COMODO
Creating Trust Online®

Comodo
Cleaning Essentials

Software Version 11.0

User Guide

Guide Version 11.0.032619

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Table of Contents

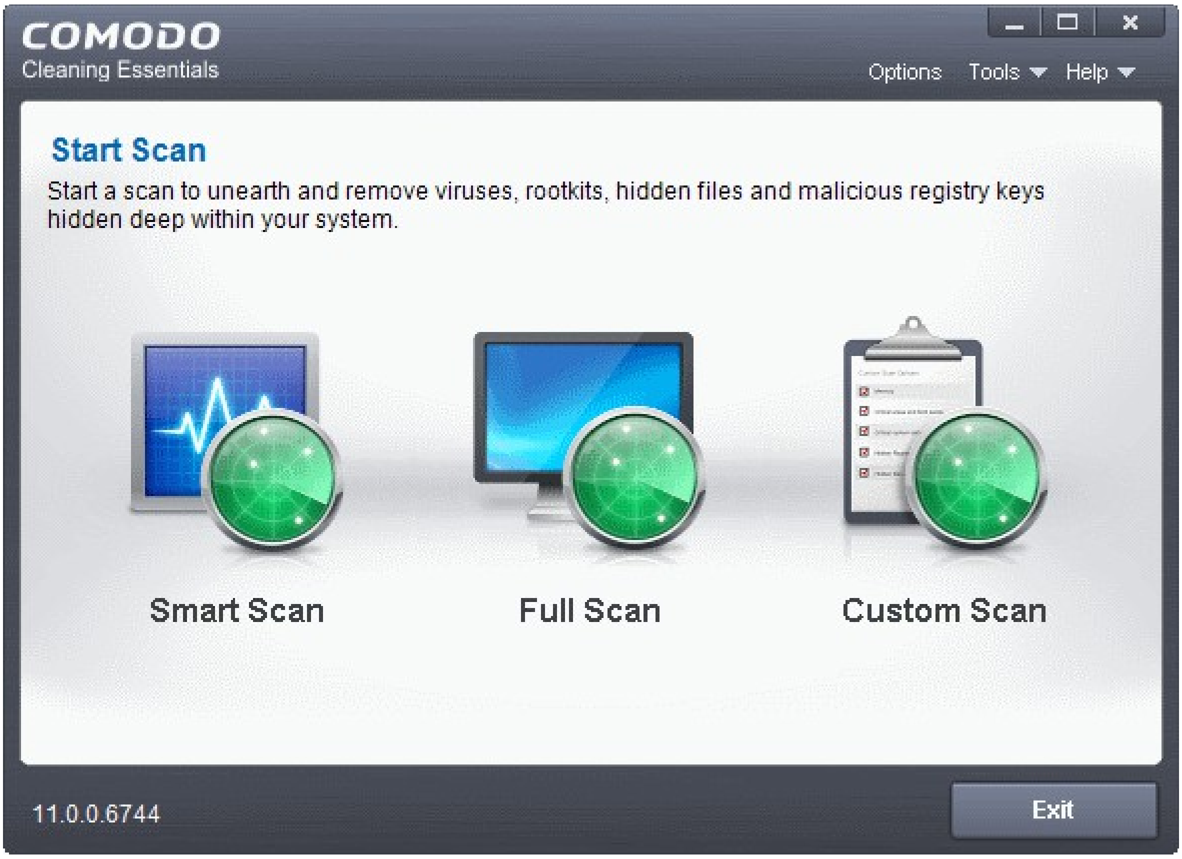
1. Introduction to Comodo Cleaning Essentials

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 lets you identify, monitor and stop any unsafe processes that are running on their system.
- **Malware scanner -** Fully customizable scanner capable of revealing and eliminating viruses, rootkits, hidden files and malicious registry keys hidden deep in your computer.
- **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 existing processes running under explorer, and explorer itself 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.
    - **Download Comodo Cleaning Essentials** - How to get CCE.
    - **Start 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, **Configure 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.
    - **Manage Quarantined Items** - How to manage and restore quarantined files.
    - **Manage Trusted Vendors** - How to add or remove vendors to/from the Trusted Vendor List.
    - **Import Antivirus Database** - How to import virus database from local storage or from network computer.
    - **Check 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
    - **Start KillSwitch** - How to start the KillSwitch tool
    - **The Main Interface** - Description of menus and options in the main interface
    - **View and Handle Processes, Applications and Services -** explains how to view the list of currently running processes, applications and services and handle them
        - **Processes**
        - **Applications**
        - **Services**
    - **View and Handle Network Connections and Usage** - explains how to view the details of currently active network connection and handle it
        - **Network Connections**
        - **Network Utilization**
    - **Configure KillSwitch** - Explains how to configure the overall behavior of KillSwitch
    - **KillSwitch Tools** - Explains how to use the tools in KillSwitch
        - **View System Information**
        - **Repair Windows Settings and Features**
        - **Analyze Program Usage**
        - **Search for handles or DLLs**

        - **Verify Authenticity of Applications**
        - **Bootlog and Handle Modules**
        - **Run Programs from Command Line Interface**
        - **View KillSwitch Logs**
        - **Find Process of Active Window**
        - **Manage 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.
    - **Start Autorun Analyzer** - How to start the Autorun Analyzer tool.
    - **The Main Interface** - Description of menus and options in the main interface.
    - **View 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, **Use the Command Line Interface** - Explanation on how to run various tasks of CCE application from Windows command line interface
    - **Run a Smart Scan from the Command Line Interface** - How to run a Smart Scan
    - **Run a Custom Scan from the Command Line Interface** - How to run a Custom Scan
    - **Run a Virus Database Update Task from the Command Line Interface** - How to update local virus database
    - **View Help** - How to view online help guide of CCE application.

1.1. System Requirements

To ensure optimal performance of Comodo Cleaning Essentials, please make sure your PC meets the following minimum requirements:

- Windows 10 (Both 32-bit and 64-bit versions), 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. Download Comodo Cleaning Essentials

CCE is available in 32bit and 64 bit versions for Windows XP, Vista, Windows 7 and Windows 10, and can be downloaded from the following locations:

32-Bit:

http://download.comodo.com/cce/download/setups/cce_public_x86.zip

64-Bit:

http://download.comodo.com/cce/download/setups/cce_public_x64.zip

Download the setup file then run CCE.exe to start using the application. No installation is required, but the latest virus definitions will be downloaded on startup.

1.3. Start Comodo Cleaning Essentials

CCE is a portable application which does not require installation. You can even run it directly from removable media such as a USB key.

You can start CCE in two modes, depending on the infection level of your computer:

- **Normal Mode**
- **Aggressive Mode**

Normal Mode

In normal mode, CCE scans your computer for malware, viruses and rootkits without terminating any currently running processes.

To start the CCE application in normal mode

- Navigate to the folder containing the CCE files.
- Double-click on the CCE.exe file.

Aggressive Mode

In aggressive mode, CCE terminates all existing processes running under explorer (and explorer itself) so it can perform a deep system scan.

> **Warning**: Make sure you have saved everything you need before you run CCE in this mode. Aggressive mode will close all running applications, and will close this help page too.

- Killing explorer leaves you at least temporarily without a desktop and start menu.
- If required, you can manually start explorer by pressing the Windows start button + 'R' then typing 'explorer.exe' in the 'Open' text box.
- Please note that starting explorer.exe may restart viruses if they are registered as explorer autoruns. You can check this with the '**Autoruns**' tool.

Start CCE in aggressive mode

- Locate CCE.exe on your local or removable drive
- Press and hold the 'Shift' key and double-click on CCE.exe

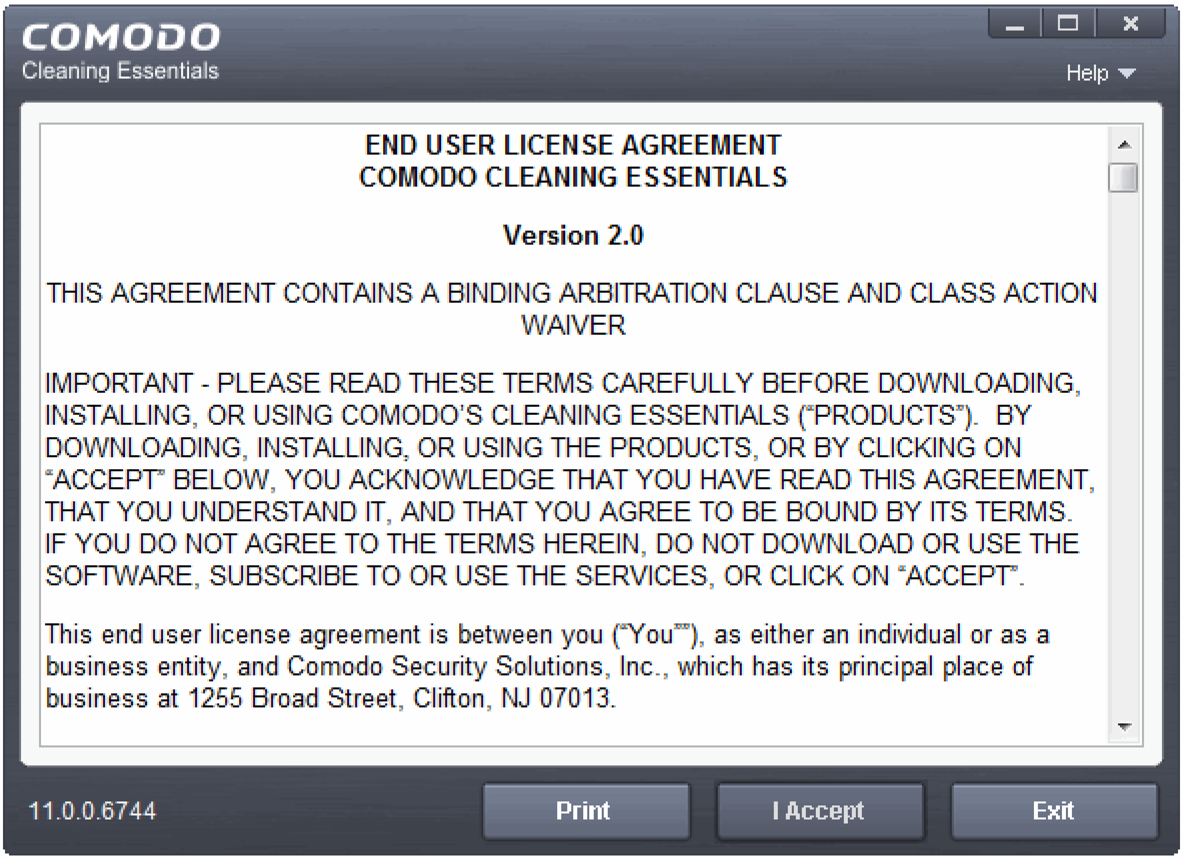
If you are starting CCE from Comodo Internet Security (CIS), then you can open CCE in aggressive mode as follows:

- Navigate to the CIS installation folder (C:\Program Files\COMODO\COMODO Internet Security)
- Press and hold the 'Shift' key and double-click on CCE.exe

OR

- Open CIS (double-click on the CIS tray icon)
- Click 'Tasks' > 'Advanced Tasks'
- Press and hold the 'Shift' key and click on 'Clean Endpoint'

You will be asked to accept the end user license agreement (EULA) the first time you run the app:



END USER LICENSE AGREEMENT
COMODO CLEANING ESSENTIALS

Version 2.0

THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE AND CLASS ACTION WAIVER

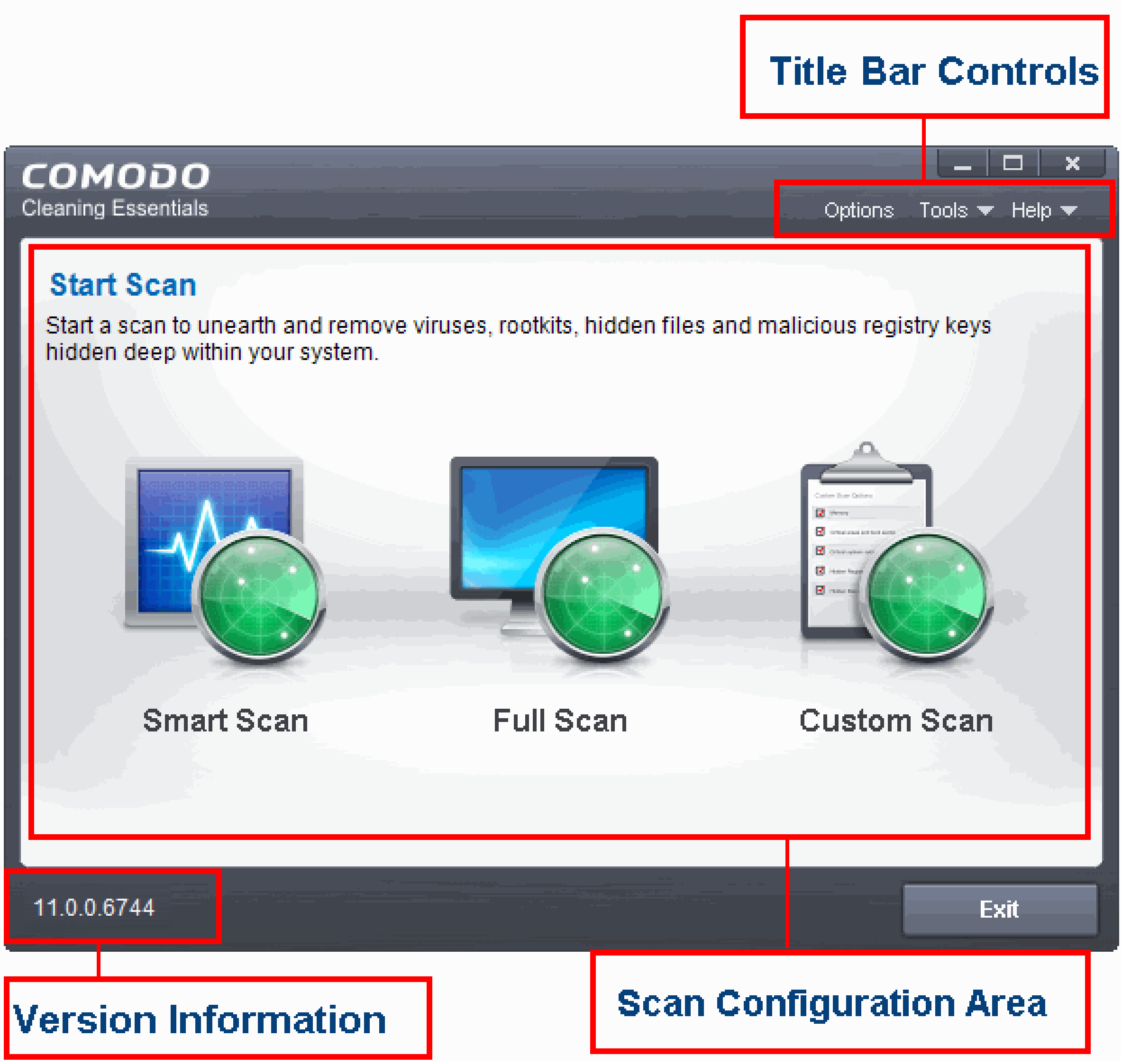
IMPORTANT - PLEASE READ THESE TERMS CAREFULLY BEFORE DOWNLOADING, INSTALLING, OR USING COMODO'S CLEANING ESSENTIALS ("PRODUCTS"). BY DOWNLOADING, INSTALLING, OR USING THE PRODUCTS, OR BY CLICKING ON "ACCEPT" BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU 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 "ACCEPT".

This end user license agreement is between you ("You""), as either an individual or as a business entity, and Comodo Security Solutions, Inc., which has its principal place of business at 1255 Broad Street, Clifton, NJ 07013.

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

1.4. The Main Interface

Comodo Cleaning Essentials' streamlined interface provides fingertip access to 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 lets you run in-depth malware scans on your system. You can run the following types of scan:

- **Smart Scan** - A targeted scan of the most important areas of your computer. Areas scanned include system memory, auto-run entries, hidden services, registry keys, boot sectors, and other critical areas.
- **Full Scan** - Scans every file and folder on your system.
- **Custom Scan** - Create your own scan of specific files/folder or drives.

Title Bar Controls

The top-right of the application contains the following items:

- **Options** - Configure various settings in the application.
- **Tools** - Manage quarantined items, trusted vendors, and the 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, you can see the version information of the software

2. Scan Your System

Comodo Cleaning Essentials allows you to perform various types of scan on your computer. These include a smart scan of critical areas in your computer, a full system scan of every file and folder, or a custom scan of just the areas you want to scan.

You can also scan an individual folder or a file by dragging and dropping it onto the CCE interface.

See the following sections for help with each scan type:

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

2.1. Smart Scan

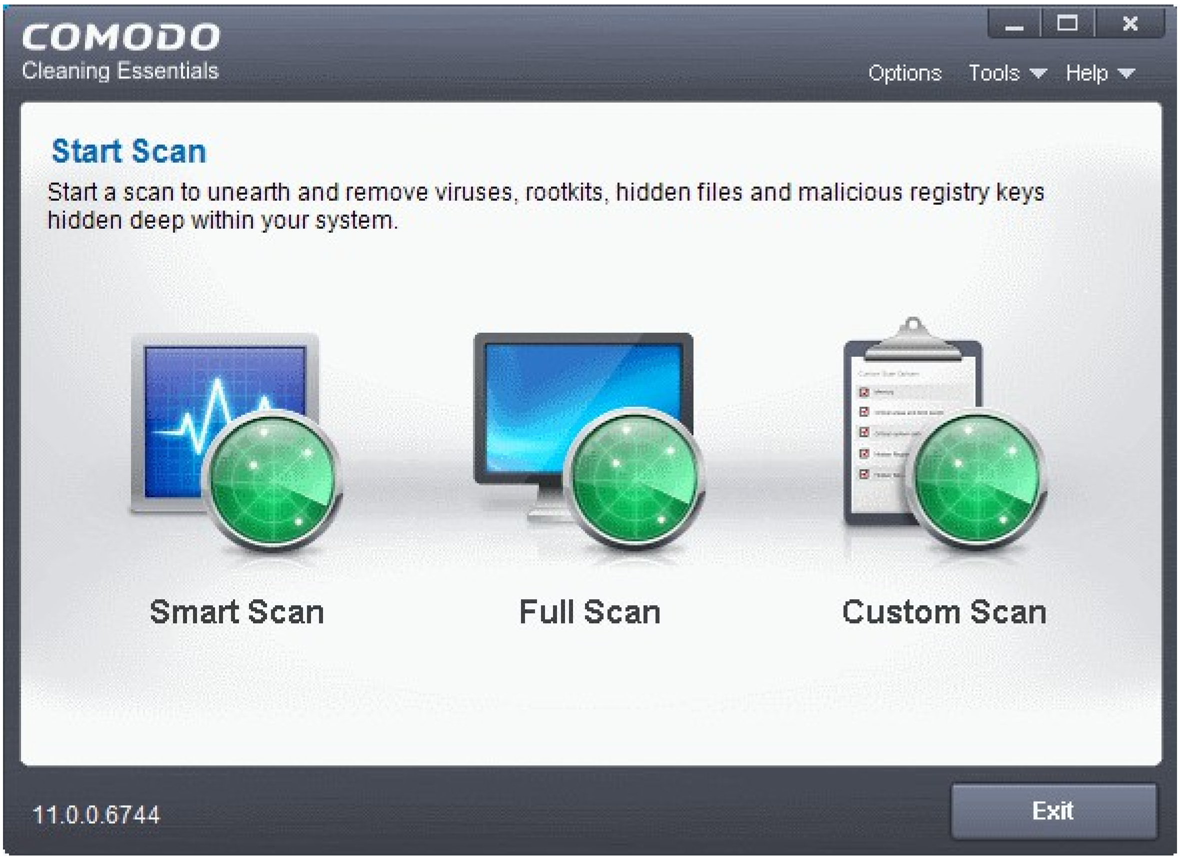
- A smart scan is a targeted scan of critical areas of your computer which are highly prone to attack by malware.
  - These include system memory, auto-run entries, hidden services, boot sectors, critical registry keys, and important operating system files/folders.
  - These areas are responsible for the stability of your computer so keeping them clean is essential.
- Your computer will be restarted during a smart scan so that CCE can search for hidden services and drivers.
  - Hidden services/drivers are threats which are designed to evade regular antivirus scans. These include rootkits and advanced persistent threats.
  - These attacks run silently in the background and can enable hackers to steal your identity and confidential information like credit card details.

After a smart scan is complete, you can:

- Clean the detected threats, or move them to quarantine.
- Exclude an application you consider as safe from the threat list
- Report the threat as a 'False Positive' to Comodo

Start a Smart scan

- Open Comodo Cleaning Essentials
- Click the 'Smart Scan' icon on the left:

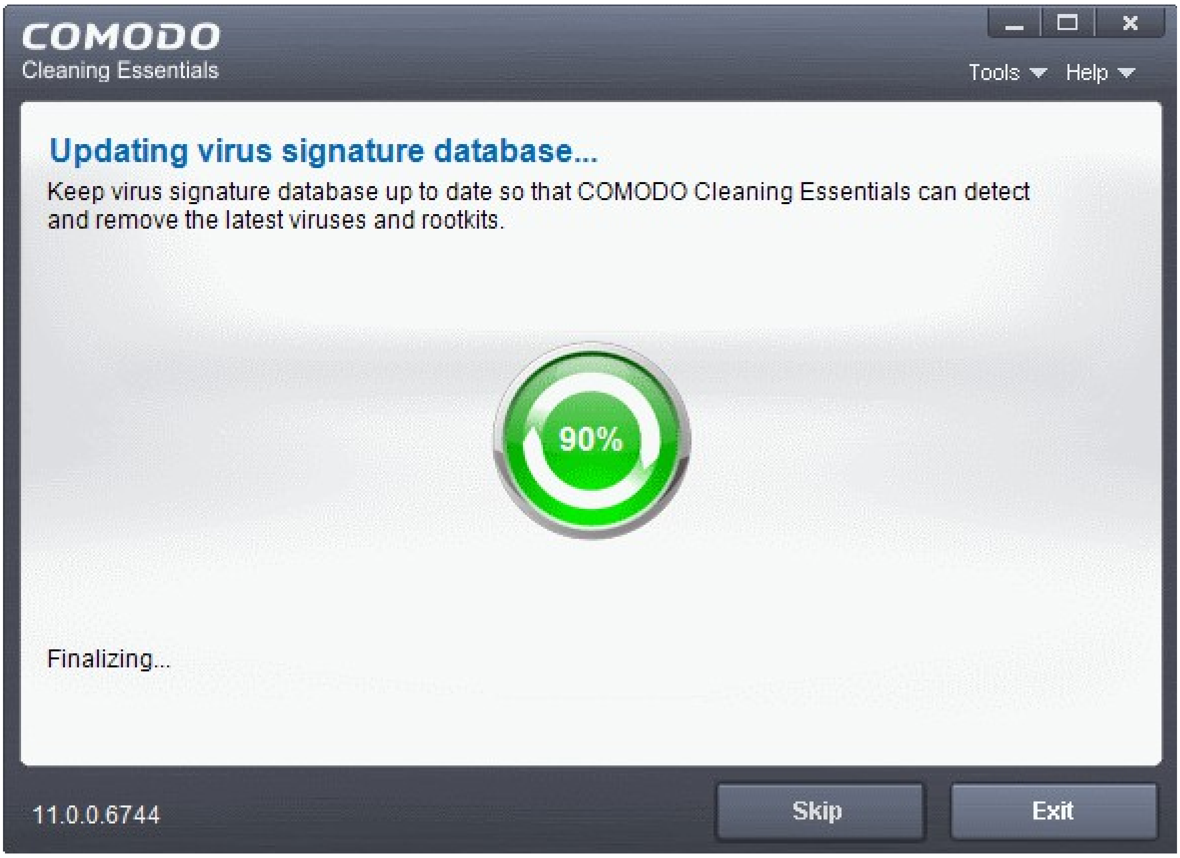


Start Scan

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

11.0.0.6744

The application will check for virus database updates before starting the scan:



Updating virus signature database...

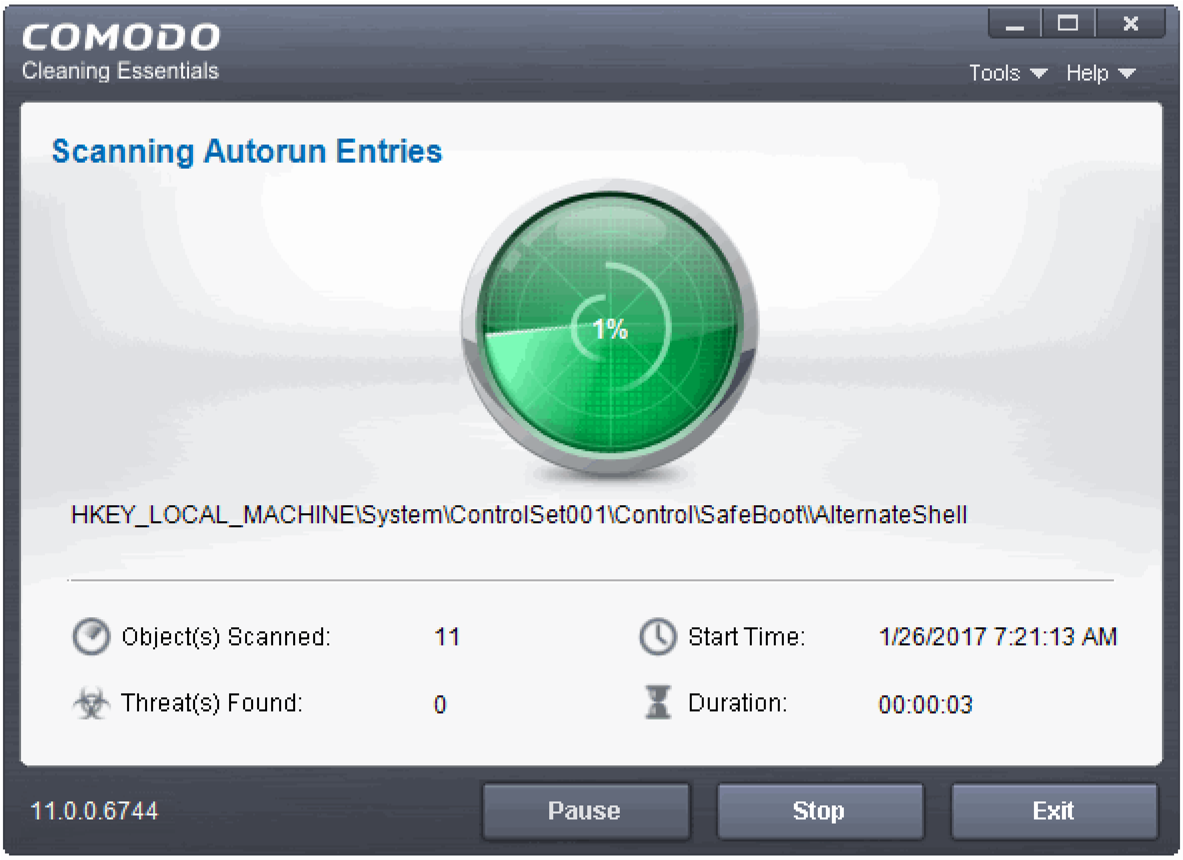
Keep virus signature database up to date so that COMODO Cleaning Essentials can detect and remove the latest viruses and rootkits.

Finalizing...

11.0.0.6744

We advise you always let the application update itself so you are protected against the very latest threats. Click 'Skip' if you don't want to download the update at this time.

The scan will start. Scan progress and results are shown in real-time:



Scanning Autorun Entries

HKEY_LOCAL_MACHINE\System\ControlSet001\Control\SafeBoot\\AlternateShell

Object(s) Scanned: 11

Threat(s) Found: 0

Start Time: 1/26/2017 7:21:13 AM

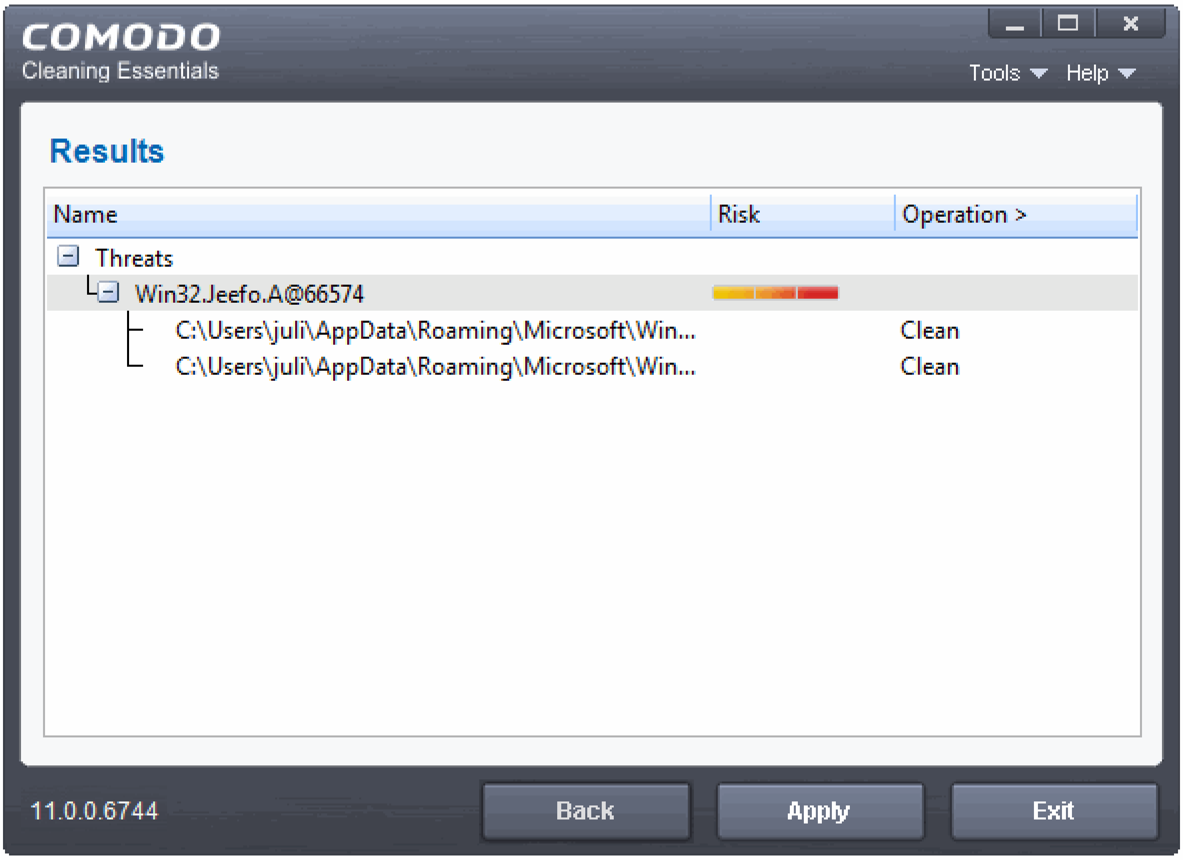
Duration: 00:00:03

11.0.0.6744

Click the 'Threat(s) Found' link at any time to view more details about the malware discovered on your system.

Results

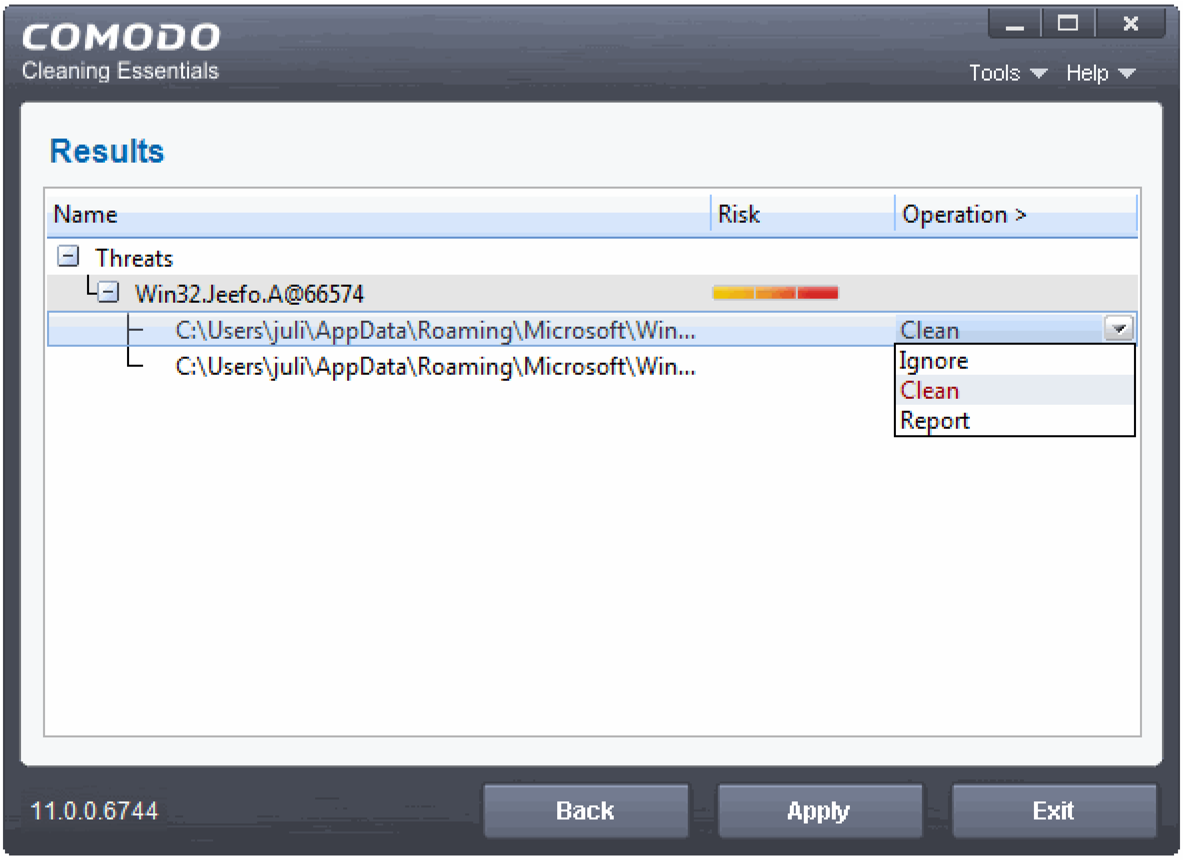
Full results are shown at the end of the scan.



Results

Name	Risk	Operation >
⊟ Threats		
⊟ Win32.Jeefo.A@66574		
C:\Users\juli\AppData\Roaming\Microsoft\Win...		Clean
C:\Users\juli\AppData\Roaming\Microsoft\Win...		Clean

- The results show the names and location of all malware found
- Click the text in the 'Operation >' column to take actions on the reported malware:

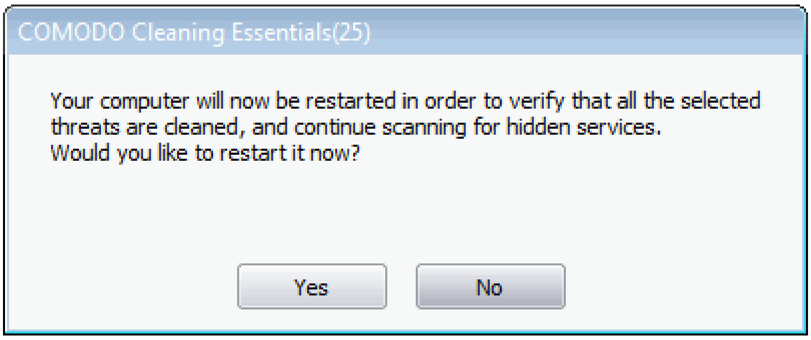


Results

Name	Risk	Operation >
⊟ Threats		
⊟ Win32.Jeefo.A@66574		
C:\Users\juli\AppData\Roaming\Microsoft\Win...		Clean
C:\Users\juli\AppData\Roaming\Microsoft\Win...		

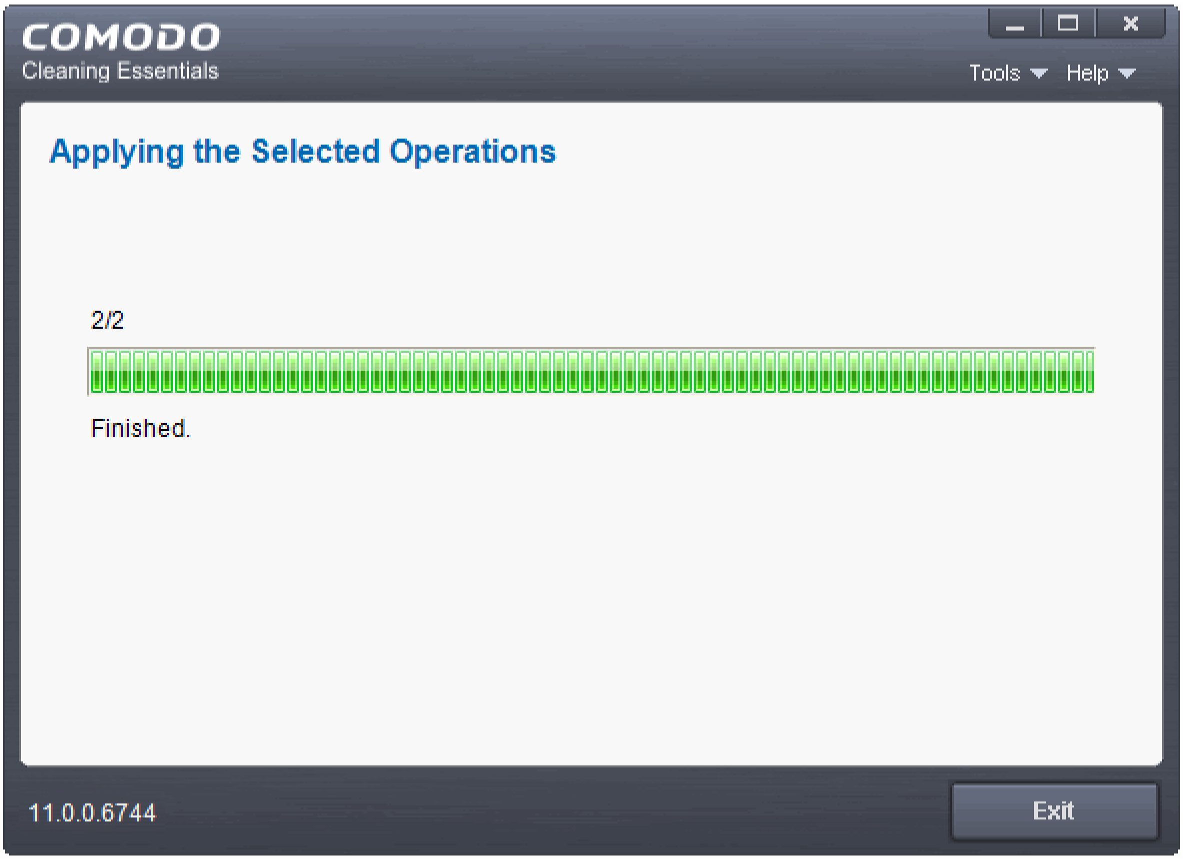
The following actions are available:

  - Clean - The file will be deleted or moved to quarantine. You can later delete the file from quarantine if required. See **Manage Quarantined Items** for more details.
  - Ignore - CCE will take no action on the file. Note - the file will be caught by the next scan you run.
  - Report - Submit the file as a false-positive to Comodo. Do this if you think the file is safe, and CCE was incorrect to flag it as malicious. The file will be analyzed by Comodo technicians.
  - Click on the 'Operations >' column header to apply one action to all files in the list.
- Click 'Apply' to implement your actions.
- You now need to restart your computer. This is so CCE can check whether the threats have been completely removed, and to scan for hidden services and drivers:



Your computer will now be restarted in order to verify that all the selected threats are cleaned, and continue scanning for hidden services.
Would you like to restart it now?

- Save all your work first, then click 'Yes' to restart your computer. If you plan to apply the operations at a later time, click 'No'. The clean operations will be implemented the next time you restart your computer.

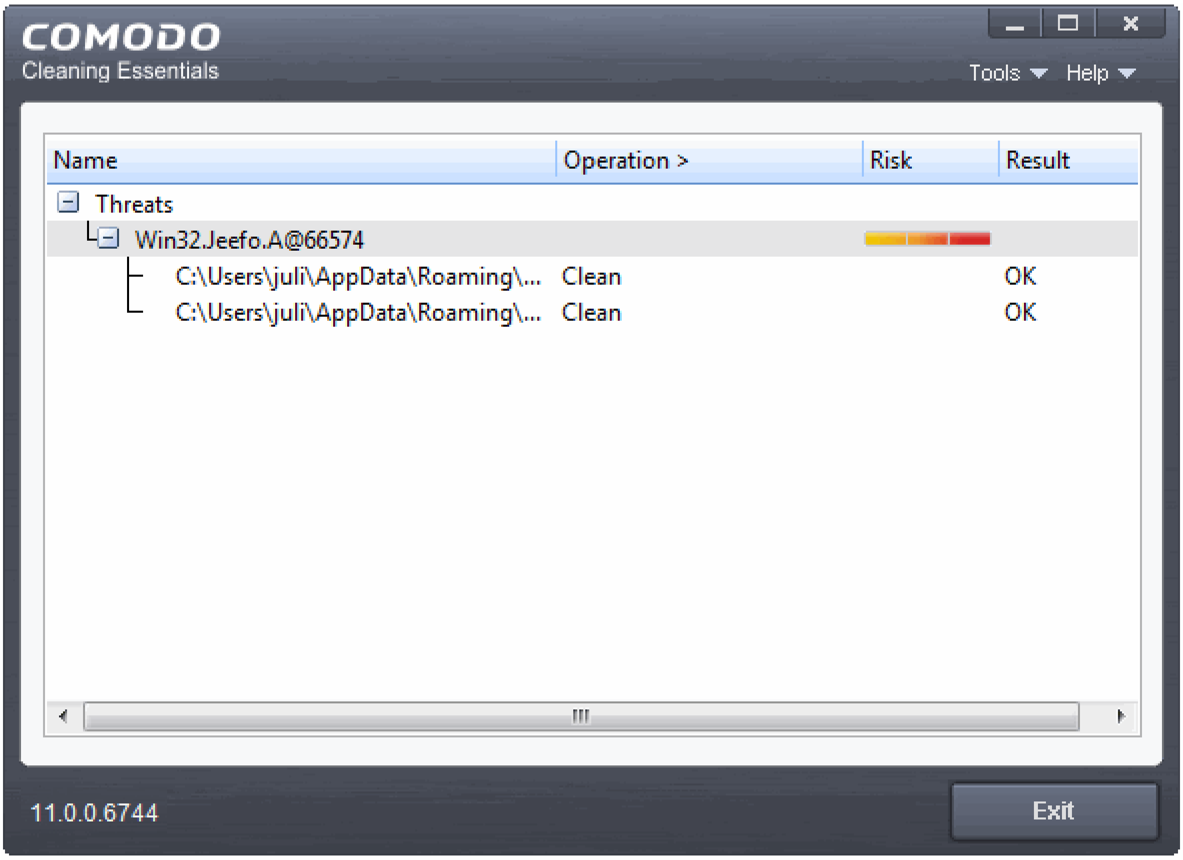


Applying the Selected Operations

2/2

Finished.

After the restart, CCE will scan for and clean any hidden processes. Results are shown as follows:



Name	Operation >	Risk	Result
Threats			
Win32.Jeefo.A@66574			
C:\Users\juli\AppData\Roaming\...	Clean		OK
C:\Users\juli\AppData\Roaming\...	Clean		OK

2.2. Full Scan

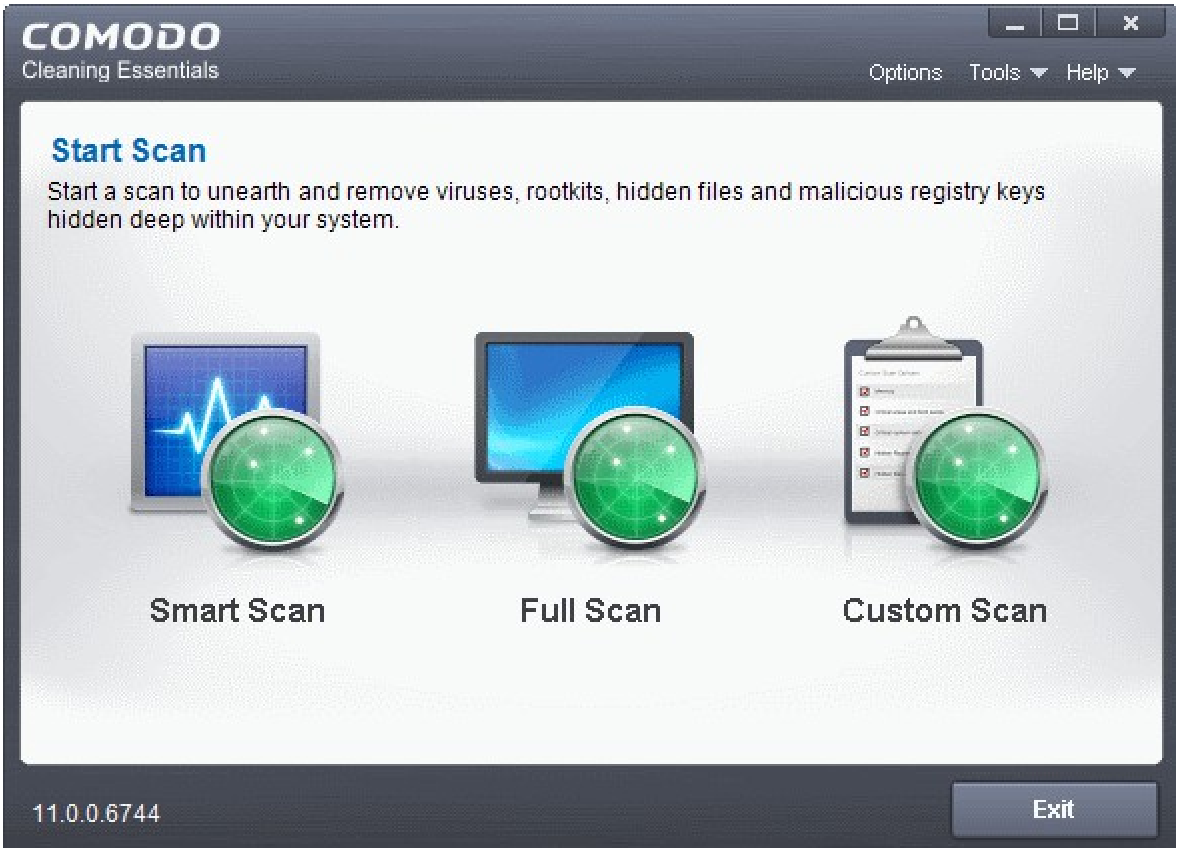
- It is essential to regularly run a full scan of your computer to detect the latest malware or viruses.
- A full scan covers all areas of your computer, including all hard drive partitions, the registry and system memory.
- Before the scan begins, the application will restart your system in order to identify any hidden services or drivers. Save all your work before starting a full scan.

When the scan is complete, you can:

- Clean detected threats, or move them to quarantine.
- Create exclusions for items detected as a threat, but you consider to be safe.
- Report potential false positives to Comodo

Start a Full scan

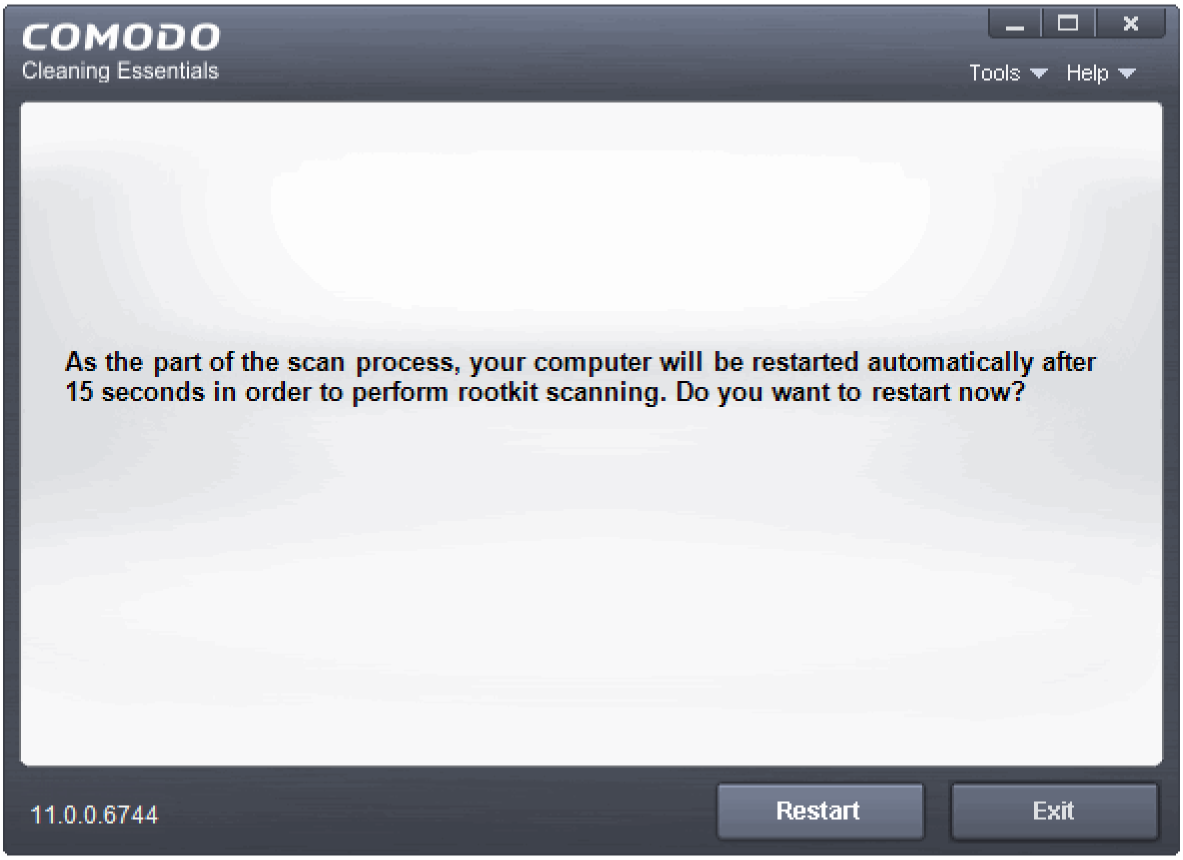
- Open Comodo Cleaning Essentials
- Click the 'Full Scan' icon in the middle of the interface.



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.



As the part of the scan process, your computer will be restarted automatically after 15 seconds in order to perform rootkit scanning. Do you want to restart now?

- A rootkit is a type of malware that is designed to avoid traditional antivirus scanners.
- Once installed, they camouflage themselves as (for example) standard operating system files, security tools and APIs.

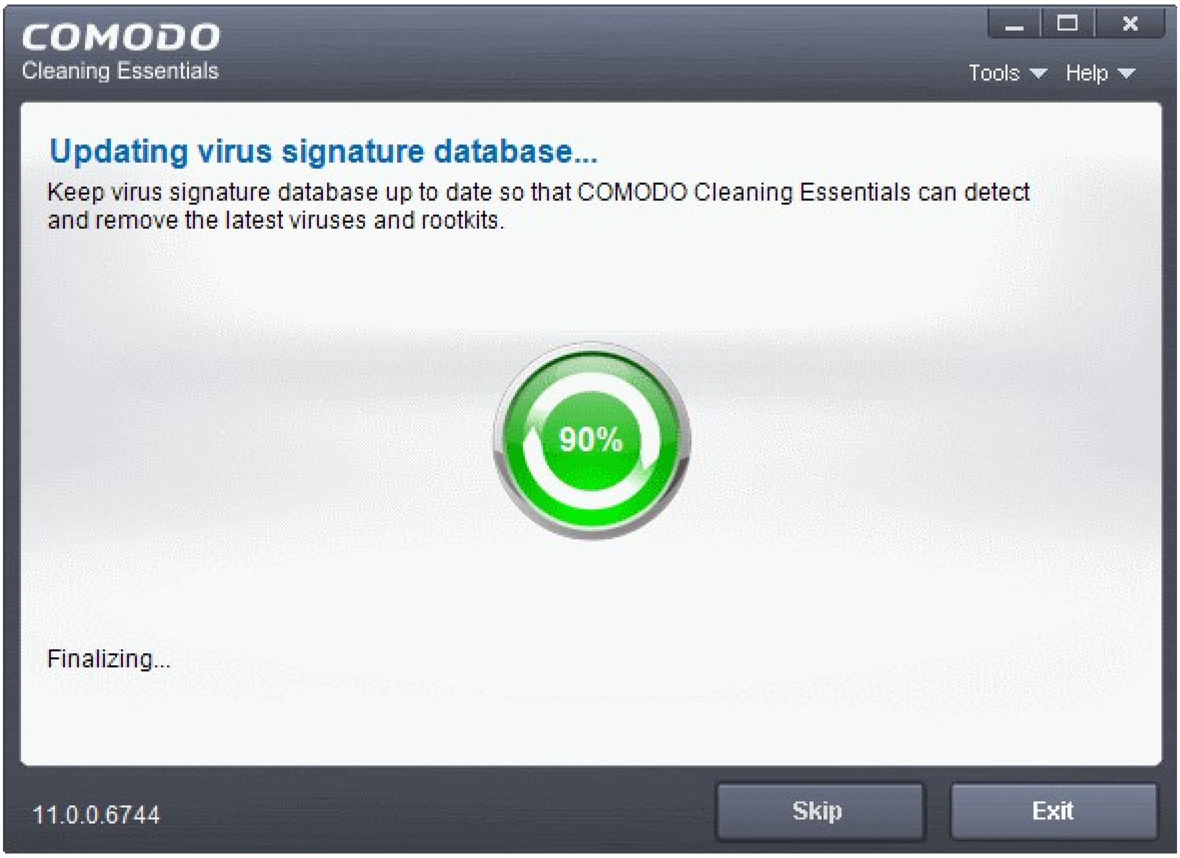
- Rootkits are usually not detectable by normal virus scanners because of this camouflage. However, CCE features a dedicated scanner that is capable of identifying rootkits, hidden files and malicious registry keys.

The restart dialog window will start a count down from 30 and if you do not choose either 'Restart' or 'Exit' button, the system will automatically restart when the count down reaches 0.

- Click 'Restart' to restart the system to perform the rootkit scanning
- If you click 'Exit', 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 for updates before starting the scan:



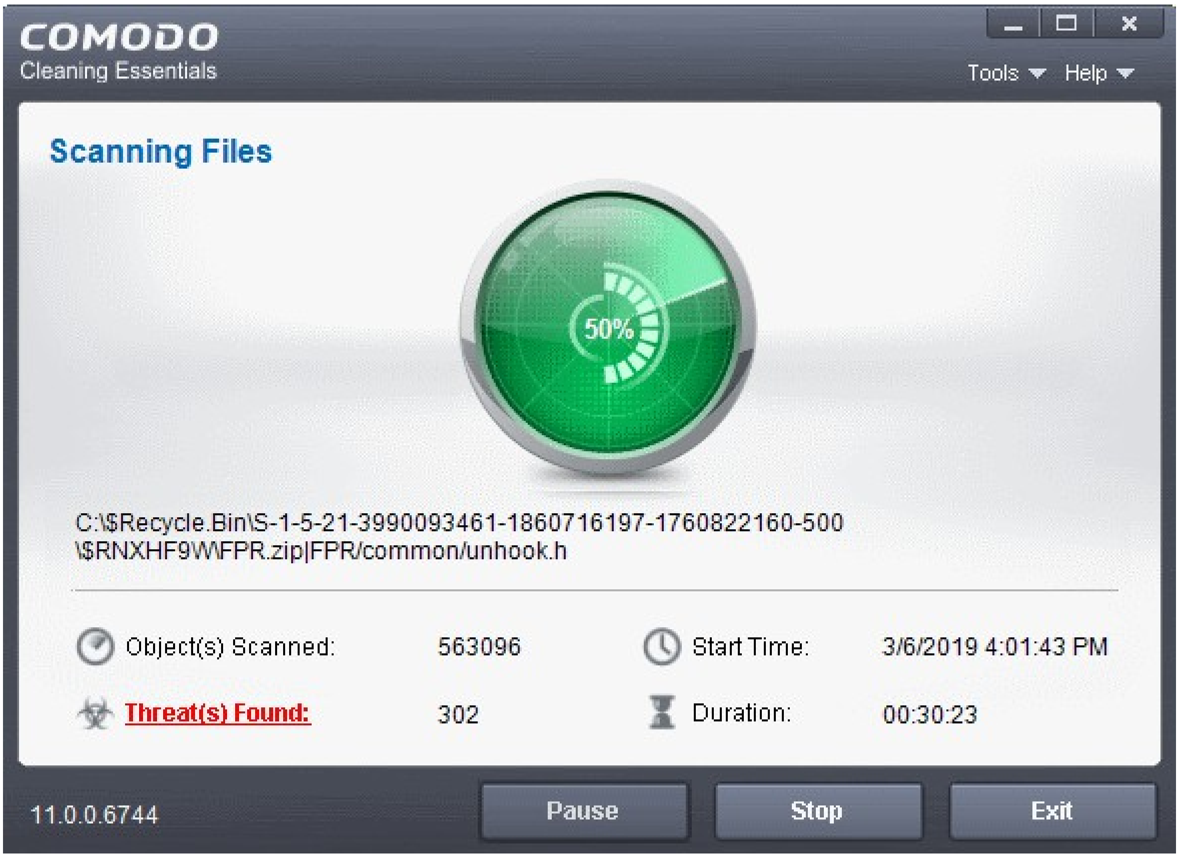
Updating virus signature database...

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

Finalizing...

We advise you always let the application update itself so you are protected against the very latest threats. Click 'Skip' if you don't want to download the update at this time.

The scan will start. Scan progress and results are shown in real-time:



Scanning Files

C:\$Recycle.Bin\S-1-5-21-3990093461-1860716197-1760822160-500
\$RNXHF9W\FPR.zip|FPR/common/unhook.h

Object(s) Scanned: 563096

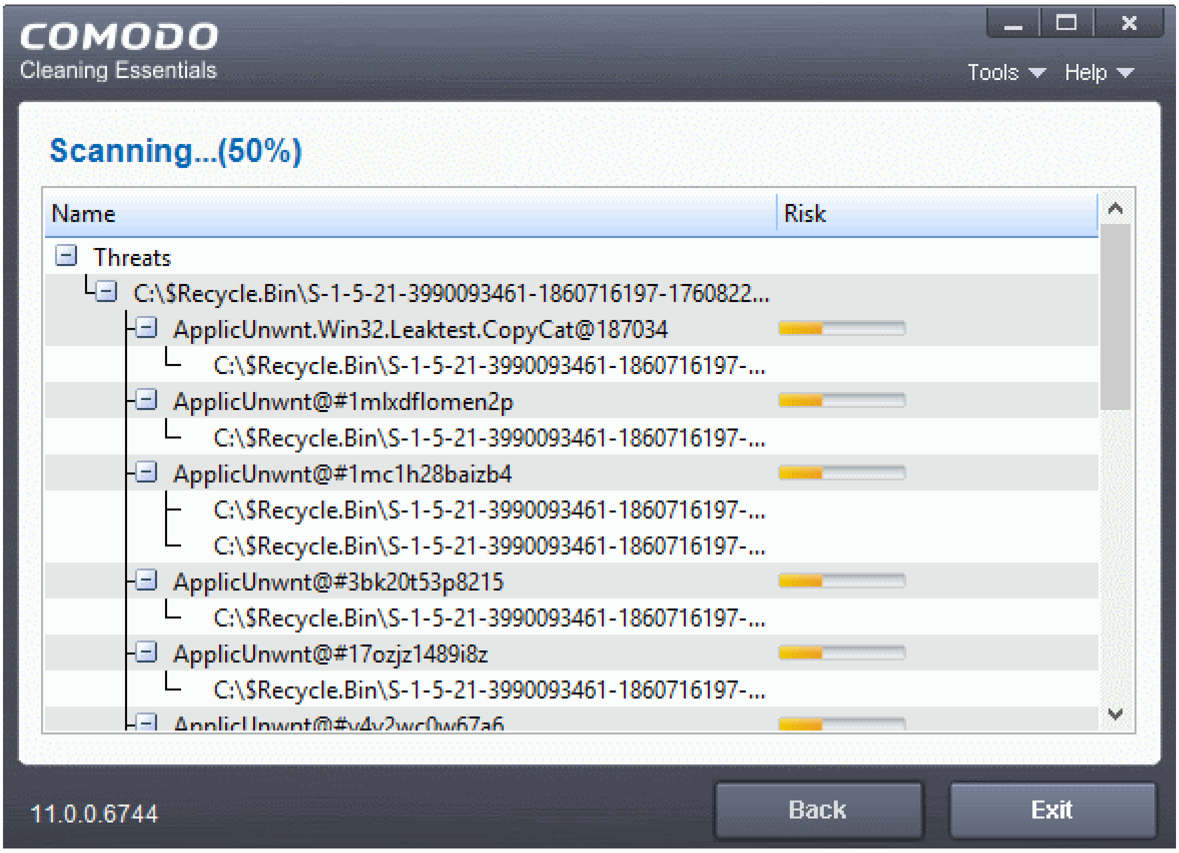
Start Time: 3/6/2019 4:01:43 PM

Threat(s) Found: 302

Duration: 00:30:23

11.0.0.6744

Click the 'Threat(s) Found' link at any time to view more details about the malware discovered on your system.

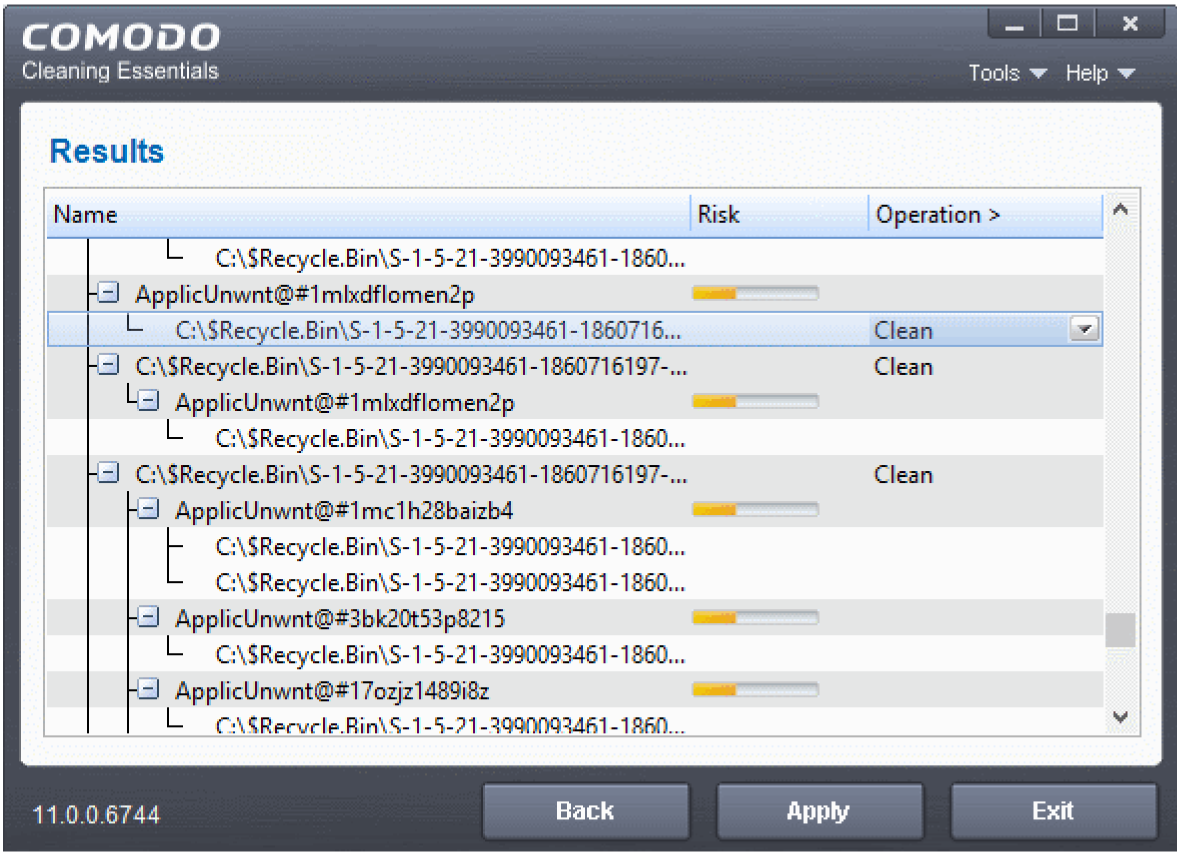


Scanning...(50%)

Name	Risk
Threats	
C:\$Recycle.Bin\S-1-5-21-3990093461-1860716197-1760822...	
ApplicUnwnt.Win32.Leaktest.CopyCat@187034	
C:\$Recycle.Bin\S-1-5-21-3990093461-1860716197-...	
ApplicUnwnt@#1mlxdflomen2p	
C:\$Recycle.Bin\S-1-5-21-3990093461-1860716197-...	
ApplicUnwnt@#1mc1h28baizb4	
C:\$Recycle.Bin\S-1-5-21-3990093461-1860716197-...	
C:\$Recycle.Bin\S-1-5-21-3990093461-1860716197-...	
ApplicUnwnt@#3bk20t53p8215	
C:\$Recycle.Bin\S-1-5-21-3990093461-1860716197-...	
ApplicUnwnt@#17ozjz1489i8z	
C:\$Recycle.Bin\S-1-5-21-3990093461-1860716197-...	
ApplicUnwnt@#v4y2wc0w67a6	

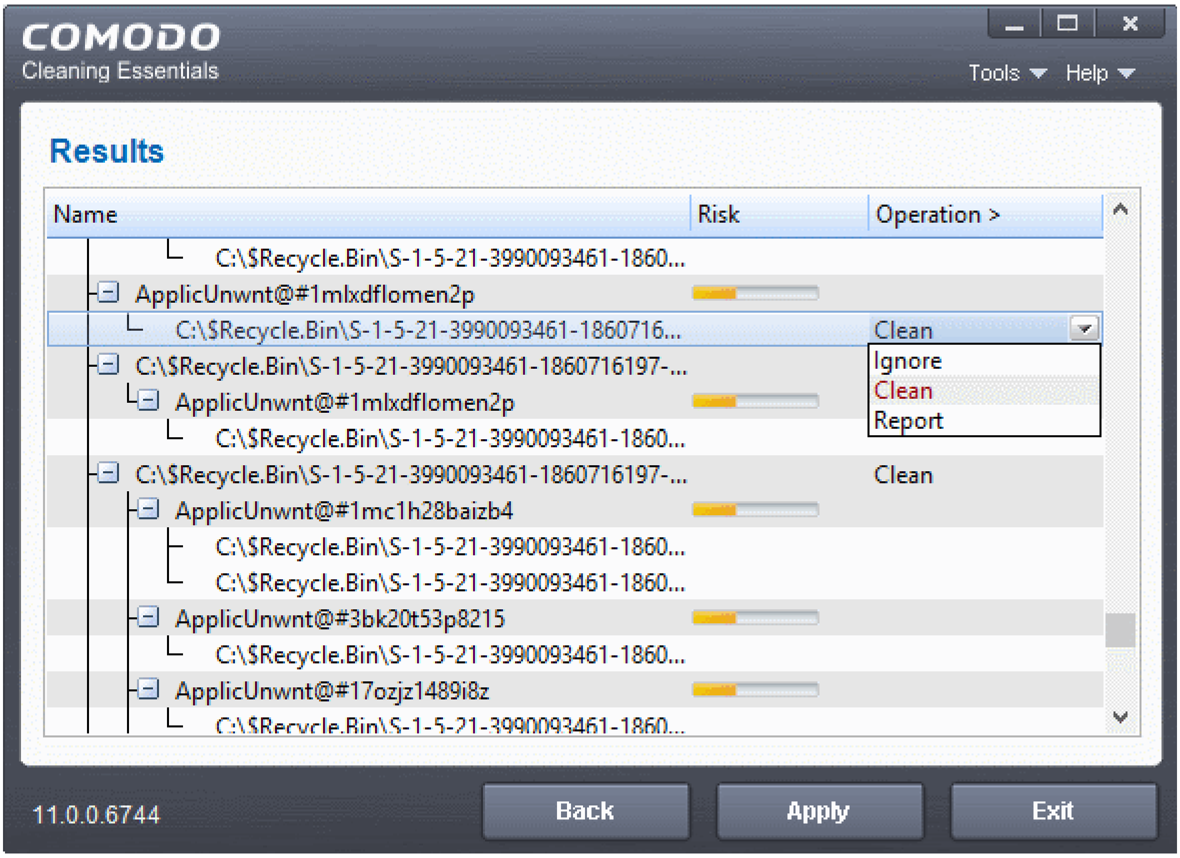
Results

Full results are shown at the end of the scan.



Name	Risk	Operation >
C:\$Recycle.Bin\S-1-5-21-3990093461-1860...		
ApplicUnwnt@#1mlxdflomen2p		
C:\$Recycle.Bin\S-1-5-21-3990093461-1860716...		Clean
C:\$Recycle.Bin\S-1-5-21-3990093461-1860716197-...		Clean
ApplicUnwnt@#1mlxdflomen2p		
C:\$Recycle.Bin\S-1-5-21-3990093461-1860...		
C:\$Recycle.Bin\S-1-5-21-3990093461-1860716197-...		Clean
ApplicUnwnt@#1mc1h28baizb4		
C:\$Recycle.Bin\S-1-5-21-3990093461-1860...		
C:\$Recycle.Bin\S-1-5-21-3990093461-1860...		
ApplicUnwnt@#3bk20t53p8215		
C:\$Recycle.Bin\S-1-5-21-3990093461-1860...		
ApplicUnwnt@#17ozjz1489i8z		
C:\$Recycle.Bin\S-1-5-21-3990093461-1860...		

- The results show the names and location of all malware found
- Click the text in the 'Operation >' column to take actions on the reported malware:



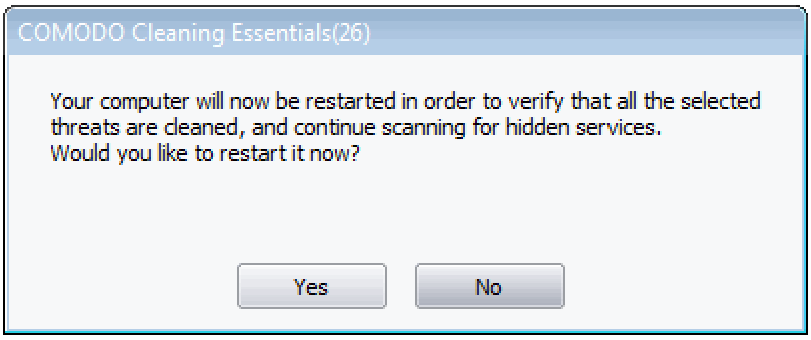
Name	Risk	Operation >
C:\$Recycle.Bin\S-1-5-21-3990093461-1860...		
ApplicUnwnt@#1mlxdflomen2p		
C:\$Recycle.Bin\S-1-5-21-3990093461-1860716...		Clean
C:\$Recycle.Bin\S-1-5-21-3990093461-1860716197-...		
ApplicUnwnt@#1mlxdflomen2p		
C:\$Recycle.Bin\S-1-5-21-3990093461-1860...		
C:\$Recycle.Bin\S-1-5-21-3990093461-1860716197-...		Clean
ApplicUnwnt@#1mc1h28baizb4		
C:\$Recycle.Bin\S-1-5-21-3990093461-1860...		
C:\$Recycle.Bin\S-1-5-21-3990093461-1860...		
ApplicUnwnt@#3bk20t53p8215		
C:\$Recycle.Bin\S-1-5-21-3990093461-1860...		
ApplicUnwnt@#17ozjz1489i8z		
C:\$Recycle.Bin\S-1-5-21-3990093461-1860...		

