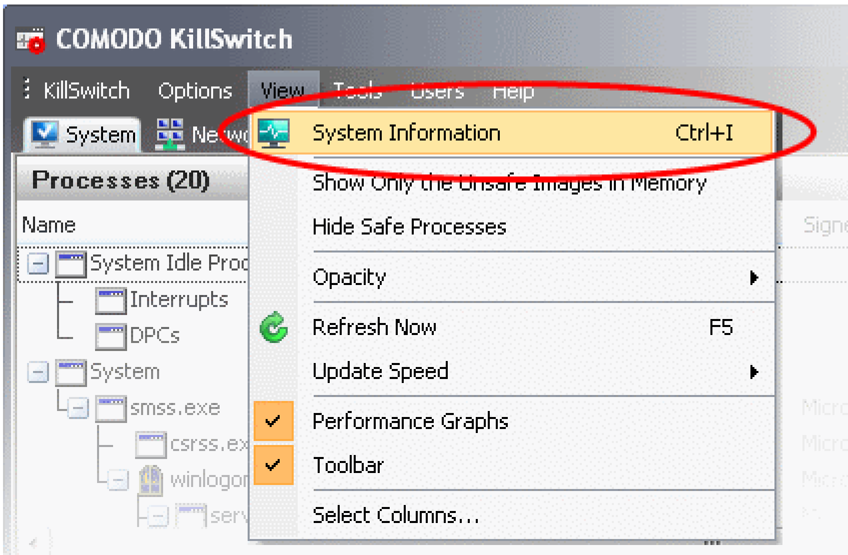
Click the links below for detailed explanations on KillSwitch Utilities:

- **Viewing System Information;**
- **Repairing Windows Settings and Features**;
- **Analyzing Program Usage;**
- **Searching for Handles or DLLs;**
- **Verifying authenticity of Applications;**
- **Enable Boot Logging;**
- **Running a Command Line Interface program;**
- **Running a Command Line Interface program as Administrator;**
- **Browsing KillSwitch Logs.**

## 5.6.1. Viewing System Information

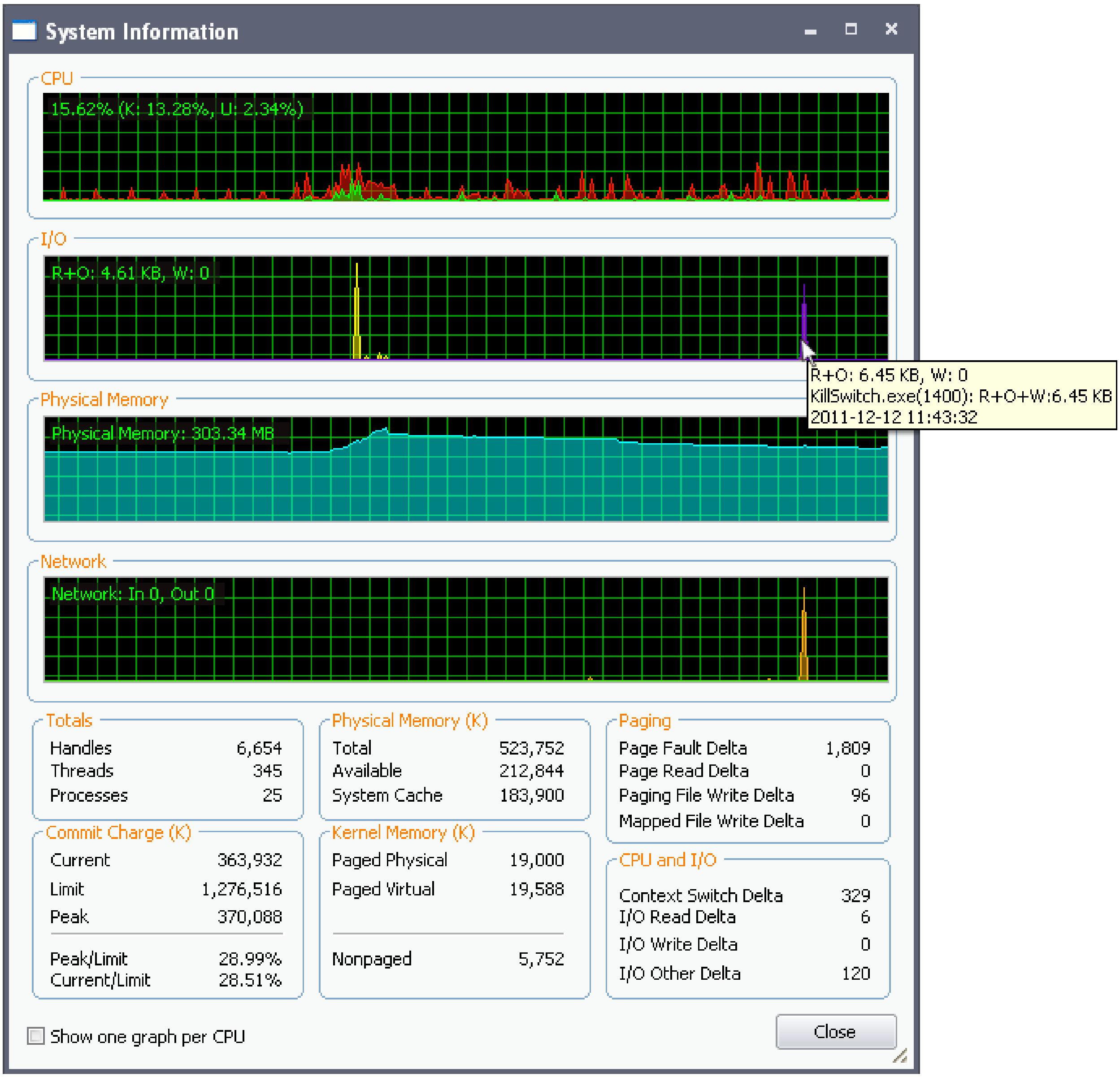
The system information pane displays the dynamic graphical representations of your CPU usage, I/O activity and physical memory usage of your system, along with the detailed statistics on current usage of various system resources.

- To view the System Information pane, Click 'View' > 'System Information'.



- Alternatively, click the 'System Information' icon from the tool bar.

The 'System Information' pane will be opened with the current resource usage details of your system.



| Totals | |
|---|---|
| Handles | 6,654 |
| Threads | 345 |
| Processes | 25 |

| Physical Memory (K) | |
|---|---|
| Total | 523,752 |
| Available | 212,844 |
| System Cache | 183,900 |

| Paging | |
|---|---|
| Page Fault Delta | 1,809 |
| Page Read Delta | 0 |
| Paging File Write Delta | 96 |
| Mapped File Write Delta | 0 |

| Commit Charge (K) | |
|---|---|
| Current | 363,932 |
| Limit | 1,276,516 |
| Peak | 370,088 |
| Peak/Limit | 28.99% |
| Current/Limit | 28.51% |

| Kernel Memory (K) | |
|---|---|
| Paged Physical | 19,000 |
| Paged Virtual | 19,588 |
| Nonpaged | 5,752 |

| CPU and I/O | |
|---|---|
| Context Switch Delta | 329 |
| I/O Read Delta | 6 |
| I/O Write Delta | 0 |
| I/O Other Delta | 120 |

## 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.
- **Network** - Shows a dynamic graphical representation of how much network traffic is being used over time by services and applications running on your computer. You can hover your mouse over the graph to view details.

## Statistical Reports

- **Totals** - 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 in KB. 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 in

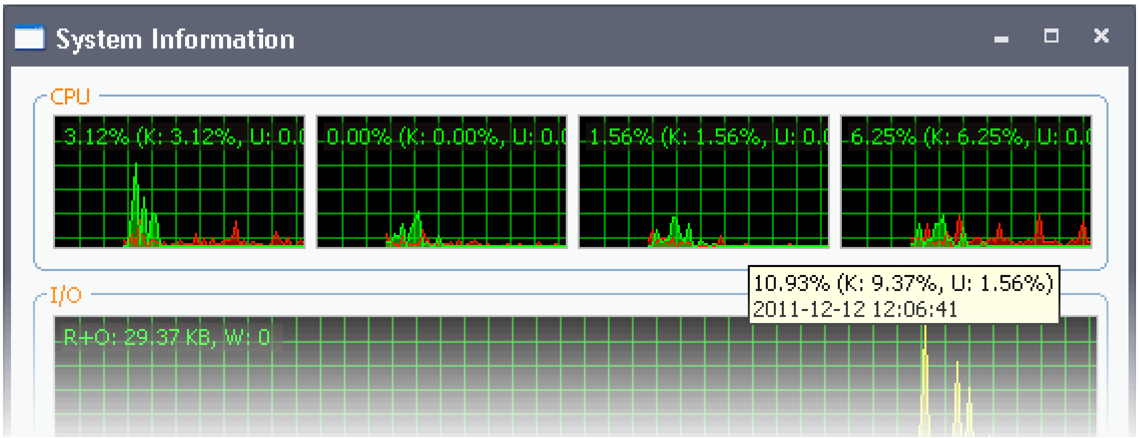
KB.

- Total - Represents the amount of total Physical Memory.
- 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 Memory** - Shows a statistical report on memory used by the operating system kernel and device drivers in KB.
  - Paged Physical - Memory that can be copied to the paging file from physical memory, thereby freeing the physical memory. The physical memory can then be used by the operating system.
  - Paged Virtual - Memory that can be copied to the paging file from virtual memory.
  - Non-paged - Memory that remains resident in physical memory and will not be copied out to the paging file.
- **Paging** - 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.
- **CPU and I/O** - Shows a statistical report on the CPU activities and Input/Out put activities of your computer.

### 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.

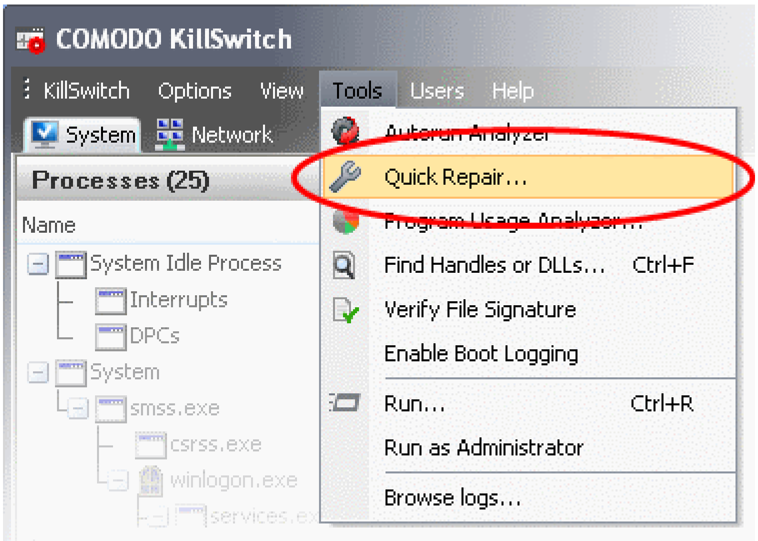


## 5.6.2. Repairing Windows Settings and Features

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.

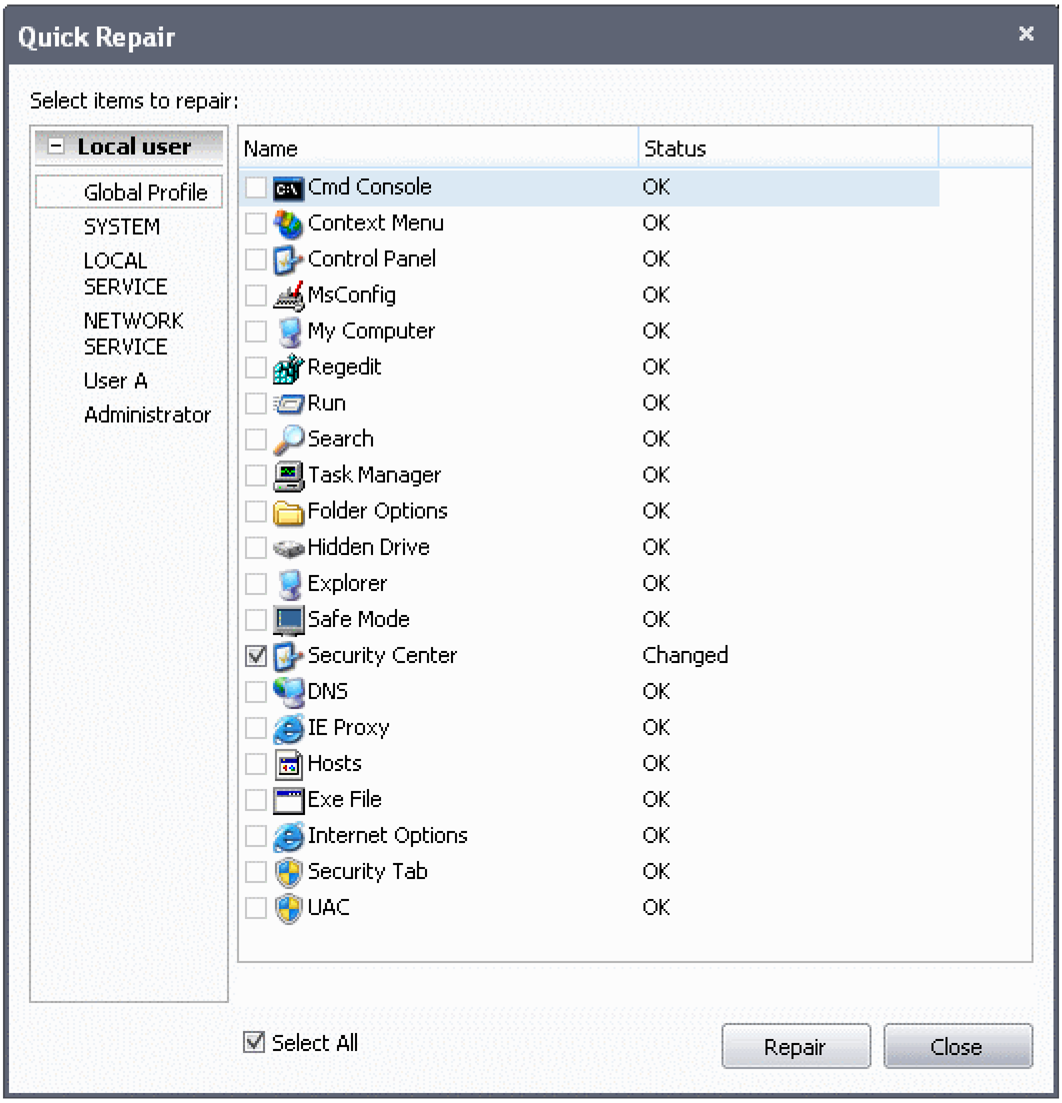
**To check start repairing the Windows settings and features**

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



- Alternatively, click the Quick Repair icon from the Tool bar.

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



| | Name | Status |
|---|---|---|
| □ | Cmd Console | OK |
| □ | Context Menu | OK |
| □ | Control Panel | OK |
| □ | MsConfig | OK |
| □ | My Computer | OK |
| □ | Regedit | OK |
| □ | Run | OK |
| □ | Search | OK |
| □ | Task Manager | OK |
| □ | Folder Options | OK |
| □ | Hidden Drive | OK |
| □ | Explorer | OK |
| □ | Safe Mode | OK |
| ☑ | Security Center | Changed |
| □ | DNS | OK |
| □ | IE Proxy | OK |
| □ | Hosts | OK |
| □ | Exe File | OK |
| □ | Internet Options | OK |
| □ | Security Tab | OK |
| □ | UAC | OK |

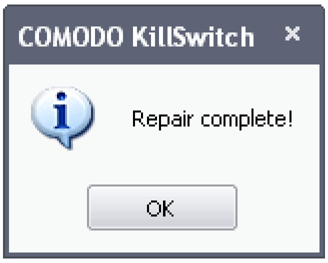
☑ Select All

You can change the profile from the left hand side pane so as to switch the display of the statuses of the features as per the selected administrator's/user's profile.

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

**Note:** The checkboxes will be active only for the items that require fixing. If you want to select all the items that need fixing, check 'Select All'.

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



COMODO KillSwitch

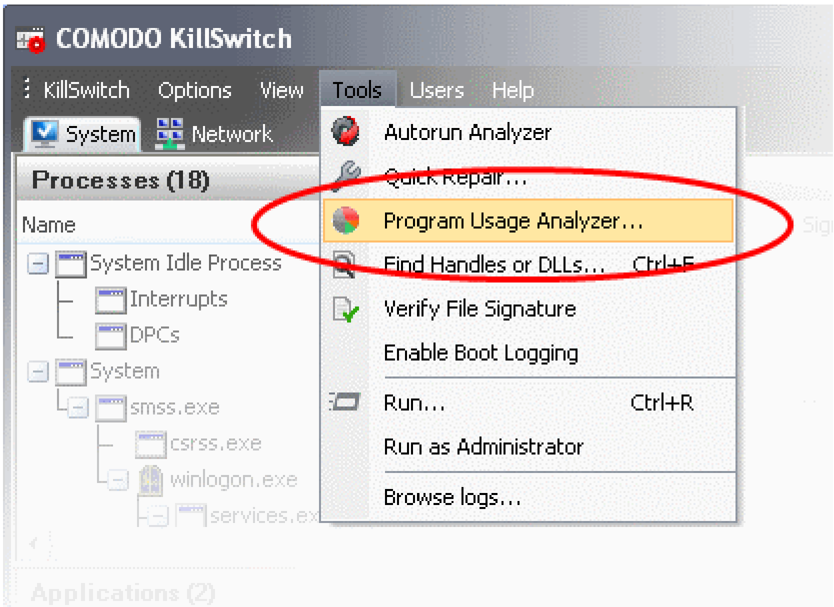
Repair complete!

## 5.6.3. Analyzing Program Usage

The Program Usage Analyzer displays usage details of programs and Windows components installed on your system along with other details such as their last run time. Usage details can be viewed on a per user basis - useful when you want to analyze overall usage when deciding which programs to keep or remove when optimizing your computer.

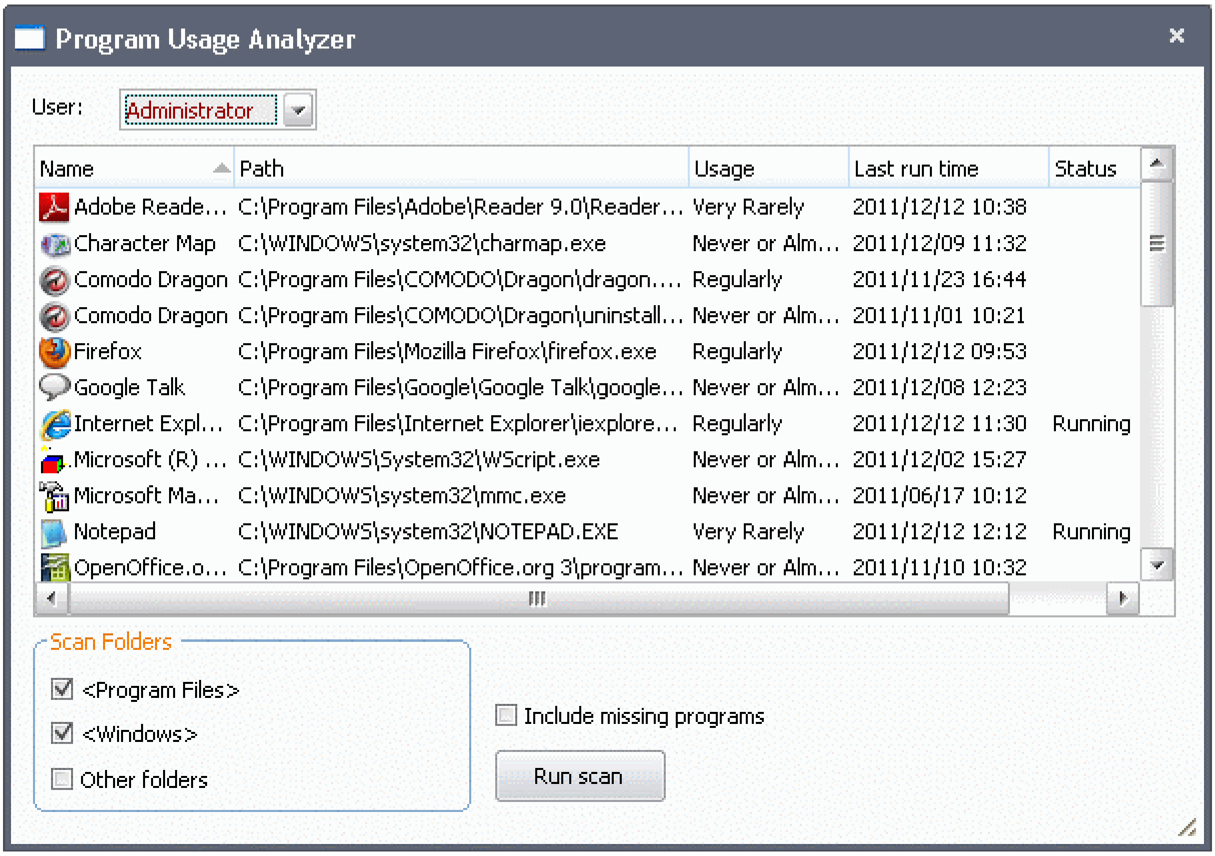
**To view the Program Usage Analyzer pane**

- From the 'Tools' menu, click 'Program Usage Analyzer'.



- Alternatively, click the 'Program Usage Analyzer' icon from the Tool bar.

The Program Usage Analyzer dialog will appear with all the programs as the user profile of the currently logged-in user.



