COMODO
Creating Trust Online®

Comodo Rescue Disk

Software Version 1.1

User Guide

Guide Version 1.1.072312

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

Table of Contents

1.Introduction to Comodo Rescue Disk

Comodo Rescue Disk (CRD) is a bootable disk image that allows users to run virus scans in a pre-boot environment (before Windows loads). CRD runs Comodo Cleaning Essentials on a lightweight distribution of the Linux operating system. It is a powerful virus, spyware, rootkit scanner and cleaner which works in both GUI and text mode. The tool can provide a more comprehensive and thorough scan than regular malware cleaning applications because it cleans your system before Windows is loaded. CRD is intended to be used when malware embeds itself so deeply into your system that regular AV software cannot remove it. The rescue disk is also very effective at removing infections that are preventing Windows from booting in the first place. Apart from the virus scanner, CRD also provides tools to explore files in your hard drive, take screenshot and browse web pages.

Main Features:

- **Smart Scan** – Quick scan on the critical areas in your system
- **Full Scan** – Scans all areas in your system including partitions and system memory
- **Custom Scan** - Scans only the selected files and folders

Guide Structure

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

- Section 1 - **Introduction to Comodo Rescue Disk**, 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.
  - **Downloading Comodo Rescue Disk** - A brief outline of the download procedure.
  - **Starting Comodo Rescue Disk** - How to boot your system using CRD.
  - **CCE Interface** - Description of menus and options in the main interface.
- Section 2, **Scanning your System**, explains the various methods of scanning your computer.
  - **Smart Scan** - Explains how to run a scan on critical areas of your system.
  - **Full Scan** - Explains how to run a full scan of your system.
  - **Custom Scan** - Explains how to scan on selected items.
  - **Comparison of Scan Types** – Provides details on scanners used and the scan sequences followed for different

types of scans in CCE.

- Section 3, **Configuring Comodo Cleaning Essentials** - Explains how to configure the overall behavior of the CCE.
- Section 4, **The Tools Menu** – Explains how to use the tools in CCE.
  - **Managing Quarantined Items** - How to manage and restore quarantined files.
  - **Importing Antivirus Database** – How to import virus database from local storage or from network computer.
  - **Checking for Software Updates** - How to manually check for program updates.

1.1. Downloading Comodo Rescue Disk

Comodo Rescue Disk is an ISO image file and can be downloaded from the following path:

http://download.comodo.com/crd/download/setups/comodo_rescue_disk_1.1.232326.14.iso

After downloading the image file, burn it to a CD or DVD so that it becomes a bootable disk. CRD bootable disk can be used for both 32 and 64 bit systems.

1.2. Starting Comodo Rescue Disk

Since CRD is bootable disk image, you need to change the boot order in your system. Click on the following links for more details:

- **Changing boot order**
- **Booting to and starting Comodo Rescue Disk**

1.2.1. Changing boot order

To boot your computer to CRD, you need to make sure the BIOS is set to boot from the correct drive (either CD/DVD or USB depending on where you placed the ISO). In most cases, this will require you to manually prioritize the CD/DVD/USB as the boot drive ahead of your usual C: drive. To make this change, you first have to access your computer's BIOS configuration utility. While the specifics vary from computer to computer, the following steps should be of use to most users:

- Place the CD/DVD in your drive or insert the USB key as appropriate
- Shut down your computer. Note – do a full shut down. A soft restart will not clear memory and the BIOS setup might not appear.
- Turn your computer back on and be ready to react quickly. During system start up, you will see a message similar to one of the following:
  - Press <key> to enter setup

    Or
  - Press <key> to open bios configuration utility

    Or
  - Press <key> to change boot order

It is usually one of the F1 – F12 keys or the DEL key (F2 and DEL are popular). Quickly press whichever key you are requested to press. If you miss it this time, simply try again by shutting down then starting your computer.

- Having hit the correct key, the bios configuration utility will start. Look for an entry that states 'Boot Order', 'Change Boot Order', 'Change Boot Sequence' or similar. Select it and press enter.
- Use the arrow keys to select the CD/DVD drive or USB port that you wish to boot from. If you are shown a sequential boot order, make sure CD/DVD/USB (as applicable) is first on the list.
- Save and exit. Your machine should automatically reboot to the CRD drive, allowing you to use the program.

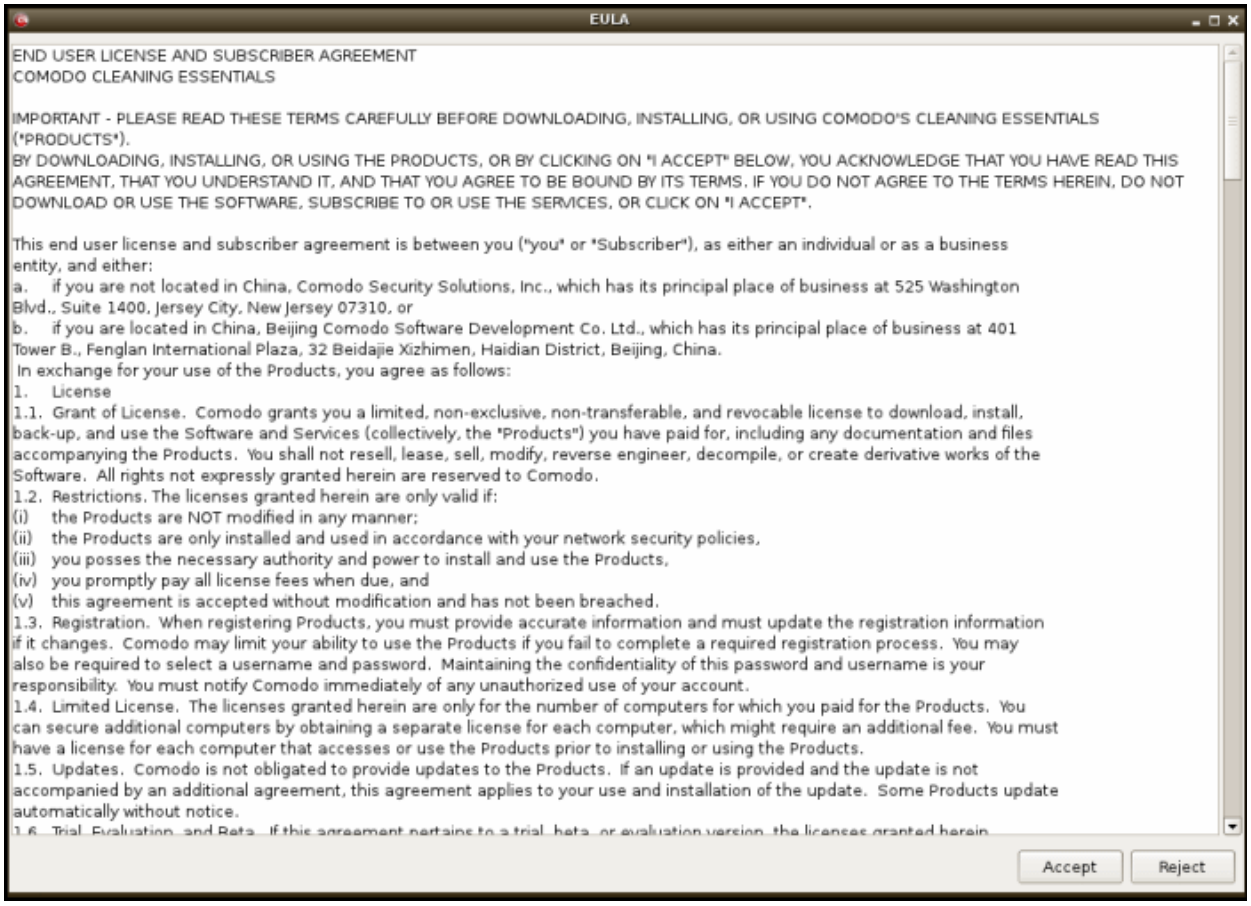
Note – if these instructions do not help then please consult your system manufacturer's website (or call their support) for more details on how to change boot order.

1.2.2. Booting to and starting Comodo Rescue Disk

Having successfully booted your computer to the required drive, Comodo Rescue disk will open at the following screen:

You have a choice of using either Graphic mode or Text mode. By default, the Graphic mode will be selected and if you want to use the Text mode, press the down-arrow in your keyboard and press the Enter button. If you do not select Text mode within 10 seconds, your system will automatically enter the Graphic mode.

Next, the End User License and Subscriber Agreement screen will be displayed.



- Read the agreement and click 'Accept'.

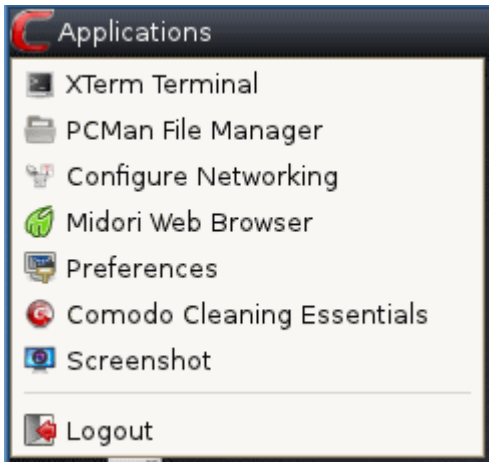
The CRD desktop will be displayed and Comodo Cleaning Essentials (CCE) starts automatically...

...and is ready for the scan process.

Start the **scan process** of your choice or click the 'Exit' button to scan your system at a later time. The CRD desktop will be displayed.

CRD uses Linux OS and you have the following options in the desktop:

Applications



- **Xterm Terminal** - Used for entering commands
- **PCMan File Manager** - Used for navigating to your files and drives
- **Configure Networking** - Opens Netbox Manager for advanced network configuration
- **Midori Web Browser** - Used for browsing the internet if connection is available
- **Comodo Cleaning Essentials** - Opens the CCE interface for scanning your system
- **Screenshot** - Takes a picture of the current process in the screen
- **Logout** - Provides a choice to Logout X session, Shutdown computer or Reboot system

1.3. Starting Comodo Cleaning Essentials

After you have **booted your system** with CRD, you can start CCE in the Applications menu or by double-clicking the CCE icon in the CRD desktop.

- In the Applications menu, click on Comodo Cleaning Essentials.

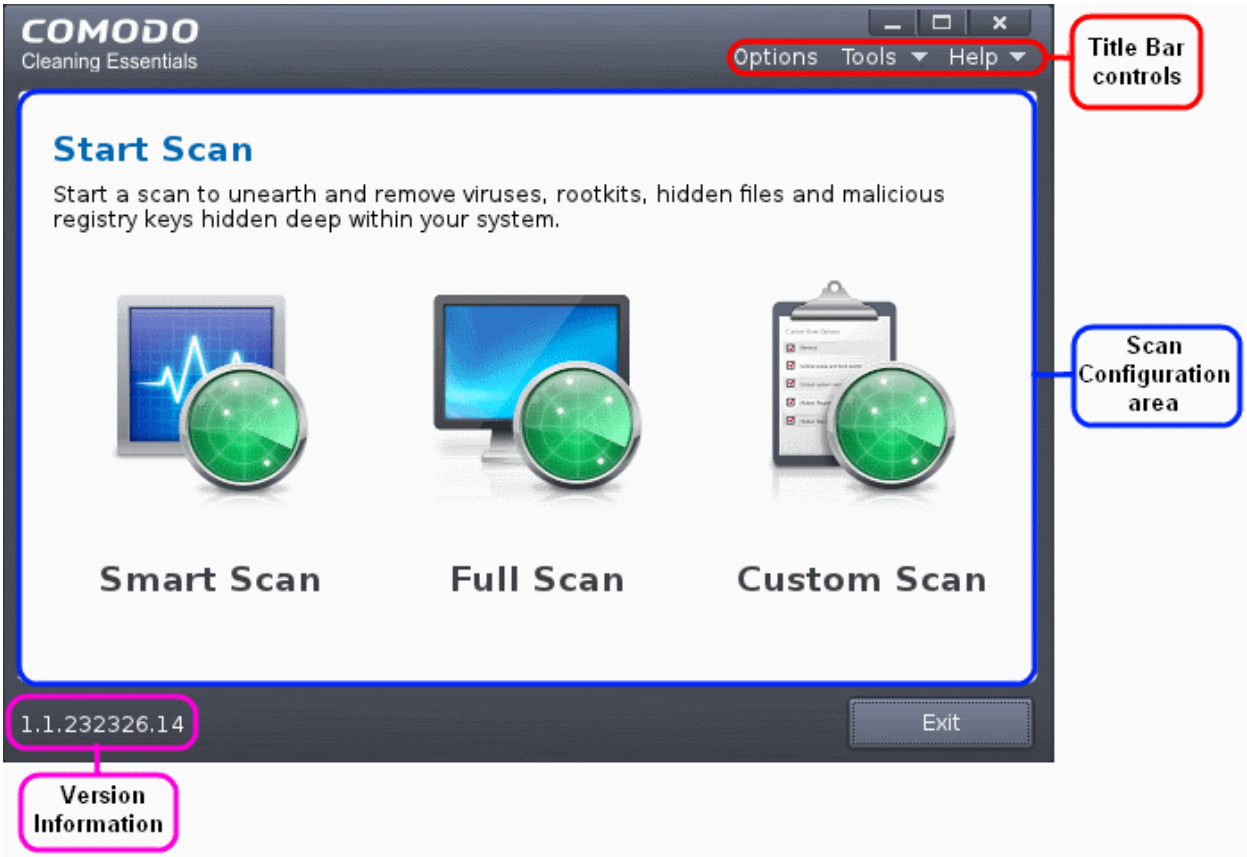
Or

- In the CRD desktop, double-click on the CCE icon 

The CCE interface will open.

1.4. CCE Interface

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



The main interface CCE has the following areas:

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

Scan Configuration Area

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

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

Title Bar Controls

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

- **Options** - Allows you to configure various settings in the application.
- **Tools** - Allows you to manage Quarantined items, import virus database, browse log files and check for updates.
- **Help** - Launches the online help guide

Version Information

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

2.Scanning Your System

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

Customized scanning is very useful if you want to scan only a particular file/folder/drive or if you have installed a program and suspect it may be infected. You can also scan an individual folder or a file you just downloaded from Internet or copied into your system instantly by dragging and dropping it over the CCE interface.

Refer to the following sections for more details on:

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

2.1.Smart Scan

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

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

On completion of scanning, you can:

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

To start a Smart scan

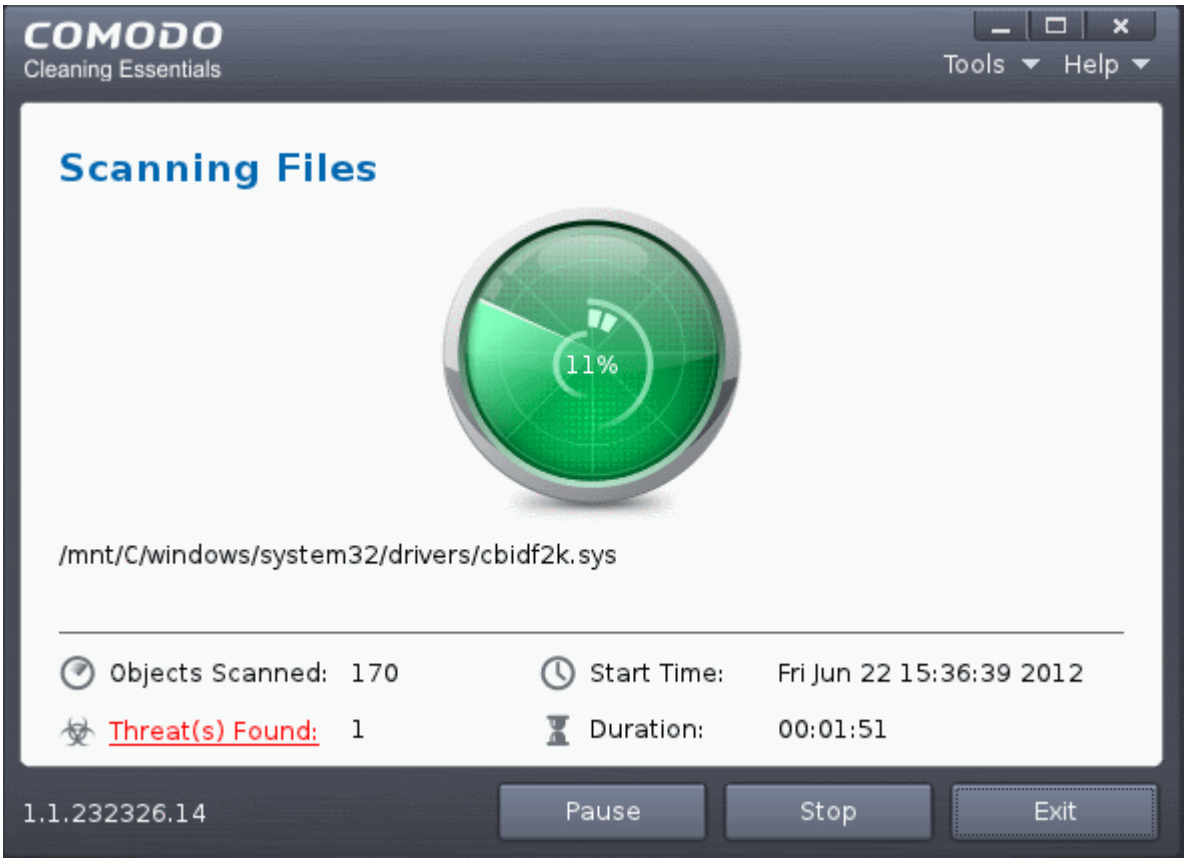
1. Click the 'Smart Scan' from the CCE main interface.

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

It is advised that you always let the application to update the database as scanning with your virus database up-to-date detects

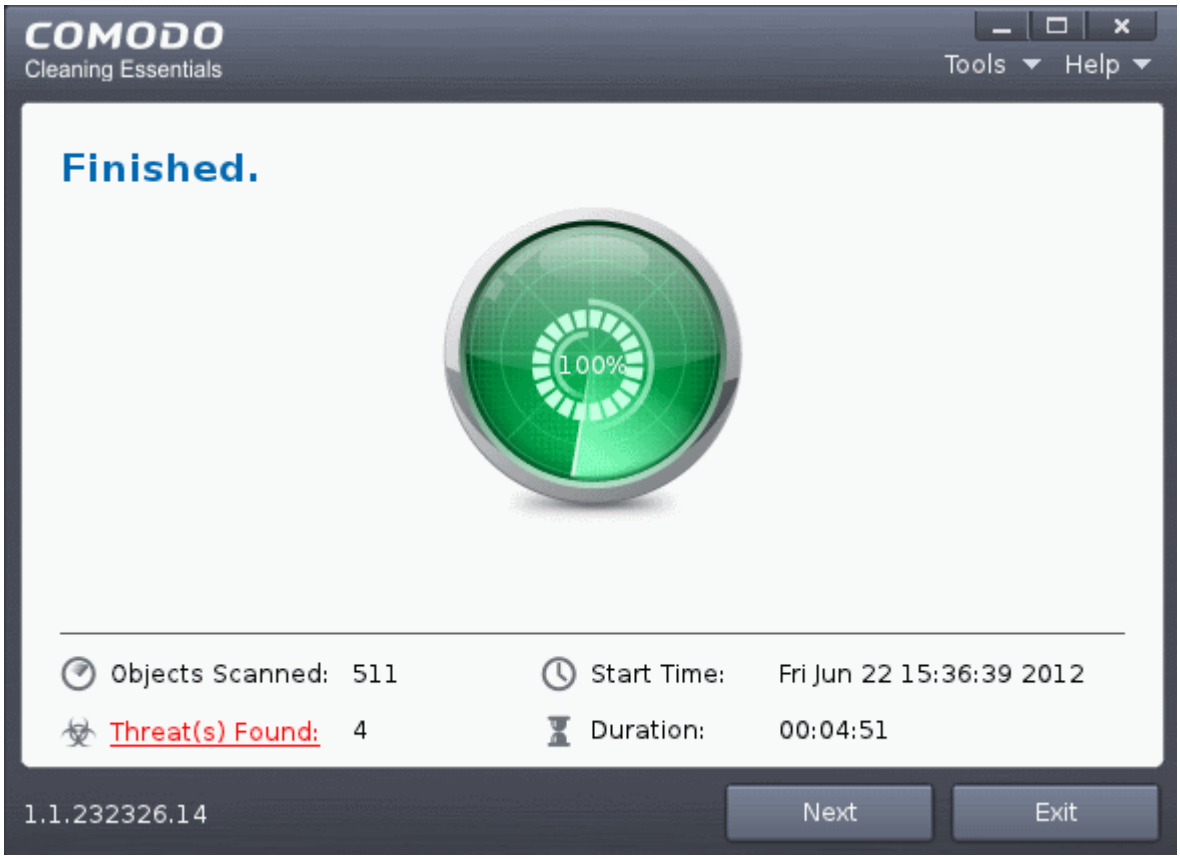
even the zero-hour threats. However, if you do not want the database update at this moment, you can skip this step by clicking 'Skip'.