The following actions are available:

- Clean - The file will be deleted or moved to quarantine. You can later delete the file from quarantine if required. See **Manage Quarantined Items** for more details.

- Ignore - CCE will take no action on the file. Note - the file will be caught by the next scan you run.
- Report - Submit the file as a false-positive to Comodo. Do this if you think the file is safe, and CCE was incorrect to flag it as malicious. The file will be analyzed by Comodo technicians.
- Click on the 'Operations >' column header to apply one action to all files in the list.

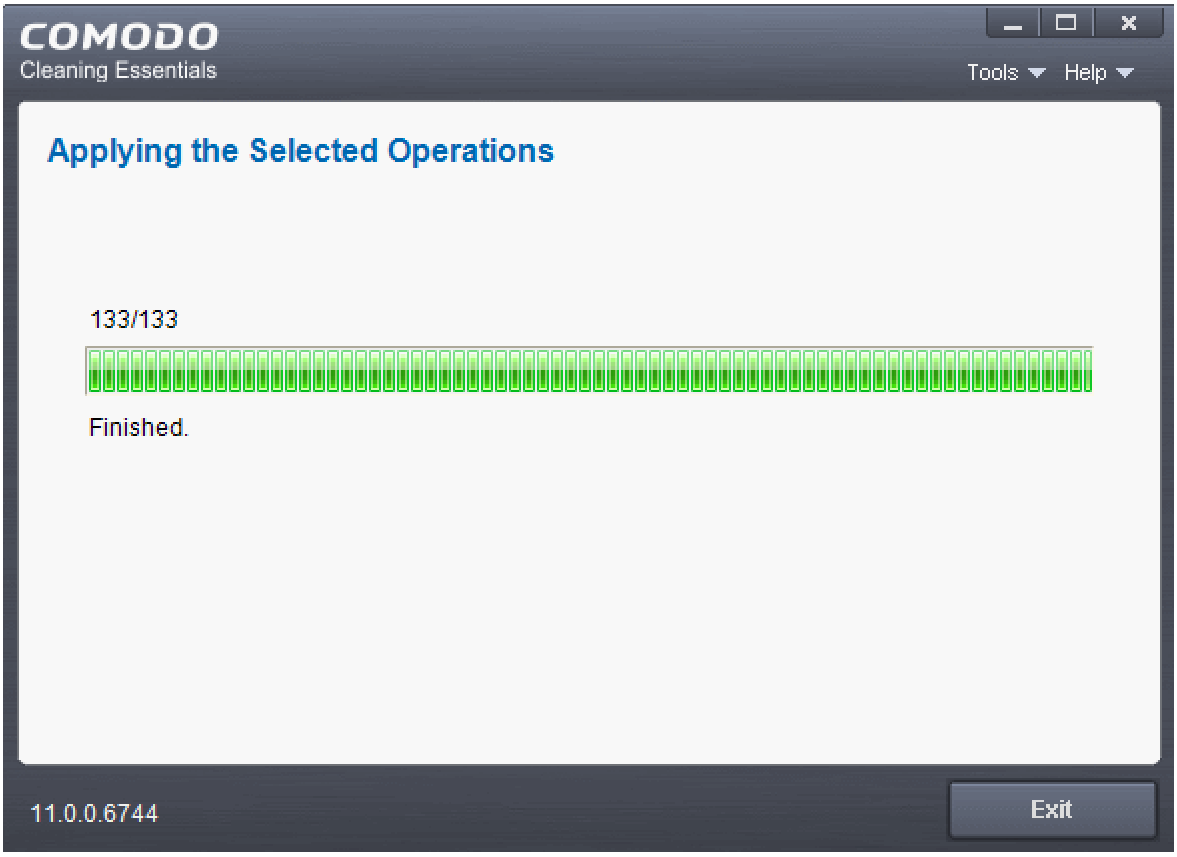
- Click 'Apply' to implement your actions.
- You now need to restart your computer. This is so CCE can check whether the threats have been completely removed, and to scan for hidden services and drivers:



COMODO Cleaning Essentials(26)

Your computer will now be restarted in order to verify that all the selected threats are cleaned, and continue scanning for hidden services.
Would you like to restart it now?

- Save all your work first, then click 'Yes' to restart your computer. If you plan to apply the operations at a later time, click 'No'. The clean operations will be implemented the next time you restart your computer.



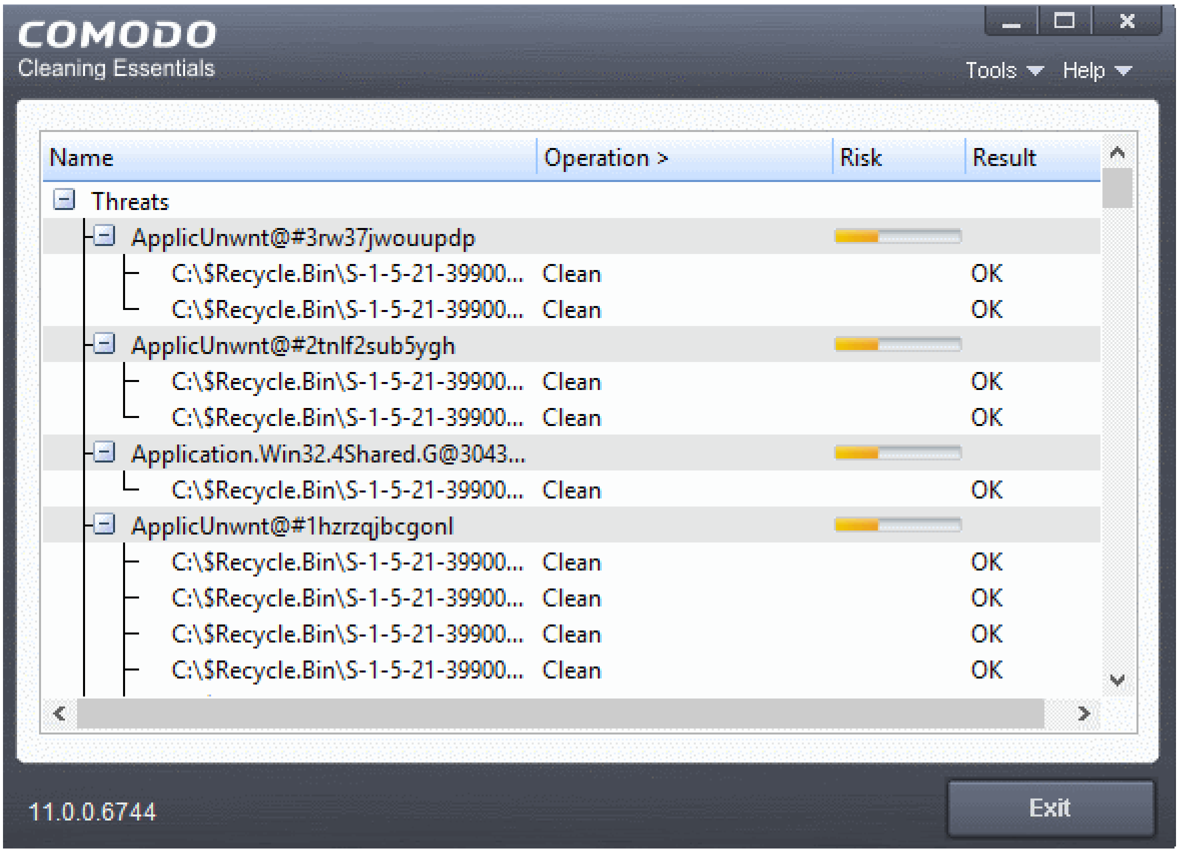
Applying the Selected Operations

133/133

Finished.

11.0.0.6744

After the restart, CCE will scan for and clean any hidden processes. Results are shown as follows:



Name	Operation >	Risk	Result
Threats			
ApplicUnwnt@#3rw37jwouupdp			
C:\$Recycle.Bin\S-1-5-21-39900...	Clean		OK
C:\$Recycle.Bin\S-1-5-21-39900...	Clean		OK
ApplicUnwnt@#2tnlf2sub5ygh			
C:\$Recycle.Bin\S-1-5-21-39900...	Clean		OK
C:\$Recycle.Bin\S-1-5-21-39900...	Clean		OK
Application.Win32.4Shared.G@3043...			
C:\$Recycle.Bin\S-1-5-21-39900...	Clean		OK
ApplicUnwnt@#1hzrzqjbcgonl			
C:\$Recycle.Bin\S-1-5-21-39900...	Clean		OK
C:\$Recycle.Bin\S-1-5-21-39900...	Clean		OK
C:\$Recycle.Bin\S-1-5-21-39900...	Clean		OK
C:\$Recycle.Bin\S-1-5-21-39900...	Clean		OK

2.3. Custom Scan

- The custom scan feature allows you to check for malware in specific files/folders/drives.
- You will need to restart your computer if you choose to scan memory, critical areas, or hidden registry services/files/folders.

When the scan is complete, you can:

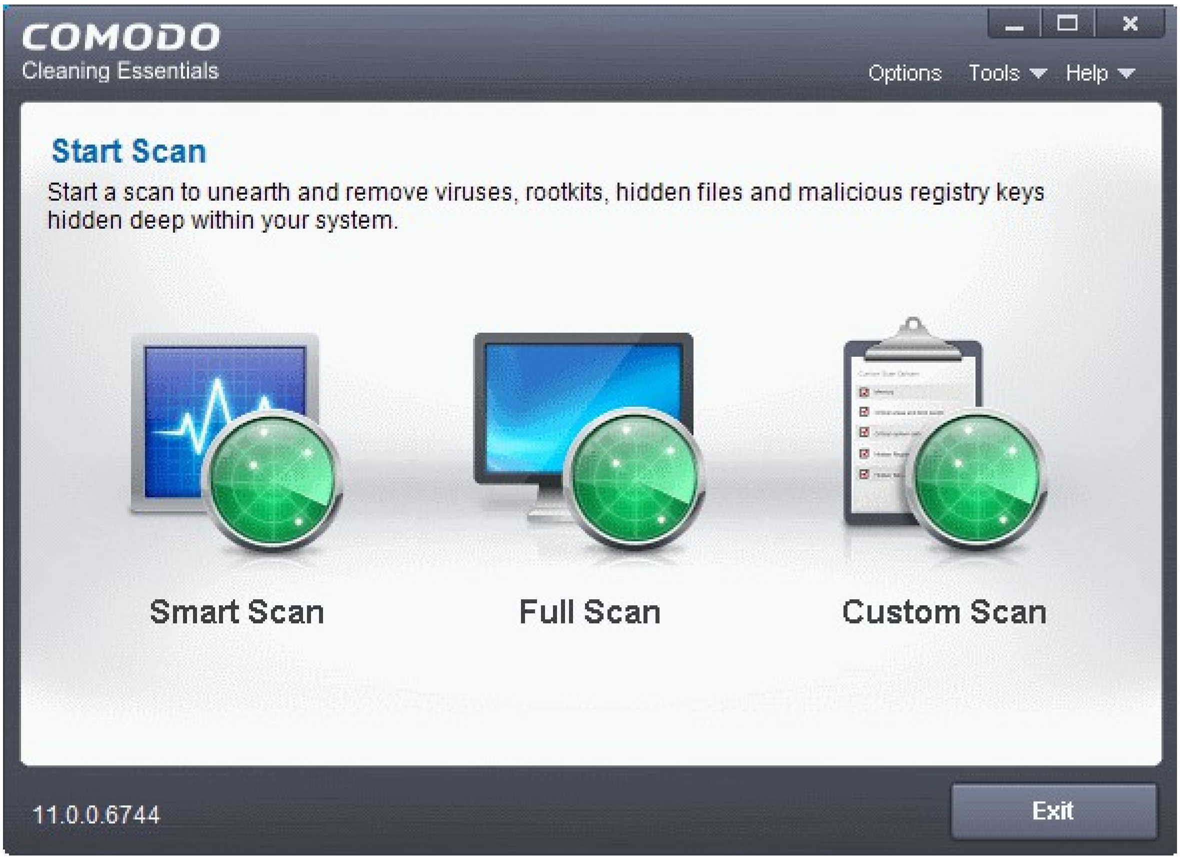
- Clean the detected threats, or move them to quarantine
- Exclude an application you consider as safe from the threat list
- Report false positives to Comodo.

See the following areas for more help:

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

Start a Custom Scan

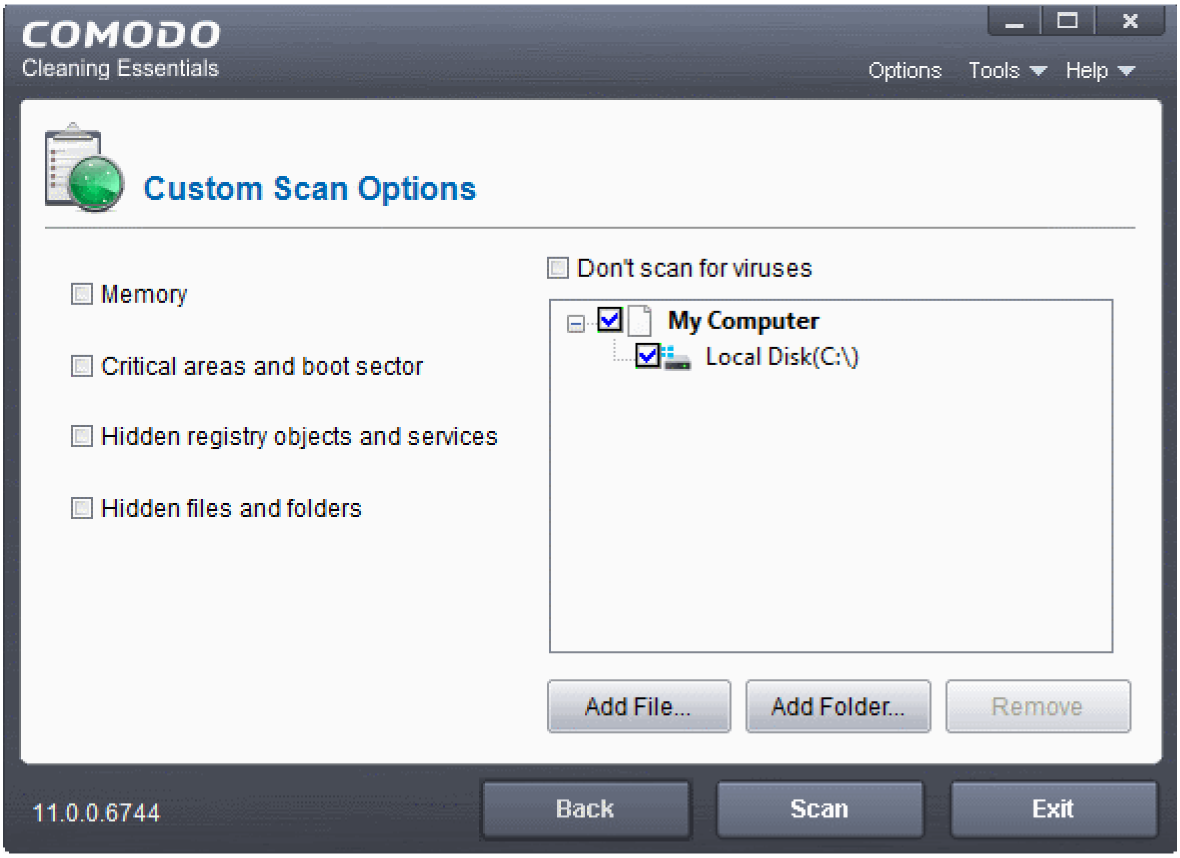
- Open Comodo Cleaning Essentials
- Click the 'Custom Scan' icon on the right:



Start Scan

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

You can now configure which locations you want to scan:



Custom Scan Options

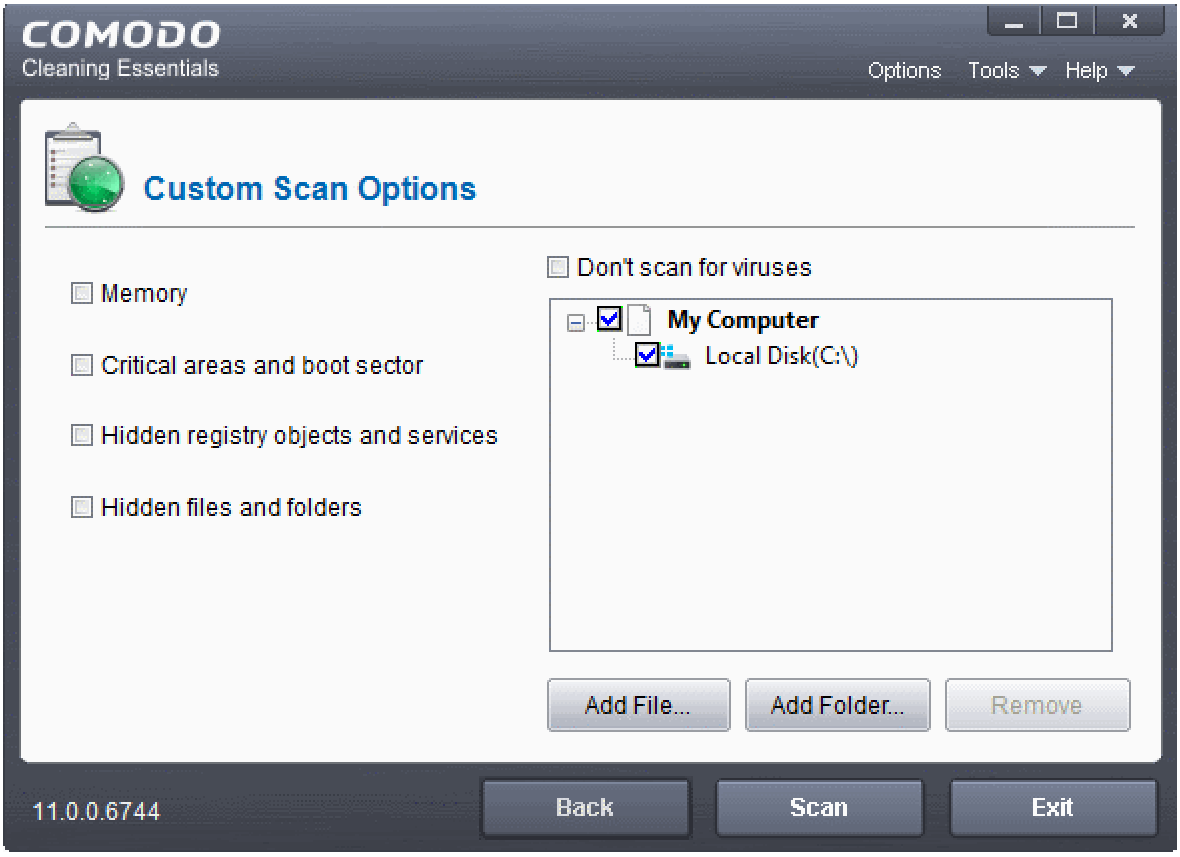
- □ Memory
- □ Critical areas and boot sector
- □ Hidden registry objects and services
- □ Hidden files and folders

□ Don't scan for viruses

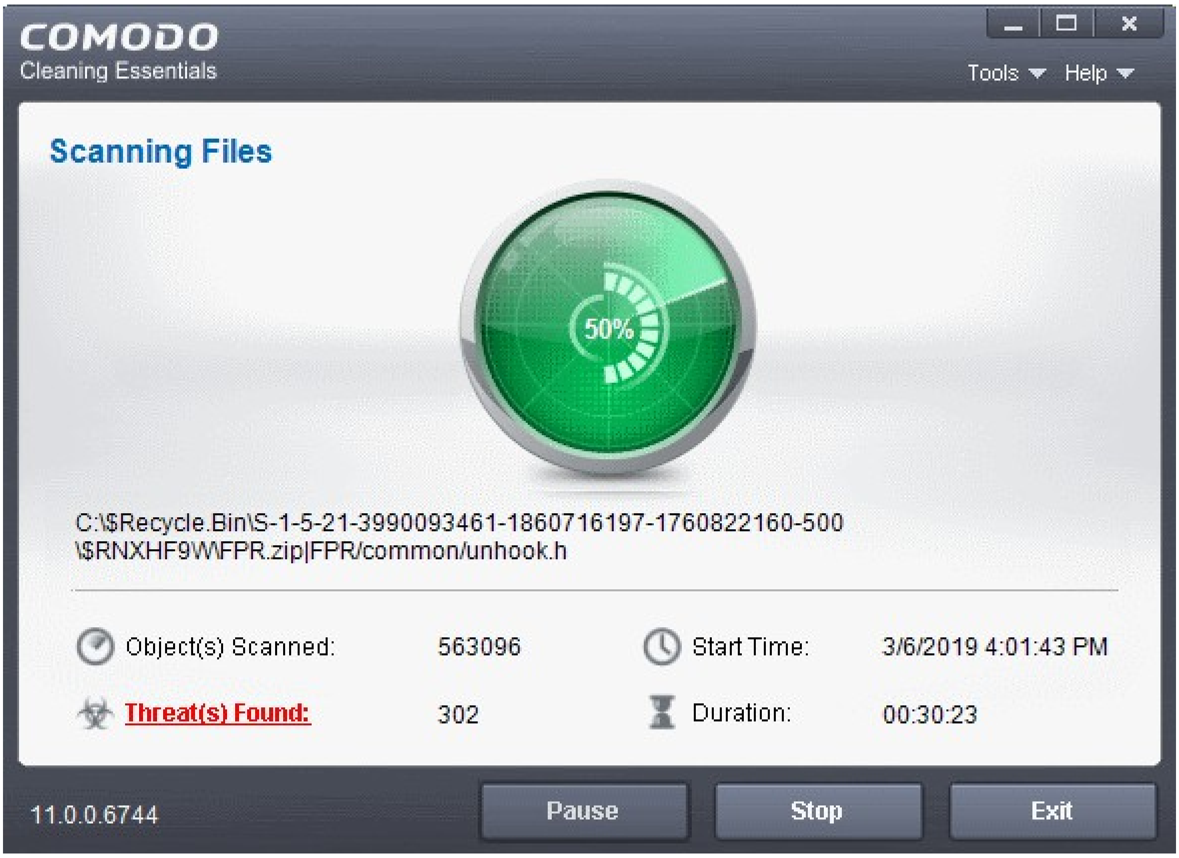
- ☑ My Computer
  - ☑ Local Disk(C:\)

Select your scan preferences on the left. Choose which files, folders or drives you want to scan on the right.

- **Memory -** CCE scans system memory at the start of the scan.
- **Critical areas and boot sector -** CCE scans the 'Program Files' and 'Windows' folders, all user folders, important registry keys, and the system startup area of your hard drive.
- **Hidden registry objects and services -** CCE will identify and scan obfuscated files and services.
- **Hidden files and folders -** CCE scans any invisible items on drives in the 'Scan Target' area.
- **Don't scan for viruses -** CCE will NOT scan any target in the box on the right (it will be grayed out). If this option is selected, you must choose at least option on the left.



- Use the 'Add File...' and 'Add Folder...' buttons to browse for specific items.
- Click 'Scan' to run your scan

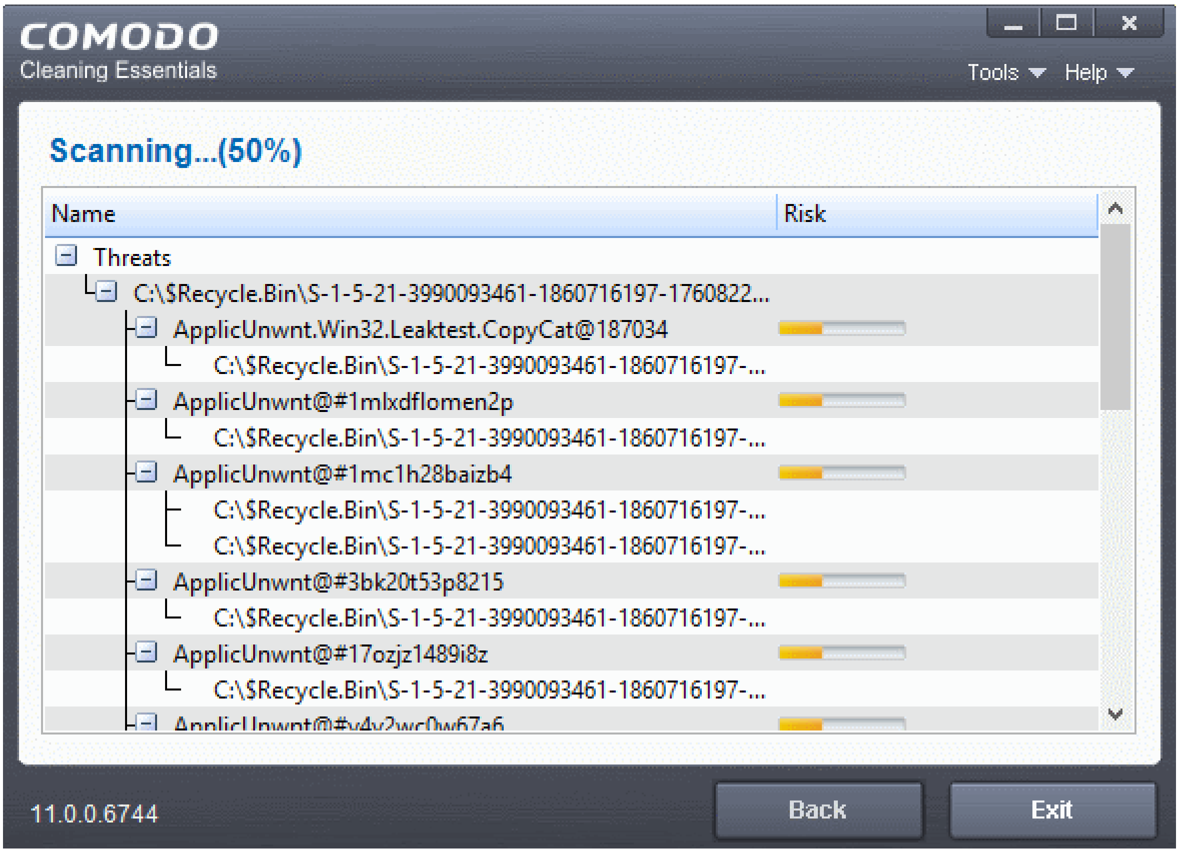


Scanning Files

C:\$Recycle.Bin\S-1-5-21-3990093461-1860716197-1760822160-500
\$RNXHF9W\FPR.zip|FPR/common/unhook.h

Object(s) Scanned:	563096	Start Time:	3/6/2019 4:01:43 PM
Threat(s) Found:	302	Duration:	00:30:23

Click the 'Threat(s) Found' link at any time to view more details about the malware discovered on your system.

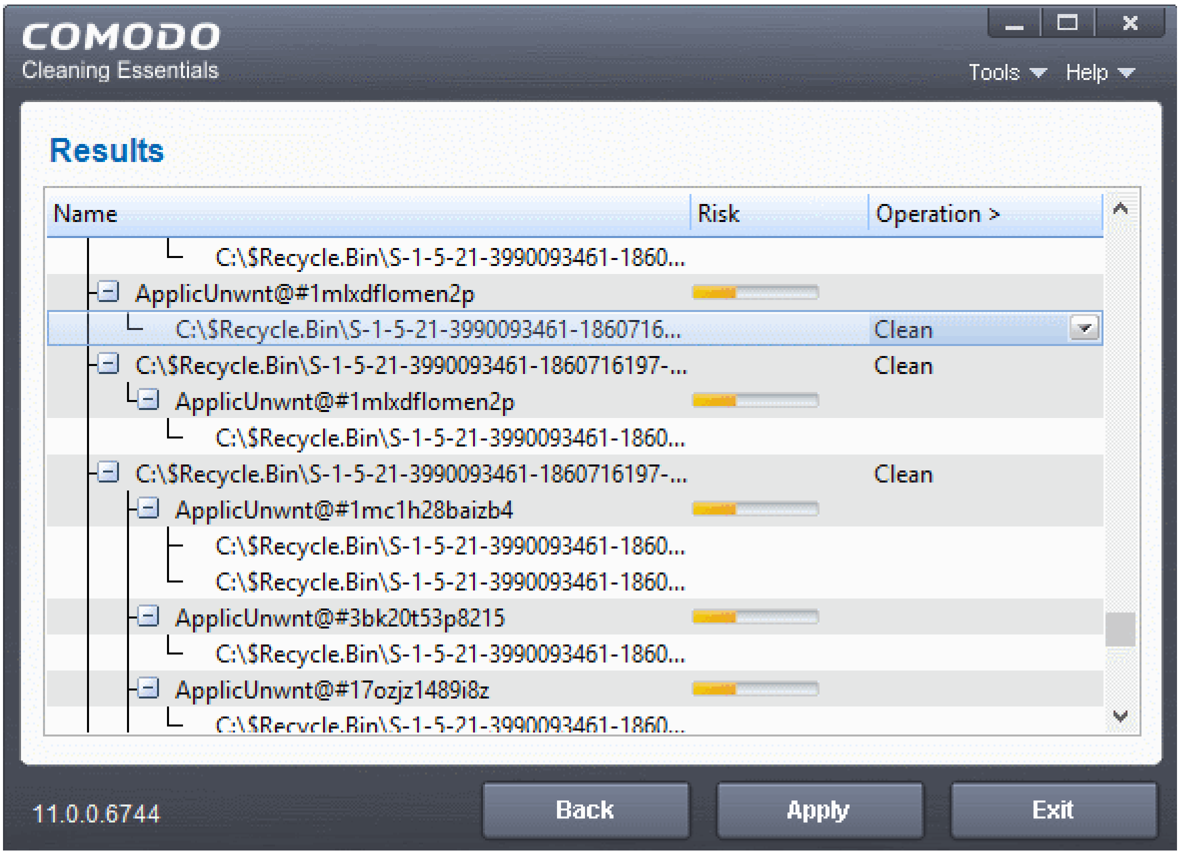


Scanning...(50%)

Name	Risk
Threats	
C:\$Recycle.Bin\S-1-5-21-3990093461-1860716197-1760822...	
ApplicUnwnt.Win32.Leaktest.CopyCat@187034	
C:\$Recycle.Bin\S-1-5-21-3990093461-1860716197-...	
ApplicUnwnt@#1mlxdflomen2p	
C:\$Recycle.Bin\S-1-5-21-3990093461-1860716197-...	
ApplicUnwnt@#1mc1h28baizb4	
C:\$Recycle.Bin\S-1-5-21-3990093461-1860716197-...	
C:\$Recycle.Bin\S-1-5-21-3990093461-1860716197-...	
ApplicUnwnt@#3bk20t53p8215	
C:\$Recycle.Bin\S-1-5-21-3990093461-1860716197-...	
ApplicUnwnt@#17ozjz1489i8z	
C:\$Recycle.Bin\S-1-5-21-3990093461-1860716197-...	
ApplicUnwnt@#v4y2wc0w67a6	

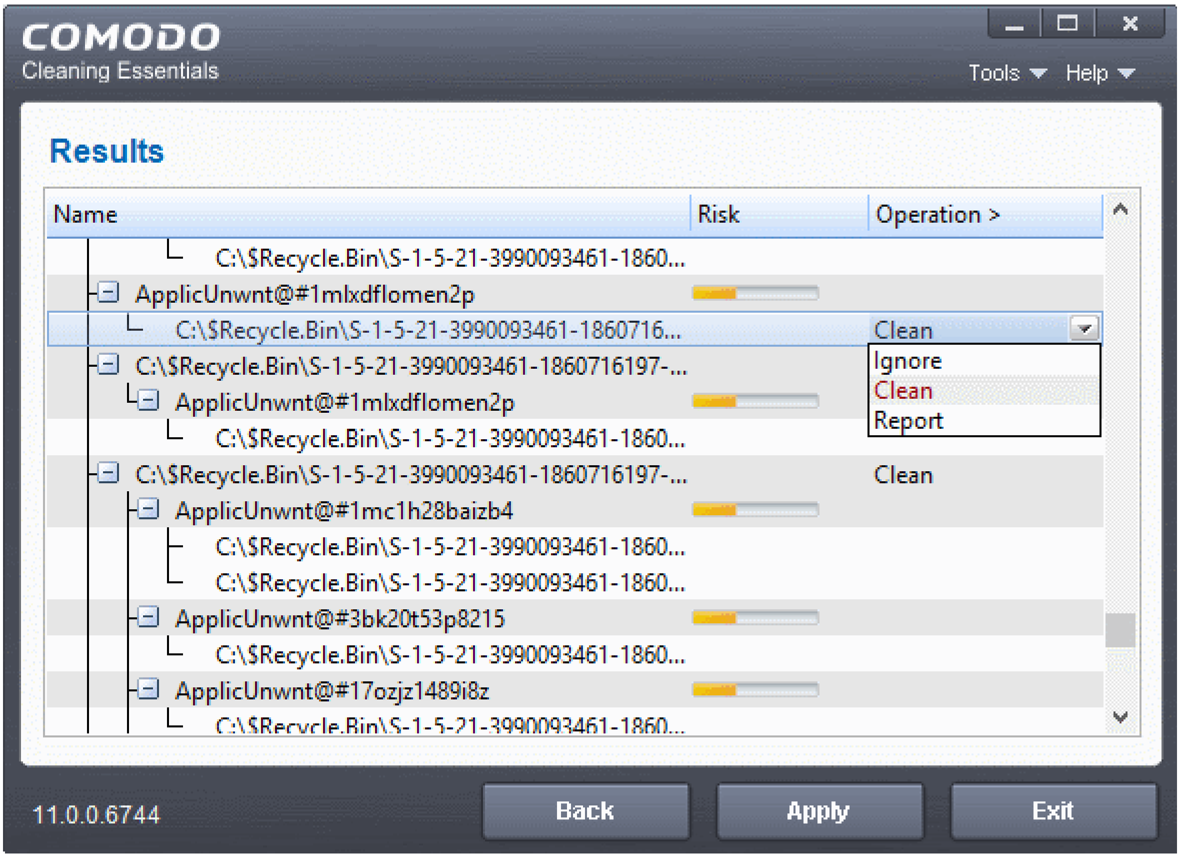
Results

Full results are shown at the end of the scan.



Name	Risk	Operation >
C:\$Recycle.Bin\S-1-5-21-3990093461-1860...		
ApplicUnwnt@#1mlxdflomen2p		
C:\$Recycle.Bin\S-1-5-21-3990093461-1860716...		Clean
C:\$Recycle.Bin\S-1-5-21-3990093461-1860716197-...		Clean
ApplicUnwnt@#1mlxdflomen2p		
C:\$Recycle.Bin\S-1-5-21-3990093461-1860...		
C:\$Recycle.Bin\S-1-5-21-3990093461-1860716197-...		Clean
ApplicUnwnt@#1mc1h28baizb4		
C:\$Recycle.Bin\S-1-5-21-3990093461-1860...		
C:\$Recycle.Bin\S-1-5-21-3990093461-1860...		
ApplicUnwnt@#3bk20t53p8215		
C:\$Recycle.Bin\S-1-5-21-3990093461-1860...		
ApplicUnwnt@#17ozjz1489i8z		
C:\$Recycle.Bin\S-1-5-21-3990093461-1860...		

- The results show the names and location of all malware found
- Click the text in the 'Operation >' column to take actions on the reported malware:



Results

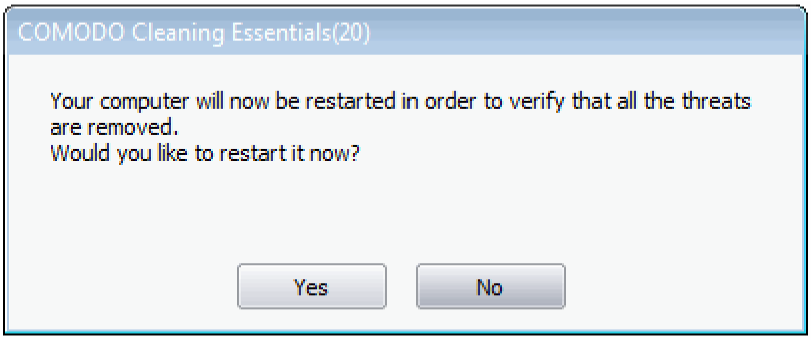
Name	Risk	Operation >
C:\$Recycle.Bin\S-1-5-21-3990093461-1860...		
ApplicUnwnt@#1mlxdflomen2p		
C:\$Recycle.Bin\S-1-5-21-3990093461-1860716...		Clean
C:\$Recycle.Bin\S-1-5-21-3990093461-1860716197-...		
ApplicUnwnt@#1mlxdflomen2p		
C:\$Recycle.Bin\S-1-5-21-3990093461-1860...		
C:\$Recycle.Bin\S-1-5-21-3990093461-1860716197-...		Clean
ApplicUnwnt@#1mc1h28baizb4		
C:\$Recycle.Bin\S-1-5-21-3990093461-1860...		
C:\$Recycle.Bin\S-1-5-21-3990093461-1860...		
ApplicUnwnt@#3bk20t53p8215		
C:\$Recycle.Bin\S-1-5-21-3990093461-1860...		
ApplicUnwnt@#17ozjz1489i8z		
C:\$Recycle.Bin\S-1-5-21-3990093461-1860...		

The following actions are available:

- **Clean** - The file will be deleted or moved to quarantine. You can later delete the file from quarantine if required. See **Manage Quarantined Items** for more details.
- **Ignore** - CCE will take no action on the file. Note - the file will still be caught by the next scan you run.
- **Report** - Submit the file as a false-positive to Comodo. Do this if you think the file is safe, and CCE was incorrect to flag it as malicious. The file will be analyzed by Comodo technicians.

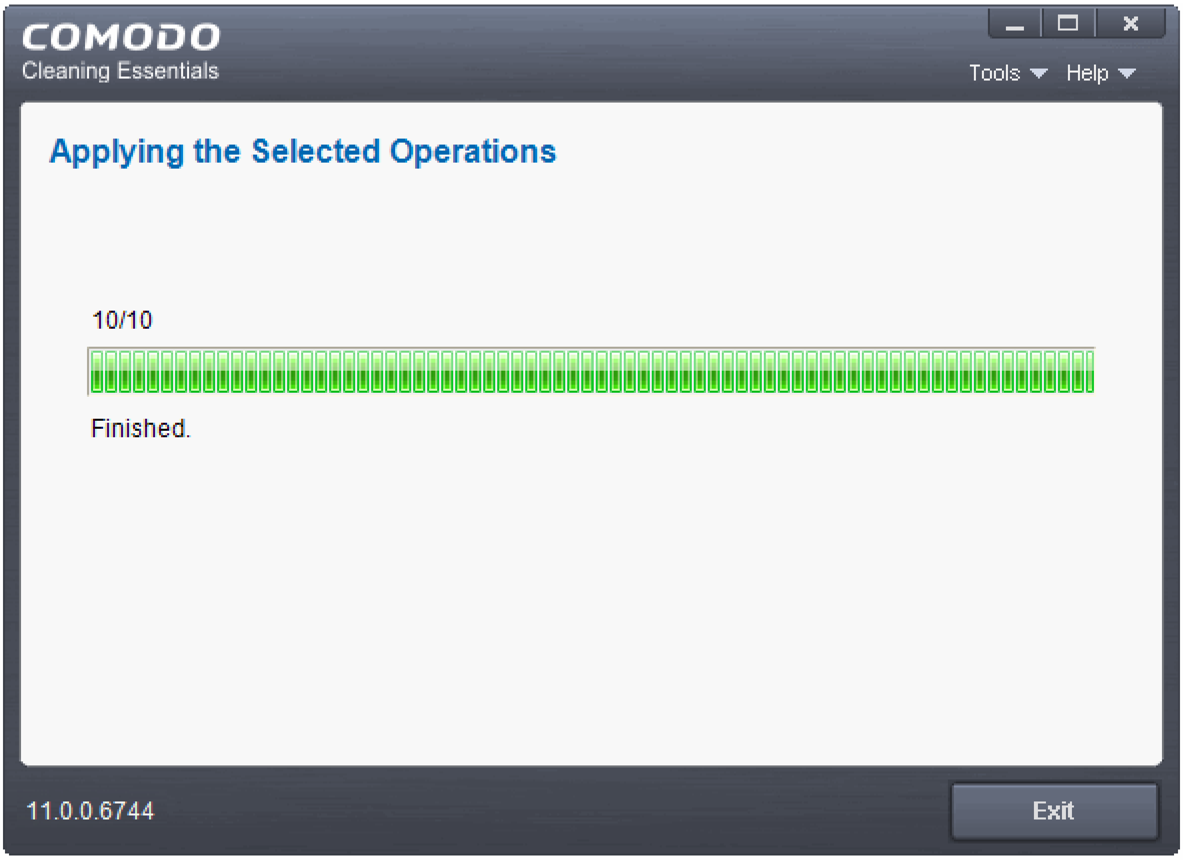
Click on the 'Operations >' column header to apply one action to all files in the list.

- Click 'Apply' to implement your actions.
- You now need to restart your computer. This is so CCE can check whether the threats have been completely removed, and to scan for hidden services and drivers:



Your computer will now be restarted in order to verify that all the threats are removed.
Would you like to restart it now?

- Save all your work first then click 'Yes' to restart your computer. If you plan to restart later, click 'No'. The scan will run the next time you restart your computer.

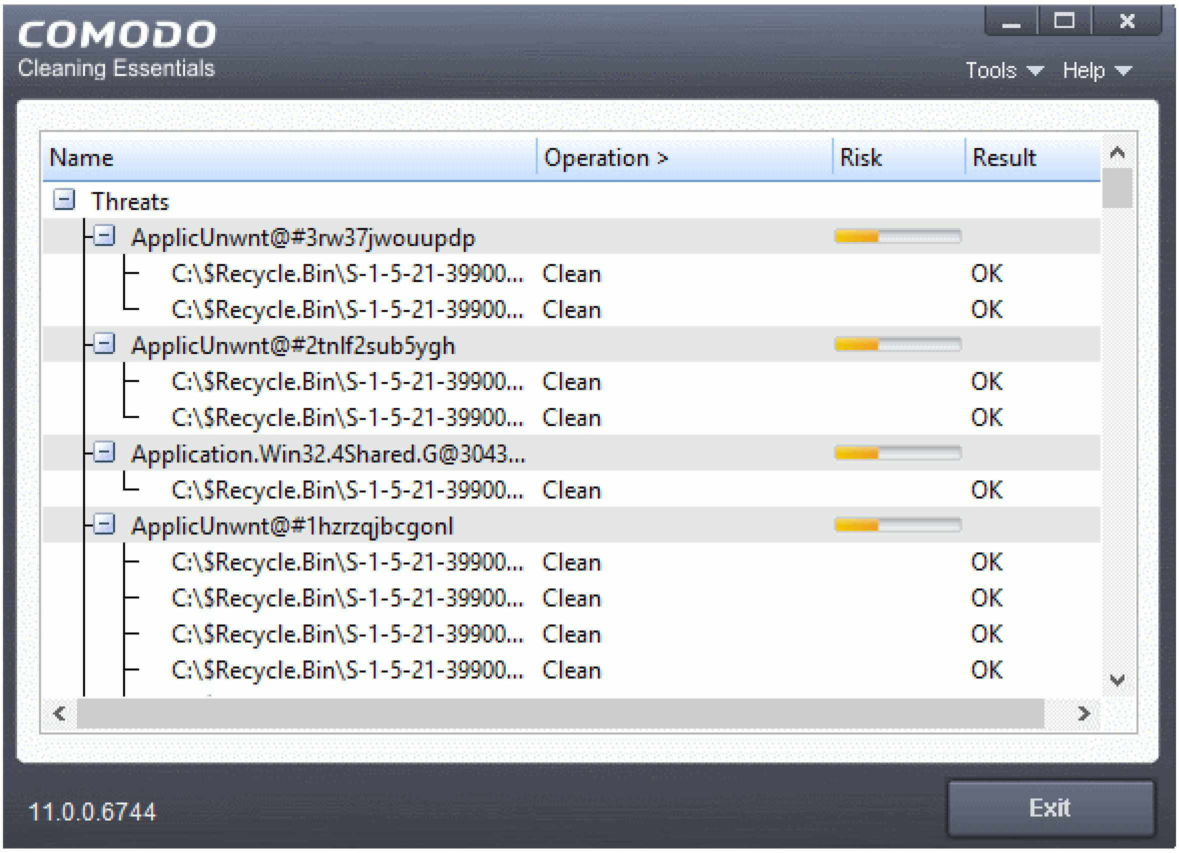


Applying the Selected Operations

10/10

Finished.

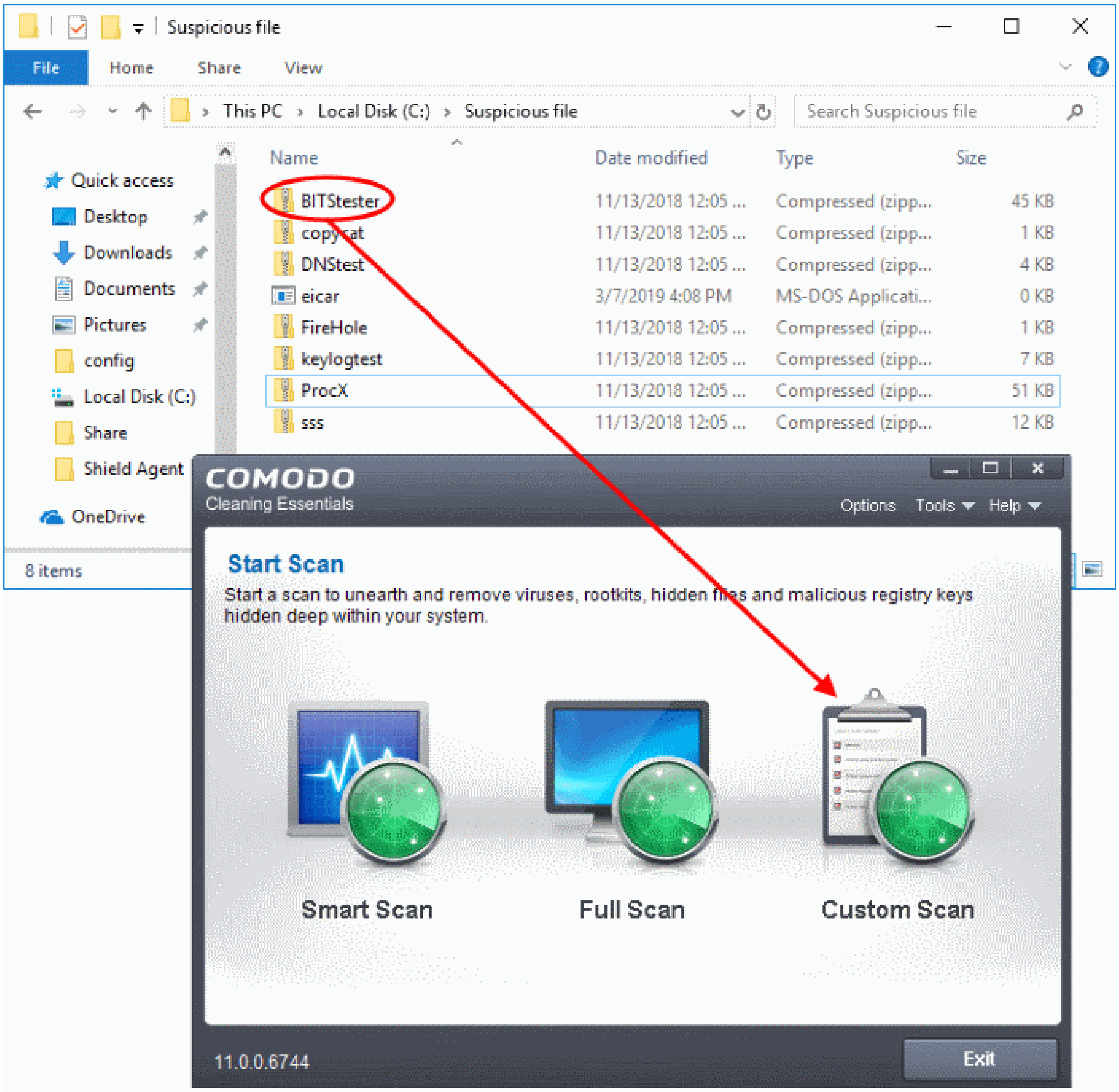
After the restart, CCE will scan for and clean any hidden processes. Results are shown as follows:



Name	Operation >	Risk	Result
Threats			
ApplicUnwnt@#3rw37jwouupdp			
C:\$Recycle.Bin\S-1-5-21-39900...	Clean		OK
C:\$Recycle.Bin\S-1-5-21-39900...	Clean		OK
ApplicUnwnt@#2tnlf2sub5ygh			
C:\$Recycle.Bin\S-1-5-21-39900...	Clean		OK
C:\$Recycle.Bin\S-1-5-21-39900...	Clean		OK
Application.Win32.4Shared.G@3043...			
C:\$Recycle.Bin\S-1-5-21-39900...	Clean		OK
ApplicUnwnt@#1hzrzqjbcgonl			
C:\$Recycle.Bin\S-1-5-21-39900...	Clean		OK
C:\$Recycle.Bin\S-1-5-21-39900...	Clean		OK
C:\$Recycle.Bin\S-1-5-21-39900...	Clean		OK
C:\$Recycle.Bin\S-1-5-21-39900...	Clean		OK

Instant Scans

- You can scan a folder or file any file or folder by dragging it on to the CCE interface:

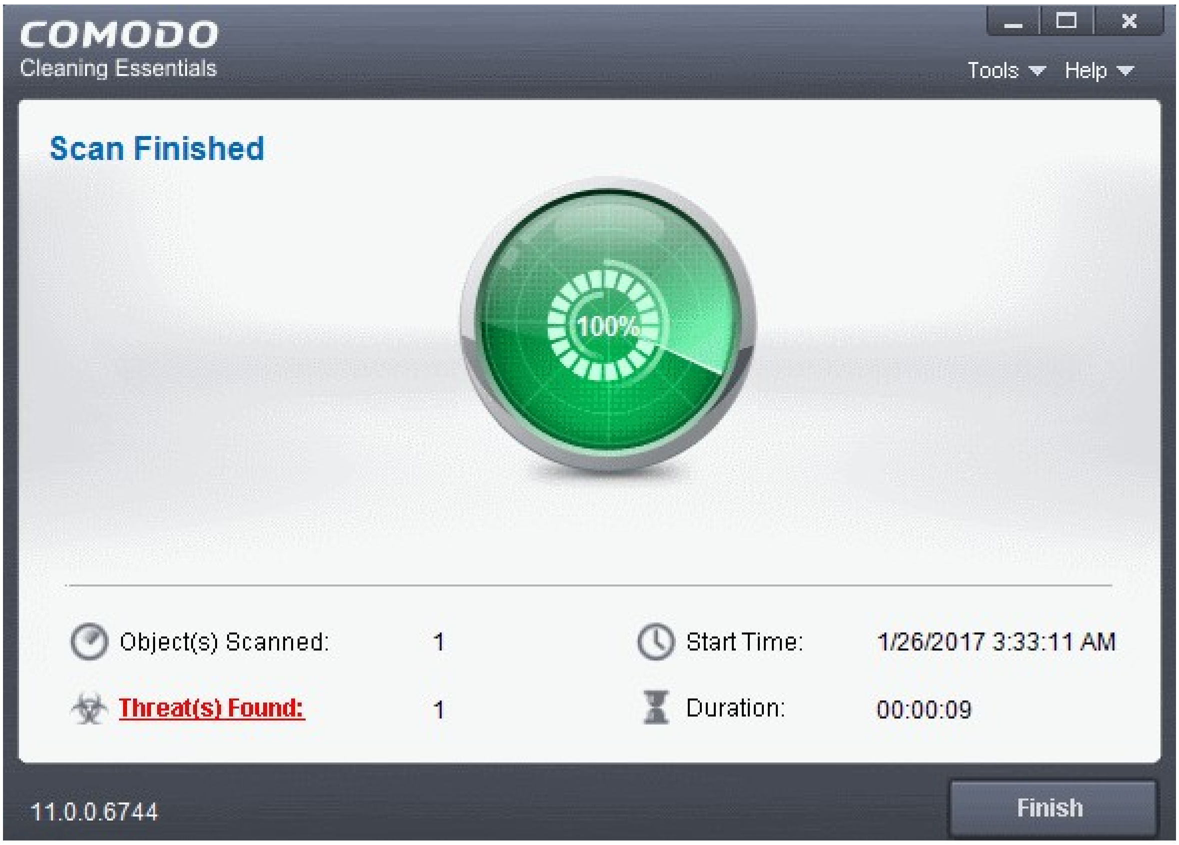


Name	Date modified	Type	Size
BITStester	11/13/2018 12:05 ...	Compressed (zipp...	45 KB
copycat	11/13/2018 12:05 ...	Compressed (zipp...	1 KB
DNStest	11/13/2018 12:05 ...	Compressed (zipp...	4 KB
eicar	3/7/2019 4:08 PM	MS-DOS Applicati...	0 KB
FireHole	11/13/2018 12:05 ...	Compressed (zipp...	1 KB
keylogtest	11/13/2018 12:05 ...	Compressed (zipp...	7 KB
ProcX	11/13/2018 12:05 ...	Compressed (zipp...	51 KB
sss	11/13/2018 12:05 ...	Compressed (zipp...	12 KB

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: 1

Start Time: 1/26/2017 3:33:11 AM

Duration: 00:00:09

Results are shown at the end of the scan. See **Results** if you want help with the actions you can take on this screen.

2.4. Comparison of Scan Types

Scanners

The following table shows the types of scanners in Comodo Cleaning Essentials:

Scanner	Description
Basic	Local, signature based antivirus scanner.
FLS	File Lookup System. The FLS attempts to establish the trust rating 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 then it passes onto Comodo's cloud based AV scanner.
CAMAS	COMODO Automated Malware Analysis System (CAMAS). CCE uploads files that have an unknown trust rating to CAMA for further inspection. This needs to be enabled in options.
Memory	Scans running processes and modules.
Hidden file	Scan for invisible files and directories.
Hidden key	Scan for invisible keys and values.
Hidden service	Scan for invisible services and drivers (requires restart).
Critical areas	Scan important registry keys, user data folders, and system files/folders
MBR	Scan boot sector (available if enabled in options).

Scan Types

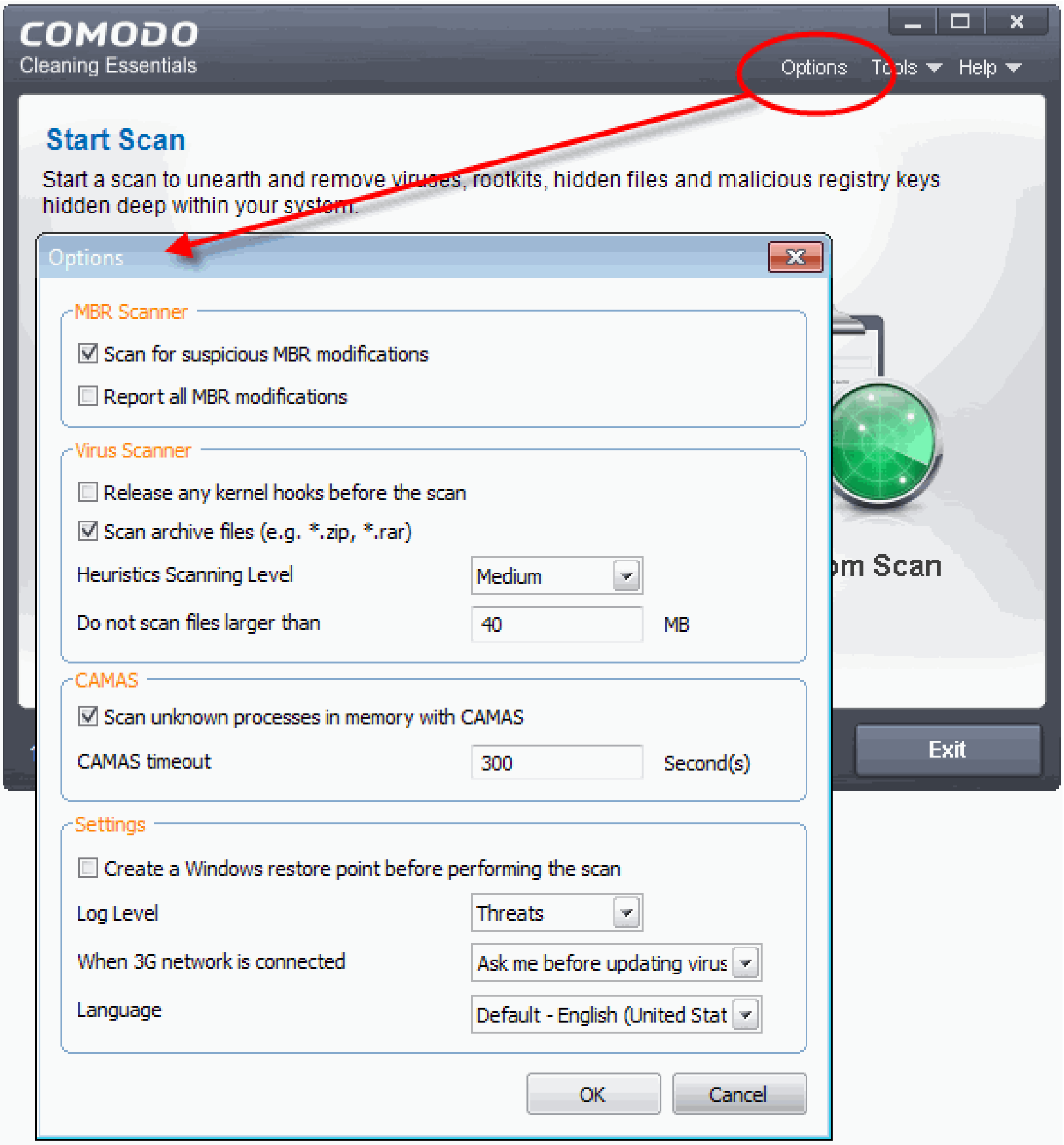
The following table shows the sequence of scanners used during different scan types.

For example, ‘Basic > FLS’ means that the item is first checked using the Basic (local) AV scanner. If the item is not identified as malware then it passes onto the next scan type - ‘FLS’.

Scan Options	Smart Scan	Full Scan	Custom Scan (Scanners are the same as Full Scan)
Memory	Basic > FLS Scope: all running modules	Basic > FLS > CAMAS > Memory Scope: all running modules	Optional. Scope: all running modules
Critical areas and boot sector	Critical areas > MBR Scope: entire areas	Critical areas > MBR Scope: entire areas	Optional. Scope: entire areas
Hidden registry objects and services	Hidden keys > Hidden services Scope: autorun registry entries	Hidden key > Hidden service Scope: entire registry	Optional. Scope: entire registry
Hidden files and folders	Hidden files/folders Scope: autorun files	Hidden files/folders Scope: files in all drives	Optional. Scope: files in all drives
Virus	Basic > FLS Scope: autorun files	Basic > FLS Scope: files in all drives	Optional. Scope: Customizable

3. Configure Comodo Cleaning Essentials

- Click 'Options' in the title bar to configure CCE to your preferences:



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.
om Scan
Exit

Options

MBR Scanner

☑ Scan for suspicious MBR modifications

□ Report all MBR modifications

Virus Scanner

□ Release any kernel hooks before the scan

☑ Scan archive files (e.g. *.zip, *.rar)

Heuristics Scanning Level: Medium

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: Threats

When 3G network is connected: Ask me before updating virus

Language: Default - English (United Stat

MBR Options

- **Scan for suspicious MBR modifications -** CCE automatically scans the master boot record (MBR) for malware, unknown files and suspicious changes. The MBR is a favorite target of advanced persistent threats.
- **Report all MBR modifications** - CCE records MBR modifications in a log file.

Virus Scanner Settings

- **Release any kernel hooks before the scan -** Advanced users only. Releasing the kernel hooks will deactivate any other security products installed on your system. This may cause system instability and lead to potential data loss. Select this option only if you are an advanced user and have knowledge on the risks of the process.
- **Scan archive files (e.g. *zip, *rar)** - Comodo Cleaning Essentials scans all types of archive files. These include RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB archives. (Default = Enabled)
- **Heuristics Scanning/Level** - CCE employs various heuristic techniques to identify previously unknown viruses and Trojan horses. Heuristics means analyzing a file to see whether it contains code typical of a virus. If it is found to do so then the application recommends it for quarantine. Heuristics detectis virus-like

attributes rather than looking for a malware signature that matches a signature on our blacklist.

The drop-down menu lets you select from four levels of heuristic sensitivity. The sensitivity determines how likely the scanner is to decide a file is malware based on its code.

  - **Off** - Disable heuristic scanning.
  - **Low** - A high level of protection with a low rate of false positives. Comodo recommends this setting for most users.
  - **Medium** - Better at detecting previously unknown malware than the 'Low' setting, but has a higher chance of producing false positives.
  - **High** - Highest sensitivity to detecting unknown threats, but with a raised level of possible false positives.

- **Do not scan files larger than** - Set the maximum size of files that CCE should scan. CCE will skip files larger than the size specified here. (Default = 40 MB)

CAMAS Settings

- CAMAS (Comodo Automated Malware Analysis System) is our cloud-based file analysis system. Unknown files submitted to CAMAS undergo thorough inspections by our cloud virus and behavior monitoring systems.
- Files which behave maliciously are added to the global blacklist. This list is passed to all CCE users via our regular database updates, protecting everyone against the newest threats.

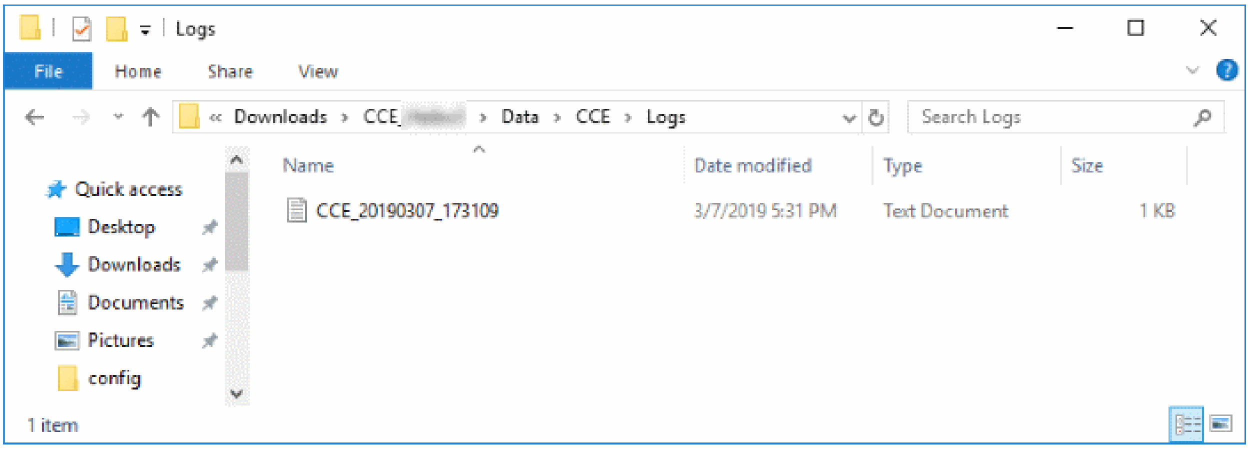
You can set the following options regarding CAMAS:

- **Scan unknown processes in memory with CAMAS** - Unknown processes running in memory will be automatically submitted to CAMAS for testing. (Default=Enabled)
- **CAMAS timeout** - Set the maximum length of time (in seconds) that CCE should spend submitting files to CAMAS. If the timeout is exceeded then CCE will stop attempting to contact CAMAS, and it is possible that no results will be returned. (Default=300 seconds)

Miscellaneous Settings

- **Create a Windows restore point before performing the scan** - CCE will create a Windows restore point just before starting a scan. You can revert your system to this previous state if any problems occur after the scan.
- **Log level** - Select CCE event log options. There are two types of logs - KillSwitch logs and CCE (scan) logs. The following options apply to both:
  - **Disable** - CCE does not create any log files.
  - **Threats** - CCE creates a log entry when it detects a malicious file. Default.
  - **All** - CCE creates log entries for all scanned files and all events. The log includes system information, cleanup results, file path and file verdict, actions taken on the file, and whether the action has been implemented.

Logs are saved in the CCE folder at Data\CCE\Logs:



« Downloads › CCE_[redacted] › Data › CCE › Logs

Name	Date modified	Type	Size
CCE_20190307_173109	3/7/2019 5:31 PM	Text Document	1 KB

To view the logs:

- Click 'Tools' > 'Browse Logs'

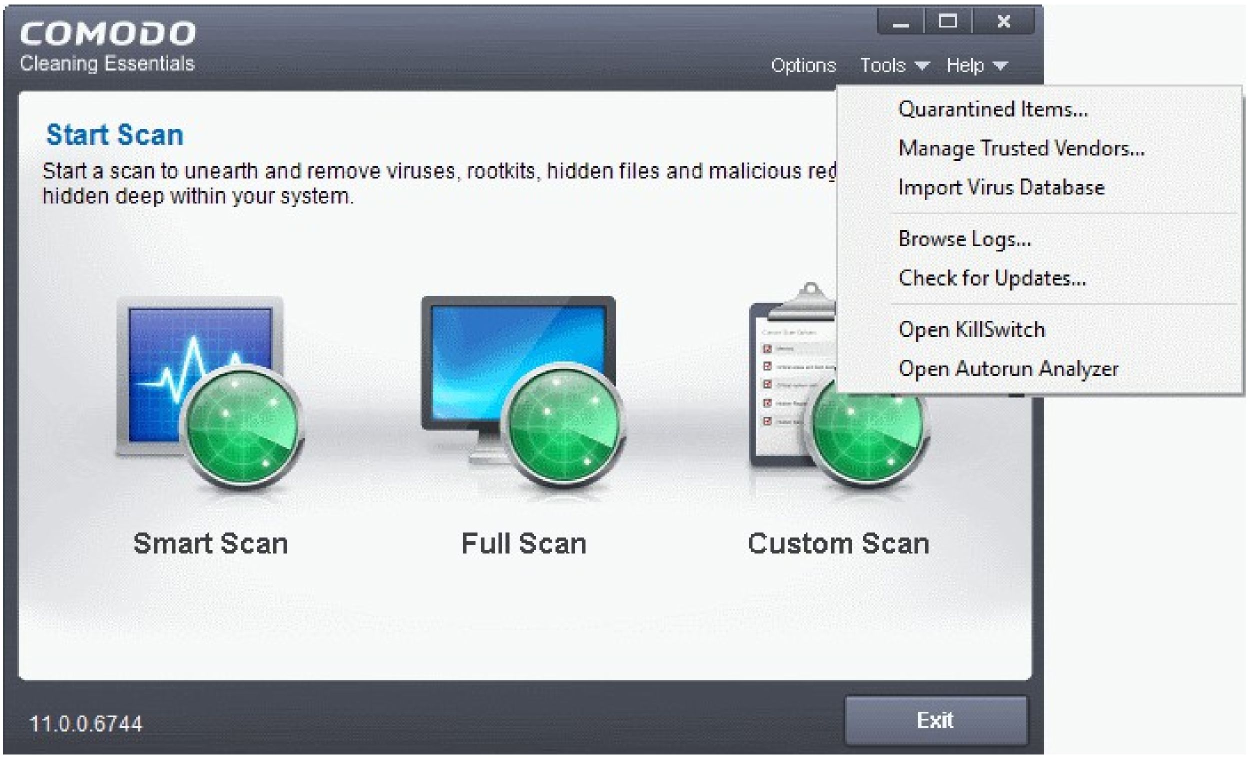
- **When 3G network is connected -** Specify how updates should be handled if CCE detects you are on a 3G connection. 3G networks are slower than regular connections and may incur additional bandwidth charges.
  - **Ask me before updating the virus database -** CCE requests your permission before downloading updates over 3G.
  - **Always update virus database** - CCE automatically downloads updates even if you are on a 3G connection
  - **Skip updating virus database** - CCE never downloads updates if you are on a 3G connection
- **Select Language -** CCE is available in several languages with the default being English (US). Use the drop-down menu to change language if required.
- Click 'OK' for your changes to take effect .

4. The Tools Menu

Click 'Tools' on the top-right menu to open this interface.

The 'Tools' menu lets you:

- **Manage Quarantined Items**
- **Manage the Trusted Vendor list**
- **Import Antivirus Database**
- **Browse Logs**
- **Check for Updates**
- **Open the KillSwitch Utility**
- **Open the Autorun Analyser**



4.1. Manage Quarantined Items

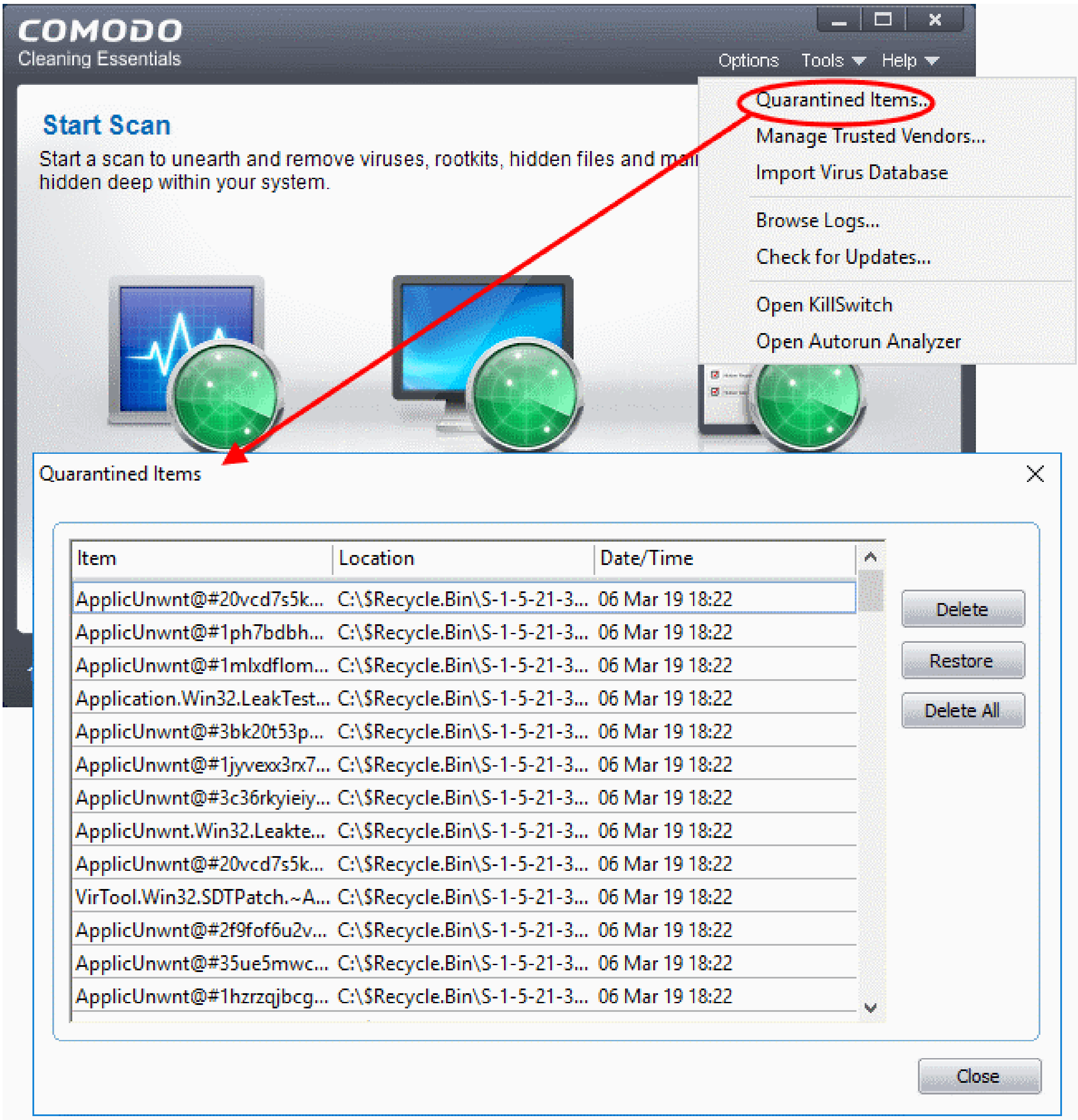
Click 'Tools' > 'Quarantined Items' to open this area.