User: Administrator

| Name | Path | Usage | Last run time | Status |
|---|---|---|---|---|
| Adobe Reade… | C:\Program Files\Adobe\Reader 9.0\Reader… | Very Rarely | 2011/12/12 10:38 | |
| Character Map | C:\WINDOWS\system32\charmap.exe | Never or Alm… | 2011/12/09 11:32 | |
| Comodo Dragon | C:\Program Files\COMODO\Dragon\dragon.… | Regularly | 2011/11/23 16:44 | |
| Comodo Dragon | C:\Program Files\COMODO\Dragon\uninstall… | Never or Alm… | 2011/11/01 10:21 | |
| Firefox | C:\Program Files\Mozilla Firefox\firefox.exe | Regularly | 2011/12/12 09:53 | |
| Google Talk | C:\Program Files\Google\Google Talk\google… | Never or Alm… | 2011/12/08 12:23 | |
| Internet Expl… | C:\Program Files\Internet Explorer\iexplore… | Regularly | 2011/12/12 11:30 | Running |
| Microsoft (R) … | C:\WINDOWS\System32\WScript.exe | Never or Alm… | 2011/12/02 15:27 | |
| Microsoft Ma… | C:\WINDOWS\system32\mmc.exe | Never or Alm… | 2011/06/17 10:12 | |
| Notepad | C:\WINDOWS\system32\NOTEPAD.EXE | Very Rarely | 2011/12/12 12:12 | Running |
| OpenOffice.o… | C:\Program Files\OpenOffice.org 3\program… | Never or Alm… | 2011/11/10 10:32 | |

Scan Folders

☑ <Program Files>

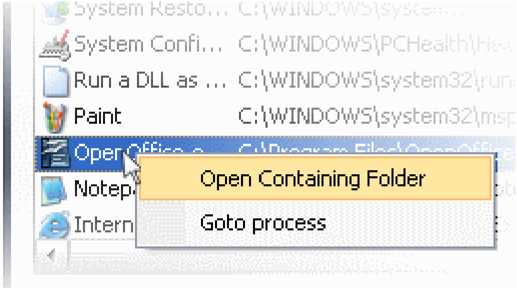
☑ <Windows>

□ Other folders

□ Include missing programs

| Program Usage Analyzer - Descriptions of Columns | |
|---|---|
| **Column** | **Description** |
| Name | Shows the name of the program/application. Clicking the column header sorts the entries in alphabetical order of the names. |
| Path | Shows the installation path of the program/application. |
| Usage | Shows the frequency of usage of the program/application. |
| Last Run Time | Shows the date and time at which the program was executed last time. |
| Status | Shows the current running status of the program/application. |

- To view the usage of the program by other users, select the user profile from the 'User' drop-down.
- To filter the entries based on their installation paths, select the folders for scanning from the 'Scan Folders' area.
- To include programs/Windows components which were uninstalled from your computer,  select 'Include missing programs' and click 'Run Scan'.
- Right clicking on an entry enables you to open the installation folder of the program and to access the process invoked by the program.


System Resto... C:\WINDOWS\system...
System Confi... C:\WINDOWS\PCHealth\He...
Run a DLL as ... C:\WINDOWS\system32\run...
Paint C:\WINDOWS\system32\msp...
Open Office ... C:\Program Files\OpenOffice...
Notep...
Intern...
Open Containing Folder
Goto process

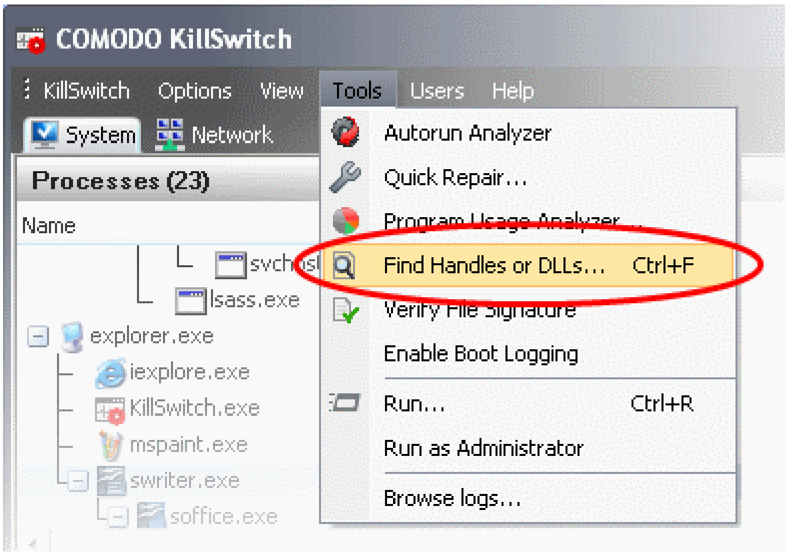
- **Open Containing Folder** - Opens the installation folder of the program in Windows Explorer.
- **Go to Process** - Highlights the process associated with the program in the 'Processes' window. This is useful when you want to terminate or suspend the process associated with the program. Refer to **Stopping, Starting and Handling Processes** for more details. This option will be available only for the programs that are currently running.

## 5.6.4. Searching for Handles or DLLs

The 'Find Handles or DLLs' tool enables you to search for specific handles, DLLs and mapped files of the currently running processes by entering their names.

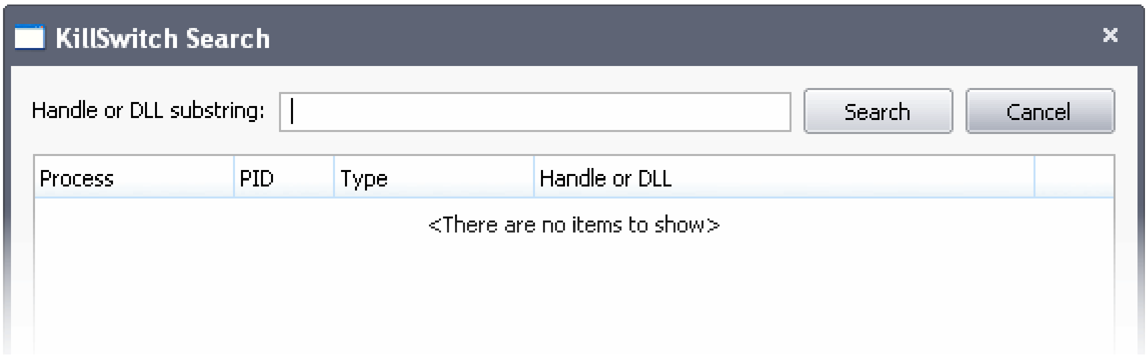
**To search for a specific handles, DLLs and mapped files**

- From the 'Tools' menu, click 'Find Handles or DLLs'.



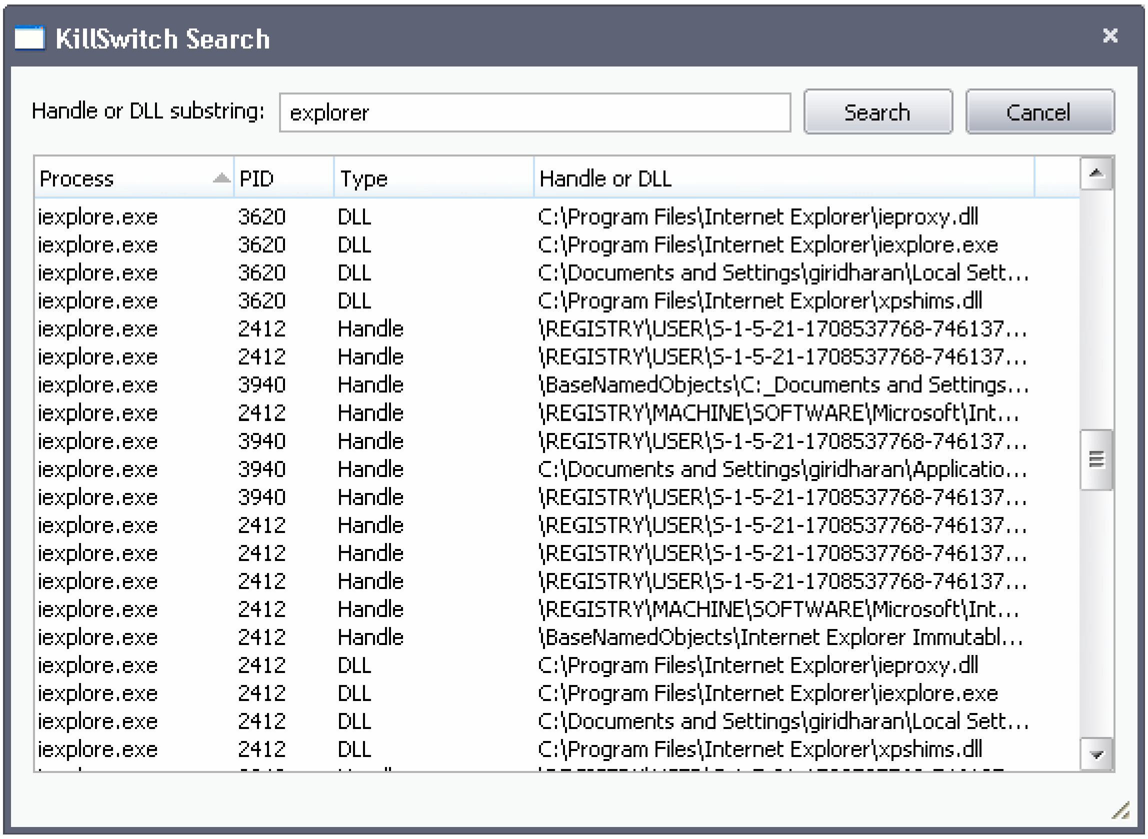
- Alternatively, click the Find Handles or DLLs icon from Tool bar.

The 'Find Handles or DLLs' dialog will open.



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

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



Handle or DLL substring: explorer

| Process | PID | Type | Handle or DLL |
|---|---|---|---|
| iexplore.exe | 3620 | DLL | C:\Program Files\Internet Explorer\ieproxy.dll |
| iexplore.exe | 3620 | DLL | C:\Program Files\Internet Explorer\iexplore.exe |
| iexplore.exe | 3620 | DLL | C:\Documents and Settings\giridharan\Local Sett... |
| iexplore.exe | 3620 | DLL | C:\Program Files\Internet Explorer\xpshims.dll |
| iexplore.exe | 2412 | Handle | \REGISTRY\USER\S-1-5-21-1708537768-746137... |
| iexplore.exe | 2412 | Handle | \REGISTRY\USER\S-1-5-21-1708537768-746137... |
| iexplore.exe | 3940 | Handle | \BaseNamedObjects\C:_Documents and Settings... |
| iexplore.exe | 2412 | Handle | \REGISTRY\MACHINE\SOFTWARE\Microsoft\Int... |
| iexplore.exe | 3940 | Handle | \REGISTRY\USER\S-1-5-21-1708537768-746137... |
| iexplore.exe | 3940 | Handle | C:\Documents and Settings\giridharan\Applicatio... |
| iexplore.exe | 3940 | Handle | \REGISTRY\USER\S-1-5-21-1708537768-746137... |
| iexplore.exe | 2412 | Handle | \REGISTRY\USER\S-1-5-21-1708537768-746137... |
| iexplore.exe | 2412 | Handle | \REGISTRY\USER\S-1-5-21-1708537768-746137... |
| iexplore.exe | 2412 | Handle | \REGISTRY\USER\S-1-5-21-1708537768-746137... |
| iexplore.exe | 2412 | Handle | \REGISTRY\MACHINE\SOFTWARE\Microsoft\Int... |
| iexplore.exe | 2412 | Handle | \BaseNamedObjects\Internet Explorer Immutabl... |
| iexplore.exe | 2412 | DLL | C:\Program Files\Internet Explorer\ieproxy.dll |
| iexplore.exe | 2412 | DLL | C:\Program Files\Internet Explorer\iexplore.exe |
| iexplore.exe | 2412 | DLL | C:\Documents and Settings\giridharan\Local Sett... |
| iexplore.exe | 2412 | DLL | C:\Program Files\Internet Explorer\xpshims.dll |

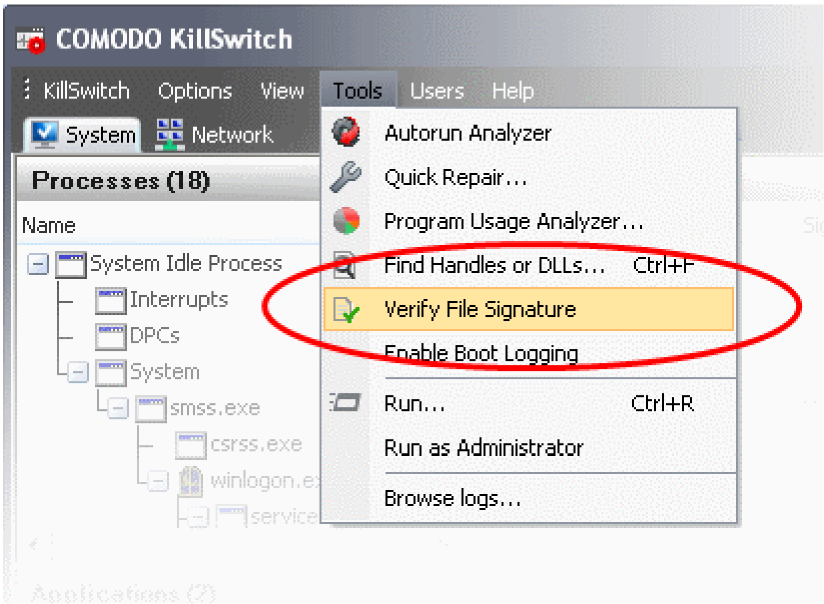
| Handle or DLL search results window - Descriptions of Columns | |
|---|---|
| **Column** | **Description** |
| Process | Shows the name of the process triggered by the handle or the DLL. Clicking the column header sorts the entries in alphabetical order of the process names. |
| PID | Process Identification number of the process. Clicking the column header sorts the entries in numerical order of the PIDs. |
| Type | Shows whether the process is triggered by Handle or DLL. |
| Handle or DLL | Shows the Handle or the DLL that has triggered the process along with its storage location. |

## 5.6.5. Verifying Authenticity of Applications

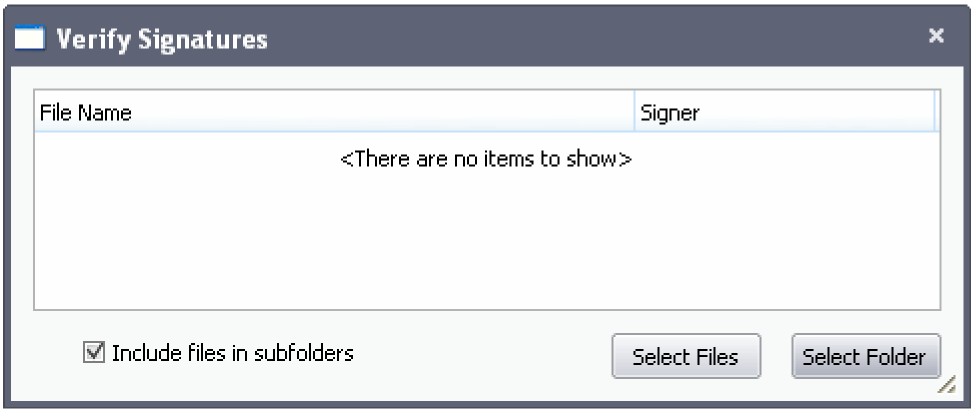
A software application can be treated 'Trusted' if it is published by a Trusted Software publisher/vendor. To prove the authenticity of their executables, software publishers digitally sign their software using a code signing certificate obtained from a Trusted Certificate Authority (CA). If you would like to know more about this process, refer to **Background details** later in this section.

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

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

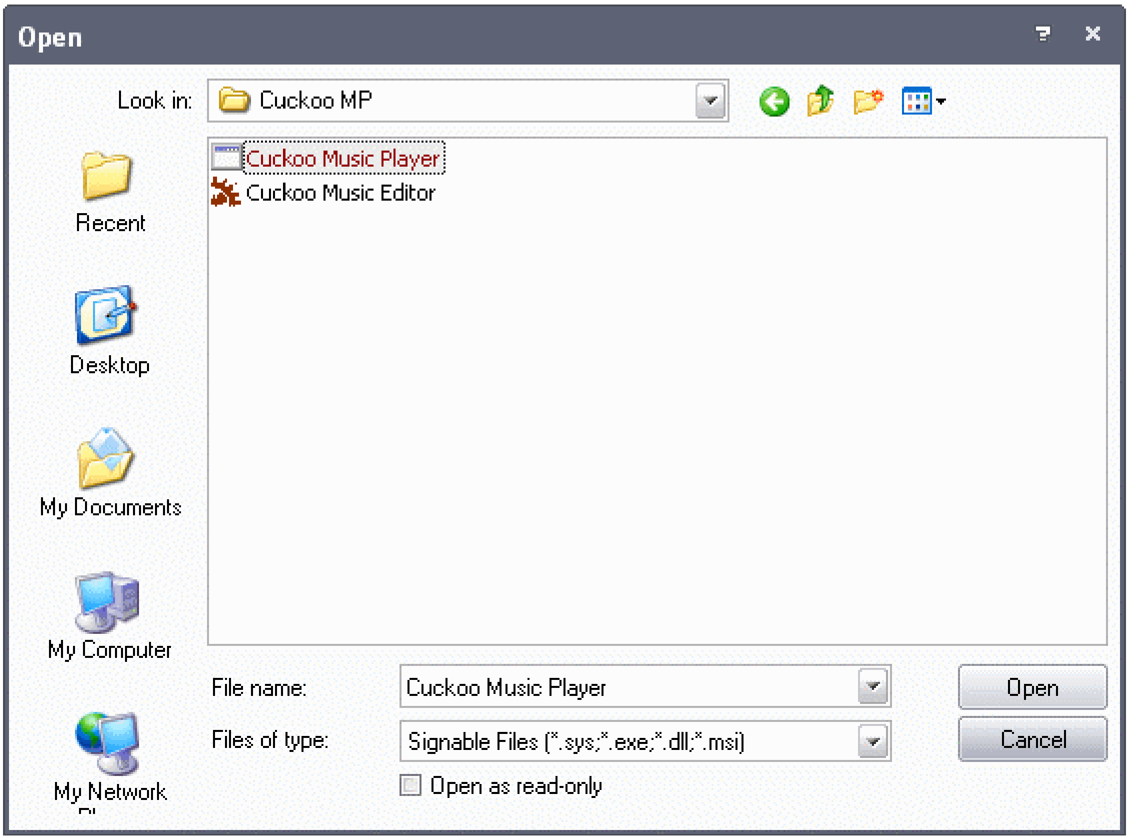


The 'Verify Signatures' dialog will be opened.



You can check the authenticity of a specific executable or make KillSwitch to scan a folder to identify all the .exe, .dll, .msi and .sys files in it and verify their authenticity.

- To check the authenticity of specific file, click 'Select Files'...

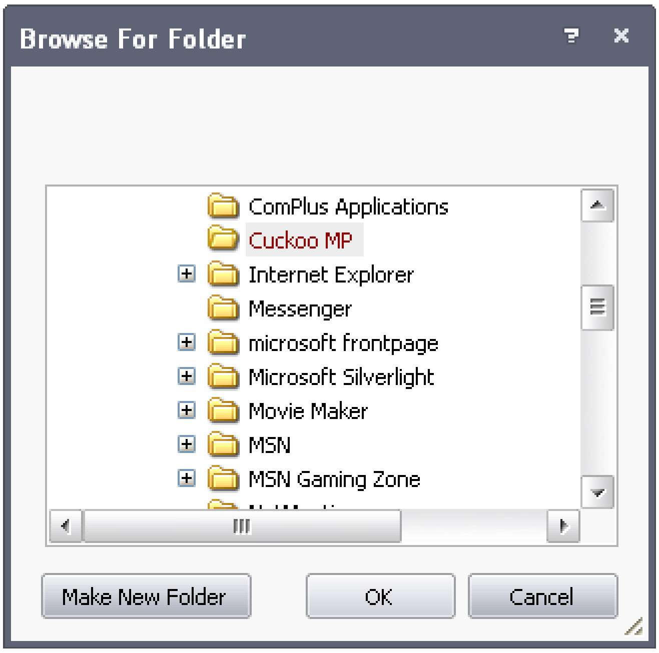


File name: Cuckoo Music Player

Files of type: Signable Files (*.sys;*.exe;*.dll;*.msi)

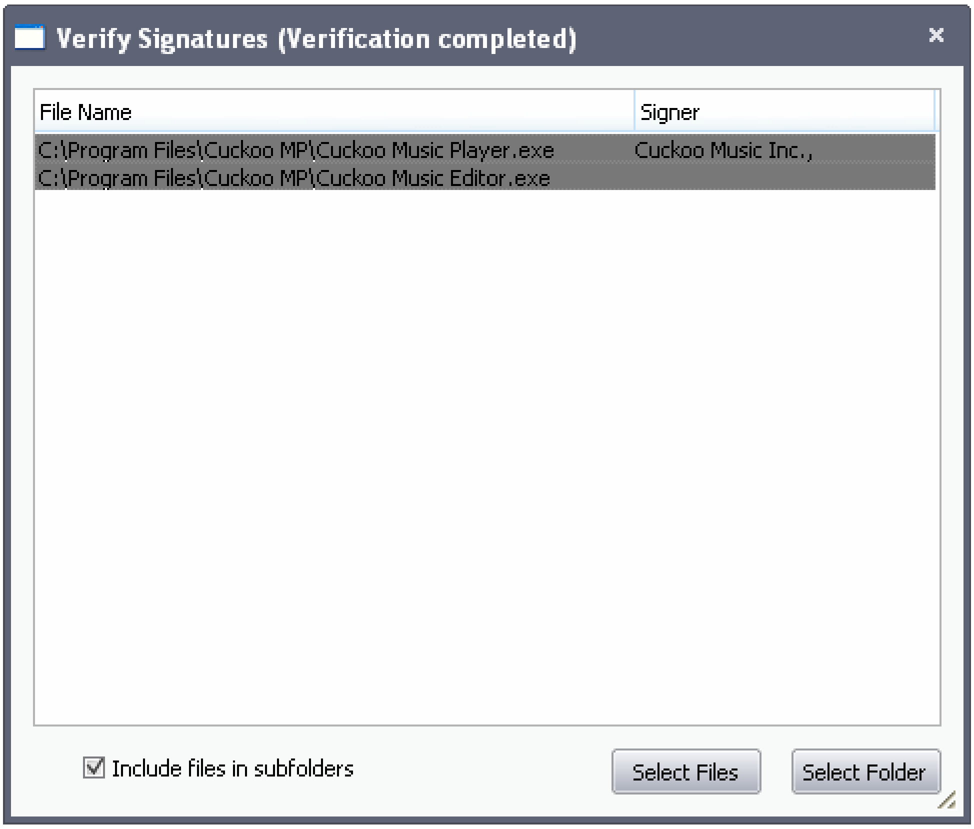
...and navigate to the folder containing the files of the program and select the binary/executable file.