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

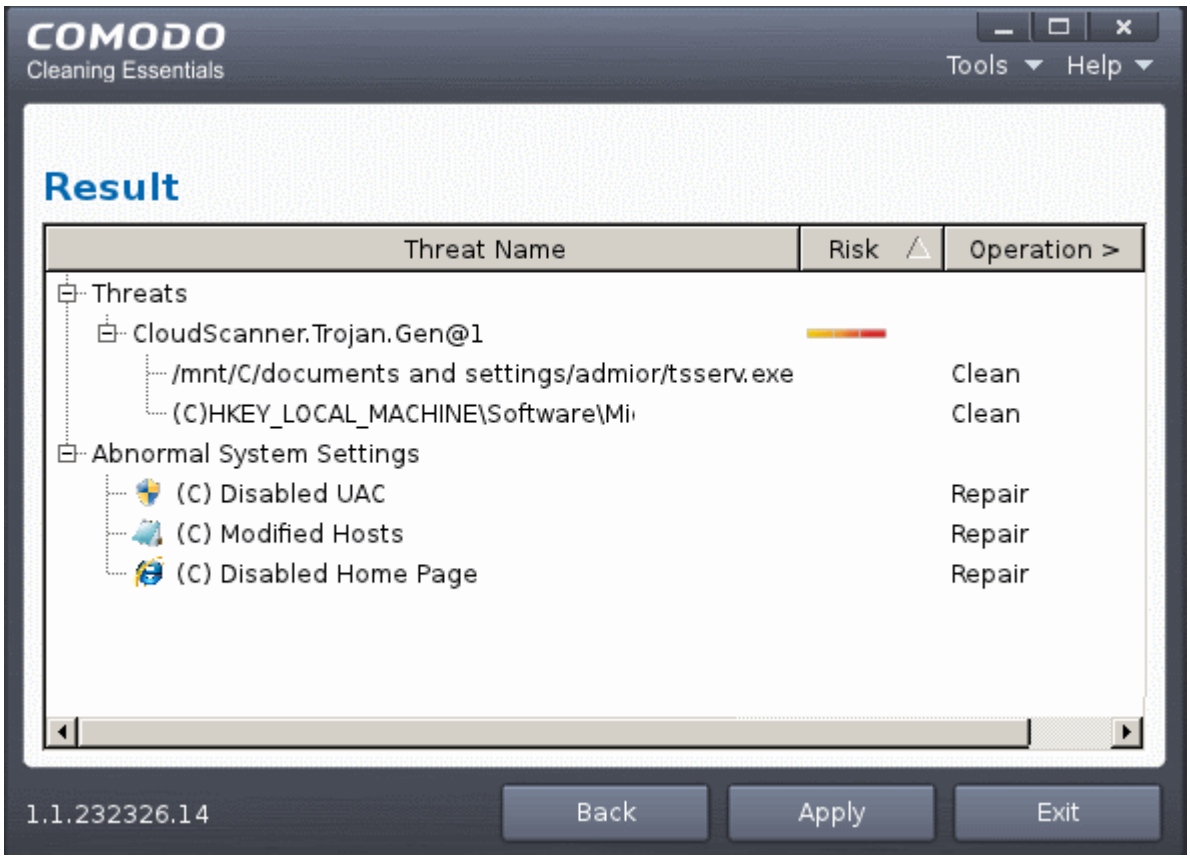


During the course of scanning, if you want to see details on the threats detected so far, click Threats Found link. A results window with the threats identified thus far will be displayed.

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



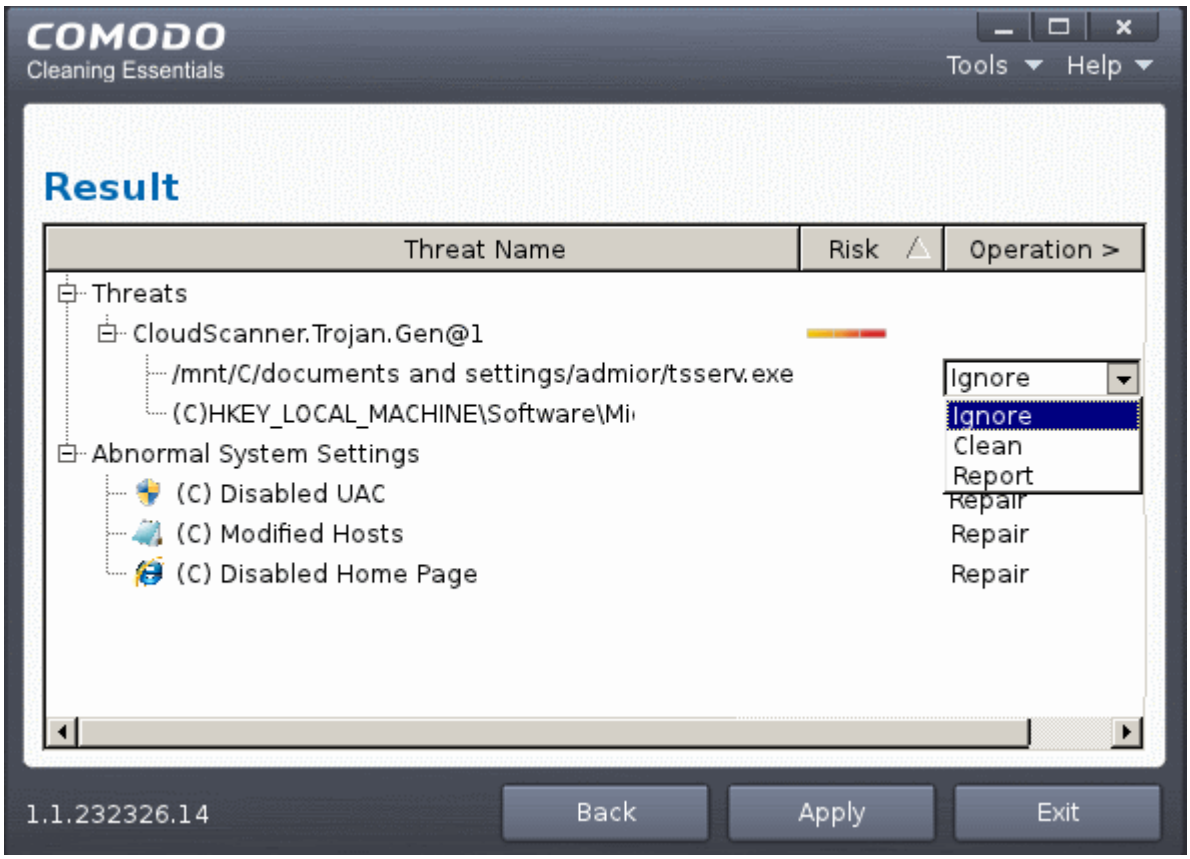
2. Click 'Next' to view the results.



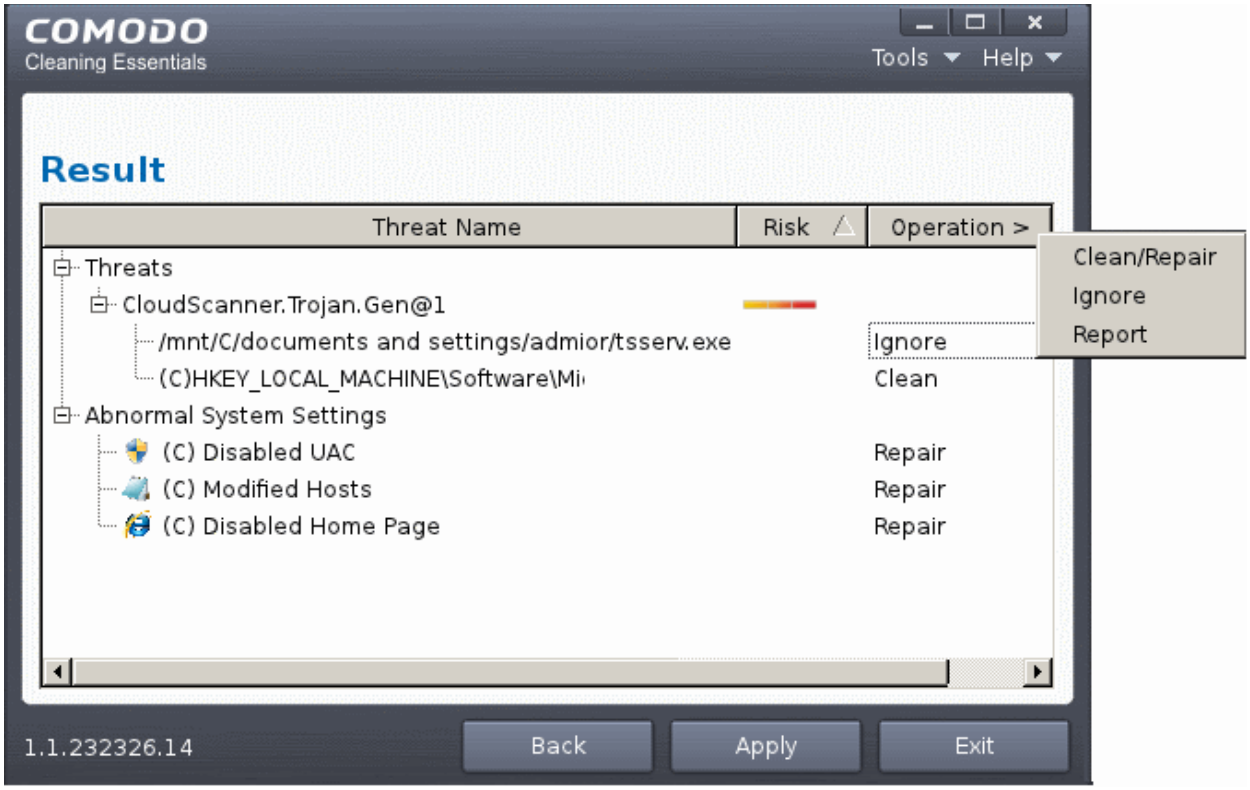
- If malicious executables or abnormal system settings are discovered on your system, the 'Results' window displays the list of those items (Viruses, Malware and so on).

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

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



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



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

If you have opted to use the **text mode**, scroll to 'Smart Scan' by using the down or up arrow and click the 'Enter' button.

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

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

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

For each and every malware detected by CCE, a 'Choose Action to Virus Detected' screen will be displayed.

The 'Results' screen allows you to quarantine and later remove, ignore the threat if it is a safe file or to submit it as a false positive to Comodo if you are sure about the authenticity of the file. The default operation is 'Clean All', that means CCE will clean the threat if a disinfection routine is available for it, else, will move it to quarantine. For abnormal system settings, you have the option to either repair the setting or ignore.

- To clean a threat, select 'Clean' using the left or right arrows and press the 'Enter' key. The file will be disinfected or moved to quarantine upon applying the operation. You can later remove the file from your system from the 'Quarantined Items' interface. Refer to **Managing Quarantined Items** for more details.
- To ignore a threat if you consider the file is safe, select 'Ignore' using the left or right arrows and press the 'Enter' button.
- To report threat as a false-positive result, select 'Report' using the left or right arrows and press the 'Enter' key. The file will be sent to Comodo. Experts in Comodo will analyze the file and add it to whitelist, if found safe.

2.2. Full Scan

It is essential to run a full scan of your system periodically to detect any malware or viruses. During a full scan, CCE scans all areas including all partitions of hard disk drive, system memory of your computer to identify threats from viruses, malware, spyware and so on.

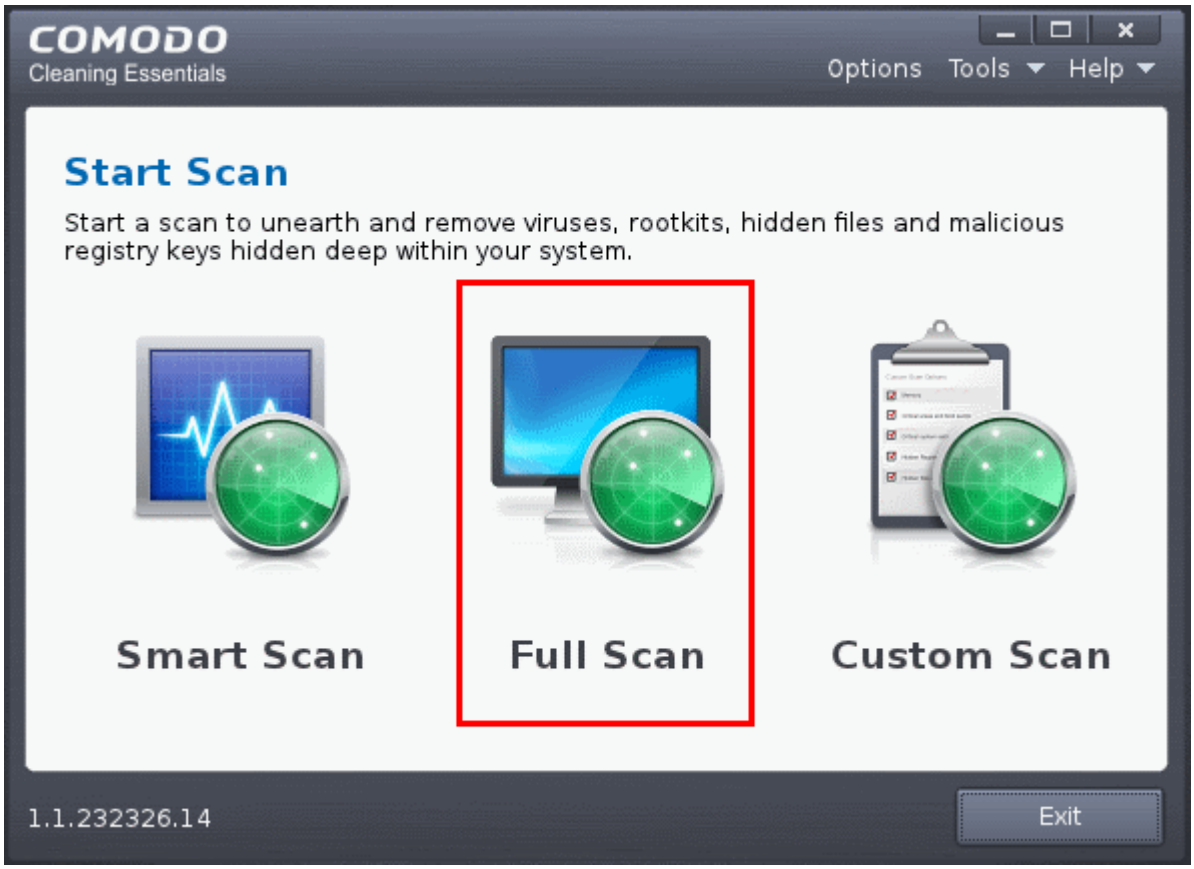
A rootkit is a type of malware that is designed to conceal the fact that the user's system has been compromised. Once installed, they camouflage themselves as, for example, standard operating system files, security tools and APIs used for diagnosis, scanning, and monitoring. Rootkits are usually not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

On completion of scanning, you can:

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

To start a Full scan

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



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

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

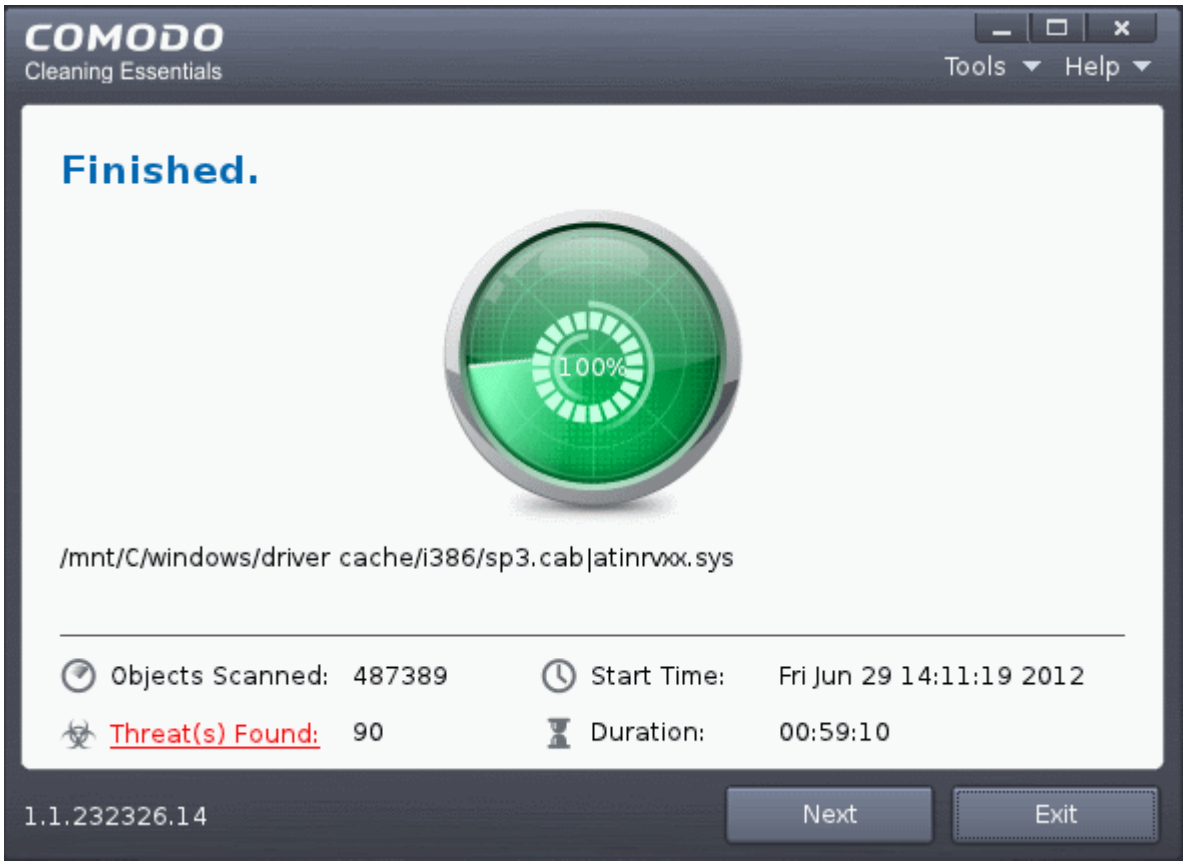
'Skip'.

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

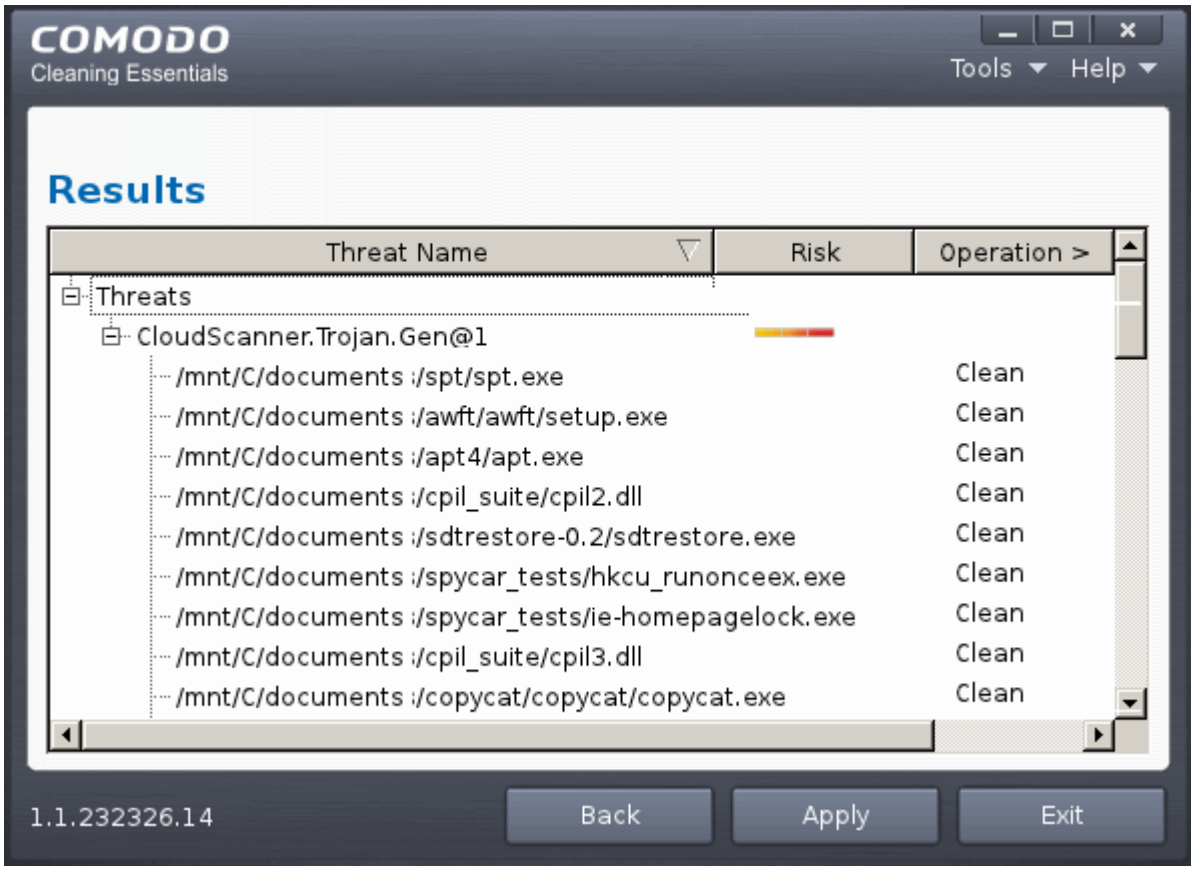
During the course of scanning, if you want to see details on the threats detected so far, click 'Threat(s) Found' link. A results window with the threats identified thus far will be displayed.