- CCE places suspicious and harmful files in the quarantine area, where you can review them and take further actions.
- Quarantined files cannot be run or executed. This isolation prevents infected files from affecting the rest of your PC.

You can take the following actions on quarantined items:

- **Delete / Delete All** - Remove the selected files from your system.
- **Restore** - Return the file to its original location. If the file is actually malware then it will be detected by future antivirus scans.

.



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

Quarantined Items

Item	Location	Date/Time
ApplicUnwnt@#20vcd7s5k...	C:\$Recycle.Bin\S-1-5-21-3...	06 Mar 19 18:22
ApplicUnwnt@#1ph7bdbh...	C:\$Recycle.Bin\S-1-5-21-3...	06 Mar 19 18:22
ApplicUnwnt@#1mlxdflom...	C:\$Recycle.Bin\S-1-5-21-3...	06 Mar 19 18:22
Application.Win32.LeakTest...	C:\$Recycle.Bin\S-1-5-21-3...	06 Mar 19 18:22
ApplicUnwnt@#3bk20t53p...	C:\$Recycle.Bin\S-1-5-21-3...	06 Mar 19 18:22
ApplicUnwnt@#1jyvexx3rx7...	C:\$Recycle.Bin\S-1-5-21-3...	06 Mar 19 18:22
ApplicUnwnt@#3c36rkyieiy...	C:\$Recycle.Bin\S-1-5-21-3...	06 Mar 19 18:22
ApplicUnwnt.Win32.Leakte...	C:\$Recycle.Bin\S-1-5-21-3...	06 Mar 19 18:22
ApplicUnwnt@#20vcd7s5k...	C:\$Recycle.Bin\S-1-5-21-3...	06 Mar 19 18:22
VirTool.Win32.SDTPatch.~A...	C:\$Recycle.Bin\S-1-5-21-3...	06 Mar 19 18:22
ApplicUnwnt@#2f9fof6u2v...	C:\$Recycle.Bin\S-1-5-21-3...	06 Mar 19 18:22
ApplicUnwnt@#35ue5mwc...	C:\$Recycle.Bin\S-1-5-21-3...	06 Mar 19 18:22
ApplicUnwnt@#1hzrzqjbcg...	C:\$Recycle.Bin\S-1-5-21-3...	06 Mar 19 18:22

4.2. Manage Trusted Vendors

There are two way that an application can be treated as safe in Comodo Cleaning Essentials.

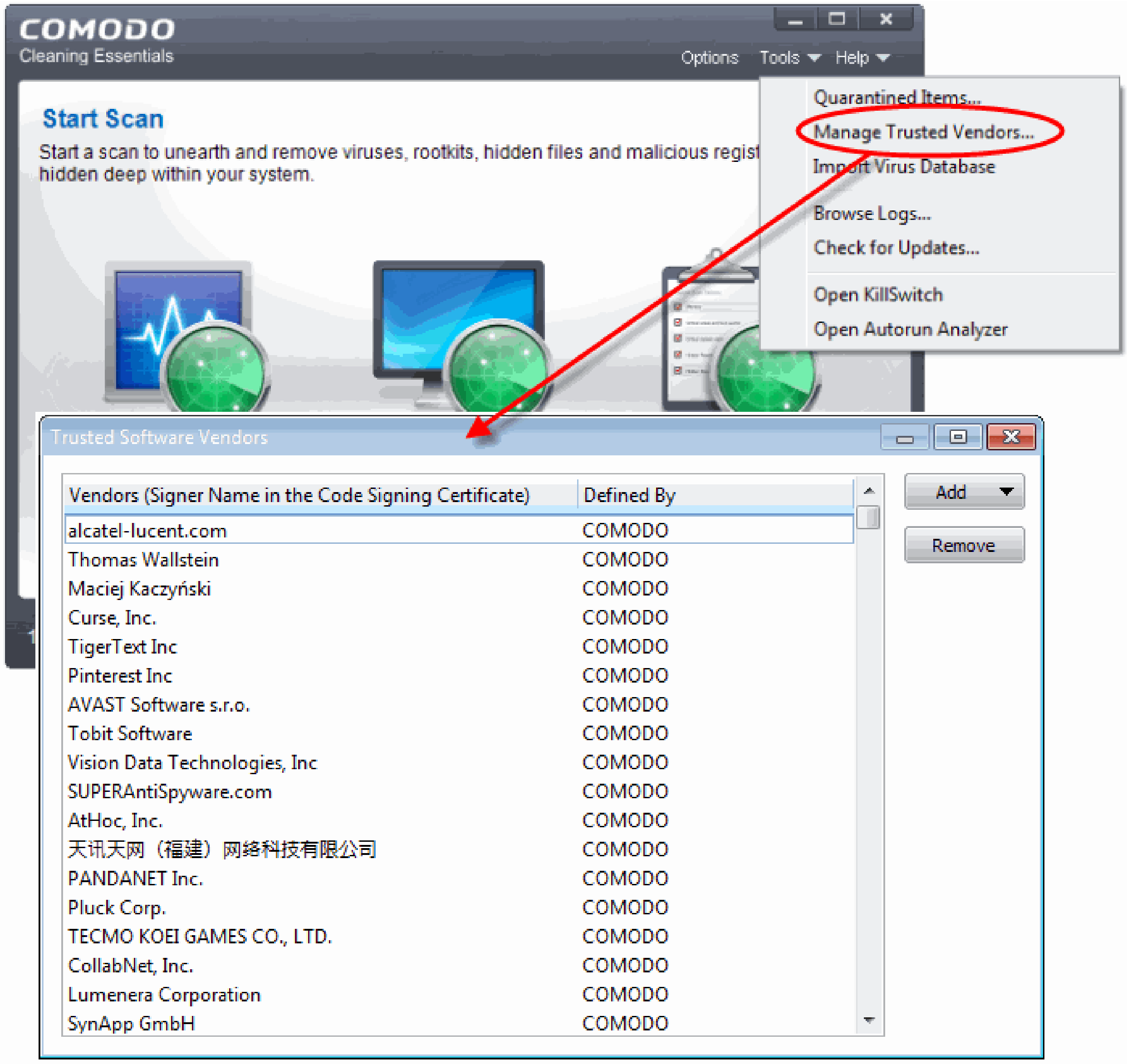
- It is whitelisted. This means it is on Comodo's list of software which we have tested and know to be safe.
- It is signed by one of the vendors in the 'Trusted Software Vendor' list.

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
alcatel-lucent.com	COMODO
Thomas Wallstein	COMODO
Maciej Kaczyński	COMODO
Curse, Inc.	COMODO
TigerText Inc	COMODO
Pinterest Inc	COMODO
AVAST Software s.r.o.	COMODO
Tobit Software	COMODO
Vision Data Technologies, Inc	COMODO
SUPERAntiSpyware.com	COMODO
AtHoc, Inc.	COMODO
天讯天网（福建）网络科技有限公司	COMODO
PANDANET Inc.	COMODO
Pluck Corp.	COMODO
TECMO KOEI GAMES CO., LTD.	COMODO
CollabNet, Inc.	COMODO
Lumenera Corporation	COMODO
SynApp GmbH	COMODO

Column Descriptions

- **Vendors** - The company that published the software, and digitally signed their software.
- **Defined By** - Indicates whether the vendor was added to 'Trusted Software Vendor' list by Comodo (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**: The software they are downloading and are about to install has not be modified or corrupted since it was signed.

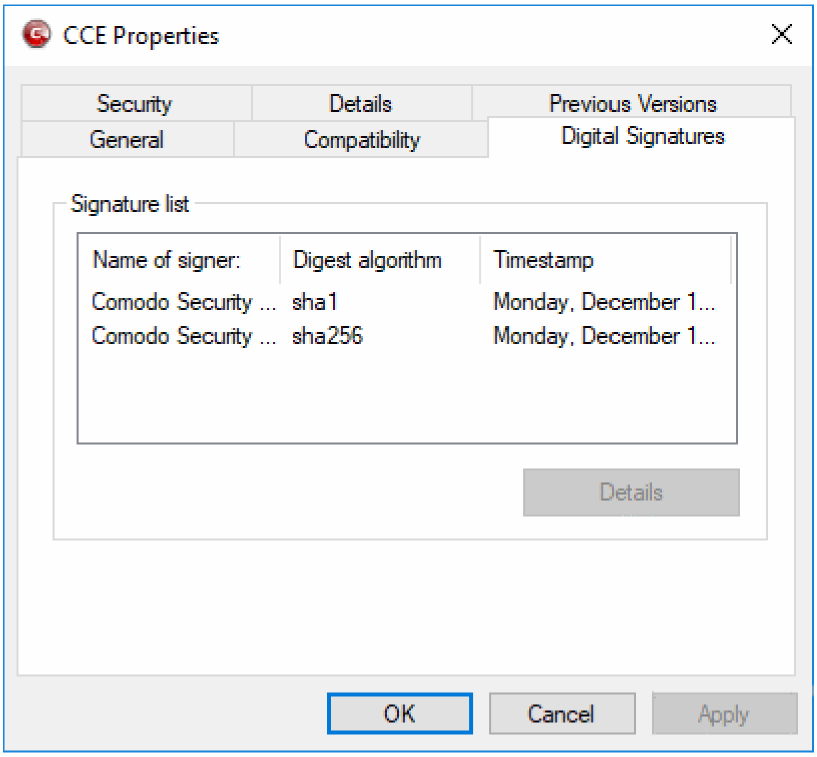
However, companies can't just 'sign' their own software and expect it to be trusted. This is why each code signing certificate is counter-signed by an organization called a 'Trusted Certificate Authority'. 'Comodo CA Limited' and 'Symantec' are two examples of Trusted CA's and are authorized to counter-sign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

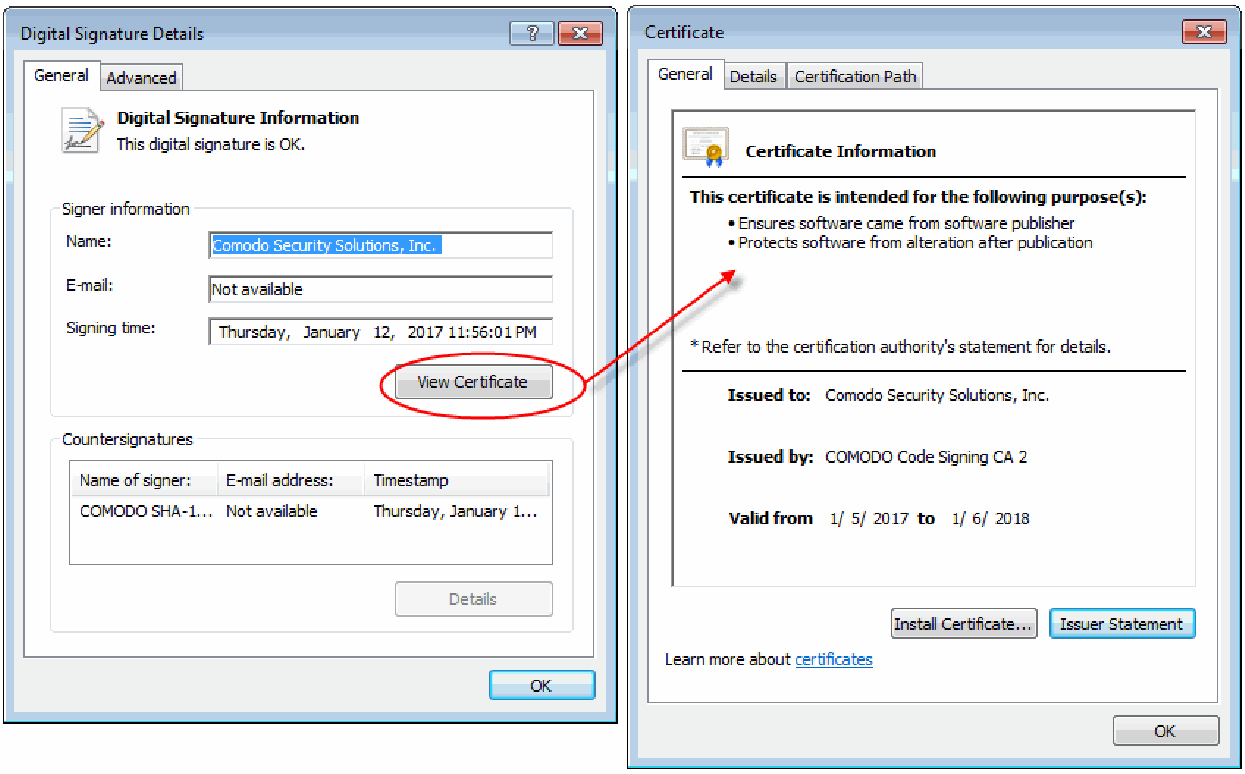
- Browse to the (default) installation directory of Comodo Cleaning Essentials
- Right click on the file cce.exe
- Select 'Properties' from the menu
- Click the tab 'Digital Signatures' (if there is no such tab then the software has not been signed).

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



Name of signer:	Digest algorithm	Timestamp
Comodo Security ...	sha1	Monday, December 1...
Comodo Security ...	sha256	Monday, December 1...

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



Digital Signature Details

Digital Signature Information

This digital signature is OK.

Signer information

Name: Comodo Security Solutions, Inc.

E-mail: Not available

Signing time: Thursday, January 12, 2017 11:56:01 PM

Countersignatures

Name of signer:	E-mail address:	Timestamp
COMODO SHA-1...	Not available	Thursday, January 1...

Certificate

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: COMODO Code Signing CA 2

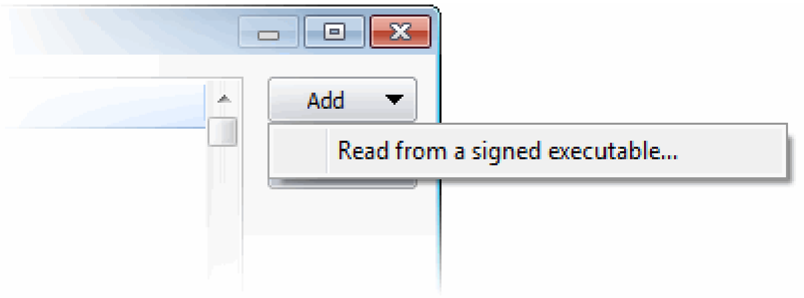
Valid from 1/ 5/ 2017 **to** 1/ 6/ 2018

Learn more about certificates

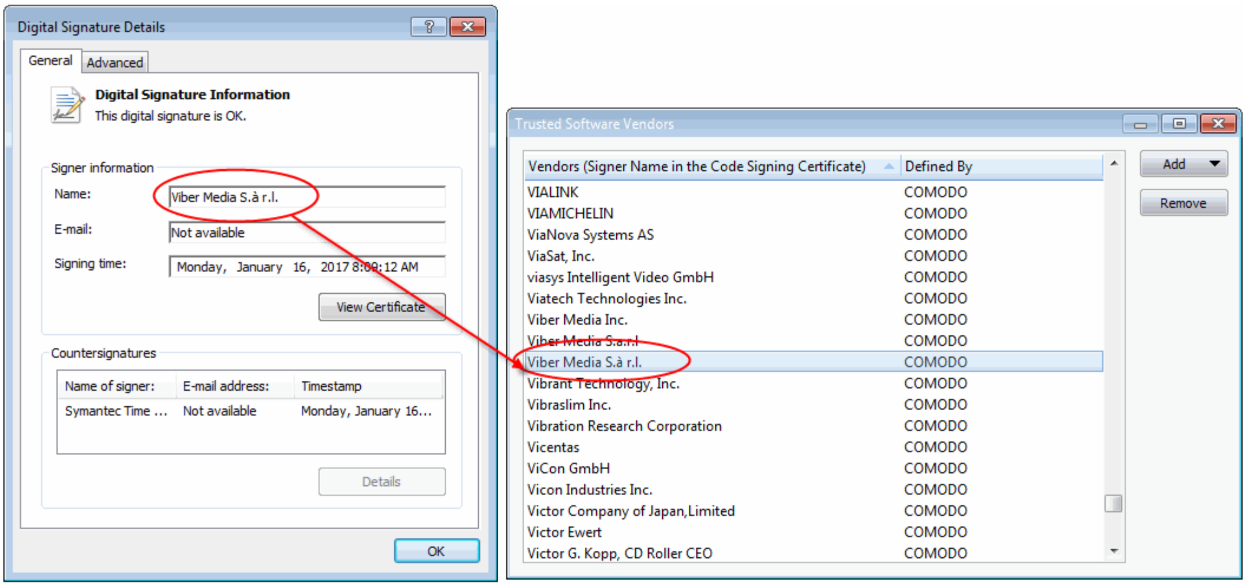
It should be noted that the example above is a special case in that Comodo, as creator of 'cce.exe', is both the signer of the software and, as a trusted CA, it is also the counter-signer (see the 'Countersignatures' box). In the vast majority of cases, the signer or the certificate (the vendor) and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

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



Digital Signature Information
This digital signature is OK.

Signer information

Name: Viber Media S.à r.l.

E-mail: Not available

Signing time: Monday, January 16, 2017 8:09:12 AM

Countersignatures

Name of signer:	E-mail address:	Timestamp
Symantec Time ...	Not available	Monday, January 16...

Vendors (Signer Name in the Code Signing Certificate)	Defined By
VIALINK	COMODO
VIAMICHELIN	COMODO
ViaNova Systems AS	COMODO
ViaSat, Inc.	COMODO
viasys Intelligent Video GmbH	COMODO
Viatech Technologies Inc.	COMODO
Viber Media Inc.	COMODO
Viber Media S.a.r.l	COMODO
Viber Media S.à r.l.	COMODO
Vibrant Technology, Inc.	COMODO
Vibraslim Inc.	COMODO
Vibration Research Corporation	COMODO
Vicentas	COMODO
ViCon GmbH	COMODO
Vicon Industries Inc.	COMODO
Victor Company of Japan,Limited	COMODO
Victor Ewert	COMODO
Victor G. Kopp, CD Roller CEO	COMODO

In the example above, CCE was able to verify and trust the vendor signature on Viber.exe because it had been counter-signed by the trusted CA 'Symantec'. The software signer 'Viber Media S.à r.l.' is now a Trusted Software Vendor and is added to the list. All future software that is signed by the vendor 'Viber Media 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. Import Antivirus Database

- CCE will periodically check Comodo servers to see whether a virus database update is available for download.
- Alternatively, you can import the updates from local storage, or from any other computer in your network that uses the same database.
- This can accelerate updates across large networks of endpoints and reduce bandwidth costs.

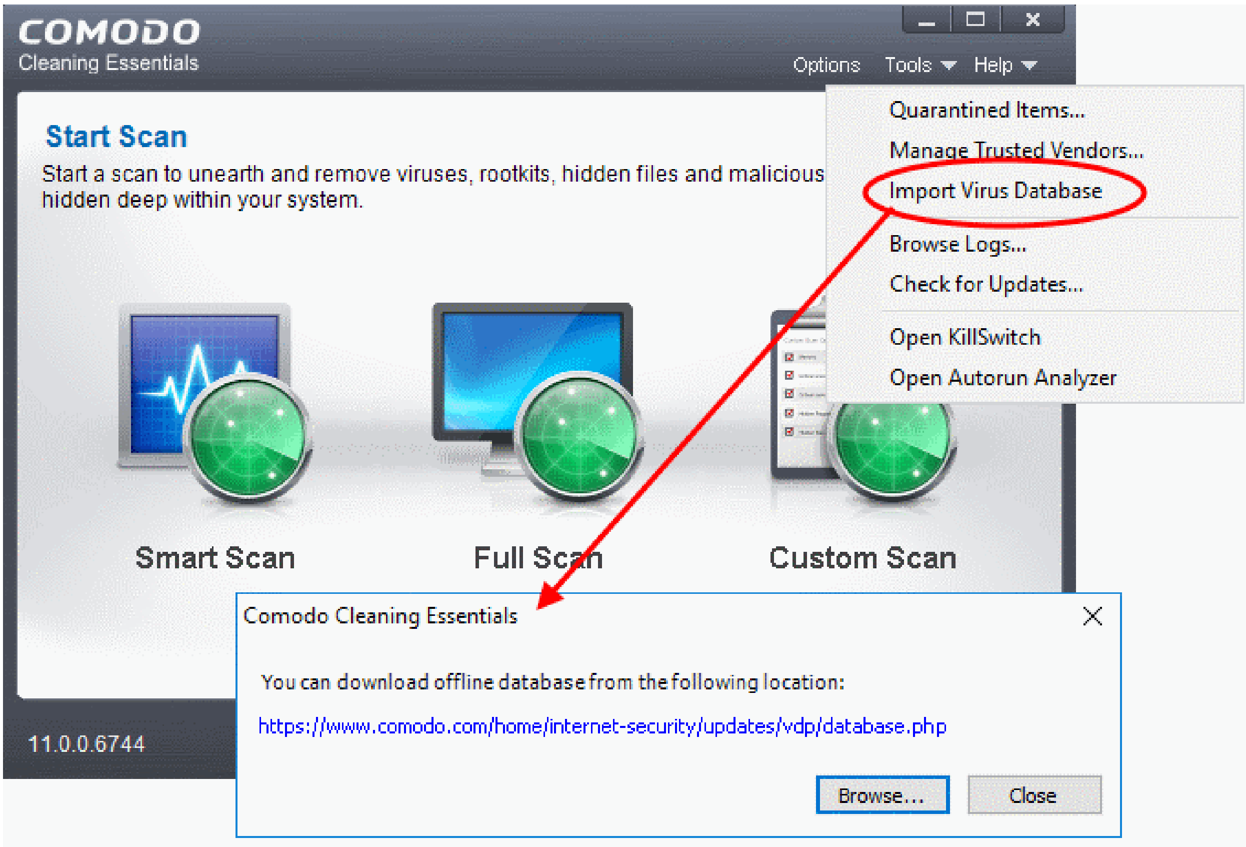
Example Scenarios:

- 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 CCE or CIS installed.

Import a virus database

- Click 'Tools' > 'Import Virus Database'



Comodo Cleaning Essentials

You can download offline database from the following location:

https://www.comodo.com/home/internet-security/updates/vdp/database.php

The dialog containing the last updated database will be displayed.

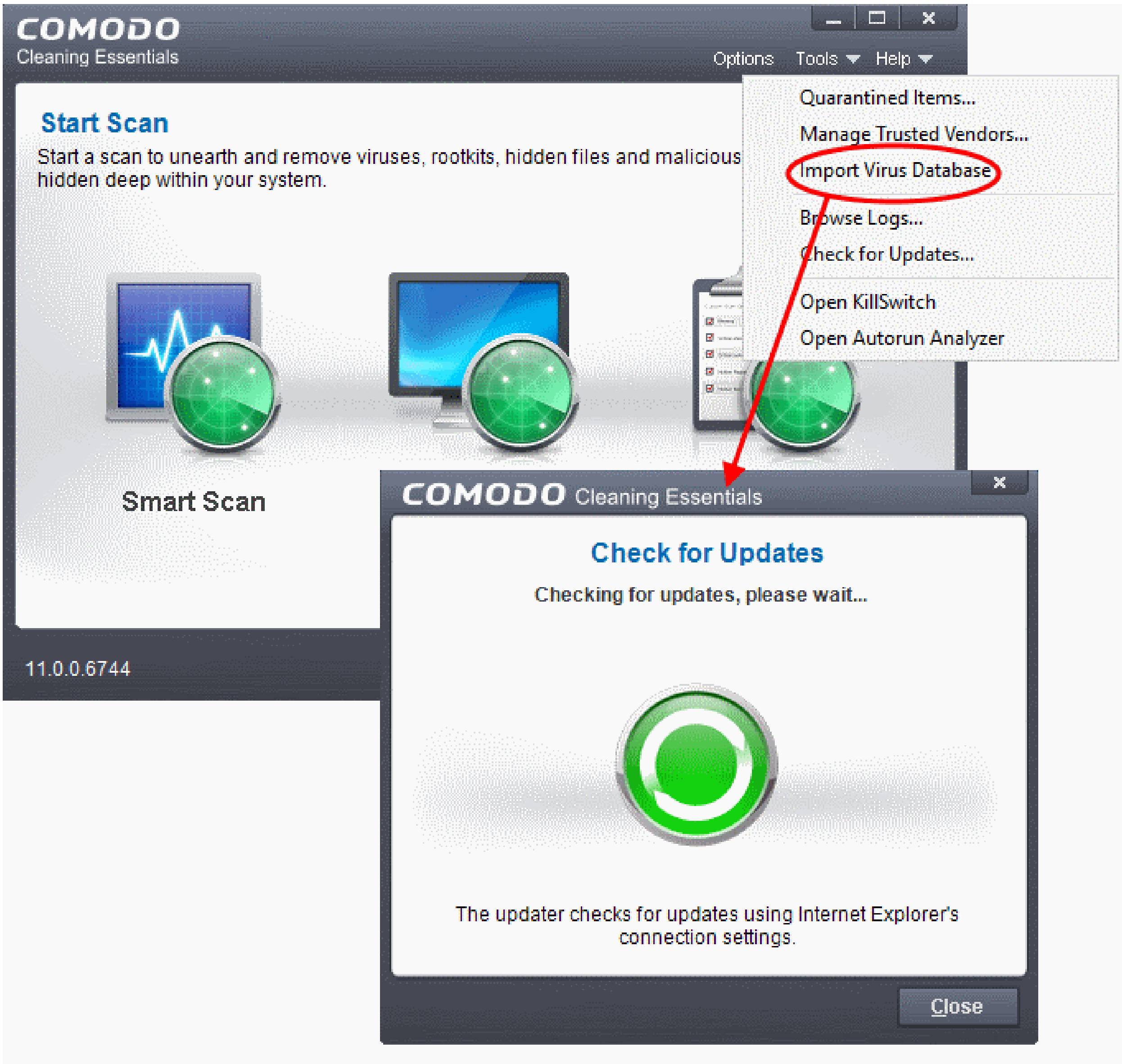
- If required, click the link to download the latest database from the Comodo web site. Save the file to a local or network location.
- Click 'Browse' to select and open a local/network copy of the database.

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.

The database file will be immediately imported to CCE.

4.4. Check for Software Updates

CCE will periodically check for application updates. If an updated version is available you will be prompted to download the new version.



Start Scan

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

Check for Updates

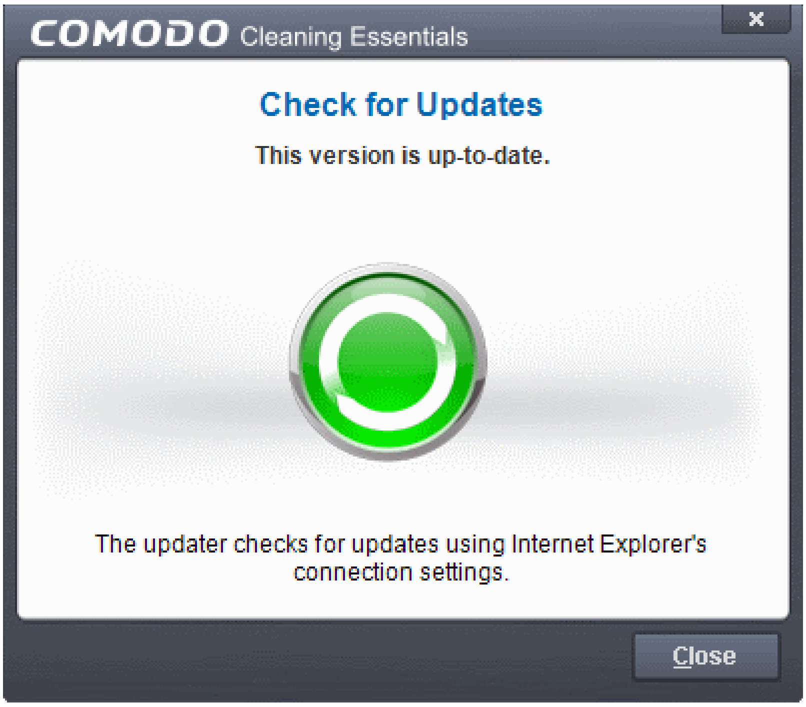
Checking for updates, please wait...

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

To manually check for the software updates

- Click 'Tools' > 'Check for Updates'

The application will connect to Comodo servers and check for updates:



COMODO Cleaning Essentials

Check for Updates

This version is up-to-date.

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 receive a message that your software is up-to-date..

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 terminates all running applications and processes created by the currently logged-in user.
    - 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**
    - **Start KillSwitch**
    - **The Main Interface**
- **View and Handle Processes, Applications and Services**
    - **Processes**
        - **Stop, Start and Handle the Processes**
        - **View Properties of a Process**
    - **Applications**
        - **Handle the Applications**
    - **Services**
        - **Stop, Start and Delete the Services**
- **View and Handle Network Connections and Usage**
    - **Network Connections**
        - **Inspect and Close Network Connections**
    - **Network Utilization**
- **Configure KillSwitch**
- **KillSwitch Tools**
    - **View System Information**
    - **Repair Windows Settings and Features**
    - **Analyze Program Usage**
    - **Search for Handles or DLLs**
    - **Verify Authenticity of Applications**
    - **Boot Log and Handle Loaded Modules**
    - **Run Programs from Command Line Interface**
    - **View KillSwitch Logs**
    - **Find Process of the Active Window**
- **Manage Currently Logged-in Users**
- **Help and About Details**

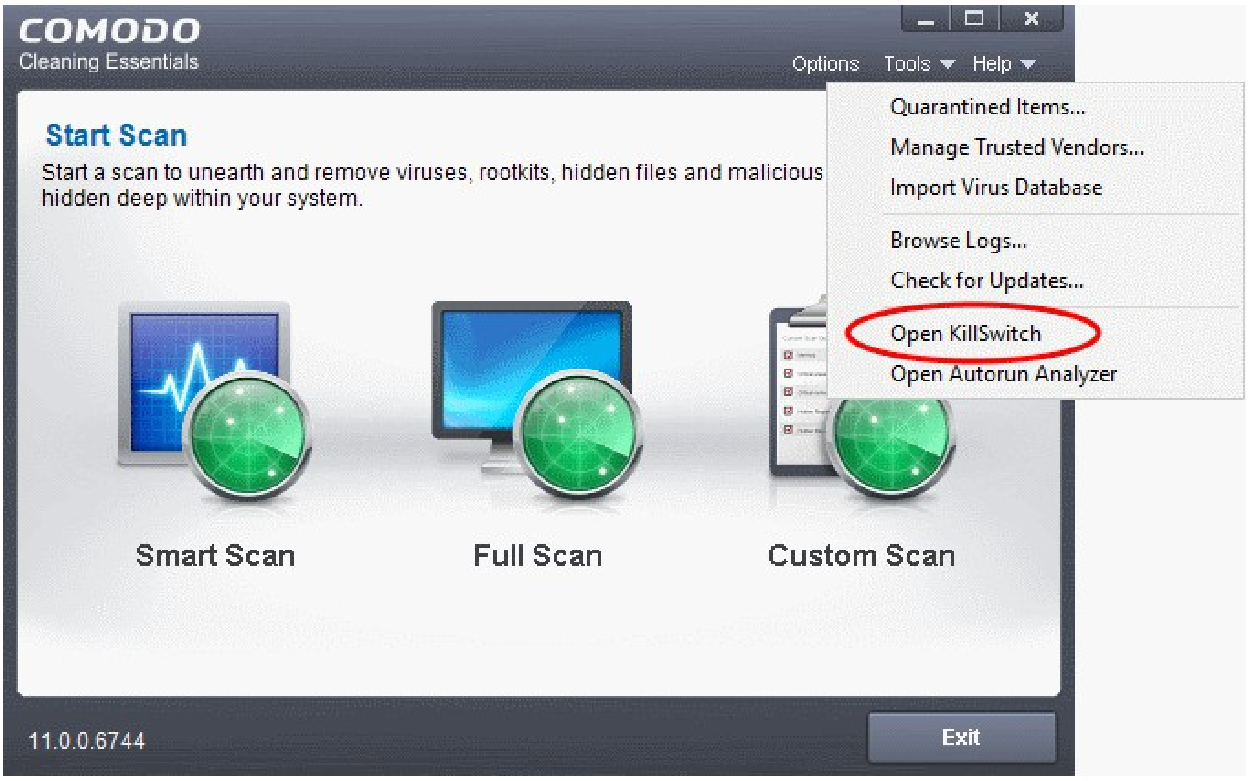
5.1. Start KillSwitch

KillSwitch can be started in 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

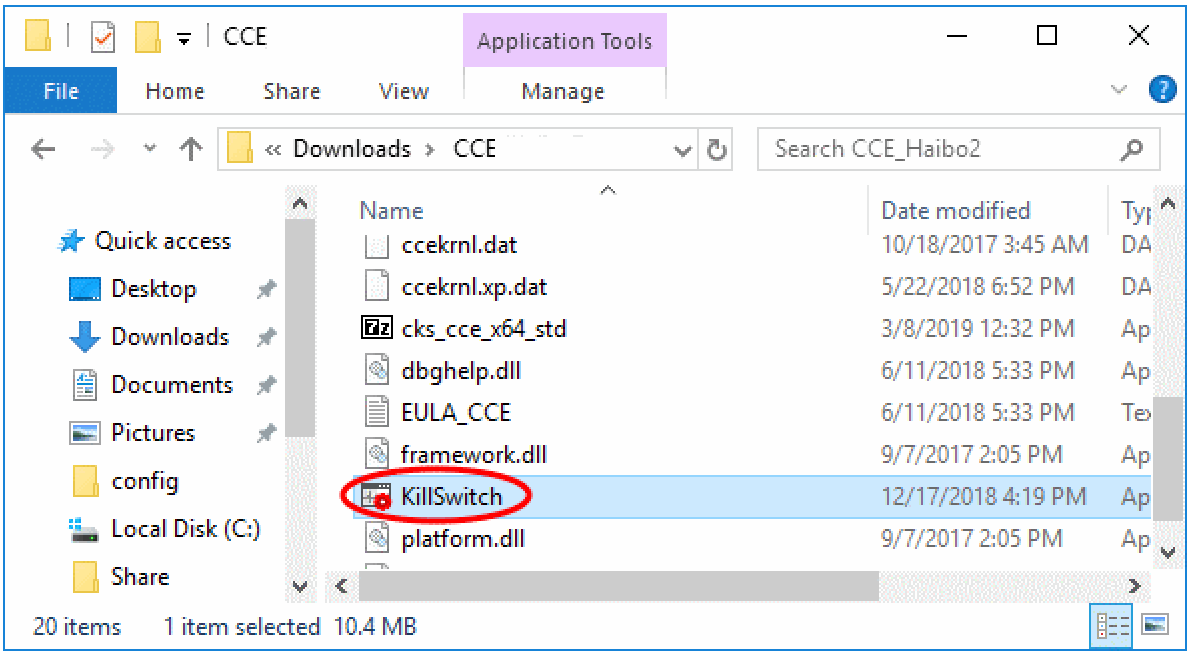
- Open CCE
- Click 'Tools' > 'Open KillSwitch'
  - Hold 'Shift' then click 'Tools' > 'Open KillSwitch' to open the app in **aggressive mode**



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

5.1.2. From the Folder Containing Comodo Cleaning Essentials Files

- Open the folder containing the CCE files
- Open 'KillSwitch.exe' (double-click the file)
  - Hold 'Shift' then double-click to open the app in **aggressive mode**



Name	Date modified	Typ
ccekrnl.dat	10/18/2017 3:45 AM	DA
ccekrnl.xp.dat	5/22/2018 6:52 PM	DA
cks_cce_x64_std	3/8/2019 12:32 PM	Ap
dbghelp.dll	6/11/2018 5:33 PM	Ap
EULA_CCE	6/11/2018 5:33 PM	Te
framework.dll	9/7/2017 2:05 PM	Ap
KillSwitch	12/17/2018 4:19 PM	Ap
platform.dll	9/7/2017 2:05 PM	Ap

20 items 1 item selected 10.4 MB

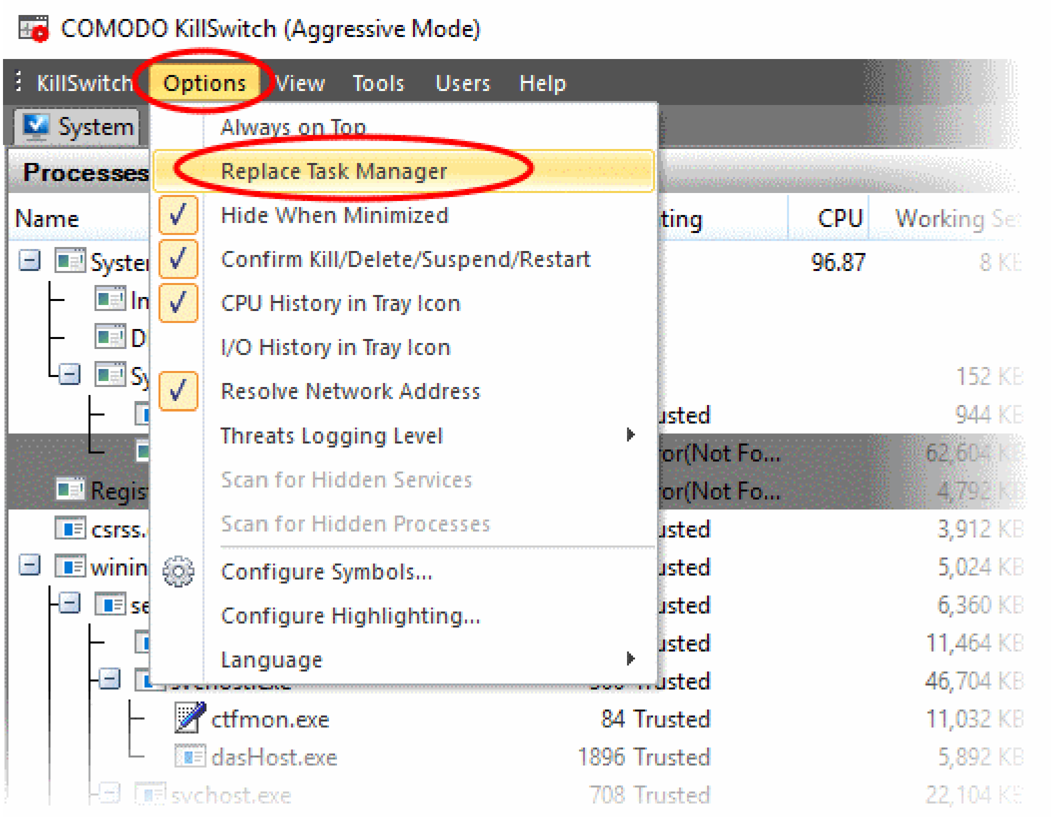
5.1.3. Replace Windows Task Manager with KillSwitch

You can configure your system to open KillSwitch instead of Windows Task Manager. If enabled, KillSwitch will open when you perform any of the following actions:

- Press Ctrl + Alt + Del then select 'Task Manager'
- Right-click on the Windows task bar and select 'Start Task Manager'
- Press Ctrl + Shift + Esc
- Click 'Start' > 'Run' and type 'taskmgr'.
  - Hold 'Shift' + any of the above to open KillSwtich in **aggressive mode**

Replace Task Manager' as follows:

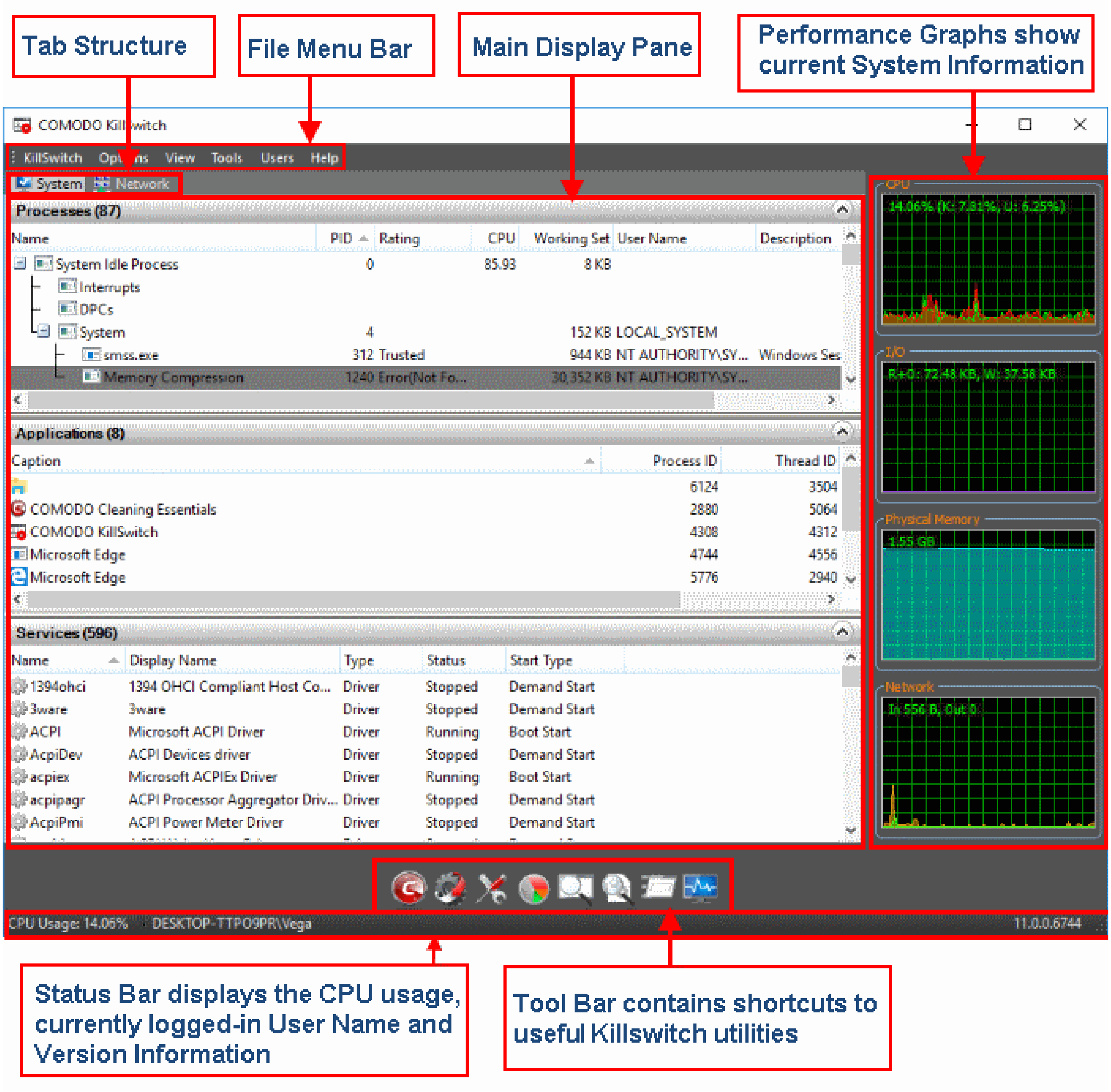
- Open CCE
- Click 'Tools' > 'Open KillSwitch'
- Click 'Options' > 'Replace Task Manager':



See '**Replace Task Manager with KillSwitch**' in '**Configure KillSwitch**', for more details.

5.2. The Main Interface

KillSwitch's streamlined interface provides easy access to all important features and options:


Tab Structure

File Menu Bar

Main Display Pane

Performance Graphs show current System Information

Status Bar displays the CPU usage, currently logged-in User Name and Version Information

Tool Bar contains shortcuts to useful Killswitch utilities

Processes (87)

Name	PID	Rating	CPU	Working Set	User Name	Description
System Idle Process	0		85.93	8 KB		
Interrupts						
DPCs						
System	4			152 KB	LOCAL_SYSTEM	
smss.exe	312	Trusted		944 KB	NT AUTHORITY\SY...	Windows Ses
Memory Compression	1240	Error(Not Fo...		30,352 KB	NT AUTHORITY\SY...	

Applications (8)

Caption	Process ID	Thread ID
	6124	3504
COMODO Cleaning Essentials	2880	5064
COMODO KillSwitch	4308	4312
Microsoft Edge	4744	4556
Microsoft Edge	5776	2940

Services (596)

Name	Display Name	Type	Status	Start Type
1394ohci	1394 OHCI Compliant Host Co...	Driver	Stopped	Demand Start
3ware	3ware	Driver	Stopped	Demand Start
ACPI	Microsoft ACPI Driver	Driver	Running	Boot Start
AcpiDev	ACPI Devices driver	Driver	Stopped	Demand Start
acpiex	Microsoft ACPIEx Driver	Driver	Running	Boot Start
acpipagr	ACPI Processor Aggregator Driv...	Driver	Stopped	Demand Start
AcpiPmi	ACPI Power Meter Driver	Driver	Stopped	Demand Start

CPU Usage: 14.06% DESKTOP-TTPO9PR\Vega 11.0.0.6744

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 Untrusted Processes	Stops all running processes that KillSwitch has identified as unknown. • An untrusted process is one with an 'unknown' trust rating. The process is not in our malware blacklist, but is also not on our whitelist of safe processes. • All malware starts life as an unknown process. It is only after the process has demonstrated malicious intent that the virus companies will add it to their blacklists. • By killing unknown processes you ensure that only verified safe processes are running on your machine. Note - stopping a process means you lose any unsaved data being used by the application. Save all data you need before selecting this option.
	Suspend All Untrusted Process	Temporarily halts all running processes that KillSwitch has identified as unknown. • Processes will be held in their current states. • They can be restarted in the 'Process' tab by right-clicking on the process and selecting 'Resume'.
	Save Current View	Export the data currently shown in the main display area as a .csv file.
	Save	Export the data in all displayed panes as a .csv file.
	Shutdown	Perform power and login actions. Place your mouse over the shut-down options to open the following menu: • Shutdown • Power-off • Restart • Sleep • Hibernate • Lock • Log off
	Exit	Closes the KillSwitch application.
Options		Configure the overall behavior of the application. See '**Configure KillSwitch**' for more details.
View		Options related to application display:

	System Information	Statistics about system resource usage. See '**View System Information'** for more details.
	Show Only the Untrusted Images in Memory	Display only memory items considered risky by KillSwitch
	Show Only Untrusted Processes	Display only running processes that KillSwitch considers unknown.
	Show Only Sandboxed Processes	Display only applications that are running in the container.
	Hide Processes Signed by Microsoft	Temporarily remove Microsoft certified processes from the list. This makes analysis easier by reducing the number of processes on display.
	Show All Processes	Display all running applications, startup programs, system resources and more.
	Opacity	Set the transparency level of the KillSwitch window. The choices range from 10% to full opaque.
	Refresh Now	Updates and renews the KillSwitch window.
	Set Refreshing Rate	Set the interval at which KillSwitch will update details in the main display area. Choices range from fast (0.5 seconds) to very slow (10 seconds).
	Performance Graphs	Switches the display of the performance graphs at the right hand side of the main interface.
	Toolbar	Switches the display of the toolbar containing shortcuts to utilities at the bottom of the interface.
	Select Columns	Configure which column are shown in different KillSwitch screens. See '**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. See '**The Tools Menu**' for more details.
	Start Comodo Cleaning Essentials	Opens the scan interface which allows you to run full, smart or custom scans on your system. See **Scan Your System** 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. See **Repair 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. See **Analyze 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. See **Search 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. See '**Verify 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. See **Boot Log and Handle Loaded Modules** for more details.
	Run	Opens the Windows 'Run' dialog for executing command line interface programs with default limited user privileges. See **Run 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. See **Viewing KillSwitch Logs** for more details.
Users		Enables to manage the status of user(s) that have currently logged-on to the system. See '**Manage 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. See **Help and About Details** for more details.
	Search	Opens online Comodo Cleaning Essentials help guide.
	About	View product version, license and copyright information.

Tab Structure

The tab pane 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		Shows currently running processes, applications and services. Click the rows to expand each pane:
	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		
	Network Connections	Running processes that have active network connections.
	Network Utilization	Shows how much network traffic is used by your system.

Main Display Pane

The main display pane shows processes, applications, services etc as per the selected tab. Right-click an entry to open a menu with relevant options.

Graphical Reports Pane

The pane shows 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
C	Opens the scan interface, allowing you to launch smart, full or custom scans on your system. See **Scan Your System** for more details.
⚙	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. See **Repair Windows Settings and Features** for more details.
◔	Opens the 'Program Usage Analyzer' window that displays a summary of usage of all the programs installed in your computer by different users. See **Analyze 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. See **Find 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. See **Search for Handles or DLLs** for more details.
▭	Opens the windows 'Run' dialog for executing command line interface programs with default limited user privileges. See **Run Programs from Command Line Interface** for more details.

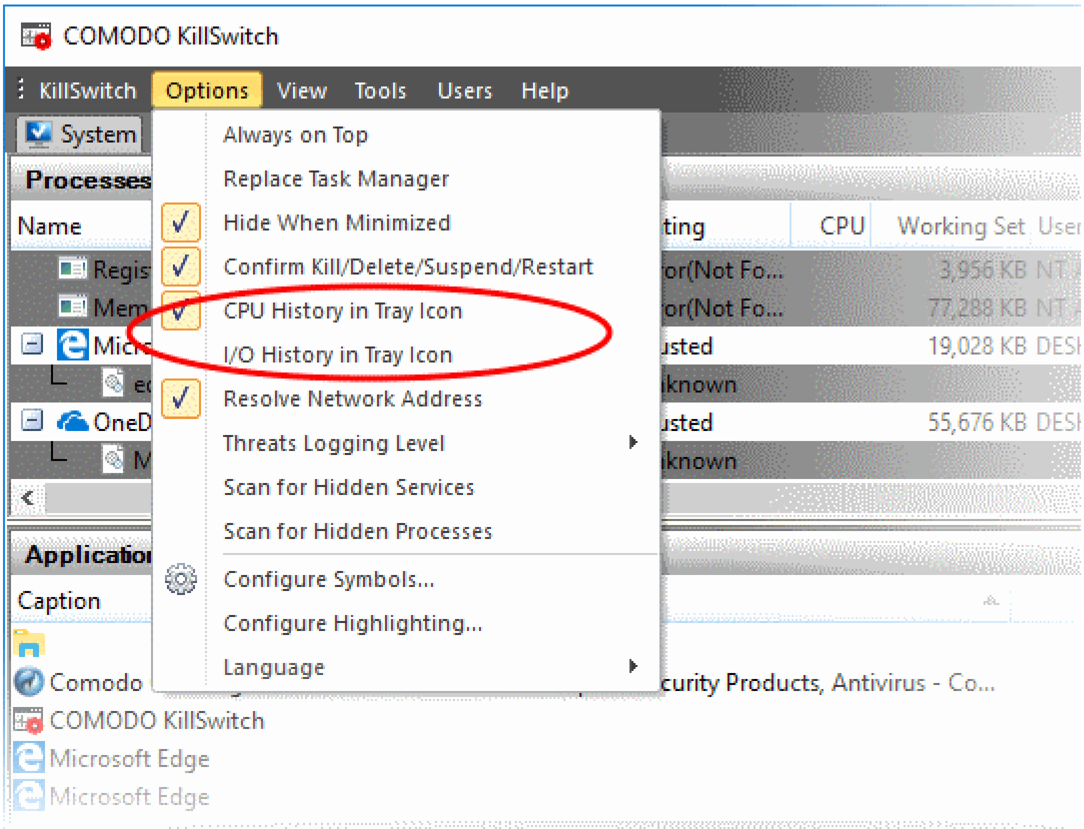
	Opens the System 'Information' panel that shows the graphical representations and statistics of the usage/history of your system resources. See '**View System Information**' for more details.

The Status Bar

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

5.2.1. The System Tray Icon

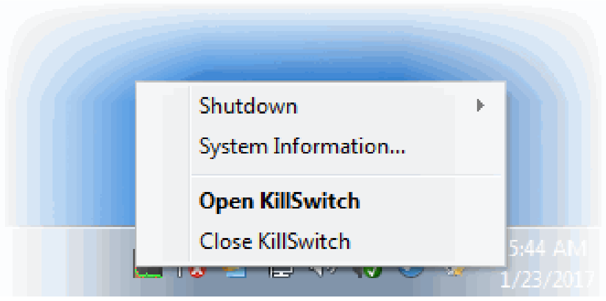
- The KillSwitch tray icon is located at the bottom-right corner of the screen.
- You can make it show CPU history, or I/O history as required:



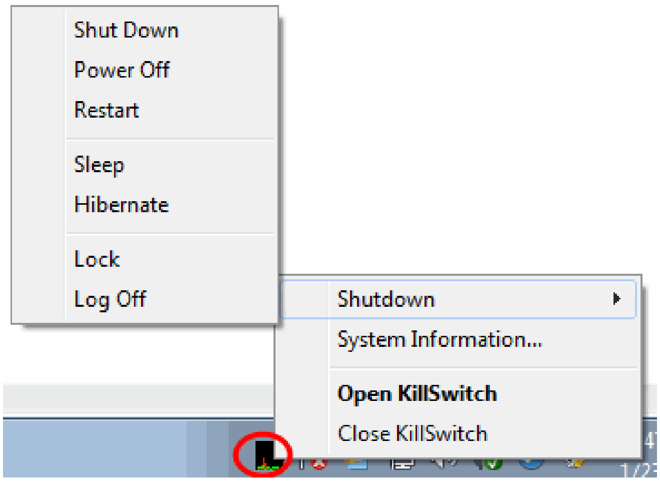
See **Configure KillSwitch** for more details.

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. See '**View System Information**' for more details.
- **Open KillSwitch -** Displays the 'KillSwitch' main interface window.
- **Close KillSwitch** - Exits the 'KillSwitch' application.

5.3. View and Handle Processes, Applications and Services

- Click 'Tools' > 'Open KillSwitch'
- Click the 'Services' tab on the KillSwitch home screen
- There are separate sections for running processes, applications, and services.

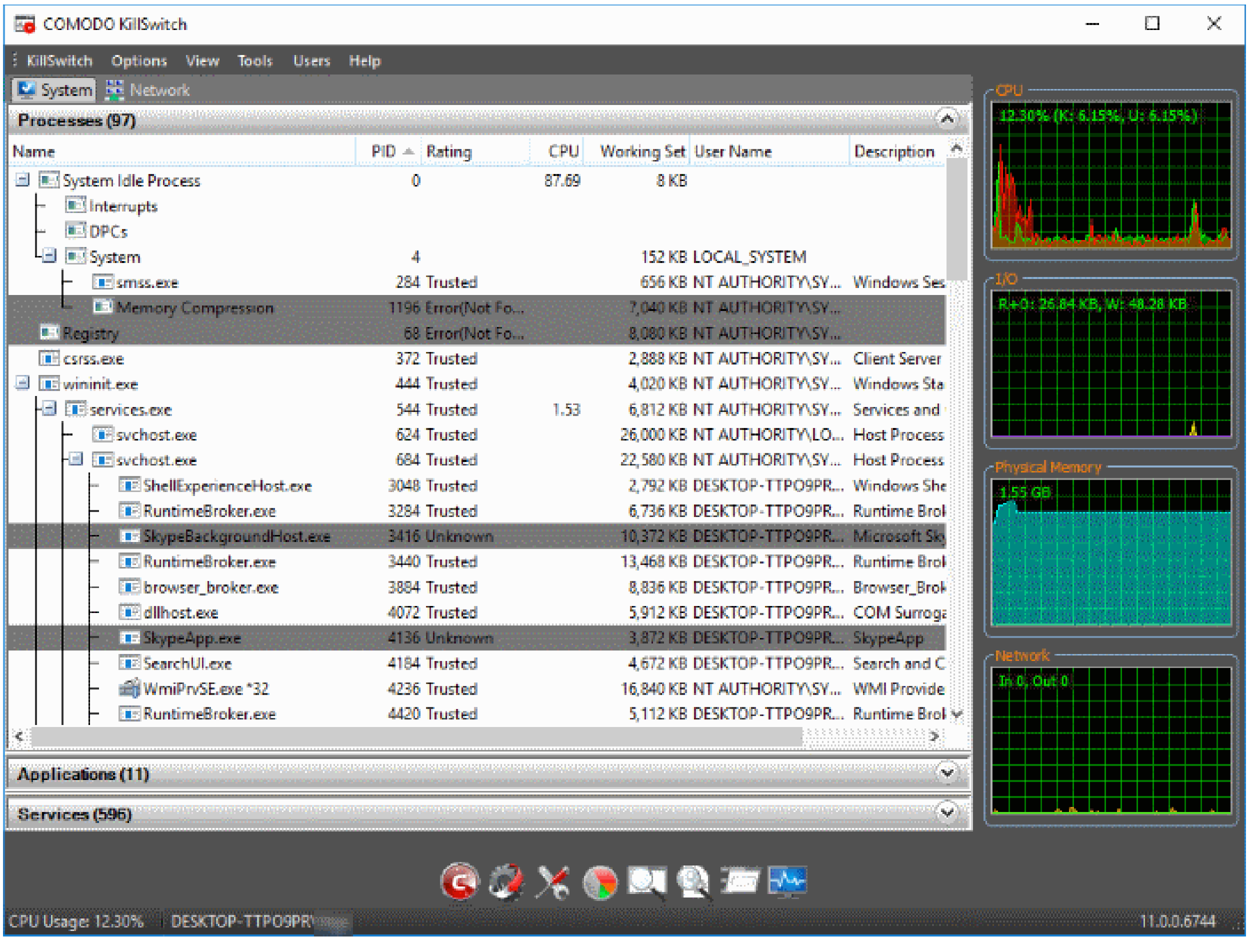
Click the links below for an explanation of each:

- **Processes**
- **Applications**
- **Services**

5.3.1. Processes

- Click 'Tools' > 'Open KillSwitch'
- Click the 'System' tab on the KillSwitch home screen
- Click the 'Processes' stripe to expand the area. The default view is all running processes.
- Different colors are used for different types of processes and the process status. Clicking 'Options' > 'Configure Highlighting' to configure these colors.
- Right-click on a process to stop, restart, set process priority, view properties etc.

- You can select multiple process by holding the 'Ctrl' key.



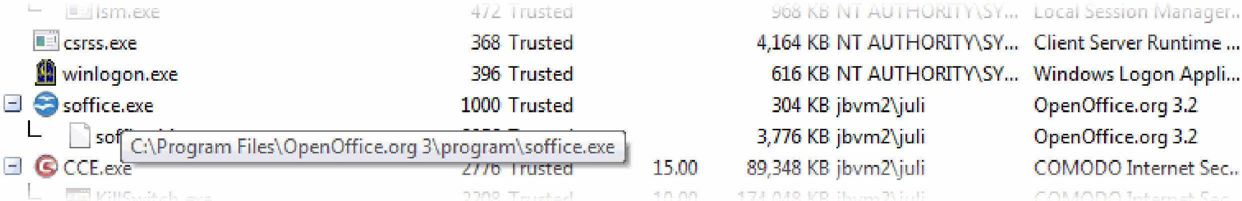
Name	PID	Rating	CPU	Working Set	User Name	Description
System Idle Process	0		87.69	8 KB		
Interrupts						
DPCs						
System	4			152 KB	LOCAL_SYSTEM	
smss.exe	284	Trusted		656 KB	NT AUTHORITY\SY...	Windows Ses
Memory Compression	1196	Error(Not Fo...		7,040 KB	NT AUTHORITY\SY...	
Registry	68	Error(Not Fo...		8,080 KB	NT AUTHORITY\SY...	
csrss.exe	372	Trusted		2,888 KB	NT AUTHORITY\SY...	Client Server
wininit.exe	444	Trusted		4,020 KB	NT AUTHORITY\SY...	Windows Sta
services.exe	544	Trusted	1.53	6,812 KB	NT AUTHORITY\SY...	Services and
svchost.exe	624	Trusted		26,000 KB	NT AUTHORITY\LO...	Host Process
svchost.exe	684	Trusted		22,580 KB	NT AUTHORITY\SY...	Host Process
ShellExperienceHost.exe	3048	Trusted		2,792 KB	DESKTOP-TTPO9PR...	Windows She
RuntimeBroker.exe	3284	Trusted		6,736 KB	DESKTOP-TTPO9PR...	Runtime Brol
SkypeBackgroundHost.exe	3416	Unknown		10,372 KB	DESKTOP-TTPO9PR...	Microsoft Sk
RuntimeBroker.exe	3440	Trusted		13,468 KB	DESKTOP-TTPO9PR...	Runtime Brol
browser_broker.exe	3884	Trusted		8,836 KB	DESKTOP-TTPO9PR...	Browser_Brol
dllhost.exe	4072	Trusted		5,912 KB	DESKTOP-TTPO9PR...	COM Surroga
SkypeApp.exe	4136	Unknown		3,872 KB	DESKTOP-TTPO9PR...	SkypeApp
SearchUI.exe	4184	Trusted		4,672 KB	DESKTOP-TTPO9PR...	Search and C
WmiPrvSE.exe *32	4236	Trusted		16,840 KB	NT AUTHORITY\SY...	WMI Provide
RuntimeBroker.exe	4420	Trusted		5,112 KB	DESKTOP-TTPO9PR...	Runtime Brol

The table below shows the default table columns. You can add or remove columns in 'View' > 'Select Columns'.

Process Table - Descriptions of Columns	
Column	**Description**
Name	Labels of the parent and child processes.
PID	Windows process identification number.
Rating	Trust rating of the process. **Trusted** - The process is on our white-list and is verified as safe to run. **Untrusted** - A process with an 'unknown' trust rating. The process is not in our malware blacklist, but is also not on our whitelist of safe processes.
Signer	The name of the entity that digitally signed the software. This is usually the company that created the software behind the process.
CPU	Processor usage as a percent of total available processor power.
Working Set	The number of page files in virtual memory referenced by the process. Background Note: The working set is the collection of information referenced by the process. Collections are stored as page files in secondary memory.
User Name	The user that started the process.
Description	Additional information about the process. This is usually provided by the software vendor to

	explain the purpose of the process.
Network Received Traffic	The total volume of traffic data received by the process since opening KillSwitch.
Network Send Traffic	The total volume of traffic data sent by the process since opening KillSwitch.

- Place your mouse over a process to view the location of the process:



lsm.exe	472	Trusted		968 KB	NT AUTHORITY\SY...	Local Session Manager..
csrss.exe	368	Trusted		4,164 KB	NT AUTHORITY\SY...	Client Server Runtime ...
winlogon.exe	396	Trusted		616 KB	NT AUTHORITY\SY...	Windows Logon Appli...
soffice.exe	1000	Trusted		304 KB	jbvm2\juli	OpenOffice.org 3.2
sof				3,776 KB	jbvm2\juli	OpenOffice.org 3.2
CCE.exe	2776	Trusted	15.00	89,348 KB	jbvm2\juli	COMODO Internet Sec..

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

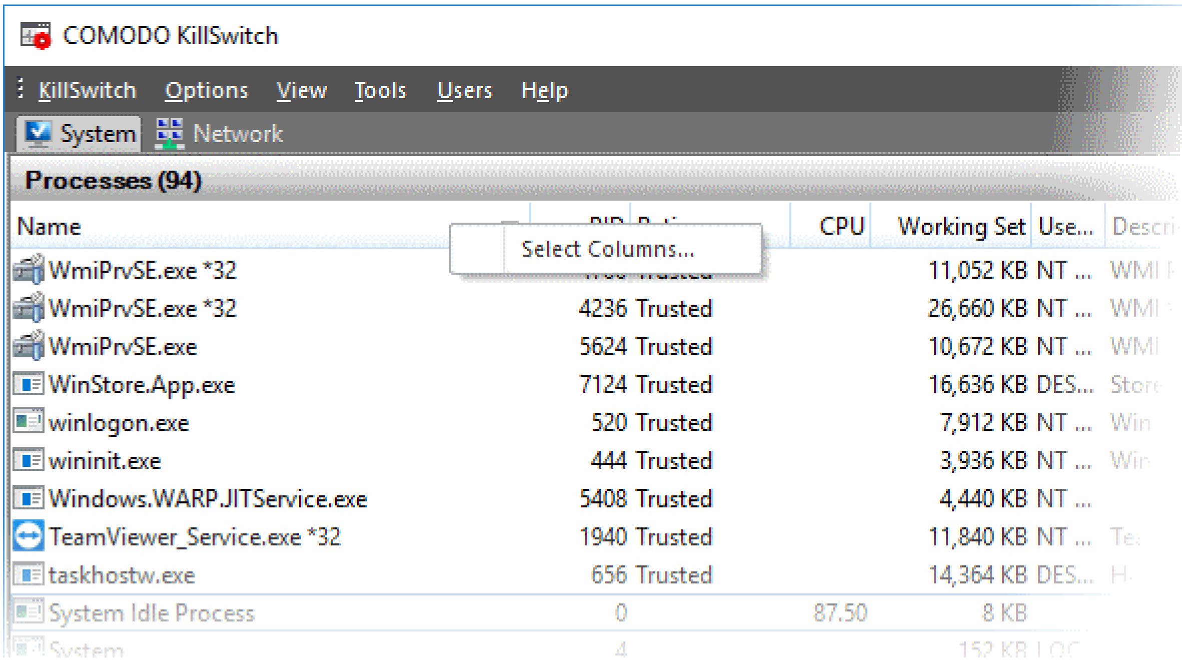
Column Selection

If you wish to view more details on each process, you can add more columns to the table:

- Click 'View ' > 'Select Columns'

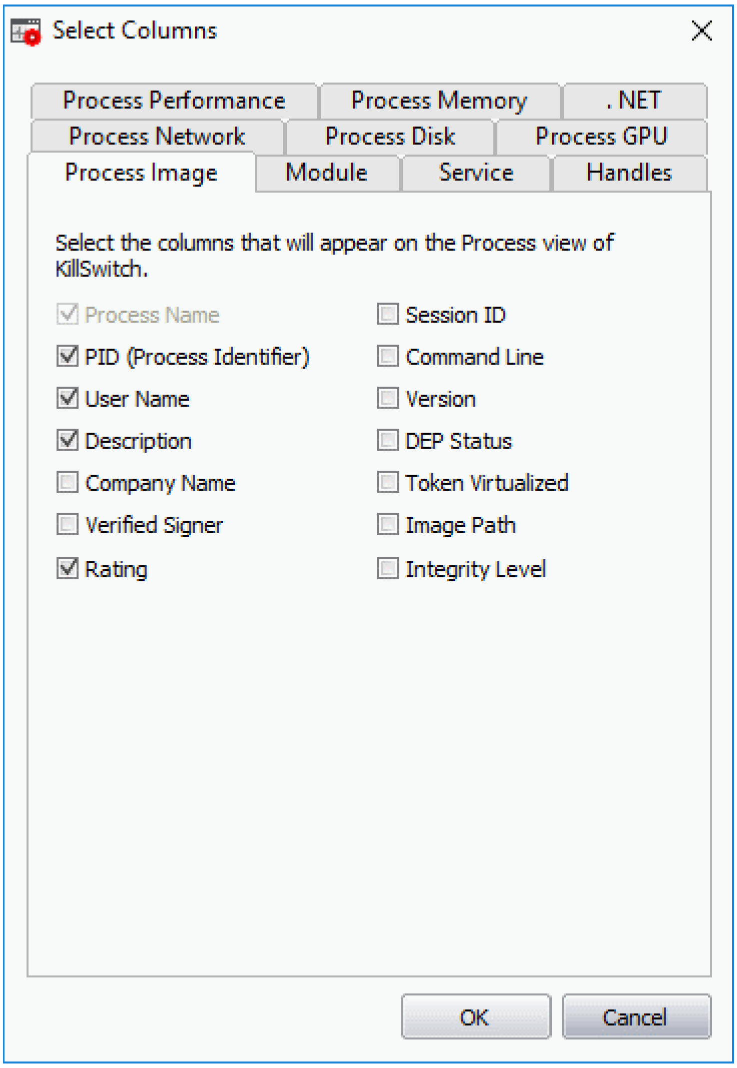
Or

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



Name	PID		CPU	Working Set	Use...	Descri
WmiPrvSE.exe *32				11,052 KB	NT ...	WMI
WmiPrvSE.exe *32	4236	Trusted		26,660 KB	NT ...	WMI
WmiPrvSE.exe	5624	Trusted		10,672 KB	NT ...	WMI
WinStore.App.exe	7124	Trusted		16,636 KB	DES...	Store
winlogon.exe	520	Trusted		7,912 KB	NT ...	Win
wininit.exe	444	Trusted		3,936 KB	NT ...	Win
Windows.WARP.JITService.exe	5408	Trusted		4,440 KB	NT ...	
TeamViewer_Service.exe *32	1940	Trusted		11,840 KB	NT ...	Te
taskhostw.exe	656	Trusted		14,364 KB	DES...	H
System Idle Process	0		87.50	8 KB		
System	4			152 KB	LOC	

Click the tab which corresponds to the interface whose columns you want to configure:



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

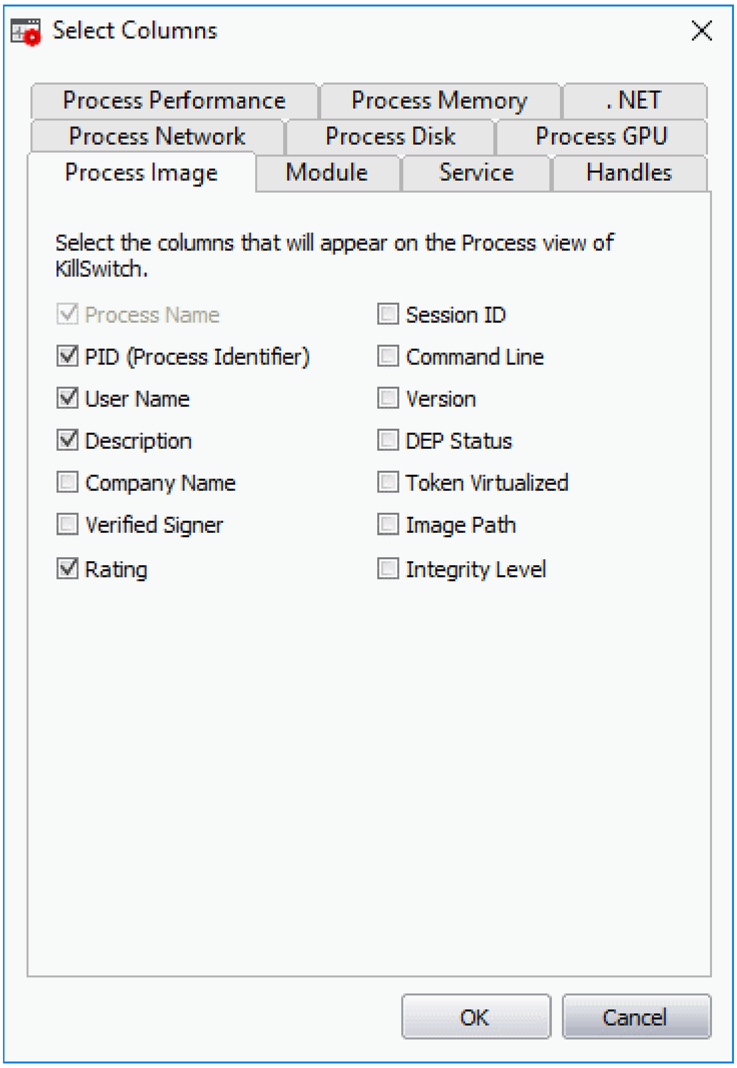
☑ Process Name	□ Session ID
☑ PID (Process Identifier)	□ Command Line
☑ User Name	□ Version
☑ Description	□ DEP Status
□ Company Name	□ Token Virtualized
□ Verified Signer	□ Image Path
☑ Rating	□ Integrity Level

See the following for more details on each tab:

- Process Image
- Process Performance
- Process Memory
- Process Disk
- Process Network
- Process GPU
- .NET
- Module
- Service
- Handles

Process Image

The process image tab lets you select which columns are shown in the 'Process' window. The columns in this tab provide general information about the process.