- To scan a folder for binaries and verify their signatures, click 'Select Folder'...



… and navigate to the folder. KillSwitch will identify the .exe, .sys, .msi and .dll files in the selected folder. If you want KillSwitch to check the files in the sub-folder(s) of the selected folder, select 'Include files in subfolders'.

KillSwitch will immediately scan the files and if signatures are present, displays the signer information under the Signer column else, leaves the column blank.



| File Name | Signer |
|---|---|
| C:\Program Files\Cuckoo MP\Cuckoo Music Player.exe | Cuckoo Music Inc., |
| C:\Program Files\Cuckoo MP\Cuckoo Music Editor.exe | |

☑ Include files in subfolders

## 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.

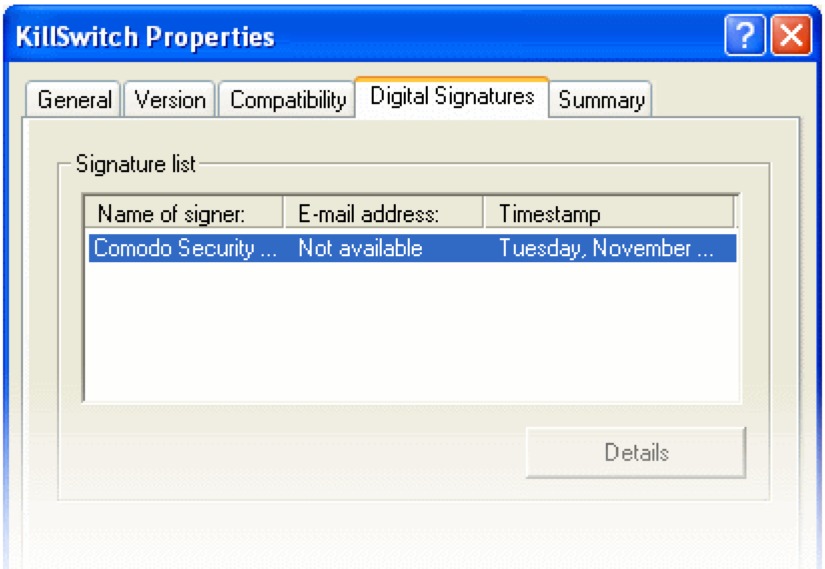
However, companies can't just 'sign' their own software and expect it to be trusted. This is why each code signing certificate is counter-signed by an organization called a 'Trusted Certificate Authority'. 'Comodo CA Limited' and 'Verisign' are two examples of a Trusted CA's and are authorized to counter-sign 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:



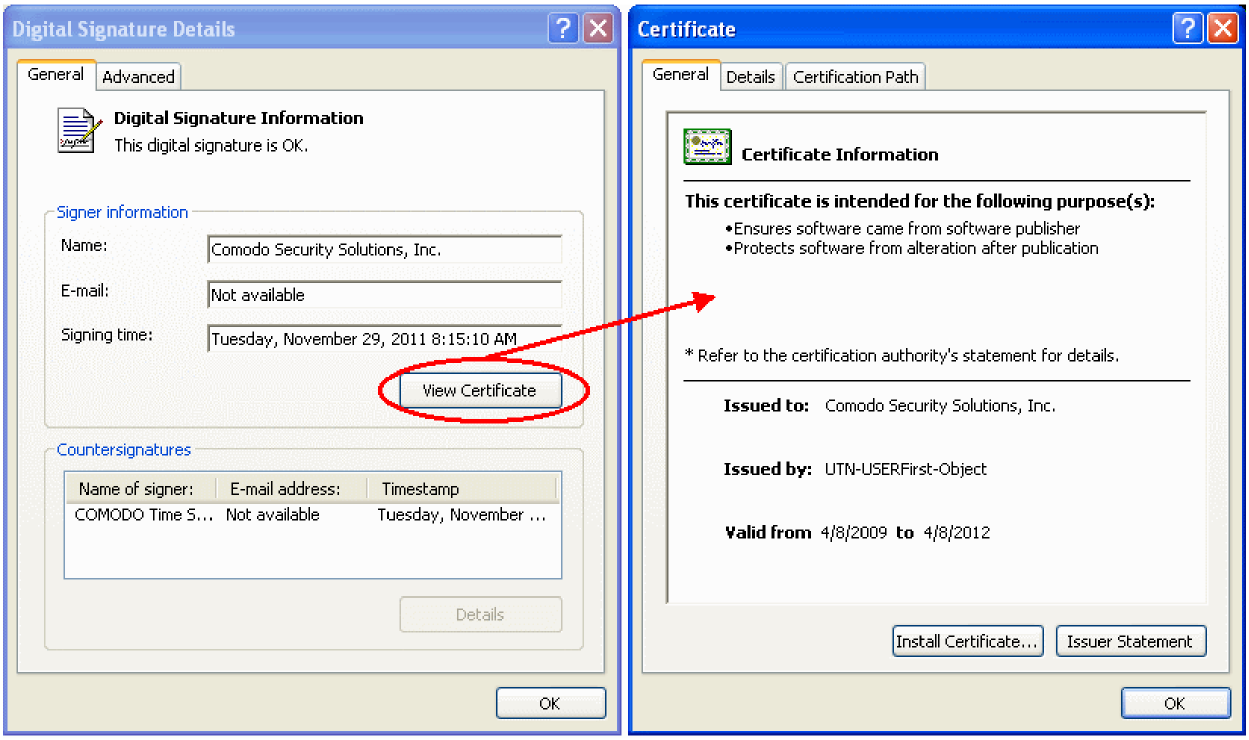
KillSwitch Properties

General | Version | Compatibility | Digital Signatures | Summary

Signature list

| Name of signer: | E-mail address: | Timestamp |
|---|---|---|
| Comodo Security ... | Not available | Tuesday, November ... |

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)



Digital Signature Details

General | Advanced

**Digital Signature Information**

This digital signature is OK.

Signer information

Name: Comodo Security Solutions, Inc.

E-mail: Not available

Signing time: Tuesday, November 29, 2011 8:15:10 AM

Countersignatures

| Name of signer: | E-mail address: | Timestamp |
|---|---|---|
| COMODO Time S... | Not available | Tuesday, November ... |

Certificate

General | Details | Certification Path

**Certificate Information**

**This certificate is intended for the following purpose(s):**

- Ensures software came from software publisher
- Protects software from alteration after publication

* Refer to the certification authority's statement for details.

**Issued to:** Comodo Security Solutions, Inc.

**Issued by:** UTN-USERFirst-Object

**Valid from** 4/8/2009 **to** 4/8/2012

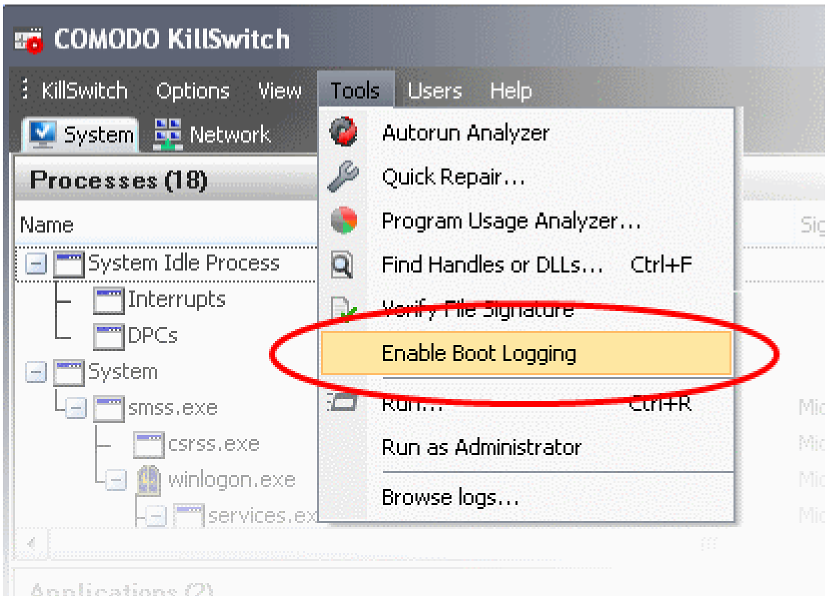
It should be noted that the example above is a special case in that Comodo, as creator of 'KillSwitch.exe', is both the signer of the software and, as a trusted CA, it is also the counter-signer (see the 'Countersignatures' box). In the vast majority of cases, the signer or the certificate (the vendor)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

## 5.6.6. Boot Logging and Handling Loaded Modules

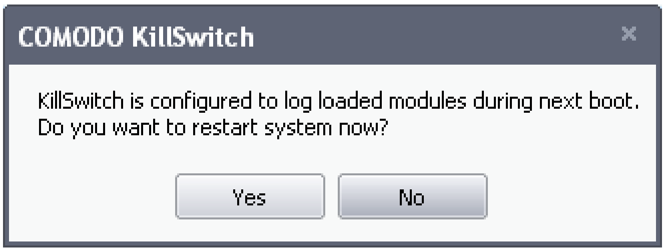
The Boot logger feature records all the modules loaded when your system boots. These include items like drivers, system files, DLLs, executables and so on. KillSwitch displays these modules along with their attributes and a trust rating under a new 'Loaded Modules' tab after your system has rebooted. This functionality allows you to check whether unsafe (or even just unwanted) modules are being loaded. In extreme cases, it will allow you to detect and delete malicious boot items installed by spyware, key loggers, rootkits or other malware.

To configure for Boot Logging:

1. From the 'Tools' menu, click 'Enable Boot Logging'.

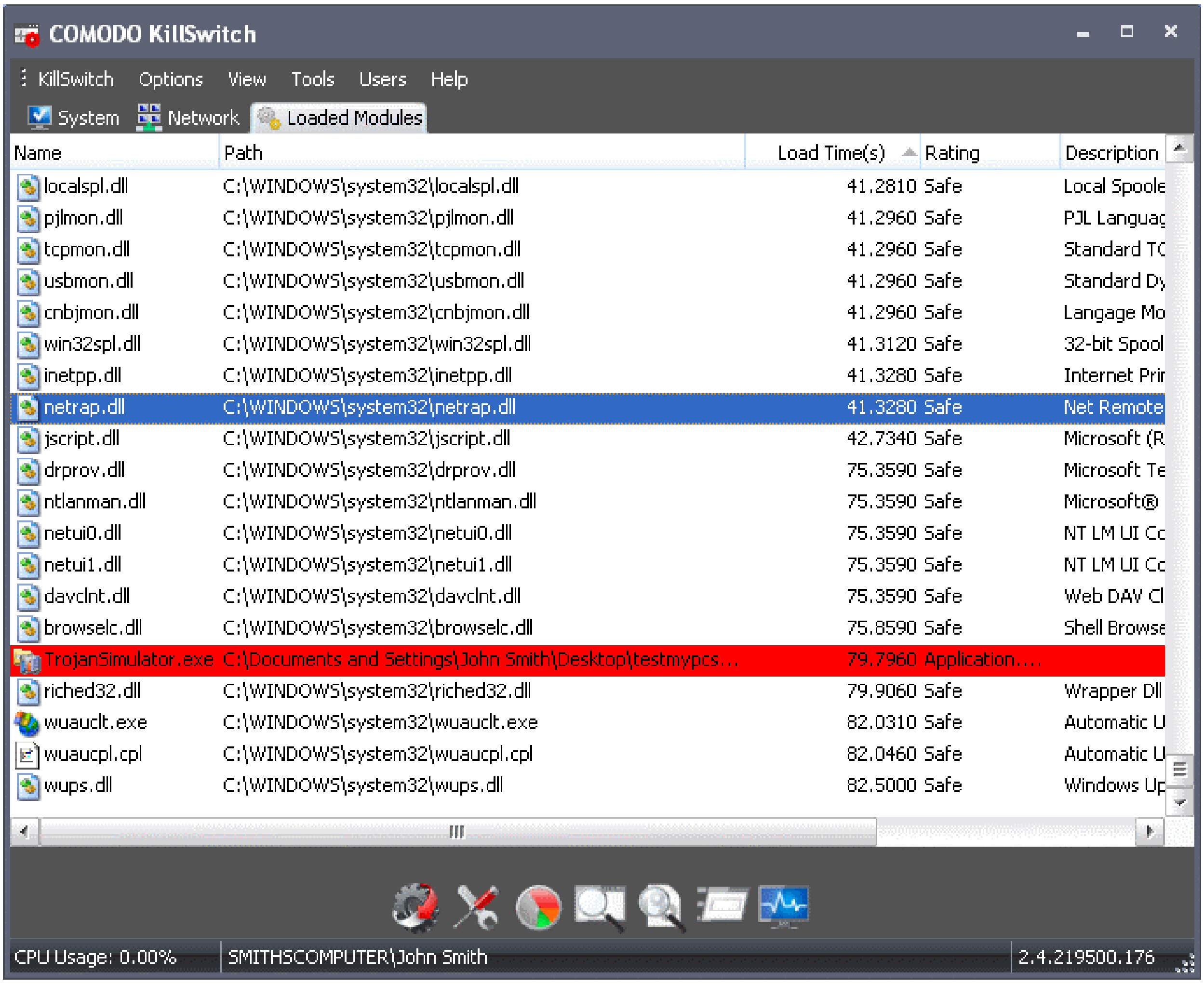


KillSwitch will request a restart of your computer to log all the modules that are loaded during the next re-boot.


COMODO KillSwitch

KillSwitch is configured to log loaded modules during next boot. Do you want to restart system now?

2. Save all your work and click 'Yes'. Your system will re-start. Upon restart, KillSwitch will be started automatically and show all the loaded modules loaded to your system.



| Name | Path | Load Time(s) | Rating | Description |
|---|---|---|---|---|
| localspl.dll | C:\WINDOWS\system32\localspl.dll | 41.2810 | Safe | Local Spoole |
| pjlmon.dll | C:\WINDOWS\system32\pjlmon.dll | 41.2960 | Safe | PJL Languag |
| tcpmon.dll | C:\WINDOWS\system32\tcpmon.dll | 41.2960 | Safe | Standard TC |
| usbmon.dll | C:\WINDOWS\system32\usbmon.dll | 41.2960 | Safe | Standard Dy |
| cnbjmon.dll | C:\WINDOWS\system32\cnbjmon.dll | 41.2960 | Safe | Langage Mo |
| win32spl.dll | C:\WINDOWS\system32\win32spl.dll | 41.3120 | Safe | 32-bit Spool |
| inetpp.dll | C:\WINDOWS\system32\inetpp.dll | 41.3280 | Safe | Internet Prir |
| netrap.dll | C:\WINDOWS\system32\netrap.dll | 41.3280 | Safe | Net Remote |
| jscript.dll | C:\WINDOWS\system32\jscript.dll | 42.7340 | Safe | Microsoft (R |
| drprov.dll | C:\WINDOWS\system32\drprov.dll | 75.3590 | Safe | Microsoft Te |
| ntlanman.dll | C:\WINDOWS\system32\ntlanman.dll | 75.3590 | Safe | Microsoft® |
| netui0.dll | C:\WINDOWS\system32\netui0.dll | 75.3590 | Safe | NT LM UI Cc |
| netui1.dll | C:\WINDOWS\system32\netui1.dll | 75.3590 | Safe | NT LM UI Cc |
| davclnt.dll | C:\WINDOWS\system32\davclnt.dll | 75.3590 | Safe | Web DAV Cl |
| browselc.dll | C:\WINDOWS\system32\browselc.dll | 75.8590 | Safe | Shell Browse |
| TrojanSimulator.exe | C:\Documents and Settings\John Smith\Desktop\testmypcs... | 79.7960 | Application.... | |
| riched32.dll | C:\WINDOWS\system32\riched32.dll | 79.9060 | Safe | Wrapper Dll |
| wuauclt.exe | C:\WINDOWS\system32\wuauclt.exe | 82.0310 | Safe | Automatic U |
| wuaucpl.cpl | C:\WINDOWS\system32\wuaucpl.cpl | 82.0460 | Safe | Automatic U |
| wups.dll | C:\WINDOWS\system32\wups.dll | 82.5000 | Safe | Windows Up |

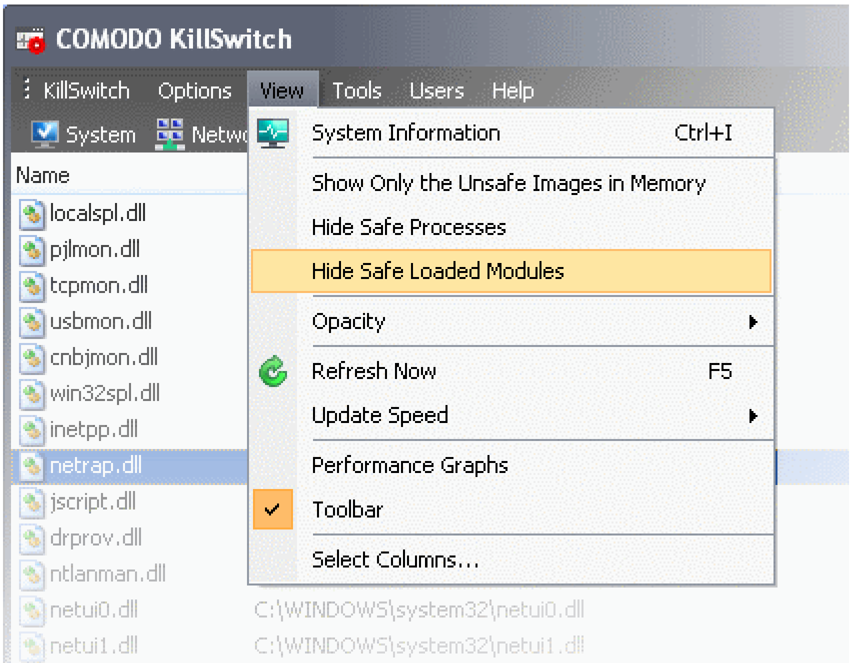
CPU Usage: 0.00% | SMITHSCOMPUTER\John Smith | 2.4.219500.176

| Loaded Modules window - Descriptions of Columns | |
|---|---|
| **Column** | **Description** |
| Name | Shows the name of the module. Clicking the column header sorts the entries in alphabetical order of the module names. |
| Path | Shows the storage path of the module. |
| Load Time (in seconds) | Shows time taken for loading the module. |
| Rating | Shows the result of scanning performed by KillSwitch on the module. Modules that are rated as unsafe or unknown will be highlighted for easy identification. |
| Description | Shows a brief description of the module. |
| Company Name | Shows the vendor of the module. |

**Tip**: Clicking any of the column header sorts the list in alphabetical/numerical order of the entries in it.

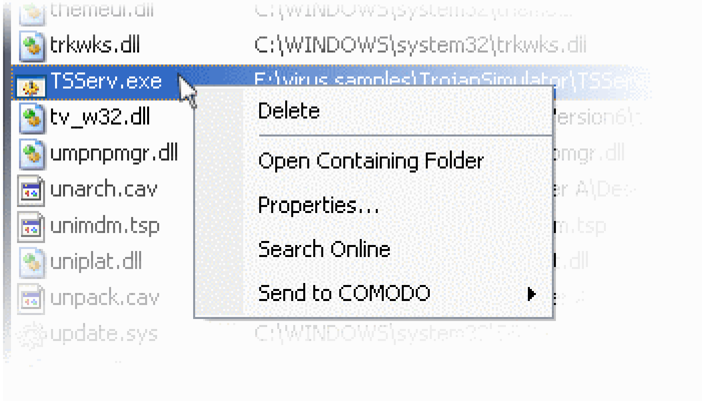
## Filtering the Loaded Modules List

You can filter the list to hide the modules identified as 'Safe' and show only the modules identified as 'unsafe' or 'unknown' by clicking View > Hide Safe Loaded Modules.

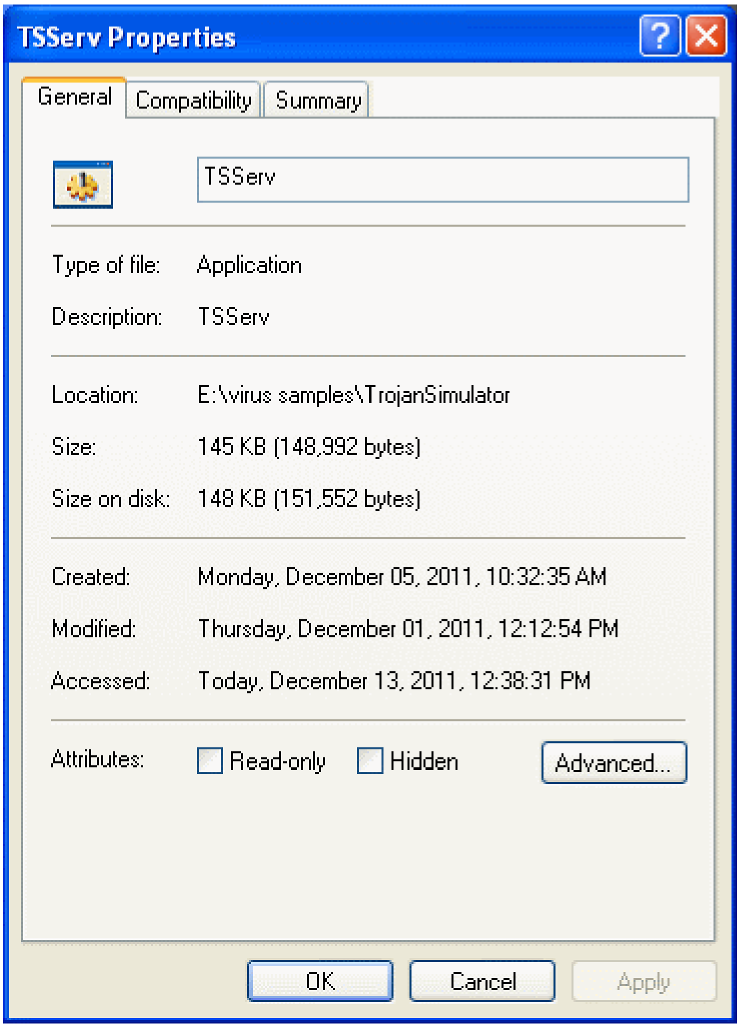


## Handling Loaded Modules

You can viewing properties of or remove loaded module by right clicking on it and selecting the required option from the context sensitive menu.