The Results

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



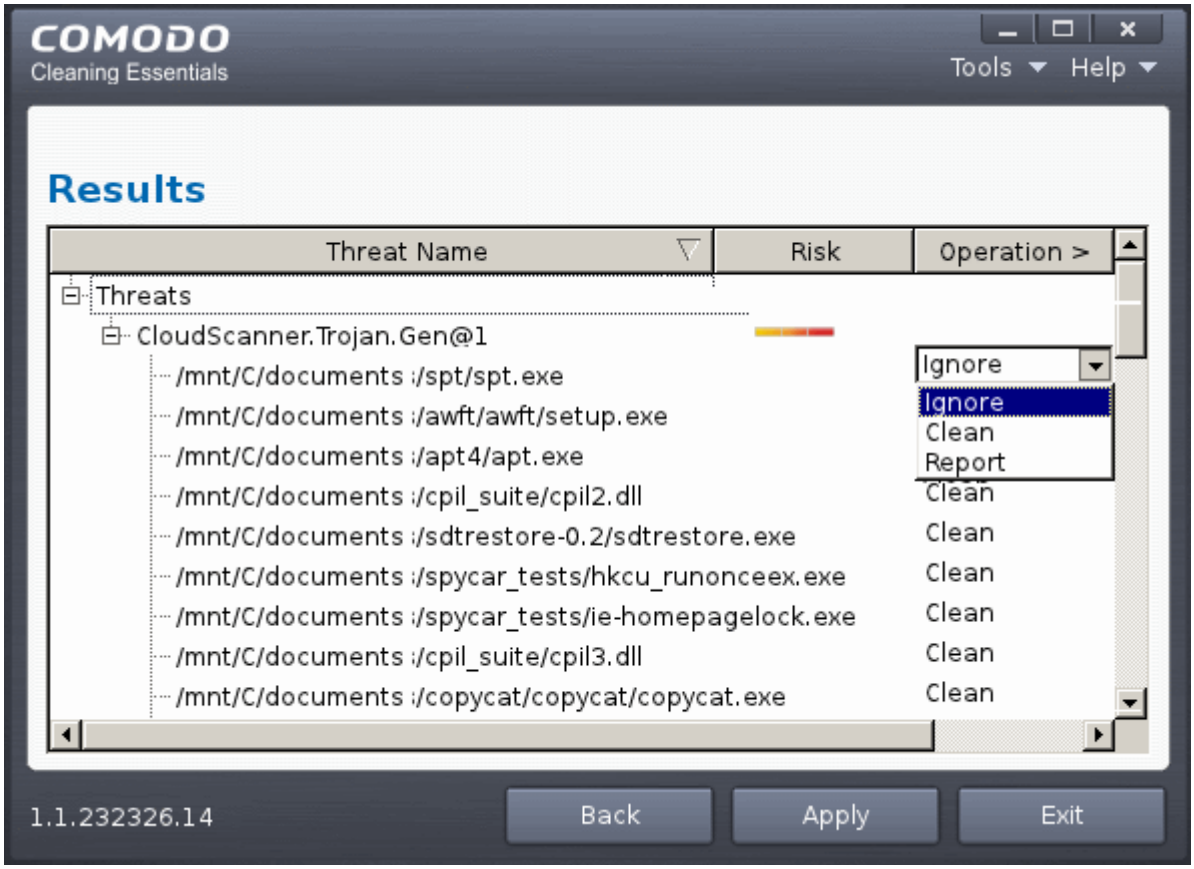
2. Click 'Next' to view the results.



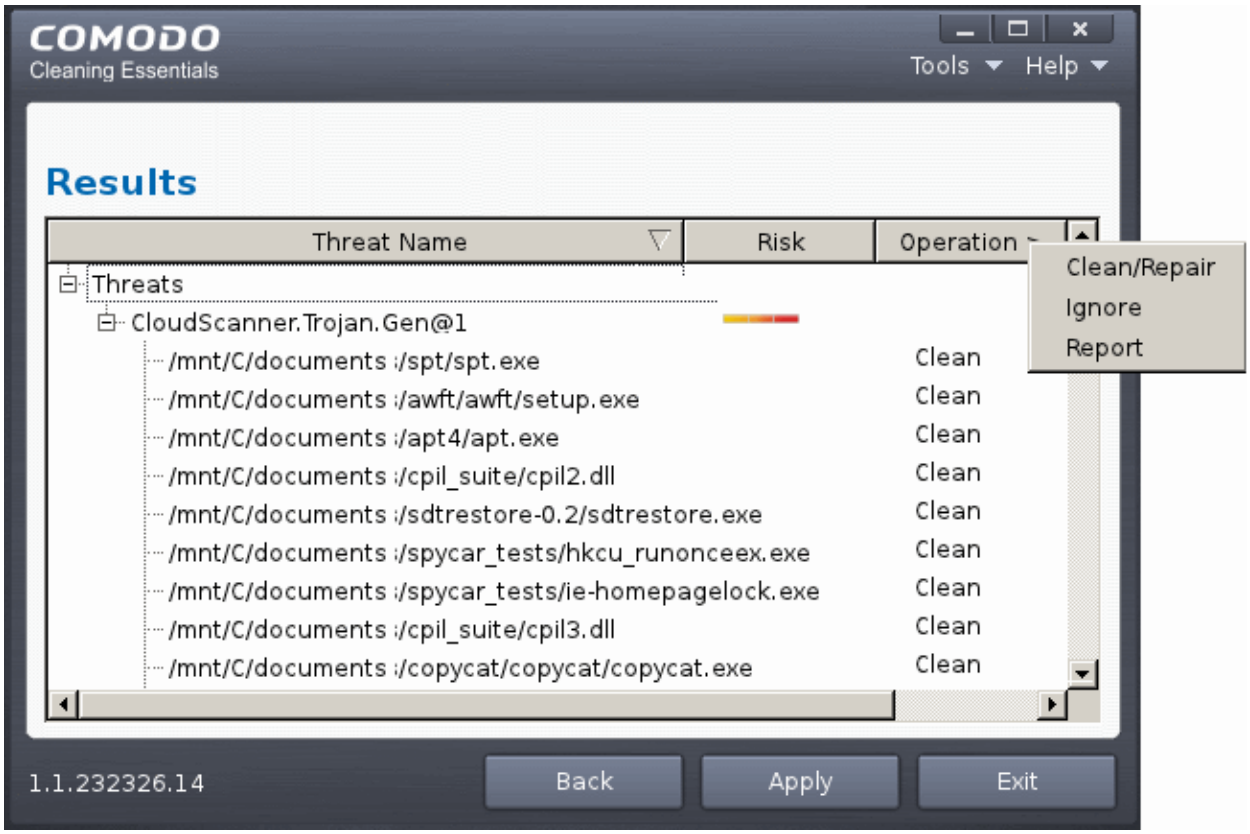
- If malicious executables are discovered on the scanned areas, the 'Results' window displays the list of those items (Viruses, Malware and so on).

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

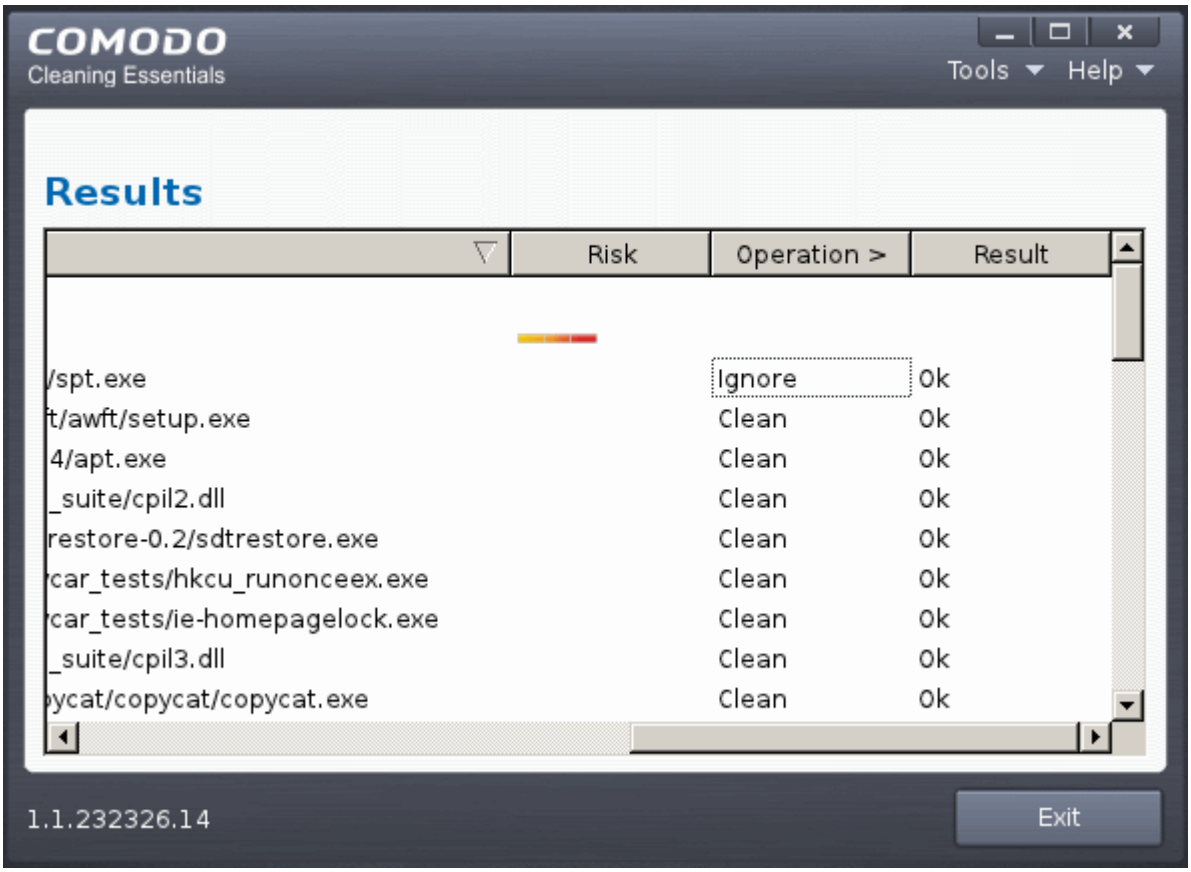
The 'Results' window allows you to quarantine and later remove, ignore the threat if it is a safe file or to submit it as a false positive to Comodo if you are sure about the authenticity of the file. The default operation is 'Clean', that means CCE will clean the threat if a disinfection routine is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



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

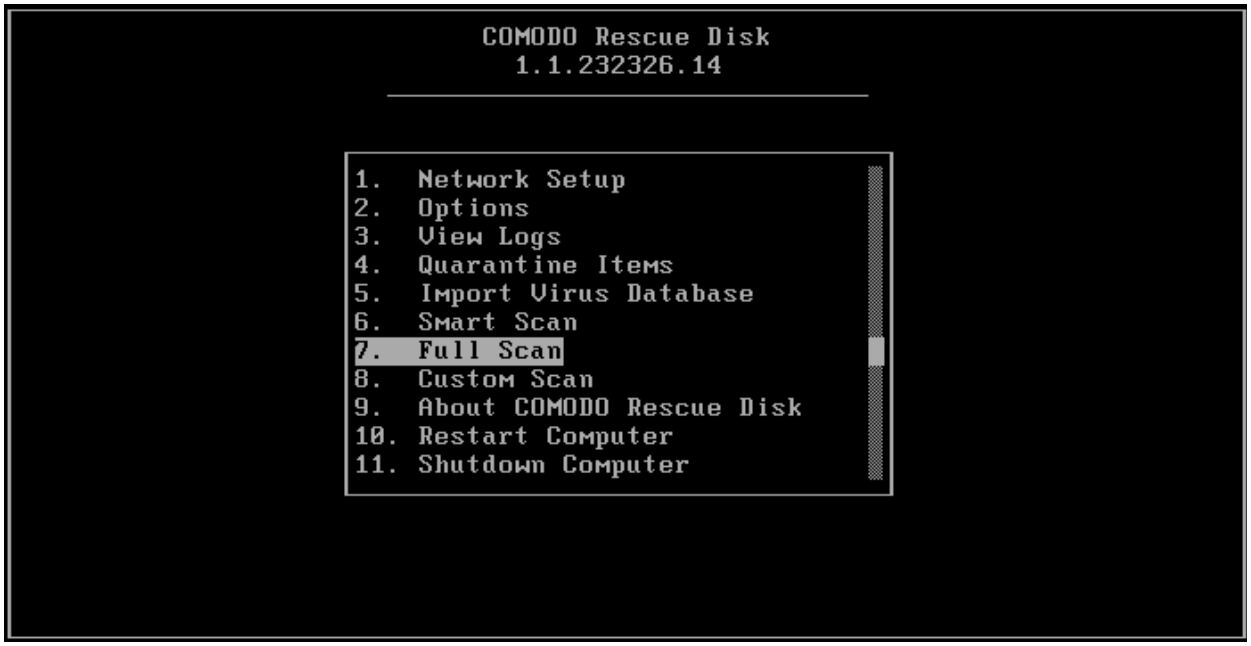


3. Click 'Apply' to apply the selected operations to the threats. The selected operations will be applied and the results will be displayed.

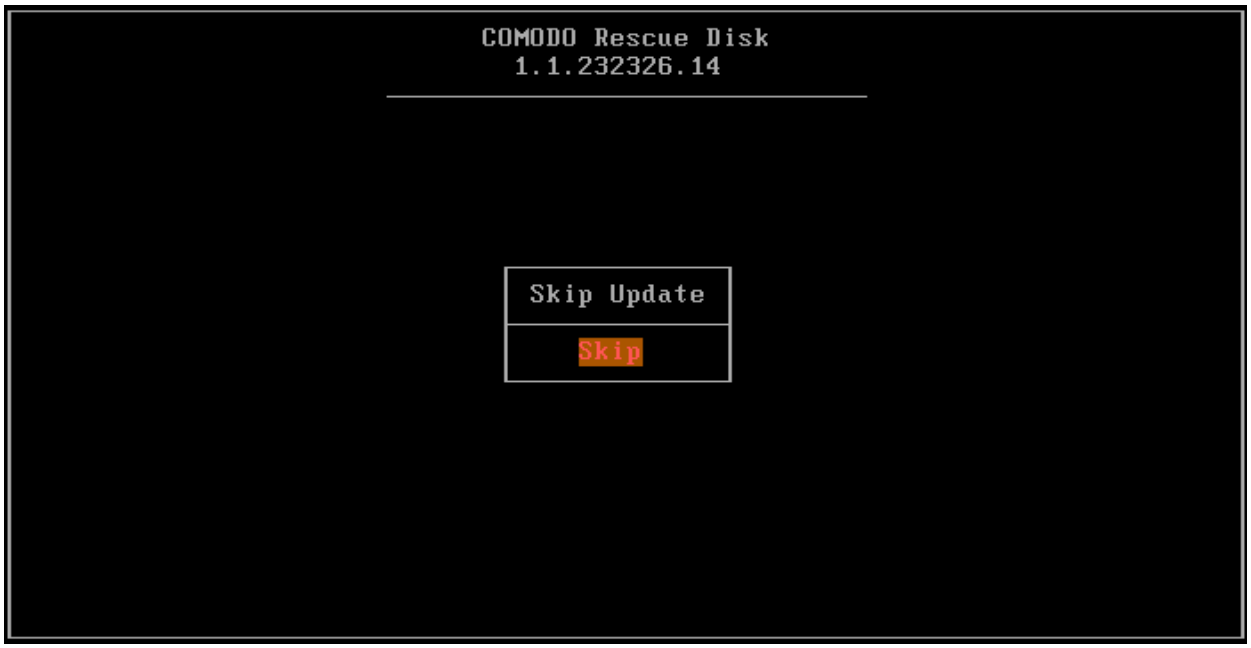


4. Click 'Exit'.

If you have opted to use the **text mode**, scroll to 'Full Scan' by using the down or up arrow and click the 'Enter' button.



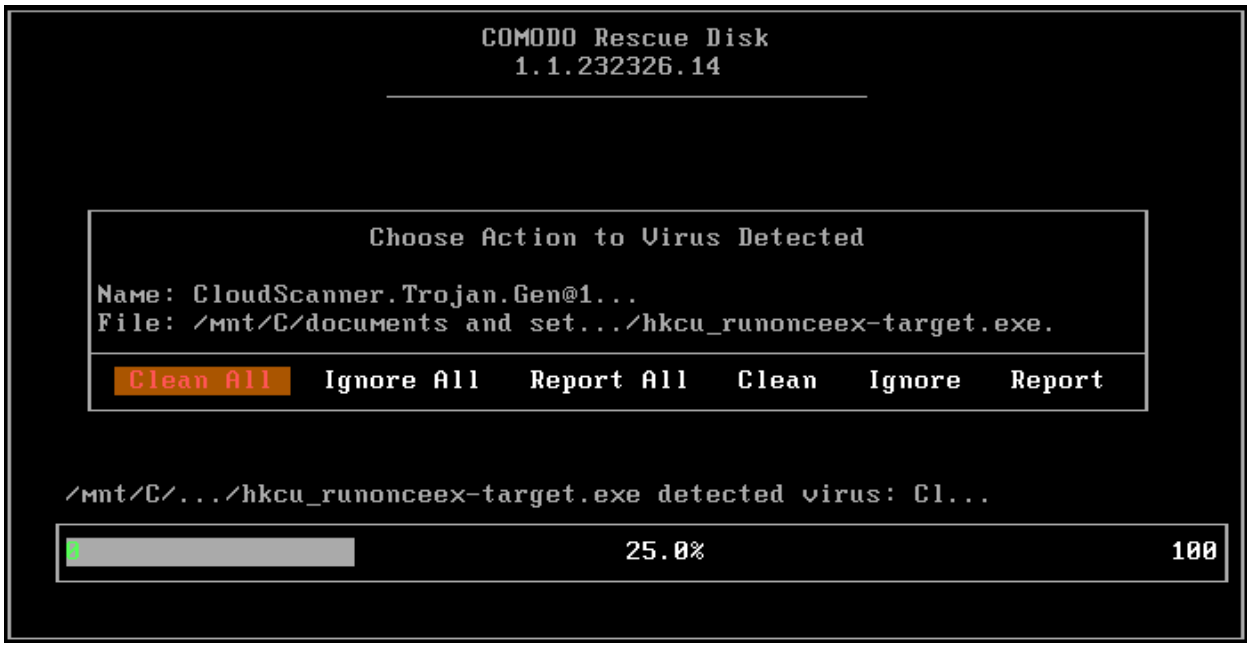
The application will check whether any updates are available for the virus database before commencing the scan. If available, it will first update the local virus database.



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

The application will start scanning the selected areas of your system and the progress will be displayed. Press 'Ctrl+C' buttons to abort the scan.

For each and every malware detected by CCE, a 'Choose Action to Virus Detected' screen will be displayed.



The 'Results' screen allows you to quarantine and later remove, ignore the threat if it is a safe file or to submit it as a false positive to Comodo if you are sure about the authenticity of the file. The default operation is 'Clean All', that means CCE will clean the threat if a disinfection routine is available for it, else, will move it to quarantine. For abnormal system settings, you have the option to either repair the setting or ignore.

- To clean a threat, select 'Clean' using the left or right arrows and press the 'Enter' key. The file will be disinfected or moved to quarantine upon applying the operation. You can later remove the file from your system from the 'Quarantined Items' interface. Refer to **Managing Quarantined Items** for more details.
- To ignore a threat if you consider the file is safe, select 'Ignore' using the left or right arrows and press the 'Enter' button.
- To report threat as a false-positive result, select 'Report' using the left or right arrows and press the 'Enter' key. The file will be sent to Comodo. Experts in Comodo will analyze the file and add it to whitelist, if found safe.

2.3. Custom Scan

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

Custom Scan is relatively agile scan method. You can choose what would you want to scan, and where would you want to scan.