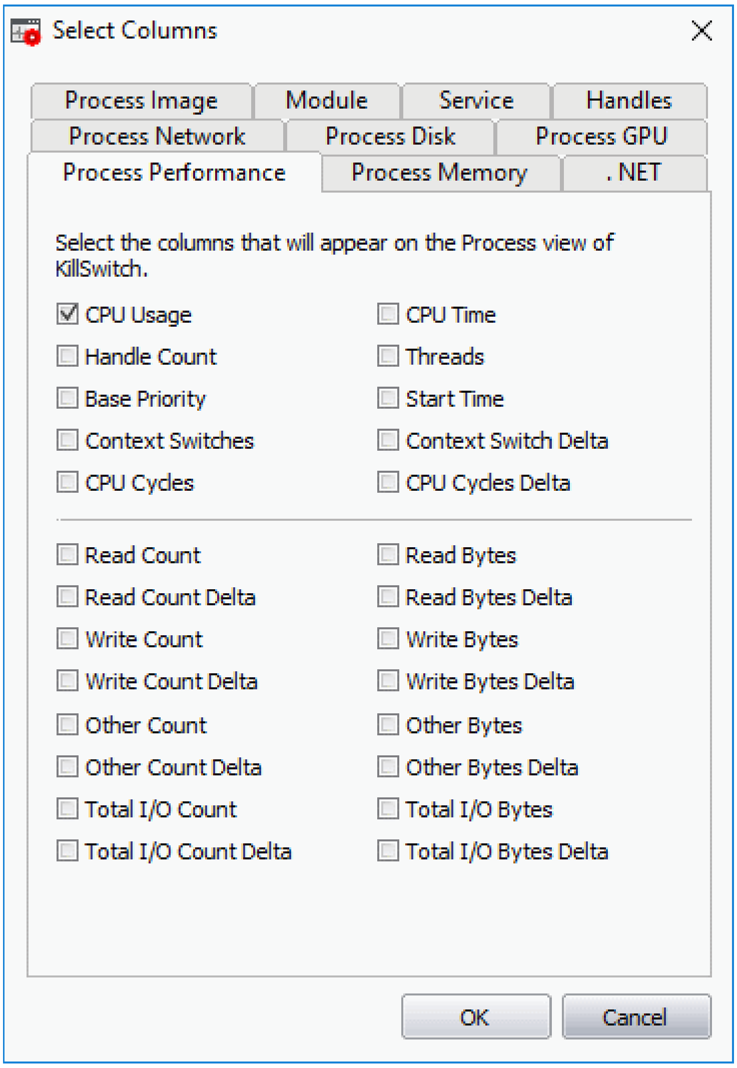
Select the columns that will appear on the Process view of KillSwitch.

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

- Use the check-boxes to specify which columns are shown in the process list
- Click 'OK' for your configuration to take effect.

Process Performance

The process performance tab lets you select which columns are shown in the 'Process' window to provide the detailed statistics and performance information like CPU usage, I/O activity and so on. This data is useful to track the resource overhead of a process at a granular level.



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

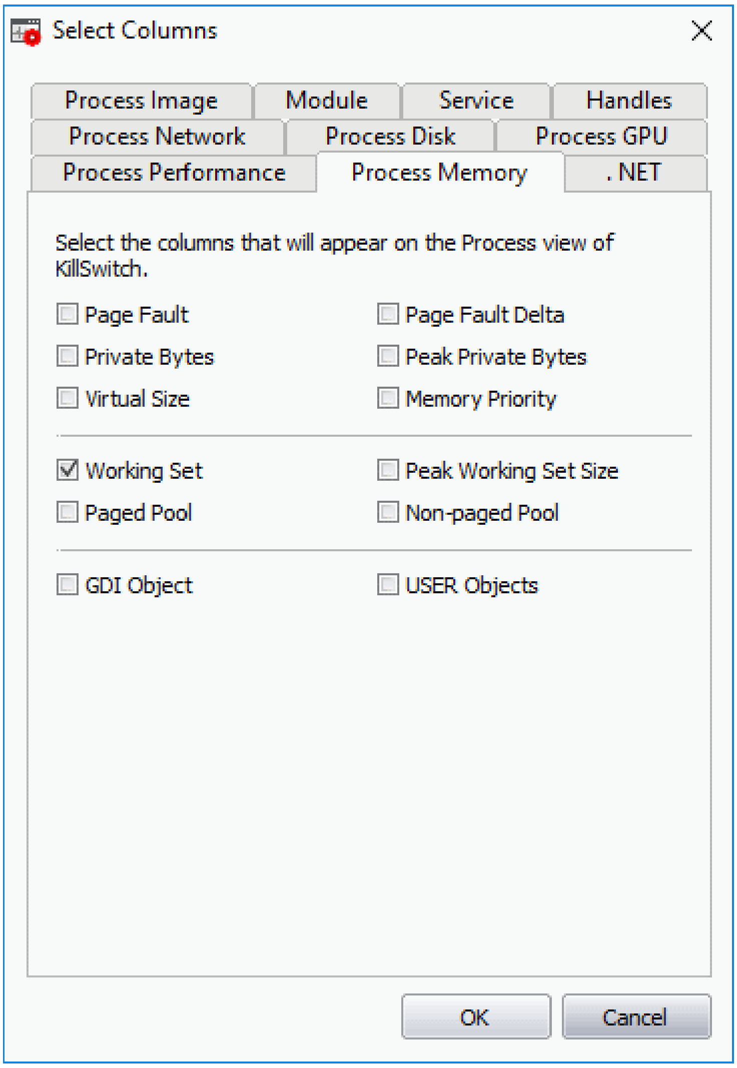
☑ CPU Usage
□ Handle Count
□ Base Priority
□ Context Switches
□ CPU Cycles
□ CPU Time
□ Threads
□ Start Time
□ Context Switch Delta
□ CPU Cycles Delta

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

- Use the check-boxes to specify which columns are shown in the process list.
- Click 'OK' for your configuration to take effect.

Process Memory

The process memory tab lets you select which columns are shown in the 'Process' window. These columns provide granular details about the memory usage of a process.



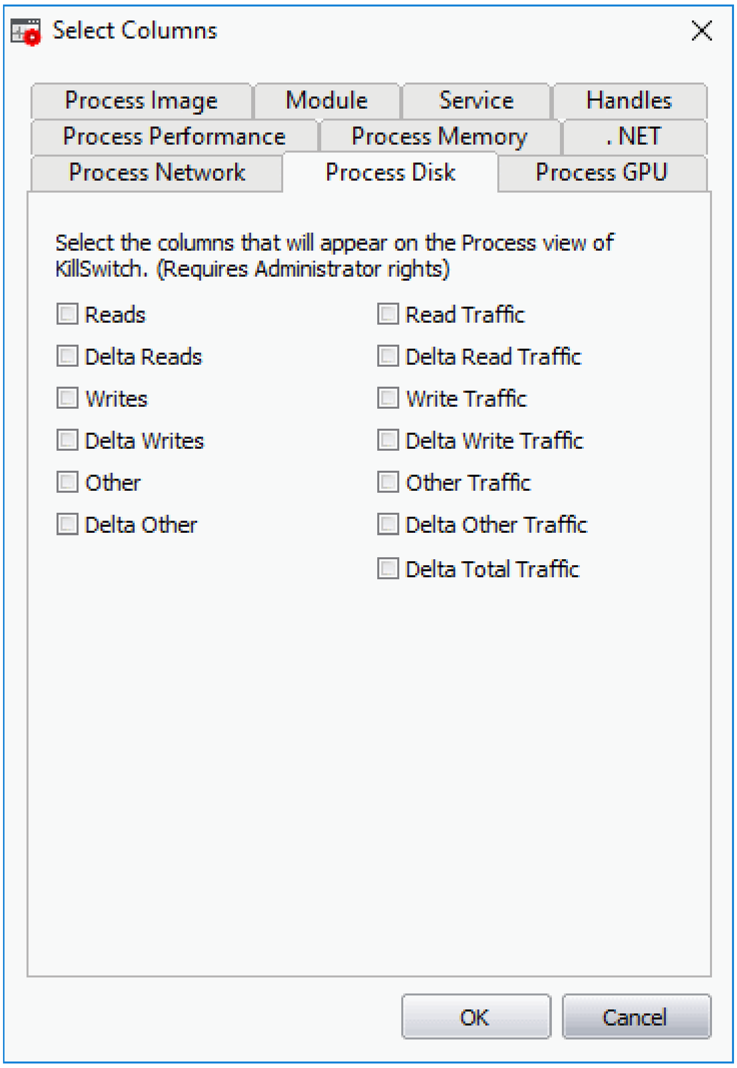
Select the columns that will appear on the Process view of KillSwitch.

□ 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

- Use the check-boxes to specify which columns are shown in the process list.
- Click 'OK' for your configuration to take effect.

Process Disk

The process disk tab lets you select which columns are shown in 'Processes' window. This data is useful to track disk access activities by processes.



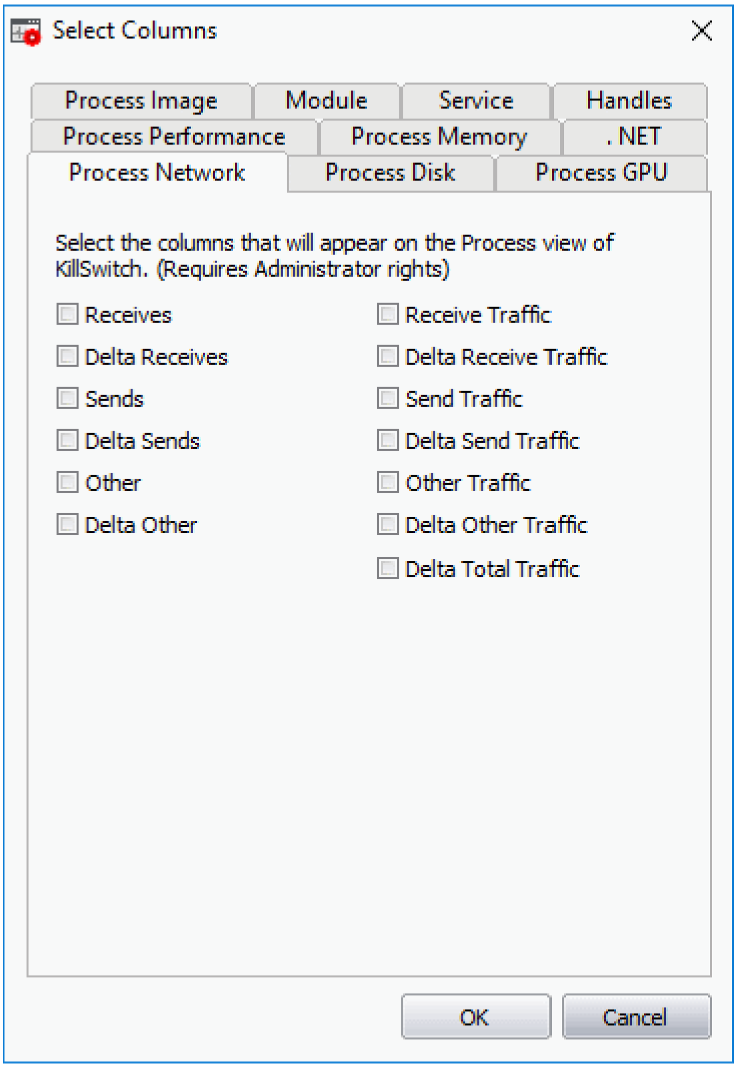
Select the columns that will appear on the Process view of KillSwitch. (Requires Administrator rights)

□ Reads
□ Delta Reads
□ Writes
□ Delta Writes
□ Other
□ Delta Other
□ Read Traffic
□ Delta Read Traffic
□ Write Traffic
□ Delta Write Traffic
□ Other Traffic
□ Delta Other Traffic
□ Delta Total Traffic

- Use the check-boxes to specify which columns are shown in the process list.
- Click 'OK' for your configuration to take effect.

Process Network

The process network window lets you configure which columns are shown in 'Process' list. This is useful to track how and which processes are handling network traffic. This data helps to monitor and log internet usage, to provide details which applications consumed that data.



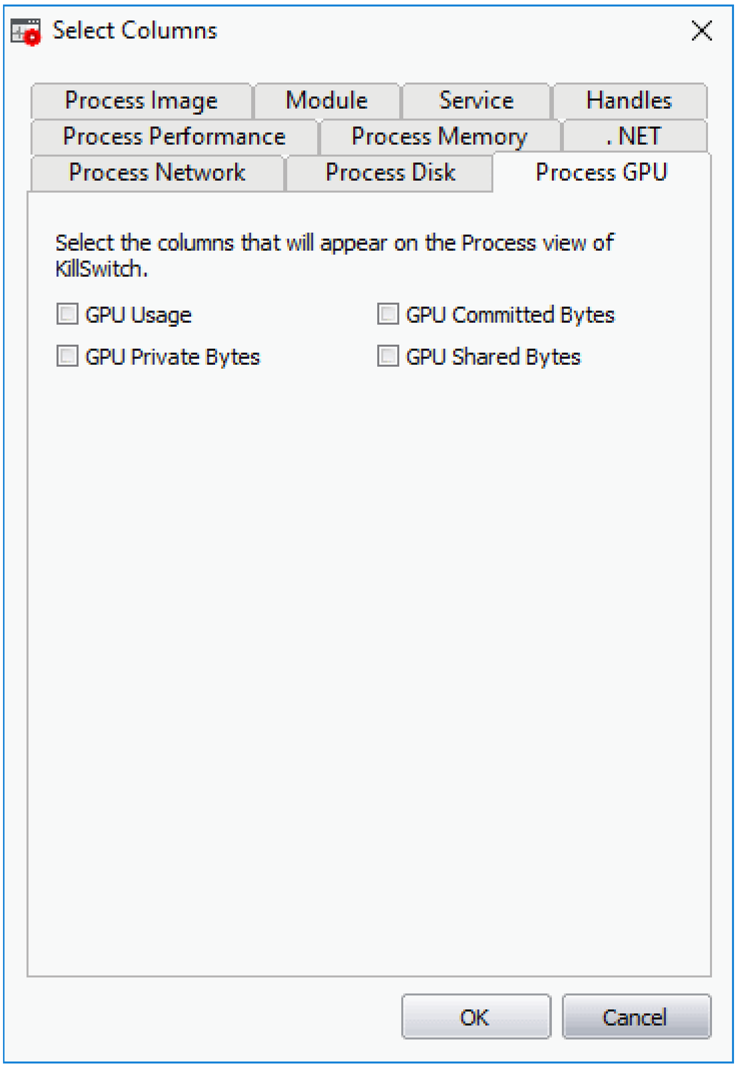
Select the columns that will appear on the Process view of KillSwitch. (Requires Administrator rights)

□ Receives
□ Delta Receives
□ Sends
□ Delta Sends
□ Other
□ Delta Other
□ Receive Traffic
□ Delta Receive Traffic
□ Send Traffic
□ Delta Send Traffic
□ Other Traffic
□ Delta Other Traffic
□ Delta Total Traffic

- Use the check-boxes to specify which columns are shown in the process list.
- Click 'OK' for your configuration to take effect.

Process GPU

The GPU processing tab lets you configure which columns are shown in under the 'GPU' area. This is useful to track how and which processes are handling graphic memory. This processor manipulates computer graphics and renders images.



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

□ GPU Usage

□ GPU Committed Bytes

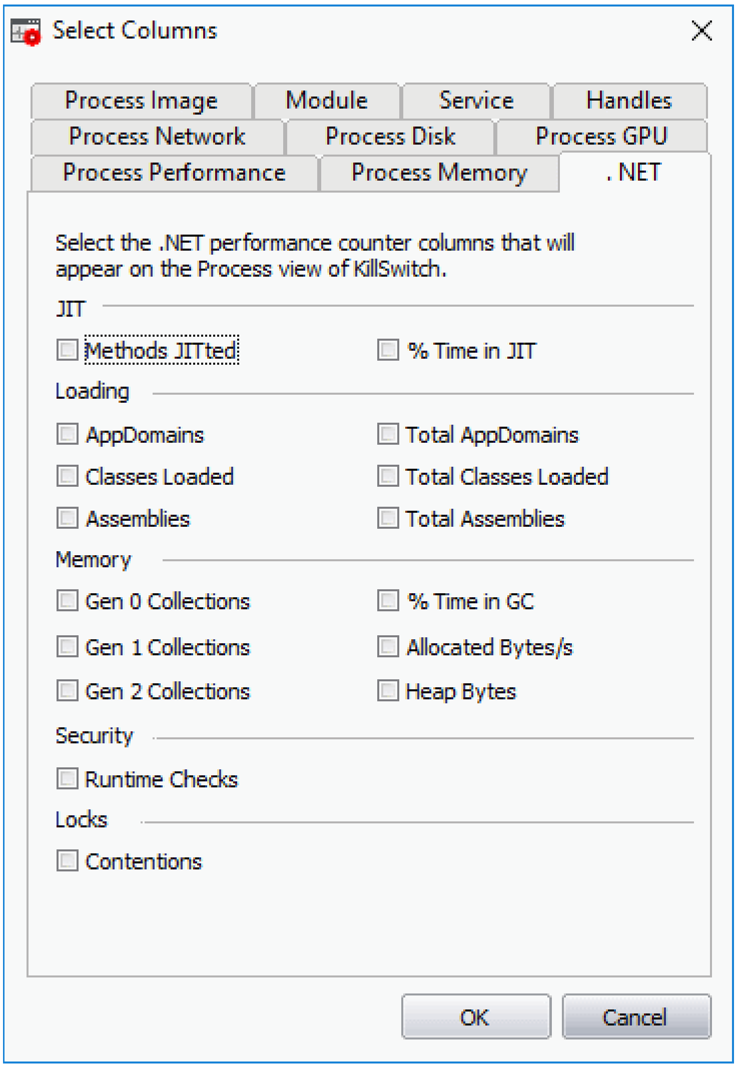
□ GPU Private Bytes

□ GPU Shared Bytes

- Use the check-boxes to specify which columns are shown in the process list.
- Click 'OK' for your configuration to take effect.

.NET

The .Net tab lets you configure which columns are shown in the '.Net performance' tab. Each column provides insight into the performance of .NET on your system.



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

JIT

□ Methods JITted □ % Time in JIT

Loading

□ AppDomains □ Total AppDomains

□ Classes Loaded □ Total Classes Loaded

□ Assemblies □ Total Assemblies

Memory

□ Gen 0 Collections □ % Time in GC

□ Gen 1 Collections □ Allocated Bytes/s

□ Gen 2 Collections □ Heap Bytes

Security

□ Runtime Checks

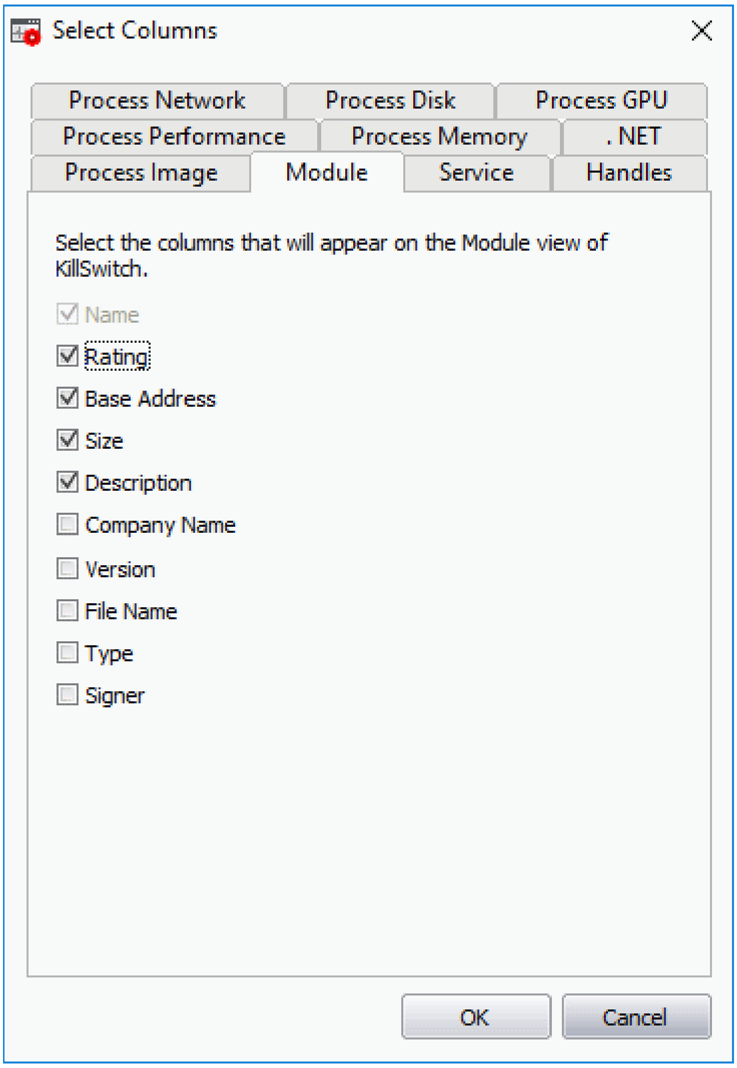
Locks

□ Contentions

- Use the check-boxes to specify which columns are shown in the process list.
- Click 'OK' for your configuration to take effect.

Module

The module tab lets you configure the columns shown in the 'Modules' tab. See **View Properties of a Process > Modules**, for more details on the 'Properties' dialog and the 'Modules' tab.



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

☑ Name

☑ Rating

☑ Base Address

☑ Size

☑ Description

□ Company Name

□ Version

□ File Name

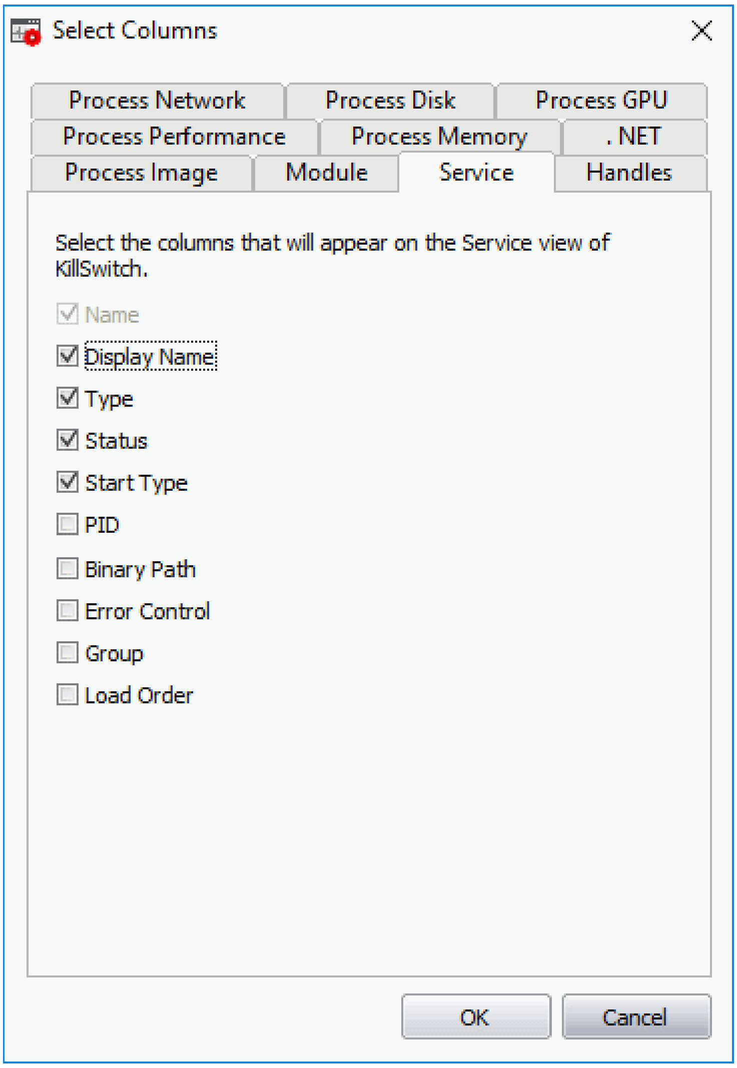
□ Type

□ Signer

- Use the check-boxes to specify which columns are shown in the process list.
- Click 'OK' for your configuration to take effect.

Service

The service tab lets you select which columns are shown in the 'Services' window. See **Services > Select Columns** for more details.



Select Columns

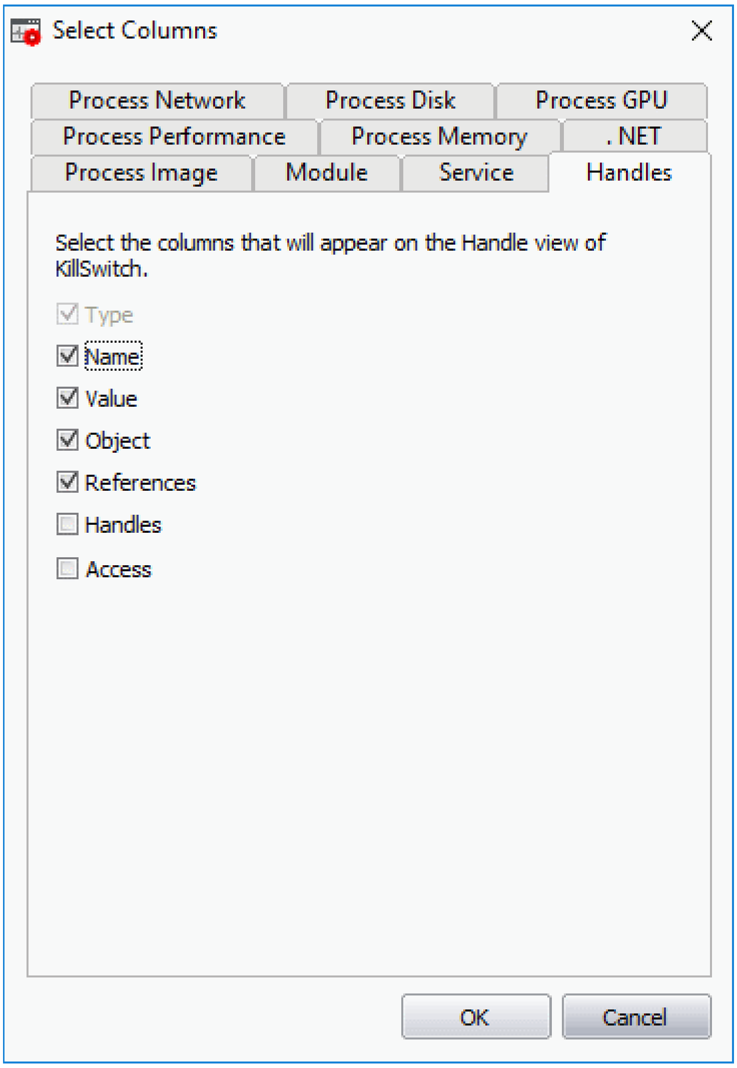
Select the columns that will appear on the Service view of KillSwitch.

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

- Use the check-boxes to specify which columns are shown in the process list.
- Click 'OK' for your configuration to take effect.

Handles

The handles tab lets you select which columns are shown in the 'Handles' window. See **View Properties of a Process** > **Handles**, for more details on the properties dialog and the handles tab.



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

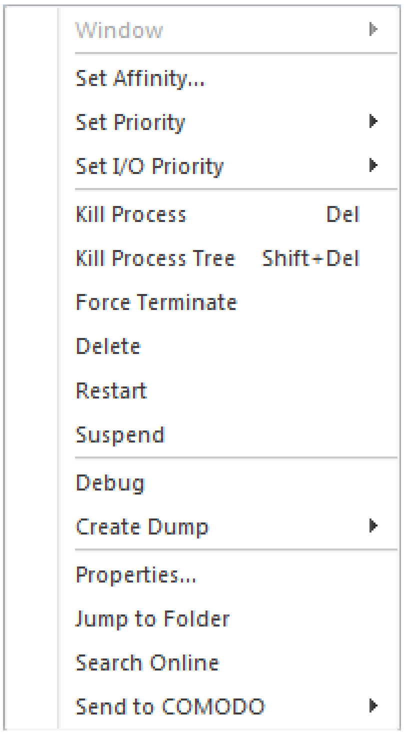
☑ Type
☑ Name
☑ Value
☑ Object
☑ References
□ Handles
□ Access

- Use the check-boxes to specify which columns are shown in the process list.
- Click 'OK' for your configuration to take effect.

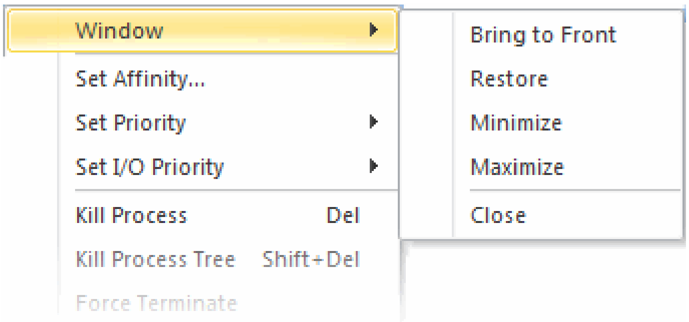
5.3.1.1. Stop, Start and Handle the Processes

- Click 'Tools' > 'Open KillSwitch'
- Click the 'Services' tab on the KillSwitch home screen
- Click the 'Processes' stripe to view all running processes.

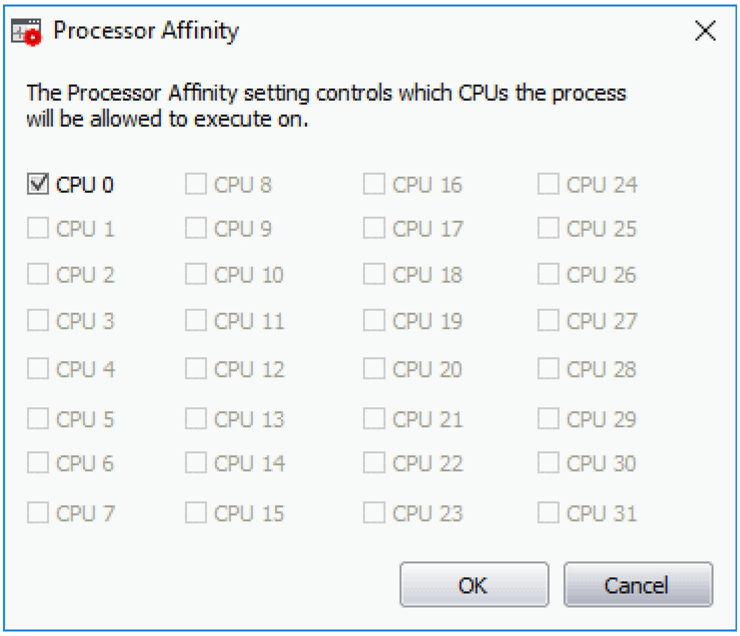
You can right-click on a process to perform various actions:



- **Window** - Re-position/re-size the process window, if one was found. The menu is disabled if the process doesn't have any open windows. The options available are:



- **Set Affinity** - View and modify the processor affinity (the CPU to which the process is assigned) in a symmetric multiprocessing operating system.



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

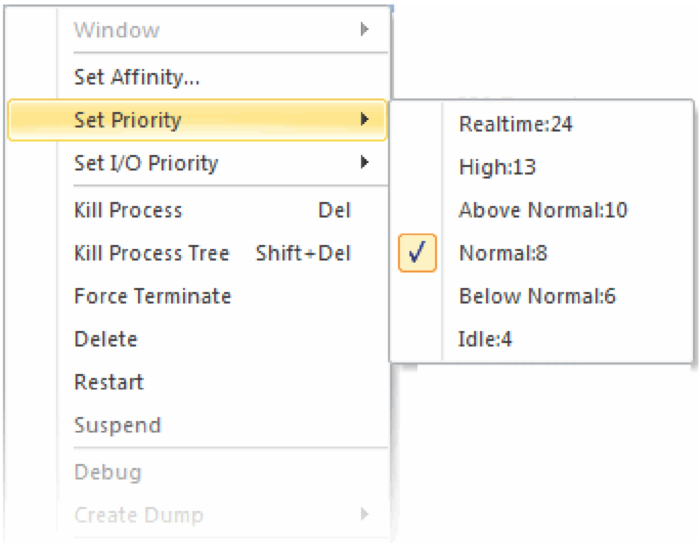
Background Note:

- In a symmetric multiprocessing operating system, each task (process or thread) is assigned a tag which indicates its preferred processor. This processor is assigned to the task at run 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 overall system efficiency.

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

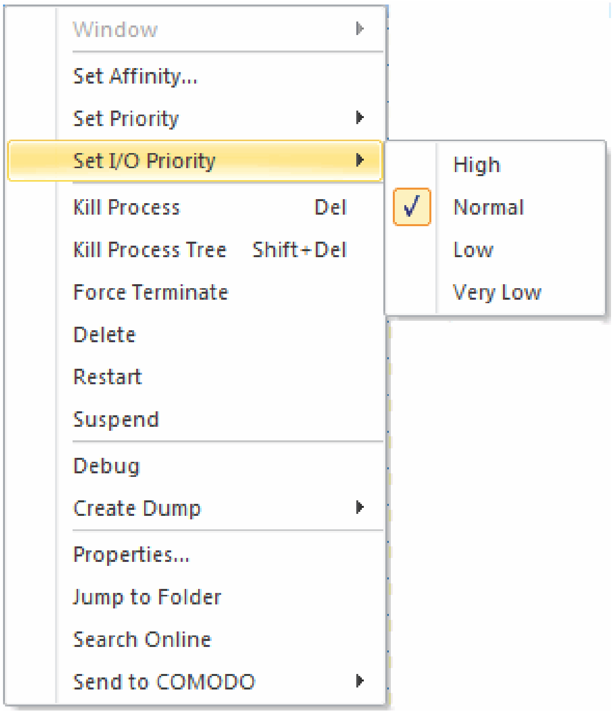
- **Set Priority -** Set the importance of the process. The available options are:

- Realtime
- High
- Above Normal
- Normal
- Below Normal
- Idle



- **Set I/O Priority -** Allows windows to control and gauge the value of all processes. This setting reduces performance bottlenecks. The available options are:

- High
- Normal (Default)
- Low
- Very Low



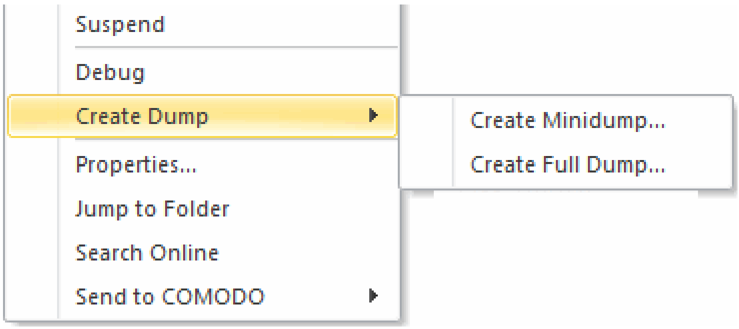
In most cases, the level estimated by the operating system is an appropriate background mode or very low priority.

- **Kill Process -** Terminates the selected processes. KillSwitch can, except under extraordinary circumstances, terminate any process. This includes processes which are protected by rootkits or security software.
- **Kill Process Tree -** Terminates the selected process and its descendants (child processes).
- **Force Terminate -** Stops the selected process(es) abruptly. This option helps for closing any programs that are under 'Not Responding' status.

- **Delete -** Omits the selected (running or suspended) process(es) from the disk. KillSwitch can destroy any process, including the ones protected by rootkits or security software. The application requests for confirmation before eliminating a process. Your computer should restart for this action to take effect.

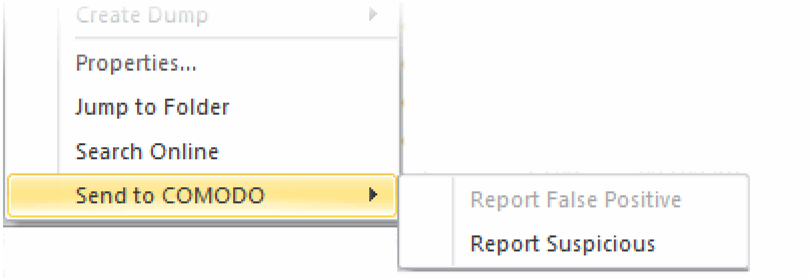
Warning: Deleting a process will permanently remove the application that triggered the process.

- **Restart -** Reboots the selected process with the same command line arguments and working directory.
- **Suspend -** Temporarily stop the selected processes. KillSwitch can hang any process, including ones protected by rootkits or security
- **Debug -** Starts bug fixing for the selected process. This is useful for software developers and testers to find issues in applications.
- **Create Dump -** Enables you to create a crash log file for the process. This operation does not actually cause the process to crash or terminate. The available options are:



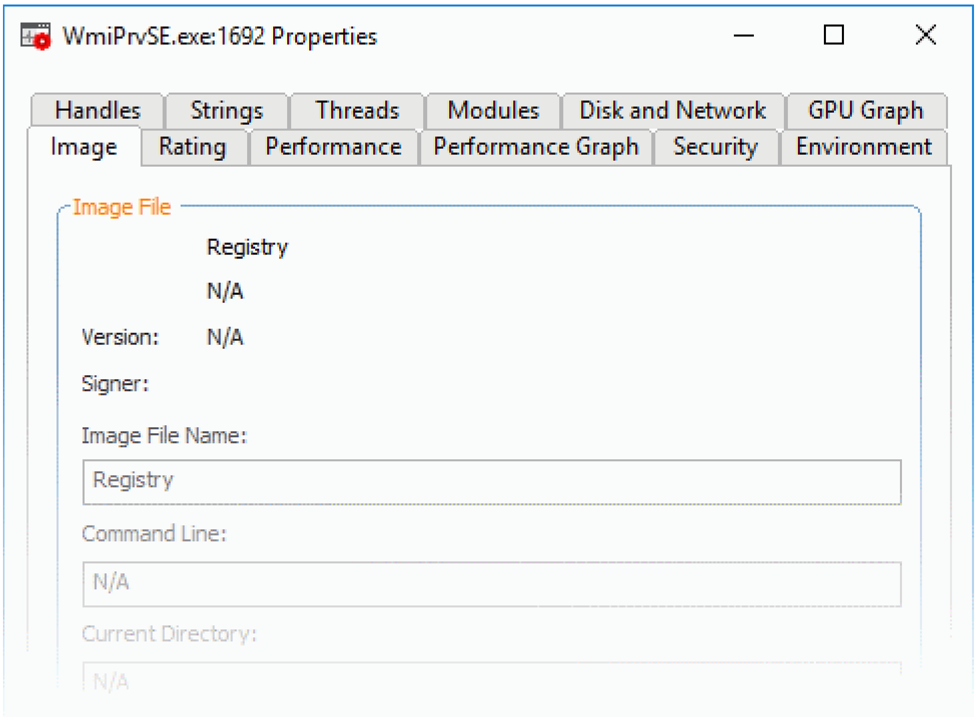
- Create Minidump... - Creates a small dump file containing only essential data.
- Create Fulldump... - Creates a dump containing all available data.

- **Properties -** displays the various attributes of selected process in a dialog. See **View the Properties of a Process** for more details.
- **Jump to Folder -** Directly opens the folder containing the file in Windows Explorer.
- **Search Online** - Opens the default web browser with the specified search engine and searches for information on the process.
- **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 to assist all the users.



5.3.1.2. View Properties of a Process

- Open CCE > right-click on a process > select 'Properties'
- The 'Properties' interface is divided into 11 separate tabs, each containing important information about a process.



WmiPrvSE.exe:1692 Properties

Registry

N/A

Version: N/A

Signer:

Image File Name: Registry

Command Line: N/A

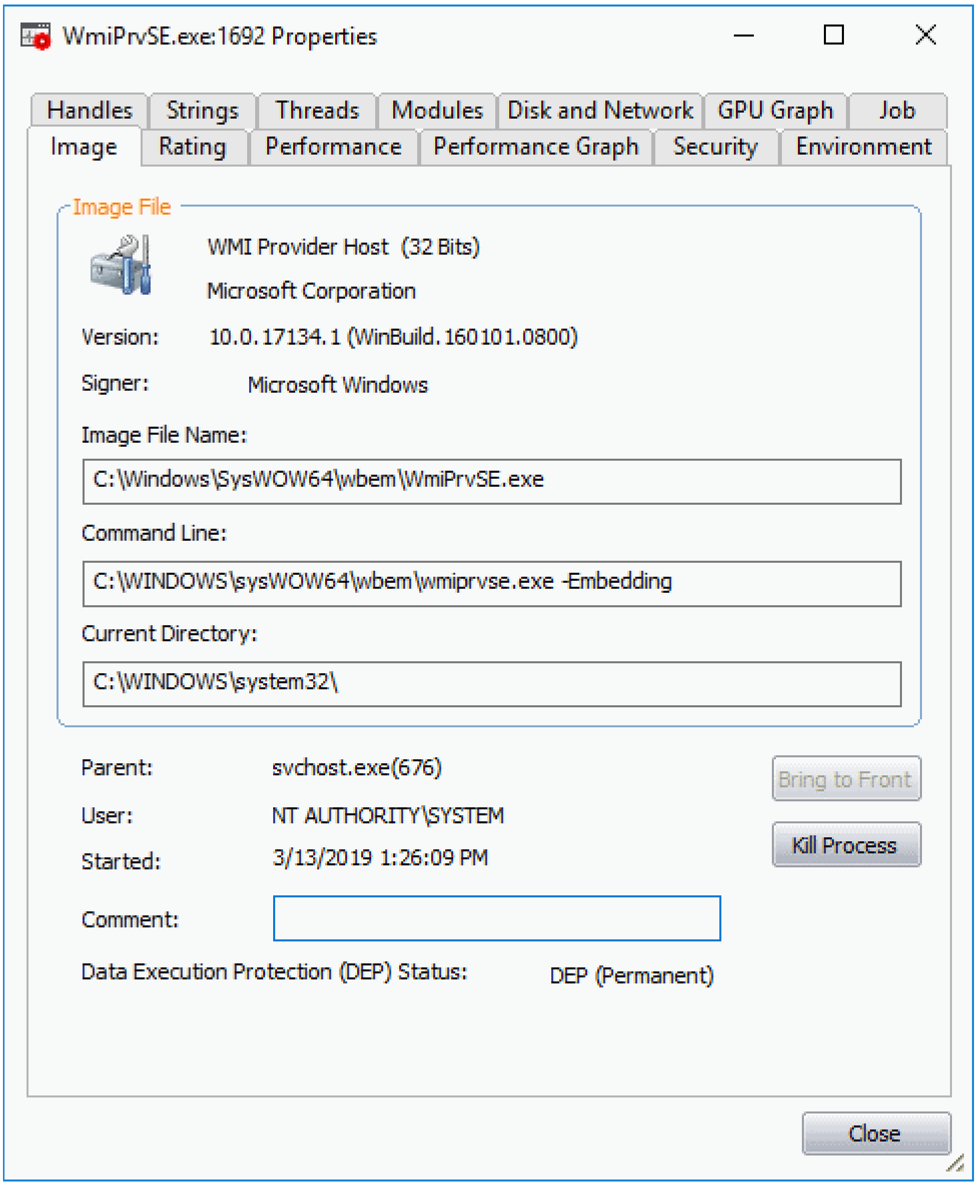
Current Directory: N/A

Click the following links for more details on each tab:

- Image
- Rating
- Performance
- Performance Graph
- Security
- Environment
- Handles
- Strings
- Threads
- Modules
- Disk and Network
- GPU Graph

Image

The image tab shows 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 lets you make the parent application window of the selected process active and terminate the process.



WmiPrvSE.exe:1692 Properties

Image File

WMI Provider Host (32 Bits)

Microsoft Corporation

Version: 10.0.17134.1 (WinBuild.160101.0800)

Signer: Microsoft Windows

Image File Name:

C:\Windows\SysWOW64\wbem\WmiPrvSE.exe

Command Line:

C:\WINDOWS\sysWOW64\wbem\wmiprvse.exe -Embedding

Current Directory:

C:\WINDOWS\system32\

Parent: svchost.exe(676)

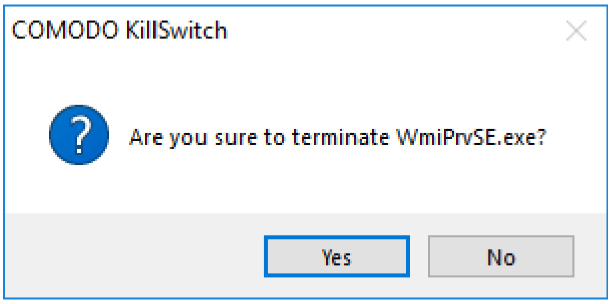
User: NT AUTHORITY\SYSTEM

Started: 3/13/2019 1:26:09 PM

Comment:

Data Execution Protection (DEP) Status: DEP (Permanent)

- **Terminate** - Click 'Kill Process' to stop the process. Confirm termination before stopping the process by clicking 'Yes' in the confirmation dialog.



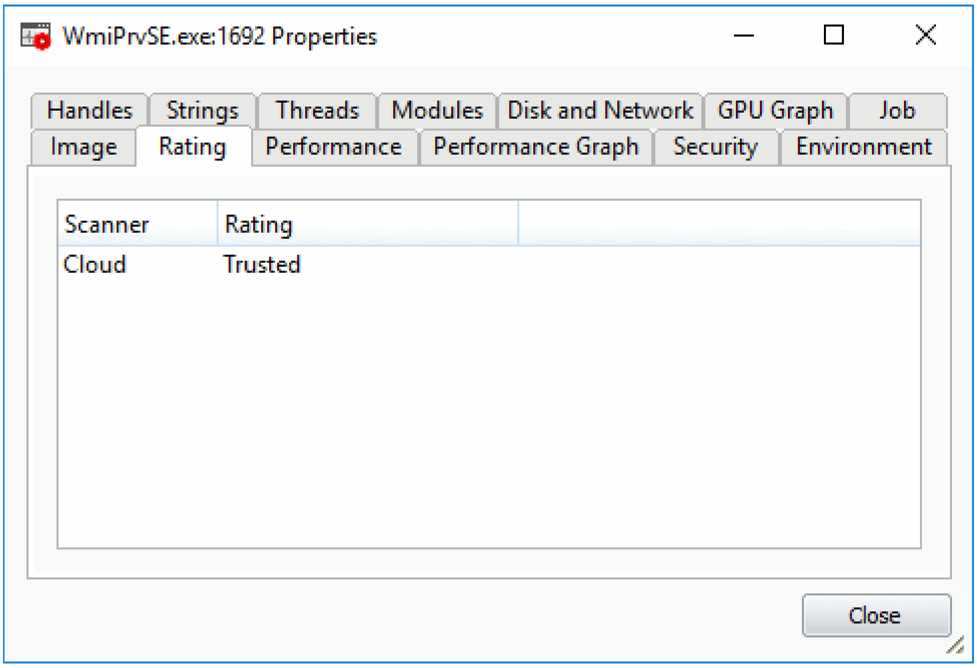
COMODO KillSwitch

Are you sure to terminate WmiPrvSE.exe?

Click here to go back to list of properties.

Rating

The rating tab shows 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
Cloud	Trusted

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):

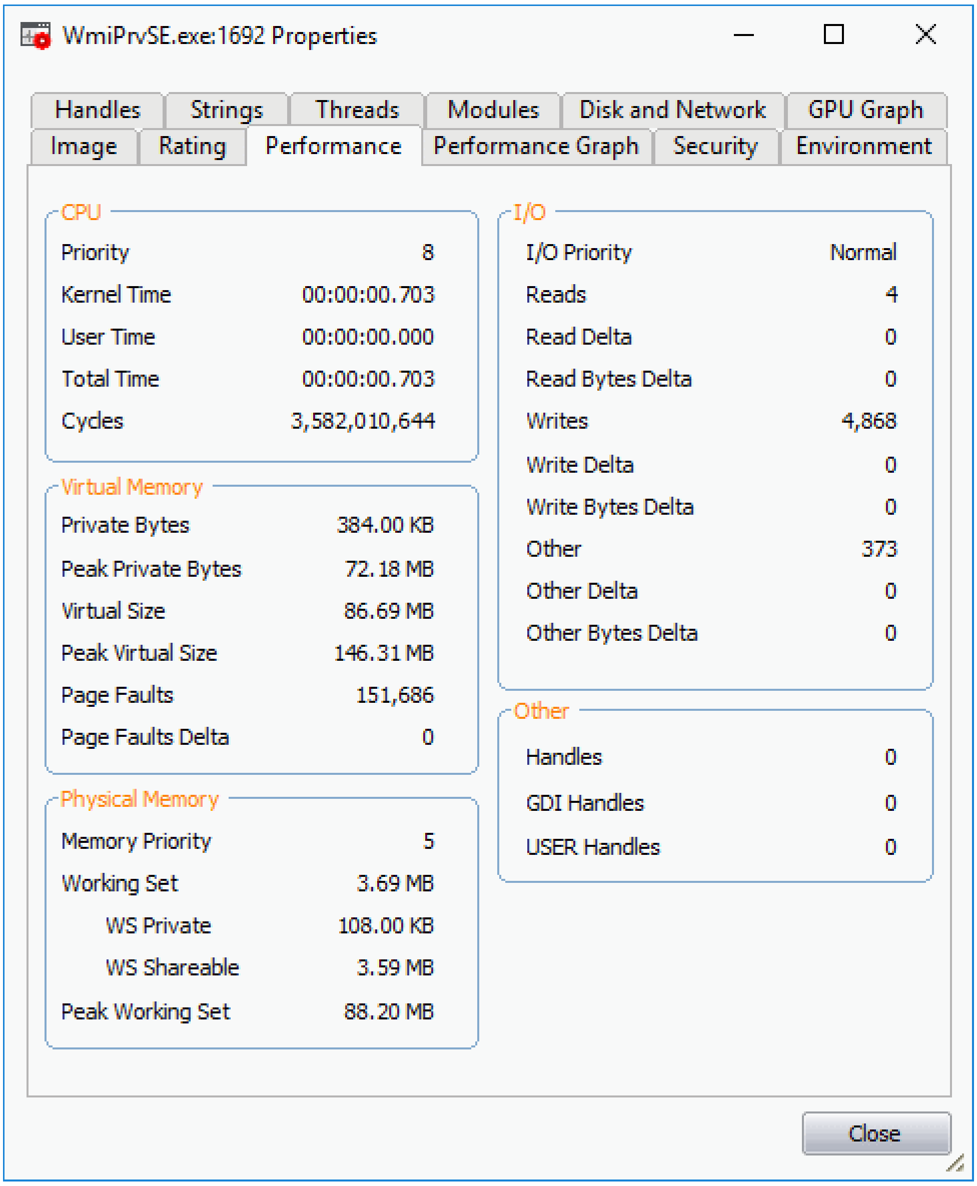
1. Basic.Malware
2. FLS.Malware
3. FLS.Trusted

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 shows 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.



WmiPrvSE.exe:1692 Properties

CPU

Priority	8
Kernel Time	00:00:00.703
User Time	00:00:00.000
Total Time	00:00:00.703
Cycles	3,582,010,644

Virtual Memory

Private Bytes	384.00 KB
Peak Private Bytes	72.18 MB
Virtual Size	86.69 MB
Peak Virtual Size	146.31 MB
Page Faults	151,686
Page Faults Delta	0

Physical Memory

Memory Priority	5
Working Set	3.69 MB
WS Private	108.00 KB
WS Shareable	3.59 MB
Peak Working Set	88.20 MB

I/O

I/O Priority	Normal
Reads	4
Read Delta	0
Read Bytes Delta	0
Writes	4,868
Write Delta	0
Write Bytes Delta	0
Other	373
Other Delta	0
Other Bytes Delta	0

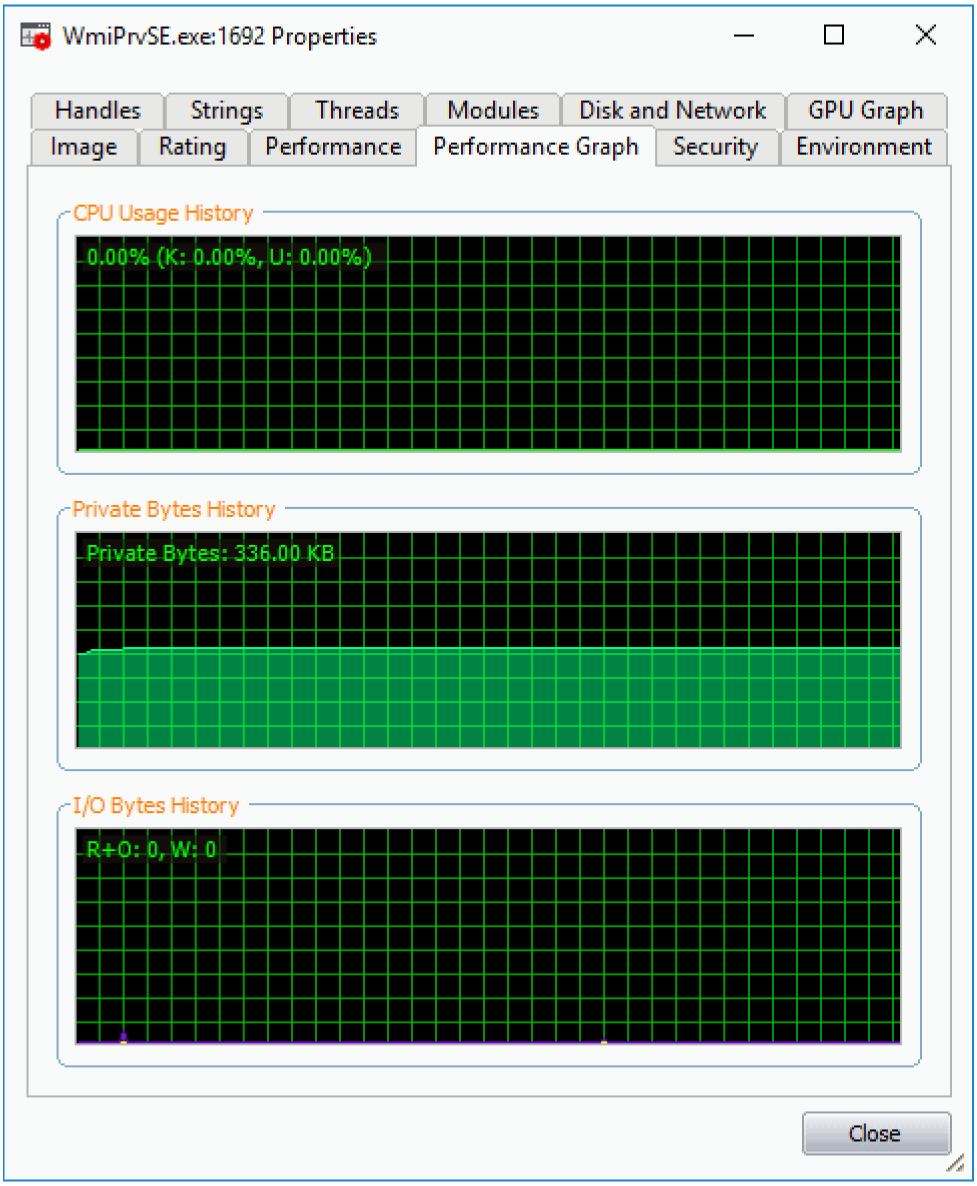
Other

Handles	0
GDI Handles	0
USER Handles	0

Click here to go back to list of properties.

Performance Graph

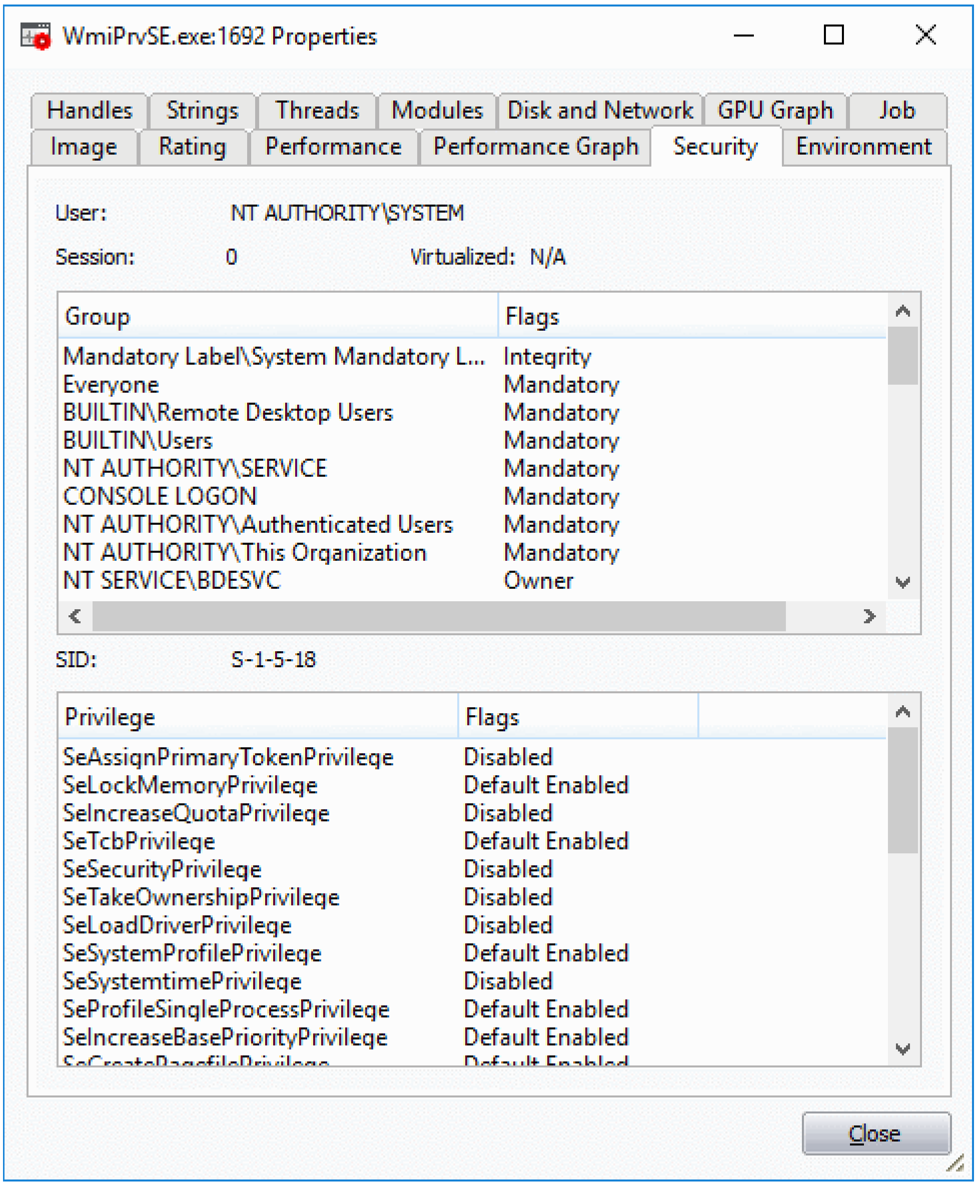
The performance graph tab represents three graphs of the process' performance - CPU Usage, Private Bytes, and I/O activity. This window helps the advanced users to monitor the resource overhead of a process pictorially. You can hover your mouse over the graphs to view details.



Click here to go back to list of properties.

Security

The security tab shows 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: NT AUTHORITY\SYSTEM

Session: 0 Virtualized: N/A

Group	Flags
Mandatory Label\System Mandatory L...	Integrity
Everyone	Mandatory
BUILTIN\Remote Desktop Users	Mandatory
BUILTIN\Users	Mandatory
NT AUTHORITY\SERVICE	Mandatory
CONSOLE LOGON	Mandatory
NT AUTHORITY\Authenticated Users	Mandatory
NT AUTHORITY\This Organization	Mandatory
NT SERVICE\BDESVC	Owner

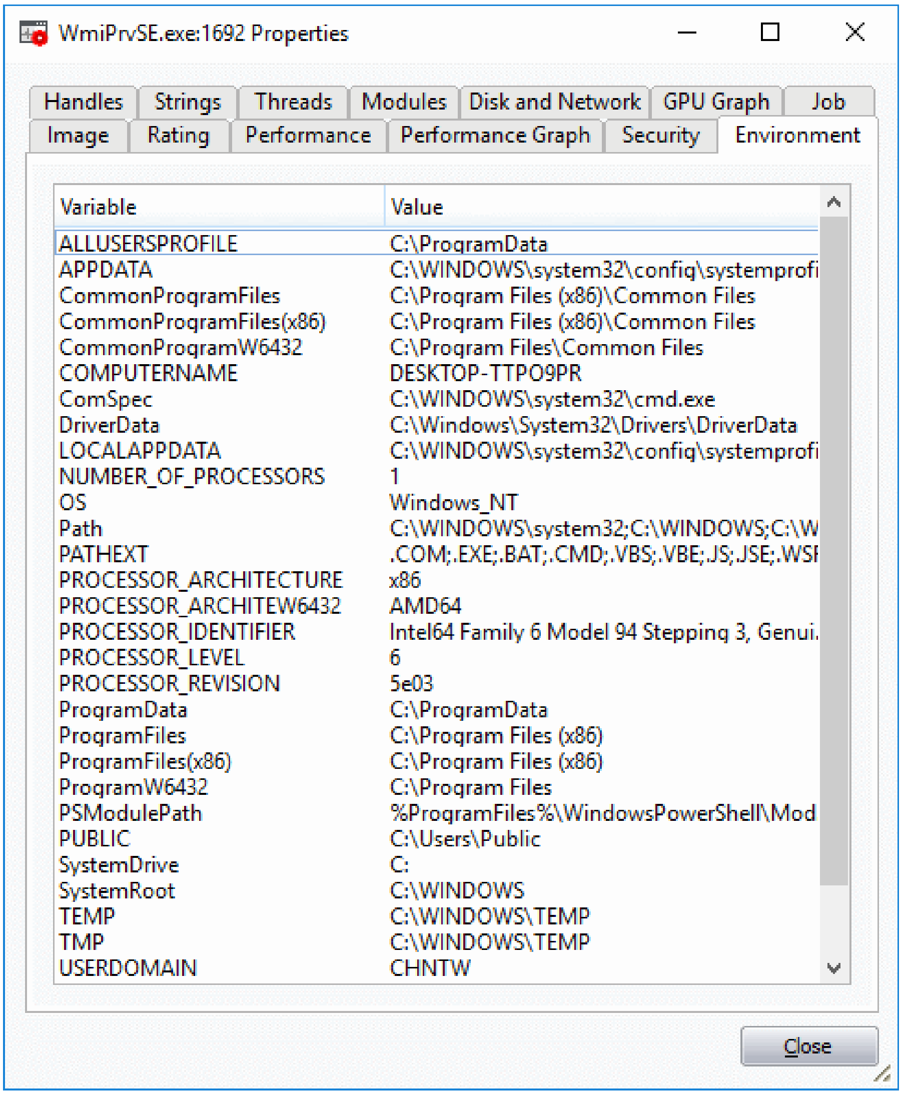
SID: S-1-5-18

Privilege	Flags
SeAssignPrimaryTokenPrivilege	Disabled
SeLockMemoryPrivilege	Default Enabled
SeIncreaseQuotaPrivilege	Disabled
SeTcbPrivilege	Default Enabled
SeSecurityPrivilege	Disabled
SeTakeOwnershipPrivilege	Disabled
SeLoadDriverPrivilege	Disabled
SeSystemProfilePrivilege	Default Enabled
SeSystemtimePrivilege	Disabled
SeProfileSingleProcessPrivilege	Default Enabled
SeIncreaseBasePriorityPrivilege	Default Enabled
SeCreatePagefilePrivilege	Default Enabled

Click here to go back to list of properties.

Environment

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



WmiPrvSE.exe:1692 Properties

Variable	Value
ALLUSERSPROFILE	C:\ProgramData
APPDATA	C:\WINDOWS\system32\config\systemprofi
CommonProgramFiles	C:\Program Files (x86)\Common Files
CommonProgramFiles(x86)	C:\Program Files (x86)\Common Files
CommonProgramW6432	C:\Program Files\Common Files
COMPUTERNAME	DESKTOP-TTPO9PR
ComSpec	C:\WINDOWS\system32\cmd.exe
DriverData	C:\Windows\System32\Drivers\DriverData
LOCALAPPDATA	C:\WINDOWS\system32\config\systemprofi
NUMBER_OF_PROCESSORS	1
OS	Windows_NT
Path	C:\WINDOWS\system32;C:\WINDOWS;C:\W
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF
PROCESSOR_ARCHITECTURE	x86
PROCESSOR_ARCHITEW6432	AMD64
PROCESSOR_IDENTIFIER	Intel64 Family 6 Model 94 Stepping 3, Genui.
PROCESSOR_LEVEL	6
PROCESSOR_REVISION	5e03
ProgramData	C:\ProgramData
ProgramFiles	C:\Program Files (x86)
ProgramFiles(x86)	C:\Program Files (x86)
ProgramW6432	C:\Program Files
PSModulePath	%ProgramFiles%\WindowsPowerShell\Mod
PUBLIC	C:\Users\Public
SystemDrive	C:
SystemRoot	C:\WINDOWS
TEMP	C:\WINDOWS\TEMP
TMP	C:\WINDOWS\TEMP
USERDOMAIN	CHNTW

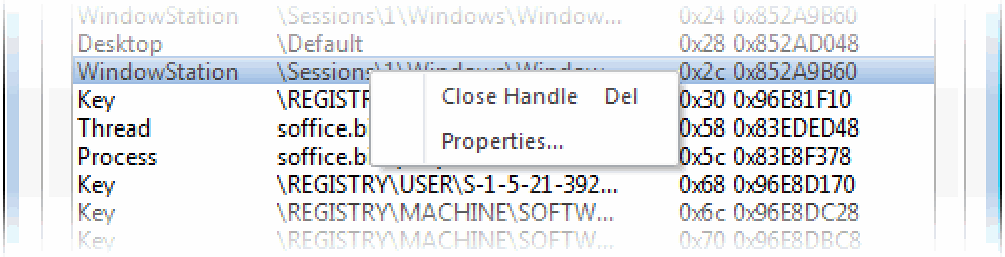
Click here to go back to list of properties.

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.

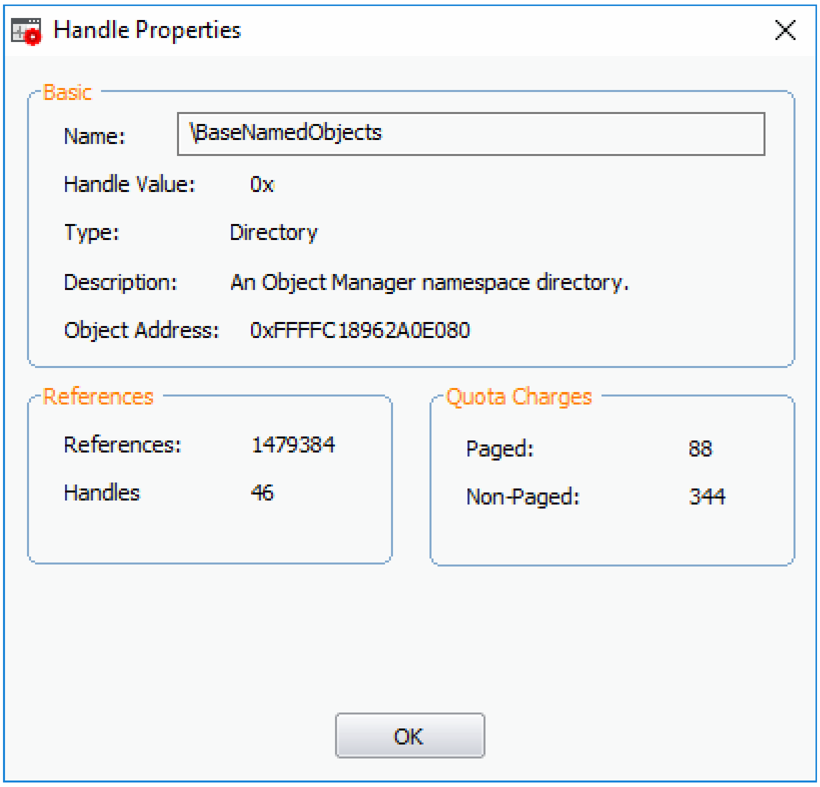
Tip: The columns displayed in 'Handles' interface can be configured to display the details as required. See **Column Selection** > **Handles** for more details.

- **Hide unnamed handles -** Select this option to remove 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 you to close or view the properties of the handle.



WindowStation	\Sessions\1\Windows\Window...	0x24 0x852A9B60
Desktop	\Default	0x28 0x852AD048
WindowStation	\Sessions\1\Windows\Window...	0x2c 0x852A9B60
Key	\REGISTR	0x30 0x96E81F10
Thread	soffice.b	0x58 0x83EDED48
Process	soffice.b	0x5c 0x83E8F378
Key	\REGISTRY\USER\S-1-5-21-392...	0x68 0x96E8D170
Key	\REGISTRY\MACHINE\SOFTW...	0x6c 0x96E8DC28
Key	\REGISTRY\MACHINE\SOFTW...	0x70 0x96E8DBC8

- **Close Handle** - Closing a process handle does not terminate the associated process or remove the process object.
- **Properties** - Opens the 'Handle Properties' dialog. Also you can open this dialog by double-clicking a handle.