- **Delete** - Removes the Module from your system. This ensures that the module is not loaded to your system from the next boot onwards.
- **Open Containing Folder** - Opens the folder containing the module in Windows Explorer.
- **Properties...** - Opens the properties dialog of the selected Module.



TSServ Properties

General | Compatibility | Summary

TSServ

Type of file: Application

Description: TSServ

Location: E:\virus samples\TrojanSimulator

Size: 145 KB (148,992 bytes)

Size on disk: 148 KB (151,552 bytes)

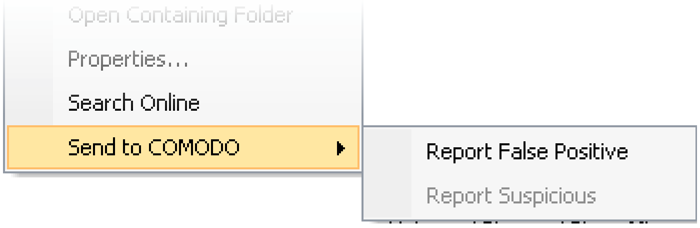
Created: Monday, December 05, 2011, 10:32:35 AM

Modified: Thursday, December 01, 2011, 12:12:54 PM

Accessed: Today, December 13, 2011, 12:38:31 PM

Attributes: □ Read-only □ Hidden

- **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.
- **Send to COMODO** - Submits the module for analysis to Comodo, as False Positive (if identified as suspicious by KillSwitch) or as Suspicious file 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 global white list or black list accordingly in order to benefit all the users of Comodo security products world wide.

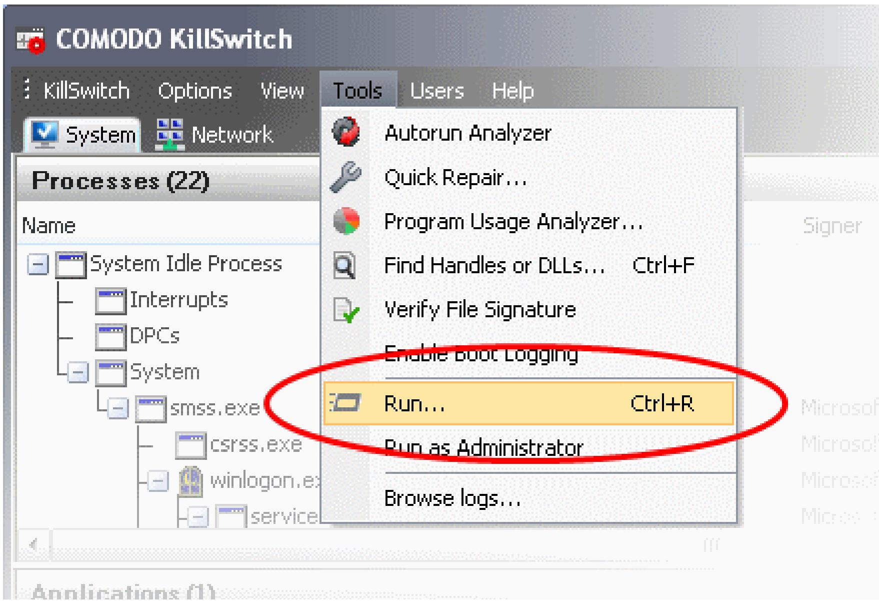


## 5.6.7. Running Programs from Command Line Interface

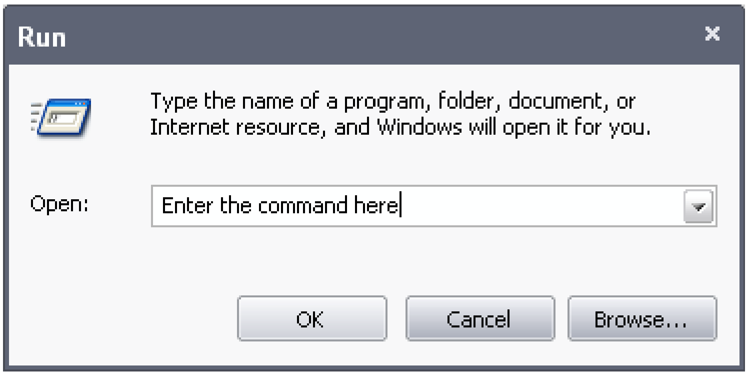
KillSwitch allows you to run Command Line Interface programs with the account privileges of currently logged-in user or those requiring administrative privileges from its 'Tools' menu.

To run a program with the currently logged-in user privileges:

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



- Alternatively, click the Run icon  from the toolbar. The 'Run' dialog will open.


Run

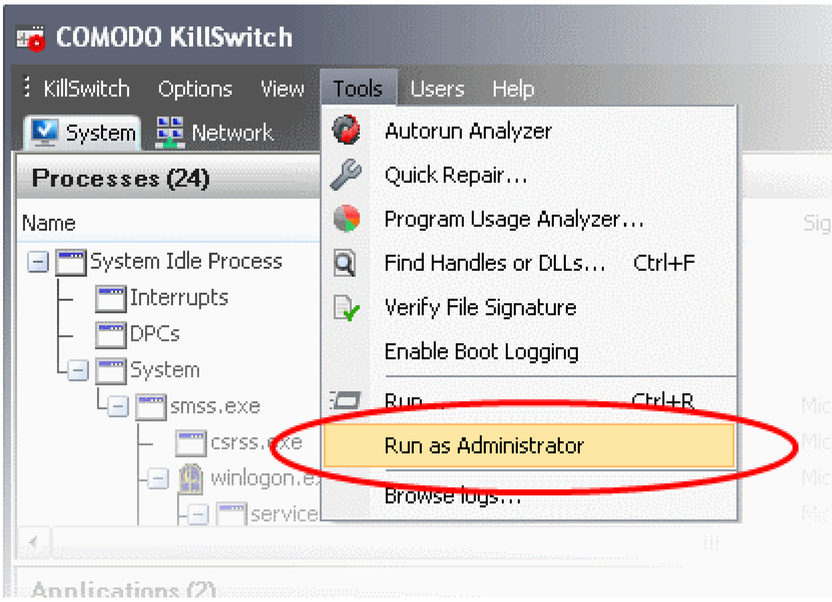
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: Enter the command here

- Enter the command or browse to the file/program you wish to open by clicking 'Browse'.
- Click 'OK'.

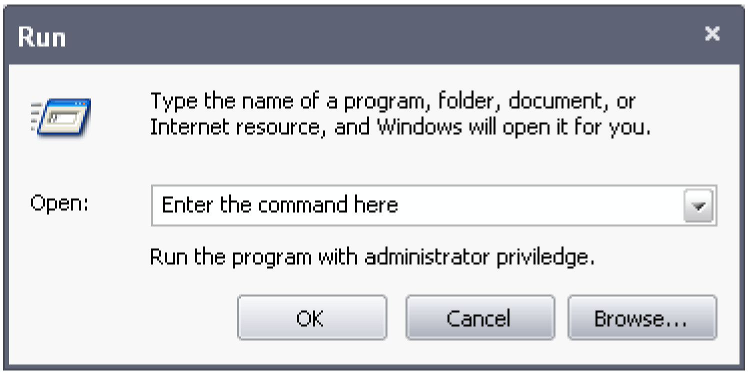
To run programs that require Administrative privileges:

- From the 'Tools' menu, click 'Run as Administrator'.



The Run dialog will open.

- Enter the command or browse to the file/program you wish to open with administrative privileges by clicking 'Browse'.



Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: Enter the command here

Run the program with administrator priviledge.

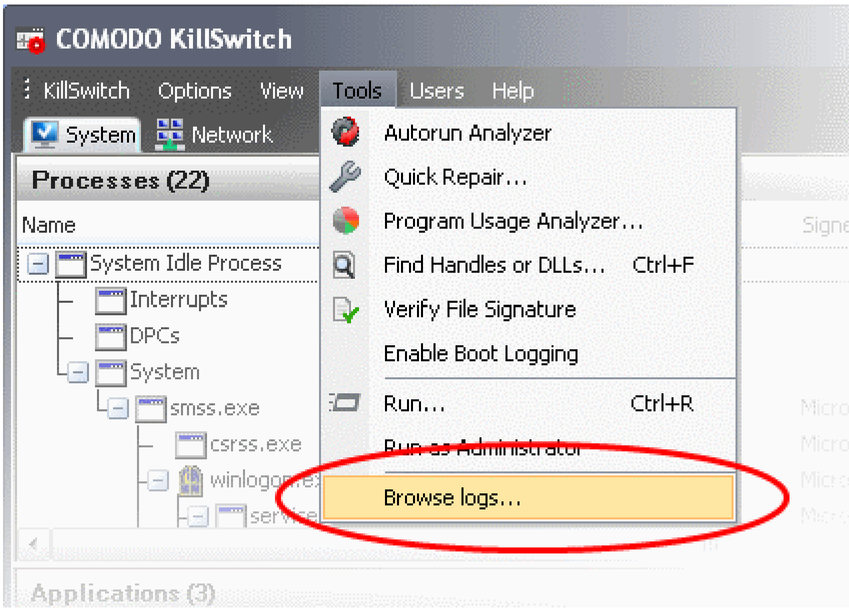
- Click 'OK'.

## 5.6.8. Viewing KillSwitch Logs

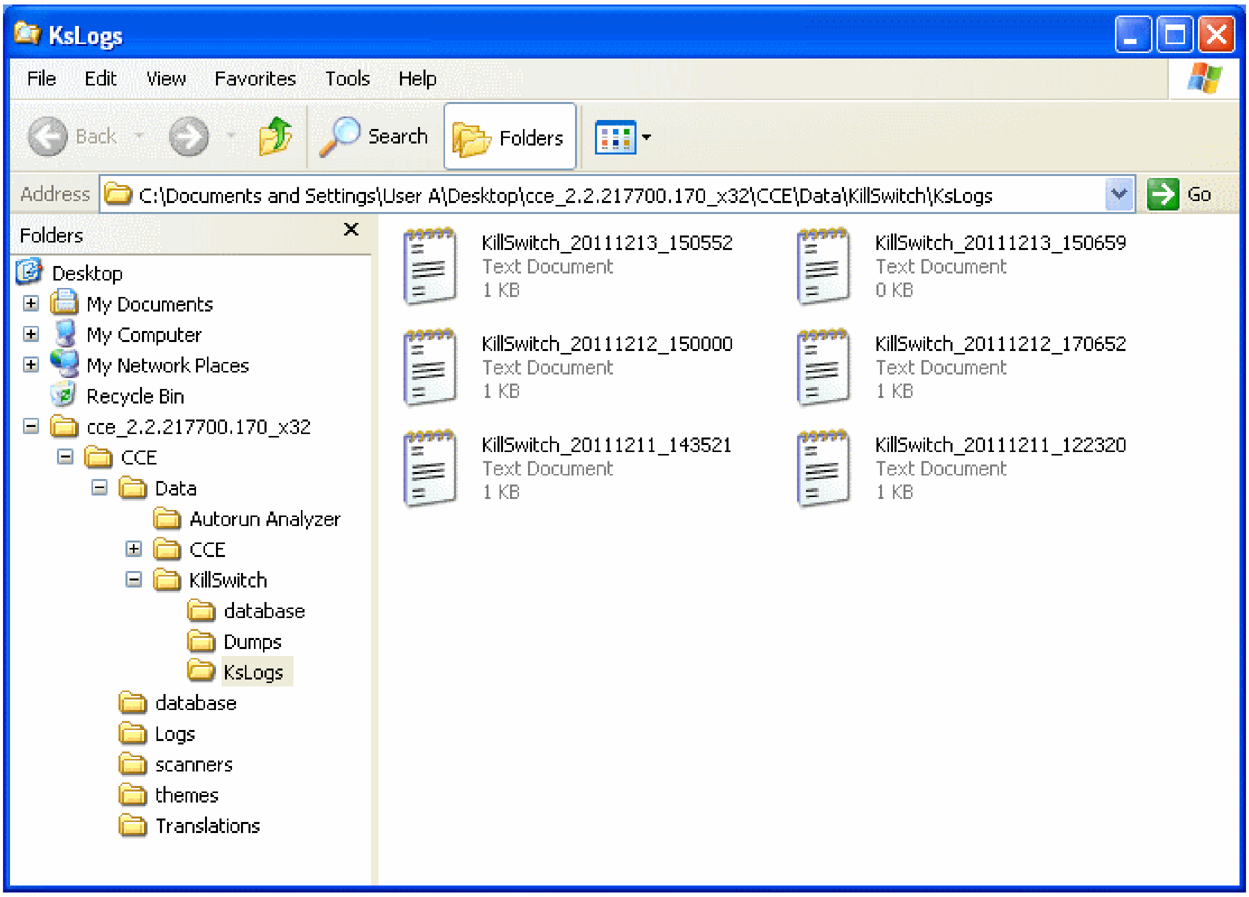
KillSwitch maintains logs of threats found and actions taken against them as configured through 'Options' > 'Threats Log Level'. The logs are stored as date stamped text files in the folder ...\CCE\Data\KillSwitch\KsLogs.

To view the log files:

- From the 'Tools' menu, click 'Browse Logs'.



The logs folder will open in Windows Explorer.



Address: C:\Documents and Settings\User A\Desktop\cce_2.2.217700.170_x32\CCE\Data\KillSwitch\KsLogs

KillSwitch_20111213_150552
Text Document
1 KB

KillSwitch_20111213_150659
Text Document
0 KB

KillSwitch_20111212_150000
Text Document
1 KB

KillSwitch_20111212_170652
Text Document
1 KB

KillSwitch_20111211_143521
Text Document
1 KB

KillSwitch_20111211_122320
Text Document
1 KB

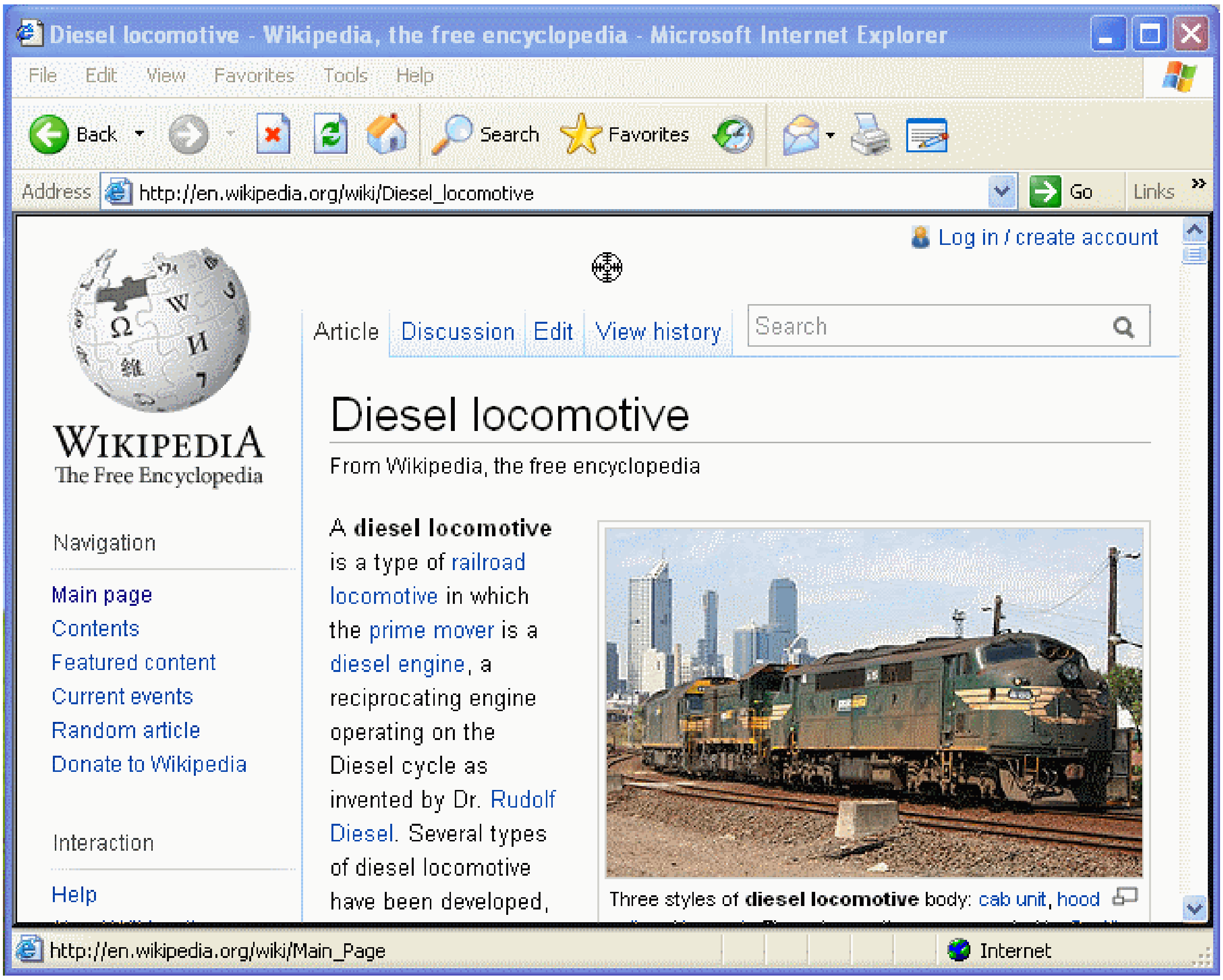
- Double click on the file you wish to view.

## 5.6.9. Finding Process of the Active Window

The 'Find Window' tool enables you to identify the process associated with the active application window or the window components in it.

To find the process related to active application window:

1. Click on the Find Window icon in the Toolbar.
2. Drag the bulls-eye to the portion of the window for which you want to find the process


Diesel locomotive - Wikipedia, the free encyclopedia - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://en.wikipedia.org/wiki/Diesel_locomotive
Go Links
Log in / create account
WIKIPEDIA
The Free Encyclopedia
Article Discussion Edit View history
Search
Navigation
Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Interaction
Help
http://en.wikipedia.org/wiki/Main_Page
Internet

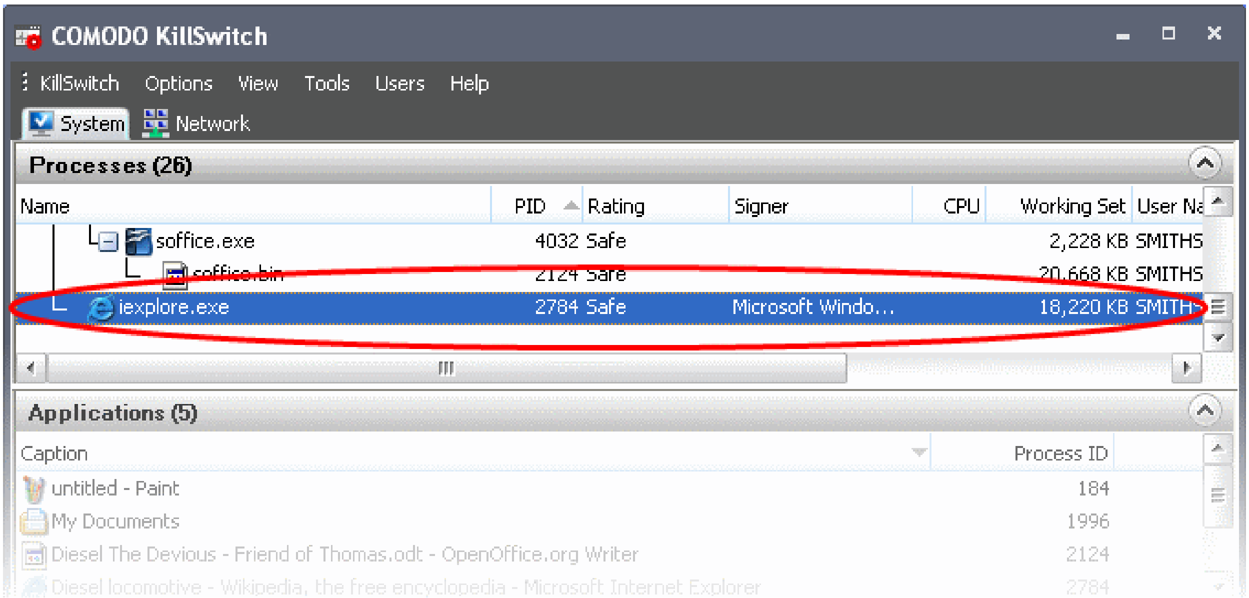
Diesel locomotive

From Wikipedia, the free encyclopedia

A **diesel locomotive** is a type of railroad locomotive in which the prime mover is a diesel engine, a reciprocating engine operating on the Diesel cycle as invented by Dr. Rudolf Diesel. Several types of diesel locomotive have been developed,

Three styles of **diesel locomotive** body: cab unit, hood

3. On release of the mouse button, the process related to the highlighted window will be shown highlighted in the 'Processes' window of KillSwitch.