On completion of scanning, you can:

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

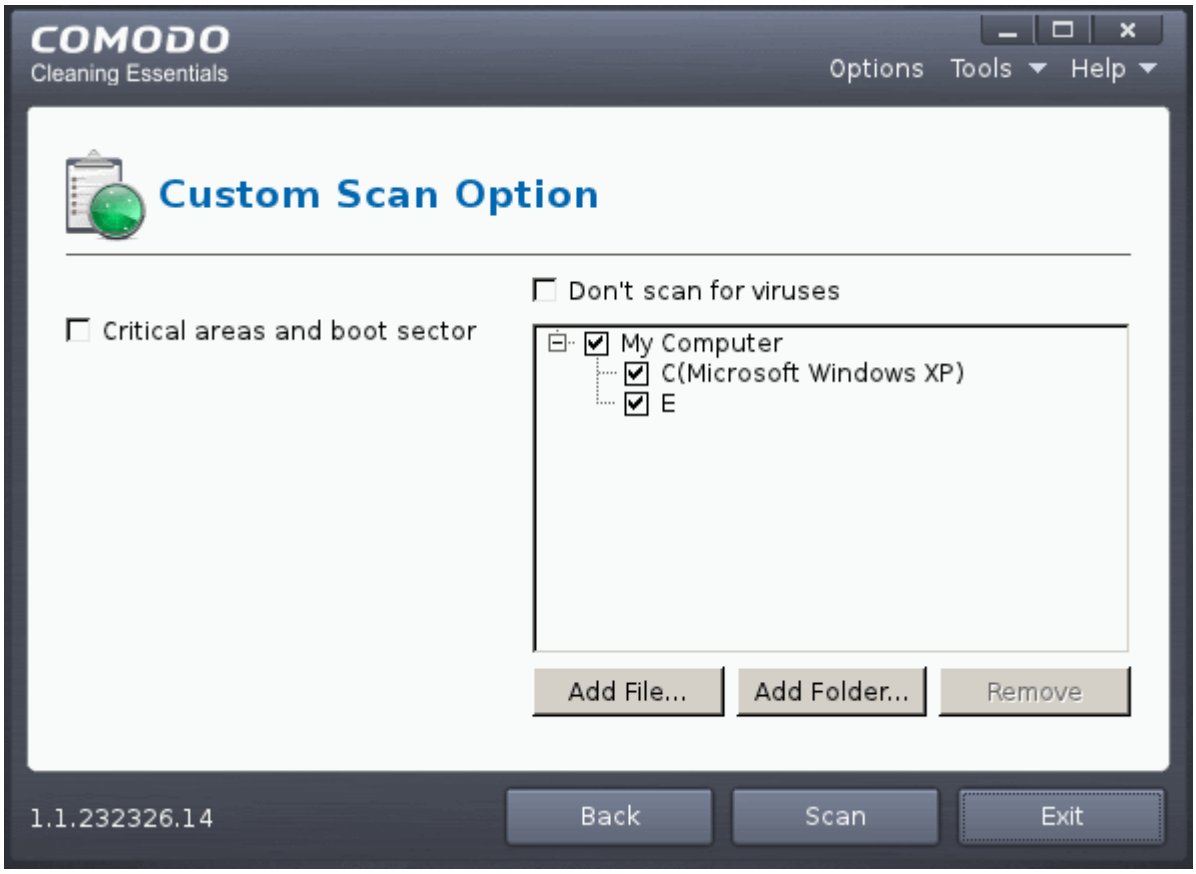
Comodo Cleaning Essentials allows you to:

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

Starting a Custom Scan

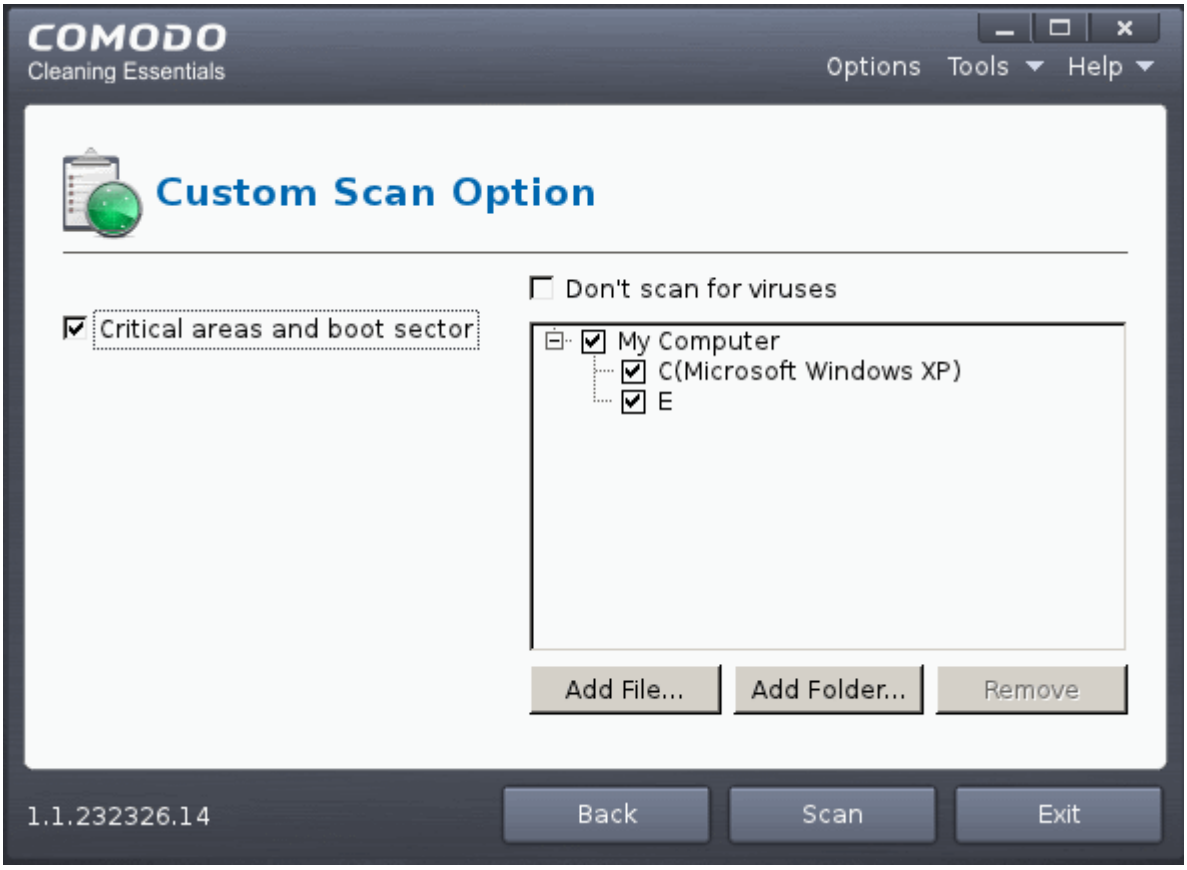
1. Click the 'Custom Scan' from the CCE main interface.

The Custom Scan Setting dialog window will be displayed.



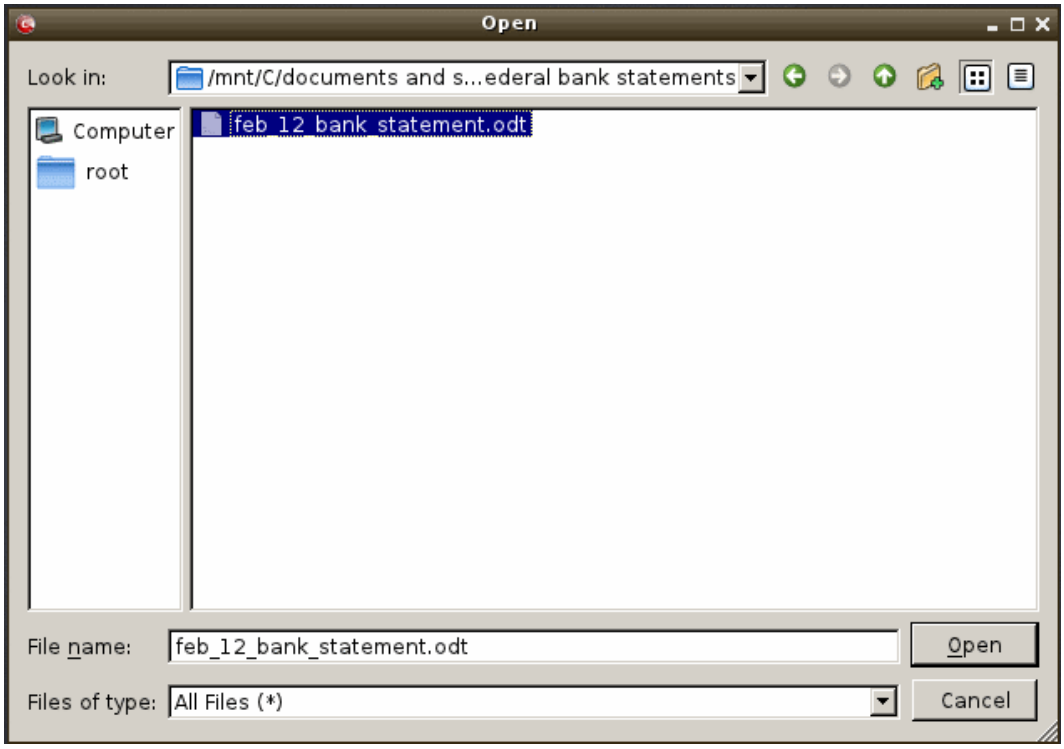
You can select which options you prefer for the custom scan and also choose which specific files, folders or drives are to be included in the scan in the Scan Target area.

2. Choose the Scan Options
    - **Critical areas and Boot Sector** - When selected, CCE scans the Program Files folder and WINDOWS folder of the Operating System of your computer and the Boot Sector of your hard disk drive during the start of any custom scan.
    - **Don't scan for viruses** - When selected, CCE will not check for viruses in the target areas as specified by the above options. This option is only for scanning the above said areas and not on any target areas in your hard disk drive. Hence, the target selection area will become inactive and grayed out.
3. Choose the scan target area(s). By default, all the drives in your system will be selected for custom scan.

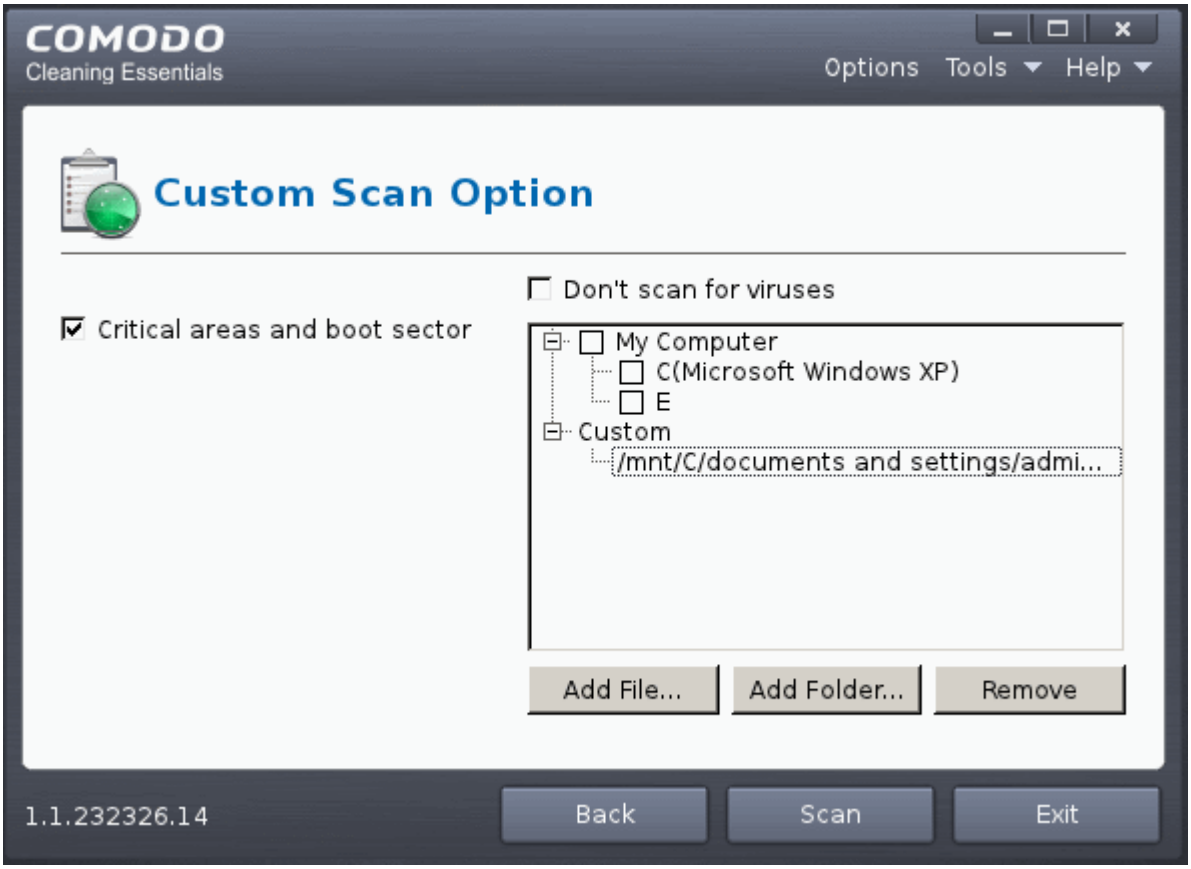


To add file(s)

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



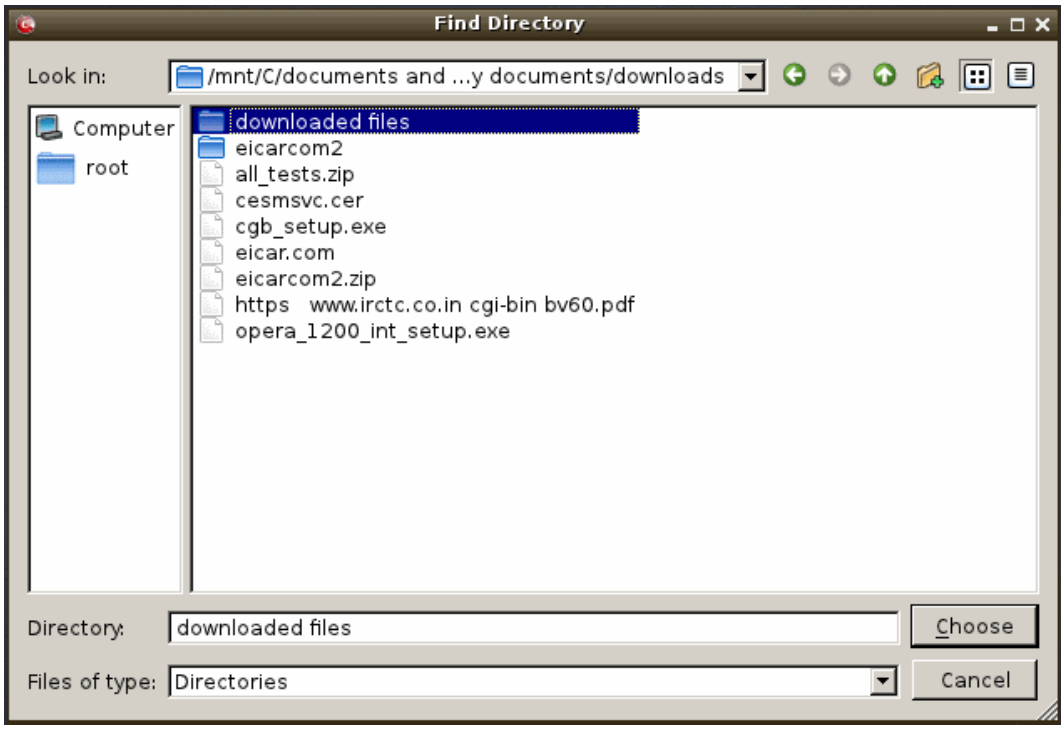
The selected file will be added to the custom Scan Target area.



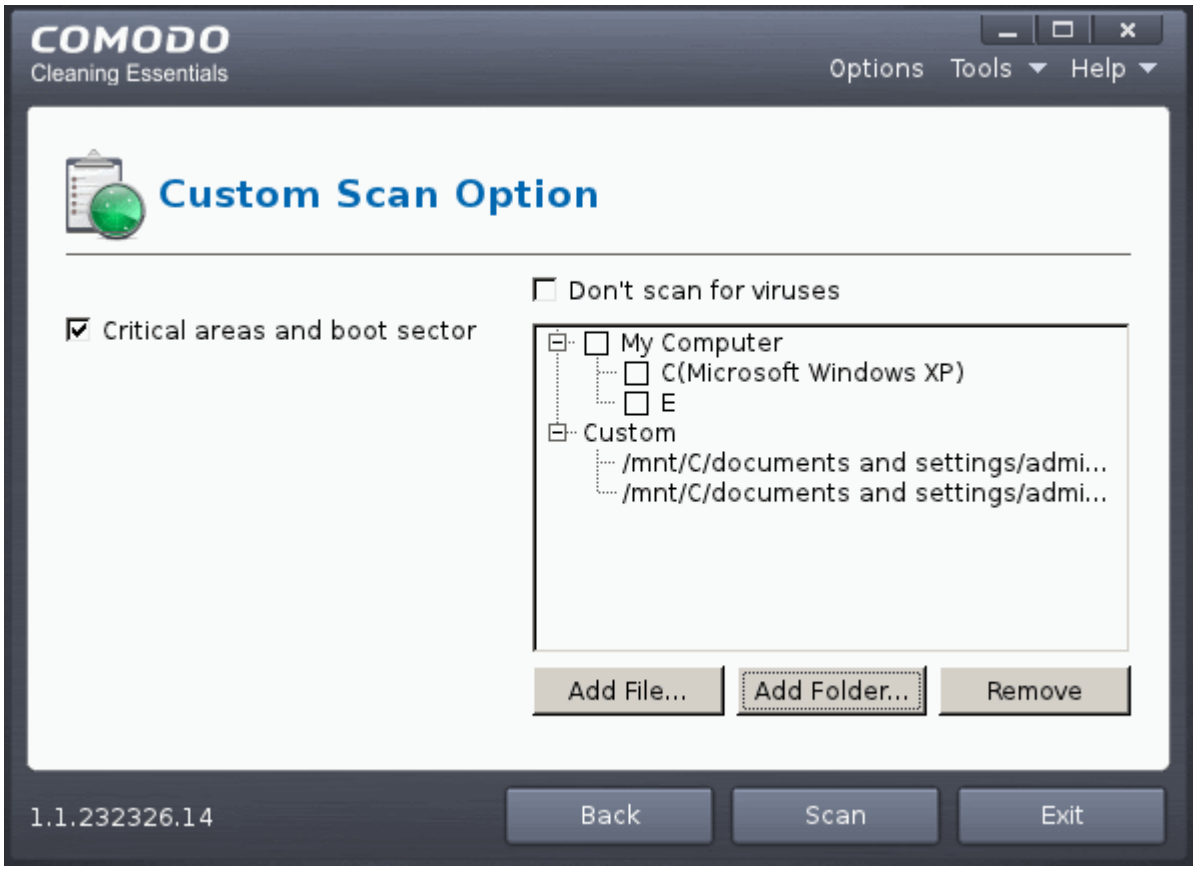
- You can add more files and folders for a simultaneous custom scan. Repeat the process to add more files.

To add Folder(s):

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

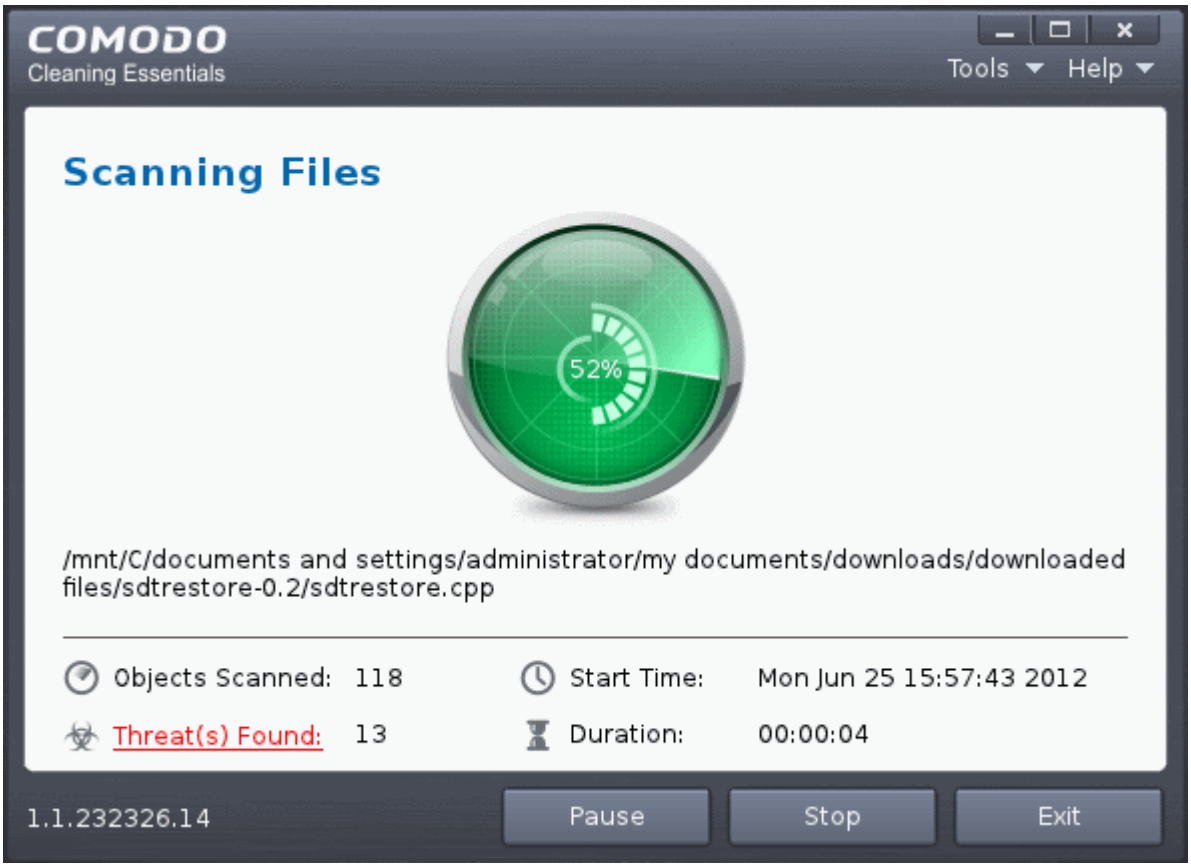


The selected folder will be added to the custom Scan Target area.