Basic

Name: \BaseNamedObjects

Handle Value: 0x

Type: Directory

Description: An Object Manager namespace directory.

Object Address: 0xFFFFC18962A0E080

References

References: 1479384

Handles 46

Quota Charges

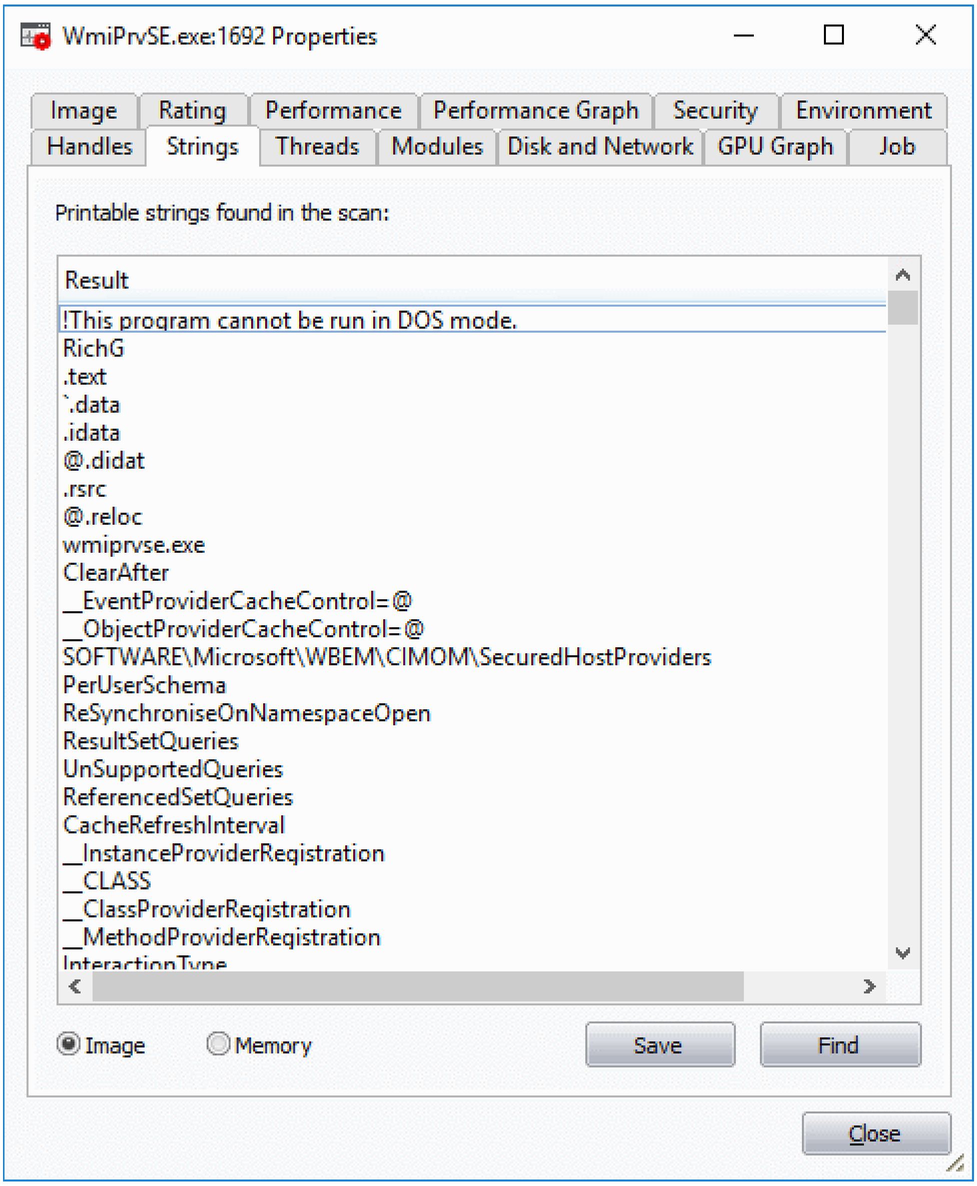
Paged: 88

Non-Paged: 344

Click here to go back to list of properties.

Strings

The strings tab shows 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:

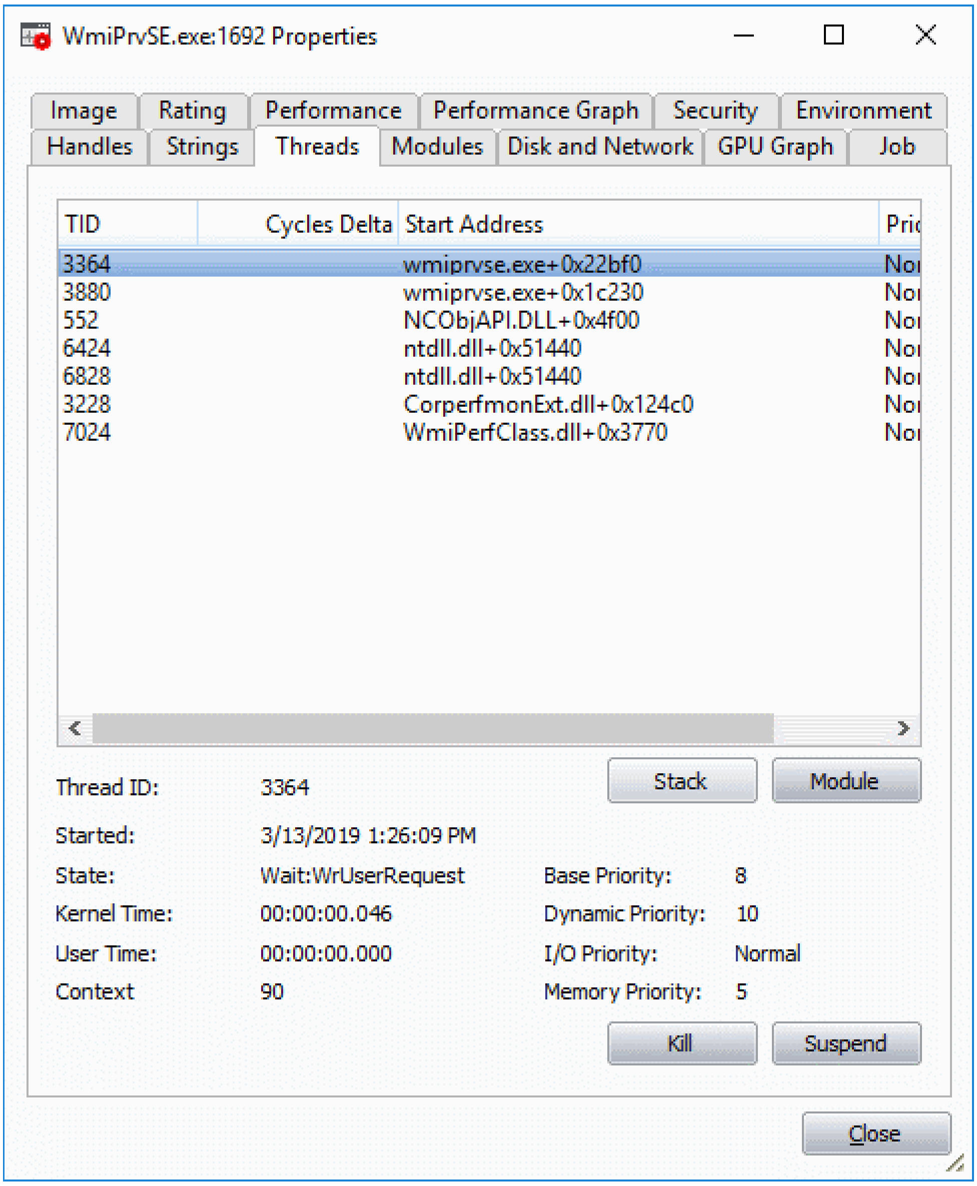
```
Result
!This program cannot be run in DOS mode.
RichG
.text
`.data
.idata
@.didat
.rsrc
@.reloc
wmiprvse.exe
ClearAfter
__EventProviderCacheControl=@
__ObjectProviderCacheControl=@
SOFTWARE\Microsoft\WBEM\CIMOM\SecuredHostProviders
PerUserSchema
ReSynchroniseOnNamespaceOpen
ResultSetQueries
UnSupportedQueries
ReferencedSetQueries
CacheRefreshInterval
__InstanceProviderRegistration
__CLASS
__ClassProviderRegistration
__MethodProviderRegistration
InteractionType
```

● Image ○ Memory

- Select ‘Image’ or ‘Memory’ to extract and view the strings from process image or the process memory respectively.
- Click 'Save' to store a copy of the list of strings as a text file.

Threads

The threads tab shows child processes started by 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	Cycles Delta	Start Address	Pric
3364		wmiprvse.exe+0x22bf0	Nor
3880		wmiprvse.exe+0x1c230	Nor
552		NCObjAPI.DLL+0x4f00	Nor
6424		ntdll.dll+0x51440	Nor
6828		ntdll.dll+0x51440	Nor
3228		CorperfmonExt.dll+0x124c0	Nor
7024		WmiPerfClass.dll+0x3770	Nor

Thread ID: 3364

Started: 3/13/2019 1:26:09 PM

State: Wait:WrUserRequest

Kernel Time: 00:00:00.046

User Time: 00:00:00.000

Context 90

Base Priority: 8

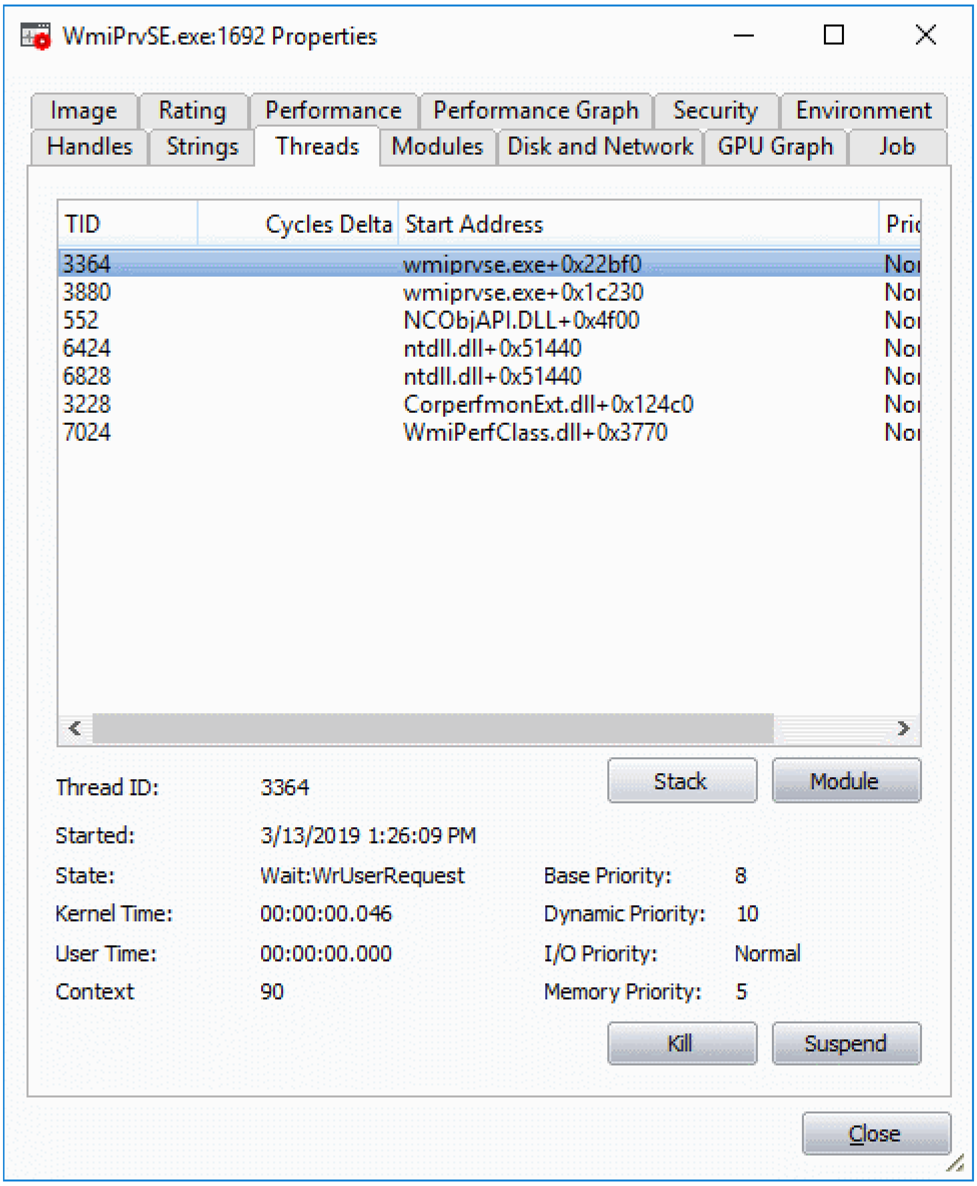
Dynamic Priority: 10

I/O Priority: Normal

Memory Priority: 5

Handle Threads

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



TID	Cycles Delta	Start Address	Pri
3364		wmiprvse.exe+0x22bf0	Noi
3880		wmiprvse.exe+0x1c230	Noi
552		NCObjAPI.DLL+0x4f00	Noi
6424		ntdll.dll+0x51440	Noi
6828		ntdll.dll+0x51440	Noi
3228		CorperfmonExt.dll+0x124c0	Noi
7024		WmiPerfClass.dll+0x3770	Noi

Thread ID: 3364

Started: 3/13/2019 1:26:09 PM

State: Wait:WrUserRequest

Base Priority: 8

Kernel Time: 00:00:00.046

Dynamic Priority: 10

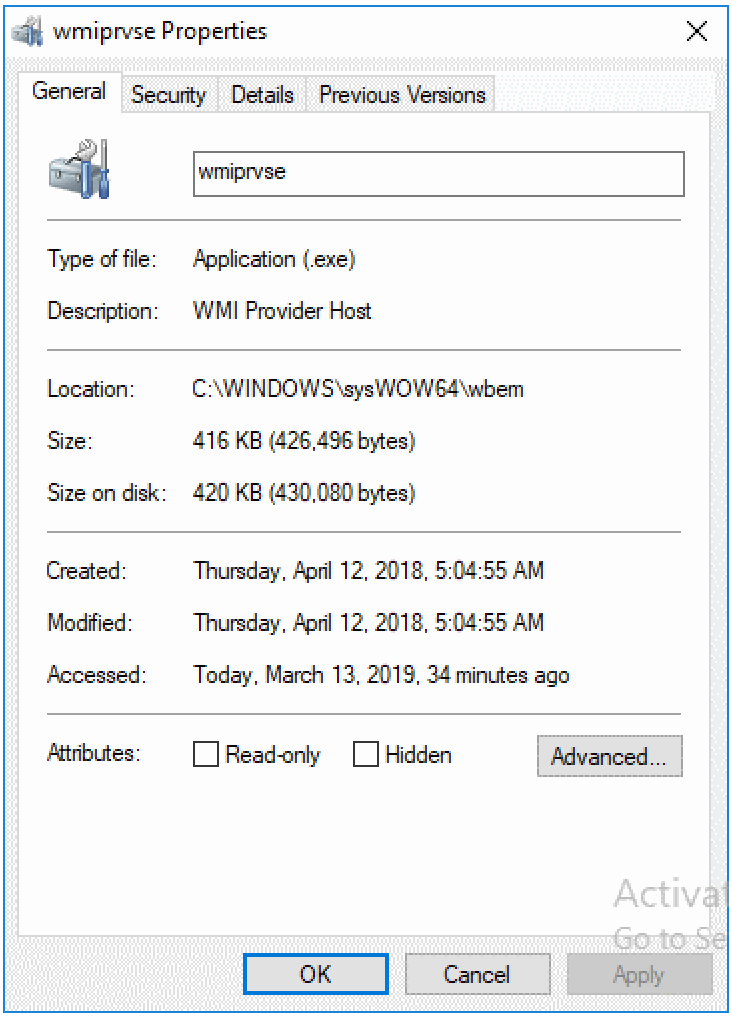
User Time: 00:00:00.000

I/O Priority: Normal

Context 90

Memory Priority: 5

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



wmiprvse Properties

wmiprvse

Type of file: Application (.exe)

Description: WMI Provider Host

Location: C:\WINDOWS\sysWOW64\wbem

Size: 416 KB (426,496 bytes)

Size on disk: 420 KB (430,080 bytes)

Created: Thursday, April 12, 2018, 5:04:55 AM

Modified: Thursday, April 12, 2018, 5:04:55 AM

Accessed: Today, March 13, 2019, 34 minutes ago

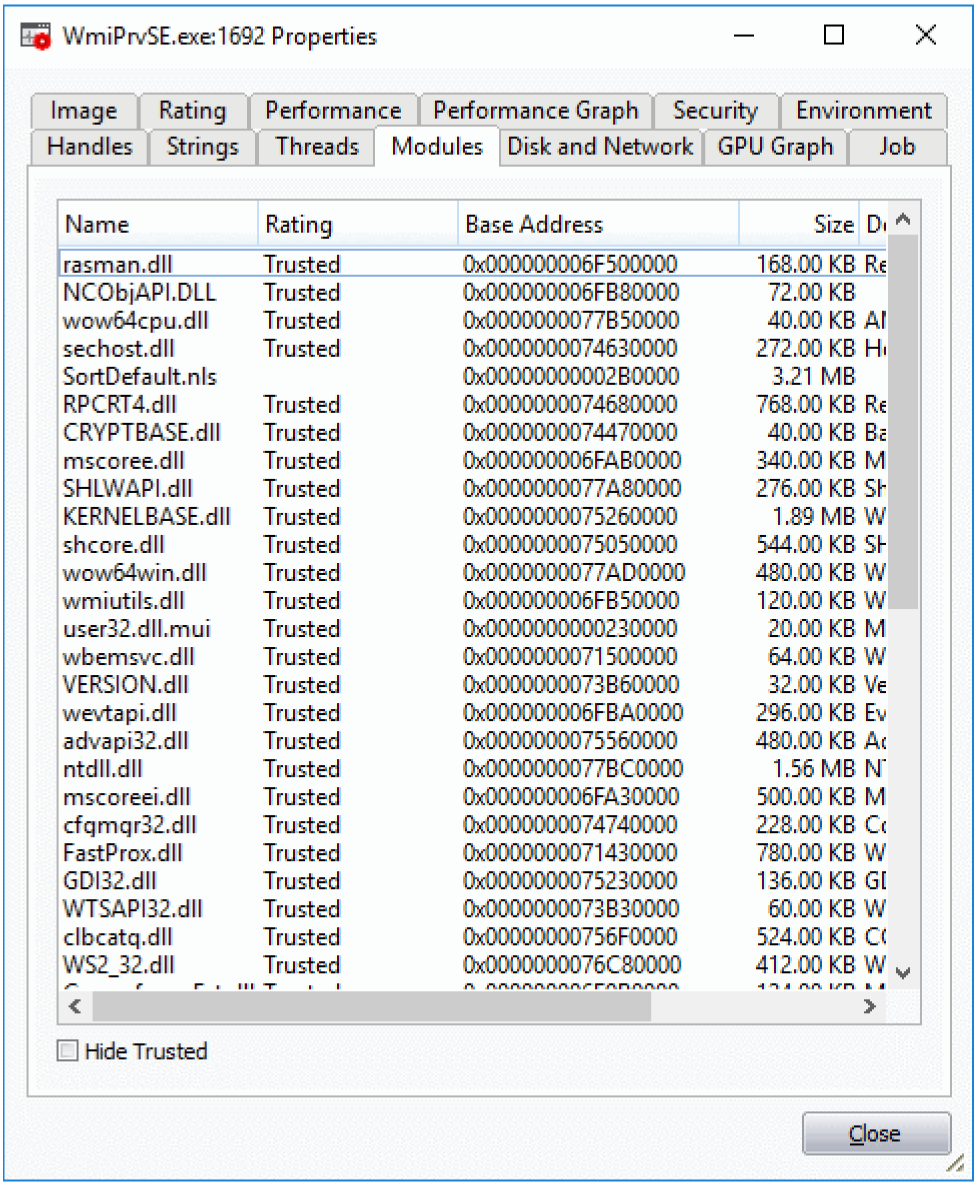
Attributes: □ Read-only □ Hidden

- **Kill -** Terminates the thread. Terminating the thread does not stop the associated process or remove the process object.
- **Suspend -** Temporarily stops the thread.

Click here to go back to list of properties.

Modules

The modules tab displays the executable files(DLL files) loaded by the process. Modules are the dynamic link library (DLL) files that are loaded to the system memory by the selected process. You can also open this window by double clicking on a module that opens its 'Properties' dialog.



Name	Rating	Base Address	Size	D
rasman.dll	Trusted	0x000000006F500000	168.00 KB	Re
NCObjAPI.DLL	Trusted	0x000000006FB80000	72.00 KB	
wow64cpu.dll	Trusted	0x0000000077B50000	40.00 KB	AI
sechost.dll	Trusted	0x0000000074630000	272.00 KB	H
SortDefault.nls		0x00000000002B0000	3.21 MB	
RPCRT4.dll	Trusted	0x0000000074680000	768.00 KB	Re
CRYPTBASE.dll	Trusted	0x0000000074470000	40.00 KB	Ba
mscoree.dll	Trusted	0x000000006FAB0000	340.00 KB	M
SHLWAPI.dll	Trusted	0x0000000077A80000	276.00 KB	Sh
KERNELBASE.dll	Trusted	0x0000000075260000	1.89 MB	W
shcore.dll	Trusted	0x0000000075050000	544.00 KB	SH
wow64win.dll	Trusted	0x0000000077AD0000	480.00 KB	W
wmiutils.dll	Trusted	0x000000006FB50000	120.00 KB	W
user32.dll.mui	Trusted	0x0000000000230000	20.00 KB	M
wbemsvc.dll	Trusted	0x0000000071500000	64.00 KB	W
VERSION.dll	Trusted	0x0000000073B60000	32.00 KB	Ve
wevtapi.dll	Trusted	0x000000006FBA0000	296.00 KB	Ev
advapi32.dll	Trusted	0x0000000075560000	480.00 KB	Ac
ntdll.dll	Trusted	0x0000000077BC0000	1.56 MB	N
mscoreei.dll	Trusted	0x000000006FA30000	500.00 KB	M
cfgmgr32.dll	Trusted	0x0000000074740000	228.00 KB	Cc
FastProx.dll	Trusted	0x0000000071430000	780.00 KB	W
GDI32.dll	Trusted	0x0000000075230000	136.00 KB	GI
WTSAPI32.dll	Trusted	0x0000000073B30000	60.00 KB	W
clbcatq.dll	Trusted	0x00000000756F0000	524.00 KB	C(
WS2_32.dll	Trusted	0x0000000076C80000	412.00 KB	W

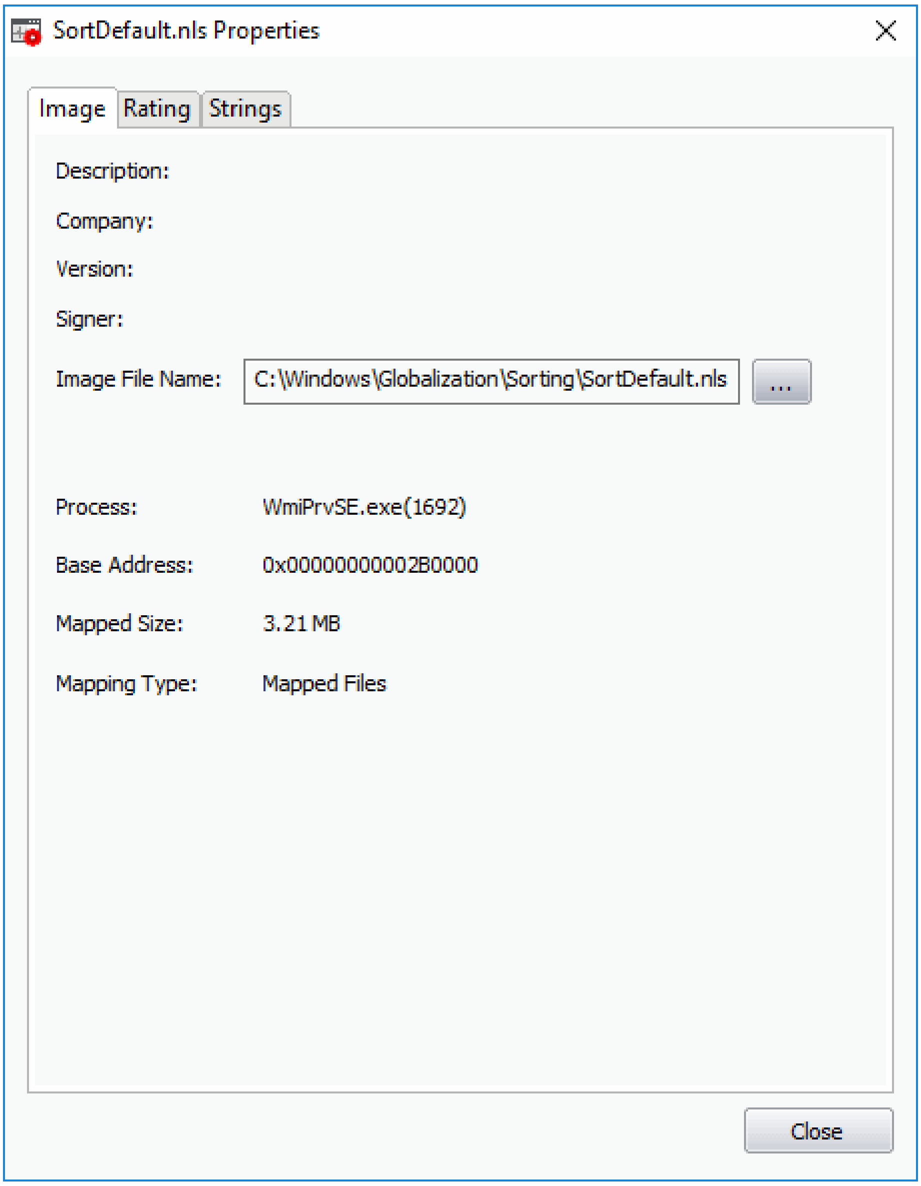
☐ Hide Trusted

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

- **Hide Trusted** - Removes DLL modules identified as trusted by KillSwitch and displays only unknown and untrusted modules.

Handle the Modules

Double-clicking on one of the modules open the 'Properties' dialog of the module.



Description:

Company:

Version:

Signer:

Image File Name: C:\Windows\Globalization\Sorting\SortDefault.nls

Process: WmiPrvSE.exe(1692)

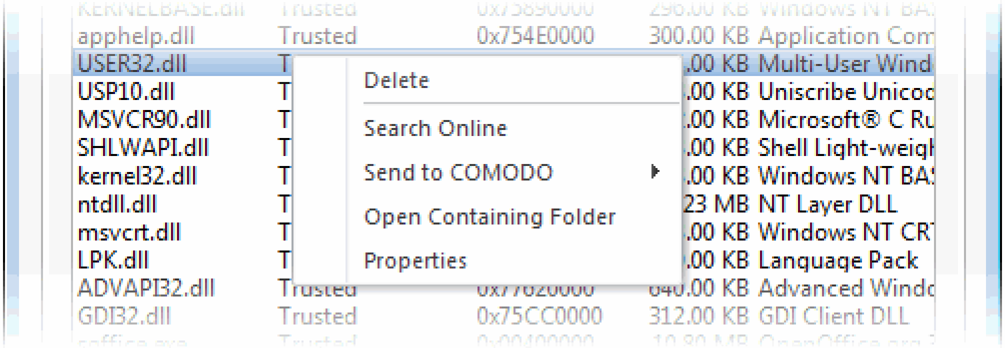
Base Address: 0x00000000002B0000

Mapped Size: 3.21 MB

Mapping Type: Mapped Files

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

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.



apphelp.dll	Trusted	0x754E0000	300.00 KB	Application Com
USER32.dll	T		.00 KB	Multi-User Wind
USP10.dll	T		.00 KB	Uniscribe Unicod
MSVCR90.dll	T		.00 KB	Microsoft® C Ru
SHLWAPI.dll	T		.00 KB	Shell Light-weigh
kernel32.dll	T		.00 KB	Windows NT BAS
ntdll.dll	T		23 MB	NT Layer DLL
msvcrt.dll	T		.00 KB	Windows NT CRT
LPK.dll	T		.00 KB	Language Pack
ADVAPI32.dll	Trusted		640.00 KB	Advanced Windo
GDI32.dll	Trusted	0x75CC0000	312.00 KB	GDI Client DLL

- **Delete -** Removes the selected module from your computer. You need to confirm before deleting the module.

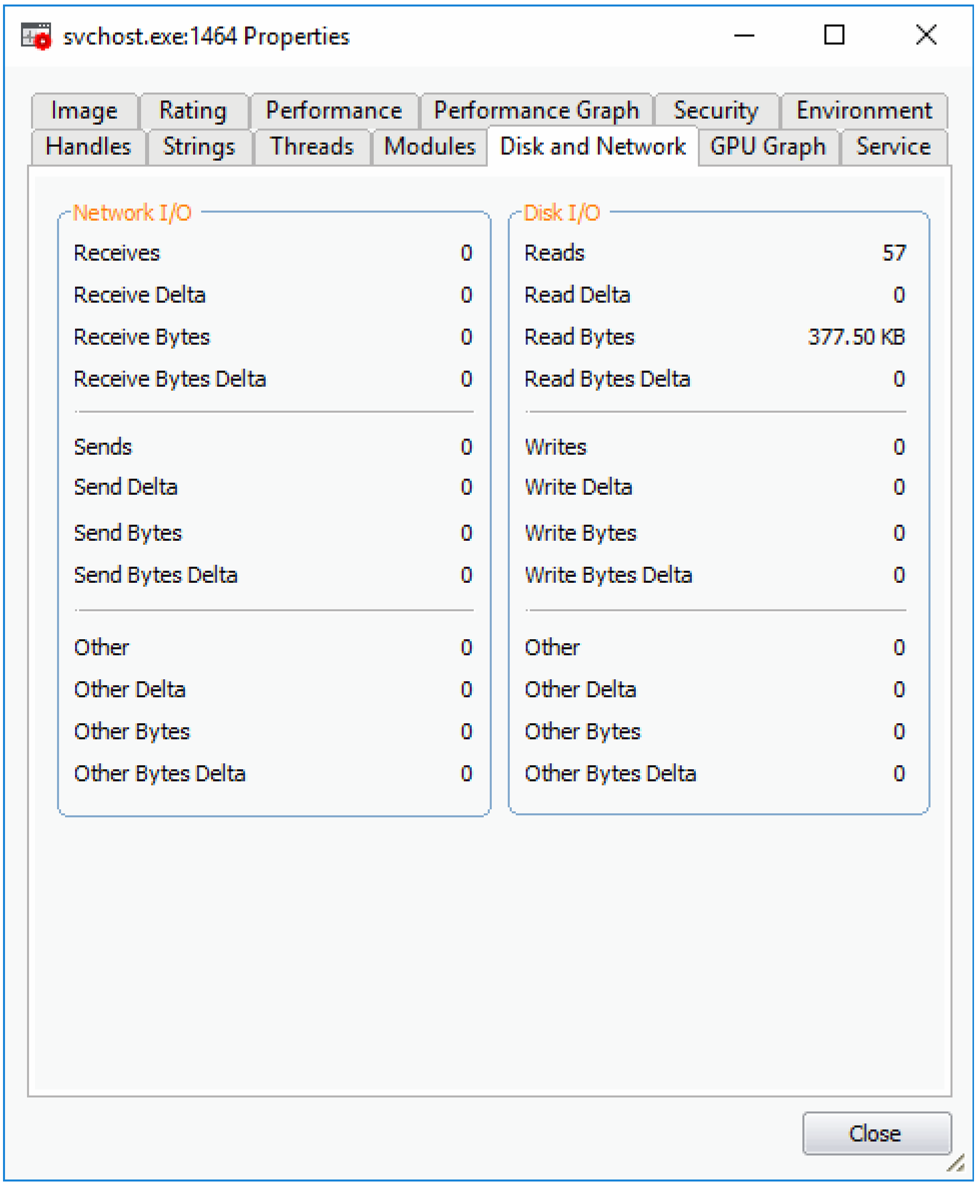
Warning: Deleting some critical modules of an application may render the application unusable.

- **Search Online -** Opens the default web browser with the specified search engine and searches for information on the module.
- **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 -** Displays the folder in which the module is stored, through 'Windows Explorer'.
- **Properties -** Shows the 'Properties' dialog of the module.

Click here to go back to list of properties.

Disk and Network

The disk and network tab contains two areas which display a range of network and disk I/O (input/output) statistics per program.



Network I/O

Receives	0
Receive Delta	0
Receive Bytes	0
Receive Bytes Delta	0
Sends	0
Send Delta	0
Send Bytes	0
Send Bytes Delta	0
Other	0
Other Delta	0
Other Bytes	0
Other Bytes Delta	0

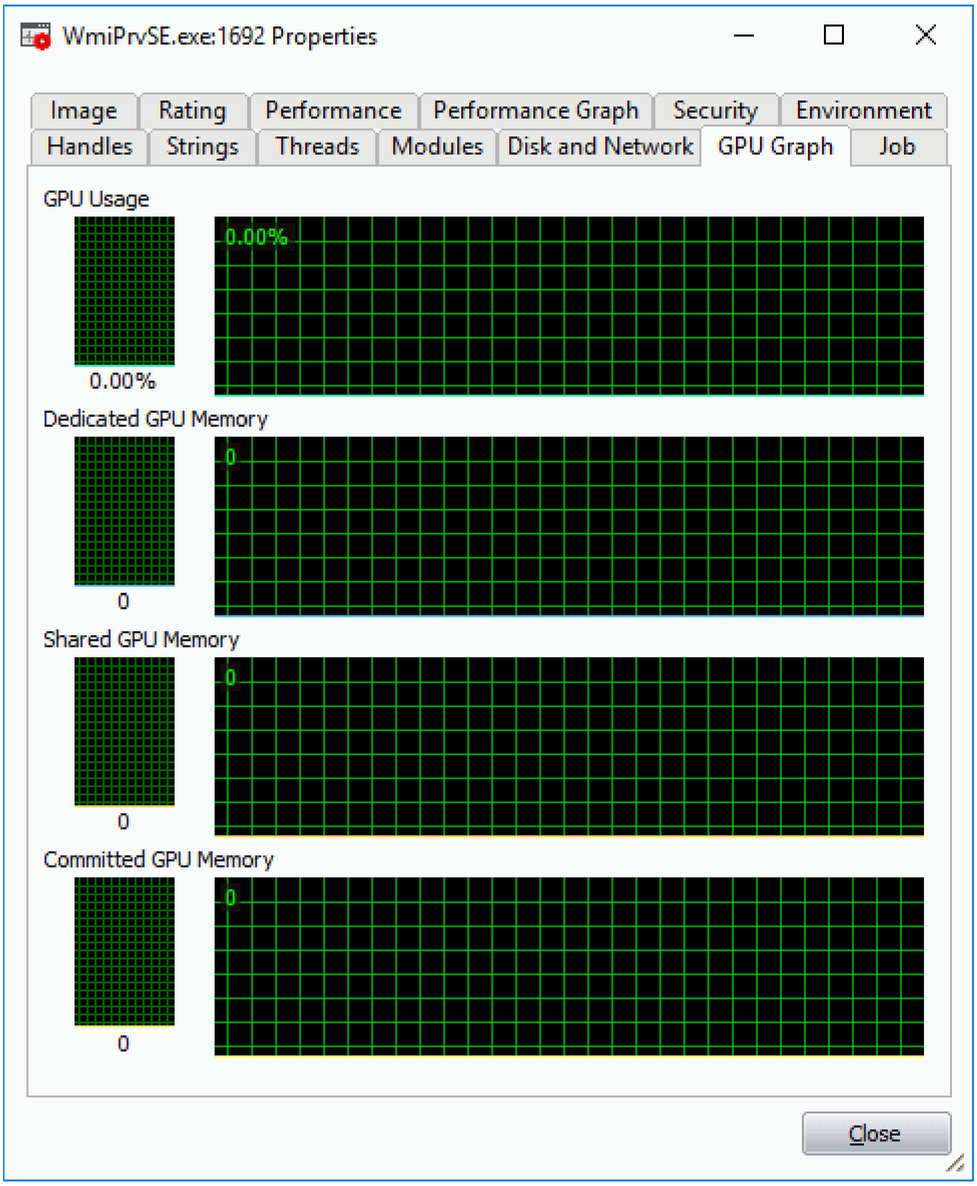
Disk I/O

Reads	57
Read Delta	0
Read Bytes	377.50 KB
Read Bytes Delta	0
Writes	0
Write Delta	0
Write Bytes	0
Write Bytes Delta	0
Other	0
Other Delta	0
Other Bytes	0
Other Bytes Delta	0

Click here to go back to list of properties.

GPU Graph

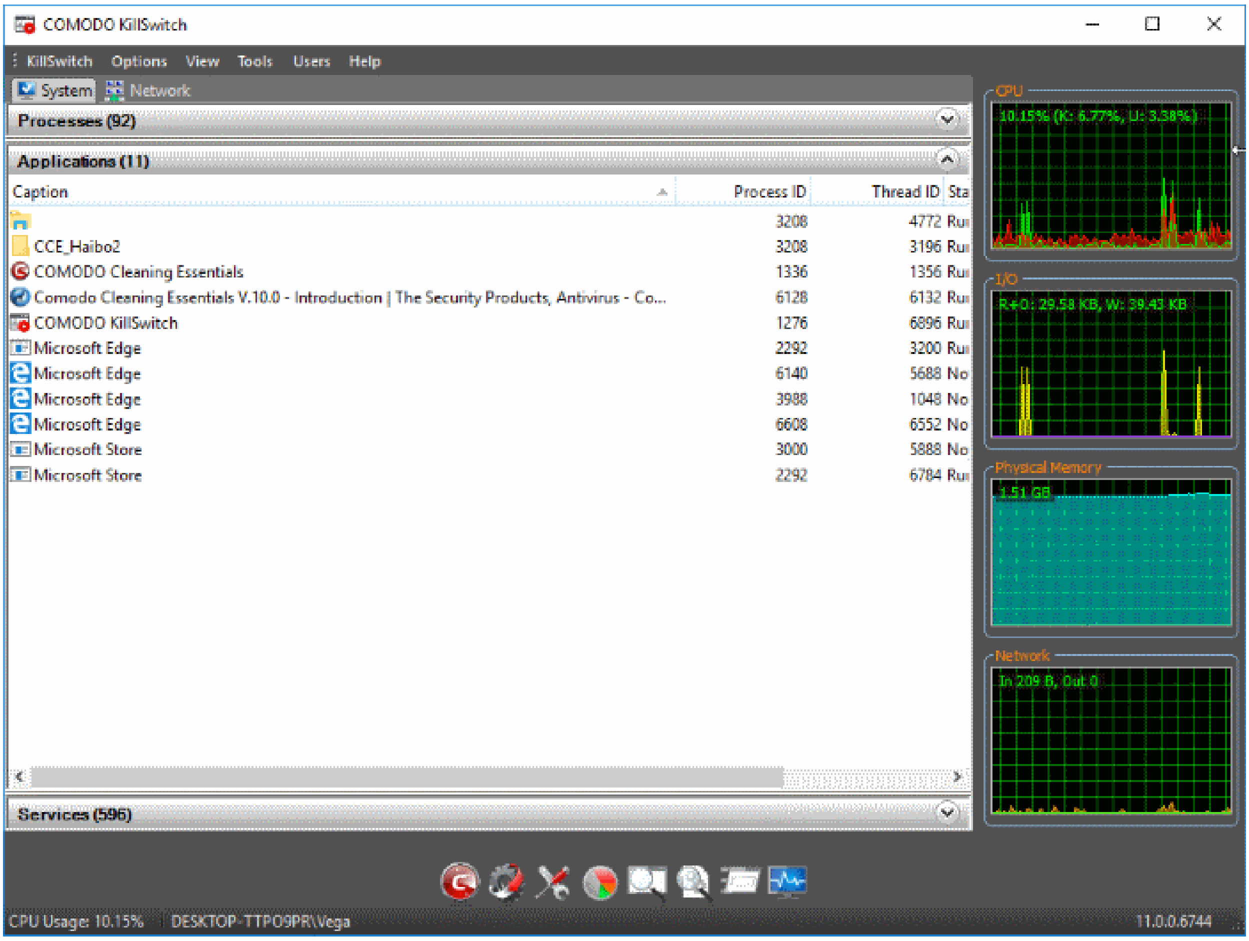
The GPU graph represents four graphs of the graphical memory process' performance - GPU Usage, Dedicated GPU Memory, Shared GPU Memory and Committed GPU Memory. This window helps the advanced users to monitor the resource overhead of a process pictorially. You can hover your mouse over the graphs to view details.



Click here to go back to list of properties.

5.3.2. Applications

- Open CCE > click the 'System' tab > click the 'Applications' bar.
- The applications window shows all programs that are currently running in your system.
- Right-click on an application to close the application, access the application process and more.

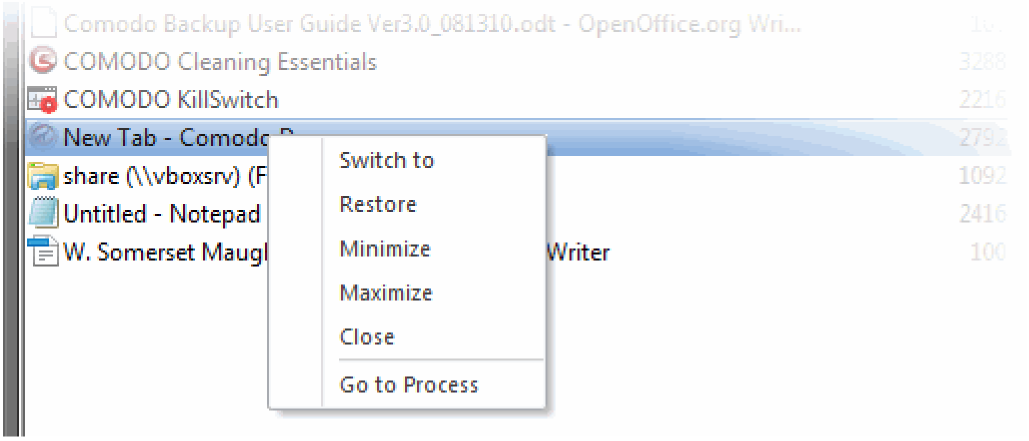


Caption	Process ID	Thread ID	Sta
	3208	4772	Ru
CCE_Haibo2	3208	3196	Ru
COMODO Cleaning Essentials	1336	1356	Ru
Comodo Cleaning Essentials V.10.0 - Introduction | The Security Products, Antivirus - Co...	6128	6132	Ru
COMODO KillSwitch	1276	6896	Ru
Microsoft Edge	2292	3200	Ru
Microsoft Edge	6140	5688	No
Microsoft Edge	3988	1048	No
Microsoft Edge	6608	6552	No
Microsoft Store	3000	5888	No
Microsoft Store	2292	6784	Ru

Applications Table - Descriptions of Columns	
Column	**Description**
Caption	The names of the applications. Click the column header to sort items in ascending or descending order.
Process ID	The unique process identification number of the process started by the application. Click the column header to sort items in ascending or descending order.
Thread ID	The unique thread identification number of the thread started by the application. Click the column header to sort items in ascending or descending order.
Status	The current execution status of the application. For example, 'Running', 'Not running' etc.

5.3.2.1. Handle the Applications

- Open KillSwitch > click the 'System' tab > click the 'Applications' bar > right-click on an application:



- **Switch to -** Makes the application active, minimizing the KillSwitch window
- **Restore -** Resurrects a minimized application to its last state
- **Minimize -** Move the application window to the Windows task bar
- **Maximize -** Run the application in a full-screen window
- **Close** - Exit 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. See **Stop, Start and Handle Processes** for more details.

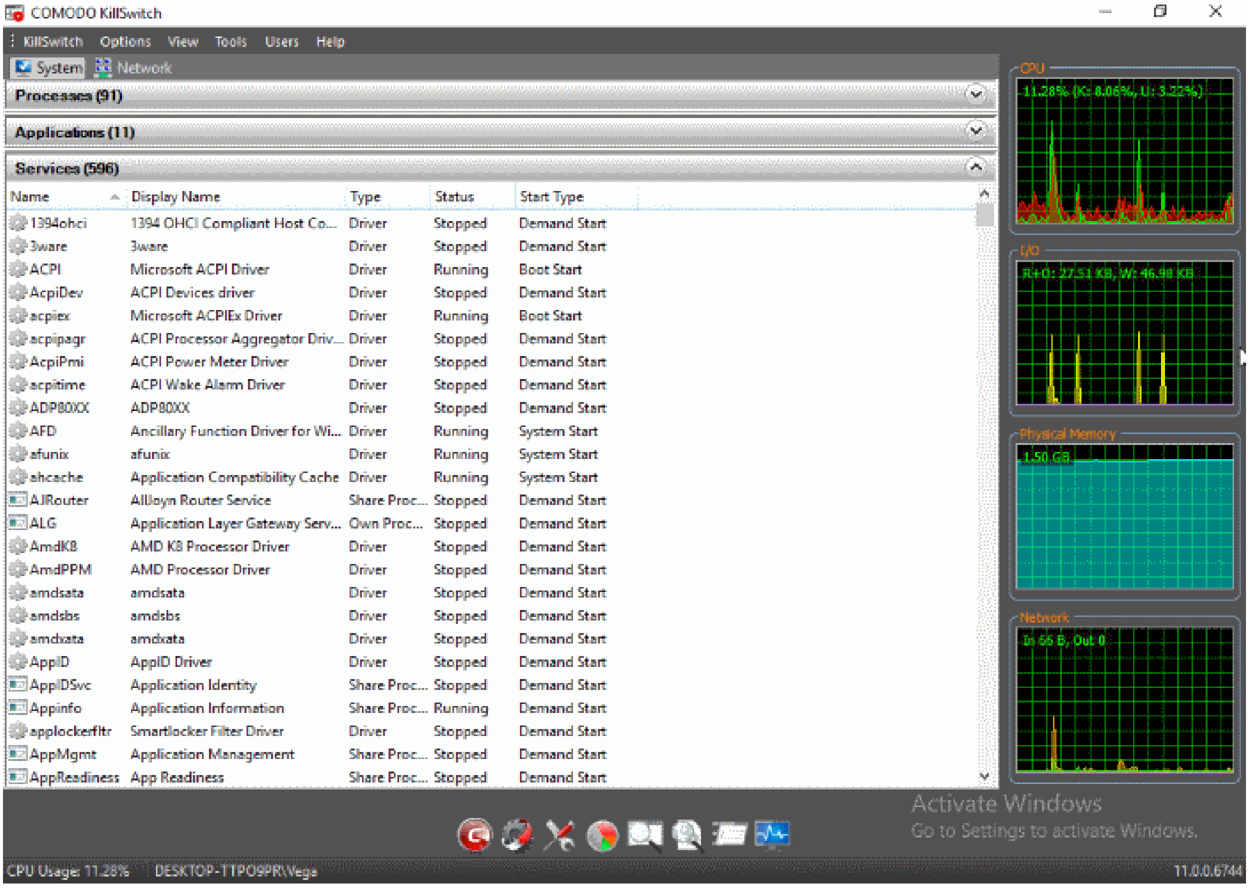
5.3.3. Services

- Click 'Tools' > 'Open KillSwitch'
- Click the 'System' tab > click the 'Services' bar.

The services area shows all windows services/drivers loaded in your system. You can review, start, stop, restart or delete services as required.

- ▤ - The service is associated with a process/application
- ⚙ - The service is associated with a driver

- Right-click on a service to start, stop, restart or delete the service. Hold the 'Ctrl' key to select multiple services.



Name	Display Name	Type	Status	Start Type
1394ohci	1394 OHCI Compliant Host Co...	Driver	Stopped	Demand Start
3ware	3ware	Driver	Stopped	Demand Start
ACPI	Microsoft ACPI Driver	Driver	Running	Boot Start
AcpiDev	ACPI Devices driver	Driver	Stopped	Demand Start
acpiex	Microsoft ACPIEx Driver	Driver	Running	Boot Start
acpipagr	ACPI Processor Aggregator Driv...	Driver	Stopped	Demand Start
AcpiPmi	ACPI Power Meter Driver	Driver	Stopped	Demand Start
acpitime	ACPI Wake Alarm Driver	Driver	Stopped	Demand Start
ADP80XX	ADP80XX	Driver	Stopped	Demand Start
AFD	Ancillary Function Driver for Wi...	Driver	Running	System Start
afunix	afunix	Driver	Running	System Start
ahcache	Application Compatibility Cache	Driver	Running	System Start
AJRouter	AllJoyn Router Service	Share Proc...	Stopped	Demand Start
ALG	Application Layer Gateway Serv...	Own Proc...	Stopped	Demand Start
AmdK8	AMD K8 Processor Driver	Driver	Stopped	Demand Start
AmdPPM	AMD Processor Driver	Driver	Stopped	Demand Start
amdsata	amdsata	Driver	Stopped	Demand Start
amdsbs	amdsbs	Driver	Stopped	Demand Start
amdxata	amdxata	Driver	Stopped	Demand Start
AppID	AppID Driver	Driver	Stopped	Demand Start
AppIDSvc	Application Identity	Share Proc...	Stopped	Demand Start
Appinfo	Application Information	Share Proc...	Running	Demand Start
applockerfltr	Smartlocker Filter Driver	Driver	Stopped	Demand Start
AppMgmt	Application Management	Share Proc...	Stopped	Demand Start
AppReadiness	App Readiness	Share Proc...	Stopped	Demand Start

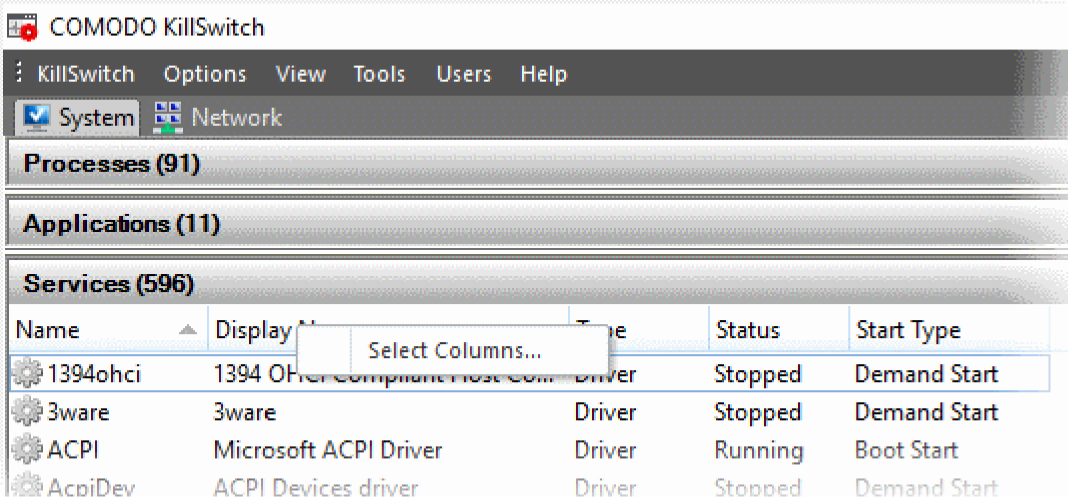
The table below describes the columns that are displayed by default. You can add or remove the columns as per your requirement. See **Column Selection** for more detailed explanation on this.

Services Table - Descriptions of Columns	
Column	**Description**
Name	• The title of the service. • Clicking the column header sorts the entries in ascending or descending order of the names.
Display Name	• Shows the title by which the service is indicated in the Windows System Configuration Utility. Clicking on the column header sorts the entries in ascending or descending order of the display labels.
Type	• The category 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 situation 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 initiated, i.e. whether it automatically starts with Windows, starts on demand or disabled. • Clicking on the column header sorts the entries in based on their start types.

Column Selection

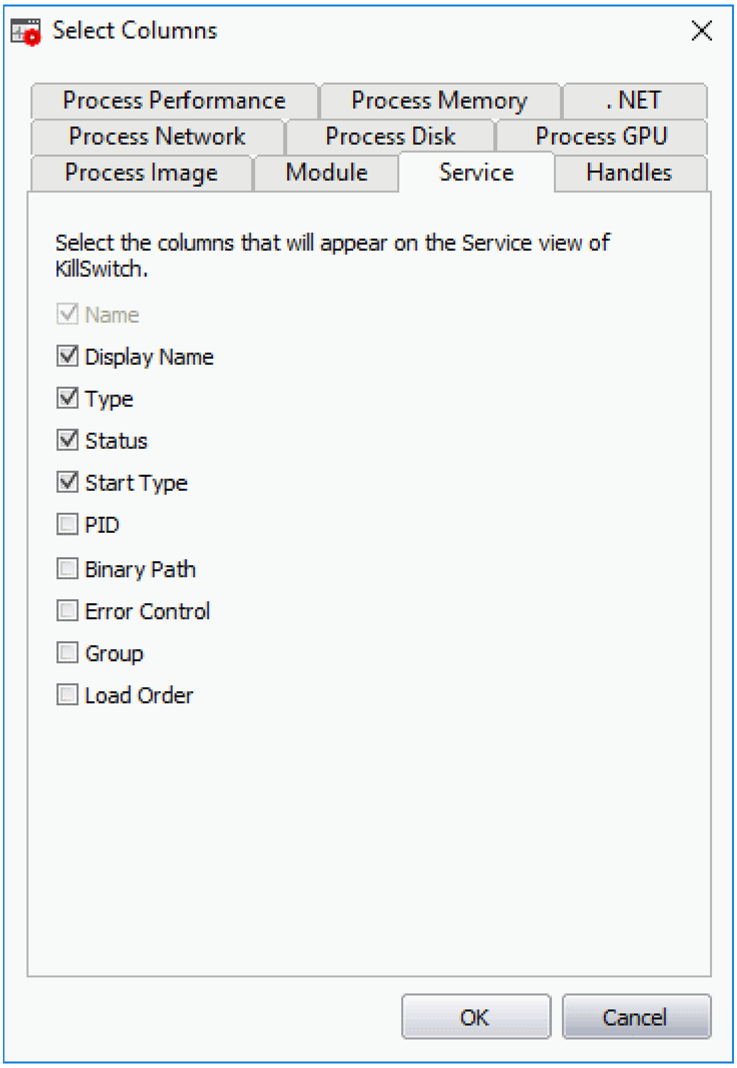
The services window displays details about each process in five columns. Advanced users can view more details by adding more columns as required.

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



Name	Display N...	Type	Status	Start Type
1394ohci	1394 OHCI Compliant Host Co...	Driver	Stopped	Demand Start
3ware	3ware	Driver	Stopped	Demand Start
ACPI	Microsoft ACPI Driver	Driver	Running	Boot Start
AcpiDev	ACPI Devices driver	Driver	Stopped	Demand Start

The 'Select Columns' dialog opens.



Select Columns

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

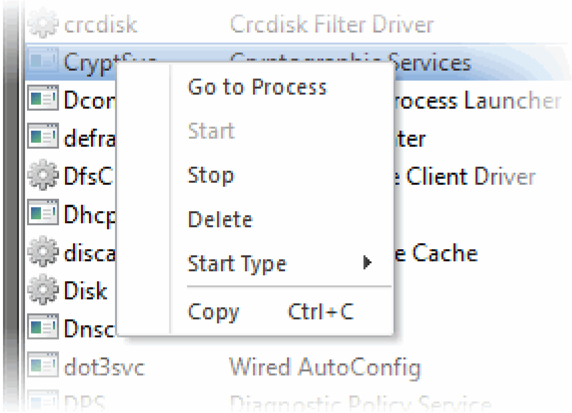
☑ Name
☑ Display Name
☑ Type
☑ Status
☑ Start Type
□ PID
□ Binary Path
□ Error Control
□ Group
□ Load Order

- Enable the columns by choosing the respective check-boxes
- Click 'OK' for your configuration to take effect.

See **Processes** for more information.

5.3.3.1. Stop, Start and Delete Services

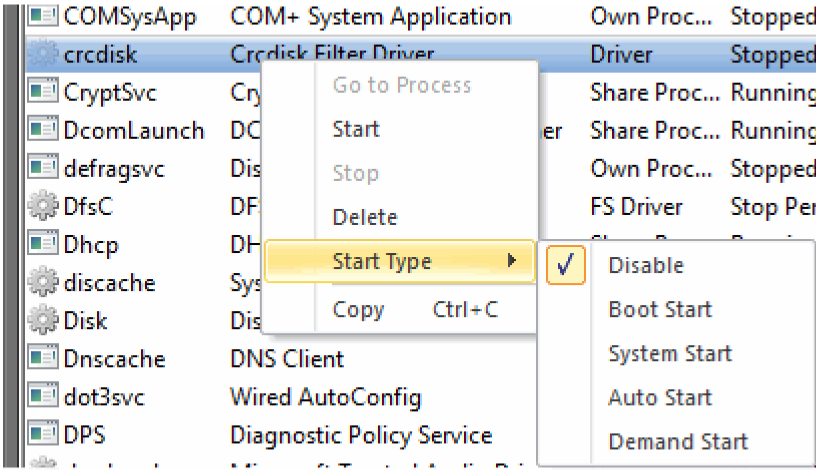
In the services window, you can start, stop and delete services by right-clicking the selected service and selecting the desired option from the context sensitive menu:



- **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. See Stop, Start and Handle Processes for more details
- **Start** - Initiates the selected service. This option is available only for the services with 'Stopped' status
- **Stop** - Terminates the running service. This option is available only for the services with 'Running' status
- **Restart** - Reboots the running service. This option is available only for the services with 'Running' status
- **Delete** - Removes 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 need to confirm 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 should commence. Hovering the mouse cursor over 'Start Type' will open a sub-menu with the options:


COMSysApp COM+ System Application Own Proc... Stopped
crcdisk Crcdisk Filter Driver Driver Stopped
CryptSvc Cry Share Proc... Running
DcomLaunch DC er Share Proc... Running
defragsvc Dis Own Proc... Stopped
DfsC DF FS Driver Stop Pe
Dhcp DH
discache Sys
Disk Dis
Dnscache DNS Client
dot3svc Wired AutoConfig
DPS Diagnostic Policy Service
Go to Process
Start
Stop
Delete
Start Type
Copy Ctrl+C
✓ Disable
Boot Start
System Start
Auto Start
Demand Start

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

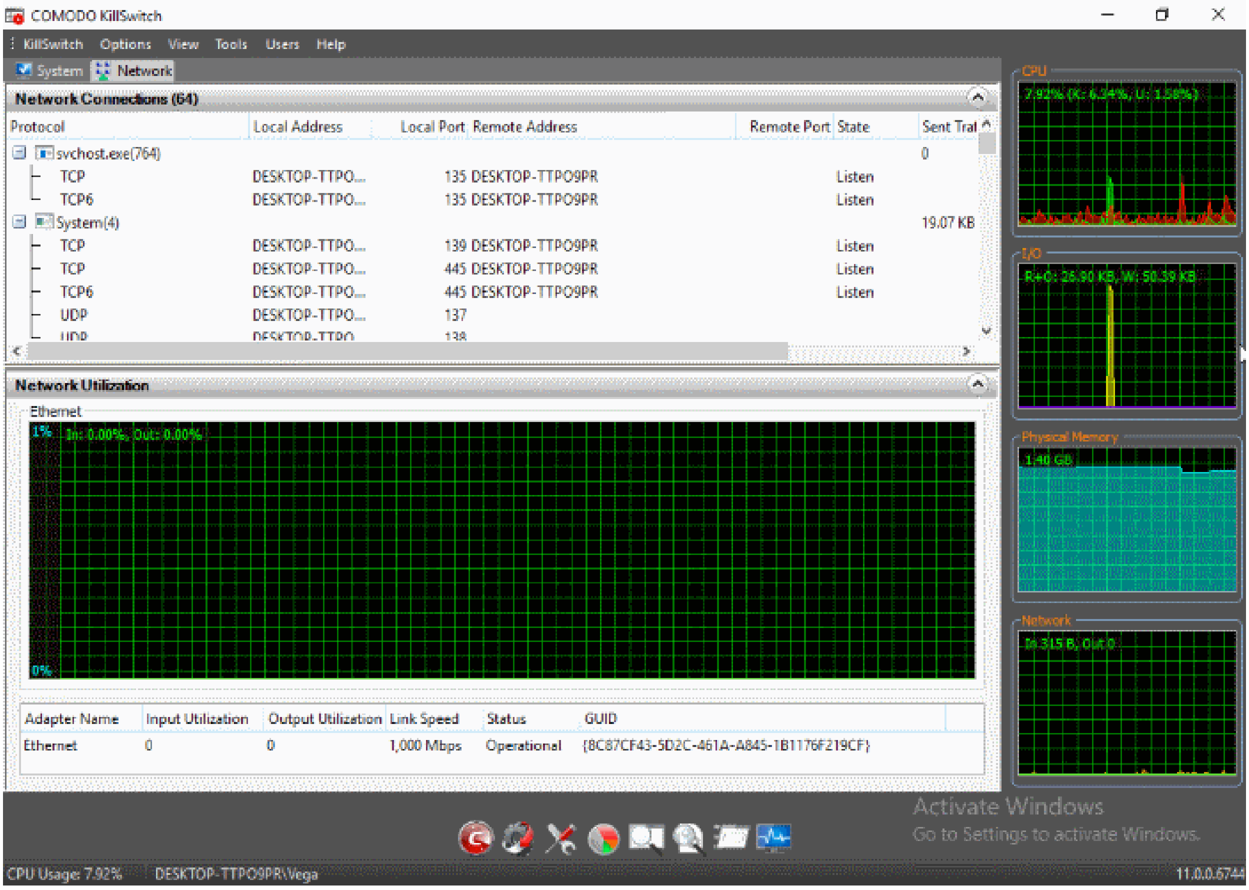
- **Disable** - The service stops from running
- Boot Start - The service loads by the boot loader and starts when the system is booted
- **System Start** - The service starts during kernel initialization automatically
- **Auto Start** - The service starts automatically upon each restart of the computer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

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

5.4. View and Handle Network Connections and Usage

- Click 'Tools' > 'Open KillSwitch'
- Click the 'Network' tab
- The network tab contains details about currently active connections on your system:

  - Network Connections - A list of all open connections. Right-click on a connection to manage the connection
- Network Utilization - A chart which shows traffic usage in real-time
- CPU, I/O and memory usage are shown on the right



Network Connections (64)

Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Tra
svchost.exe(764)						0
TCP	DESKTOP-TTPO...	135	DESKTOP-TTPO9PR		Listen	
TCP6	DESKTOP-TTPO...	135	DESKTOP-TTPO9PR		Listen	
System(4)						19.07 KB
TCP	DESKTOP-TTPO...	139	DESKTOP-TTPO9PR		Listen	
TCP	DESKTOP-TTPO...	445	DESKTOP-TTPO9PR		Listen	
TCP6	DESKTOP-TTPO...	445	DESKTOP-TTPO9PR		Listen	
UDP	DESKTOP-TTPO...	137				
UDP	DESKTOP-TTPO	138				

Network Utilization

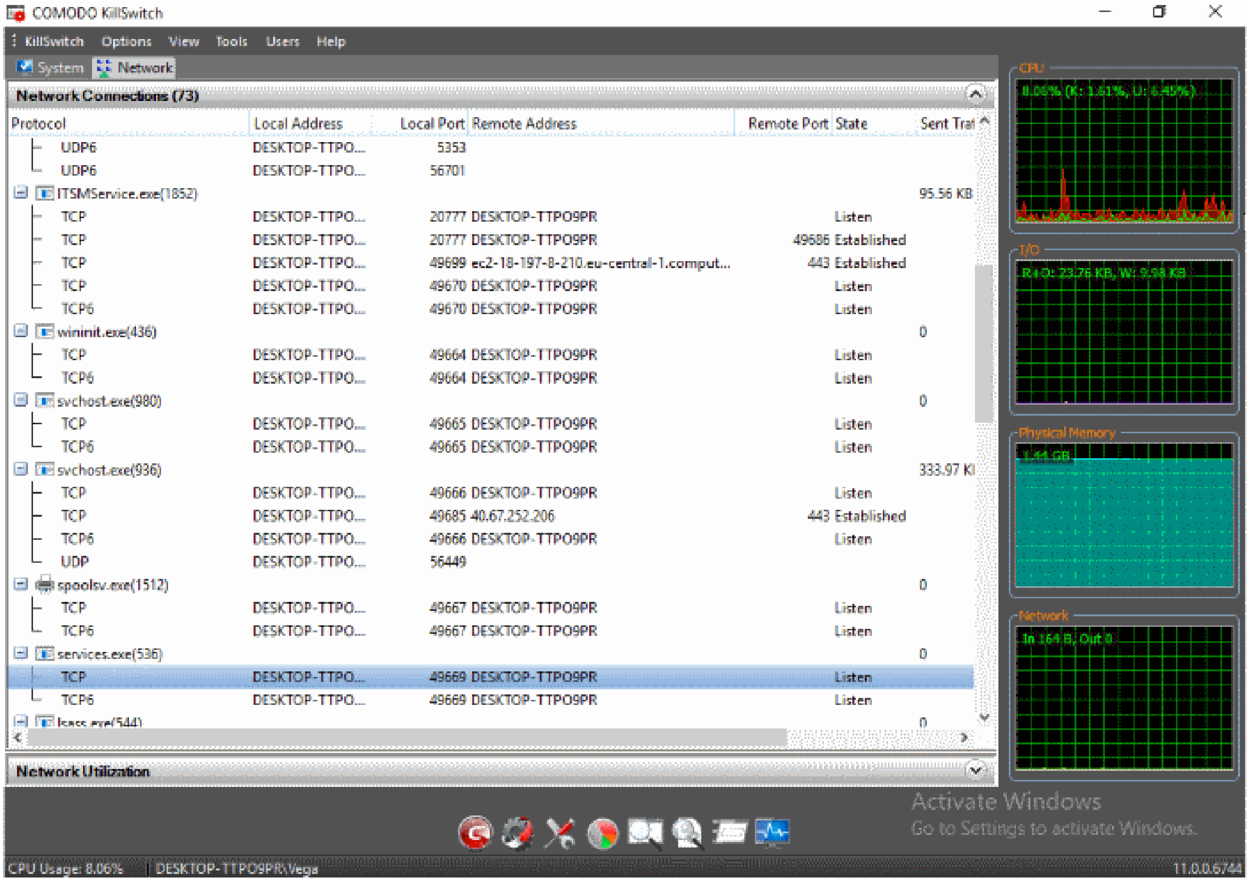
Adapter Name	Input Utilization	Output Utilization	Link Speed	Status	GUID
Ethernet	0	0	1,000 Mbps	Operational	{8C87CF43-5D2C-461A-A845-1B1176F219CF}

See the following for more details:

- **Network Connections**
- **Network Utilization**

5.4.1. Network Connections

- Click 'Tools' > 'Open KillSwitch'
- Click the 'Network' tab > Click the 'Network Connections' bar
- Right-click on a connection to view the process associated with the connection, and to close the connection.



Network Connections (73)

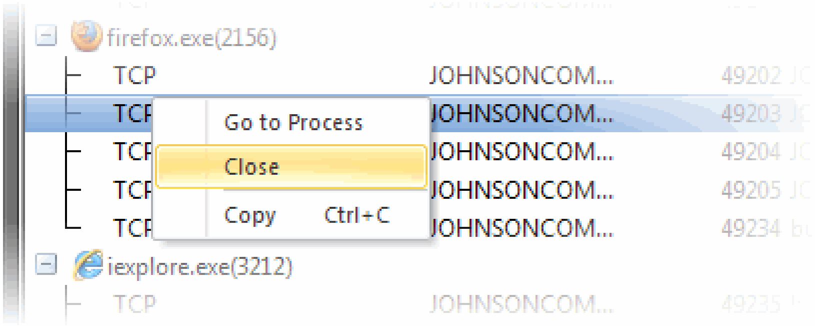
Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Traf
UDP6	DESKTOP-TTPO...	5353				
UDP6	DESKTOP-TTPO...	56701				
ITSMService.exe(1852)						95.56 KB
TCP	DESKTOP-TTPO...	20777	DESKTOP-TTPO9PR		Listen	
TCP	DESKTOP-TTPO...	20777	DESKTOP-TTPO9PR	49686	Established	
TCP	DESKTOP-TTPO...	49699	ec2-18-197-8-210.eu-central-1.comput...	443	Established	
TCP	DESKTOP-TTPO...	49670	DESKTOP-TTPO9PR		Listen	
TCP6	DESKTOP-TTPO...	49670	DESKTOP-TTPO9PR		Listen	
wininit.exe(436)						0
TCP	DESKTOP-TTPO...	49664	DESKTOP-TTPO9PR		Listen	
TCP6	DESKTOP-TTPO...	49664	DESKTOP-TTPO9PR		Listen	
svchost.exe(980)						0
TCP	DESKTOP-TTPO...	49665	DESKTOP-TTPO9PR		Listen	
TCP6	DESKTOP-TTPO...	49665	DESKTOP-TTPO9PR		Listen	
svchost.exe(936)						333.97 KI
TCP	DESKTOP-TTPO...	49666	DESKTOP-TTPO9PR		Listen	
TCP	DESKTOP-TTPO...	49685	40.67.252.206	443	Established	
TCP6	DESKTOP-TTPO...	49666	DESKTOP-TTPO9PR		Listen	
UDP	DESKTOP-TTPO...	56449				
spoolsv.exe(1512)						0
TCP	DESKTOP-TTPO...	49667	DESKTOP-TTPO9PR		Listen	
TCP6	DESKTOP-TTPO...	49667	DESKTOP-TTPO9PR		Listen	
services.exe(536)						0
TCP	DESKTOP-TTPO...	49669	DESKTOP-TTPO9PR		Listen	
TCP6	DESKTOP-TTPO...	49669	DESKTOP-TTPO9PR		Listen	
lsass.exe(544)						0

Network Connections Table - Descriptions of Columns	
Column	**Description**
Protocol	• Shows the connection protocol type. • Click on the column header to sort the entries in based on the protocols.
Local Address	• Shows your system's name • Click on the column header to sort the entries in ascending or descending numerical/alphabetical order of the addresses. • **Note**: The host names are displayed only if the option '**Resolve addresses for Network Address**' is enabled under '**Options**' menu. • Else only the IP addresses are displayed.
Local Port	• Shows the system port number through which the connection is established. • Click on the column header to sort the entries in ascending or descending order of the port numbers.
Remote Address	• Shows the system name of the remote host of the connection. • Click on the column header to sort the entries in ascending or descending numerical/alphabetical order of the addresses. • **Note**: The host names are displayed only if the option '**Resolve addresses for Network Address**' is enabled under '**Options**' menu.

	- Else only the IP addresses are displayed.
Remote Port	- Shows the port number of the remote host through which the connection is established. - Click on the column header to sort the entries in ascending or descending order of the port numbers.
State	- Shows the level of the connection established - Click on the column header to sort the entries in based on the status of each connection.