Processes (26)

| Name | PID | Rating | Signer | CPU | Working Set | User Na |
|---|---|---|---|---|---|---|
| soffice.exe | 4032 | Safe | | | 2,228 KB | SMITHS |
| soffice.bin | 2124 | Safe | | | 20,668 KB | SMITHS |
| iexplore.exe | 2784 | Safe | Microsoft Windo... | | 18,220 KB | SMITH- |

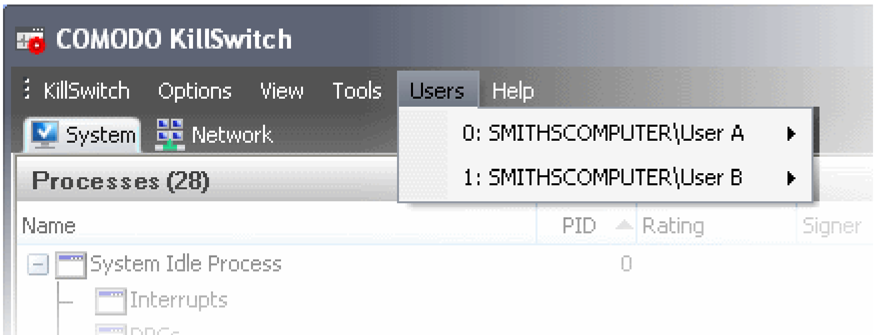
Applications (5)

| Caption | Process ID |
|---|---|
| untitled - Paint | 184 |
| My Documents | 1996 |
| Diesel The Devious - Friend of Thomas.odt - OpenOffice.org Writer | 2124 |
| Diesel locomotive - Wikipedia, the free encyclopedia - Microsoft Internet Explorer | 2784 |

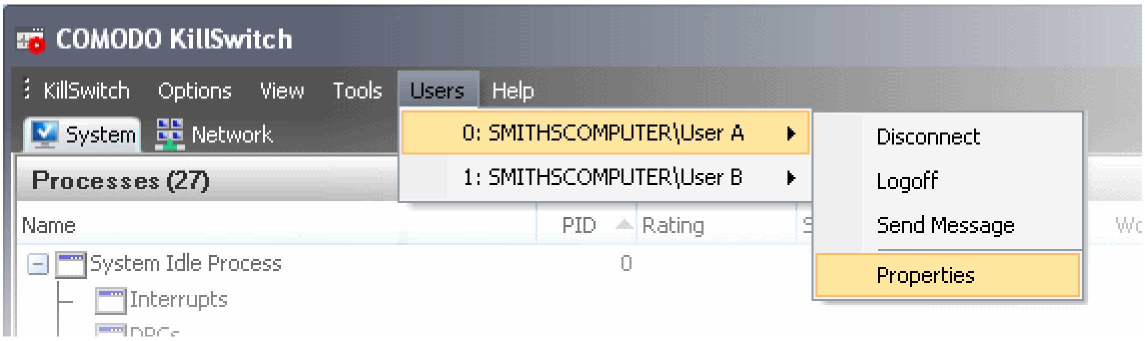
## 5.7. Managing Currently Logged-in Users

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

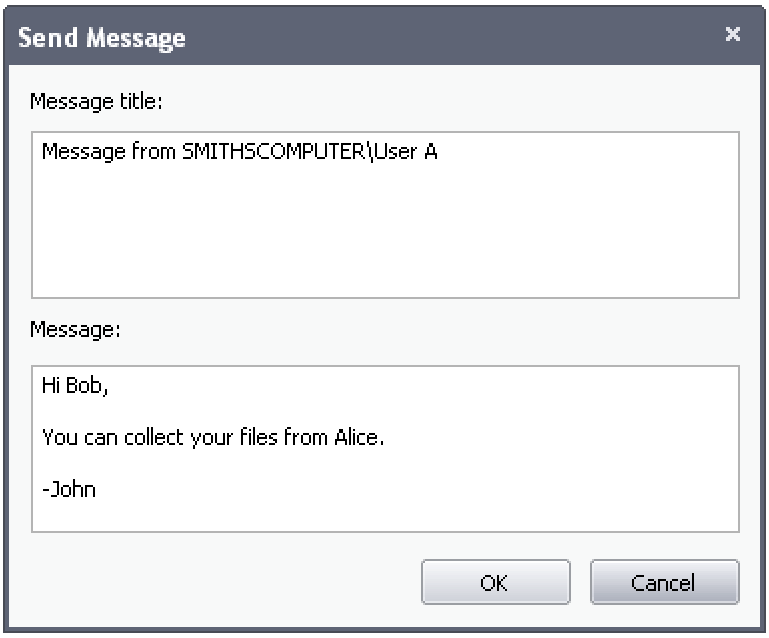
To view the the currently logged-in users, click the 'Users' menu from the file menu bar.



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



- **Disconnect** - Enables you to disconnect the connected user account from your Windows session.
- **Log off** - Forcedly logs-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.


Send Message

Message title:

Message from SMITHSCOMPUTER\User A

Message:

Hi Bob,

You can collect your files from Alice.

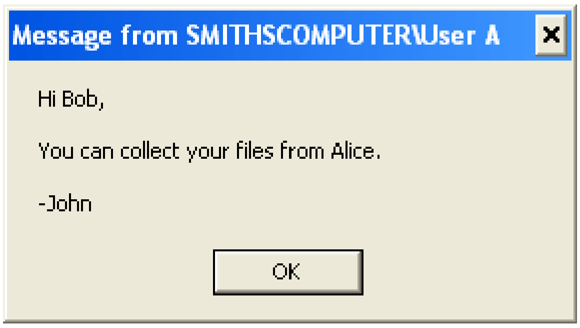
-John

**To send a message to a selected user**

- Enter your message in the 'Text' field and click OK.

**Tip**: Press 'Ctrl' + 'Enter' for moving to next line while typing messages with more than one line. Pressing just 'Enter' from your keyboard will immediately send the message.

The message will be displayed in the user's desktop.



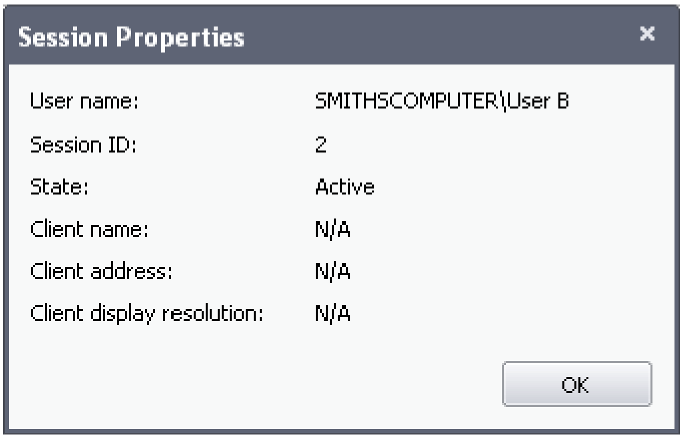
Message from SMITHSCOMPUTER\User A

Hi Bob,

You can collect your files from Alice.

-John

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



Session Properties

User name: SMITHSCOMPUTER\User B

Session ID: 2

State: Active

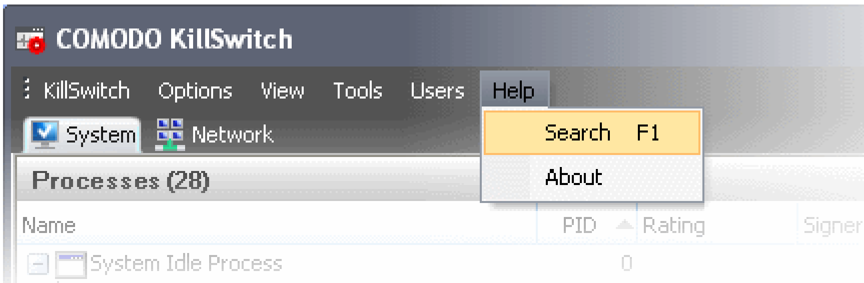
Client name: N/A

Client address: N/A

Client display resolution: N/A

## 5.8. Help and About Details

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

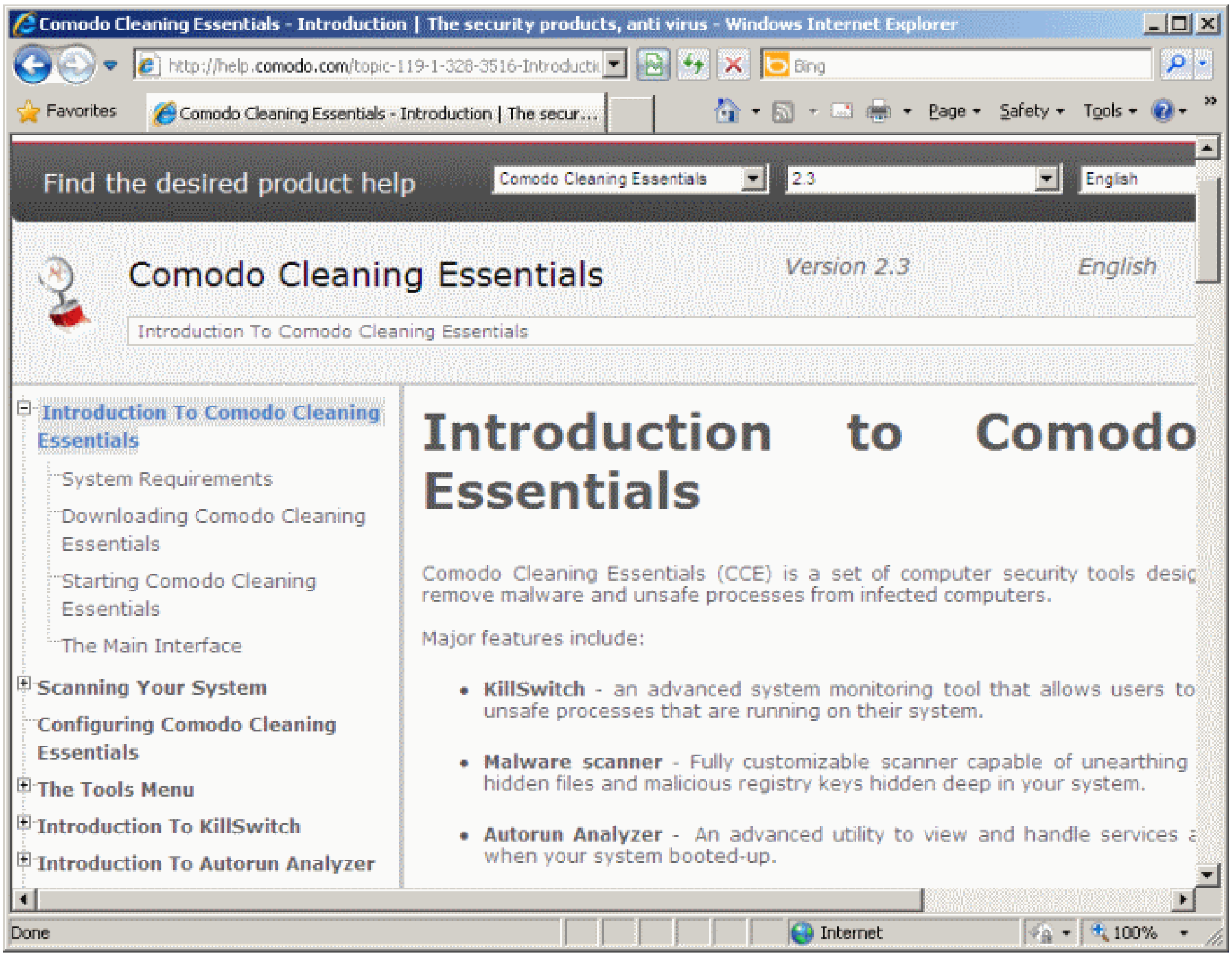


Clicking on the Help menu has the two options:

- Search
- About

### 5.8.1. 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.


Comodo Cleaning Essentials - Introduction | The security products, anti virus - Windows Internet Explorer
http://help.comodo.com/topic-119-1-328-3516-Introducti
Bing
Favorites
Comodo Cleaning Essentials - Introduction | The secur...
Page
Safety
Tools
Find the desired product help
Comodo Cleaning Essentials
2.3
English
Comodo Cleaning Essentials
Version 2.3
English
Introduction To Comodo Cleaning Essentials
Introduction To Comodo Cleaning Essentials
System Requirements
Downloading Comodo Cleaning Essentials
Starting Comodo Cleaning Essentials
The Main Interface
Scanning Your System
Configuring Comodo Cleaning Essentials
The Tools Menu
Introduction To KillSwitch
Introduction To Autorun Analyzer
Done
Internet
100%

Introduction to Comodo Essentials

Comodo Cleaning Essentials (CCE) is a set of computer security tools desig remove malware and unsafe processes from infected computers.

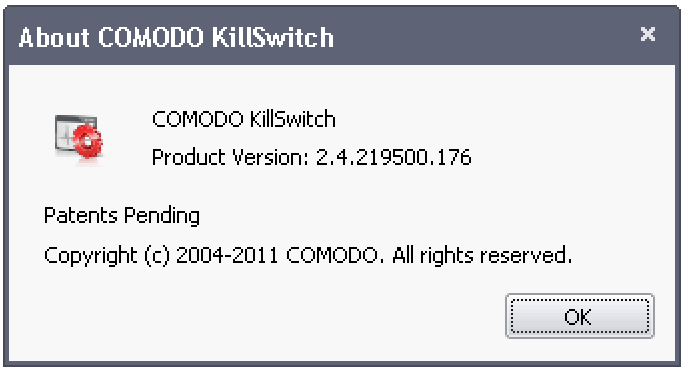
Major features include:

- **KillSwitch** - an advanced system monitoring tool that allows users to unsafe processes that are running on their system.
- **Malware scanner** - Fully customizable scanner capable of unearthing hidden files and malicious registry keys hidden deep in your system.
- **Autorun Analyzer** - An advanced utility to view and handle services a when your system booted-up.

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

## 5.8.2. About

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



COMODO KillSwitch

Product Version: 2.4.219500.176

Patents Pending

Copyright (c) 2004-2011 COMODO. All rights reserved.

The About dialog displays the Version Number of KillSwitch and the copyright information.

# 6. Introduction to Autorun Analyzer

The services, drivers, system files, programs and so forth,  that are loaded when your system boots-up can have a significant impact on the security your system. Certain programs and services must be loaded at start-up because they are essential to the security and smooth operation.

Unfortunately, any malware will add a start-up item, and make it to run at the background, to pave way for malicious attempts like key logger, rootkits, buffer overflow or Denial of Service (DoS) attacks. These attacks will be running silently in the computer and enable hackers to steal your identity and confidential information like your credit card details.

The Autorun Analyzer makes a thorough check on the Start-up items that are loaded during system start-up and shows them as a list with their threat rating. The interface allows you to choose precisely which programs and services are to be enabled and to delete the items that are identified as malware.

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

- **Introduction to Autorun Analyzer**
  - **Starting Autorun Analyzer**
  - **The Main Interface**
- **Viewing and Handling Autorun Items**
  - **Handling Autorun Items**
  - **Filtering Entries based on Categories**
  - **Viewing Autorun Items for other User Accounts**
- **Help and About Details**

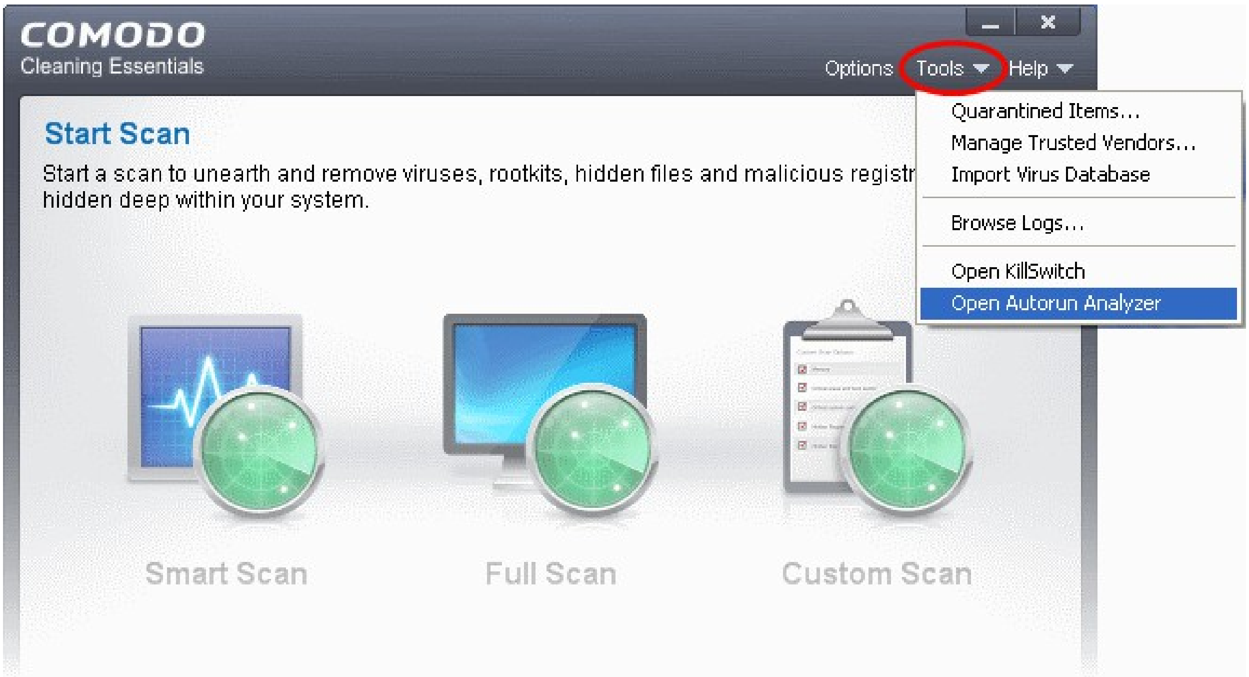
## 6.1. Starting Autorun Analyzer

Autorun Analyzer can be started by the following ways:

- **From the Comodo Cleaning Essentials interface**
- **From the KillSwitch interface**
- **From the folder containing Comodo Cleaning Essentials files**

### 6.1.1. From the Comodo Cleaning Essentials Interface

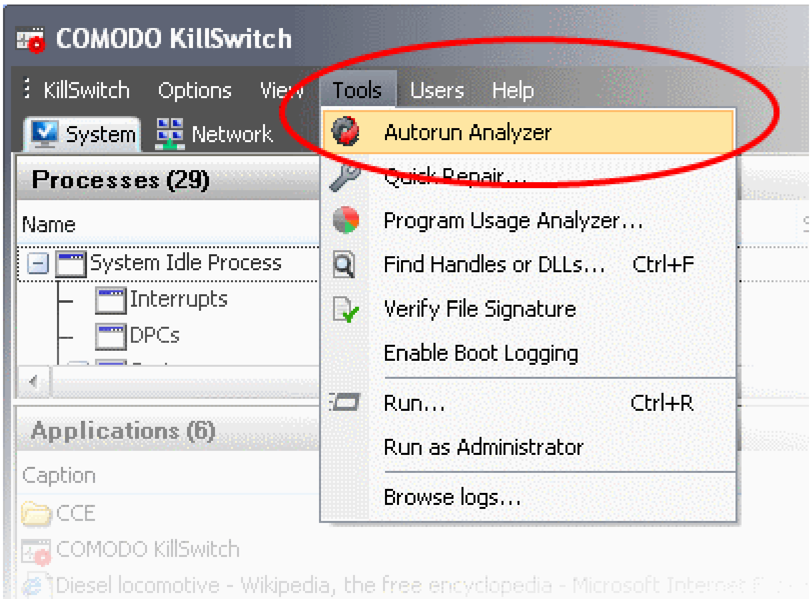
- Click 'Tools' > 'Open Autorun Analyzer' from the title bar controls of the main interface of Comodo Cleaning Essentials.



The Autorun Analyzer main interface will be opened.

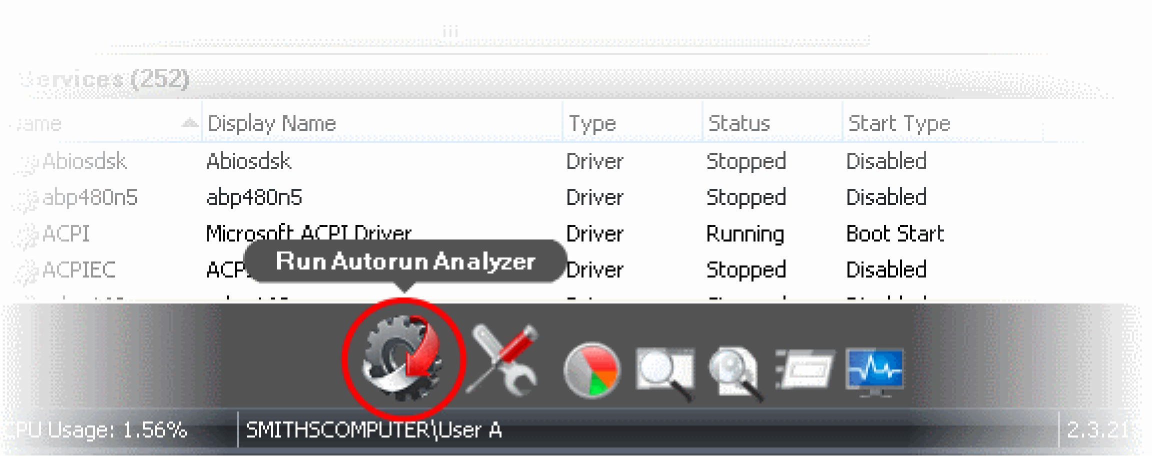
### 6.1.2. From the KillSwitch Interface

- Click 'Tools' > 'Autorun Analyzer' from the file menu  bar of the main interface of Comodo KillSwitch.



Or

- Click the Autorun Analyzer icon from the Toolbar, beneath the main display pane of KillSwitch interface.