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

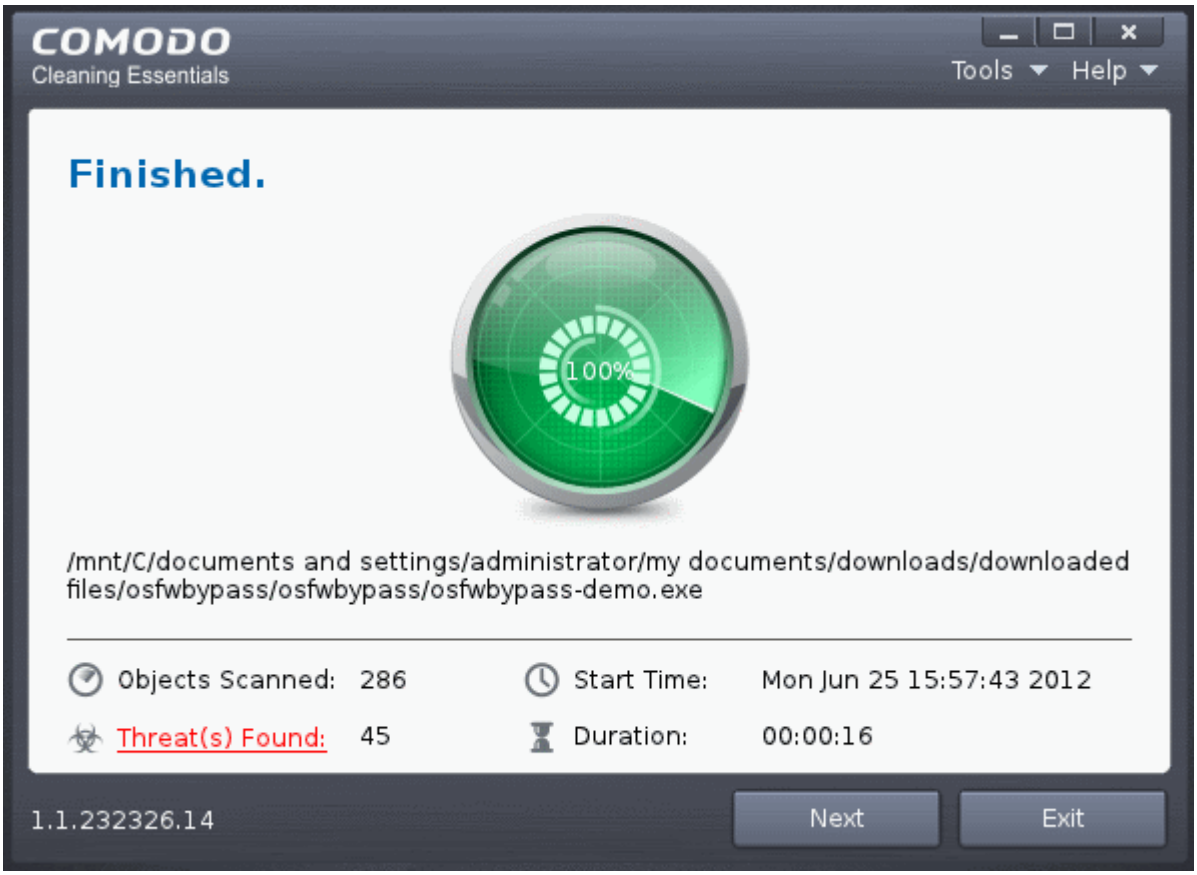
4. Click 'Scan' to run the custom scan. The selected file(s)/Folder(s) will be scanned with the scan options and the progress will be displayed.



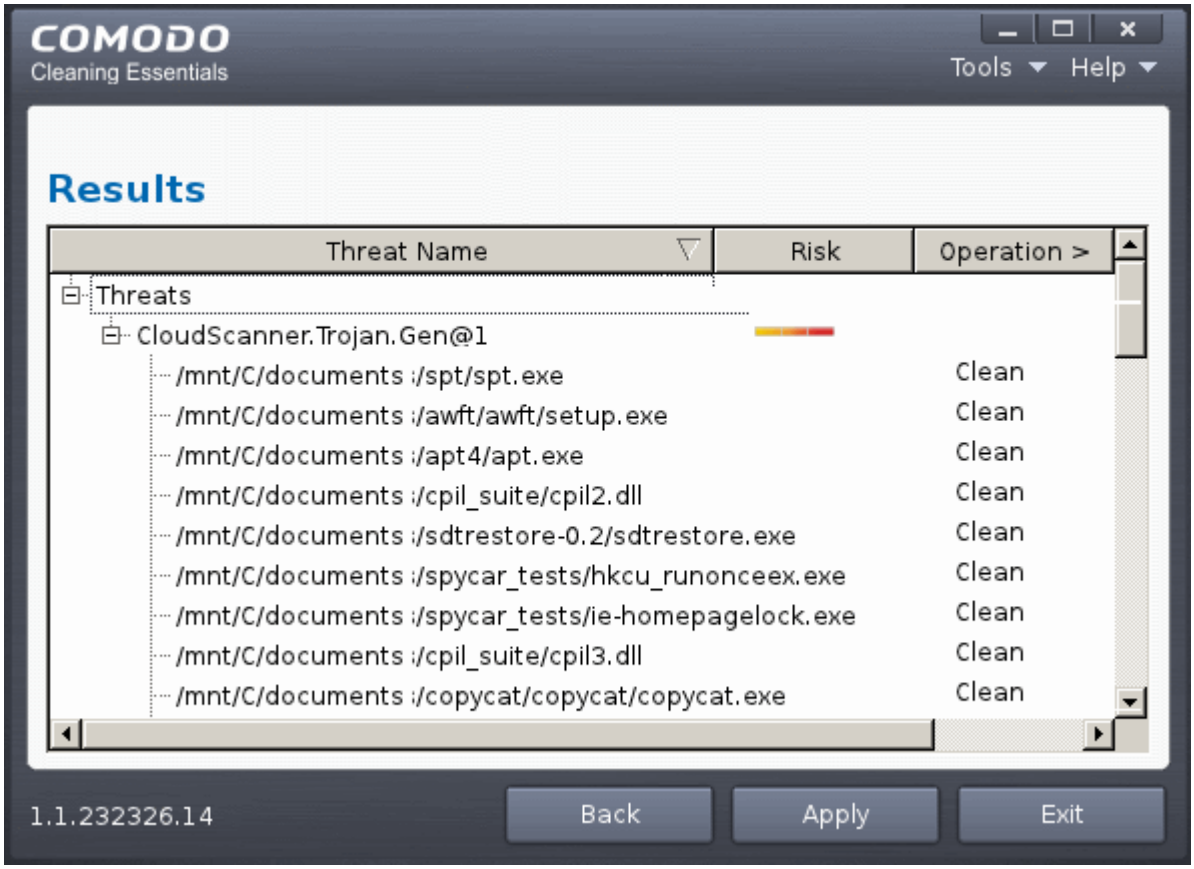
During the course of scanning, if you want to see details on the threats detected so far, click 'Threat(s) Found' link. A results window with the threats identified thus far will be displayed.

The Results

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



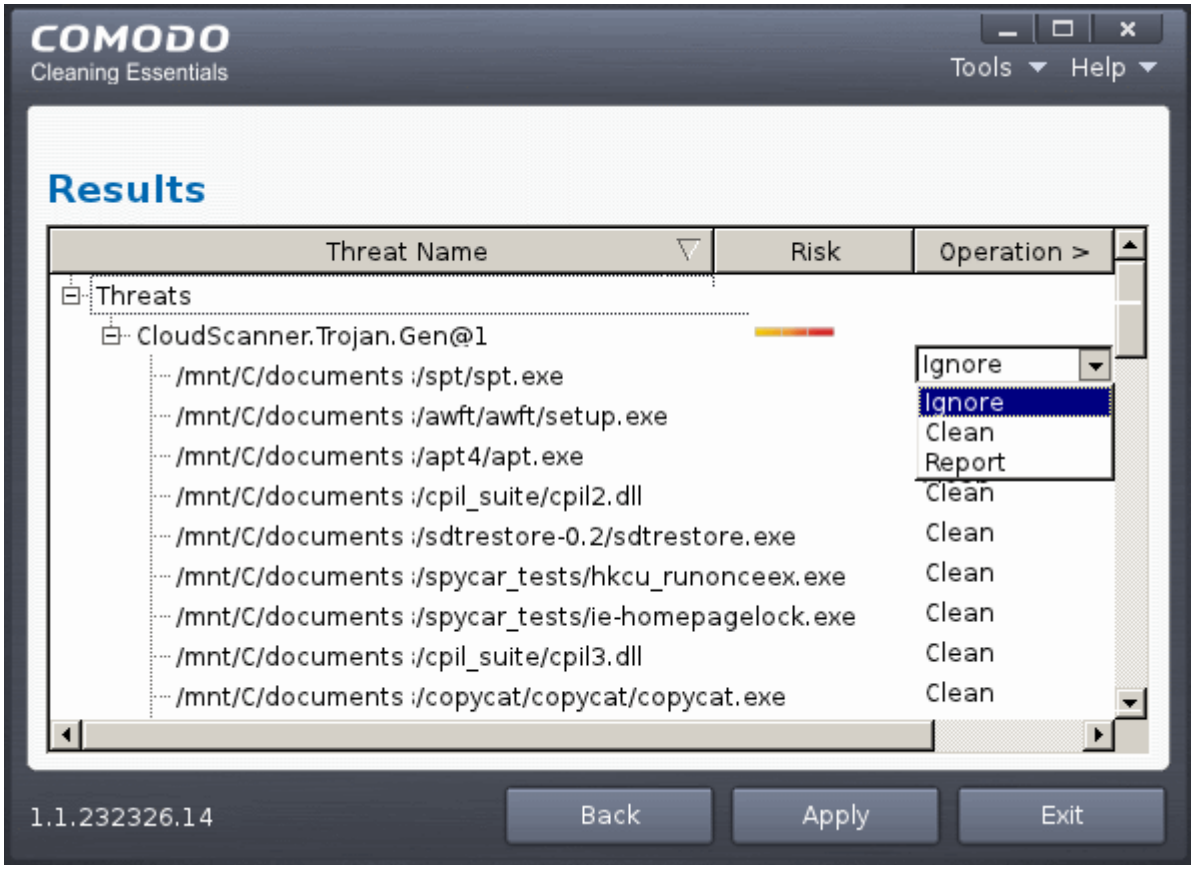
5. Click 'Next' to view the results.



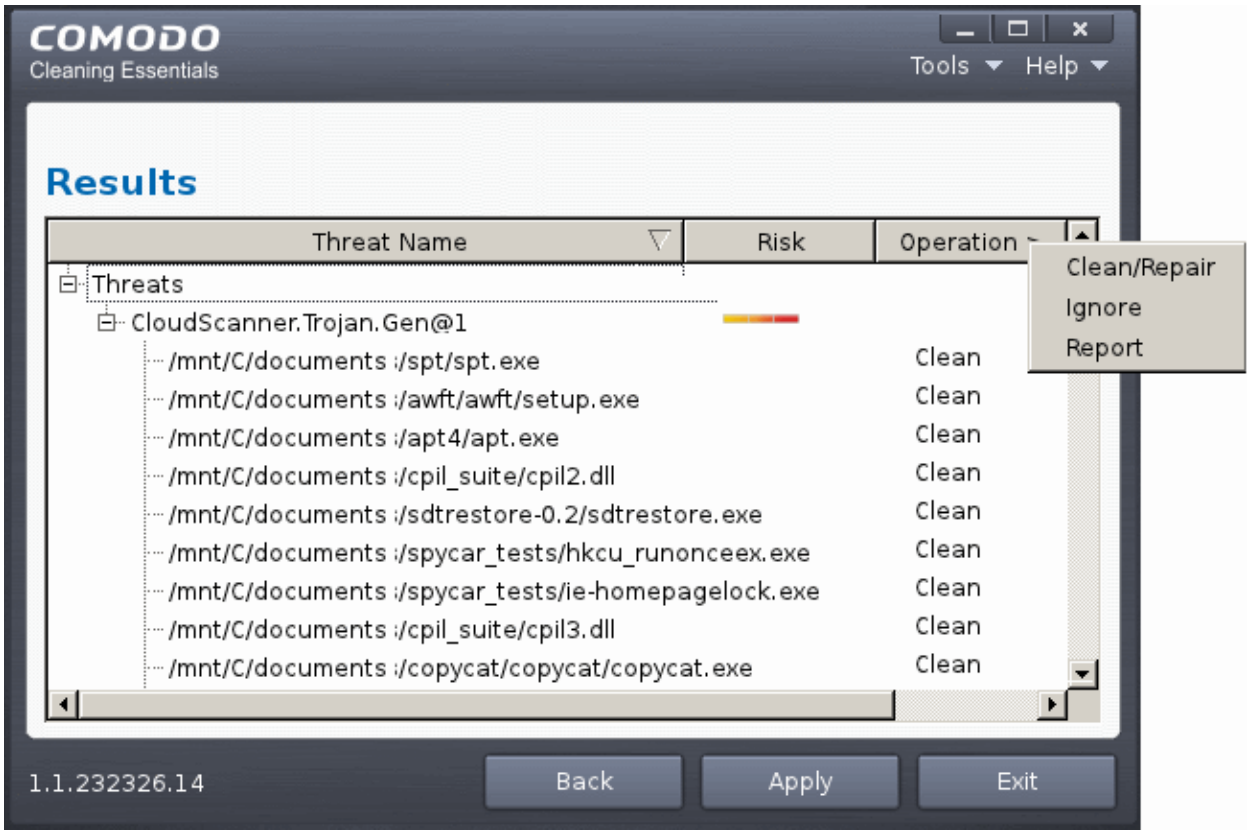
- If malicious executables are discovered on the scanned areas, the 'Results' window displays the list of those items (Viruses, Malware and so on).

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

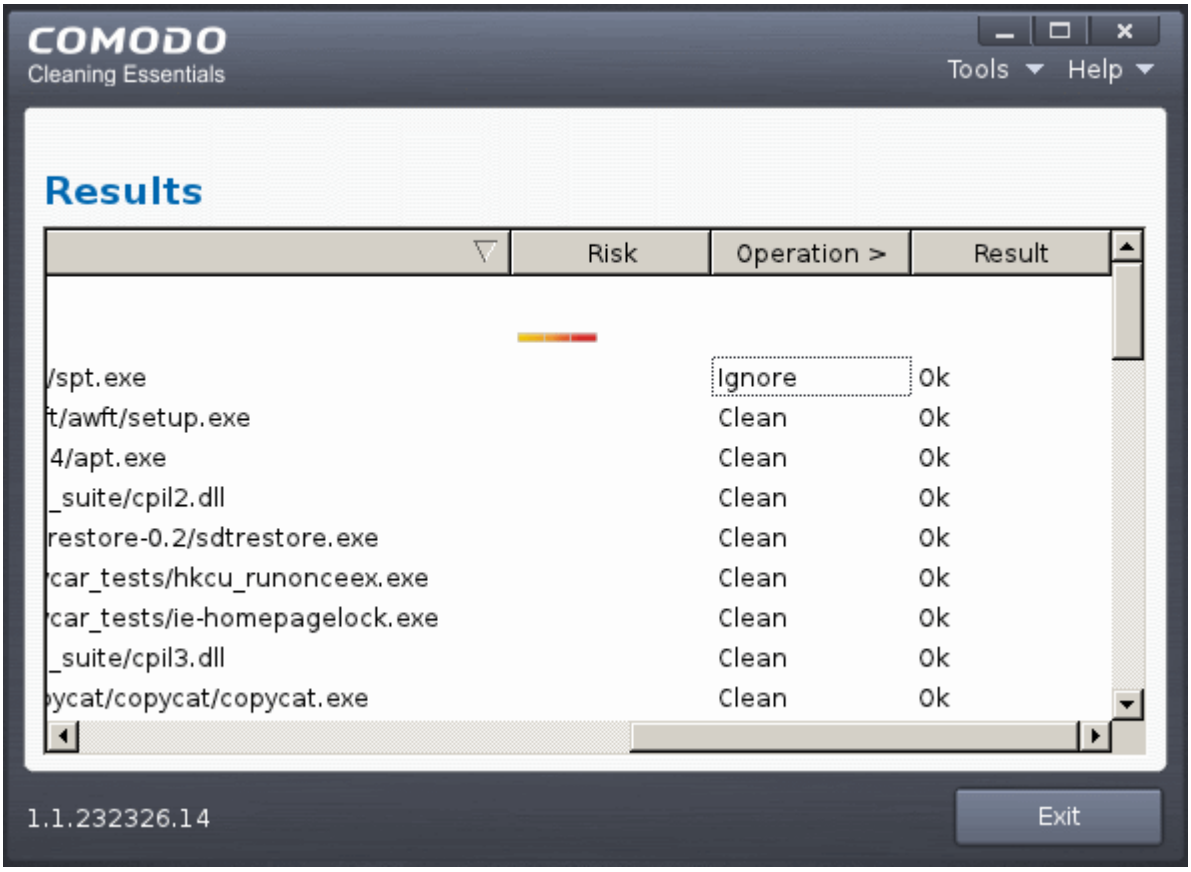
The 'Results' window allows you to quarantine and later remove, ignore the threat if it is a safe file or to submit it as a false positive to Comodo if you are sure about the authenticity of the file. The default operation is 'Clean', that means CCE will clean the threat if a disinfection routine is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



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



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



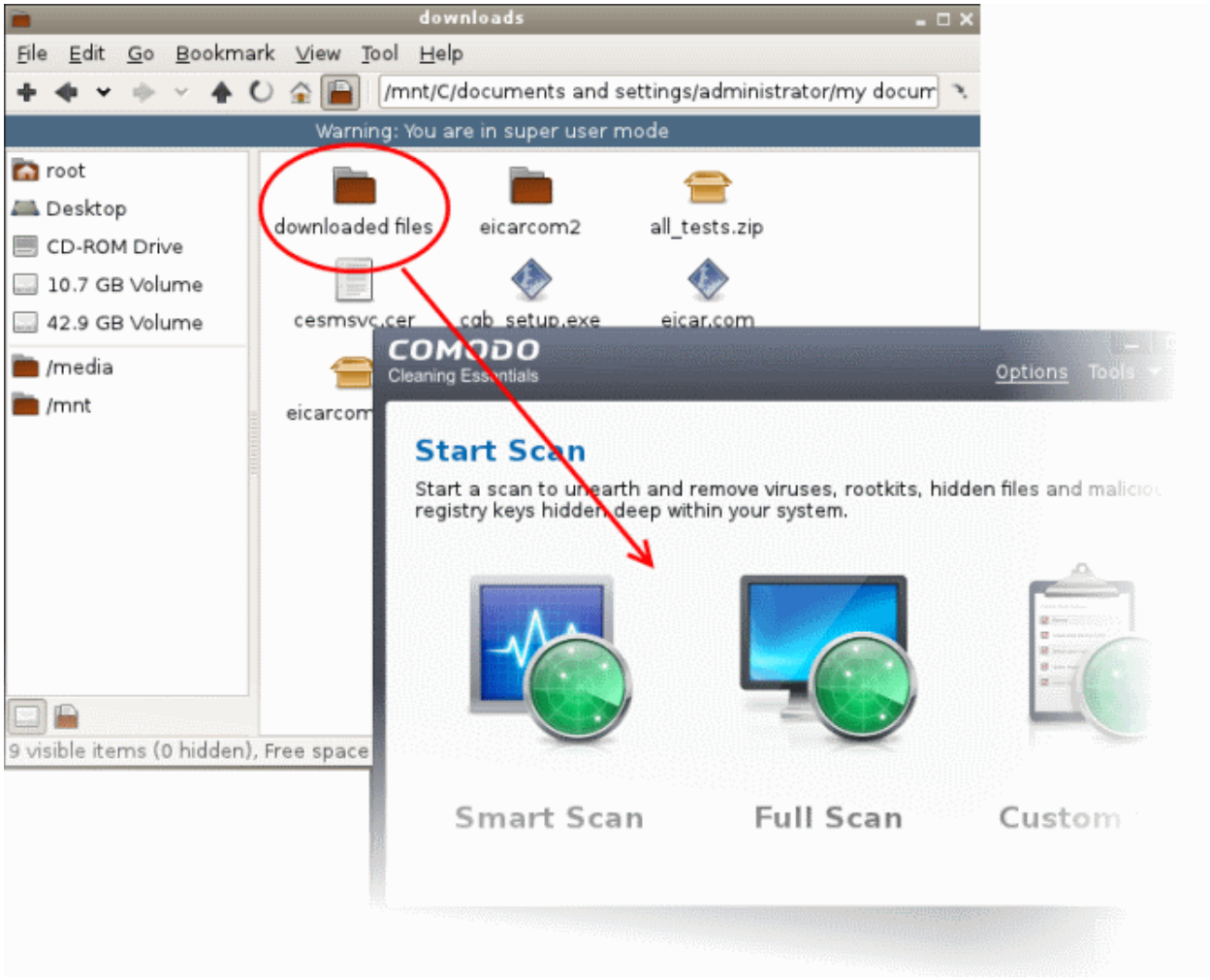
7. Click 'Exit'.