5.4.1.1. Inspect and Close Network Connections

- Click 'Tools' > 'Open KillSwitch'
- Click the 'Network' tab > Click the 'Network Connections' bar
- Right-click on a connection:



- **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 that brokered the connection.
- **Close** - Exits the network connection.
- **Copy -** Add information from the connection row to the clipboard

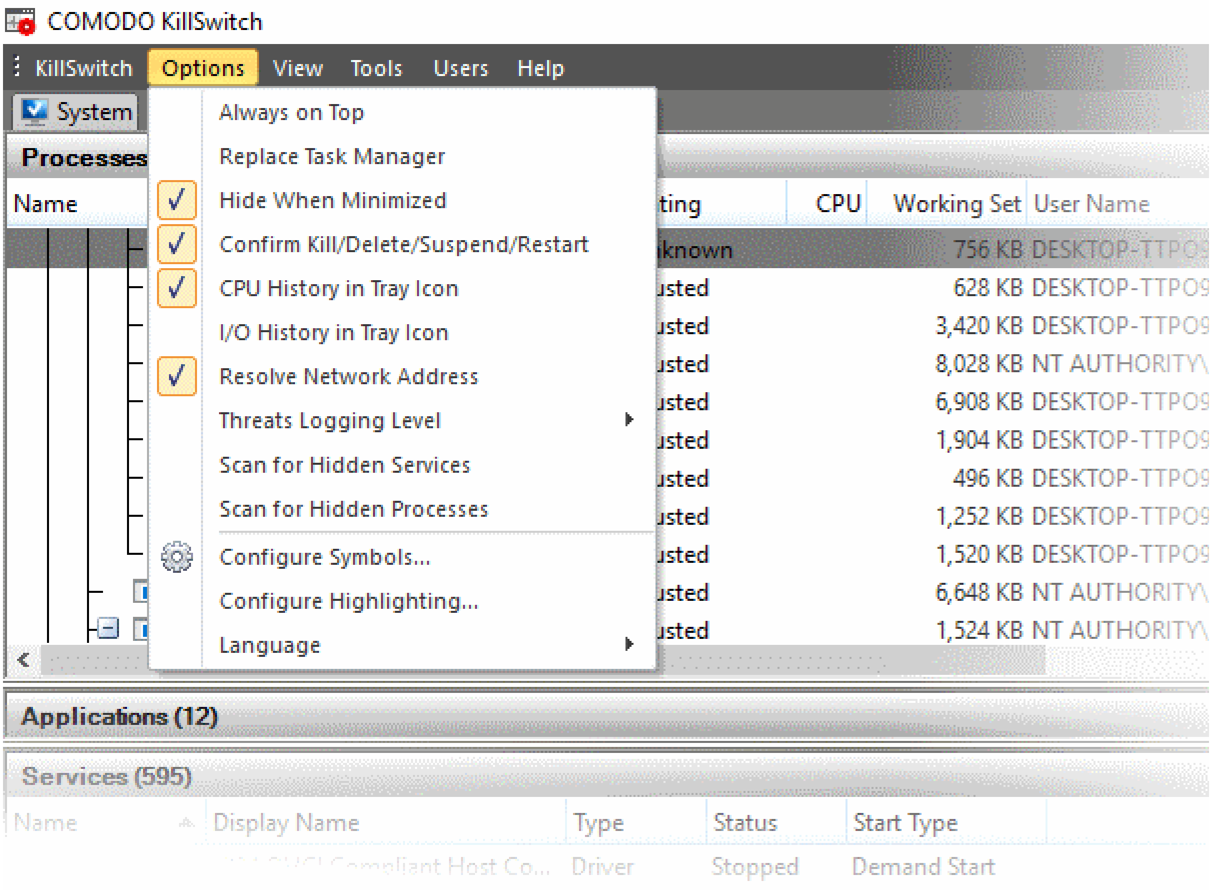
5.4.2. Network Utilization

- Click 'Tools' > 'Open KillSwitch'
- Click the 'System' tab > click the 'Network Utilization' bar
- The network utilization window shows how much traffic is being used over time by adapters on your computer.
- Hover your mouse cursor over the graph to view further details.
- The name and details of the adapter are shown under the graph.

Network Utilization Table - Descriptions of Columns	
Column	**Description**
Adapter Name	Shows the title 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 your computer with the network.
Status	Shows the traffic flow operation position through the network connection.
GUID	Shows 32 character Globally Unique Identifier of the connection.

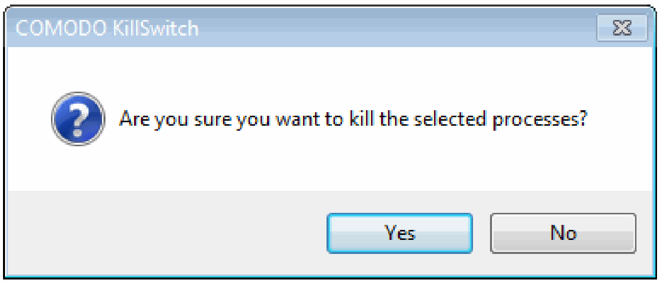
5.5. Configure KillSwitch

The 'Options' menu lets you configure 'KillSwitch' at a granular level:



- **Always on Top** - When non-minimized, the KillSwitch window is always visible ahead of any other applications. Other applications will appear in the background.
- **Replace Task Manager** - All methods used to open Windows Task Manager will instead open KillSwitch. Example methods include:
    - Ctrl + Alt + Del > Click 'Task Manager'
    - Right-click on the Windows task-bar and click 'Task Manager' Task Bar

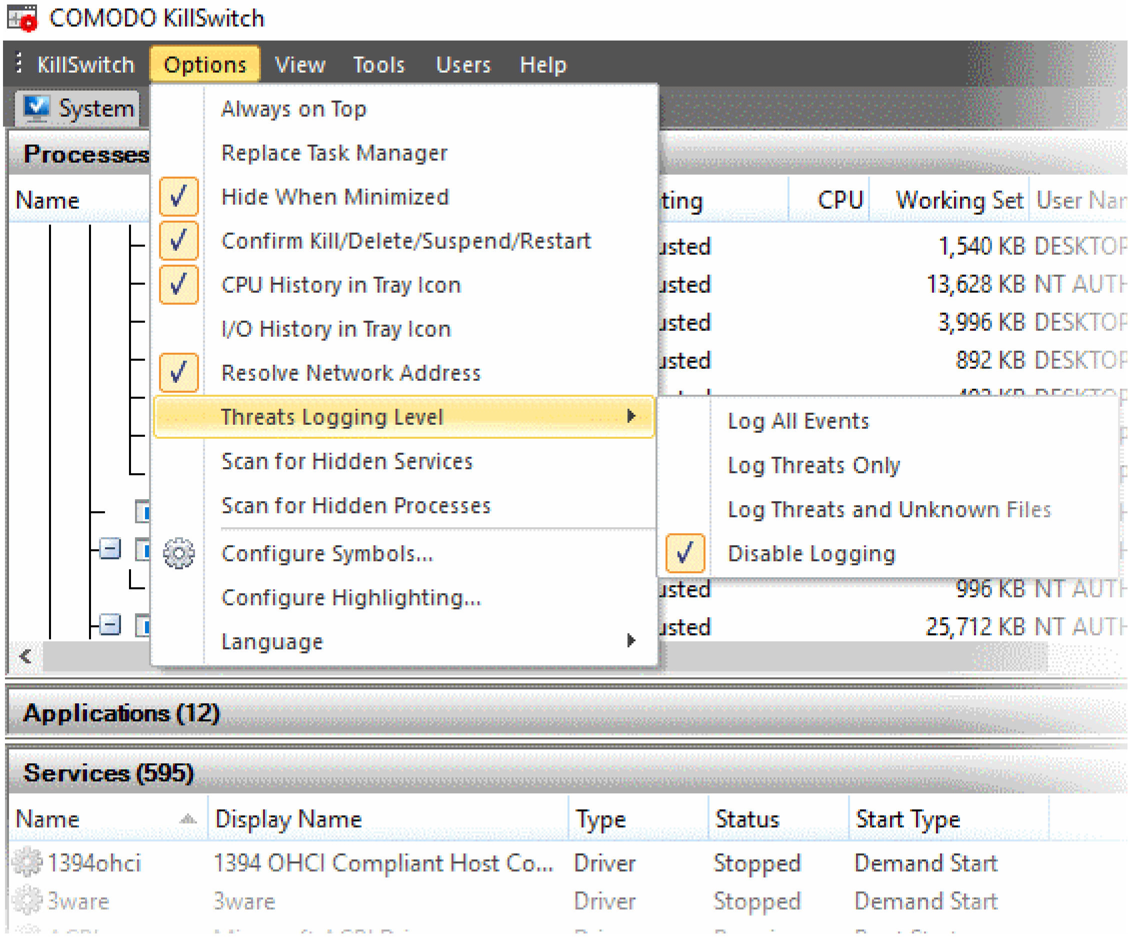
- **Hide When Minimized** - KillSwitch automatically runs in the background when it is minimized. You can double-click on the system tray icon to reopen the application.
- **Confirm Kill/Delete/Suspend/Restart** - KillSwitch shows a confirmation dialog whenever you take actions on a process:



COMODO KillSwitch

Are you sure you want to kill the selected processes?

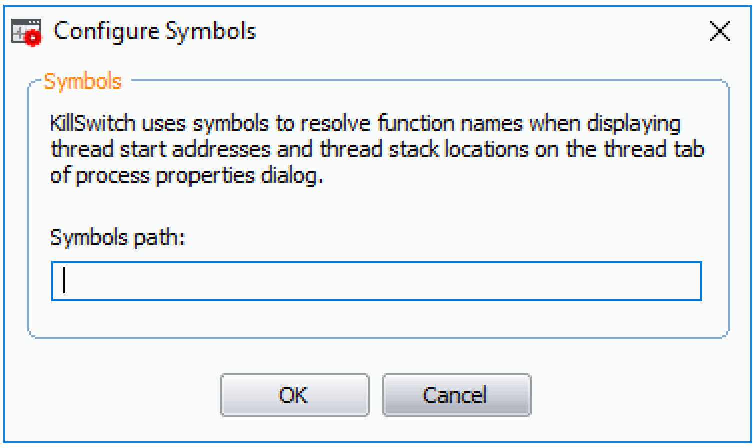
- **CPU History in Tray Icon** - A KillSwitch icon is shown in the system tray at the bottom-right corner of the screen. The icon provides a fast way to open or close the application, shutdown your system and so on. See '**The System Tray Icon**' for more details.
- **I/O History in Tray Icon** - The tray icon shows graphics to represent the input/output activities of your computer.
- **Resolve Network Address** - If enabled, KillSwitch shows host names 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 remote hosts are shown.
- **Threats Log Level** - Select which types of events you want to record in a log.



Name	Display Name	Type	Status	Start Type
1394ohci	1394 OHCI Compliant Host Co...	Driver	Stopped	Demand Start
3ware	3ware	Driver	Stopped	Demand Start

  - **Log All Events -** Record every event that takes place. This produces the most comprehensive reports but at the cost of larger file sizes.
  - **Log Threats Only -** Record only those events where KillSwitch detected a malicious process or service.
  - **Log Threats and Unknown Files -** Record events which concern malicious processes, and processes for which no trust rating exists. 'Unknown' processes have not yet been tested to establish whether they are safe to run or not.
  - **Disable Logging -** Do not record any events.

- **Scan for Hidden Services -** KillSwitch will run an instant scan for services running in the background
- **Scan for Hidden Processes -** KillSwitch will run an instant scan for programs running invisibly
- **Configure Symbols -** KillSwitch uses the program database symbols to resolve their function names to find the start addresses and stack locations of threads.
  - This is displayed in the 'Threads' tab of the process in properties dialog.
  - If you have relocated the pdb files, you can specify the new path of the file through this option.



Configure Symbols

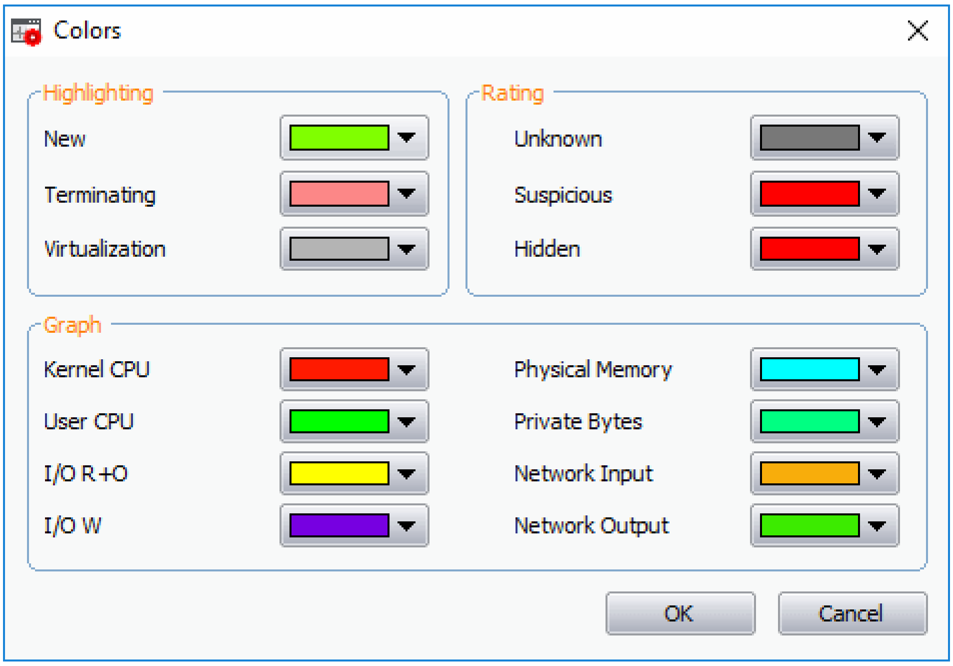
Symbols

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
  - Click 'Tools' > 'Configure Highlighting'
  - KillSwitch color codes processes as follows:
    - **Processes window -** Running, stopped, suspicious or hidden processes
    - **Applications window -** New applications and applications that are closing
    - **Services window -** New services and services that are closing
    - **Network Connections window -** New connections and connections that are closing
    - Graphs (on the right) - Various colors to represent different resources

The highlighting screen lets you change these color to your preferences:



Colors

Highlighting

New	🟩
Terminating	🟥
Virtualization	⬜

Rating

Unknown	⬛
Suspicious	🟥
Hidden	🟥

Graph

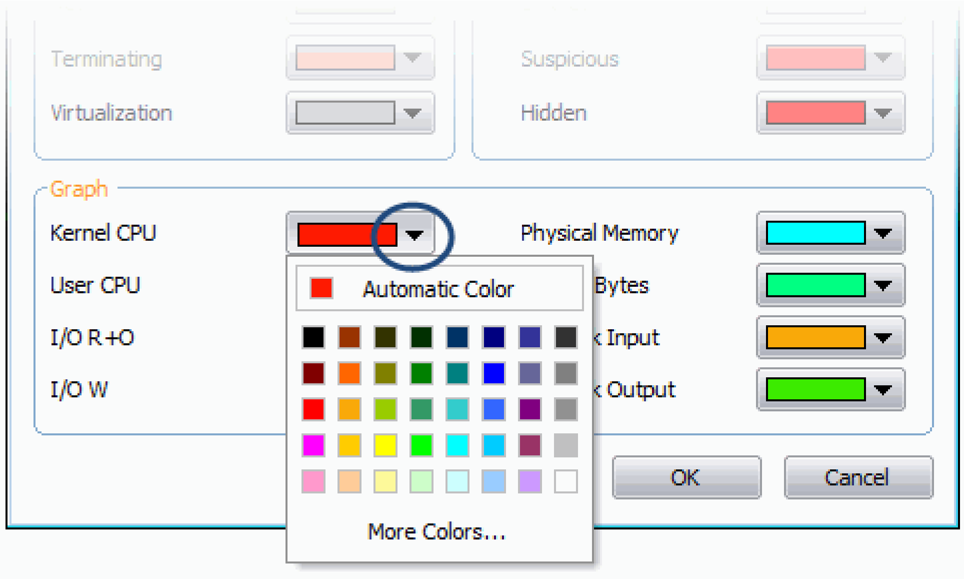
Kernel CPU	🟥	Physical Memory	🟦
User CPU	🟩	Private Bytes	🟩
I/O R+O	🟨	Network Input	🟧
I/O W	🟪	Network Output	🟩

- **Highlighting -** Set the colors you want to use for various process statuses
- **Rating -** Set the colors you want to use for the trust rating of a process
- **Graph -** Select the color of each line on a KillSwitch chart:
  - 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 opens 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'.

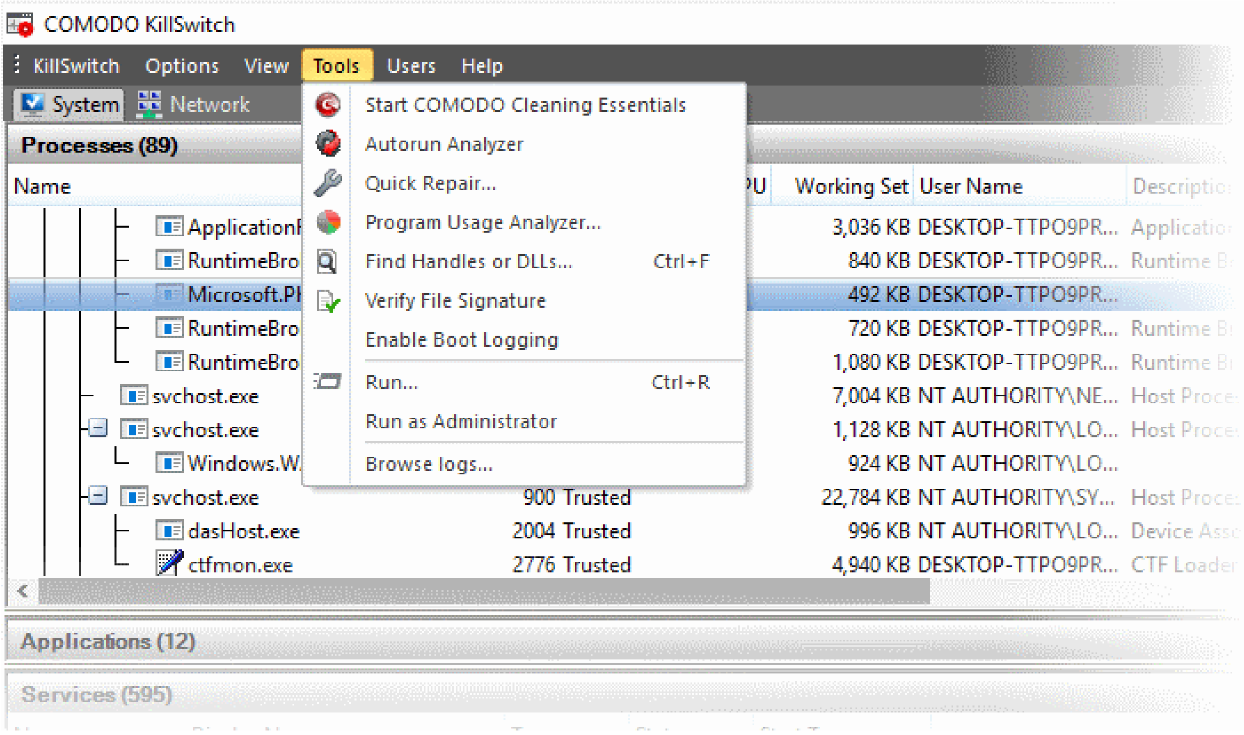
The highlighting and/or graph lines will be displayed with the colors you have chosen.

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

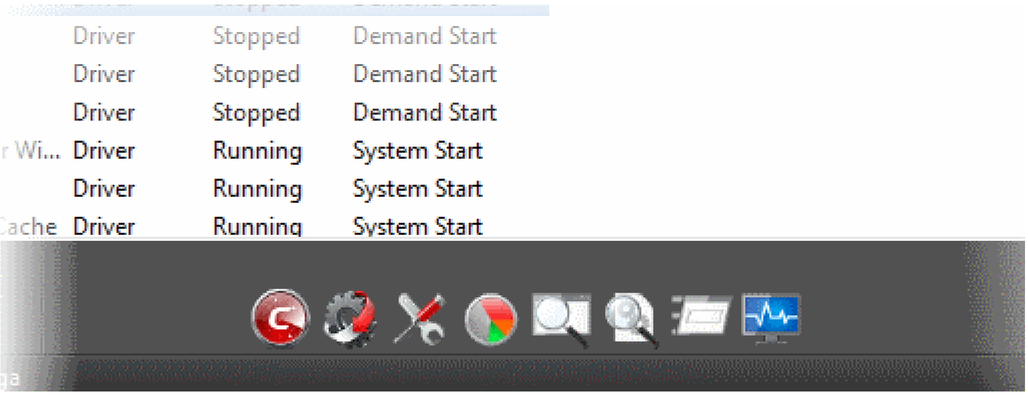
5.6. KillSwitch Tools

- Click 'Tools' in the menu-bar OR click a specific utility in the shortcut-bar under the main display.

KillSwitch utilities let you manage processes, troubleshoot issues, repair settings, and more:



Name			PU	Working Set	User Name	Descriptio
ApplicationF				3,036 KB	DESKTOP-TTPO9PR...	Applicatio
RuntimeBro				840 KB	DESKTOP-TTPO9PR...	Runtime B
Microsoft.Pl				492 KB	DESKTOP-TTPO9PR...	
RuntimeBro				720 KB	DESKTOP-TTPO9PR...	Runtime B
RuntimeBro				1,080 KB	DESKTOP-TTPO9PR...	Runtime B
svchost.exe				7,004 KB	NT AUTHORITY\NE...	Host Proce
svchost.exe				1,128 KB	NT AUTHORITY\LO...	Host Proce
Windows.W				924 KB	NT AUTHORITY\LO...	
svchost.exe	900	Trusted		22,784 KB	NT AUTHORITY\SY...	Host Proce
dasHost.exe	2004	Trusted		996 KB	NT AUTHORITY\LO...	Device Ass
ctfmon.exe	2776	Trusted		4,940 KB	DESKTOP-TTPO9PR...	CTF Loader



	Driver	Stopped	Demand Start
	Driver	Stopped	Demand Start
	Driver	Stopped	Demand Start
r Wi...	Driver	Running	System Start
	Driver	Running	System Start
Cache	Driver	Running	System Start

Icon	Description
	Scan menu - Run full, custom or smart malware scans on your system. See **Scan Your System** for more details.
	Autorun Analyzer - View and handle services that were loaded when your system boots-up.
	Quick Repair - Troubleshoot and fix important windows settings and features. See **Repair Windows Settings and Features** for more details.

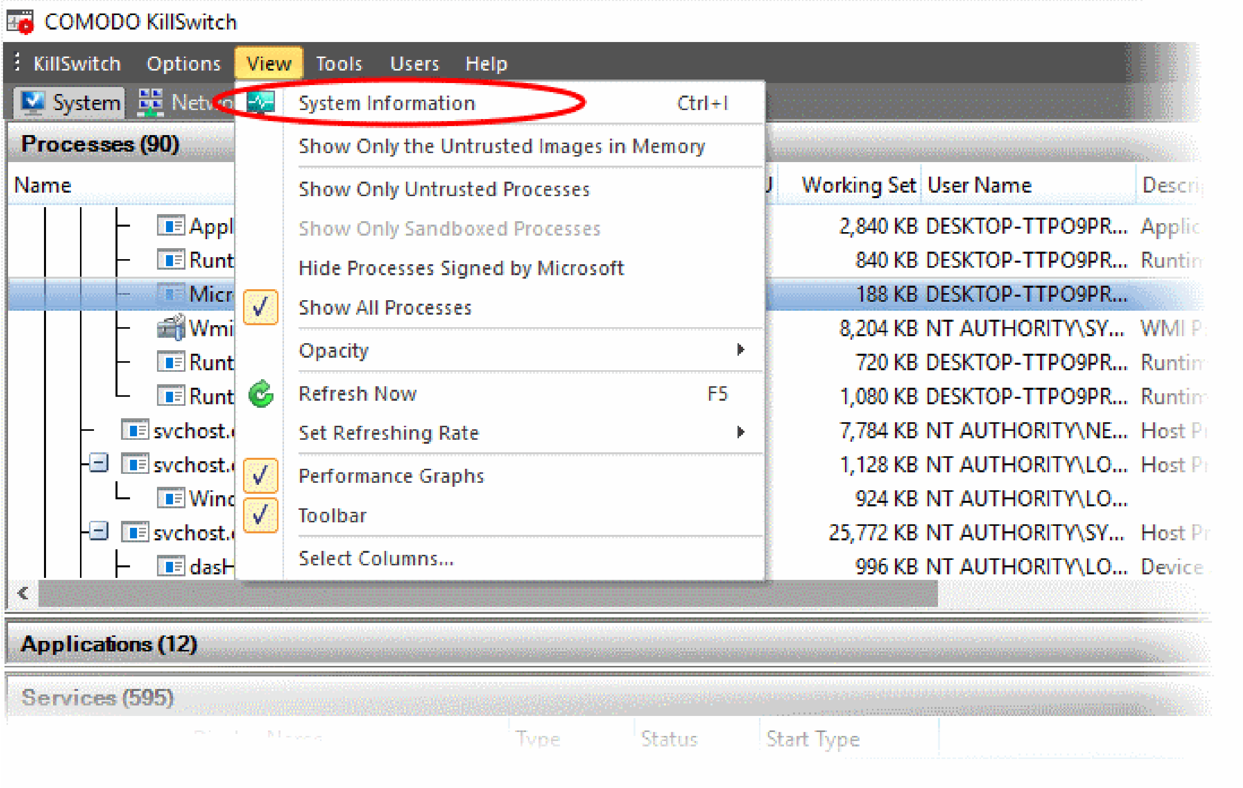
	Program Usage Analyzer - Shows a history of all programs used on your computer by all users. See **Analyze Program Usage** for more details.
	Find Window utility - Find processes related to the active application. See **Find Process of the Active Window** for more details.
	Search for handles and DLL's - Enter the name of the object. See **Search for Handles or DLLs** for more details.
	Windows 'Run' dialog - Open programs from the command line interface. See **Run Programs from Command Line Interface** for more details.
	Windows system information - Shows charts and stats about the usage/history of your system resources. See '**View System Information**' for more details.

Click the links below for detailed explanations on KillSwitch Utilities:

- **View System Information**
- **Repair Windows Settings and Features**
- **Analyze Program Usage**
- **Search for Handles or DLLs**
- **Verify authenticity of Applications**
- **Enable Boot Logging**
- **Run a Command Line Interface program**
- **Run a Command Line Interface program as Administrator**
- **Browse KillSwitch Logs**

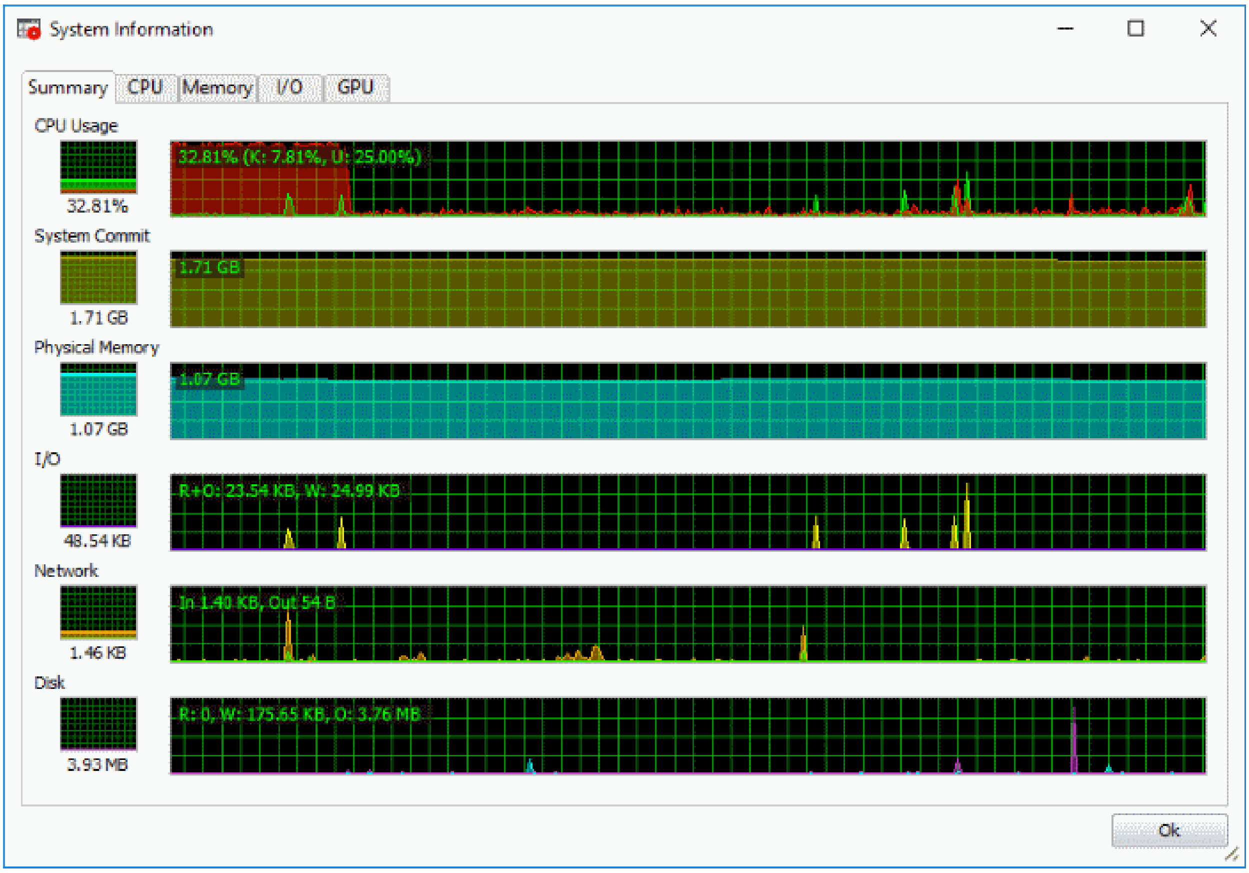
5.6.1. View System Information

- The system information pane shows the dynamic graphical representations of your CPU usage, I/O activity and physical memory usage of your system.
- It also shows the detailed statistics on current utilization of various system resources.
- Click 'View' > 'System Information', to view the system information pane.


COMODO KillSwitch
KillSwitch
Options
View
Tools
Users
Help
System
Network
System Information Ctrl+I
Show Only the Untrusted Images in Memory
Show Only Untrusted Processes
Show Only Sandboxed Processes
Hide Processes Signed by Microsoft
✓ Show All Processes
Opacity
Refresh Now F5
Set Refreshing Rate
✓ Performance Graphs
✓ Toolbar
Select Columns...
Processes (90)
Name
Working Set
User Name
Descri
Appl
Runt
Micr
Wmi
Runt
Runt
svchost.
svchost.
Winc
svchost.
dasH
2,840 KB DESKTOP-TTPO9PR... Applic
840 KB DESKTOP-TTPO9PR... Runtin
188 KB DESKTOP-TTPO9PR...
8,204 KB NT AUTHORITY\SY... WMI P
720 KB DESKTOP-TTPO9PR... Runtin
1,080 KB DESKTOP-TTPO9PR... Runtin
7,784 KB NT AUTHORITY\NE... Host P
1,128 KB NT AUTHORITY\LO... Host P
924 KB NT AUTHORITY\LO...
25,772 KB NT AUTHORITY\SY... Host P
996 KB NT AUTHORITY\LO... Device
Applications (12)
Services (595)
Type
Status
Start Type

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

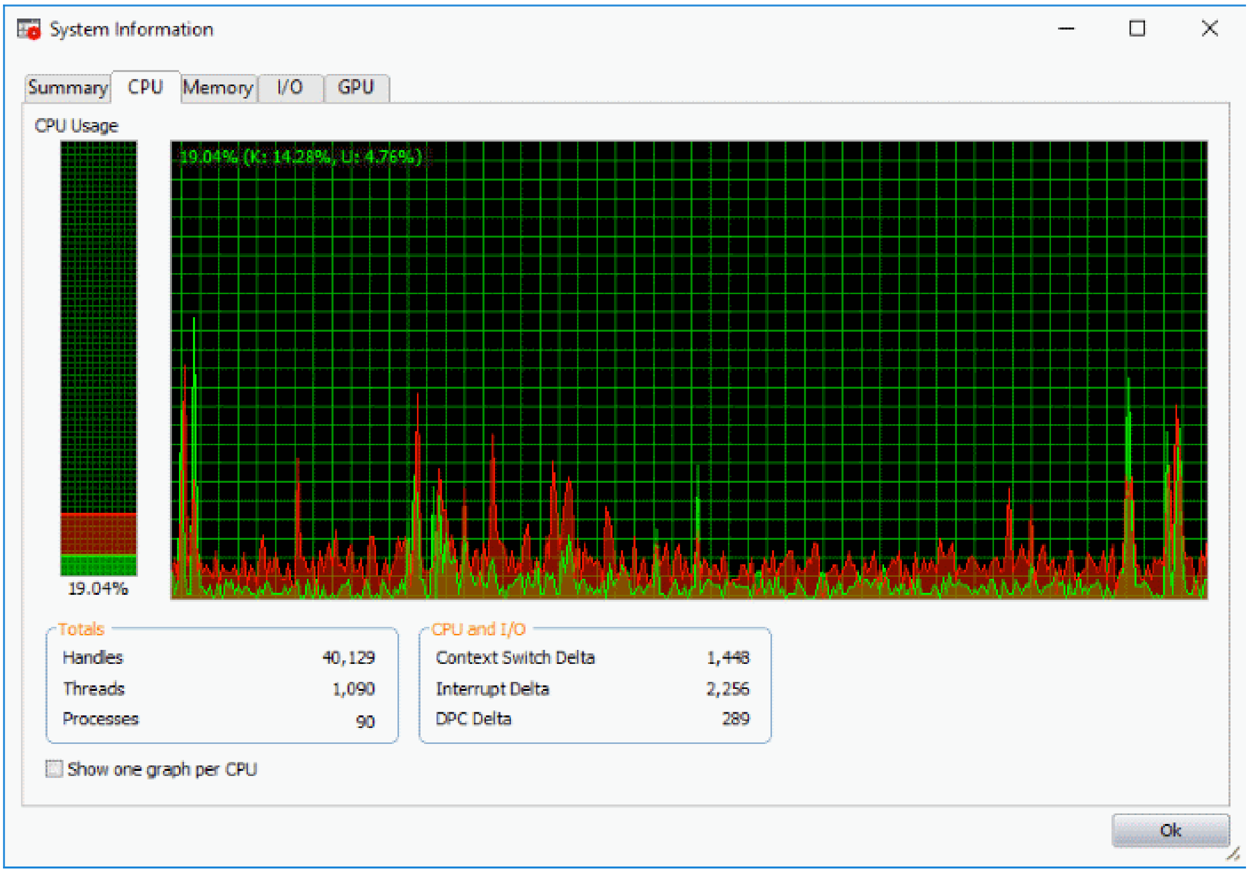
The system Information dialog opens at the 'Summary' tab:



The 'Summary' tab:

- **CPU** - Shows a dynamic graphical representation of the usage of CPU over time. In multiprocessor operating system, you can make the pane display individual graph for each CPU by selecting the otption 'Show one graph per CPU' at the bottom left of the interface.
- **System Commit** - Shows a dynamic graphical representation of performance system commit.
- **Physical Memory** - Shows a dynamic graphical representation of the usage of physical system memory over time.
- **I/O** - Shows a dynamic graphical representation of Input/Output activities of the computer over time.
- **Network** - Shows a dynamic graphical representation of how much network traffic is used over time by services and applications running on your computer.
- **Disk** - Shows a dynamic graphical representation of disk usage.

The 'CPU' tab:



Totals

Handles	40,129
Threads	1,090
Processes	90

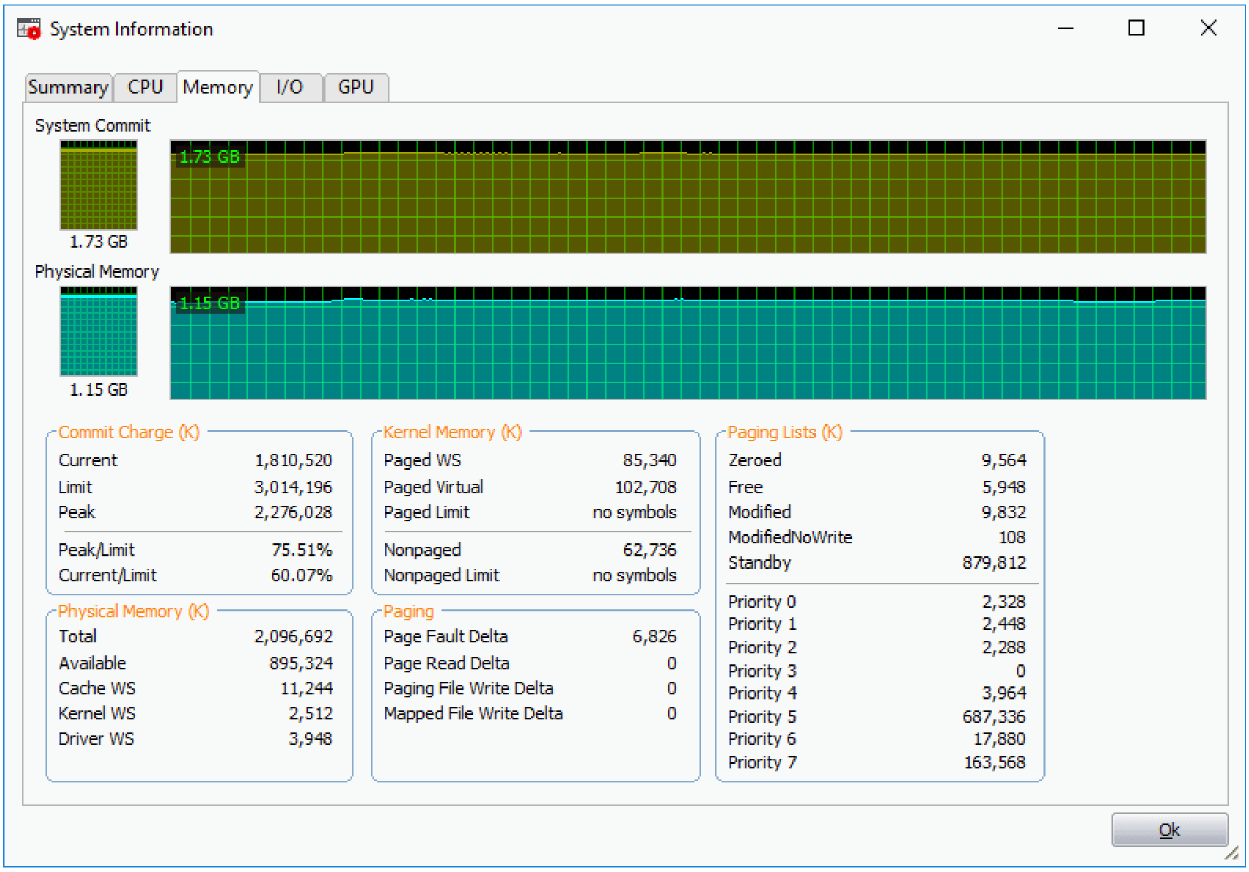
CPU and I/O

Context Switch Delta	1,448
Interrupt Delta	2,256
DPC Delta	289

□ Show one graph per CPU

- **Totals -** Shows detailed statistics on the number of processes, threads and handles that run on the computer.
- **CPU and I/O -** Shows a statistical report on the CPU activities and Input/Output activities of your computer.
- **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.

The 'Memory' tab:



Commit Charge (K)

Current	1,810,520
Limit	3,014,196
Peak	2,276,028
Peak/Limit	75.51%
Current/Limit	60.07%

Physical Memory (K)

Total	2,096,692
Available	895,324
Cache WS	11,244
Kernel WS	2,512
Driver WS	3,948

Kernel Memory (K)

Paged WS	85,340
Paged Virtual	102,708
Paged Limit	no symbols
Nonpaged	62,736
Nonpaged Limit	no symbols

Paging

Page Fault Delta	6,826
Page Read Delta	0
Paging File Write Delta	0
Mapped File Write Delta	0

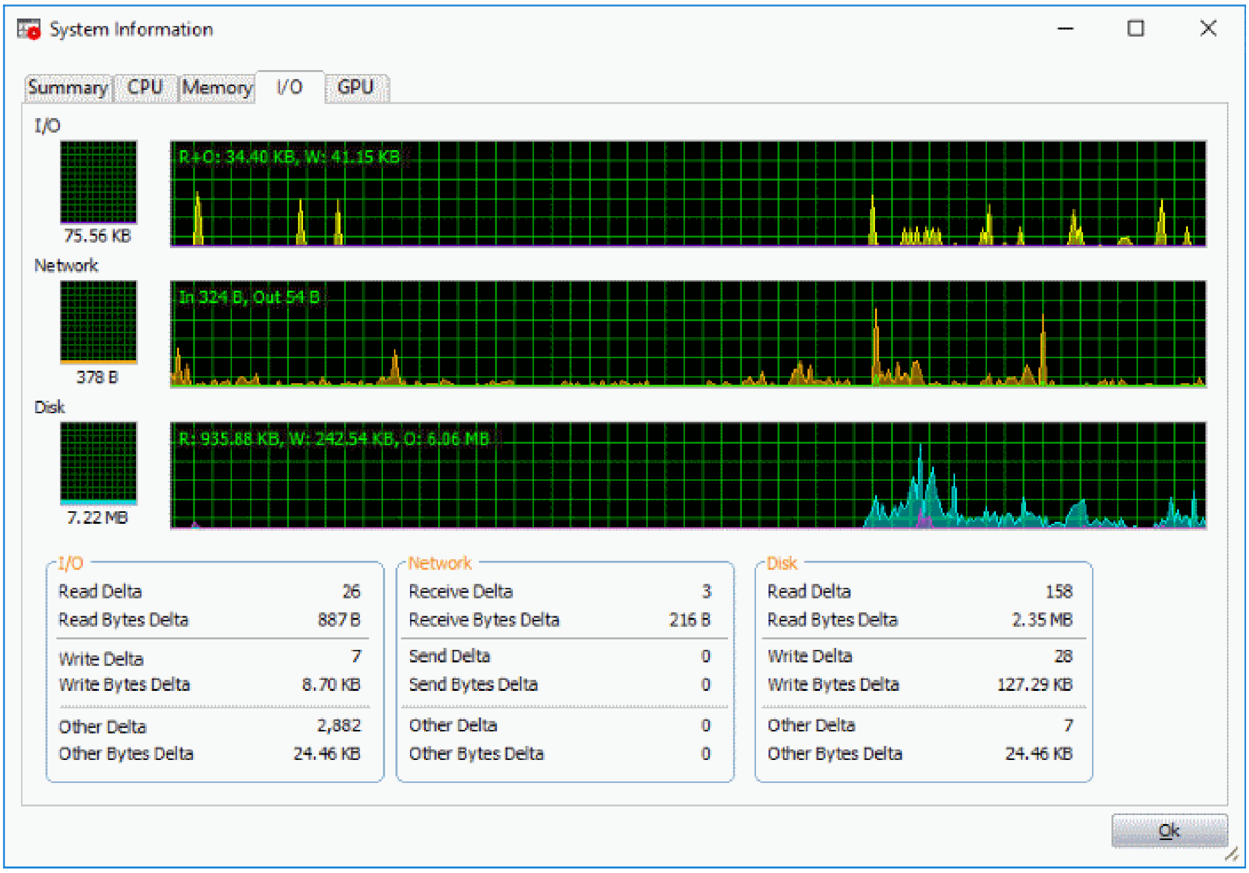
Paging Lists (K)

Zeroed	9,564
Free	5,948
Modified	9,832
ModifiedNoWrite	108
Standby	879,812
Priority 0	2,328
Priority 1	2,448
Priority 2	2,288
Priority 3	0
Priority 4	3,964
Priority 5	687,336
Priority 6	17,880
Priority 7	163,568

- **Commit Charge** - Shows 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 peak value listed may exceed the maximum physical memory.
  - Current - Shows the current amount of the system commit charge
  - Limit - Indicates the amount of physical memory and size of all paging files combined. This is the maximum total memory size which the system is allocated
  - Peak - Displays the maximum amount of the system commit charge since the last reboot the operating system
  - Peak/Limit - The percentage the peak of the system charge comparing to the system commit limit since the last reboot
  - Current/Limit - The percentage of the current value of the system commit charge comparing to the current value of the system commit limit
- **Physical Memory** - Shows 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 - Shows the current kernel-mode time usage.
  - Driver - Shows the kernel-mode drivers that are in currently enabled on the system.
- **Kernel Memory** - Shows a statistical report on memory used by the operating system kernel and device drivers in KB.
  - Paged Virtual - Memory that can be copied to the paging file from virtual memory.

  - Paged Physical - Memory that can be copied to the paging file from physical memory, thereby freeing the physical memory. Operating system uses physical memory.
  - Nonpaged - Memory that remains resident in physical memory and are not copied to the paging file.
  - Nonpages limit - The current maximum memory that remains and are not copied 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.
- **Paging Limits** - The current maximum of page fault mapped in the virtual memory but not loaded in the physical memory in KB.

The 'I/O' tab:



I/O

Read Delta	26
Read Bytes Delta	887 B
Write Delta	7
Write Bytes Delta	8.70 KB
Other Delta	2,882
Other Bytes Delta	24.46 KB

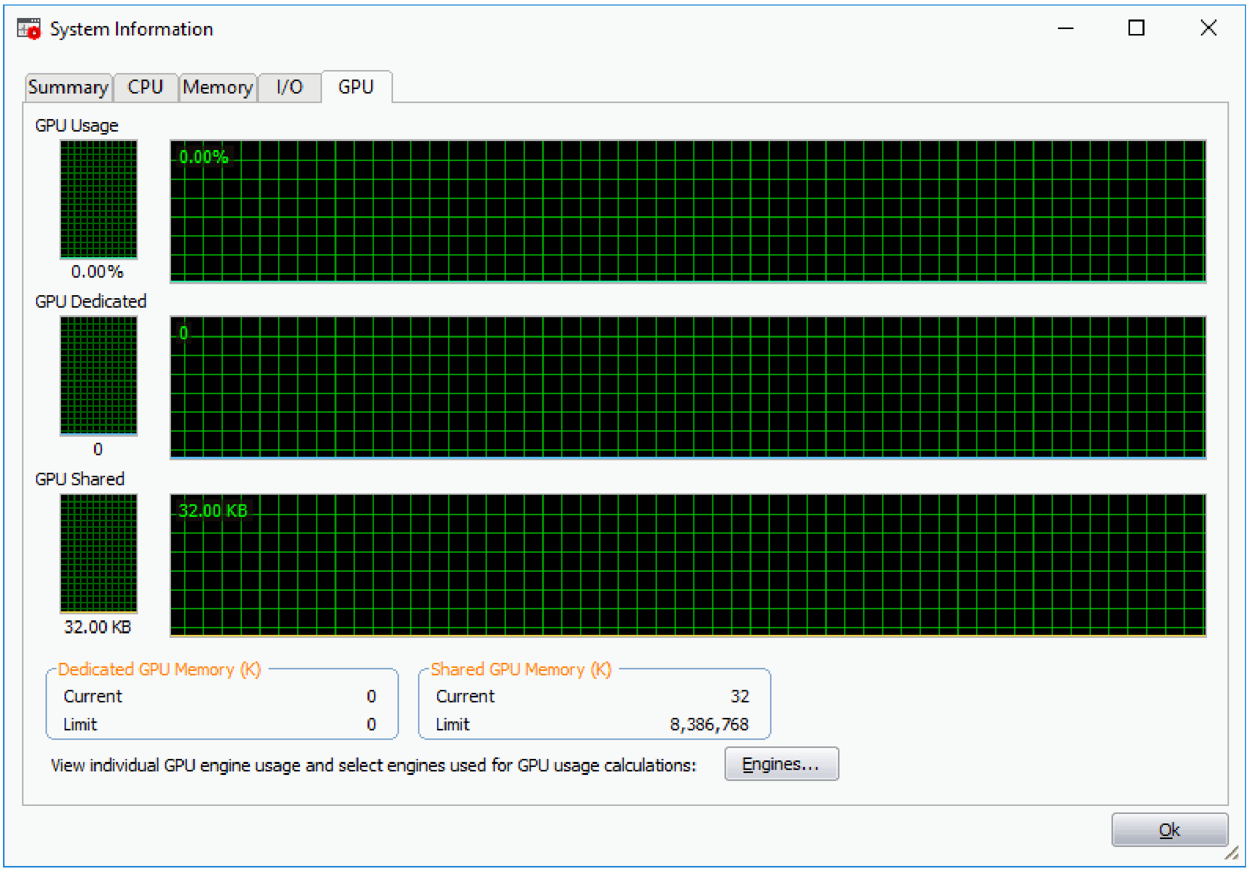
Network

Receive Delta	3
Receive Bytes Delta	216 B
Send Delta	0
Send Bytes Delta	0
Other Delta	0
Other Bytes Delta	0

Disk

Read Delta	158
Read Bytes Delta	2.35 MB
Write Delta	28
Write Bytes Delta	127.29 KB
Other Delta	7
Other Bytes Delta	24.46 KB

- **I/O** - Shows the amount of I/O operations generated by a process in KB (including files, network, and device I/Os)
- **Network** - Shows the amount of network input/output operations generated by a process in KB
- **Disk** - Shows the amount of disk input/output operations generated by a process in KB



Dedicated GPU Memory (K)

Current	0
Limit	0

Shared GPU Memory (K)

Current	32
Limit	8,386,768

View individual GPU engine usage and select engines used for GPU usage calculations:

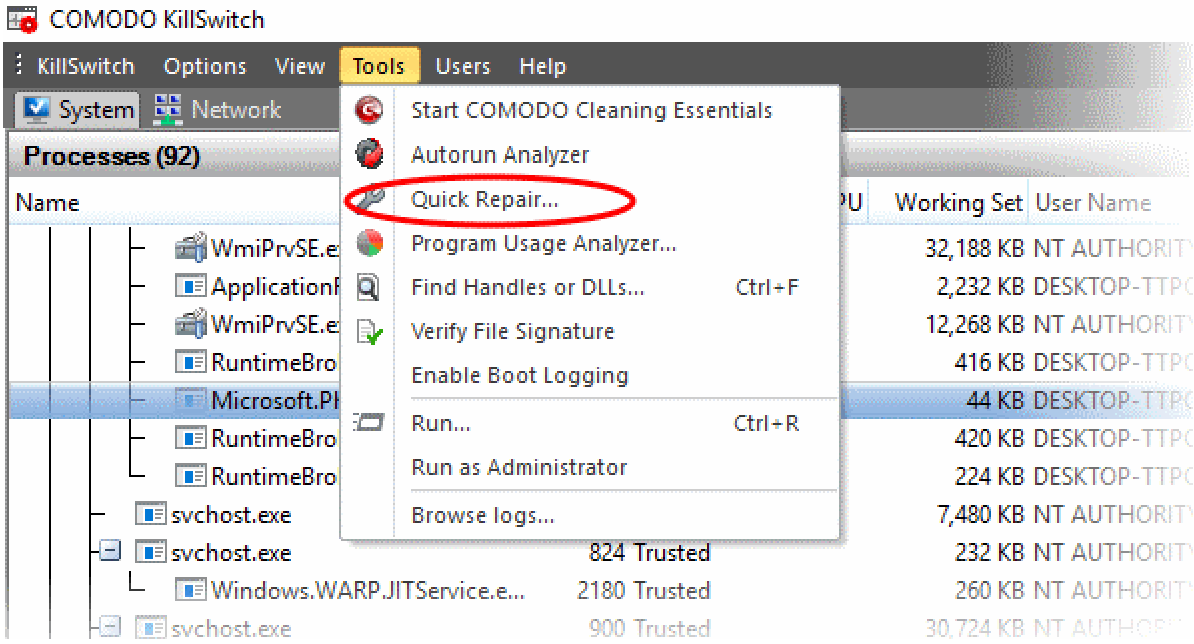
- **Dedicated GPU Memory (K) -** The exclusive source of video memory leaving the RAM of your system untouched.
- **Shared GPU Memory (K) -** This memory division is shared by RAM of your system and does not have an independent memory

5.6.2. Repair Windows Settings and Features

- KillSwitch lets you 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 does not work, 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.

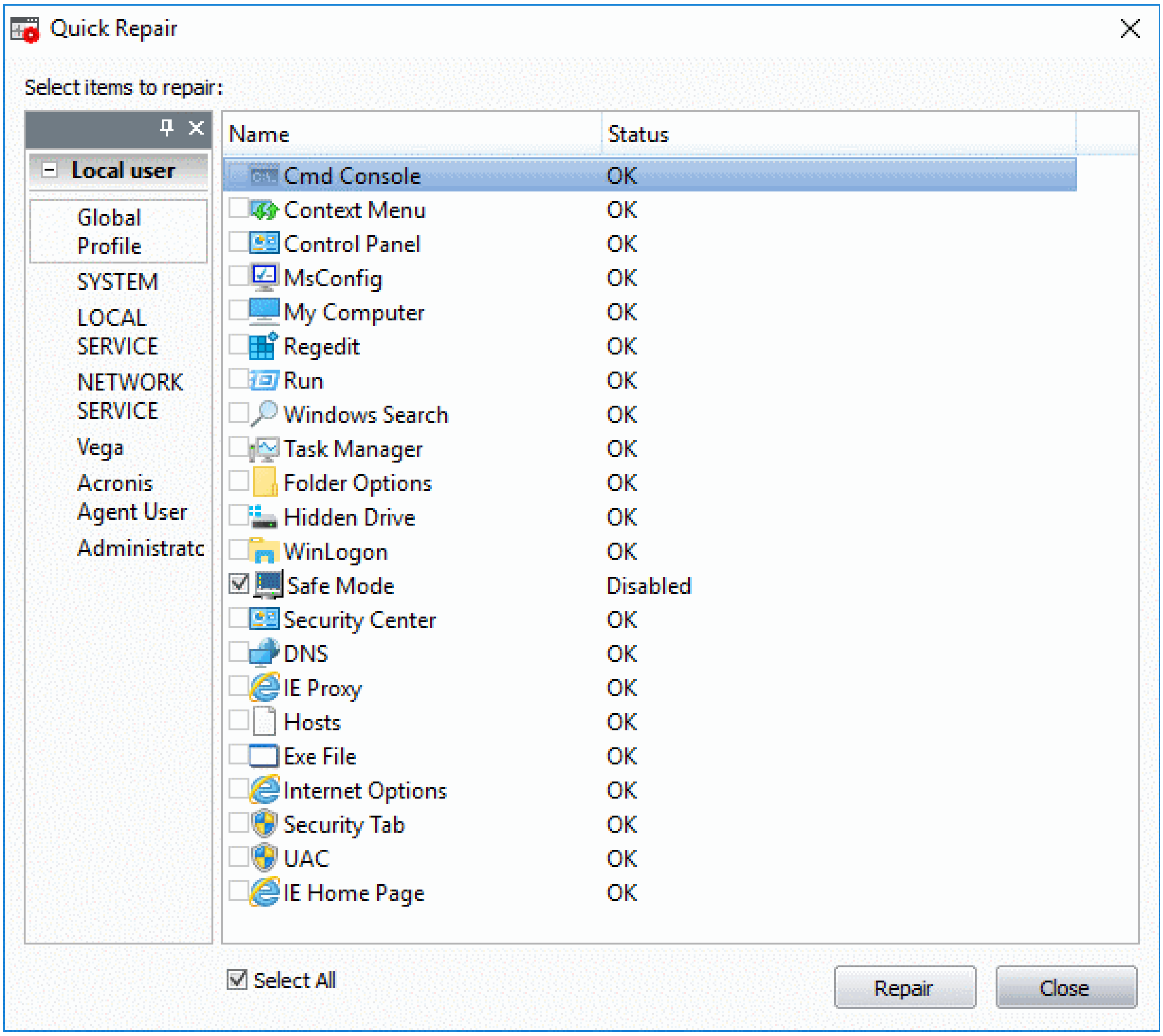
To repair the Windows settings and features

1. Click 'Quick Repair...'. from the 'Tools' menu



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

The 'Quick Repair' dialog lists set of features that can be repaired and their current status.



Select items to repair:

- Local user
- Global Profile
- SYSTEM
- LOCAL SERVICE
- NETWORK SERVICE
- Vega
- Acronis Agent User
- Administratc

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

☑ Select All

You can change the profile from the left hand side pane so as to switch the display of the statuses of features are 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 are active only for the items that require fixing. If you want to select all the items that need fixing, check 'Select All'.

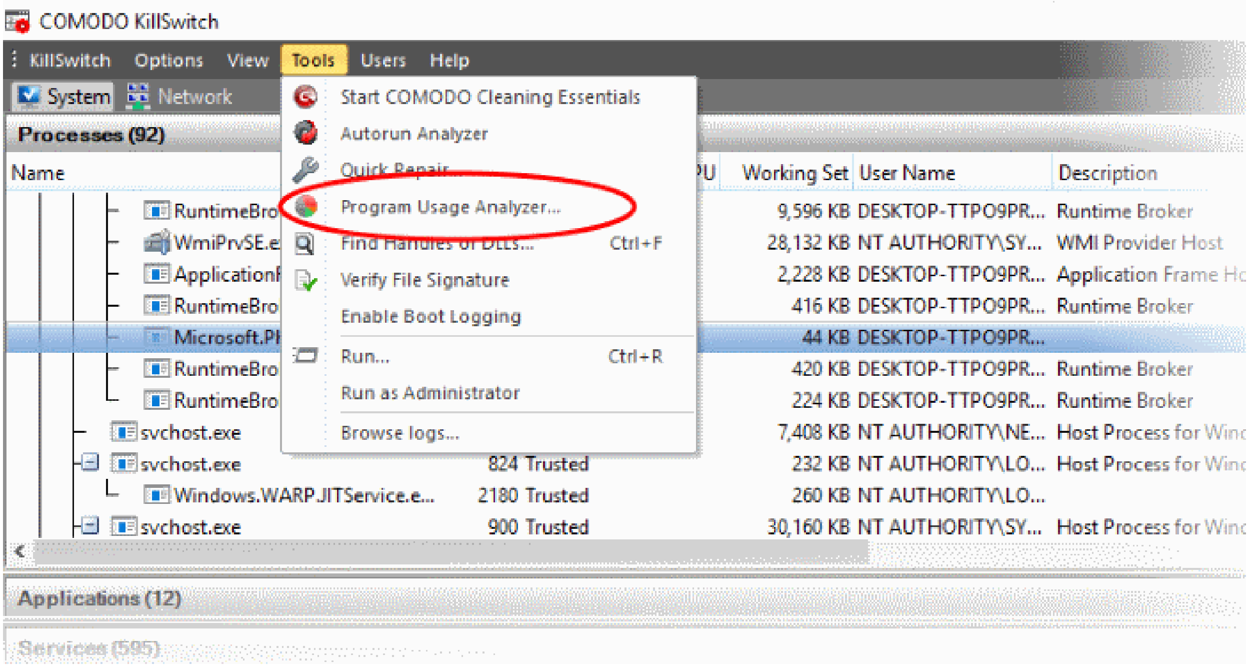
3. Click 'Repair'. KillSwitch will automatically fix the errors in the settings of the selected item. A completion dialog will appear.

5.6.3. Analyze Program Usage

- The usage analyzer shows useful information about programs that are running, or have run on your computer.

Open the Program Usage Analyzer

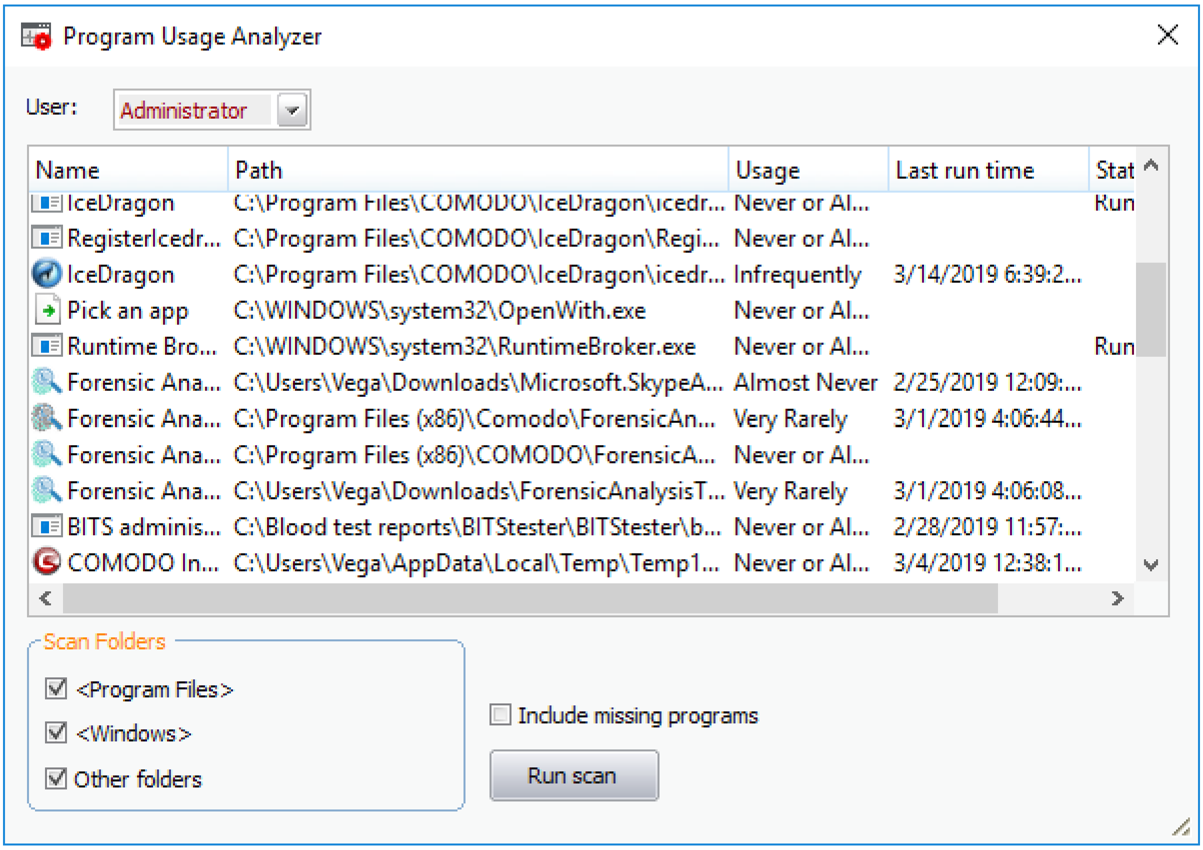
- Click 'Tools' > 'Program Usage Analyzer':



Name			Working Set	User Name	Description
RuntimeBro			9,596 KB	DESKTOP-TTPO9PR...	Runtime Broker
WmiPrvSE.e			28,132 KB	NT AUTHORITY\SY...	WMI Provider Host
ApplicationF			2,228 KB	DESKTOP-TTPO9PR...	Application Frame Hc
RuntimeBro			416 KB	DESKTOP-TTPO9PR...	Runtime Broker
Microsoft.Pl			44 KB	DESKTOP-TTPO9PR...	
RuntimeBro			420 KB	DESKTOP-TTPO9PR...	Runtime Broker
RuntimeBro			224 KB	DESKTOP-TTPO9PR...	Runtime Broker
svchost.exe			7,408 KB	NT AUTHORITY\NE...	Host Process for Winc
svchost.exe	824	Trusted	232 KB	NT AUTHORITY\LO...	Host Process for Winc
Windows.WARP.JITService.e...	2180	Trusted	260 KB	NT AUTHORITY\LO...	
svchost.exe	900	Trusted	30,160 KB	NT AUTHORITY\SY...	Host Process for Winc

- Alternatively, click the program usage icon in the tool bar.

The usage analyzer shows all programs installed by, or available to, the currently logged-in user:



Program Usage Analyzer

User: Administrator

Name	Path	Usage	Last run time	Stat
IceDragon	C:\Program Files\COMODO\IceDragon\icedr...	Never or Al...		Run
Registerlcedr...	C:\Program Files\COMODO\IceDragon\Regi...	Never or Al...		
IceDragon	C:\Program Files\COMODO\IceDragon\icedr...	Infrequently	3/14/2019 6:39:2...	
Pick an app	C:\WINDOWS\system32\OpenWith.exe	Never or Al...		
Runtime Bro...	C:\WINDOWS\system32\RuntimeBroker.exe	Never or Al...		Run
Forensic Ana...	C:\Users\Vega\Downloads\Microsoft.SkypeA...	Almost Never	2/25/2019 12:09:...	
Forensic Ana...	C:\Program Files (x86)\Comodo\ForensicAn...	Very Rarely	3/1/2019 4:06:44...	
Forensic Ana...	C:\Program Files (x86)\COMODO\ForensicA...	Never or Al...		
Forensic Ana...	C:\Users\Vega\Downloads\ForensicAnalysisT...	Very Rarely	3/1/2019 4:06:08...	
BITS adminis...	C:\Blood test reports\BITStester\BITStester\b...	Never or Al...	2/28/2019 11:57:...	
COMODO In...	C:\Users\Vega\AppData\Local\Temp\Temp1...	Never or Al...	3/4/2019 12:38:1...	

Scan Folders

☑ <Program Files>

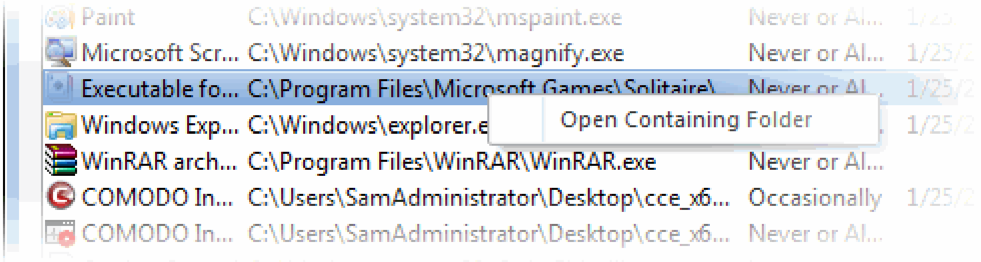
☑ <Windows>

☑ Other folders

☐ Include missing programs

Program Usage Analyzer - Descriptions of Columns	
Column	**Description**
Name	The title of the program/application. Click the column header to sort entries in alphabetical order
Path	The location of the program's installation folder.
Usage	How often the program is run by the user.
Last Run Time	Date and time the program was most recently executed.
Status	The current runtime status of the program.

- User - Choose which user's programs are shown.
- Scan Folders - Choose the folders from which the list of programs is drawn.
- Include missing programs + 'Run Scan' - Finds programs and Windows components which were uninstalled from the computer.
- Right-click on an entry to open the installation folder of the program and access the process invoked by the program.



Paint	C:\Windows\system32\mspaint.exe	Never or Al...	1/25
Microsoft Scr...	C:\Windows\system32\magnify.exe	Never or Al...	1/25/2
Executable fo...	C:\Program Files\Microsoft Games\Solitaire\	Never or Al...	1/25/2
Windows Exp...	C:\Windows\explorer.e		1/25/2
WinRAR arch...	C:\Program Files\WinRAR\WinRAR.exe	Never or Al...	
COMODO In...	C:\Users\SamAdministrator\Desktop\cce_x6...	Occasionally	1/25/2
COMODO In...	C:\Users\SamAdministrator\Desktop\cce_x6...	Never or Al...	

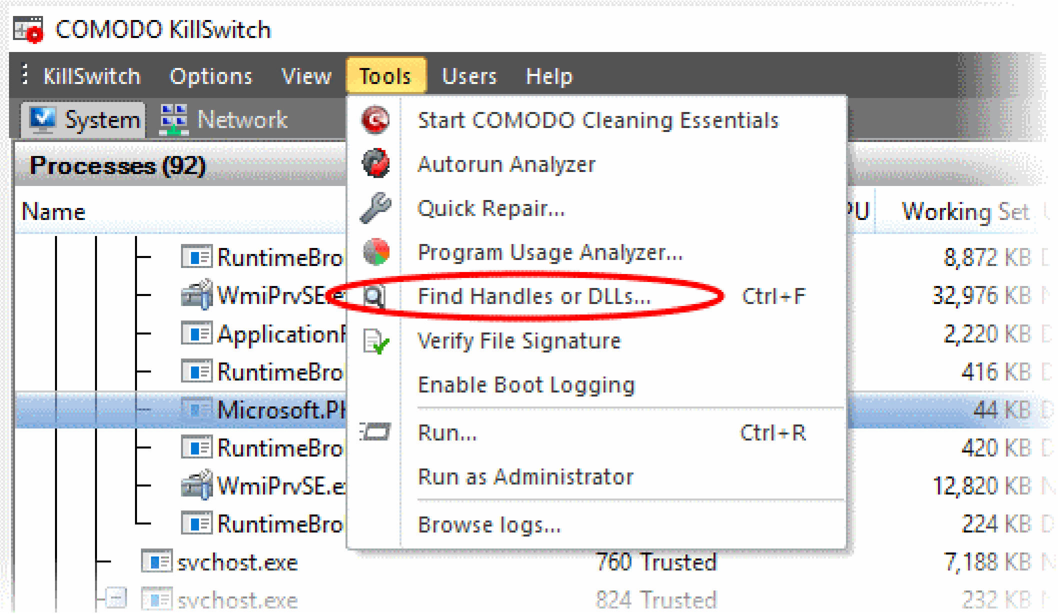
- Open Containing Folder - Opens the installation folder of the program in Windows Explorer.