Services (252)

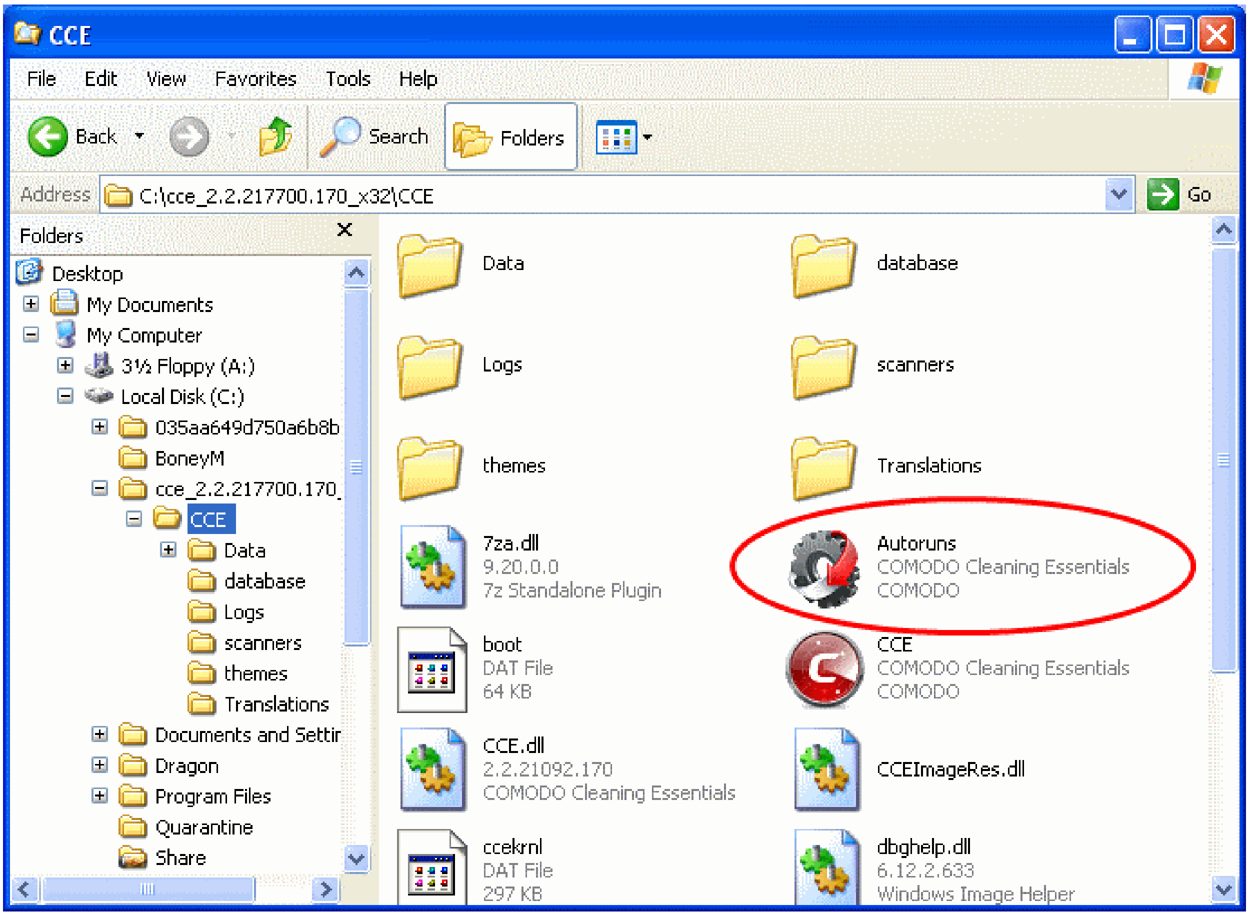
| ame | Display Name | Type | Status | Start Type |
|---|---|---|---|---|
| Abiosdsk | Abiosdsk | Driver | Stopped | Disabled |
| abp480n5 | abp480n5 | Driver | Stopped | Disabled |
| ACPI | Microsoft ACPI Driver | Driver | Running | Boot Start |
| ACPIEC | ACP | Driver | Stopped | Disabled |

CPU Usage: 1.56% | SMITHSCOMPUTER\User A | 2.3.21

The Autorun Analyzer main interface will be opened.

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

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

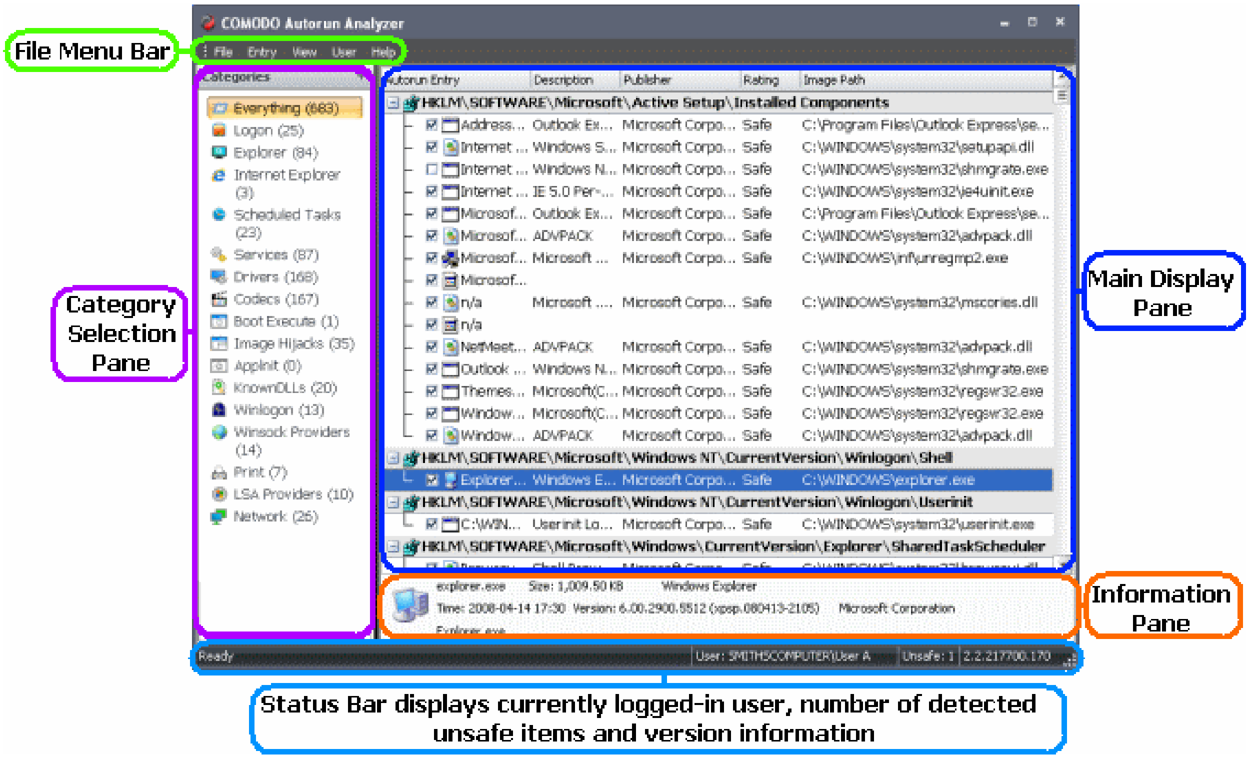


Address: C:\cce_2.2.217700.170_x32\CCE

The Autorun Analyzer main interface will be opened.

# 6.2. The Main Interface

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



| Autorun Entry | Description | Publisher | Rating | Image Path |
|---|---|---|---|---|
| HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components | | | | |
| ☑ Address... | Outlook Ex... | Microsoft Corpo... | Safe | C:\Program Files\Outlook Express\se... |
| ☑ Internet ... | Windows S... | Microsoft Corpo... | Safe | C:\WINDOWS\system32\setupapi.dll |
| □ Internet ... | Windows N... | Microsoft Corpo... | Safe | C:\WINDOWS\system32\shmgrate.exe |
| ☑ Internet ... | IE 5.0 Per-... | Microsoft Corpo... | Safe | C:\WINDOWS\system32\ie4uinit.exe |
| ☑ Microsof... | Outlook Ex... | Microsoft Corpo... | Safe | C:\Program Files\Outlook Express\se... |
| ☑ Microsof... | ADVPACK | Microsoft Corpo... | Safe | C:\WINDOWS\system32\advpack.dll |
| ☑ Microsof... | Microsoft ... | Microsoft Corpo... | Safe | C:\WINDOWS\inf\unregmp2.exe |
| ☑ Microsof... | | | | |
| ☑ n/a | Microsoft .... | Microsoft Corpo... | Safe | C:\WINDOWS\system32\mscories.dll |
| ☑ n/a | | | | |
| ☑ NetMeet... | ADVPACK | Microsoft Corpo... | Safe | C:\WINDOWS\system32\advpack.dll |
| ☑ Outlook ... | Windows N... | Microsoft Corpo... | Safe | C:\WINDOWS\system32\shmgrate.exe |
| ☑ Themes... | Microsoft(C... | Microsoft Corpo... | Safe | C:\WINDOWS\system32\regsvr32.exe |
| ☑ Window... | Microsoft(C... | Microsoft Corpo... | Safe | C:\WINDOWS\system32\regsvr32.exe |
| ☑ Window... | ADVPACK | Microsoft Corpo... | Safe | C:\WINDOWS\system32\advpack.dll |
| HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell | | | | |
| ☑ Explorer... | Windows E... | Microsoft Corpo... | Safe | C:\WINDOWS\explorer.exe |
| HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit | | | | |
| ☑ C:\WIN... | Userinit Lo... | Microsoft Corpo... | Safe | C:\WINDOWS\system32\userinit.exe |
| HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SharedTaskScheduler | | | | |

explorer.exe Size: 1,009.50 KB Windows Explorer
Time: 2008-04-14 17:30 Version: 6.00.2900.5512 (xpsp.080413-2105) Microsoft Corporation
Explorer.exe

User: SMITHSCOMPUTER\User A Unsafe: 1 2.2.217700.170

Status Bar displays currently logged-in user, number of detected unsafe items and version information

The interface is divided into five main areas:

- The File Menu bar;
- Main display Pane;
- Information Pane;
- Category Selection Pane;
- Status Bar

## The File Menu Bar

The file menu bar displays the controls for executing various tasks of the application.

| Menu | Option | Description |
|---|---|---|
| File | | Contains options related to file operations, enabling/disabling start-up items, and analyzing offline system. |
| | Find | Launches the Find dialog to search for a specific entry by entering a search parameter |
| | Open | Opens a pre-stored Autorun Analyzer file |
| | Save | Opens the 'Save as' dialog to save the data in the main display pane in the native file format of Autorun Analyzer. The file is stored with .ard extension. |
| | Enable All Unsafe Entries | Enables the start-up items identified as unsafe, all at once. |
| | Disable All Unsafe Entries | Disables the start-up items identified as unsafe, all at once. |

| | | |
|---|---|---|
| | Analyze Offline System | Starts the wizard to analyze an idle additional Windows operating system installed in your computer, e.g. a virtual machine. |
| | Refresh | Refreshes the Autorun Analyzer application. |
| | Exit | Closes the Autorun Analyzer application. |
| Entry | | Contains Options to handle the Start-up items |
| | Delete | Removes the selected item from the Autorun items and deletes the parent application from your system. |
| | Copy | Copies the data in the selected row to clip-board of your system. |
| | Jump to Entry | Opens the selected entry in Windows Registry Editor |
| | Jump to Folder | Opens the folder containing the selected entry in Windows Explorer |
| | Enabled | Enables to toggle the selected autorun entry between 'Enabled' and 'Disabled' states. |
| | Search Online | Opens the default web browser of your system with the search engine specified and searches for information on the selected autorun entry on the web. |
| | Properties | Opens the Properties dialog of the selected autorun entry. |
| View | | Contains options related to display nature of the application. |
| | Hide Safe Entries | Displays only the autorun entries identified as unsafe by Autorun Analyzer. |
| | Font | Opens the Font dialog that enables you to configure the font, font style, font size and so on, to customize the look and feel of the application. |
| | Language | Autorun Analyzer is available in several languages. The 'Language' option in the 'View' menu enables you to select the language in which the application has to be rendered. |
| Users | | Enables to filter the autorun entries displayed depending on the user that started the application. Refer to '**Filtering Entries Based on Users**' for more details. |
| Help | | Opens the 'About' dialog of the Autorun Manager application. Refer to **About Autorun Analyzer** for more details. |

## Main Display Pane

The main display pane displays the list of all Start Up items as a table. Right clicking on an entry opens the context sensitive menu that enables to handle the entry. Refer to **Viewing and Handling Autorun Items** for more details.

## Information Pane

The Information Pane displays the complete details of the autorun entry selected from the Main Display Pane.

## Category Selection Pane

The Category Selection Pane enables to filter the autorun entries displayed depending on their category. Refer to Filtering Entries Based on Category for more details.

## Status Bar

The status bar at the bottom of the interface displays the current state of the application, currently logged-in user name, number of detected unsafe entries and the version of application that you are using.

Next: **Viewing and Handling Autorun Items**

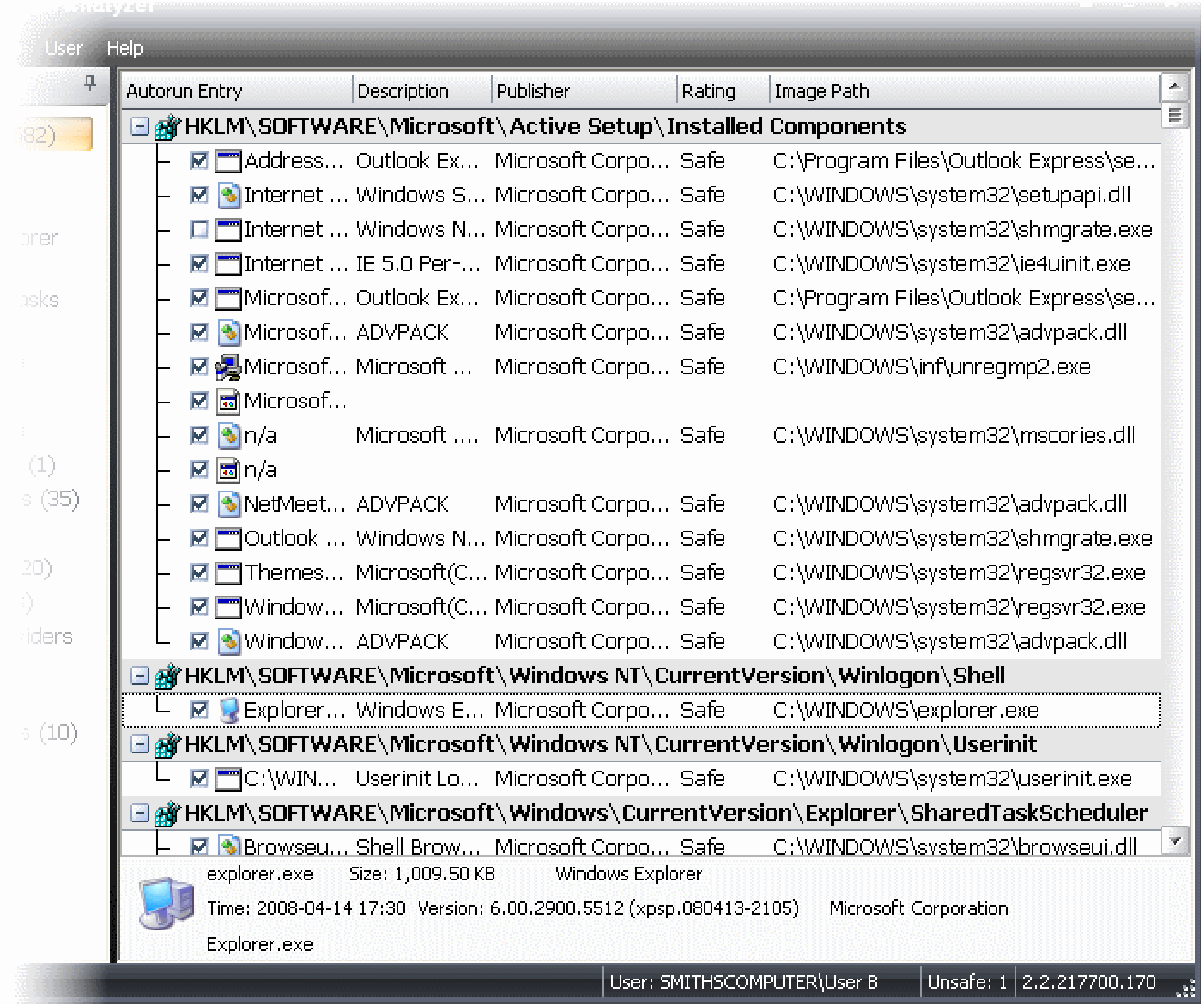
## 6.3. Viewing and Handling Autorun Items

The Autorun Analyzer allows you to manage autorun items that are loaded to your system during system start up. All autorun entries are displayed in a tree structure with their description, location, software publisher details and threat rating. Untrusted Autorun entries are highlighted for easy identification.

On selecting an autorun entry, the complete details like the parent application, installation date/time, version of the application, software publisher information are shown in the Information area beneath the main display pane for the entry.

You can filter the entries based on their categories and the users that has started them, by selecting the category from the Category Selection Pane  and the user from the  'User' menu in the file menu bar respectively.

You can perform various operations on any entry by selecting an entry and selecting an option from the 'Entry' menu in the file menu bar or right-clicking on an entry and selecting an option from the context sensitive menu. Also you can directly enable or disable an entry from the main display pane by selecting/deselecting the checkbox beside the entry.



| Autorun Entry | Description | Publisher | Rating | Image Path |
|---|---|---|---|---|
| **HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components** | | | | |
| ☑ Address… | Outlook Ex… | Microsoft Corpo… | Safe | C:\Program Files\Outlook Express\se… |
| ☑ Internet … | Windows S… | Microsoft Corpo… | Safe | C:\WINDOWS\system32\setupapi.dll |
| □ Internet … | Windows N… | Microsoft Corpo… | Safe | C:\WINDOWS\system32\shmgrate.exe |
| ☑ Internet … | IE 5.0 Per-… | Microsoft Corpo… | Safe | C:\WINDOWS\system32\ie4uinit.exe |
| ☑ Microsof… | Outlook Ex… | Microsoft Corpo… | Safe | C:\Program Files\Outlook Express\se… |
| ☑ Microsof… | ADVPACK | Microsoft Corpo… | Safe | C:\WINDOWS\system32\advpack.dll |
| ☑ Microsof… | Microsoft … | Microsoft Corpo… | Safe | C:\WINDOWS\inf\unregmp2.exe |
| ☑ Microsof… | | | | |
| ☑ n/a | Microsoft …. | Microsoft Corpo… | Safe | C:\WINDOWS\system32\mscories.dll |
| ☑ n/a | | | | |
| ☑ NetMeet… | ADVPACK | Microsoft Corpo… | Safe | C:\WINDOWS\system32\advpack.dll |
| ☑ Outlook … | Windows N… | Microsoft Corpo… | Safe | C:\WINDOWS\system32\shmgrate.exe |
| ☑ Themes… | Microsoft(C… | Microsoft Corpo… | Safe | C:\WINDOWS\system32\regsvr32.exe |
| ☑ Window… | Microsoft(C… | Microsoft Corpo… | Safe | C:\WINDOWS\system32\regsvr32.exe |
| ☑ Window… | ADVPACK | Microsoft Corpo… | Safe | C:\WINDOWS\system32\advpack.dll |
| **HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell** | | | | |
| ☑ Explorer… | Windows E… | Microsoft Corpo… | Safe | C:\WINDOWS\explorer.exe |
| **HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit** | | | | |
| ☑ C:\WIN… | Userinit Lo… | Microsoft Corpo… | Safe | C:\WINDOWS\system32\userinit.exe |
| **HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SharedTaskScheduler** | | | | |
| ☑ Browseu… | Shell Brow… | Microsoft Corpo… | Safe | C:\WINDOWS\system32\browseui.dll |

explorer.exe  Size: 1,009.50 KB  Windows Explorer
Time: 2008-04-14 17:30  Version: 6.00.2900.5512 (xpsp.080413-2105)  Microsoft Corporation
Explorer.exe

User: SMITHSCOMPUTER\User B  Unsafe: 1  2.2.217700.170

| Autorun Analyzer - Descriptions of Columns | |
|---|---|
| **Column** | **Description** |
| Autorun Entry | Displays the name of the Autorun Entry. Selecting/Deselecting the check box beside each name toggles the Autorun Item between 'Enabled' and 'Disabled' states. |
| Description | A brief description of the entry. |
| Publisher | The Software Publisher that has released the parent application. |

| | |
|---|---|
| Rating | Displays the result of the scanning performed on the item by Autorun Analyzer. Items identified as unsafe are shown highlighted for easy identification. |
| Image Path | Shows the installation path of the patent application or the loaded module. |

From this interface, you can:

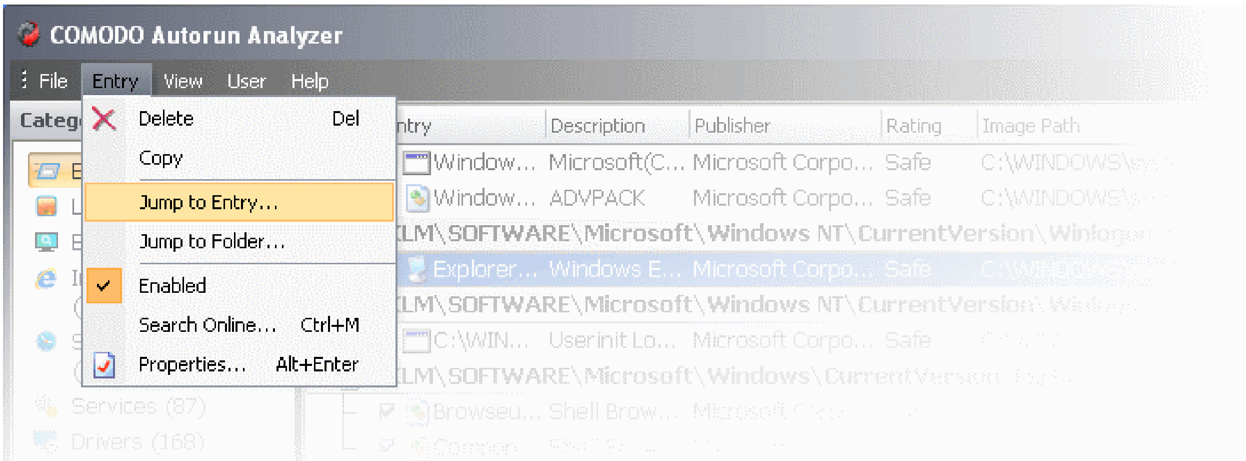
- **Handle the autorun items;**
- **View the autorun items based on categories**;
- **View the autorun items of other user accounts.**

## 6.3.1. Handling Autorun Items

Autorun Manager interface allows you to enable/disable autorun items, view the registry key associated with an item, view the parent application/module that has loaded the item and view the properties of the item. In cases where the item is found unsafe/untrusted or you do not want the item to be loaded during start-up in order to optimize your system's boot-up time and performance, you can remove the item from the start-up entries.