Instantly Scan Folder or File

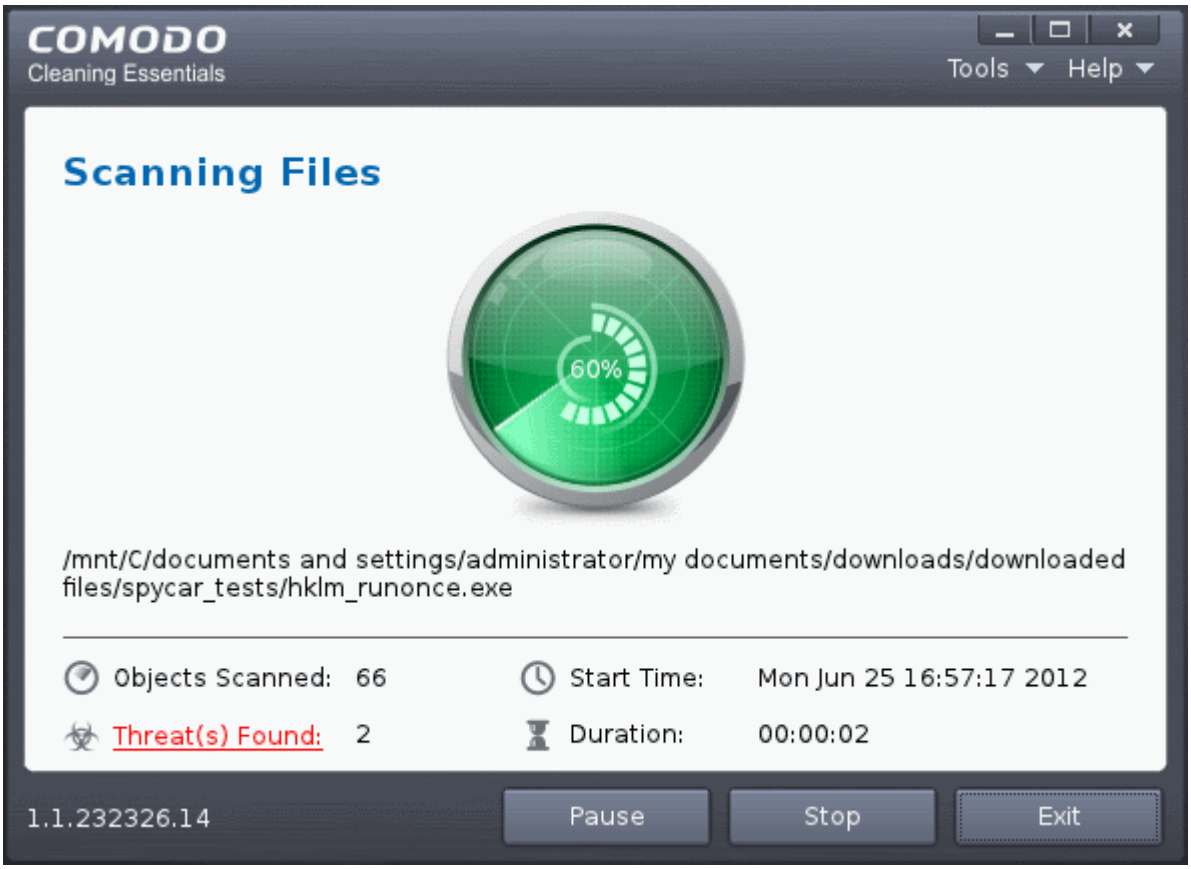
You can scan a folder or file you just downloaded from Internet / copied in to your system of items in a removable storage device like a pen drive by dragging and dropping it on to the CCE interface.

To instantly scan an item

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



The folder/file will be scanned immediately.



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

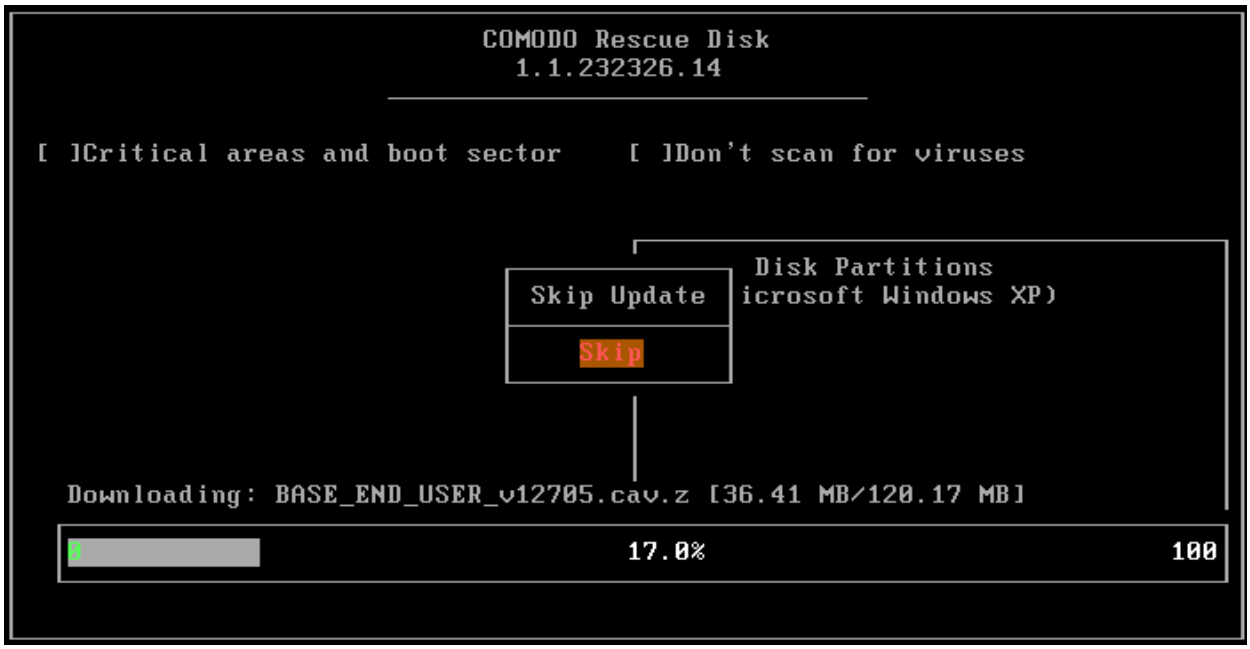
If you have opted to use the **text mode**, scroll to 'Custom Scan' by using the down or up arrow and click the 'Enter' button.

In the Custom Scan interface, you have the option to select the files or folders. Use the Tab button to navigate and 'Space' bar to select the options. For 'Select Disk Partitions' use the 'Up' or 'Down' arrows and select the drive.

Note: Unlike in Graphic mode, the Text mode for Custom scan allows only to select partitions and not individual files or folders.

- Navigate to 'Ok' and press the 'Enter' button.

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



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

The application will start scanning the selected areas of your system and the progress will be displayed. Press 'Ctrl+C' buttons to abort the scan.

For each and every malware detected by CCE, a 'Choose Action to Virus Detected' screen will be displayed.

The 'Results' screen allows you to quarantine and later remove, ignore the threat if it is a safe file or to submit it as a false positive to Comodo if you are sure about the authenticity of the file. The default operation is 'Clean All', that means CCE will clean the threat if a disinfection routine is available for it, else, will move it to quarantine. For abnormal system settings, you have the option to either repair the setting or ignore.

- To clean a threat, select 'Clean' using the left or right arrows and press the 'Enter' key. The file will be disinfected or moved to quarantine upon applying the operation. You can later remove the file from your system from the 'Quarantined Items' interface. Refer to **Managing Quarantined Items** for more details.
- To ignore a threat if you consider the file is safe, select 'Ignore' using the left or right arrows and press the 'Enter' button.
- To report threat as a false-positive result, select 'Report' using the left or right arrows and press the 'Enter' key. The file will be sent to Comodo. Experts in Comodo will analyze the file and add it to whitelist, if found safe.

2.4. Comparison of Scan Types

Scanners

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

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

Scan Types

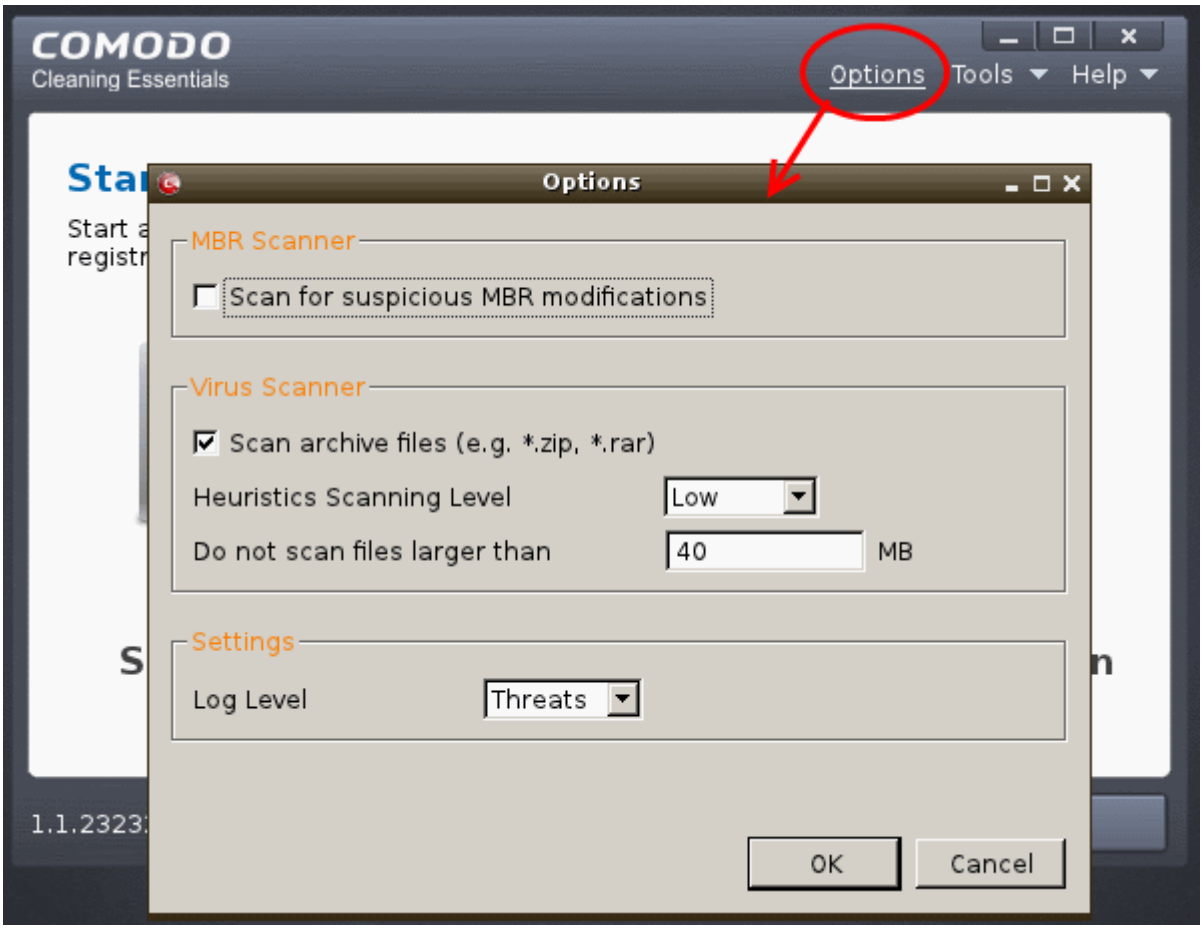
The following table gives the sequence of scanners employed while scanning various areas for different scan types. The symbol ' > ' indicates a sequential process. For example, 'Basic > FLS' means that the item is first checked using the Basic (local) AV scanner. Only if the file is not identified as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

Scan Options	Smart Scan	Full Scan	Custom Scan (Scanners are the same as Full Scan)
Critical areas and boot sector	Critical areas>MBR Scope: entire areas	Critical areas>MBR Scope: entire areas	Optional. Scope: entire areas
Virus	Basic>FLS Scope: autorun files	Basic>FLS Scope: files in all drives	Optional. Scope: Customizable

3. Configuring Comodo Cleaning Essentials

CCE can be configured according to user preferences by clicking the 'Options' from the title bar. You can manage various functions such as scanning suspicious MBR entries, scanning archive files and more.

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



MBR Options

- **Scan for suspicious MBR modifications -** When selected, CCE will automatically scan MBR (master boot record) for unknown or suspicious changes made to it.

Virus Scanner Settings

- **Scan archive files** - When this check box is selected, CCE scans archive files such as .ZIP and .RAR files. These include RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB archives.
- **Heuristics Scanning/Level** - CCE employs various heuristic techniques to identify previously unknown viruses and Trojan horses. 'Heuristics' describes the method of analyzing the code of a file to ascertain whether it contains code typical of a virus. If it is found to do so then the application recommends it for quarantine. Heuristics is about detecting virus-like behavior or attributes rather than looking for a precise virus signature that matches a signature on the virus blacklist.

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

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

  - **Off** - Selecting this option disables heuristic scanning. This means that virus scans only uses the 'traditional' virus signature database to determine whether a file is malicious or not.
  - **Low** - 'Lowest' sensitivity to detecting unknown threats but will also generate the fewest false positives. This setting combines an extremely high level of security and protection with a low rate of false positives. Comodo recommends this setting for most users.
  - **Medium** - Detects unknown threats with greater sensitivity than the 'Low' setting but with a corresponding rise in the possibility of false positives.
  - **High** - Highest sensitivity to detecting unknown threats but this also raises the possibility of more false

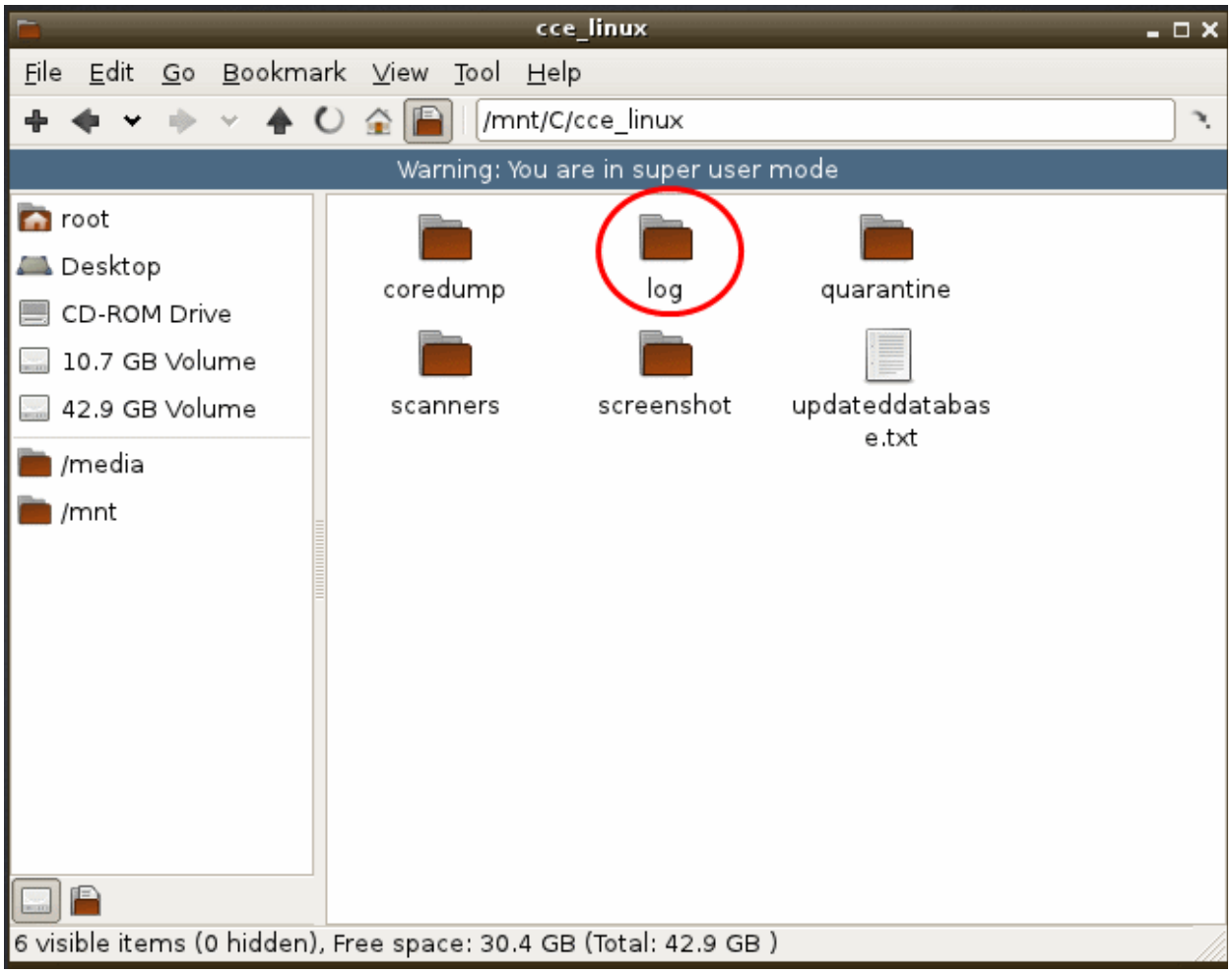
positives too.

- **Do not scan files larger than** - This box allows you to set a maximum size (in MB) for the individual files to be scanned during manual scanning. Files larger than the size specified here, are not scanned. Default = 40 MB

Miscellaneous Settings

- **Log level -** This drop down box allows you to select options for CCE event logs. The options are:
  - **Disable** - If you select this option, CCE will not create any log files.
  - **Threats** - If this option is selected, CCE will generate log reports containing files that it has detected as threats.
  - **All** - If this option is selected, CCE will generate log reports for all files that it have been scanned and will record all events. The log file will contain system information, cleanup results, details about the file path, whether it is malicious, the action taken and whether the action has been implemented.

Logs are saved in the folder <folder containing CCE Linux files>\Logs.



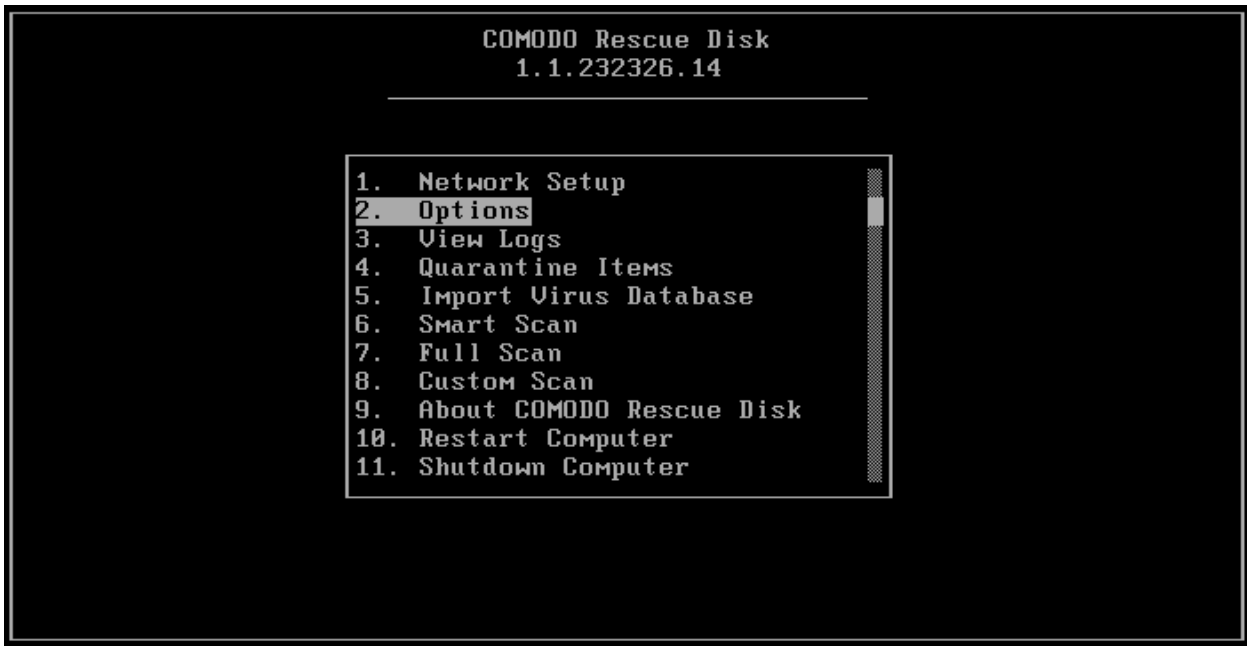
To view the logs:

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

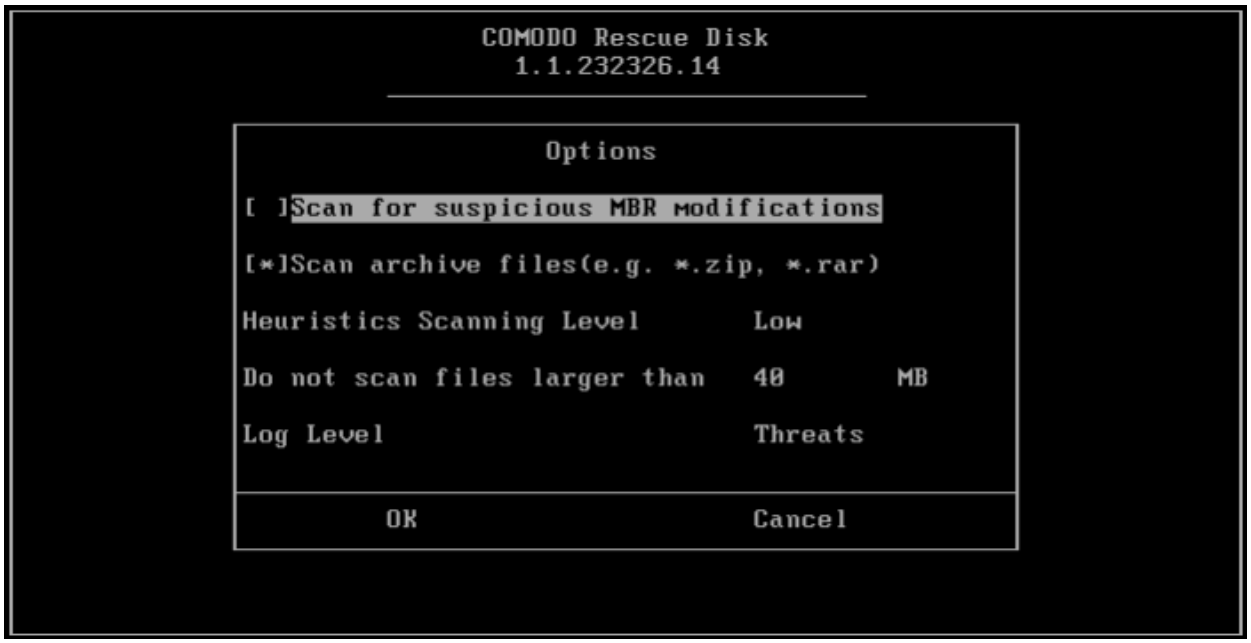
  Or

- Click Tools > Browse Logs...
- Click 'OK' for the settings to take effect.