5.6.4. Search 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.

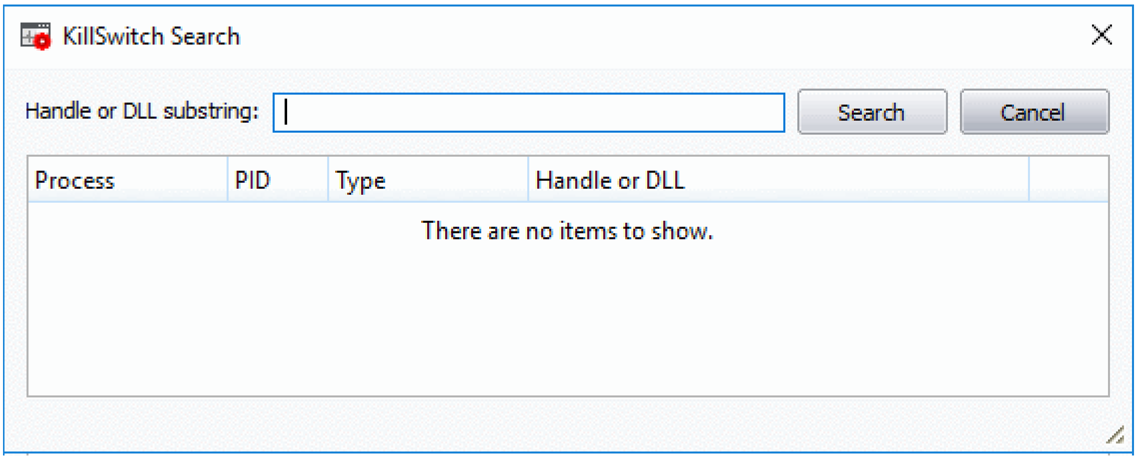
To search for a specific handles, DLLs and mapped files

- Click 'Tools' > 'Find Handles or DLLs'



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

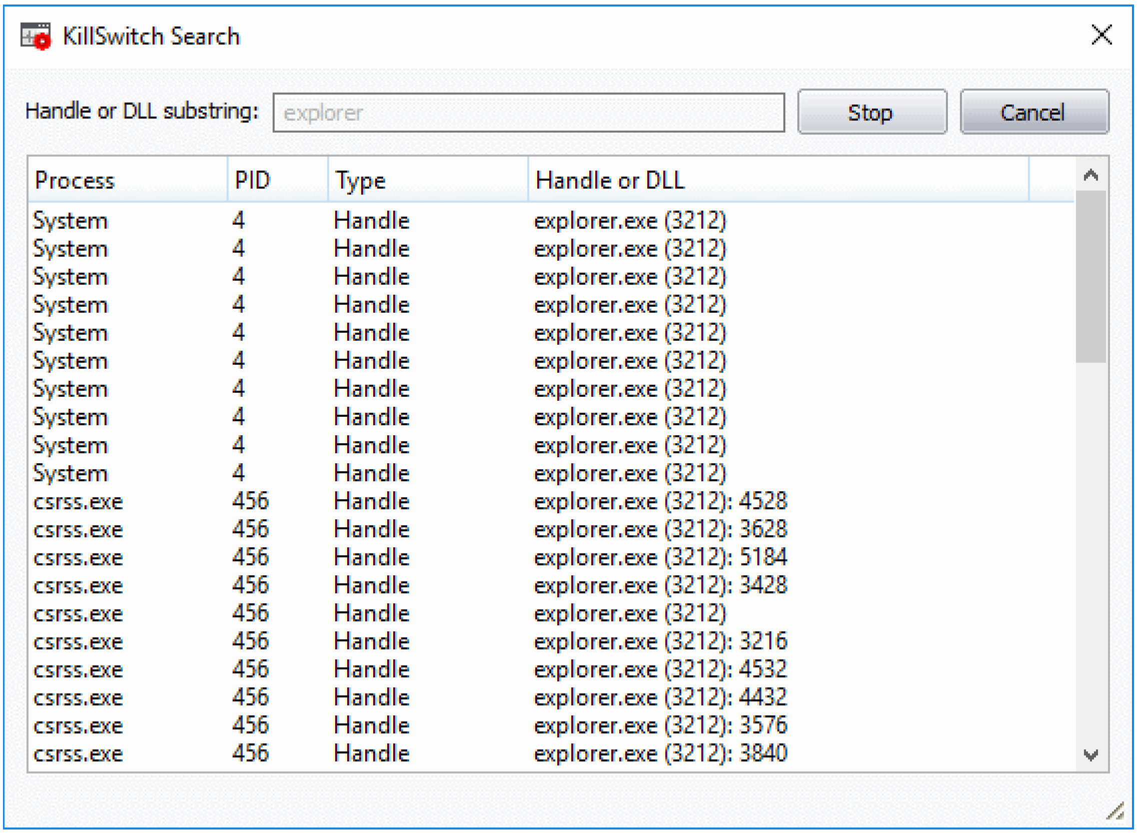
The 'Find Handles or DLLs' dialog will open:



There are no items to show.

- 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
System	4	Handle	explorer.exe (3212)
System	4	Handle	explorer.exe (3212)
System	4	Handle	explorer.exe (3212)
System	4	Handle	explorer.exe (3212)
System	4	Handle	explorer.exe (3212)
System	4	Handle	explorer.exe (3212)
System	4	Handle	explorer.exe (3212)
System	4	Handle	explorer.exe (3212)
System	4	Handle	explorer.exe (3212)
System	4	Handle	explorer.exe (3212)
csrss.exe	456	Handle	explorer.exe (3212): 4528
csrss.exe	456	Handle	explorer.exe (3212): 3628
csrss.exe	456	Handle	explorer.exe (3212): 5184
csrss.exe	456	Handle	explorer.exe (3212): 3428
csrss.exe	456	Handle	explorer.exe (3212)
csrss.exe	456	Handle	explorer.exe (3212): 3216
csrss.exe	456	Handle	explorer.exe (3212): 4532
csrss.exe	456	Handle	explorer.exe (3212): 4432
csrss.exe	456	Handle	explorer.exe (3212): 3576
csrss.exe	456	Handle	explorer.exe (3212): 3840

Handle or DLL search results window - Descriptions of Columns	
Column	**Description**
Process	The title of the activity 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 activity. Clicking the column header sorts the entries in numerical order of the PIDs.

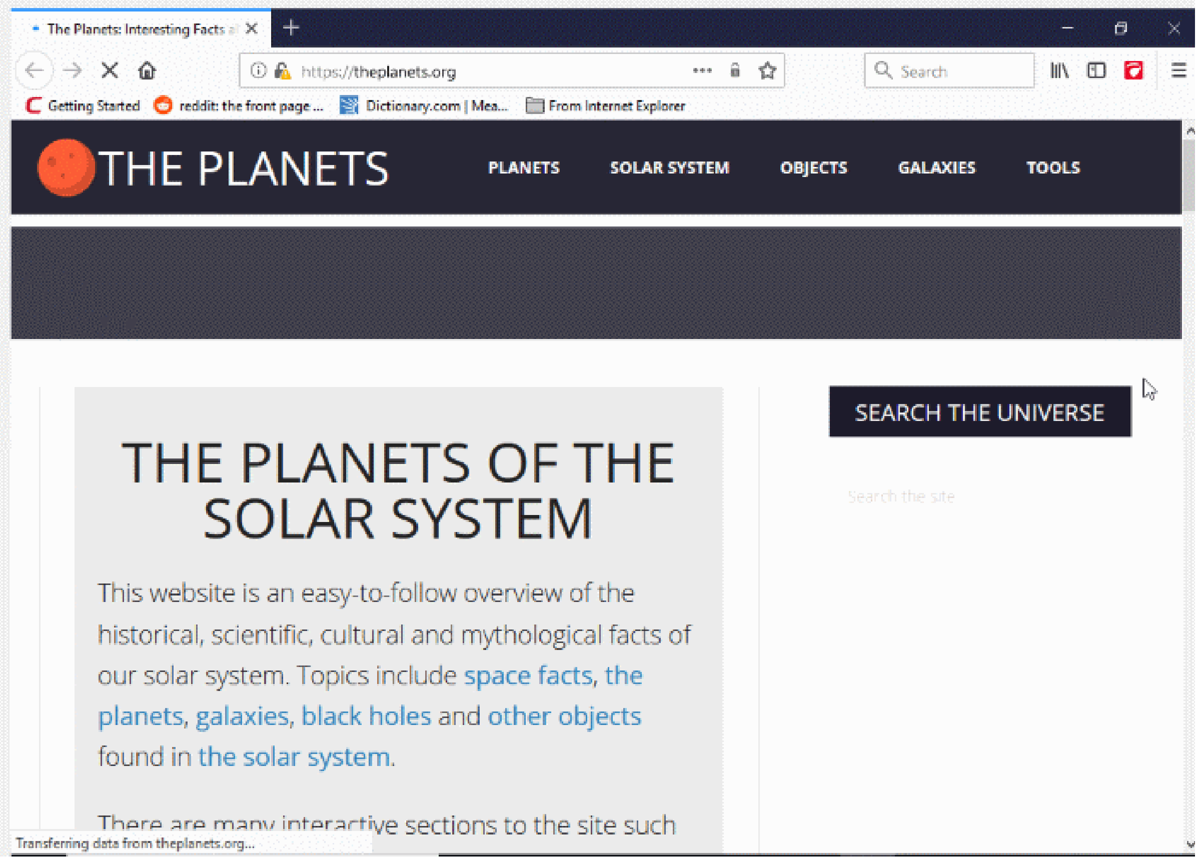
Type	Whether the process is triggered by Handle or DLL.
Handle or DLL	The executable file that has triggered the process along with its storage location.

5.6.5. Verify Authenticity of Applications

A program is considered safe to run if it is digitally signed by a 'Trusted Software publisher'. To prove their software is the genuine article, publishers digitally sign their software using a code signing certificate. If you would like to know more about this process, see **Background details** later in this section.

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

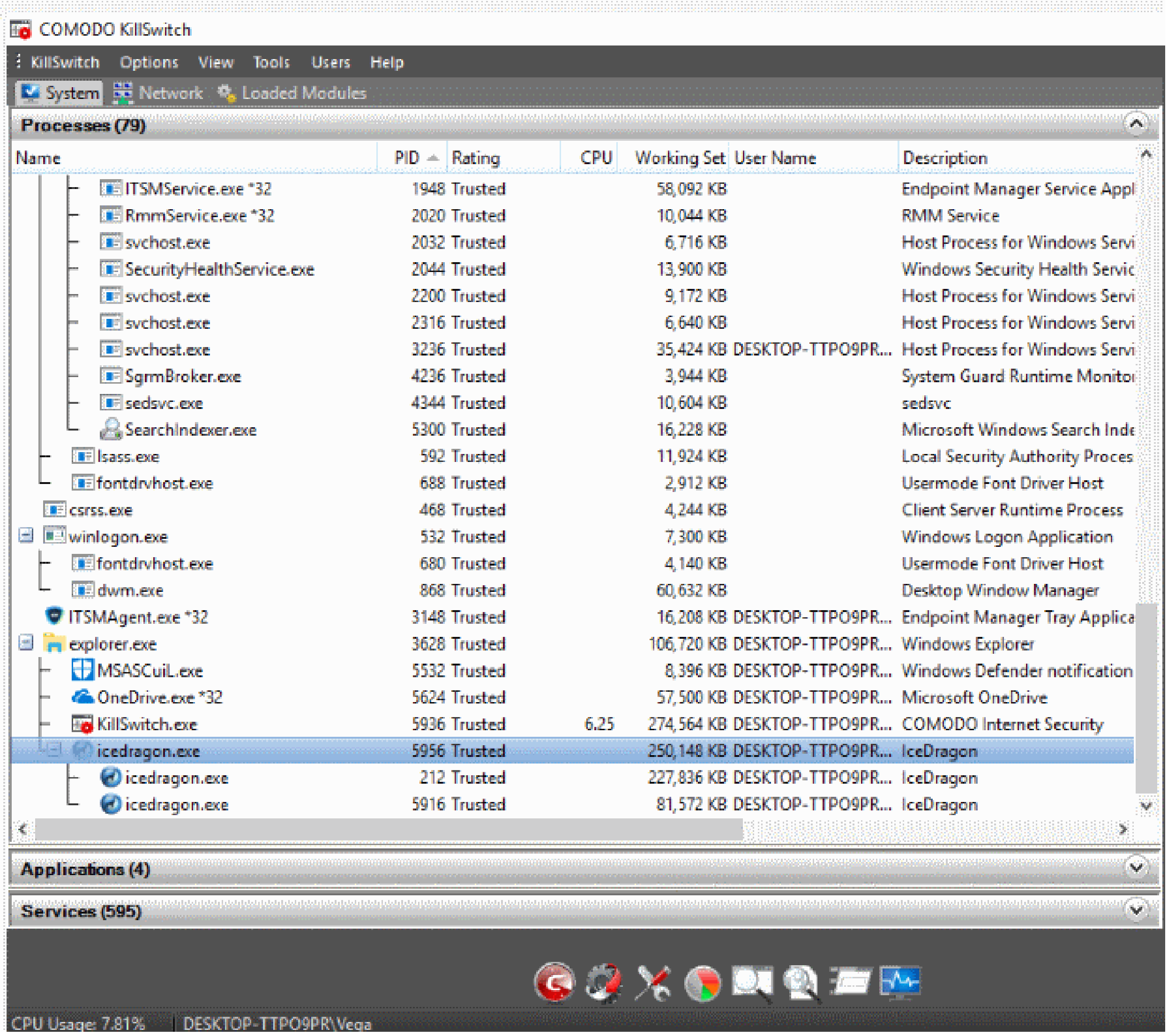
- Select a process in the KillSwitch process list
- Click 'Tools' > 'Verify File Signature'



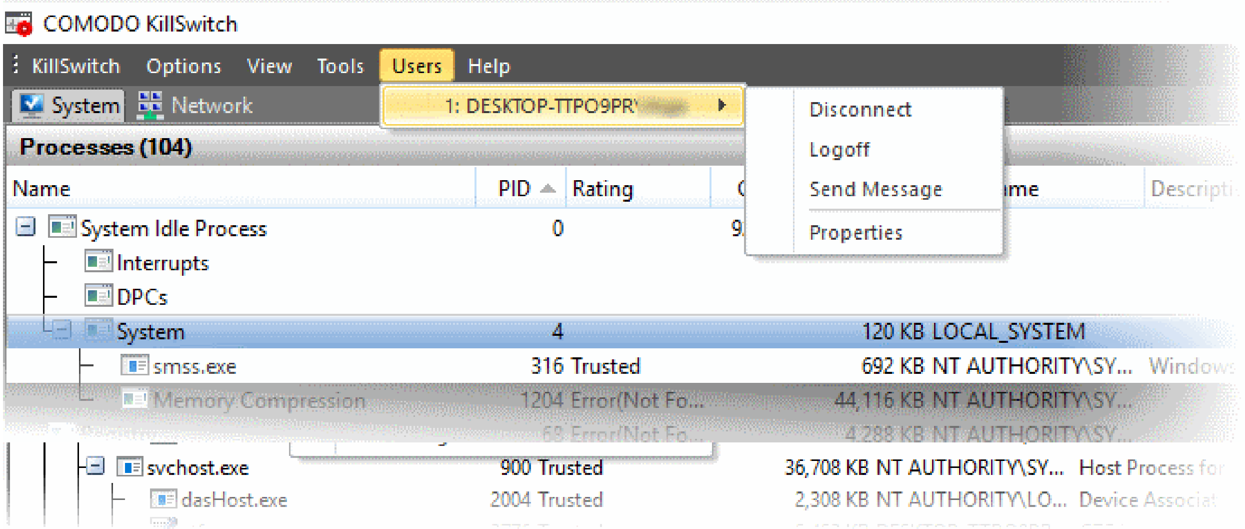
THE PLANETS OF THE SOLAR SYSTEM

This website is an easy-to-follow overview of the historical, scientific, cultural and mythological facts of our solar system. Topics include space facts, the planets, galaxies, black holes and other objects found in the solar system.

There are many interactive sections to the site such

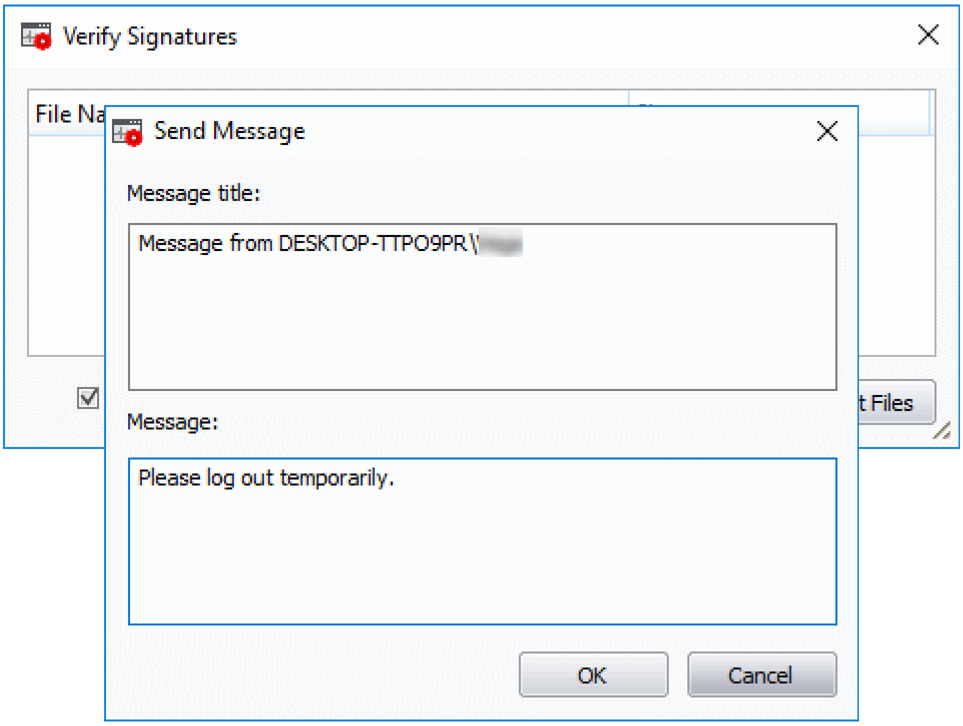


Name	PID	Rating	CPU	Working Set	User Name	Description
ITSMService.exe *32	1948	Trusted		58,092 KB		Endpoint Manager Service Appl
RmmService.exe *32	2020	Trusted		10,044 KB		RMM Service
svchost.exe	2032	Trusted		6,716 KB		Host Process for Windows Servi
SecurityHealthService.exe	2044	Trusted		13,900 KB		Windows Security Health Servic
svchost.exe	2200	Trusted		9,172 KB		Host Process for Windows Servi
svchost.exe	2316	Trusted		6,640 KB		Host Process for Windows Servi
svchost.exe	3236	Trusted		35,424 KB	DESKTOP-TTPO9PR...	Host Process for Windows Servi
SgrmBroker.exe	4236	Trusted		3,944 KB		System Guard Runtime Monitor
sedsvc.exe	4344	Trusted		10,604 KB		sedsvc
SearchIndexer.exe	5300	Trusted		16,228 KB		Microsoft Windows Search Inde
lsass.exe	592	Trusted		11,924 KB		Local Security Authority Proces
fontdrvhost.exe	688	Trusted		2,912 KB		Usermode Font Driver Host
csrss.exe	468	Trusted		4,244 KB		Client Server Runtime Process
winlogon.exe	532	Trusted		7,300 KB		Windows Logon Application
fontdrvhost.exe	680	Trusted		4,140 KB		Usermode Font Driver Host
dwm.exe	868	Trusted		60,632 KB		Desktop Window Manager
ITSMAgent.exe *32	3148	Trusted		16,208 KB	DESKTOP-TTPO9PR...	Endpoint Manager Tray Applica
explorer.exe	3628	Trusted		106,720 KB	DESKTOP-TTPO9PR...	Windows Explorer
MSASCuiL.exe	5532	Trusted		8,396 KB	DESKTOP-TTPO9PR...	Windows Defender notification
OneDrive.exe *32	5624	Trusted		57,500 KB	DESKTOP-TTPO9PR...	Microsoft OneDrive
KillSwitch.exe	5936	Trusted	6.25	274,564 KB	DESKTOP-TTPO9PR...	COMODO Internet Security
icedragon.exe	5956	Trusted		250,148 KB	DESKTOP-TTPO9PR...	IceDragon
icedragon.exe	212	Trusted		227,836 KB	DESKTOP-TTPO9PR...	IceDragon
icedragon.exe	5916	Trusted		81,572 KB	DESKTOP-TTPO9PR...	IceDragon



Name	PID	Rating	...	...me	Descripti...
System Idle Process	0		9		
Interrupts					
DPCs					
System	4		120 KB	LOCAL_SYSTEM	
smss.exe	316	Trusted	692 KB	NT AUTHORITY\SY...	Windows
Memory Compression	1204	Error(Not Fo...	44,116 KB	NT AUTHORITY\SY...	
	68	Error(Not Fo...	4,288 KB	NT AUTHORITY\SY...	
svchost.exe	900	Trusted	36,708 KB	NT AUTHORITY\SY...	Host Process for
dasHost.exe	2004	Trusted	2,308 KB	NT AUTHORITY\LO...	Device Associat

The 'Verify Signatures' dialog will open:



Message title:

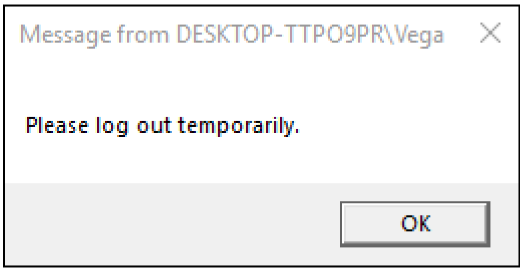
Message from DESKTOP-TTPO9PR\

Message:

Please log out temporarily.

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.

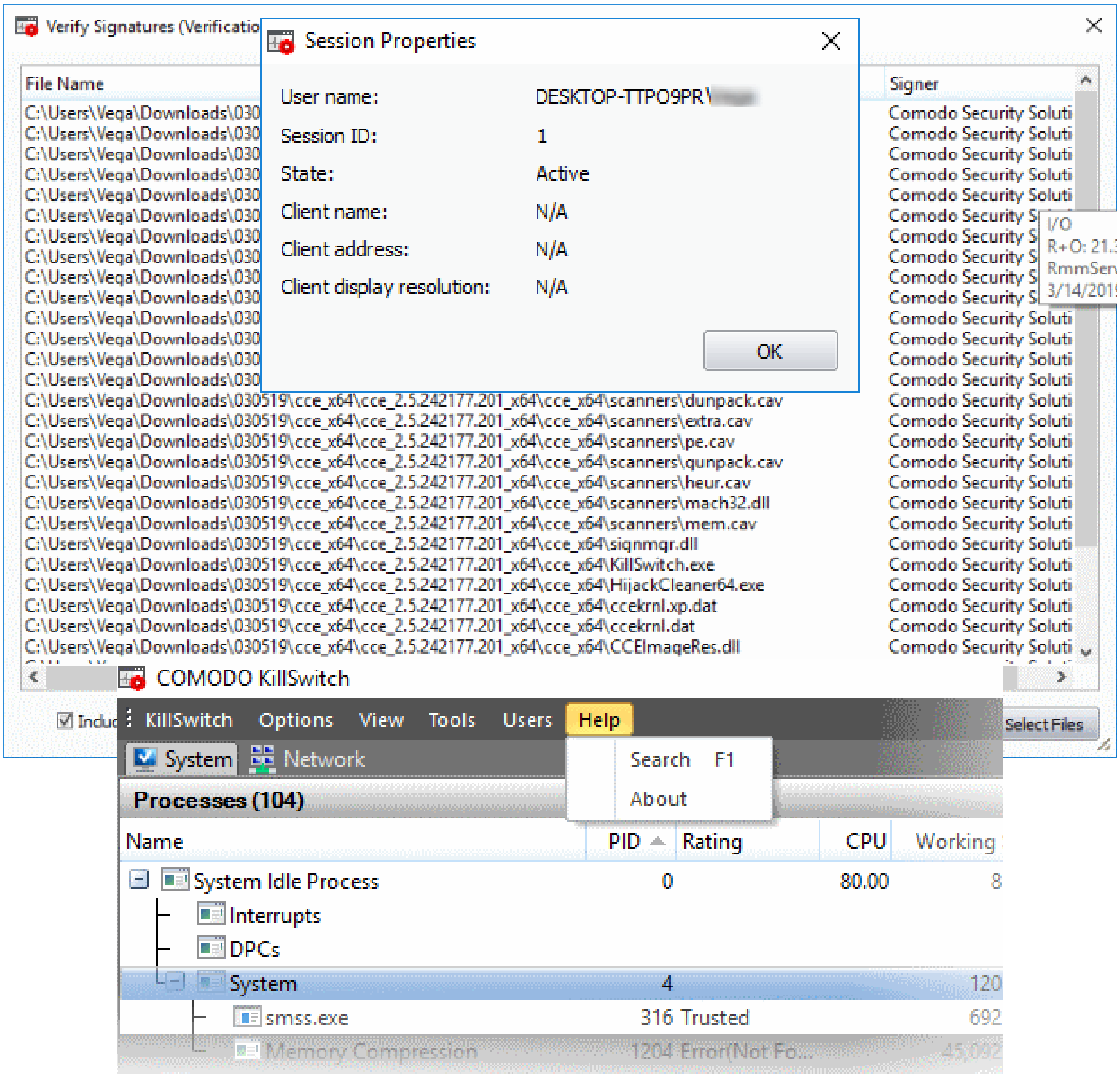
- Click 'Select Files' and navigate to the folder containing the files of the program and select the binary/executable file, to check for authenticity of a file.
- Click 'Select Folder' and navigate to the folder , to scan a folder for binaries and verify their signatures. KillSwitch will identify the .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 sub-folders'.



Message from DESKTOP-TTPO9PR\Vega

Please log out temporarily.

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



Verify Signatures (Verificatio

File Name	Signer
C:\Users\Vega\Downloads\030	Comodo Security Soluti
C:\Users\Vega\Downloads\030	Comodo Security Soluti
C:\Users\Vega\Downloads\030	Comodo Security Soluti
C:\Users\Vega\Downloads\030	Comodo Security Soluti
C:\Users\Vega\Downloads\030	Comodo Security Soluti
C:\Users\Vega\Downloads\030	Comodo Security S
C:\Users\Vega\Downloads\030	Comodo Security S
C:\Users\Vega\Downloads\030	Comodo Security S
C:\Users\Vega\Downloads\030	Comodo Security S
C:\Users\Vega\Downloads\030	Comodo Security S
C:\Users\Vega\Downloads\030	Comodo Security Soluti
C:\Users\Vega\Downloads\030	Comodo Security Soluti
C:\Users\Vega\Downloads\030	Comodo Security Soluti
C:\Users\Vega\Downloads\030	Comodo Security Soluti
C:\Users\Vega\Downloads\030519\cce_x64\cce_2.5.242177.201_x64\cce_x64\scanners\dunpack.cav	Comodo Security Soluti
C:\Users\Vega\Downloads\030519\cce_x64\cce_2.5.242177.201_x64\cce_x64\scanners\extra.cav	Comodo Security Soluti
C:\Users\Vega\Downloads\030519\cce_x64\cce_2.5.242177.201_x64\cce_x64\scanners\pe.cav	Comodo Security Soluti
C:\Users\Vega\Downloads\030519\cce_x64\cce_2.5.242177.201_x64\cce_x64\scanners\qunpack.cav	Comodo Security Soluti
C:\Users\Vega\Downloads\030519\cce_x64\cce_2.5.242177.201_x64\cce_x64\scanners\heur.cav	Comodo Security Soluti
C:\Users\Vega\Downloads\030519\cce_x64\cce_2.5.242177.201_x64\cce_x64\scanners\mach32.dll	Comodo Security Soluti
C:\Users\Vega\Downloads\030519\cce_x64\cce_2.5.242177.201_x64\cce_x64\scanners\mem.cav	Comodo Security Soluti
C:\Users\Vega\Downloads\030519\cce_x64\cce_2.5.242177.201_x64\cce_x64\signmgr.dll	Comodo Security Soluti
C:\Users\Vega\Downloads\030519\cce_x64\cce_2.5.242177.201_x64\cce_x64\KillSwitch.exe	Comodo Security Soluti
C:\Users\Vega\Downloads\030519\cce_x64\cce_2.5.242177.201_x64\cce_x64\HijackCleaner64.exe	Comodo Security Soluti
C:\Users\Vega\Downloads\030519\cce_x64\cce_2.5.242177.201_x64\cce_x64\ccekrnl.xp.dat	Comodo Security Soluti
C:\Users\Vega\Downloads\030519\cce_x64\cce_2.5.242177.201_x64\cce_x64\ccekrnl.dat	Comodo Security Soluti
C:\Users\Vega\Downloads\030519\cce_x64\cce_2.5.242177.201_x64\cce_x64\CCEImageRes.dll	Comodo Security Soluti

☑ Inclu

Session Properties

User name: DESKTOP-TTPO9PR\[redacted]

Session ID: 1

State: Active

Client name: N/A

Client address: N/A

Client display resolution: N/A

COMODO KillSwitch

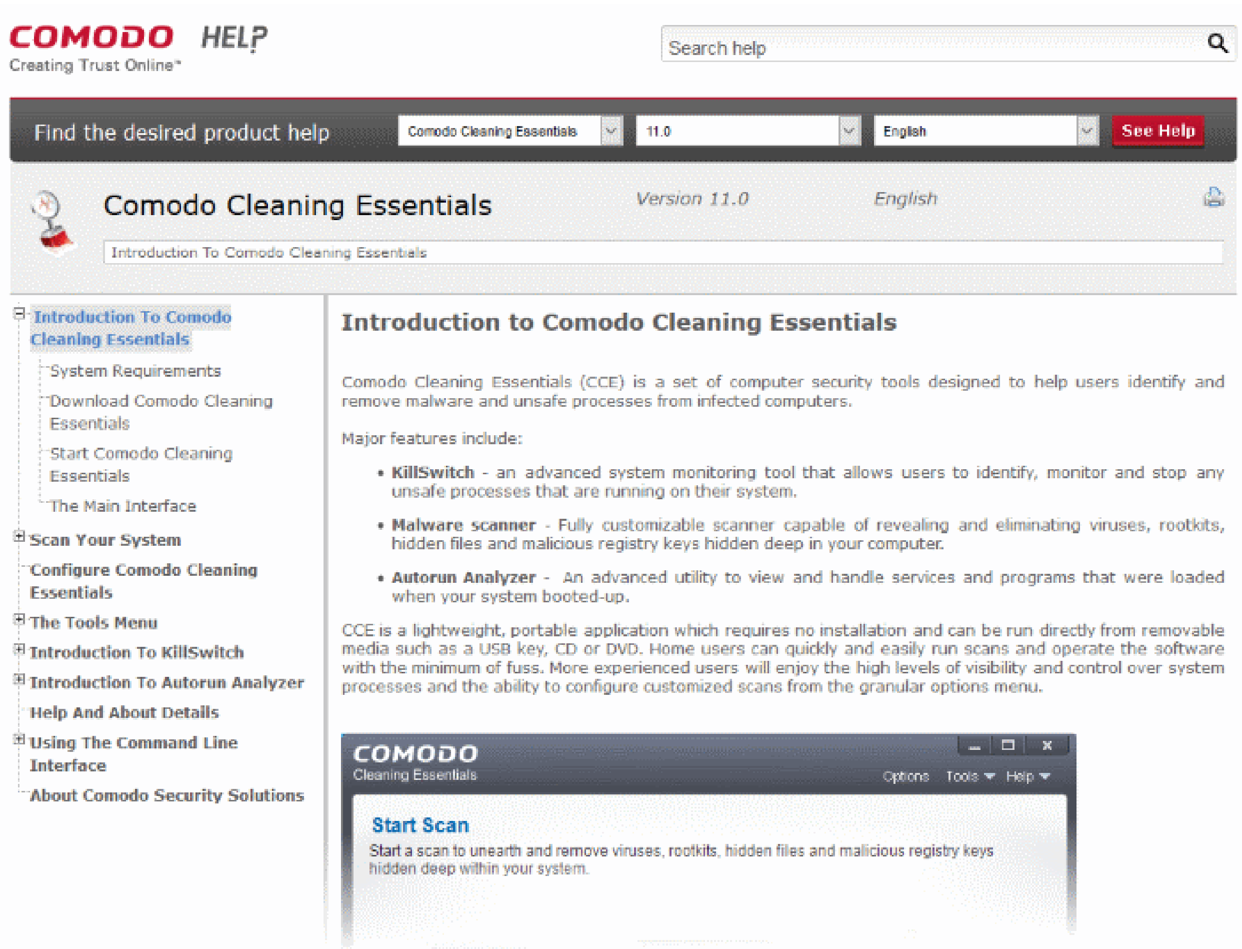
Processes (104)

Name	PID	Rating	CPU	Working
System Idle Process	0		80.00	8
Interrupts				
DPCs				
System	4			120
smss.exe	316	Trusted		692
Memory Compression	1204	Error(Not Fo...		45,092

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.



COMODO HELP
Creating Trust Online
Search help
Find the desired product help
Comodo Cleaning Essentials
11.0
English
See Help

Comodo Cleaning Essentials

Version 11.0

English

Introduction To Comodo Cleaning Essentials

Introduction To Comodo Cleaning Essentials
System Requirements
Download Comodo Cleaning Essentials
Start Comodo Cleaning Essentials
The Main Interface
Scan Your System
Configure Comodo Cleaning Essentials
The Tools Menu
Introduction To KillSwitch
Introduction To Autorun Analyzer
Help And About Details
Using The Command Line Interface
About Comodo Security Solutions

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:

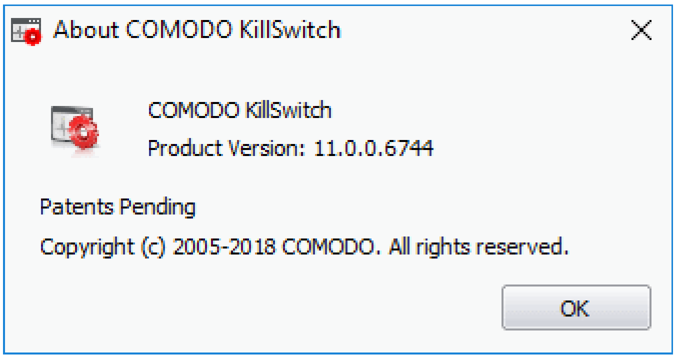
- **KillSwitch** - an advanced system monitoring tool that allows users to identify, monitor and stop any unsafe processes that are running on their system.
- **Malware scanner** - Fully customizable scanner capable of revealing and eliminating viruses, rootkits, hidden files and malicious registry keys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

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.



About COMODO KillSwitch

COMODO KillSwitch

Product Version: 11.0.0.6744

Patents Pending

Copyright (c) 2005-2018 COMODO. All rights reserved.

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.

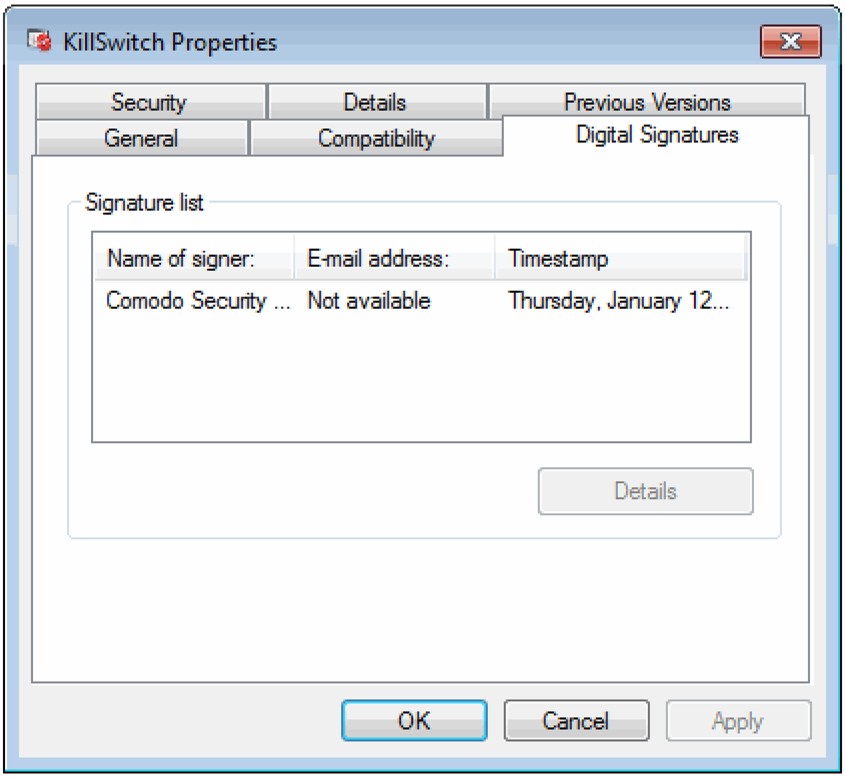
However, companies can't just 'sign' their own software and expect it to be trusted. This is why each code signing certificate is counter-signed by an organization called a 'Trusted Certificate Authority'. 'Comodo CA Limited' and 'Verisign' are two examples of a Trusted CA's and are authorized to counter-sign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

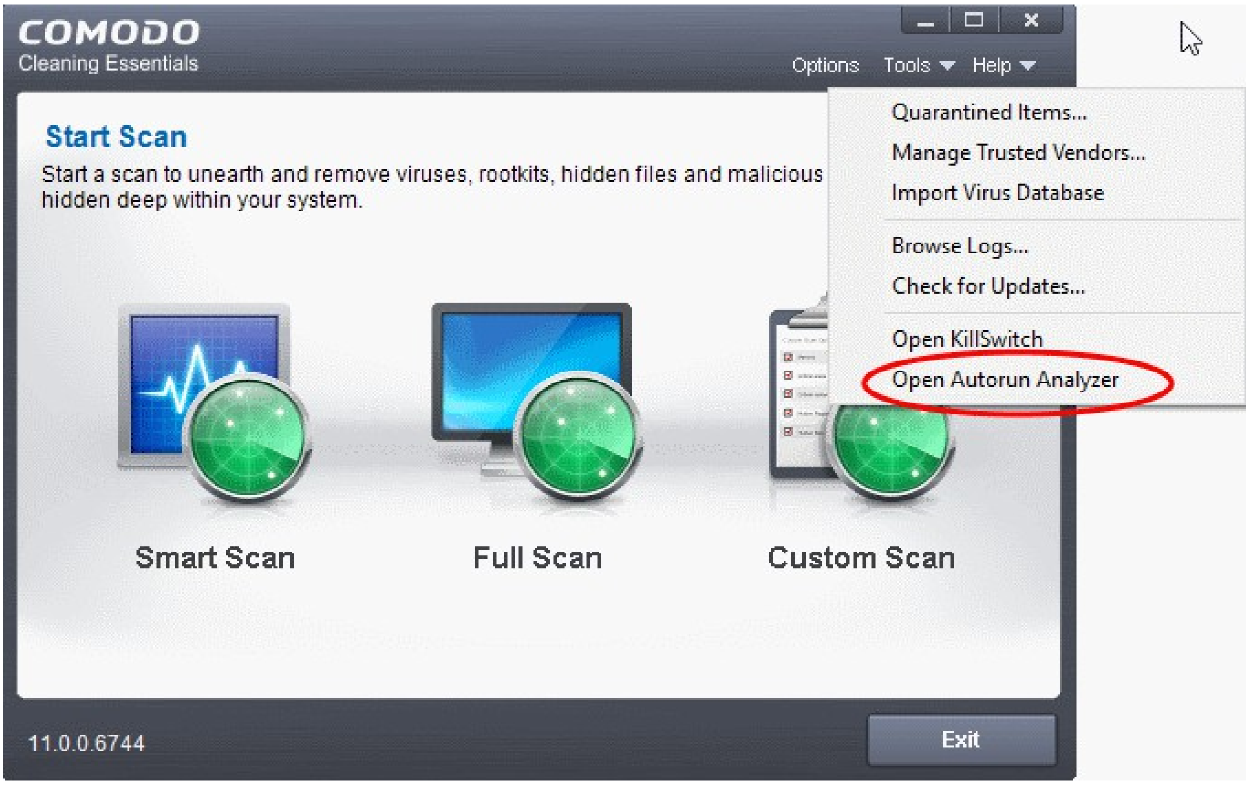
- Browse for the folder containing the Comodo Cleaning Essentials files
- Right-click on the file KillSwitch.exe
- Select 'Properties' from the menu
- Click the tab 'Digital Signatures' (if there is no such tab then the software has not been signed).

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

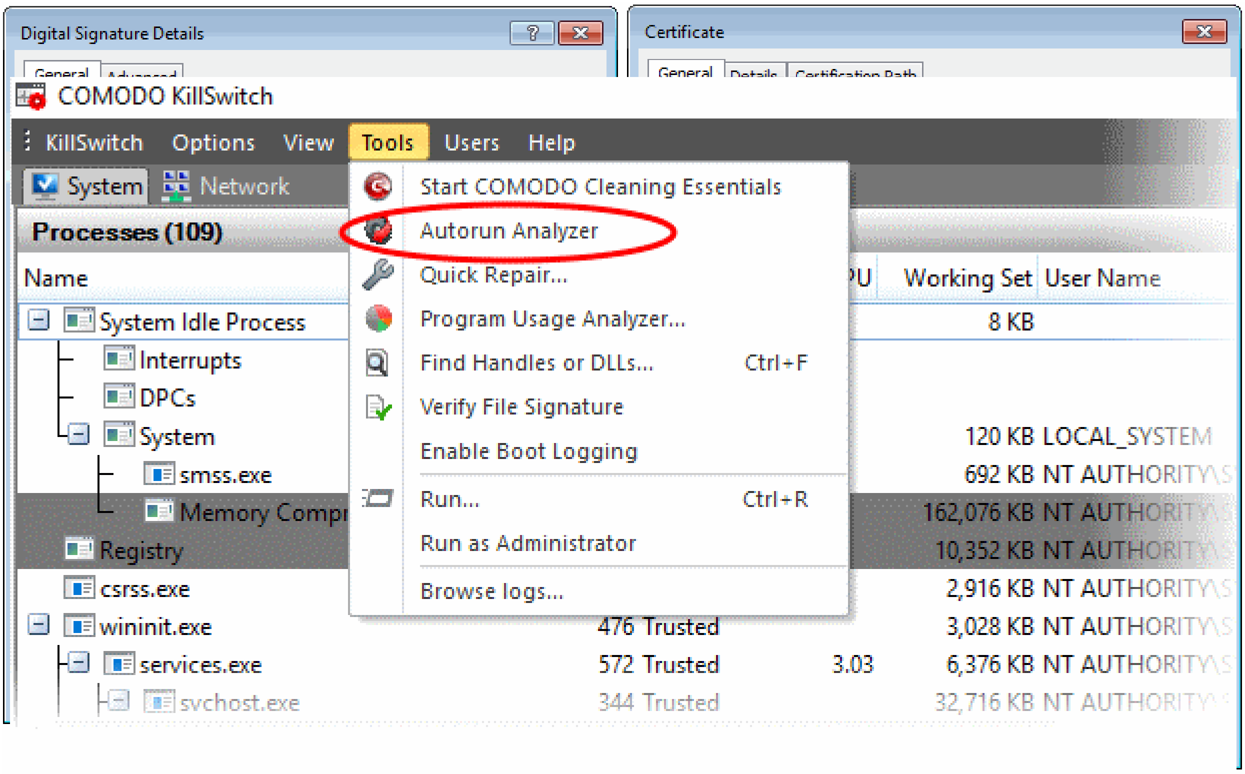


Name of signer:	E-mail address:	Timestamp
Comodo Security ...	Not available	Thursday, January 12...

- Select the certificate and click the 'Details' button to view digital signature information



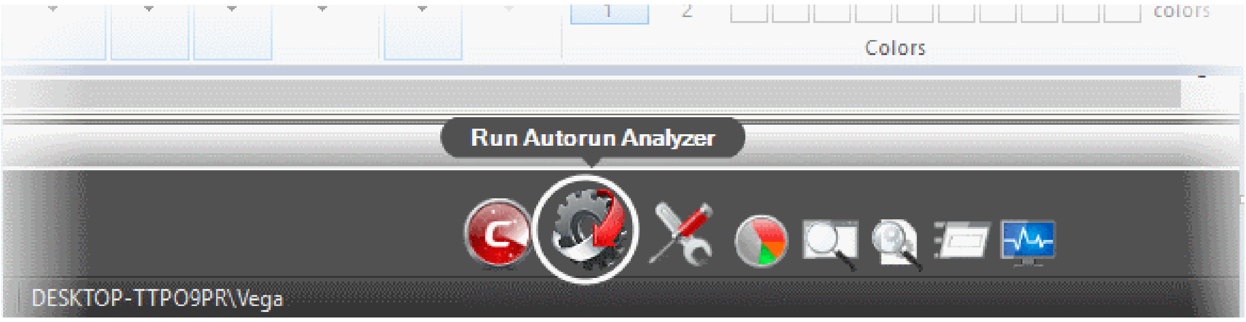
- Click the 'View Certificate' to inspect the actual code signing certificate. (see below)



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

5.6.6. Boot Log and Handle Loaded Modules

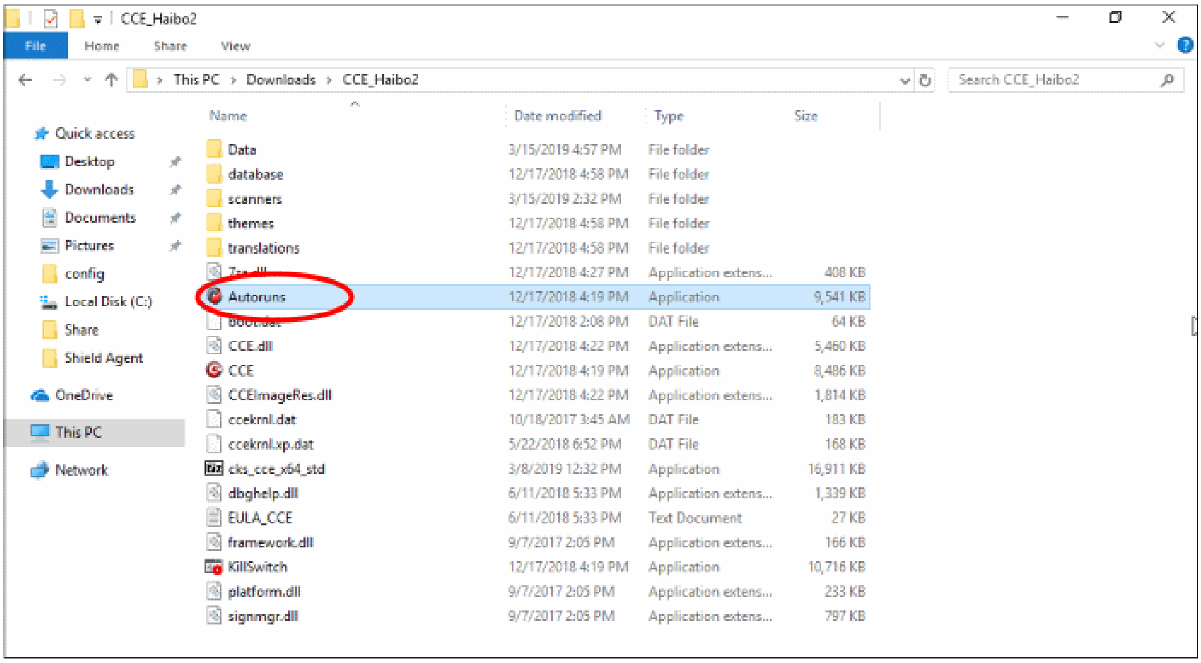
- The Boot logger feature records all modules loaded when your system boots.



- These include items like drivers, system files, DLLs, executables and so on.

- KillSwitch displays these modules in a new 'Loaded Modules' tab after your system has rebooted.

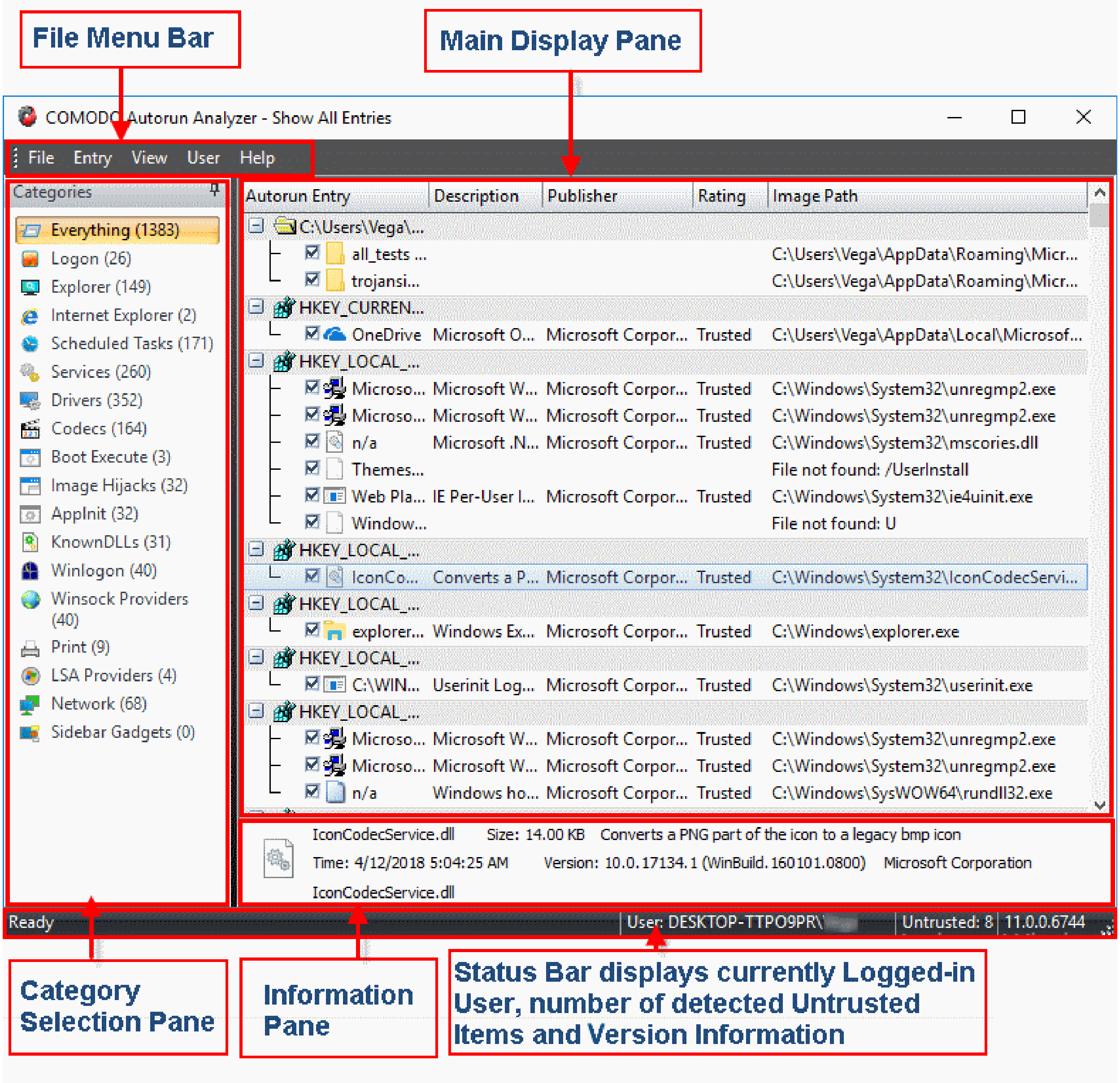
- This functionality lets you check whether unsafe (or even just unwanted) modules are being loaded. In extreme cases, it will allow you to detect and delete malicious boot items installed by spyware, key loggers, rootkits or other malware.



Name	Date modified	Type	Size
Data	3/15/2019 4:57 PM	File folder	
database	12/17/2018 4:58 PM	File folder	
scanners	3/15/2019 2:32 PM	File folder	
themes	12/17/2018 4:58 PM	File folder	
translations	12/17/2018 4:58 PM	File folder	
7za.dll	12/17/2018 4:27 PM	Application extens...	408 KB
Autoruns	12/17/2018 4:19 PM	Application	9,541 KB
boot.dat	12/17/2018 2:08 PM	DAT File	64 KB
CCE.dll	12/17/2018 4:22 PM	Application extens...	5,460 KB
CCE	12/17/2018 4:19 PM	Application	8,486 KB
CCEImageRes.dll	12/17/2018 4:22 PM	Application extens...	1,814 KB
ccekrnl.dat	10/18/2017 3:45 AM	DAT File	183 KB
ccekrnl.xp.dat	5/22/2018 6:52 PM	DAT File	168 KB
cks_cce_x64_std	3/8/2019 12:32 PM	Application	16,911 KB
dbghelp.dll	6/11/2018 5:33 PM	Application extens...	1,339 KB
EULA_CCE	6/11/2018 5:33 PM	Text Document	27 KB
framework.dll	9/7/2017 2:05 PM	Application extens...	166 KB
KillSwitch	12/17/2018 4:19 PM	Application	10,716 KB
platform.dll	9/7/2017 2:05 PM	Application extens...	233 KB
signmgr.dll	9/7/2017 2:05 PM	Application extens...	797 KB

To configure for Boot Logging

1. Click 'Tools' > 'Enable Boot Logging'



Autorun Entry	Description	Publisher	Rating	Image Path
⊟ C:\Users\Vega\...				
☑ all_tests ...				C:\Users\Vega\AppData\Roaming\Micr...
☑ trojansi...				C:\Users\Vega\AppData\Roaming\Micr...
⊟ HKEY_CURREN...				
☑ OneDrive	Microsoft O...	Microsoft Corpor...	Trusted	C:\Users\Vega\AppData\Local\Microsof...
⊟ HKEY_LOCAL_...				
☑ Microso...	Microsoft W...	Microsoft Corpor...	Trusted	C:\Windows\System32\unregmp2.exe
☑ Microso...	Microsoft W...	Microsoft Corpor...	Trusted	C:\Windows\System32\unregmp2.exe
☑ n/a	Microsoft .N...	Microsoft Corpor...	Trusted	C:\Windows\System32\mscories.dll
☑ Themes...				File not found: /UserInstall
☑ Web Pla...	IE Per-User I...	Microsoft Corpor...	Trusted	C:\Windows\System32\ie4uinit.exe
☑ Window...				File not found: U
⊟ HKEY_LOCAL_...				
☑ IconCo...	Converts a P...	Microsoft Corpor...	Trusted	C:\Windows\System32\IconCodecServi...
⊟ HKEY_LOCAL_...				
☑ explorer...	Windows Ex...	Microsoft Corpor...	Trusted	C:\Windows\explorer.exe
⊟ HKEY_LOCAL_...				
☑ C:\WIN...	Userinit Log...	Microsoft Corpor...	Trusted	C:\Windows\System32\userinit.exe
⊟ HKEY_LOCAL_...				
☑ Microso...	Microsoft W...	Microsoft Corpor...	Trusted	C:\Windows\System32\unregmp2.exe
☑ Microso...	Microsoft W...	Microsoft Corpor...	Trusted	C:\Windows\System32\unregmp2.exe
☑ n/a	Windows ho...	Microsoft Corpor...	Trusted	C:\Windows\SysWOW64\rundll32.exe

IconCodecService.dll Size: 14.00 KB Converts a PNG part of the icon to a legacy bmp icon
Time: 4/12/2018 5:04:25 AM Version: 10.0.17134.1 (WinBuild.160101.0800) Microsoft Corporation
IconCodecService.dll

Ready | User: DESKTOP-TTPO9PR\[redacted] | Untrusted: 8 | 11.0.0.6744

File Menu Bar

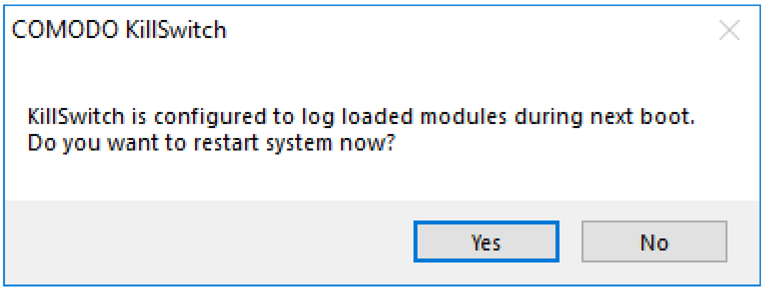
Main Display Pane

Category Selection Pane

Information Pane

Status Bar displays currently Logged-in User, number of detected Untrusted Items and Version Information

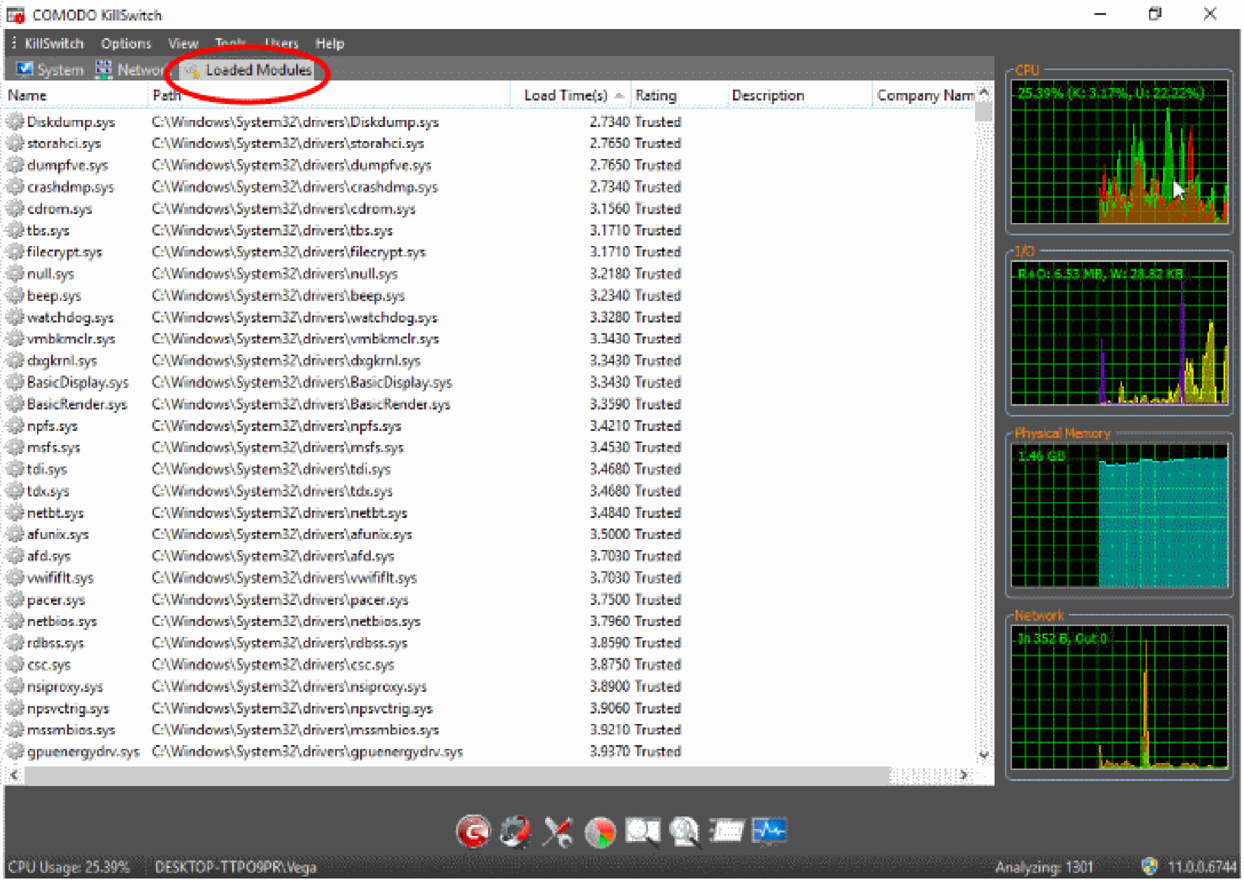
KillSwitch will request a restart of your computer to log all the modules that are loaded during the next re-boot.


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	Company Nam
Diskdump.sys	C:\Windows\System32\drivers\Diskdump.sys	2.7340	Trusted		
storahci.sys	C:\Windows\System32\drivers\storahci.sys	2.7650	Trusted		
dumpfve.sys	C:\Windows\System32\drivers\dumpfve.sys	2.7650	Trusted		
crashdmp.sys	C:\Windows\System32\drivers\crashdmp.sys	2.7340	Trusted		
cdrom.sys	C:\Windows\System32\drivers\cdrom.sys	3.1560	Trusted		
tbs.sys	C:\Windows\System32\drivers\tbs.sys	3.1710	Trusted		
filecrypt.sys	C:\Windows\System32\drivers\filecrypt.sys	3.1710	Trusted		
null.sys	C:\Windows\System32\drivers\null.sys	3.2180	Trusted		
beep.sys	C:\Windows\System32\drivers\beep.sys	3.2340	Trusted		
watchdog.sys	C:\Windows\System32\drivers\watchdog.sys	3.3280	Trusted		
vmbkmclr.sys	C:\Windows\System32\drivers\vmbkmclr.sys	3.3430	Trusted		
dxgkrnl.sys	C:\Windows\System32\drivers\dxgkrnl.sys	3.3430	Trusted		
BasicDisplay.sys	C:\Windows\System32\drivers\BasicDisplay.sys	3.3430	Trusted		
BasicRender.sys	C:\Windows\System32\drivers\BasicRender.sys	3.3590	Trusted		
npfs.sys	C:\Windows\System32\drivers\npfs.sys	3.4210	Trusted		
msfs.sys	C:\Windows\System32\drivers\msfs.sys	3.4530	Trusted		
tdi.sys	C:\Windows\System32\drivers\tdi.sys	3.4680	Trusted		
tdx.sys	C:\Windows\System32\drivers\tdx.sys	3.4680	Trusted		
netbt.sys	C:\Windows\System32\drivers\netbt.sys	3.4840	Trusted		
afunix.sys	C:\Windows\System32\drivers\afunix.sys	3.5000	Trusted		
afd.sys	C:\Windows\System32\drivers\afd.sys	3.7030	Trusted		
vwififlt.sys	C:\Windows\System32\drivers\vwififlt.sys	3.7030	Trusted		
pacer.sys	C:\Windows\System32\drivers\pacer.sys	3.7500	Trusted		
netbios.sys	C:\Windows\System32\drivers\netbios.sys	3.7960	Trusted		
rdbss.sys	C:\Windows\System32\drivers\rdbss.sys	3.8590	Trusted		
csc.sys	C:\Windows\System32\drivers\csc.sys	3.8750	Trusted		
nsiproxy.sys	C:\Windows\System32\drivers\nsiproxy.sys	3.8900	Trusted		
npsvctrig.sys	C:\Windows\System32\drivers\npsvctrig.sys	3.9060	Trusted		
mssmbios.sys	C:\Windows\System32\drivers\mssmbios.sys	3.9210	Trusted		
gpuenergydrv.sys	C:\Windows\System32\drivers\gpuenergydrv.sys	3.9370	Trusted		

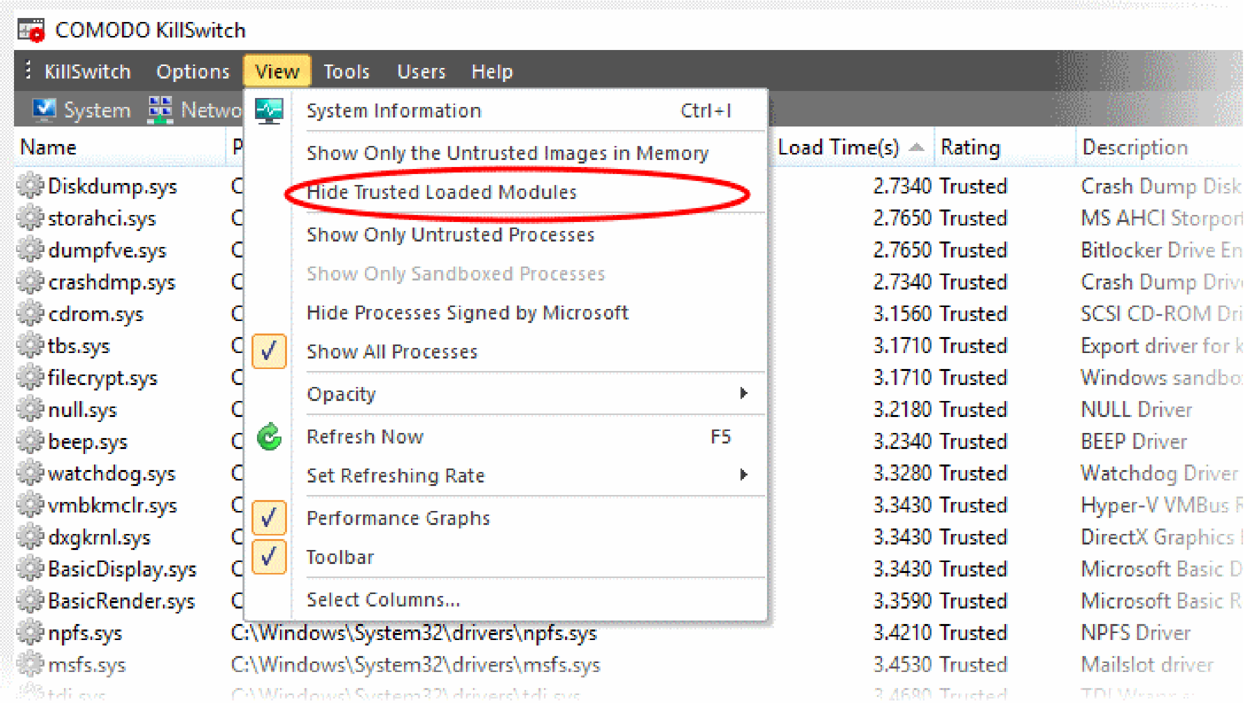
Loaded Modules window - Descriptions of Columns	
Column	**Description**
Name	The title of the module. Click the column header to sort the entries in alphabetical order of the module names.
Path	The storage location of the module.
Load Time (in seconds)	The time taken for loading the module.
Rating	The result of scanning performed by KillSwitch on the module. Modules that are rated as false positive, unsafe or unknown are highlighted for easy identification.
Description	A brief information of the module.
Company Name	The vendor of the module.

Tip: Click on any of the column header to sort the list in alphabetical/numerical order of the entries in it.

- Double-click on a module to open its 'Properties' dialog

Filter the Loaded Modules List

Click 'View' > 'Hide Trusted Loaded Modules' to show only modules identified as 'untrusted' or 'unknown':



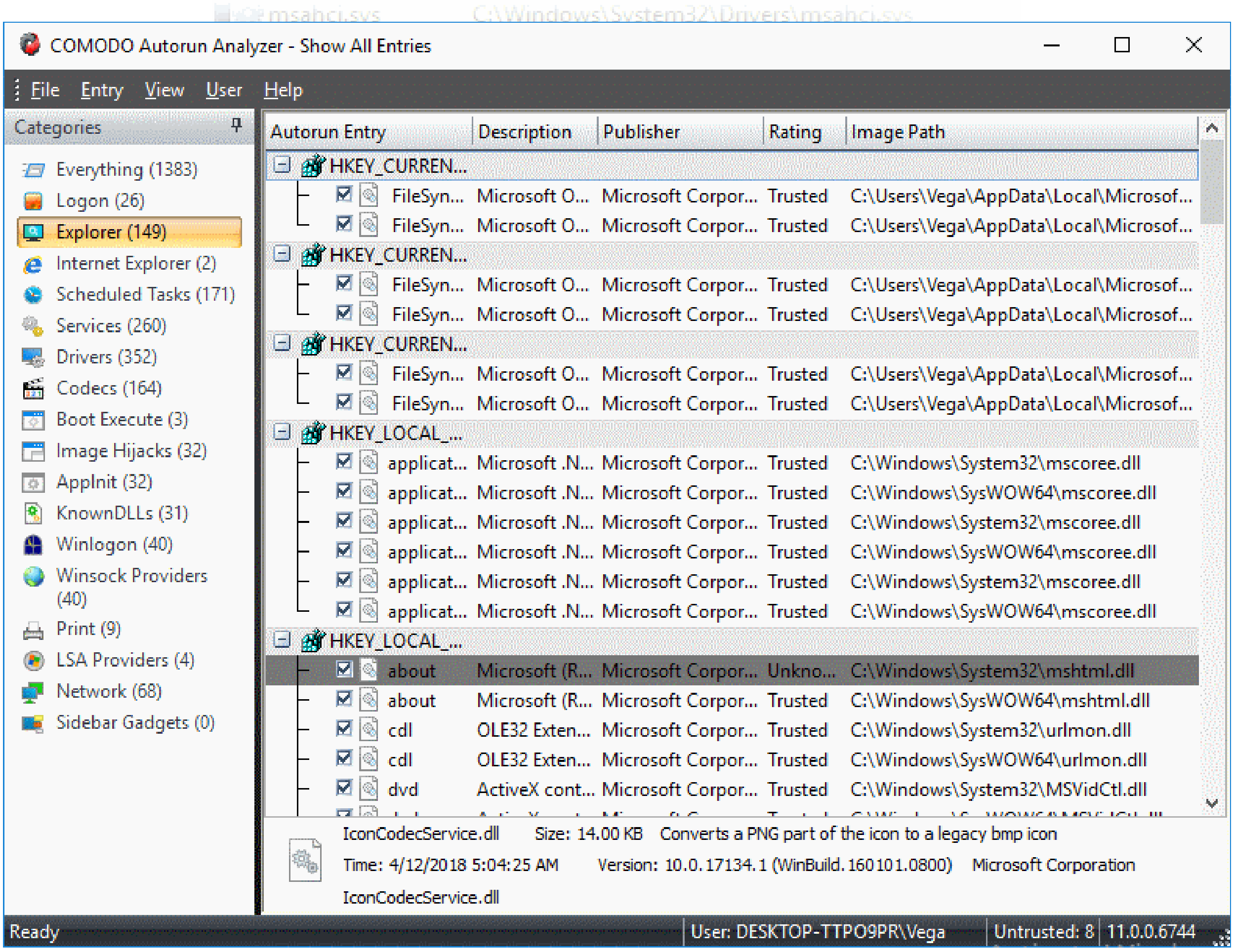
COMODO KillSwitch

- System Information Ctrl+I
- Show Only the Untrusted Images in Memory
- Hide Trusted Loaded Modules
- Show Only Untrusted Processes
- Show Only Sandboxed Processes
- Hide Processes Signed by Microsoft
- ✓ Show All Processes
- Opacity ▸
- Refresh Now F5
- Set Refreshing Rate ▸
- ✓ Performance Graphs
- ✓ Toolbar
- Select Columns...