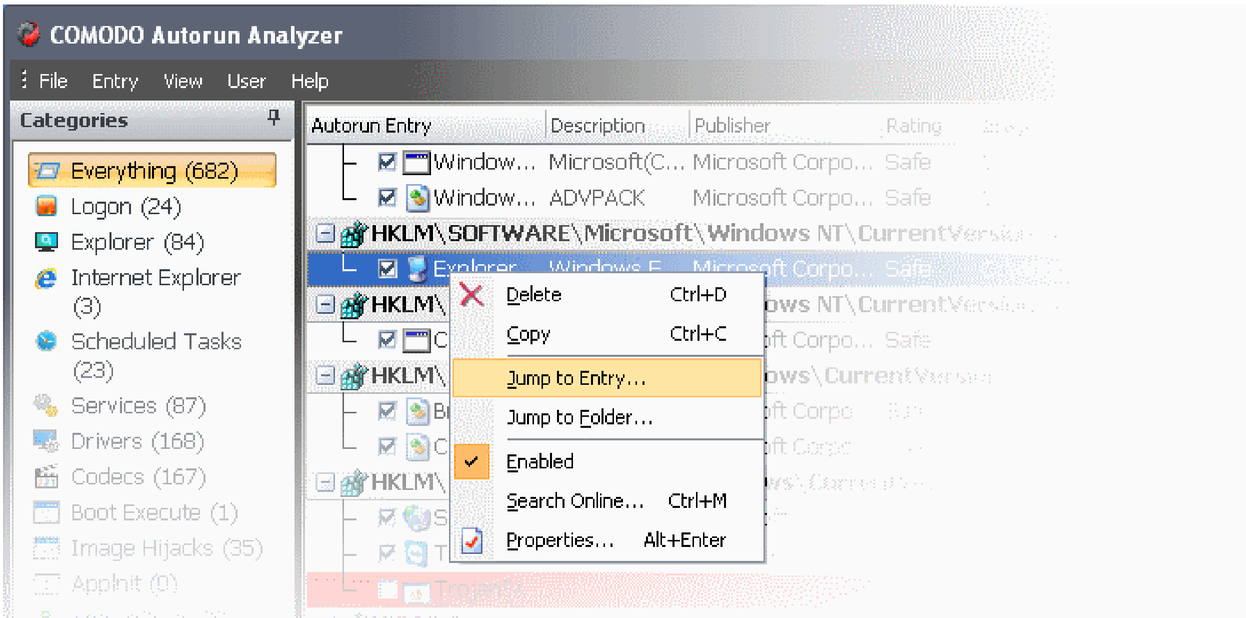
To manage an autorun item:

- Select the item from the main display pane click on the Entry menu from the file menu bar and select the option.



Or

- Right-click on the item and select the option from the context sensitive menu.

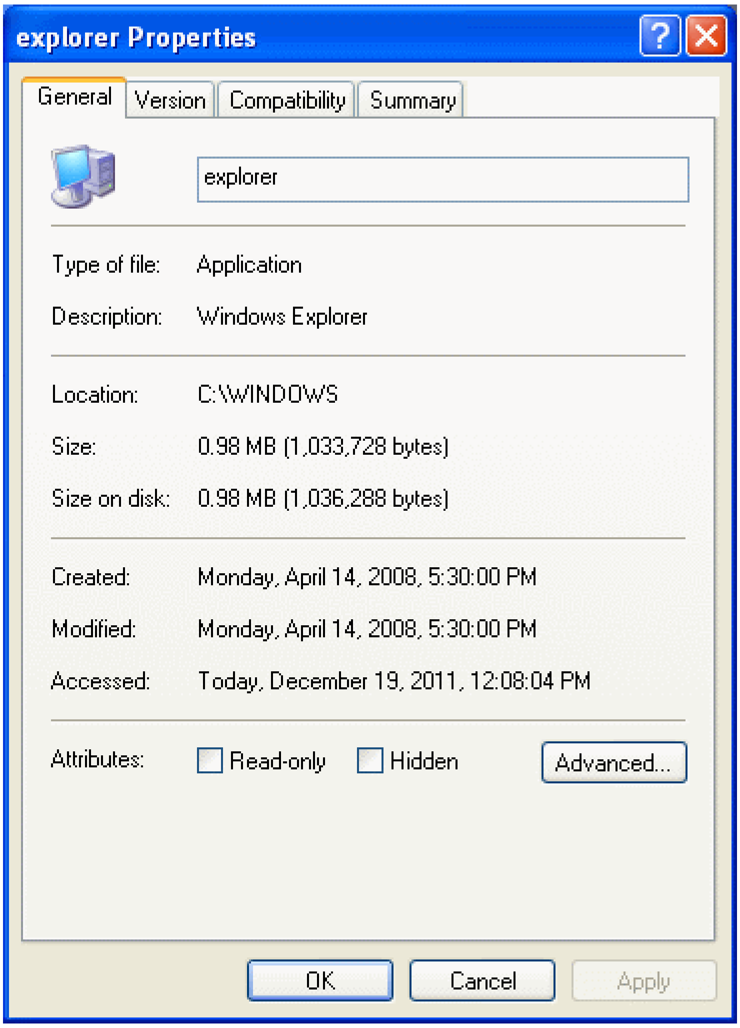


- **Delete** - Removes the selected item from the Start-up items. Removing an Autorun item just stops the parent application from loading into your system during start-up and does not remove the parent application. You can still start the application from the Windows Start Menu when required.

- **Copy** - Copies the selected row to clip-board of your system.
- **Jump to Entry** - Opens the selected entry in  Windows Registry Editor.
- **Jump to Folder** - Opens the folder containing the parent application or the module that loaded the autorun item  in Windows Explorer with the parent application or the module selected.
- **Enabled** - Toggles the selected autorun item between 'Enabled' and 'Disabled' states.

Tip: You can directly enable or disable an entry from the main display pane by selecting/deselecting the checkbox beside the entry.

- **Search Online** - Opens the default web browser of your system with the search engine specified and searches for information on the selected autorun item on the web.
- **Properties** - Opens the Properties dialog of the selected autorun item.



explorer

Type of file: Application

Description: Windows Explorer

Location: C:\WINDOWS

Size: 0.98 MB (1,033,728 bytes)

Size on disk: 0.98 MB (1,036,288 bytes)

Created: Monday, April 14, 2008, 5:30:00 PM

Modified: Monday, April 14, 2008, 5:30:00 PM

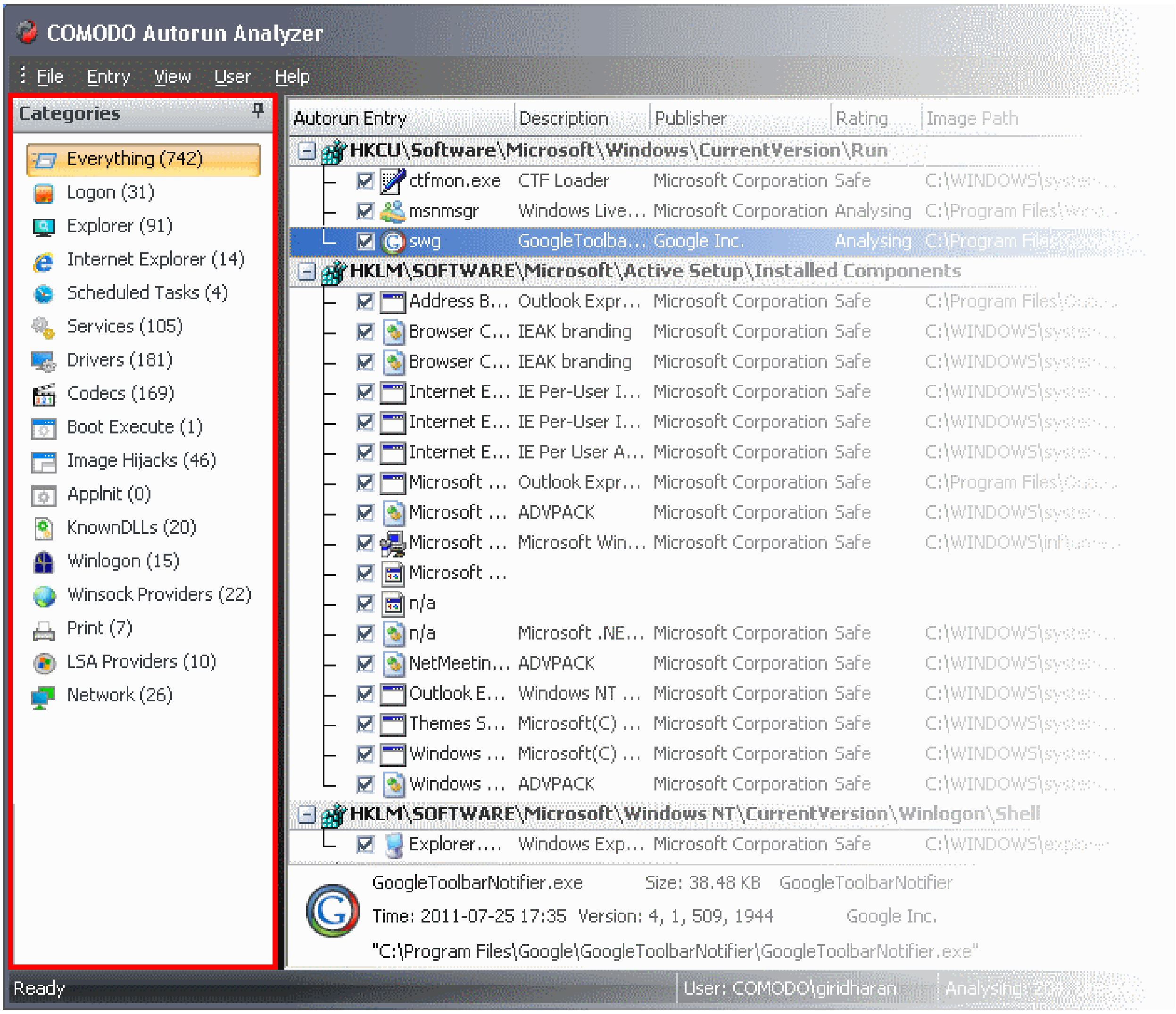
Accessed: Today, December 19, 2011, 12:08:04 PM

Attributes: □ Read-only □ Hidden

## 6.3.2. Filtering Entries based on Categories

The left hand side pane of the Autorun Analyzer interface displays a list of various  types of the autorun items and the program groups. The number of items loaded in the respective category is displayed within parentheses beside each category name.

By default, all the autorun items loaded, are displayed in the main display pane. If you want to analyze the autorun items based on their categories or to analyze the items loaded by various program groups, you can filter the items , by selecting the respective category from the list.



- Everything (742)
- Logon (31)
- Explorer (91)
- Internet Explorer (14)
- Scheduled Tasks (4)
- Services (105)
- Drivers (181)
- Codecs (169)
- Boot Execute (1)
- Image Hijacks (46)
- AppInit (0)
- KnownDLLs (20)
- Winlogon (15)
- Winsock Providers (22)
- Print (7)
- LSA Providers (10)
- Network (26)

| Autorun Entry | Description | Publisher | Rating | Image Path |
|---|---|---|---|---|
| HKCU\Software\Microsoft\Windows\CurrentVersion\Run | | | | |
| ☑ ctfmon.exe | CTF Loader | Microsoft Corporation | Safe | C:\WINDOWS\syste... |
| ☑ msnmsgr | Windows Live... | Microsoft Corporation | Analysing | C:\Program Files\... |
| ☑ swg | GoogleToolba... | Google Inc. | Analysing | C:\Program Files\... |
| HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components | | | | |
| ☑ Address B... | Outlook Expr... | Microsoft Corporation | Safe | C:\Program Files\... |
| ☑ Browser C... | IEAK branding | Microsoft Corporation | Safe | C:\WINDOWS\syste... |
| ☑ Browser C... | IEAK branding | Microsoft Corporation | Safe | C:\WINDOWS\syste... |
| ☑ Internet E... | IE Per-User I... | Microsoft Corporation | Safe | C:\WINDOWS\syste... |
| ☑ Internet E... | IE Per-User I... | Microsoft Corporation | Safe | C:\WINDOWS\syste... |
| ☑ Internet E... | IE Per User A... | Microsoft Corporation | Safe | C:\WINDOWS\syste... |
| ☑ Microsoft ... | Outlook Expr... | Microsoft Corporation | Safe | C:\Program Files\... |
| ☑ Microsoft ... | ADVPACK | Microsoft Corporation | Safe | C:\WINDOWS\syste... |
| ☑ Microsoft ... | Microsoft Win... | Microsoft Corporation | Safe | C:\WINDOWS\inf\... |
| ☑ Microsoft ... | | | | |
| ☑ n/a | | | | |
| ☑ n/a | Microsoft .NE... | Microsoft Corporation | Safe | C:\WINDOWS\syste... |
| ☑ NetMeetin... | ADVPACK | Microsoft Corporation | Safe | C:\WINDOWS\syste... |
| ☑ Outlook E... | Windows NT ... | Microsoft Corporation | Safe | C:\WINDOWS\syste... |
| ☑ Themes S... | Microsoft(C) ... | Microsoft Corporation | Safe | C:\WINDOWS\syste... |
| ☑ Windows ... | Microsoft(C) ... | Microsoft Corporation | Safe | C:\WINDOWS\syste... |
| ☑ Windows ... | ADVPACK | Microsoft Corporation | Safe | C:\WINDOWS\syste... |
| HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell | | | | |
| ☑ Explorer.... | Windows Exp... | Microsoft Corporation | Safe | C:\WINDOWS\exp... |

GoogleToolbarNotifier.exe Size: 38.48 KB GoogleToolbarNotifier
Time: 2011-07-25 17:35 Version: 4, 1, 509, 1944 Google Inc.
"C:\Program Files\Google\GoogleToolbarNotifier\GoogleToolbarNotifier.exe"

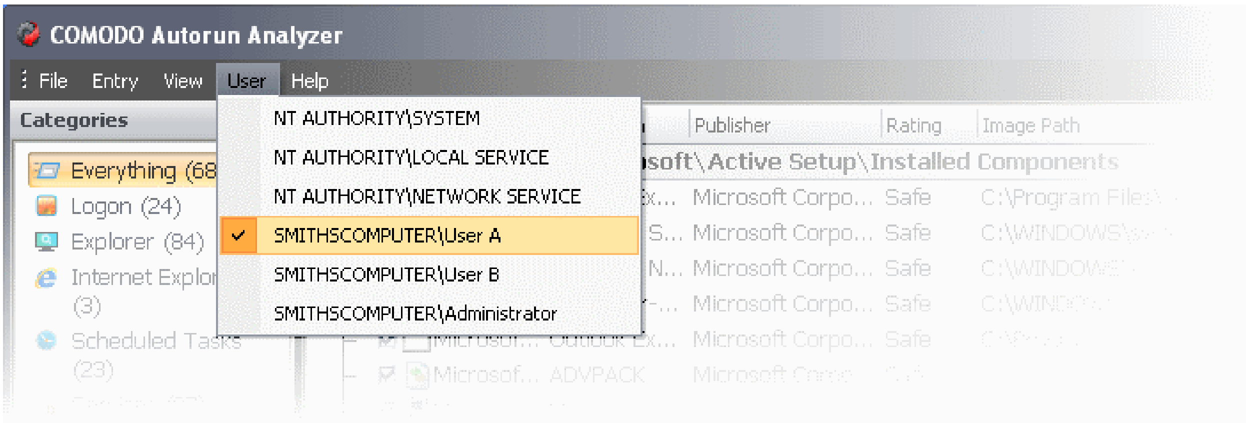
Ready | User: COMODO\giridharan | Analysing: ...

| Descriptions of Categories | |
|---|---|
| **Category** | **Description** |
| Everything | Displays all the autorun items in the main display pane. |
| Logon | Displays only  the autorun items identified from standard autostart locations such as the Startup folder for all users, the Registry Run keys, and standard application launch locations. |
| Explorer | Displays only the Explorer shell extensions from various installed applications, browser helper objects (BHO), explorer toolbars, active setup executions and shell execute hooks. |
| Internet Explorer | Displays only the BHOs, Internet Explorer toolbars and extensions. |
| Scheduled Tasks | Displays the modules loaded by tasks and applications scheduled from Windows Task Scheduler. |
| Services | Displays the modules loaded as Windows Services. |
| Drivers | Displays only the kernel-mode drivers that are in currently enabled on the system. |
| Codecs | Displays the autorun items loaded by various coders-decoders used for handling media files like audio and video files. |
| Boot Execute | Displays the autorun items loaded by applications, services and commands executed during the time |

| | |
|---|---|
| | period between the system boot-up and the user log-on. |
| Image Hijacks | Displays the modules loaded by image file execution options of various applications installed in your system. Most of the malware modify the image file execution options of a legitimate application and make themselves to run when the real application is started. Autorun Analyzer enables you to identify such illegitimate autorun items loaded by malware that affect the image file execution options of legitimate applications and to disable / remove them. |
| AppInit | Displays the application initialization Dynamic Link Library (DLL) modules loaded as autorun items. |
| KnownDLLS | Displays the DLL modules loaded by Windows for the start-up applications that reference those DLLs. |
| Winlogon | Displays the DLL modules registered for Winlogon notification of logon events. |
| Winsock Providers | Displays the DLL modules registered for Winsock protocols, including Winsock service providers.<br>An anti-malware software do not scan Winsock Service Providers as it is treated as a safe zone. Taking advantage of this, some malware enter into your system as a  Winsock Service Provider. But Autorun Analyzer can identify the DLL modules loaded by Winsock Service Providers and notify you if they are untrusted. It also enables you to remove those untrusted modules from your system. |
| Print | Displays the DLLs load into the print spoolers configured as services to start with Windows. Some malware find their entry through Print spooling service to start themselves automatically during system start-up. |
| LSA Providers | Displays the DLL modules registered by Local Security Authority (LSA) authentication, notification and security packages. |
| Network | Displays the DLL modules loaded by network connection services. |

### 6.3.3. Viewing Autorun Items for other User Accounts

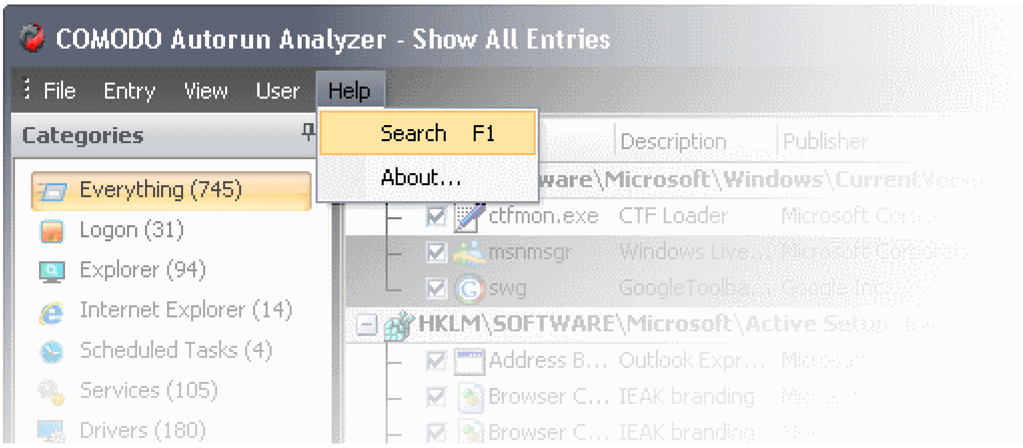
By default, Autorun Analyzer displays the autorun items loaded as per the start-up configuration of the currently logged-in user account. The 'Users' menu in the file menu bar enables you to view the autorun items for the other user accounts registered in your system.



- Selecting a user name from the User menu will display the autorun items configured for that user account.