If you have opted to use the **text mode**, scroll to 'Options' by using the down or up arrow and click the 'Enter' button.



The 'Options' screen will be displayed.



You can configure the CCE settings in the Options interface.

- Use the 'Tab' button to navigate and the 'Space' bar to select the options.
- For 'Heuristics Scanning Level' settings, use the 'Up' or 'Down' arrows to select the scanning level.
- For setting the file size for scanning, navigate to 'Do not scan files larger than * MB' and enter the value.
- For selecting what events should be logged, navigate to 'Log Level' and 'Up' or 'Down' arrows to select the log level.
- Navigate to 'OK' and press the 'Enter' button for the settings to take effect.

The details of the settings are given at the **beginning** of the section.

4.The Tools Menu

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

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

The 'Tools' menu has the following options:

- **Managing Quarantined Items** - Enables to manage the items moved to quarantine by various scans.
- **Importing Antivirus Database** - Enables you to import virus database from your local storage or a network location.
- **Browse Logs** - Enables you to view the log of events recorded by the application.
- **Check for Updates** – Enables you to check whether updated version of the application is available.

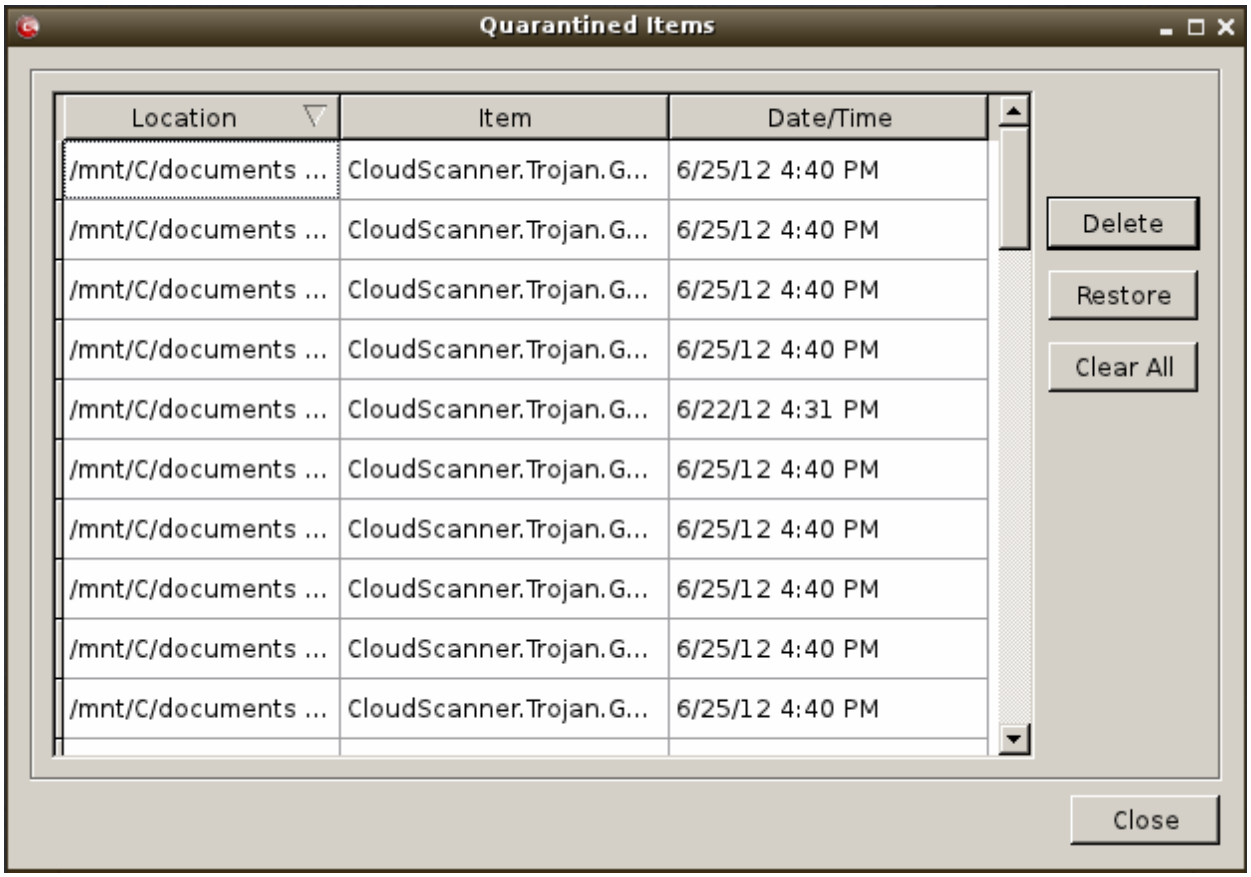
4.1.Managing Quarantined Items

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

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

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

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



Column Descriptions

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

From this interface you can:

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

To delete a quarantined item from the system

- Select the item and Click 'Delete'.

This deletes the file from your system permanently.

To restore a quarantined item to its original location

- Select the item and click 'Restore'.

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

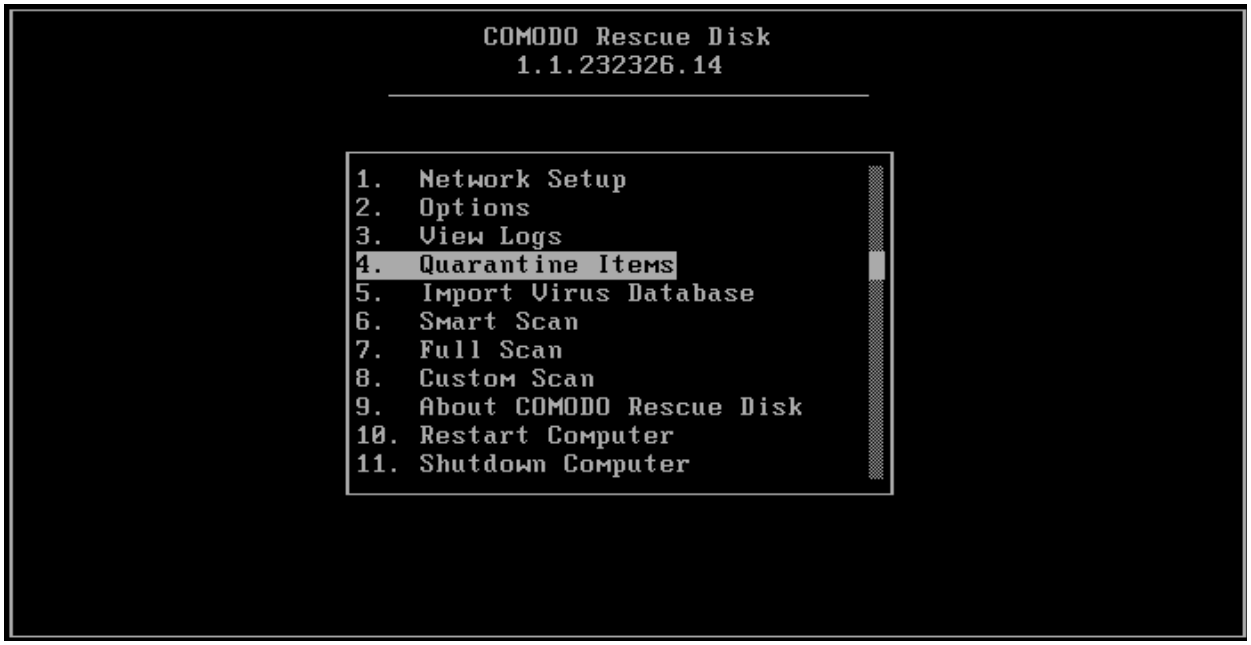
To remove all the quarantined items permanently

- Click 'Clear All'.

This deletes all the quarantined items from your system permanently.

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

If you have opted to use the **text mode**, scroll to 'Quarantine Items' by using the down or up arrow and click the 'Enter' button.



The Quarantine Items screen will be displayed.

- Use the 'Up' or 'Down' arrows and 'Space' bar to select an quarantined item
- Use the 'Tab' button to navigate and select the options.

To delete a quarantined item from the system

- Select the item and navigate to 'Delete' and press the 'Enter' button.

This deletes the file from your system permanently.

To restore a quarantined item to its original location

- Select the item and navigate to 'Restore' and press the 'Enter' button.

If the restored item does not contain a malware, it operates as usual. But if it contains a malware, it will be detected as a threat ,

during the next scan and moved to quarantine if you perform 'Clean' operation.

To remove all the quarantined items permanently

- Navigate to 'Clear All' and press the 'Enter' button.

This deletes all the quarantined items from your system permanently.

4.2. Importing Antivirus Database

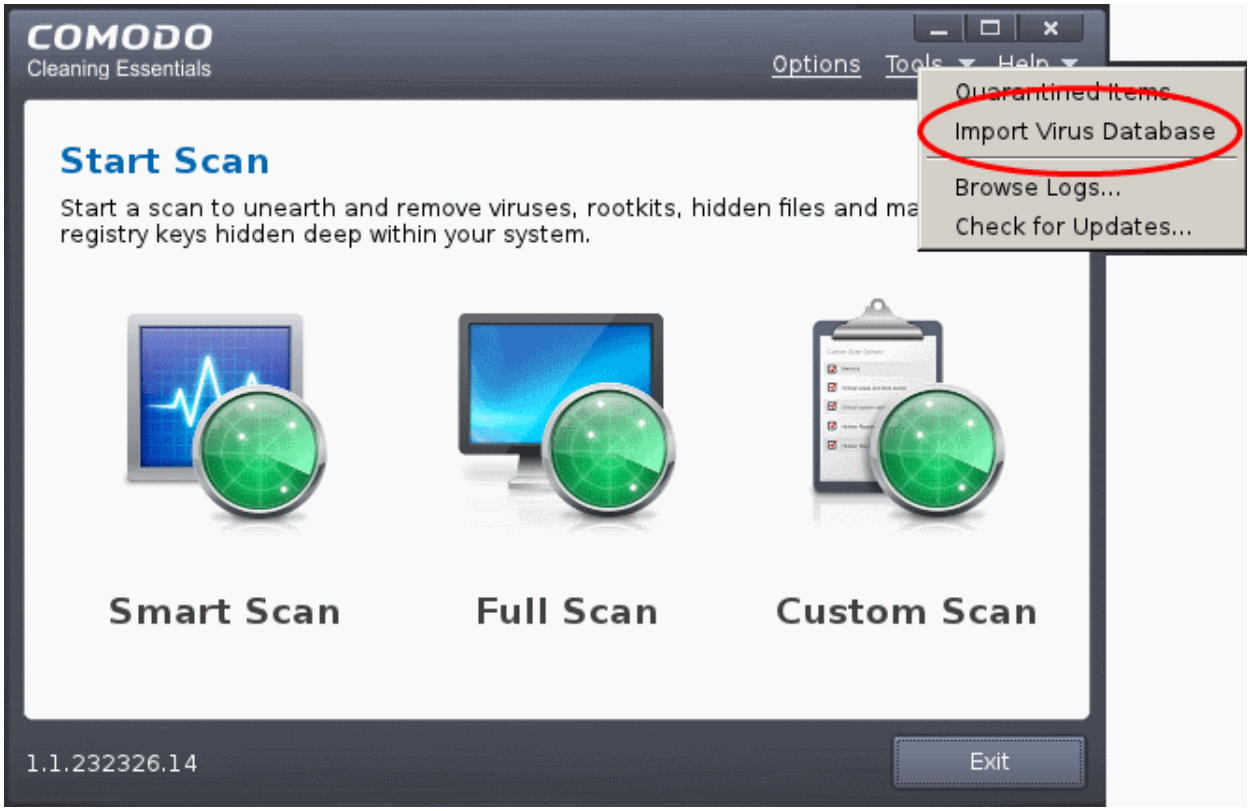
CCE is configured to check Comodo servers to see whether a virus database update is available for download whenever a scan is performed. As an alternative to downloading from Comodo servers, you can import the virus database updates from local storage or from any of the other computers in your network that uses the same database. This can help accelerate update deployment and reduce the bandwidth consumption.

Example Scenarios:

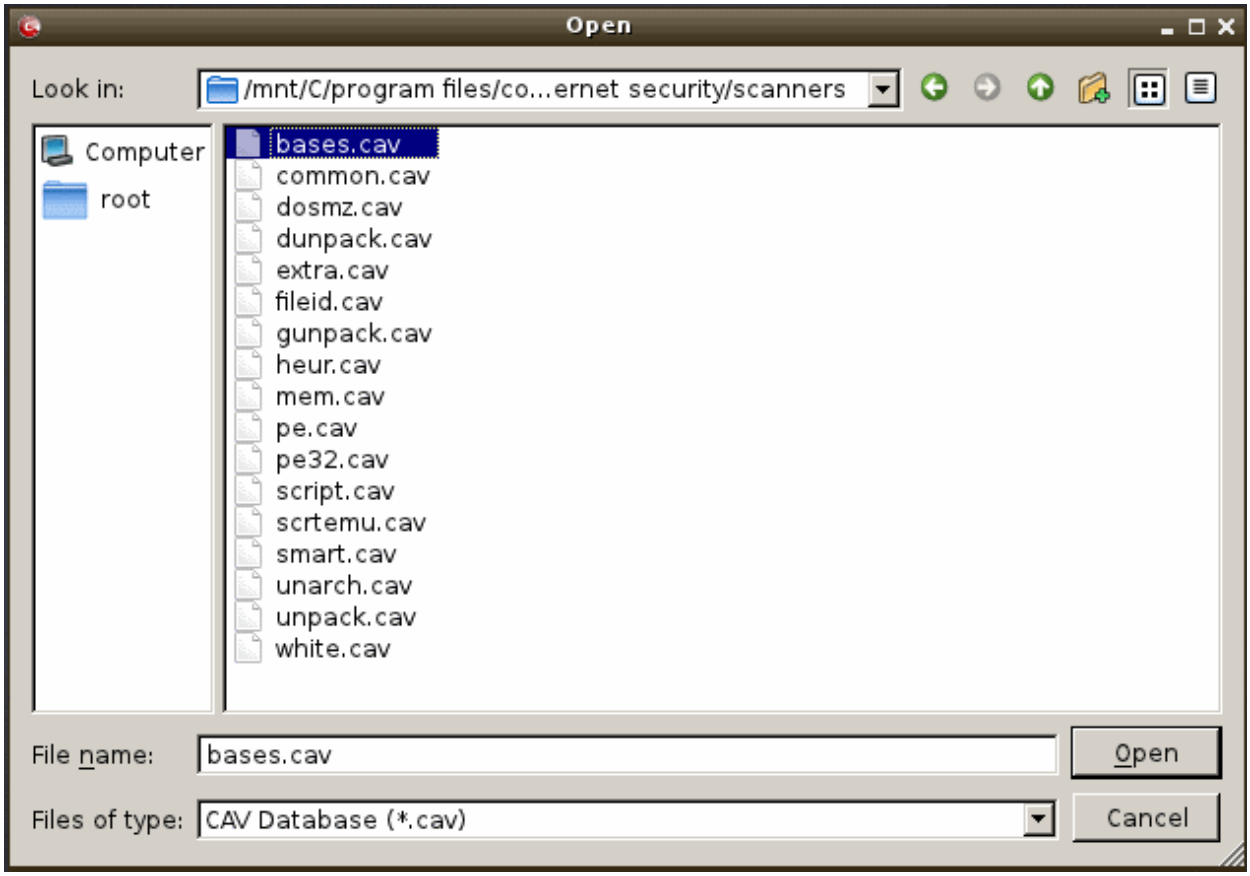
- If you also have Comodo Internet Security (CIS) installed and it is configured to regularly receive database updates then you can configure CCE to collect it's updates from your CIS folder. To do this, you just need to point CCE to the CIS folder that contains the (updated) bases.cav file. See instructions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

To import virus database

- Click Tools > Import Virus Database.



The Linux Open dialog will be displayed.



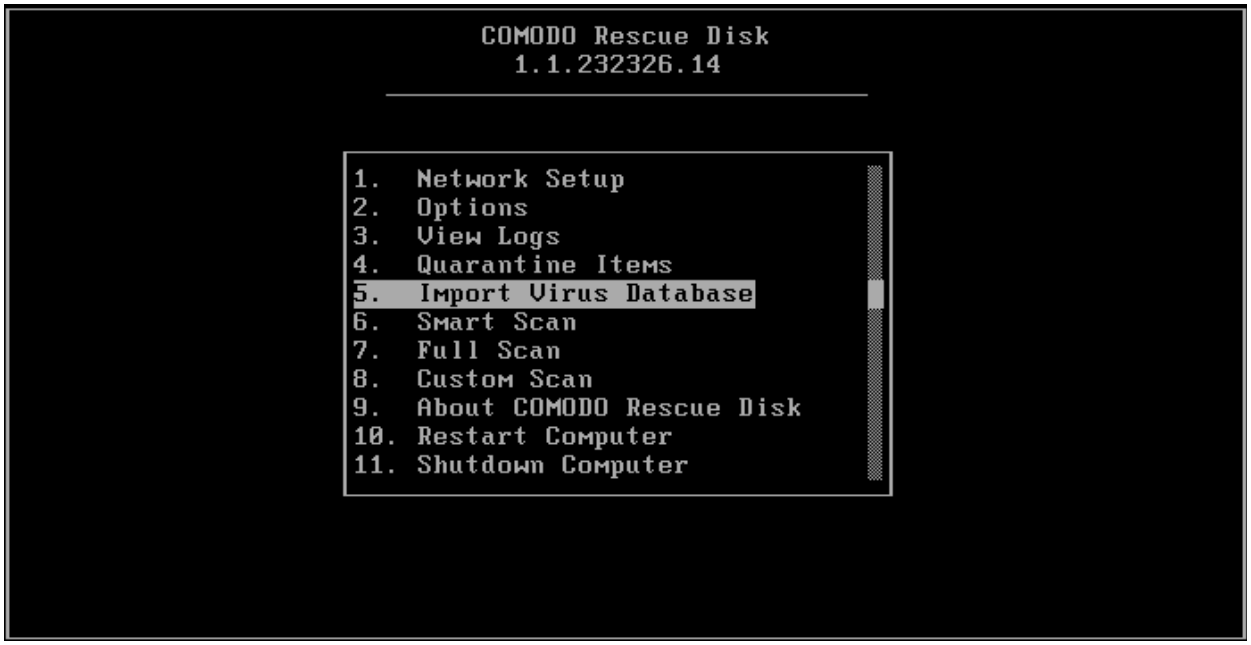
- Navigate to the folder containing the virus database file like bases.cav and select the file

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

- Click 'Open'.