Name	P	Load Time(s)	Rating	Description
Diskdump.sys	C	2.7340	Trusted	Crash Dump Disk
storahci.sys	C	2.7650	Trusted	MS AHCI Storport
dumpfve.sys	C	2.7650	Trusted	Bitlocker Drive En
crashdmp.sys	C	2.7340	Trusted	Crash Dump Driv
cdrom.sys	C	3.1560	Trusted	SCSI CD-ROM Dri
tbs.sys	C	3.1710	Trusted	Export driver for k
filecrypt.sys	C	3.1710	Trusted	Windows sandbo
null.sys	C	3.2180	Trusted	NULL Driver
beep.sys	C	3.2340	Trusted	BEEP Driver
watchdog.sys	C	3.3280	Trusted	Watchdog Driver
vmbkmclr.sys	C	3.3430	Trusted	Hyper-V VMBus F
dxgkrnl.sys	C	3.3430	Trusted	DirectX Graphics I
BasicDisplay.sys	C	3.3430	Trusted	Microsoft Basic D
BasicRender.sys	C	3.3590	Trusted	Microsoft Basic R
npfs.sys	C:\Windows\System32\drivers\npfs.sys	3.4210	Trusted	NPFS Driver
msfs.sys	C:\Windows\System32\drivers\msfs.sys	3.4530	Trusted	Mailslot driver
tdi.sys	C:\Windows\System32\drivers\tdi.sys	3.4680	Trusted	TDI Wrapper

Handle Loaded Modules

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



COMODO Autorun Analyzer - Show All Entries

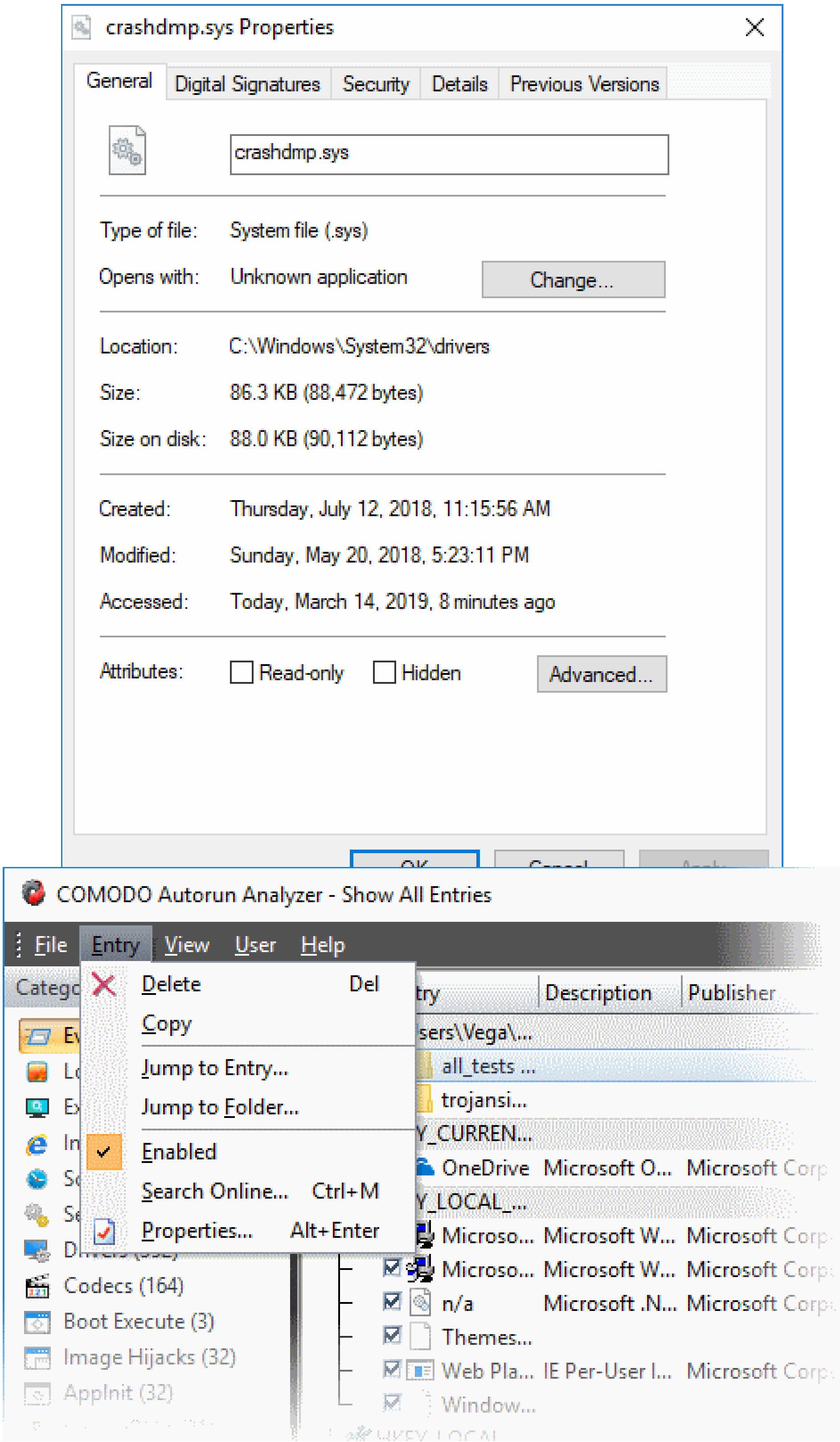
- Everything (1383)
- Logon (26)
- Explorer (149)
- Internet Explorer (2)
- Scheduled Tasks (171)
- Services (260)
- Drivers (352)
- Codecs (164)
- Boot Execute (3)
- Image Hijacks (32)
- AppInit (32)
- KnownDLLs (31)
- Winlogon (40)
- Winsock Providers (40)
- Print (9)
- LSA Providers (4)
- Network (68)
- Sidebar Gadgets (0)

Autorun Entry	Description	Publisher	Rating	Image Path
⊟ HKEY_CURREN...				
☑ FileSyn...	Microsoft O...	Microsoft Corpor...	Trusted	C:\Users\Vega\AppData\Local\Microsof...
☑ FileSyn...	Microsoft O...	Microsoft Corpor...	Trusted	C:\Users\Vega\AppData\Local\Microsof...
⊟ HKEY_CURREN...				
☑ FileSyn...	Microsoft O...	Microsoft Corpor...	Trusted	C:\Users\Vega\AppData\Local\Microsof...
☑ FileSyn...	Microsoft O...	Microsoft Corpor...	Trusted	C:\Users\Vega\AppData\Local\Microsof...
⊟ HKEY_CURREN...				
☑ FileSyn...	Microsoft O...	Microsoft Corpor...	Trusted	C:\Users\Vega\AppData\Local\Microsof...
☑ FileSyn...	Microsoft O...	Microsoft Corpor...	Trusted	C:\Users\Vega\AppData\Local\Microsof...
⊟ HKEY_LOCAL_...				
☑ applicat...	Microsoft .N...	Microsoft Corpor...	Trusted	C:\Windows\System32\mscoree.dll
☑ applicat...	Microsoft .N...	Microsoft Corpor...	Trusted	C:\Windows\SysWOW64\mscoree.dll
☑ applicat...	Microsoft .N...	Microsoft Corpor...	Trusted	C:\Windows\System32\mscoree.dll
☑ applicat...	Microsoft .N...	Microsoft Corpor...	Trusted	C:\Windows\SysWOW64\mscoree.dll
☑ applicat...	Microsoft .N...	Microsoft Corpor...	Trusted	C:\Windows\System32\mscoree.dll
☑ applicat...	Microsoft .N...	Microsoft Corpor...	Trusted	C:\Windows\SysWOW64\mscoree.dll
⊟ HKEY_LOCAL_...				
☑ about	Microsoft (R...	Microsoft Corpor...	Unkno...	C:\Windows\System32\mshtml.dll
☑ about	Microsoft (R...	Microsoft Corpor...	Trusted	C:\Windows\SysWOW64\mshtml.dll
☑ cdl	OLE32 Exten...	Microsoft Corpor...	Trusted	C:\Windows\System32\urlmon.dll
☑ cdl	OLE32 Exten...	Microsoft Corpor...	Trusted	C:\Windows\SysWOW64\urlmon.dll
☑ dvd	ActiveX cont...	Microsoft Corpor...	Trusted	C:\Windows\System32\MSVidCtl.dll

IconCodecService.dll Size: 14.00 KB Converts a PNG part of the icon to a legacy bmp icon
Time: 4/12/2018 5:04:25 AM Version: 10.0.17134.1 (WinBuild.160101.0800) Microsoft Corporation
IconCodecService.dll

Ready | User: DESKTOP-TTPO9PR\Vega | Untrusted: 8 | 11.0.0.6744

- **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 -** The location having the module in windows explorer.
- **Properties... -** The attributes dialog of the selected Module.



crashdmp.sys Properties

General | Digital Signatures | Security | Details | Previous Versions

crashdmp.sys

Type of file: System file (.sys)

Opens with: Unknown application

Location: C:\Windows\System32\drivers

Size: 86.3 KB (88,472 bytes)

Size on disk: 88.0 KB (90,112 bytes)

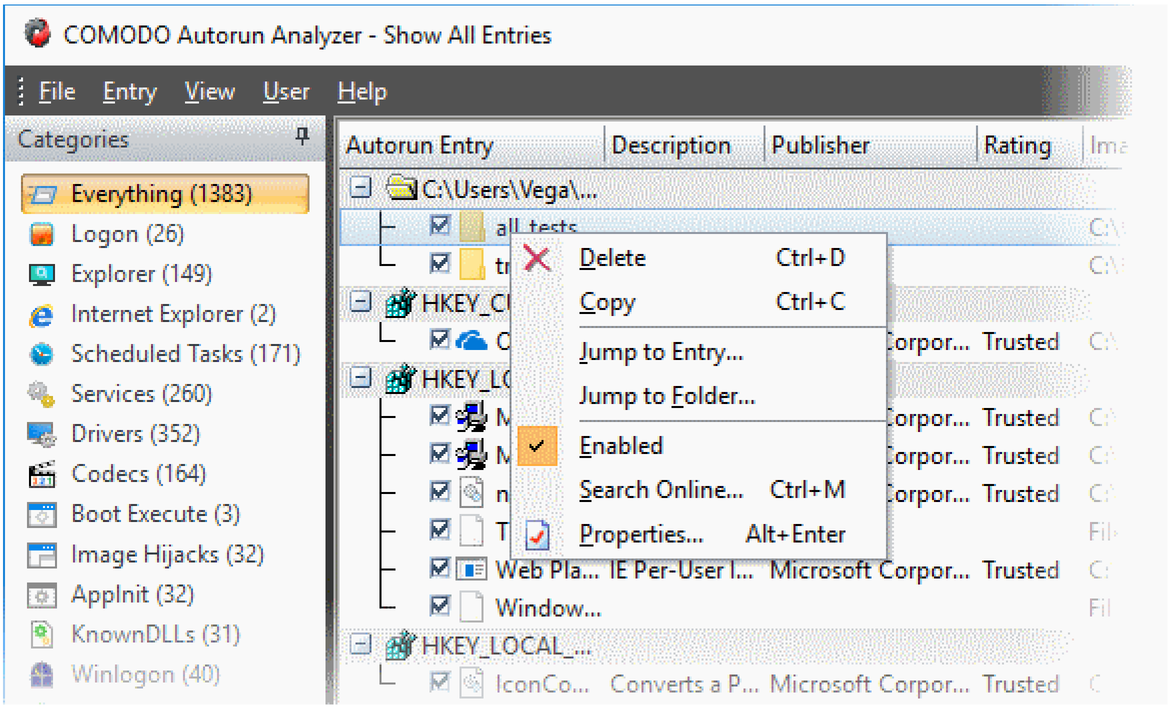
Created: Thursday, July 12, 2018, 11:15:56 AM

Modified: Sunday, May 20, 2018, 5:23:11 PM

Accessed: Today, March 14, 2019, 8 minutes ago

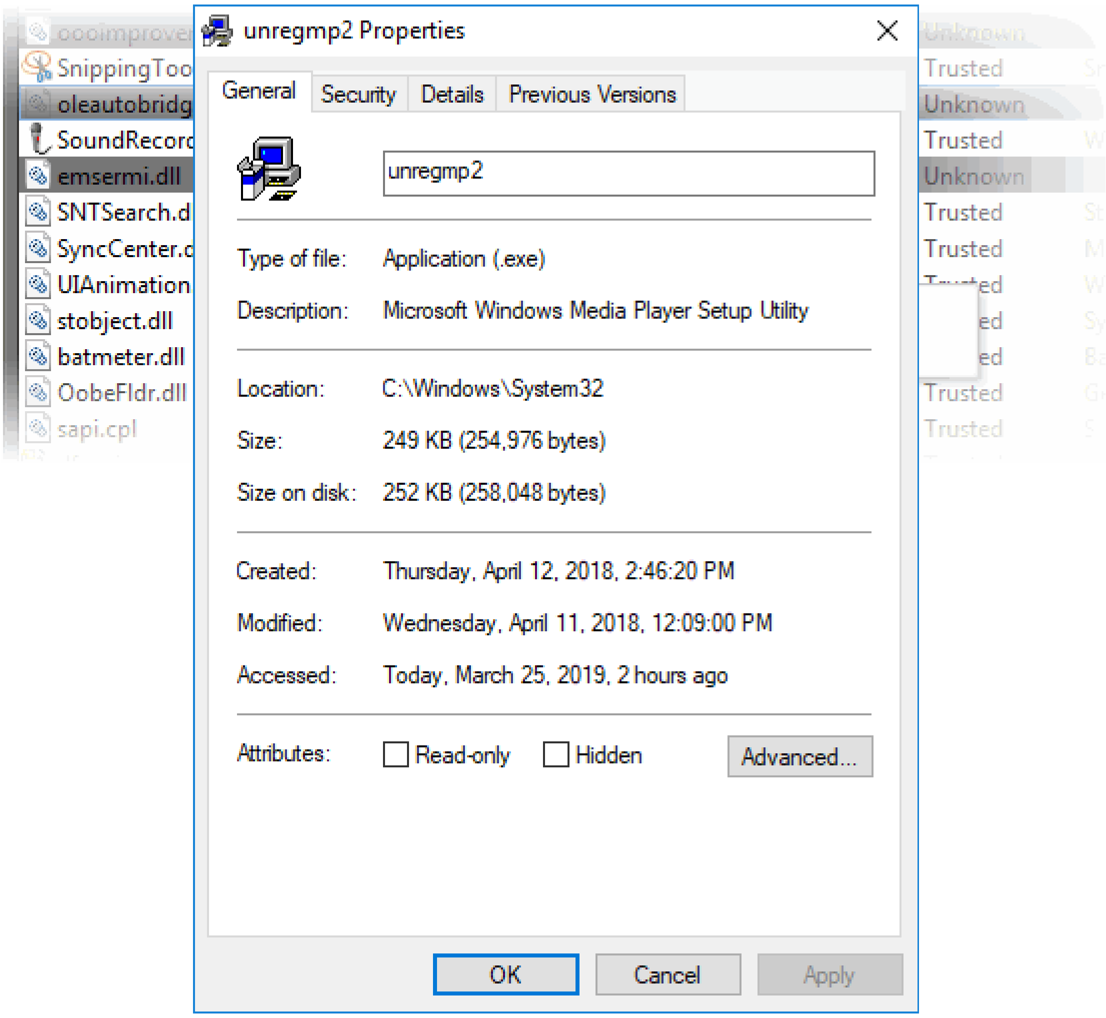
Attributes: □ Read-only □ Hidden

- **Search Online -** The default web browser of your system with the search engine specified and searches for information on the module.



- **Send to COMODO** - Submit the module to Comodo for analysis:
  - Report Suspicious - Submit items you believe are malicious but have been deemed safe by KillSwitch
  - Report 'False Positive' - Submit items you think KillSwitch has falsely identified as suspicious.

  Submitted files will be analyzed by experts and added to the global white list or black list accordingly.



unregmp2

Type of file: Application (.exe)

Description: Microsoft Windows Media Player Setup Utility

Location: C:\Windows\System32

Size: 249 KB (254,976 bytes)

Size on disk: 252 KB (258,048 bytes)

Created: Thursday, April 12, 2018, 2:46:20 PM

Modified: Wednesday, April 11, 2018, 12:09:00 PM

Accessed: Today, March 25, 2019, 2 hours ago

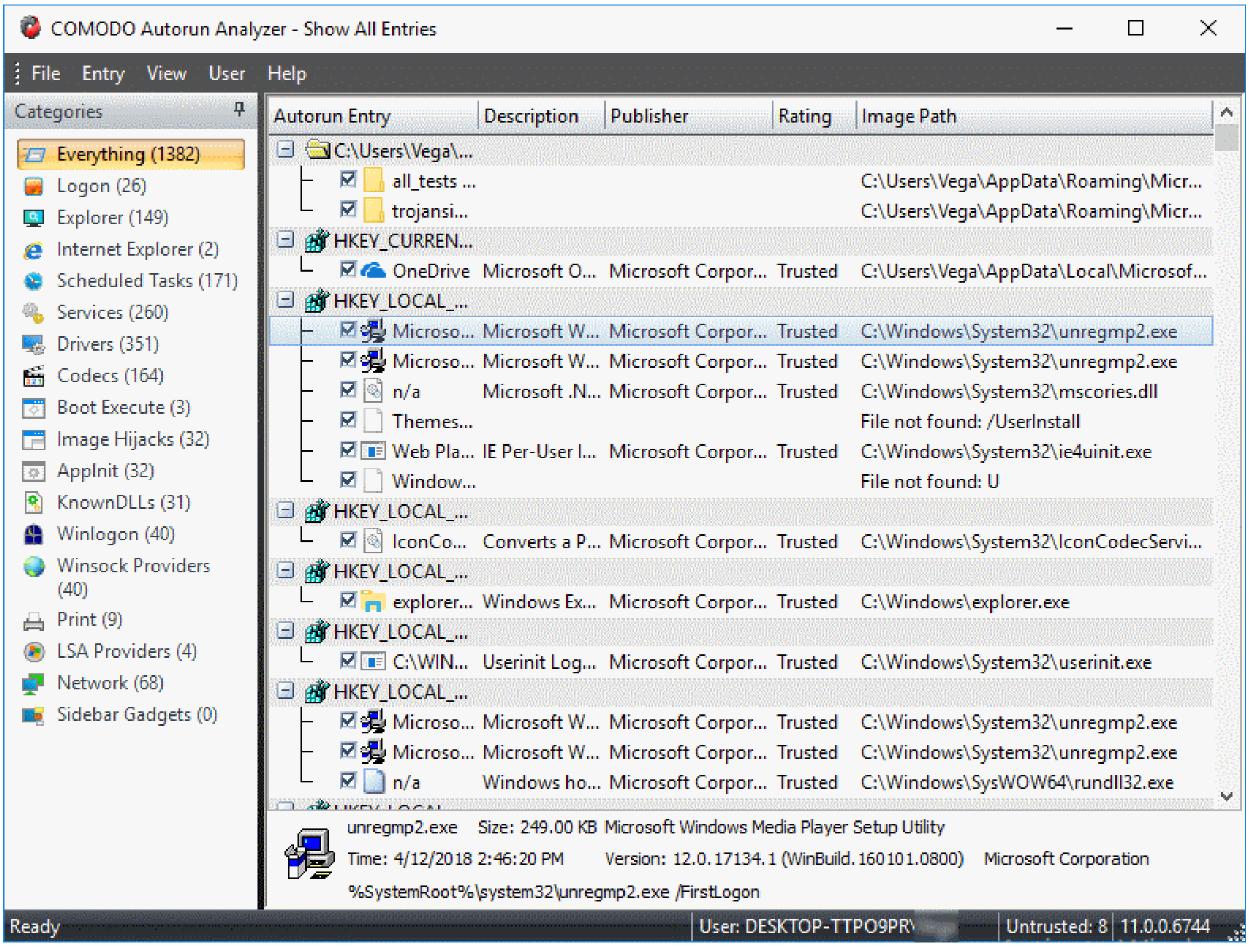
Attributes: □ Read-only □ Hidden

5.6.7. Run Programs from Command Line Interface

KillSwitch lets you run programs from the command line interface with admin privileges or the privileges of the currently logged-in user.

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

- Click 'Tools' > 'Run'



Autorun Entry	Description	Publisher	Rating	Image Path
⊟ C:\Users\Vega\...				
☑ all_tests ...				C:\Users\Vega\AppData\Roaming\Micr...
☑ trojansi...				C:\Users\Vega\AppData\Roaming\Micr...
⊟ HKEY_CURREN...				
☑ OneDrive	Microsoft O...	Microsoft Corpor...	Trusted	C:\Users\Vega\AppData\Local\Microsof...
⊟ HKEY_LOCAL_...				
☑ Microso...	Microsoft W...	Microsoft Corpor...	Trusted	C:\Windows\System32\unregmp2.exe
☑ Microso...	Microsoft W...	Microsoft Corpor...	Trusted	C:\Windows\System32\unregmp2.exe
☑ n/a	Microsoft .N...	Microsoft Corpor...	Trusted	C:\Windows\System32\mscories.dll
☑ Themes...				File not found: /UserInstall
☑ Web Pla...	IE Per-User I...	Microsoft Corpor...	Trusted	C:\Windows\System32\ie4uinit.exe
☑ Window...				File not found: U
⊟ HKEY_LOCAL_...				
☑ IconCo...	Converts a P...	Microsoft Corpor...	Trusted	C:\Windows\System32\IconCodecServi...
⊟ HKEY_LOCAL_...				
☑ explorer...	Windows Ex...	Microsoft Corpor...	Trusted	C:\Windows\explorer.exe
⊟ HKEY_LOCAL_...				
☑ C:\WIN...	Userinit Log...	Microsoft Corpor...	Trusted	C:\Windows\System32\userinit.exe
⊟ HKEY_LOCAL_...				
☑ Microso...	Microsoft W...	Microsoft Corpor...	Trusted	C:\Windows\System32\unregmp2.exe
☑ Microso...	Microsoft W...	Microsoft Corpor...	Trusted	C:\Windows\System32\unregmp2.exe
☑ n/a	Windows ho...	Microsoft Corpor...	Trusted	C:\Windows\SysWOW64\rundll32.exe

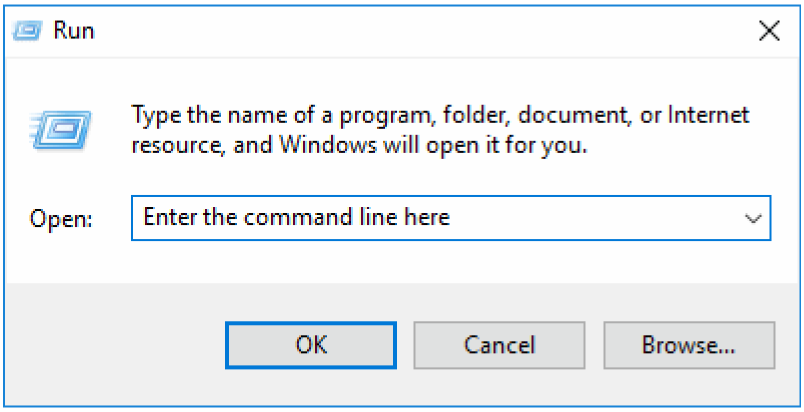
unregmp2.exe Size: 249.00 KB Microsoft Windows Media Player Setup Utility

Time: 4/12/2018 2:46:20 PM Version: 12.0.17134.1 (WinBuild.160101.0800) Microsoft Corporation

%SystemRoot%\system32\unregmp2.exe /FirstLogon

Ready | User: DESKTOP-TTPO9PR\ | Untrusted: 8 | 11.0.0.6744

- Alternatively, click the run icon from the toolbar.



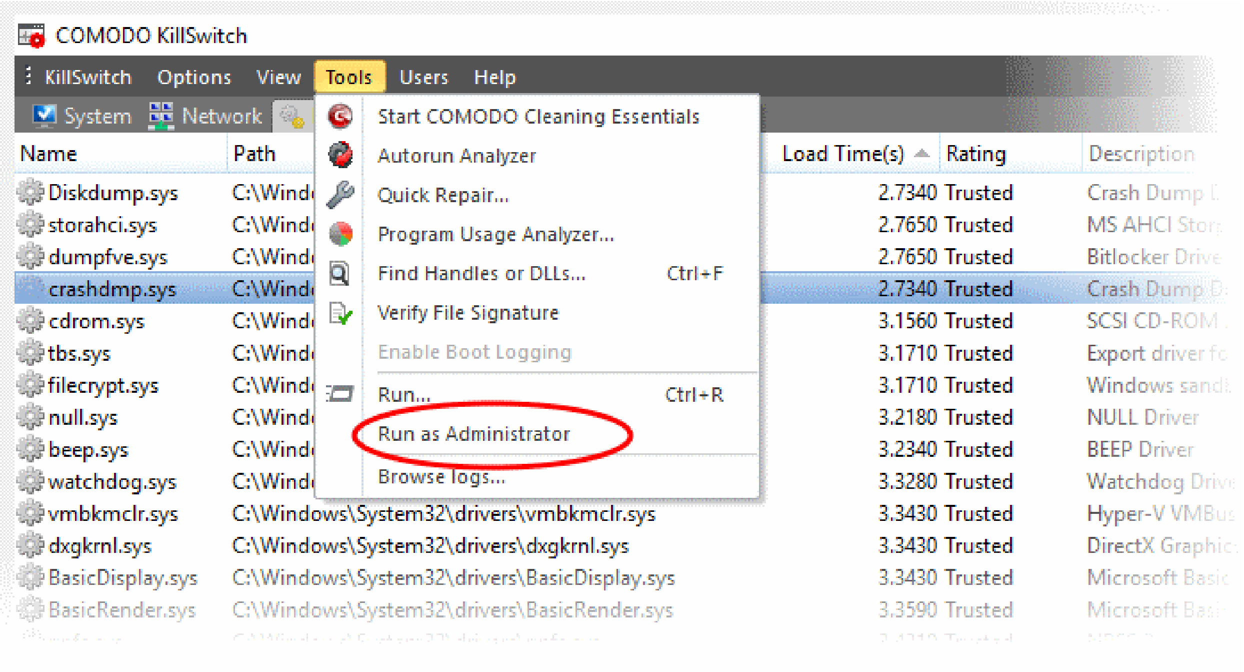
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: Enter the command line here

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

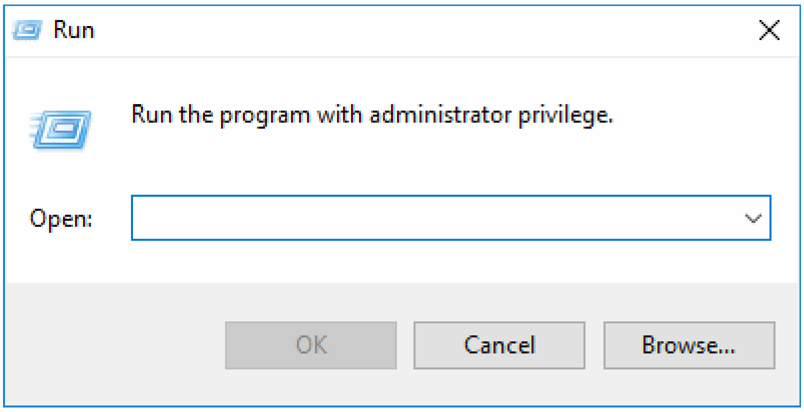
To run programs that require Administrative privileges:

- Click 'Run as Administrator', on the 'Tools' menu.



Name	Path	Load Time(s)	Rating	Description
Diskdump.sys	C:\Wind	2.7340	Trusted	Crash Dump
storahci.sys	C:\Wind	2.7650	Trusted	MS AHCI Stor
dumpfve.sys	C:\Wind	2.7650	Trusted	Bitlocker Drive
crashdmp.sys	C:\Wind	2.7340	Trusted	Crash Dump D
cdrom.sys	C:\Wind	3.1560	Trusted	SCSI CD-ROM
tbs.sys	C:\Wind	3.1710	Trusted	Export driver fo
filecrypt.sys	C:\Wind	3.1710	Trusted	Windows sand
null.sys	C:\Wind	3.2180	Trusted	NULL Driver
beep.sys	C:\Wind	3.2340	Trusted	BEEP Driver
watchdog.sys	C:\Wind	3.3280	Trusted	Watchdog Drive
vmbkmclr.sys	C:\Windows\System32\drivers\vmbkmclr.sys	3.3430	Trusted	Hyper-V VMBus
dxgkrnl.sys	C:\Windows\System32\drivers\dxgkrnl.sys	3.3430	Trusted	DirectX Graphic
BasicDisplay.sys	C:\Windows\System32\drivers\BasicDisplay.sys	3.3430	Trusted	Microsoft Basic
BasicRender.sys	C:\Windows\System32\drivers\BasicRender.sys	3.3590	Trusted	Microsoft Basi

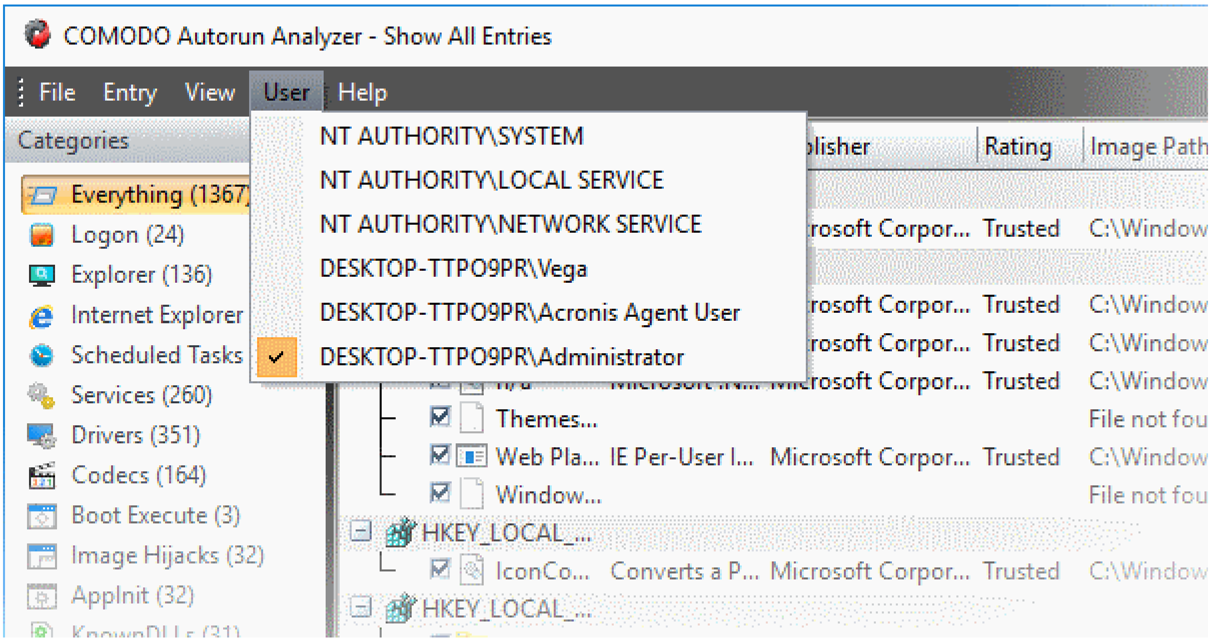
- The 'Run' dialog opens. Enter the command or browse to the file/program you wish to open with administrative privileges by clicking 'Browse'.



Run the program with administrator privilege.

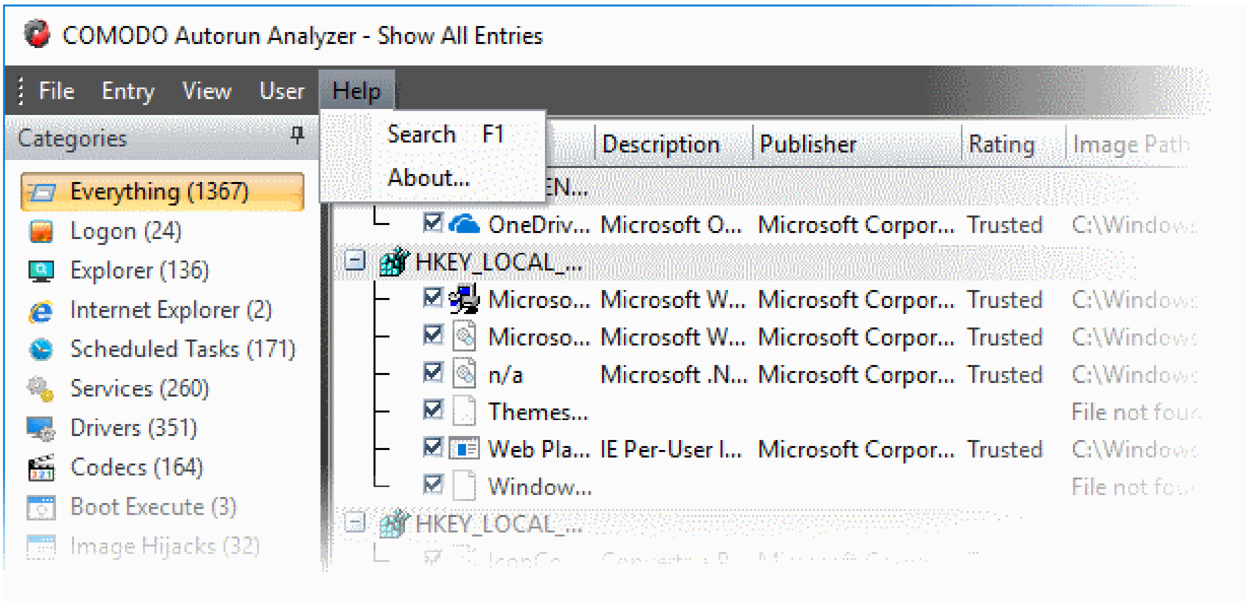
Open:

- Click 'OK'.

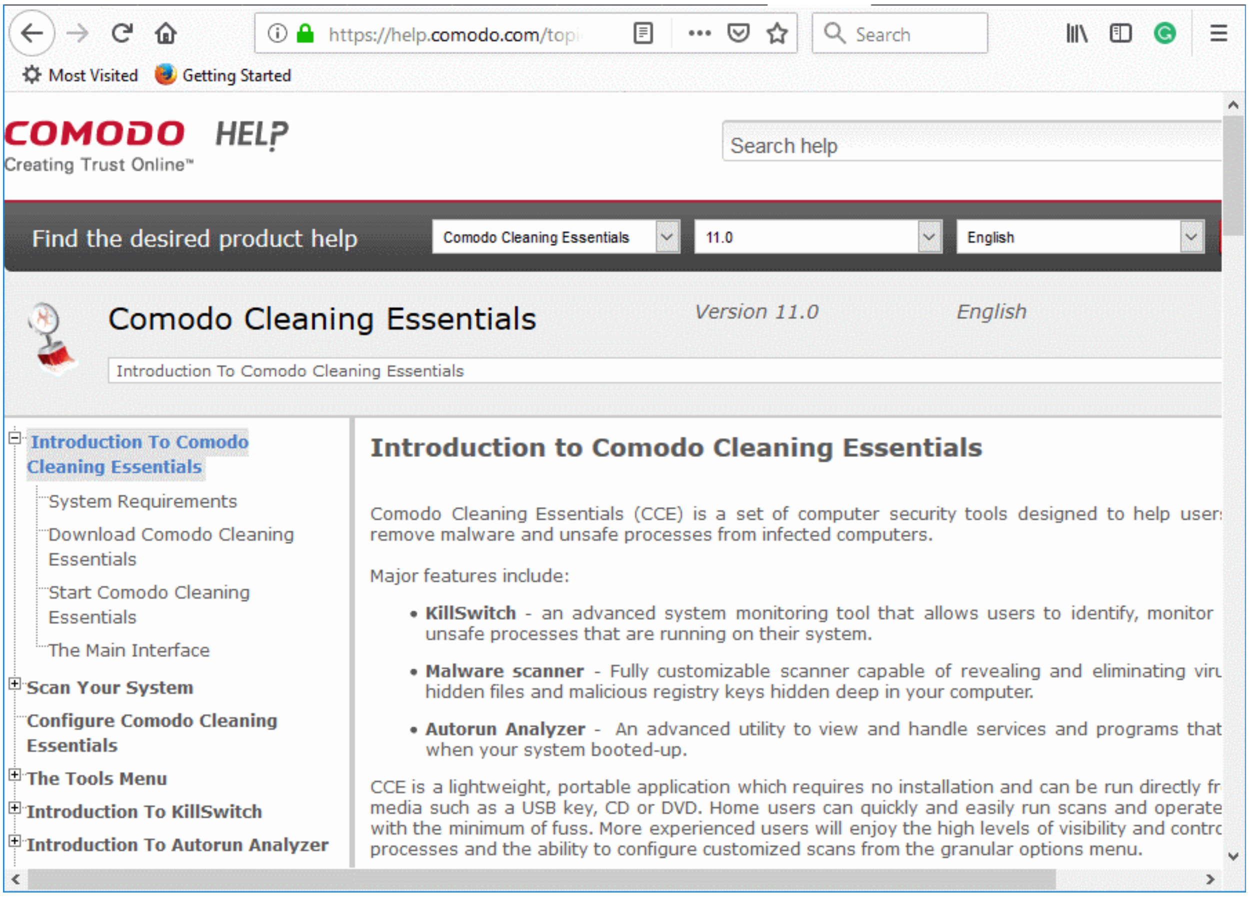

COMODO Autorun Analyzer - Show All Entries
File
Entry
View
User
Help
Categories
Everything (1367)
Logon (24)
Explorer (136)
Internet Explorer
Scheduled Tasks
Services (260)
Drivers (351)
Codecs (164)
Boot Execute (3)
Image Hijacks (32)
AppInit (32)
NT AUTHORITY\SYSTEM
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
DESKTOP-TTPO9PR\Vega
DESKTOP-TTPO9PR\Acronis Agent User
✓ DESKTOP-TTPO9PR\Administrator
Publisher
Rating
Image Path
Themes...
Web Pla... IE Per-User I... Microsoft Corpor... Trusted C:\Window
Window...
HKEY_LOCAL_...
IconCo... Converts a P... Microsoft Corpor... Trusted C:\Window

5.6.8. View KillSwitch Logs

- KillSwitch maintains a log of threats and the actions taken against them.
- Logs can be configured in 'Options' > 'Threats Logging Level'.
- The logs are stored as date stamped text files in the folder ...\CCE\Data\KillSwitch\KsLogs.


COMODO Autorun Analyzer - Show All Entries
File
Entry
View
User
Help
Search F1
About...
Categories
Everything (1367)
Logon (24)
Explorer (136)
Internet Explorer (2)
Scheduled Tasks (171)
Services (260)
Drivers (351)
Codecs (164)
Boot Execute (3)
Image Hijacks (32)
Description
Publisher
Rating
Image Path
OneDriv... Microsoft O... Microsoft Corpor... Trusted C:\Windows
HKEY_LOCAL_...
Microso... Microsoft W... Microsoft Corpor... Trusted C:\Windows
Microso... Microsoft W... Microsoft Corpor... Trusted C:\Windows
n/a Microsoft .N... Microsoft Corpor... Trusted C:\Windows
Themes... File not fou
Web Pla... IE Per-User I... Microsoft Corpor... Trusted C:\Windows
Window... File not fou
HKEY_LOCAL_...

To view the log files:



Comodo Cleaning Essentials Version 11.0 English

Introduction To Comodo Cleaning Essentials

- Introduction To Comodo Cleaning Essentials
  - System Requirements
  - Download Comodo Cleaning Essentials
  - Start Comodo Cleaning Essentials
  - The Main Interface
- Scan Your System
- Configure Comodo Cleaning Essentials
- The Tools Menu
- Introduction To KillSwitch
- Introduction To Autorun Analyzer

Introduction to Comodo Cleaning Essentials

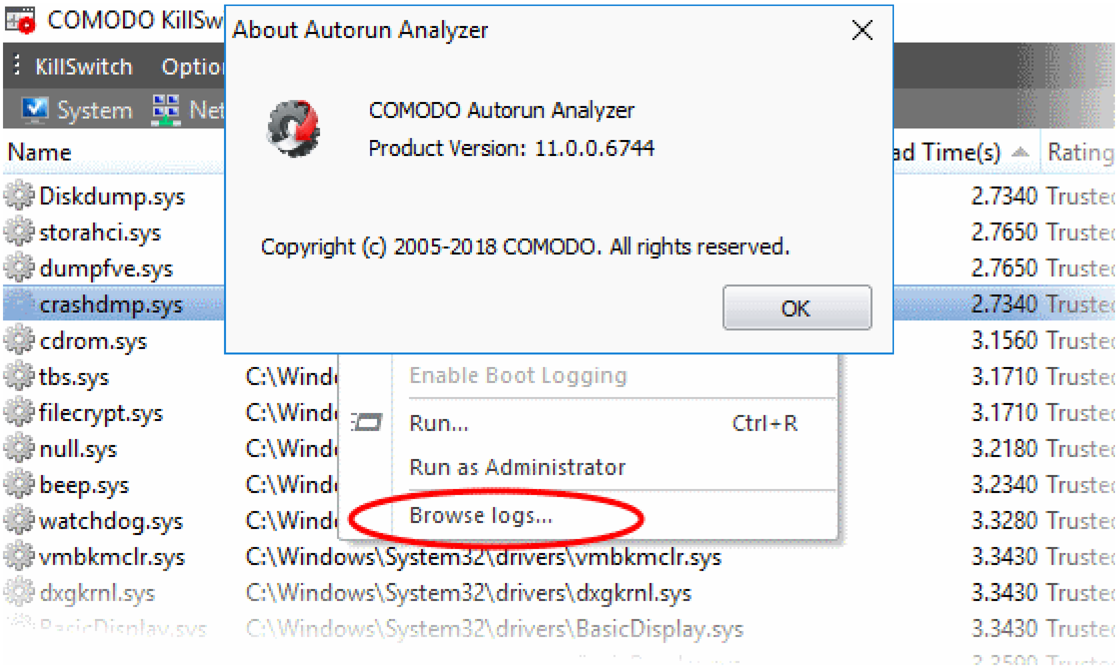
Comodo Cleaning Essentials (CCE) is a set of computer security tools designed to help user remove malware and unsafe processes from infected computers.

Major features include:

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

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

- Click 'Tools' > 'Browse Logs'



About Autorun Analyzer

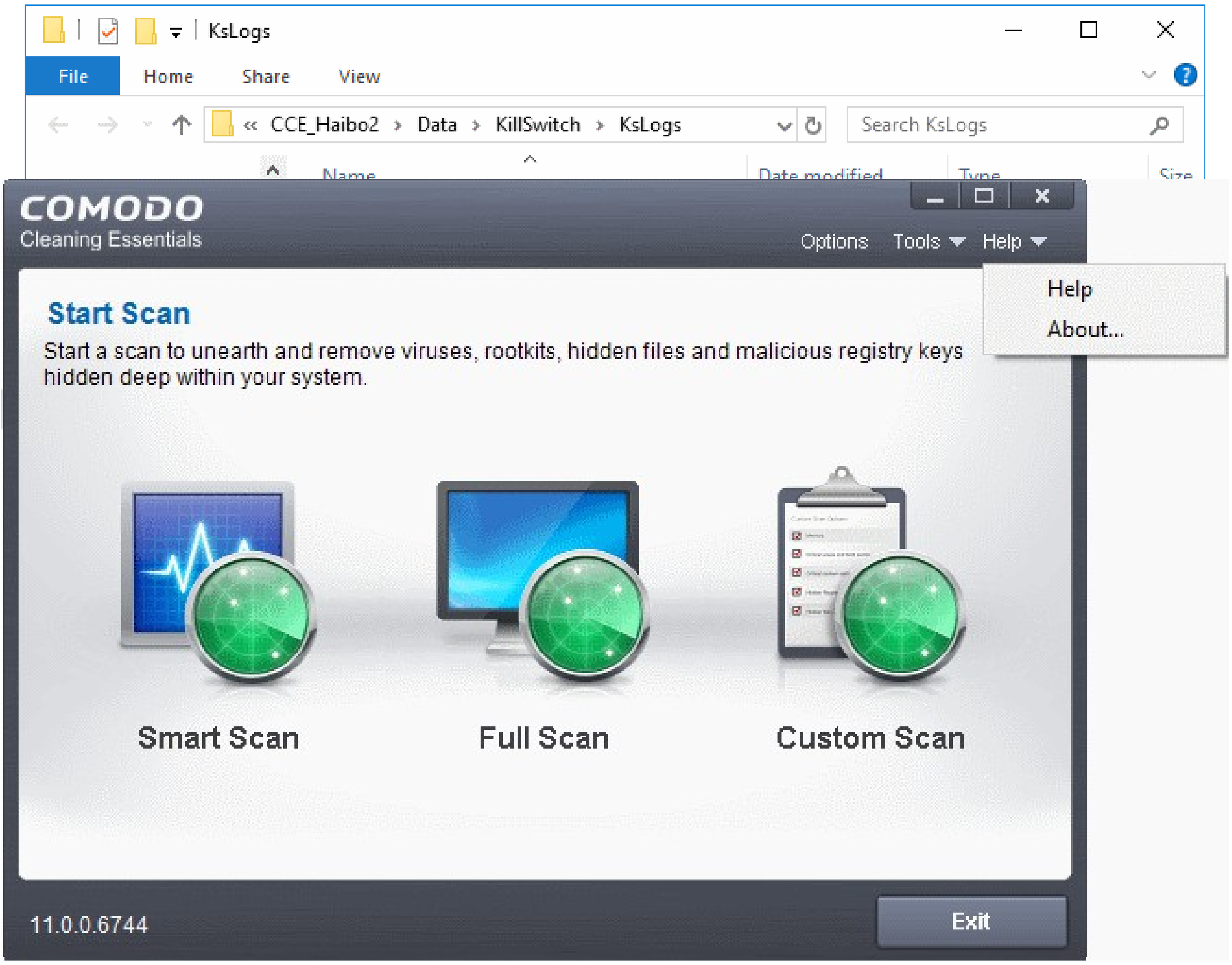
COMODO Autorun Analyzer
Product Version: 11.0.0.6744

Copyright (c) 2005-2018 COMODO. All rights reserved.

OK

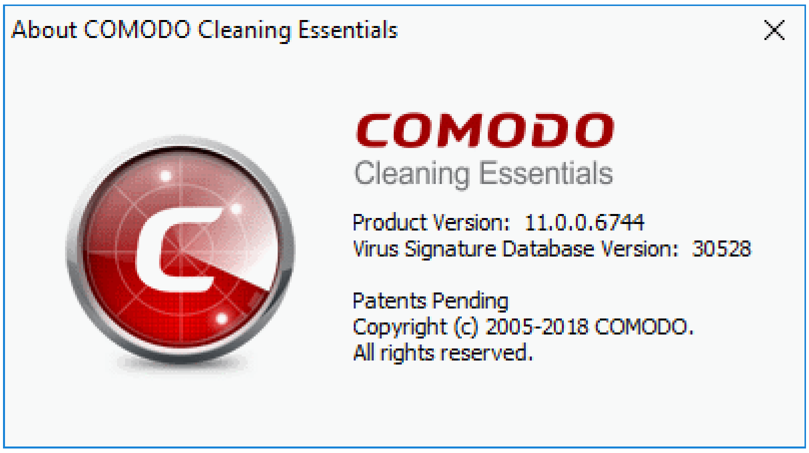
Diskdump.sys		2.7340	Truste
storahci.sys		2.7650	Truste
dumpfve.sys		2.7650	Truste
crashdmp.sys		2.7340	Truste
cdrom.sys		3.1560	Truste
tbs.sys	C:\Wind	3.1710	Truste
filecrypt.sys	C:\Wind	3.1710	Truste
null.sys	C:\Wind	3.2180	Truste
beep.sys	C:\Wind	3.2340	Truste
watchdog.sys	C:\Wind	3.3280	Truste
vmbkmclr.sys	C:\Windows\System32\drivers\vmbkmclr.sys	3.3430	Truste
dxgkrnl.sys	C:\Windows\System32\drivers\dxgkrnl.sys	3.3430	Truste
BasicDisplay.sys	C:\Windows\System32\drivers\BasicDisplay.sys	3.3430	Truste

The logs folder will open in Windows Explorer.



- Double-click on the file you wish to view.

5.6.9. Find Process of the Active Window


About COMODO Cleaning Essentials

COMODO
Cleaning Essentials

Product Version: 11.0.0.6744
Virus Signature Database Version: 30528

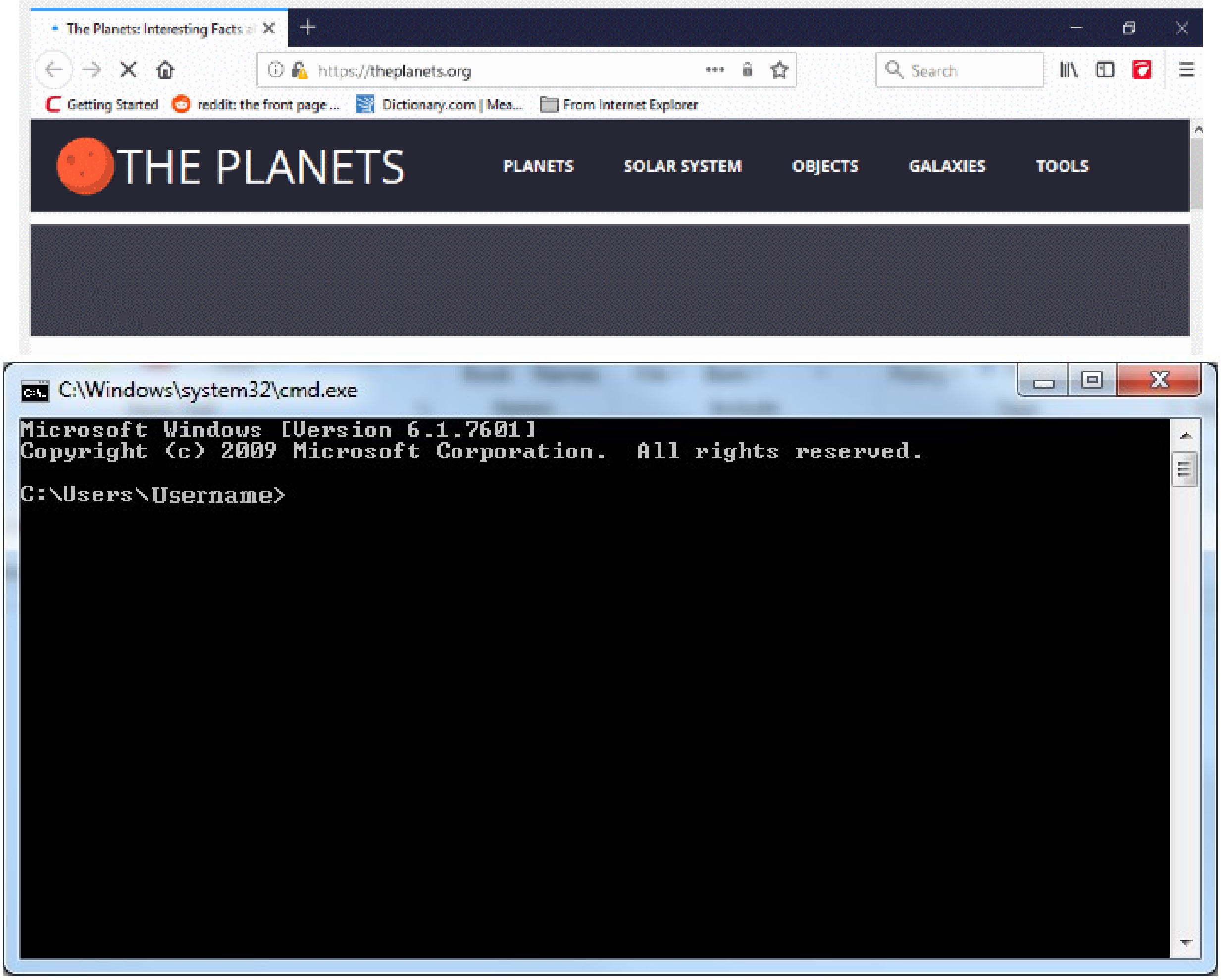
Patents Pending
Copyright (c) 2005-2018 COMODO.
All rights reserved.

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

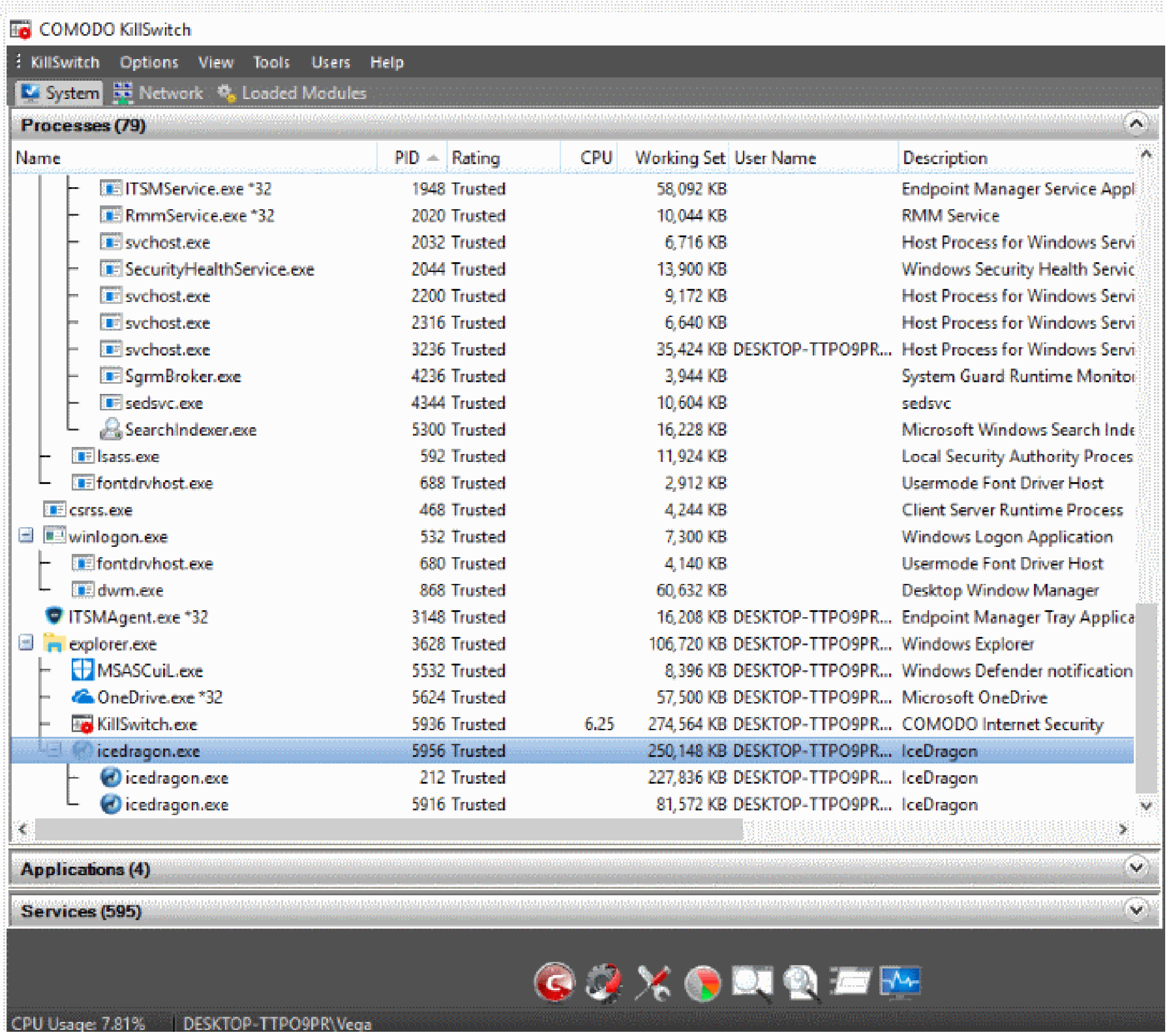
2. Drag the bulls-eye to the portion of the window for which you want to find the process



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Username>
```

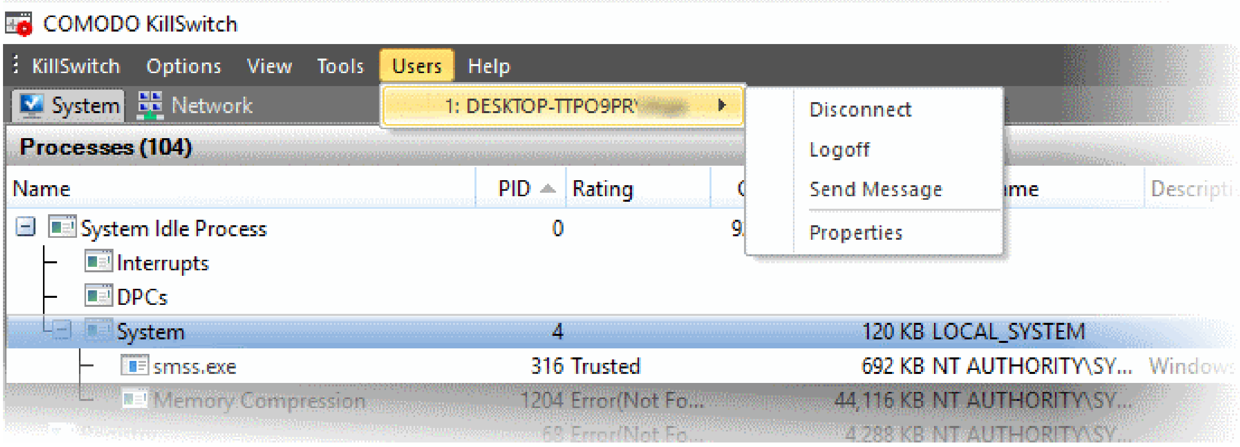
3. On release of the mouse button, the process related to the highlighted window will be shown highlighted in the 'Processes' window of KillSwitch.



Name	PID	Rating	CPU	Working Set	User Name	Description
ITSMService.exe *32	1948	Trusted		58,092 KB		Endpoint Manager Service Appl
RmmService.exe *32	2020	Trusted		10,044 KB		RMM Service
svchost.exe	2032	Trusted		6,716 KB		Host Process for Windows Servi
SecurityHealthService.exe	2044	Trusted		13,900 KB		Windows Security Health Servic
svchost.exe	2200	Trusted		9,172 KB		Host Process for Windows Servi
svchost.exe	2316	Trusted		6,640 KB		Host Process for Windows Servi
svchost.exe	3236	Trusted		35,424 KB	DESKTOP-TTPO9PR...	Host Process for Windows Servi
SgrmBroker.exe	4236	Trusted		3,944 KB		System Guard Runtime Monitor
sedsvc.exe	4344	Trusted		10,604 KB		sedsvc
SearchIndexer.exe	5300	Trusted		16,228 KB		Microsoft Windows Search Inde
lsass.exe	592	Trusted		11,924 KB		Local Security Authority Proces
fontdrvhost.exe	688	Trusted		2,912 KB		Usermode Font Driver Host
csrss.exe	468	Trusted		4,244 KB		Client Server Runtime Process
winlogon.exe	532	Trusted		7,300 KB		Windows Logon Application
fontdrvhost.exe	680	Trusted		4,140 KB		Usermode Font Driver Host
dwm.exe	868	Trusted		60,632 KB		Desktop Window Manager
ITSMAgent.exe *32	3148	Trusted		16,208 KB	DESKTOP-TTPO9PR...	Endpoint Manager Tray Applica
explorer.exe	3628	Trusted		106,720 KB	DESKTOP-TTPO9PR...	Windows Explorer
MSASCuiL.exe	5532	Trusted		8,396 KB	DESKTOP-TTPO9PR...	Windows Defender notification
OneDrive.exe *32	5624	Trusted		57,500 KB	DESKTOP-TTPO9PR...	Microsoft OneDrive
KillSwitch.exe	5936	Trusted	6.25	274,564 KB	DESKTOP-TTPO9PR...	COMODO Internet Security
icedragon.exe	5956	Trusted		250,148 KB	DESKTOP-TTPO9PR...	IceDragon
icedragon.exe	212	Trusted		227,836 KB	DESKTOP-TTPO9PR...	IceDragon
icedragon.exe	5916	Trusted		81,572 KB	DESKTOP-TTPO9PR...	IceDragon

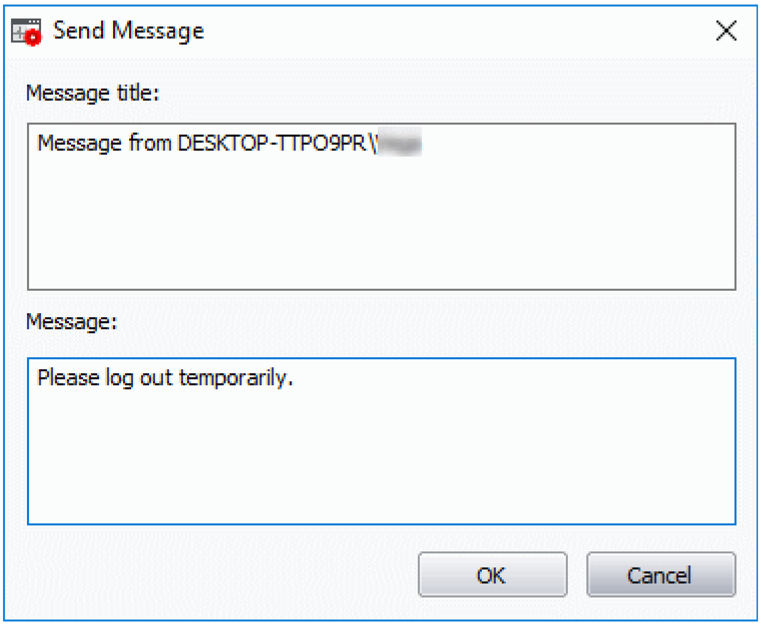
5.7. Manage Currently Logged-in Users

- The 'Users' menu in the file menu bar lists the user(s) that are logged-in to 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).
- Click the 'Users' menu from the file menu bar, to view presently logged-in users.
- Hover the mouse cursor over a user , to open an option menu.



The following options are available:

- **Disconnect -** Enables you to dissociate a user account from your windows session.
- **Log off -** Forcefully sign out the selected user from your computer.
- **Send Message -** Opens a message dialog that enables you to communicate your messages like information, warnings, questions etc. to the selected user.



Message title:

Message from DESKTOP-TTPO9PR\[redacted]

Message:

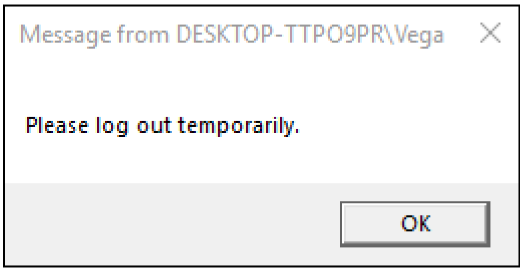
Please log out temporarily.

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.

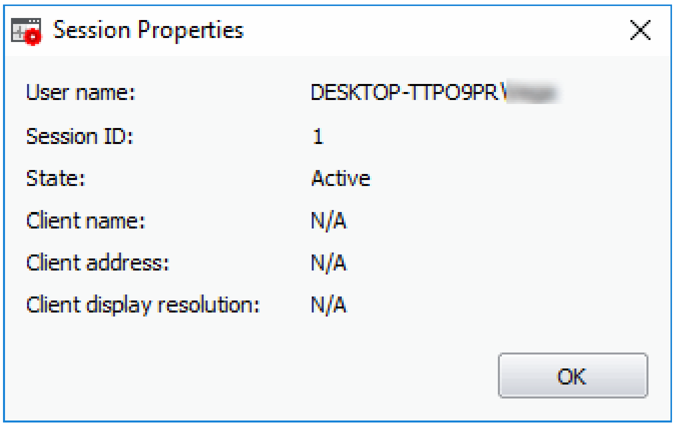
The message will be displayed in the user's desktop.



Message from DESKTOP-TTPO9PR\Vega

Please log out temporarily.

- **Properties** - Provides the user's session information.

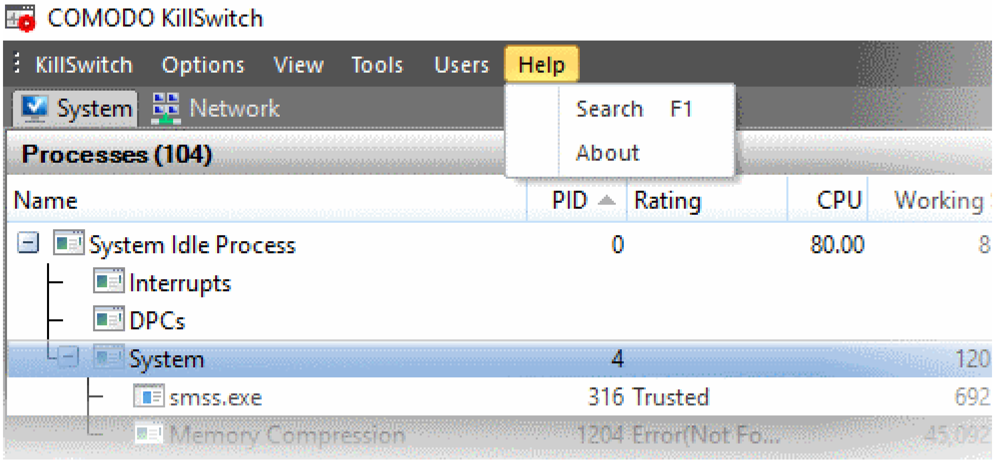


Session Properties

User name:	DESKTOP-TTPO9PR\[redacted]
Session ID:	1
State:	Active
Client name:	N/A
Client address:	N/A
Client display resolution:	N/A

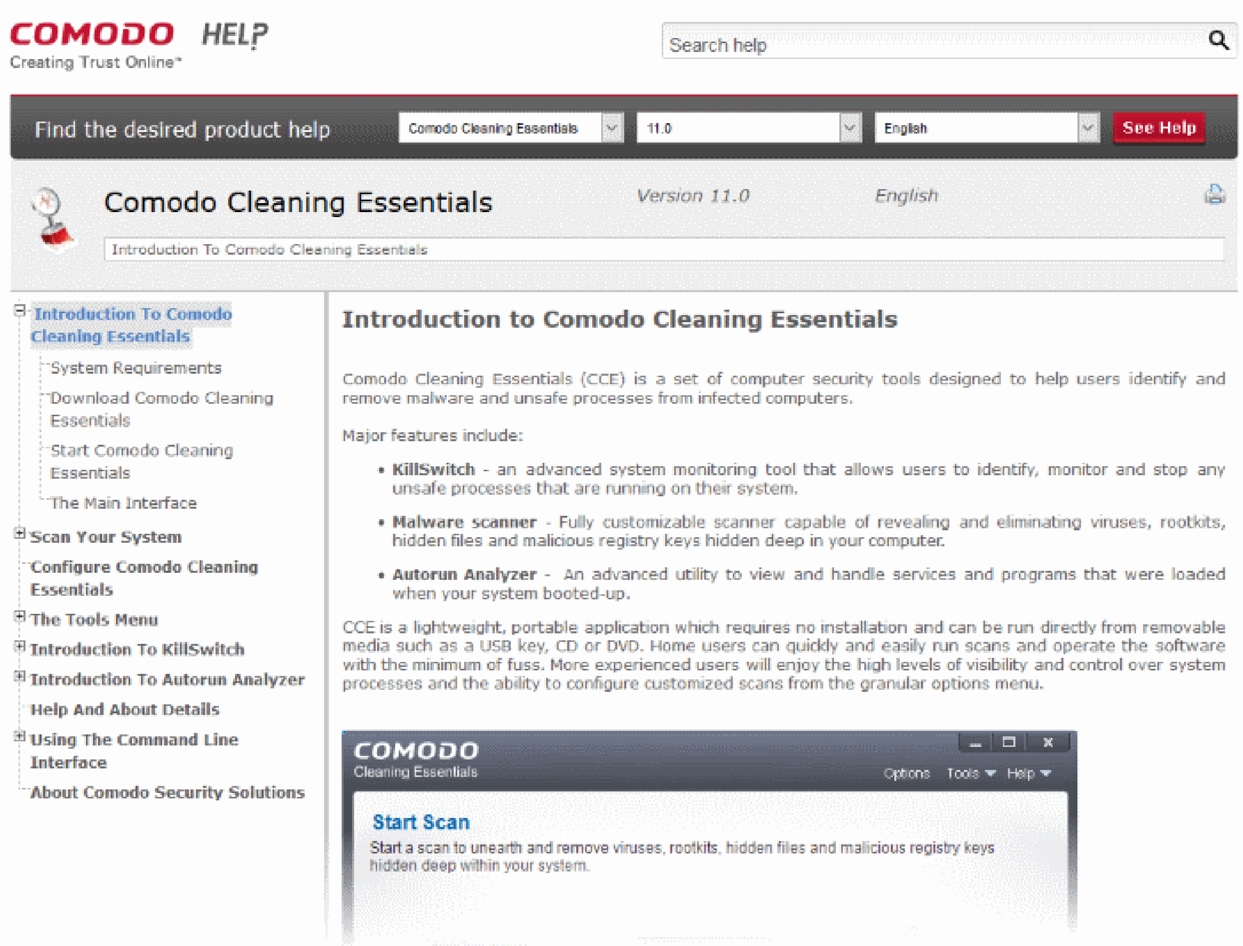
5.8. Help and About Details

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.



Name	PID	Rating	CPU	Working
System Idle Process	0		80.00	8
Interrupts				
DPCs				
System	4			120
smss.exe	316	Trusted		692
Memory Compression	1204	Error(Not Fo...		45,092

The 'Search' option opens the online help guide hosted at **http://help.comodo.com/**. Each area has its own exclusive page containing detailed descriptions of the application's functionality.



COMODO HELP
Creating Trust Online*
Search help
Find the desired product help
Comodo Cleaning Essentials
11.0
English
See Help
Comodo Cleaning Essentials
Version 11.0
English
Introduction To Comodo Cleaning Essentials

Introduction To Comodo Cleaning Essentials
System Requirements
Download Comodo Cleaning Essentials
Start Comodo Cleaning Essentials
The Main Interface
Scan Your System
Configure Comodo Cleaning Essentials
The Tools Menu
Introduction To KillSwitch
Introduction To Autorun Analyzer
Help And About Details
Using The Command Line Interface
About Comodo Security Solutions

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:

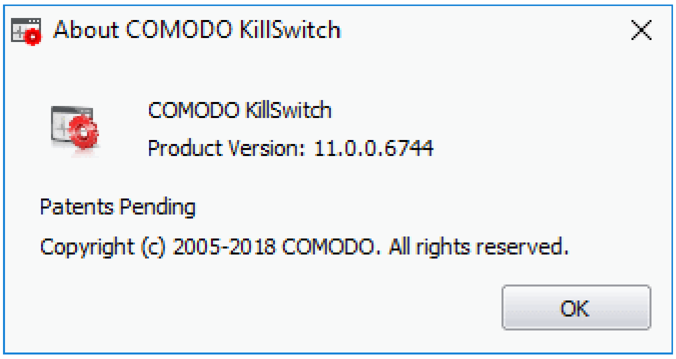
- **KillSwitch** - an advanced system monitoring tool that allows users to identify, monitor and stop any unsafe processes that are running on their system.
- **Malware scanner** - Fully customizable scanner capable of revealing and eliminating viruses, rootkits, hidden files and malicious registry keys hidden deep in your computer.
- **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, CD or DVD. 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 a scan to unearth and remove viruses, rootkits, hidden files and malicious registry keys hidden deep within your system.

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

The 'About' dialog displays the KillSwitch version number and copyright information.



COMODO KillSwitch

Product Version: 11.0.0.6744

Patents Pending

Copyright (c) 2005-2018 COMODO. All rights reserved.

6. Introduction to Autorun Analyzer

- Open CCE > Click 'Tools' > 'Autorun Analyzer'

  OR

- Open the folder containing the CCE files > Run 'autoruns.exe'

An autorun is an executable that automatically starts when you boot your computer. Autoruns include services, drivers, scripts, system files and programs.

- Certain programs and services must be loaded at start-up because they are essential to your computer's security and smooth operation.
- Unfortunately, malware can also add their own start-up items which run in the background as soon as your computer starts.
- The 'Autorun Analyzer' thoroughly checks your start-up items and assigns a trust rating to each one.
- You can then decide precisely which programs and services are allowed to run, and delete malicious and unknown items.

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

- **Introduction to Autorun Analyzer**
  - **Start Autorun Analyzer**
  - **The Main Interface**
- **View and Handle Autorun Items**
  - **Handle Autorun Items**
  - **Filter Entries based on Categories**
  - **View Autorun Items for other User Accounts**
- **Help and About Autorun Analyzer**

6.1. Start Autorun Analyzer

Autorun Analyzer can be started as follows:

- **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

- Open Comodo Cleaning Essentials
- Click 'Tools' > 'Open Autorun Analyzer'