## 6.4. 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 Autorun Analyzer in your system.

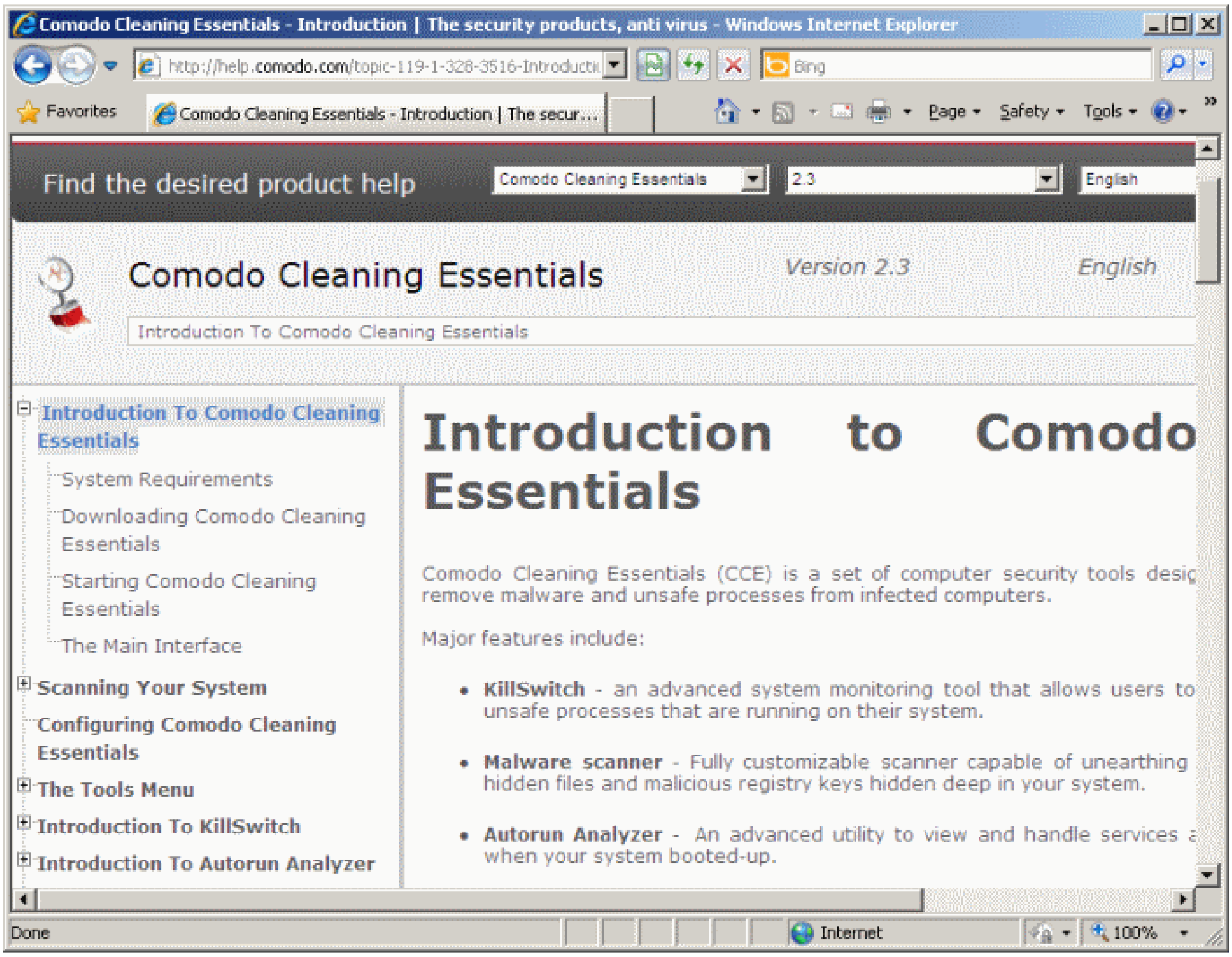

COMODO Autorun Analyzer - Show All Entries
File
Entry
View
User
Help
Search F1
About...
Categories
Everything (745)
Logon (31)
Explorer (94)
Internet Explorer (14)
Scheduled Tasks (4)
Services (105)
Drivers (180)
Description
Publisher
ware\Microsoft\Windows\CurrentVer...
ctfmon.exe CTF Loader Microsoft Cor...
msnmsgr Windows Live... Microsoft Corporati...
swg GoogleToolbar... Google Inc.
HKLM\SOFTWARE\Microsoft\Active Setup
Address B... Outlook Expr... Micros...
Browser C... IEAK branding
Browser C... IEAK branding

Clicking on the Help menu has the two options:

- Search
- About

## 6.4.1. 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.


Comodo Cleaning Essentials - Introduction | The security products, anti virus - Windows Internet Explorer
http://help.comodo.com/topic-119-1-328-3516-Introducti
Bing
Favorites
Comodo Cleaning Essentials - Introduction | The secur...
Page
Safety
Tools
Find the desired product help
Comodo Cleaning Essentials
2.3
English
Done
Internet
100%

Comodo Cleaning Essentials

Version 2.3

English

Introduction To Comodo Cleaning Essentials

- Introduction To Comodo Cleaning Essentials
  - System Requirements
  - Downloading Comodo Cleaning Essentials
  - Starting Comodo Cleaning Essentials
  - The Main Interface
- Scanning Your System
- Configuring Comodo Cleaning Essentials
- The Tools Menu
- Introduction To KillSwitch
- Introduction To Autorun Analyzer

Introduction to Comodo Essentials

Comodo Cleaning Essentials (CCE) is a set of computer security tools desic remove malware and unsafe processes from infected computers.

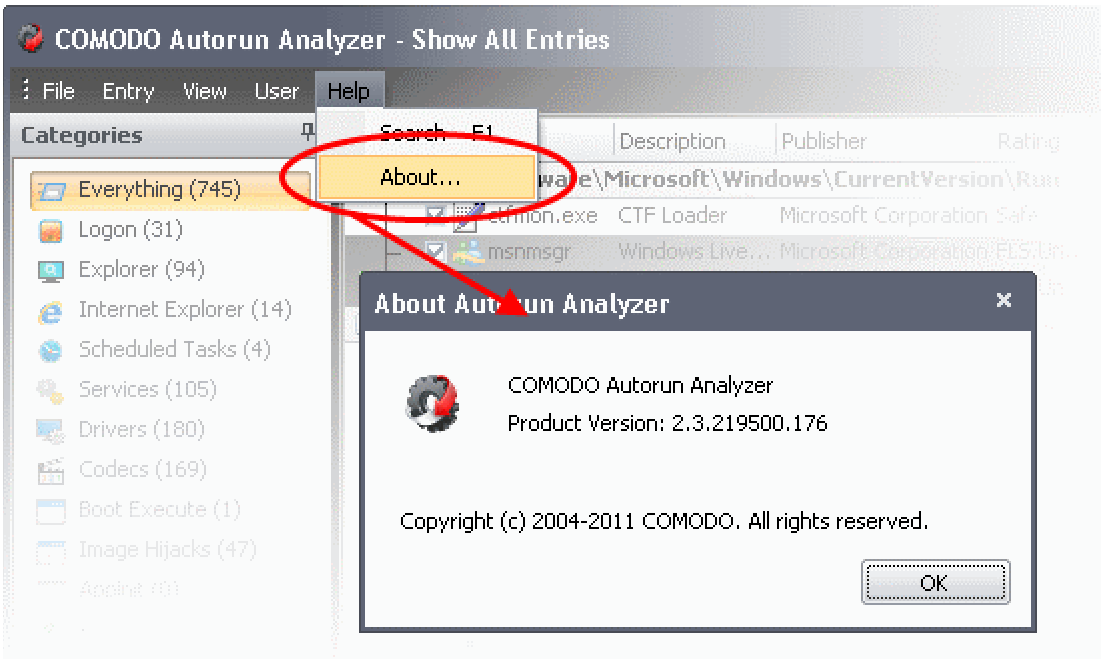
Major features include:

- **KillSwitch** - an advanced system monitoring tool that allows users to unsafe processes that are running on their system.
- **Malware scanner** - Fully customizable scanner capable of unearthing hidden files and malicious registry keys hidden deep in your system.
- **Autorun Analyzer** - An advanced utility to view and handle services a when your system booted-up.

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

## 6.4.2. About Autorun Analyzer

The Help menu in the file menu bar opens the 'About' dialog of Comodo Autorun Analyzer.



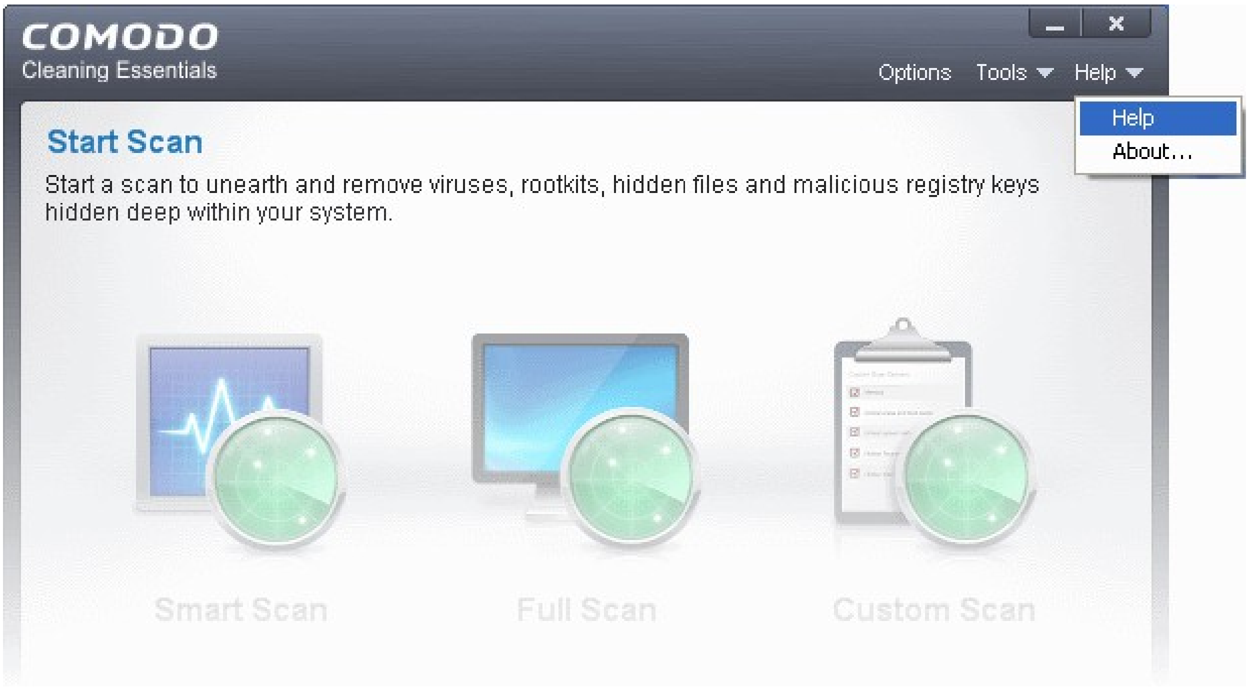
COMODO Autorun Analyzer
Product Version: 2.3.219500.176

Copyright (c) 2004-2011 COMODO. All rights reserved.

The 'About' dialog displays the version Number of Comodo Autorun Analyzer and the copyright information.

# 7.Help and About Details

The Help menu at the top right corner of the CCE main interface enables you to access the online help guide and view the About dialog of the application.



Start Scan

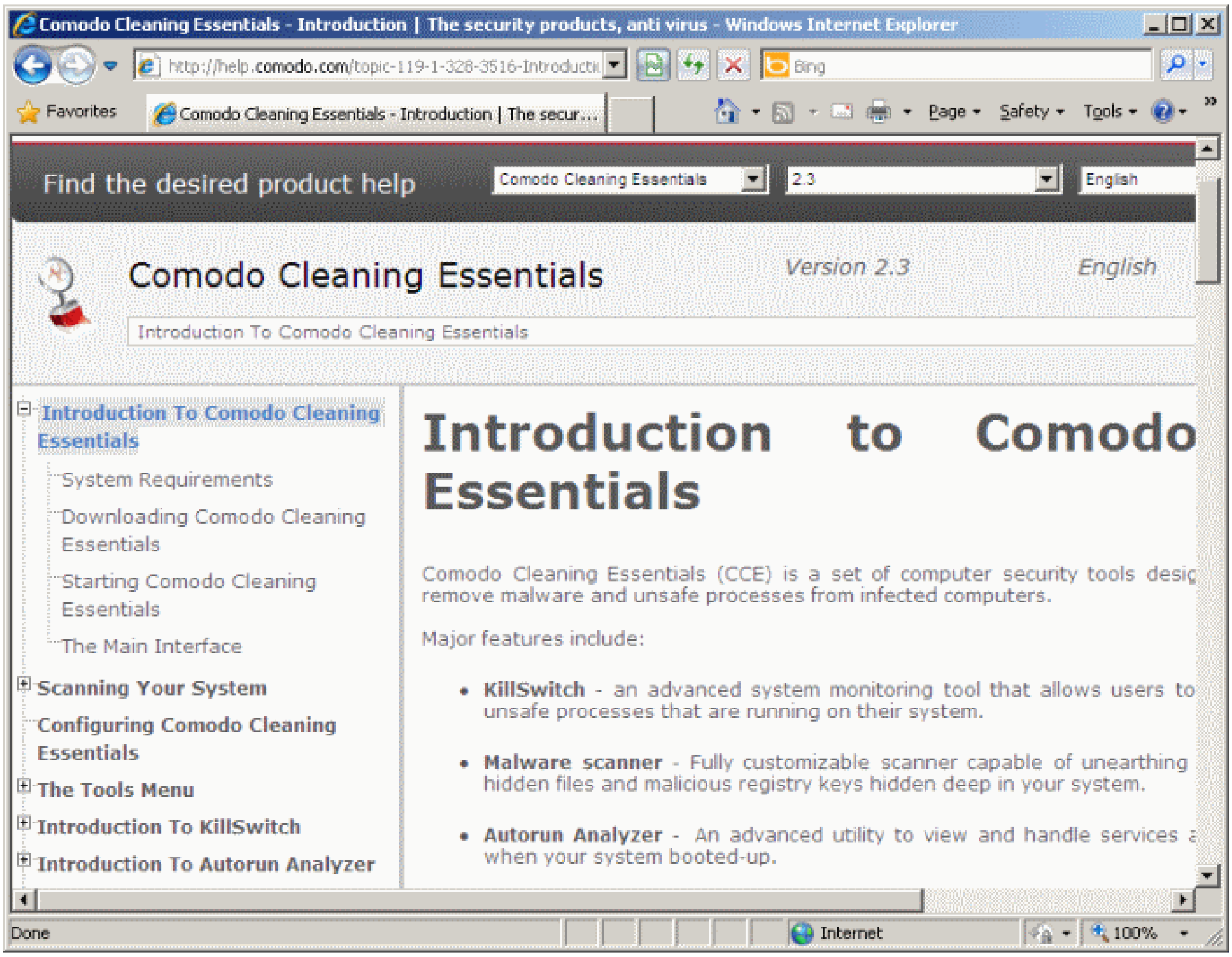
Start a scan to unearth and remove viruses, rootkits, hidden files and malicious registry keys hidden deep within your system.

Click the links below for more information:

- **Help**
- **About**

# 7.1. Help

Clicking the 'Help' 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.


Comodo Cleaning Essentials - Introduction | The security products, anti virus - Windows Internet Explorer
http://help.comodo.com/topic-119-1-328-3516-Introducti
Bing
Favorites
Comodo Cleaning Essentials - Introduction | The secur...
Page
Safety
Tools
Find the desired product help
Comodo Cleaning Essentials
2.3
English
Comodo Cleaning Essentials
Version 2.3
English
Introduction To Comodo Cleaning Essentials
Introduction To Comodo Cleaning Essentials
System Requirements
Downloading Comodo Cleaning Essentials
Starting Comodo Cleaning Essentials
The Main Interface
Scanning Your System
Configuring Comodo Cleaning Essentials
The Tools Menu
Introduction To KillSwitch
Introduction To Autorun Analyzer
Done
Internet
100%

**Introduction to Comodo Essentials**

Comodo Cleaning Essentials (CCE) is a set of computer security tools desig remove malware and unsafe processes from infected computers.

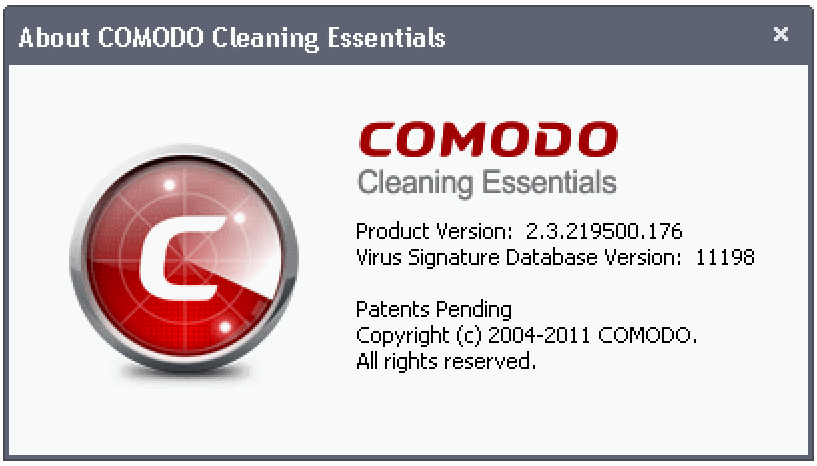
Major features include:

- **KillSwitch** - an advanced system monitoring tool that allows users to unsafe processes that are running on their system.
- **Malware scanner** - Fully customizable scanner capable of unearthing hidden files and malicious registry keys hidden deep in your system.
- **Autorun Analyzer** - An advanced utility to view and handle services a when your system booted-up.

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

# 7.2. About

Clicking 'About' from the 'Help' menu opens the the 'About' dialog of Comodo Cleaning Essentials.


About COMODO Cleaning Essentials

COMODO
Cleaning Essentials

Product Version: 2.3.219500.176
Virus Signature Database Version: 11198

Patents Pending
Copyright (c) 2004-2011 COMODO.
All rights reserved.

The 'About' dialog version of Comodo Cleaning Essentials, version of virus database that is in your computer and the copyright information.

# 8. Using the Command Line Interface

Comodo Cleaning Essentials allows users to execute smart scans, custom scans and virus database updates from the Windows command line interface..

**To access the Windows command line interface**

- Click Start > All Programs > Accessories > Command Prompt.

  or

- Click Start > Run, type 'cmd' in the Run interface and click 'OK'.

Click the links below for more details on the tasks executed from the Command Line Interface:

- **Running a Smart Scan from the Command Line Interface**
- **Running a Custom Scan from the Command Line Interface**
- **Running a Virus Database Update Task from the Command Line Interface**
- **Viewing Help**

## 8.1. Running a Smart Scan from the Command Line Interface

- Open the Windows command line interface
- Specify the command in the following format

  <file path>/ <executable> -smart

  For example, if the folder containing Comodo Cleaning Essentials files is stored in C:\Comodo, the command would be:

  C:\Comodo\CCE\CCE **- smart**

**Note:** The Commands are not case sensitive.

The CCE application will start scanning, reboot and clean threats automatically without user interaction.

## 8.2. Running a Custom Scan from the Command Line Interface

- Open the Windows command line interface
- Specify the command in the following format

```
<file path>/ <executable> -scan parameter1 - scan parameter2 -scan parameter3...
```

For example, if the folder containing Comodo Cleaning Essentials files is stored in C:\Comodo, the command would be:

```
C:\Comodo\CCE\CCE -s “<scan attribute1>;<scan attribute1>” -o “<scan option1>;<scan option1>” -d “<drive letter>” -p “<file path>” -shift
```

- The parameters -o, -d and -p are optional
- The parameters and arguments are explained in the following tables:

### Scan Attributes

| Scan Attributes | |
|---|---|
| **Argument** | **Description** |
| m | Scan memory on start. |
| c | Scan critical areas and boot sectors. |
| f | Scan selected drivers for hidden files/folders.<br>Note: if you use "f" parameter, you must add -d "drive" (**explained below**). |
| r | Scan hidden registry objects. |
| nv | Don't scan for viruses. |

**Syntax**

```
-s “<scan attribute1>;<scan attribute1>”...
```

**Examples**:

To run a scan with the attributes 'scan memory on start', 'Scan critical areas and boot sectors' and 'Scan selected drivers for hidden files/folders' on drive 'c:', then the parameters are to be entered as:

```
C:\Comodo\CCE\CCE  -s"m;c;f;r" -d "c"
```

To run a full scan of your system, just enter

```
C:\Comodo\CCE\CCE -s
```

### Scan Options

| Scan Options | |
|---|---|
| **Argument** | **Description** |
| ARCHIVE | Scan archive files (e.g. *.zip, *.rar). |
| HOOK | Restore any kernel hooks before the scan. |

| | |
|---|---|
| SUSMBR | Scan selected drivers for hidden files/folders.Scan suspicious MBR modifications in full scan (Valid for single boot computers only). |
| MODMBR | Report all MBR modifications in full scan(Valid for single boot computers only). |
| RESTORE | Create a windows restore point before performing the scan. |
| CAMAS | Scan unknown processes in memory with CAMAS. |
| CAMASTIME=NN | CAMAS timeout seconds. |
| Heur=N | Heuristics Scanning level.<br>• 0 = off;<br>• 1 = low;<br>• 2 = middle;<br>• 3 = high. |
| MAX=20 | Do not scan files larger than 20(MB). |
| LOGLEVEL=N | Specifies the log level.<br>• 0 = disable log;<br>• 1 = show threats log;<br>• 2 = show full log. |

**Syntax**

```
-o “<scan option1>;<scan option1>”
```

**Examples**:

To run a scan drive 'C:' with the options 'Scan archive files', 'Report all MBR modifications in full scan' and 'Scan unknown processes in memory with CAMAS' with CAMAS time out period of 300 seconds

```
C:\Comodo\CCE\CCE -s -o "ARCHIVE;MODMBR;CAMAS;CAMASTIME=300  -d "c"
```

## Scan Drives

The hard disk drive partition(s) to be scanned can be specified as arguments for the parameter **-d**.

**Syntax**

```
-d “<drive letter 1>;<drive letter 2>... ”
```

**Examples**:

To run a scan drive partitions  'C: and 'D:'

```
C:\Comodo\CCE\CCE -s -d "c;d"
```

## Scan Specific Folders/Files

To scan specific file(s)/folder(s), you can enter the path(s) of it/them as argument to the parameter **-p**.

**Syntax**

```
-p “<file path 1>;<file path 2>... ”
```

**Examples**:

To scan the folder 'C:\Program Files'

```
C:\Comodo\CCE\CCE  -s -p “C:\Program Files”
```

To run a scan files 'note1.txt' and 'note2.txt' in the folder 'C:\My Documents'

```
C:\Comodo\CCE\CCE  -s -p “C:\My Documents\note1.txt;C:\My Documents\note2.txt”
```

### Aggressive Mode Scanning

To start the scanning in aggressive mode, include the parameter -shift to the command.

**Example:**

```
C:\Comodo\CCE\CCE -s -shift
```

The CCE application will start scanning, reboot and clean threats automatically without user interaction.

## 8.3. Running a Virus Database Update Task from the Command Line Interface

- Open the Windows command line interface
- Specify the command in the following format

  <file path>/ <executable> -u

  For example, if the folder containing Comodo Cleaning Essentials files is stored in C:\Comodo, the command would be:

```
C:\Comodo\CCE\CCE -u
```

The local virus database will be updated.

**Note**: You should be connected to Internet in order to receive the updates.

## 8.4. Viewing Help

- Open the Windows command line interface
- Specify the command in the following format

  <file path>/ <executable> -help

  For example, if the folder containing Comodo Cleaning Essentials files is stored in C:\Comodo, the command would be:

```
C:\Comodo\CCE\CCE -help
```

The CCE online help guide hosted at **http://help.comodo.com/** will open.

# 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.**

1255 Broad Street
STE 100
Clifton, NJ 07013
United States
Tel: +1.877.712.1309
Tel: +1.703.637.9361
Email: **EnterpriseSolutions@Comodo.com**

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