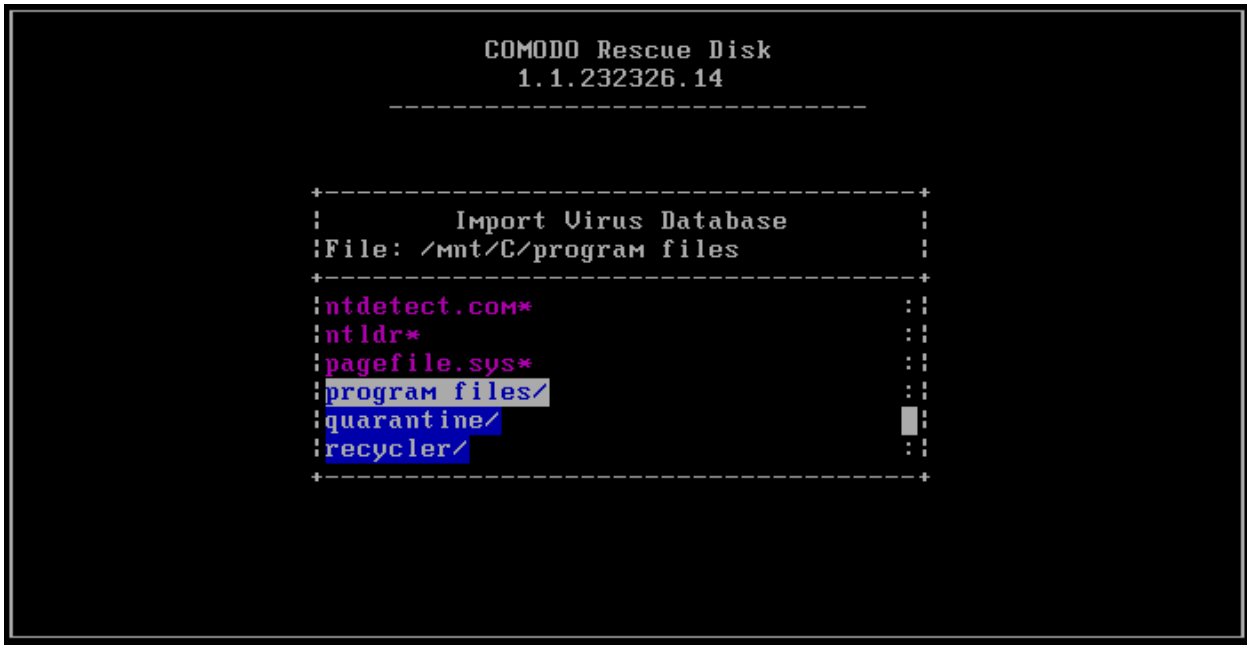
The database file will be immediately imported to CCE.

If you have opted to use the **text mode**, scroll to 'Quarantine Items' by using the down or up arrow and click the 'Enter' button.

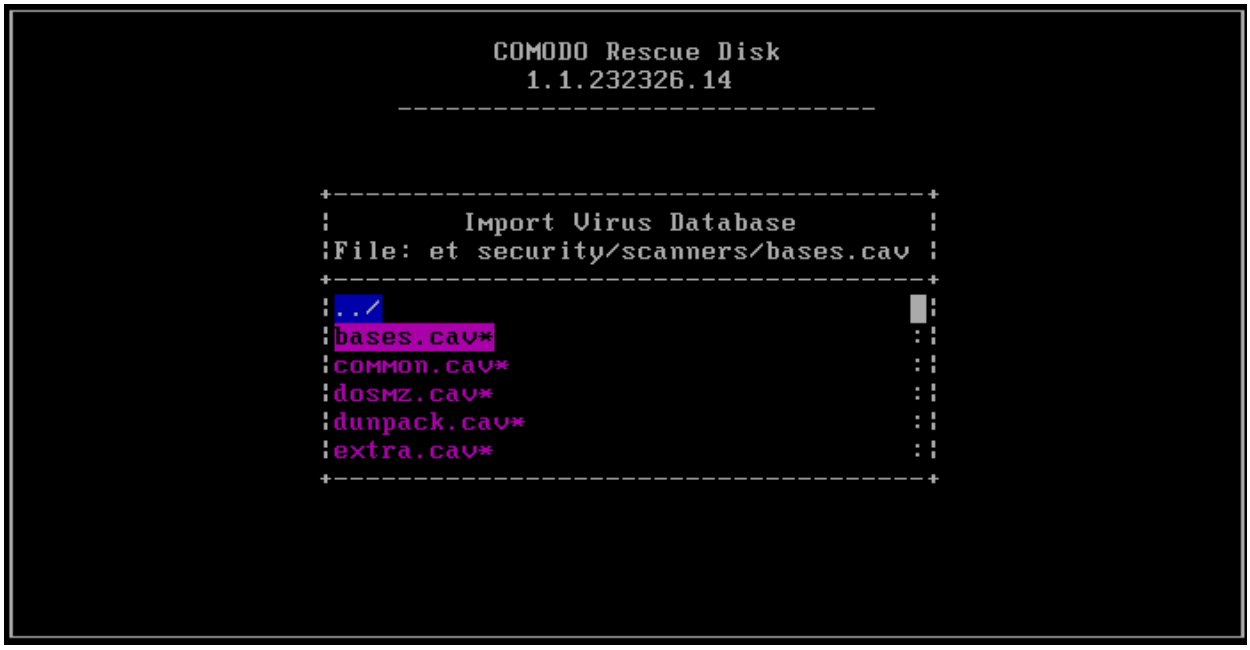


The 'Import Virus Database' screen will be displayed.

- Use the 'Up' or 'Down' arrow keys to select the item.
- Press the 'Enter' button twice on '../' to navigate to program folders.

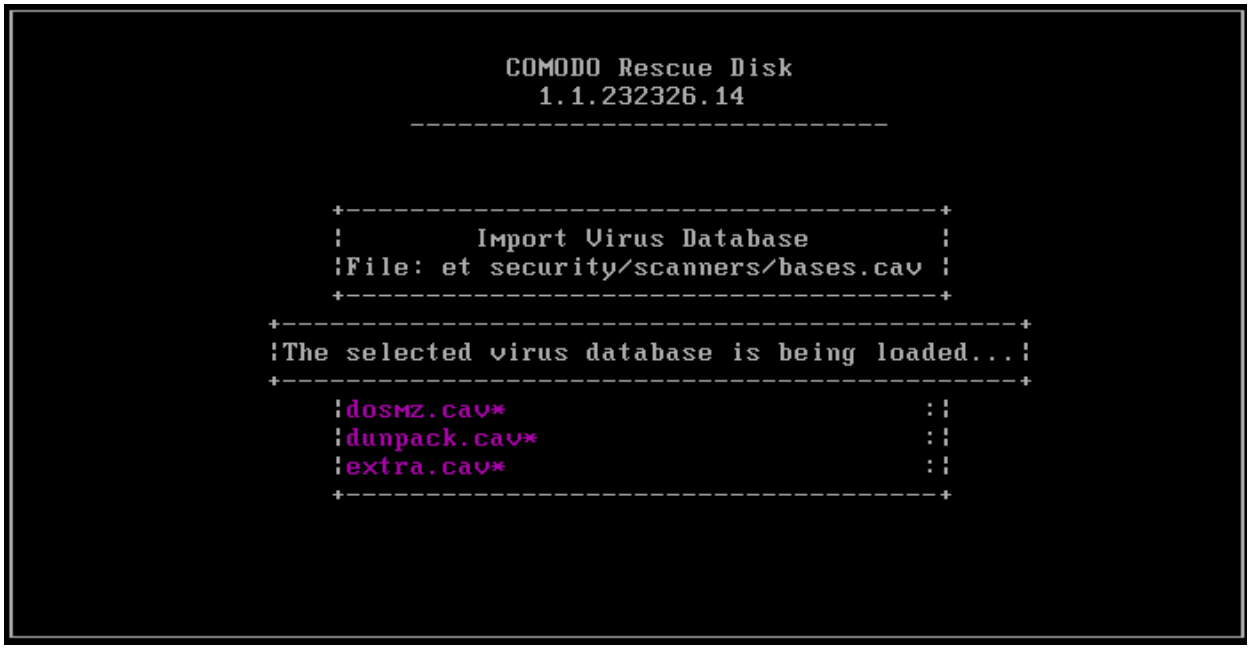


- Press the 'Enter' button and navigate to .cav files, for example, Comodo Internet Security/scanners/bases.cav.

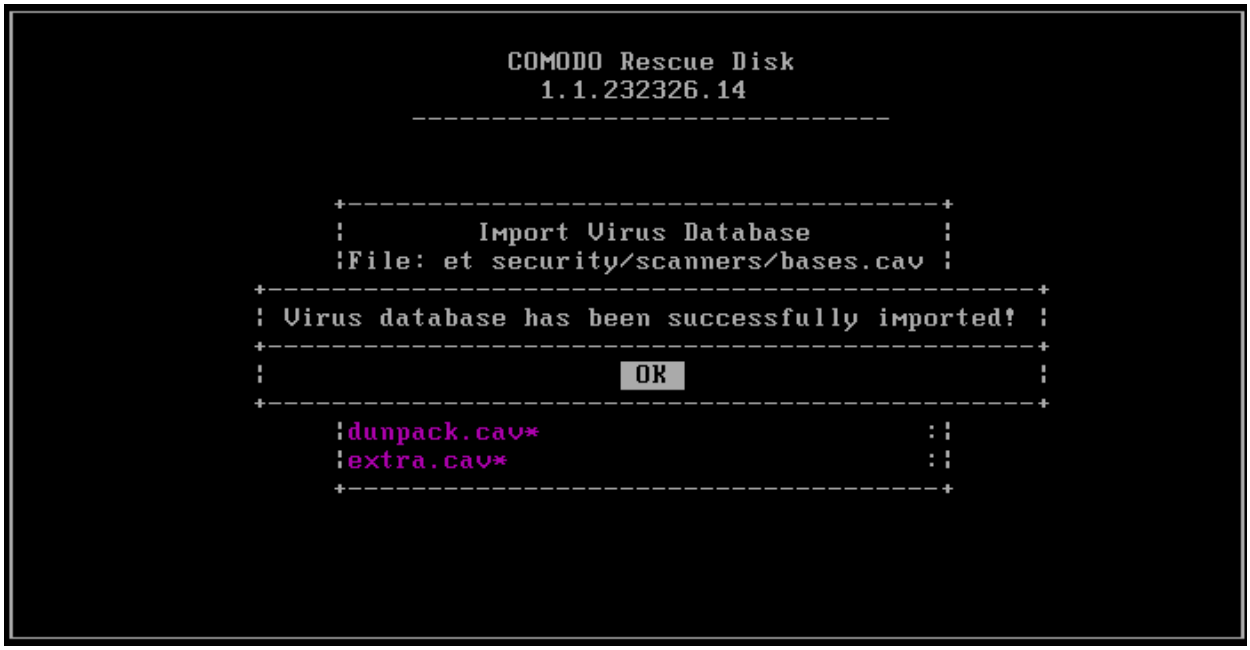


- Press the 'Enter' button.

The selected virus database upload progress will be displayed...



...and on completion, the successfully completed screen will be displayed.



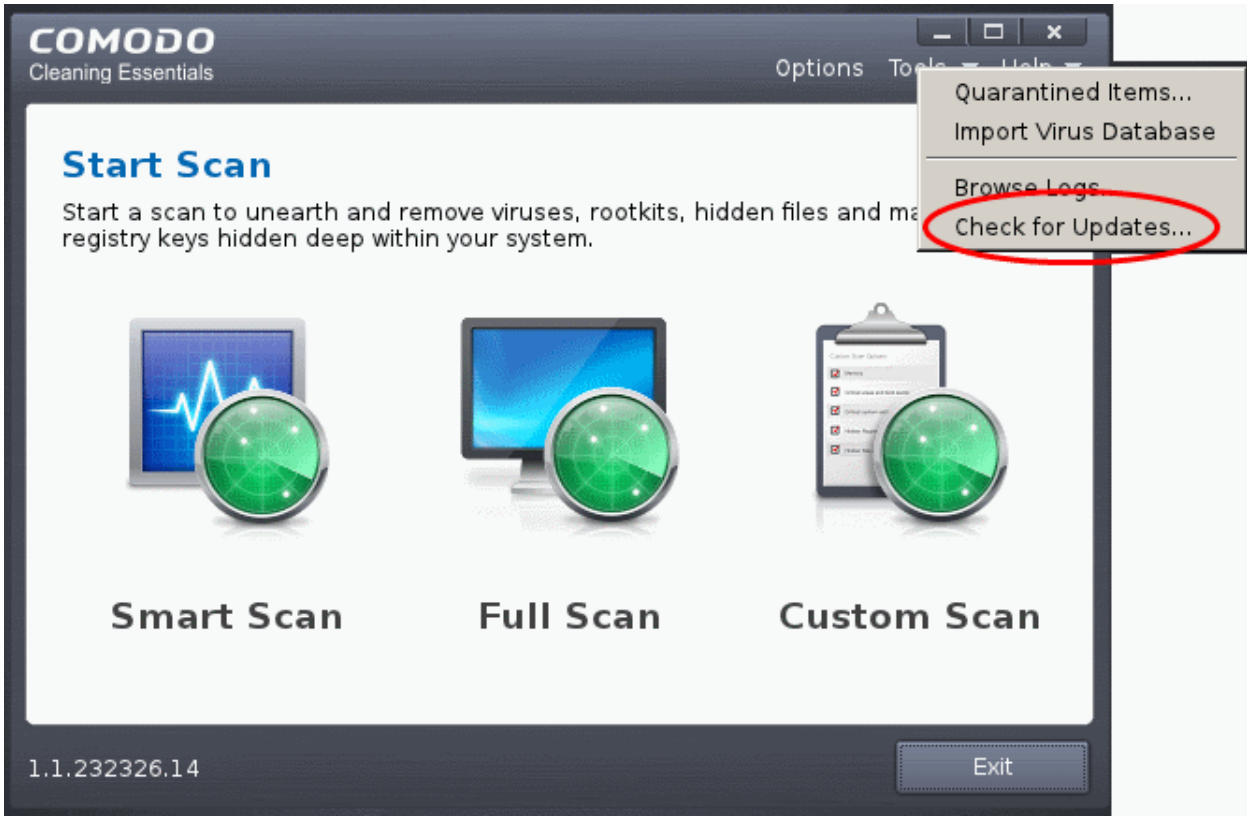
- Press the 'Enter' button to return to main menu.

4.3. Checking for Software Updates

You can check if the CRD bootable disk that you are using is the latest version or if an updated version of CRD is available.

To check for the software updates

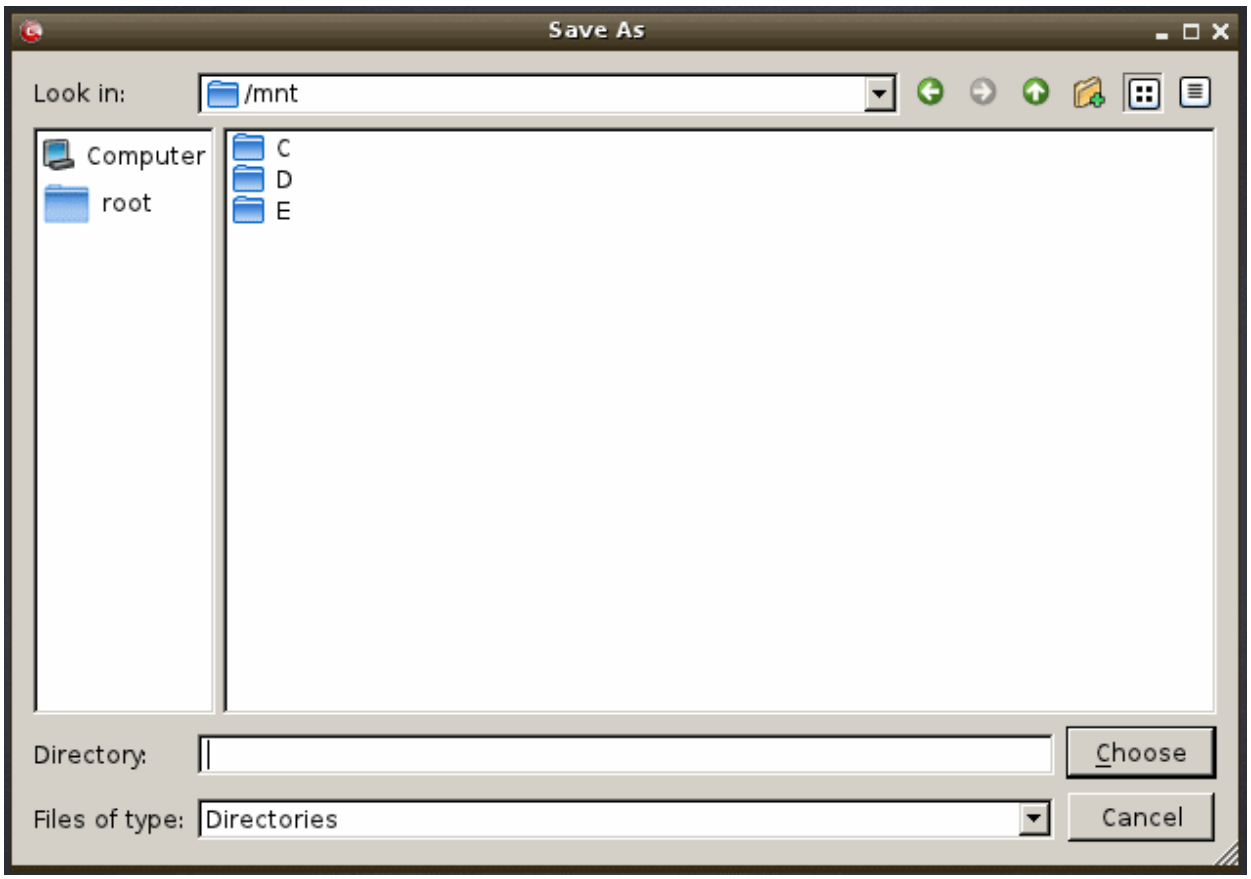
- Click 'Tools' > 'Check for Updates'



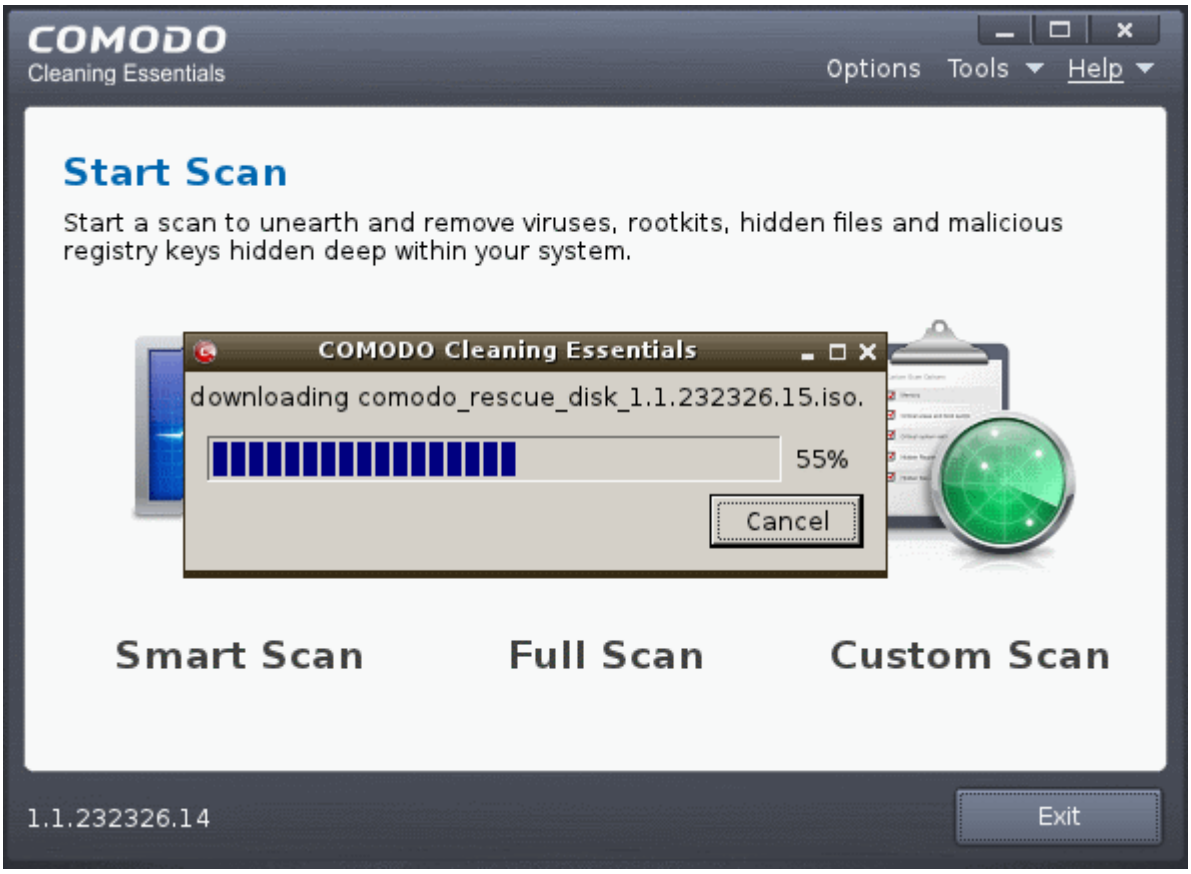
CRD will check for any updated version and if the ISO image is the latest, the following screen will be displayed.

If a new version of CRD is available, 'New version is available' screen will be displayed.

- Click the 'Download' button to save the latest version of CRD in your system.
- Choose the location where you want to save the ISO file.



The download progress will be displayed...



… and saved in the chosen location. Burn this new version of CRD ISO file to CD, DVD or USB for future use.

5.Help and About Details

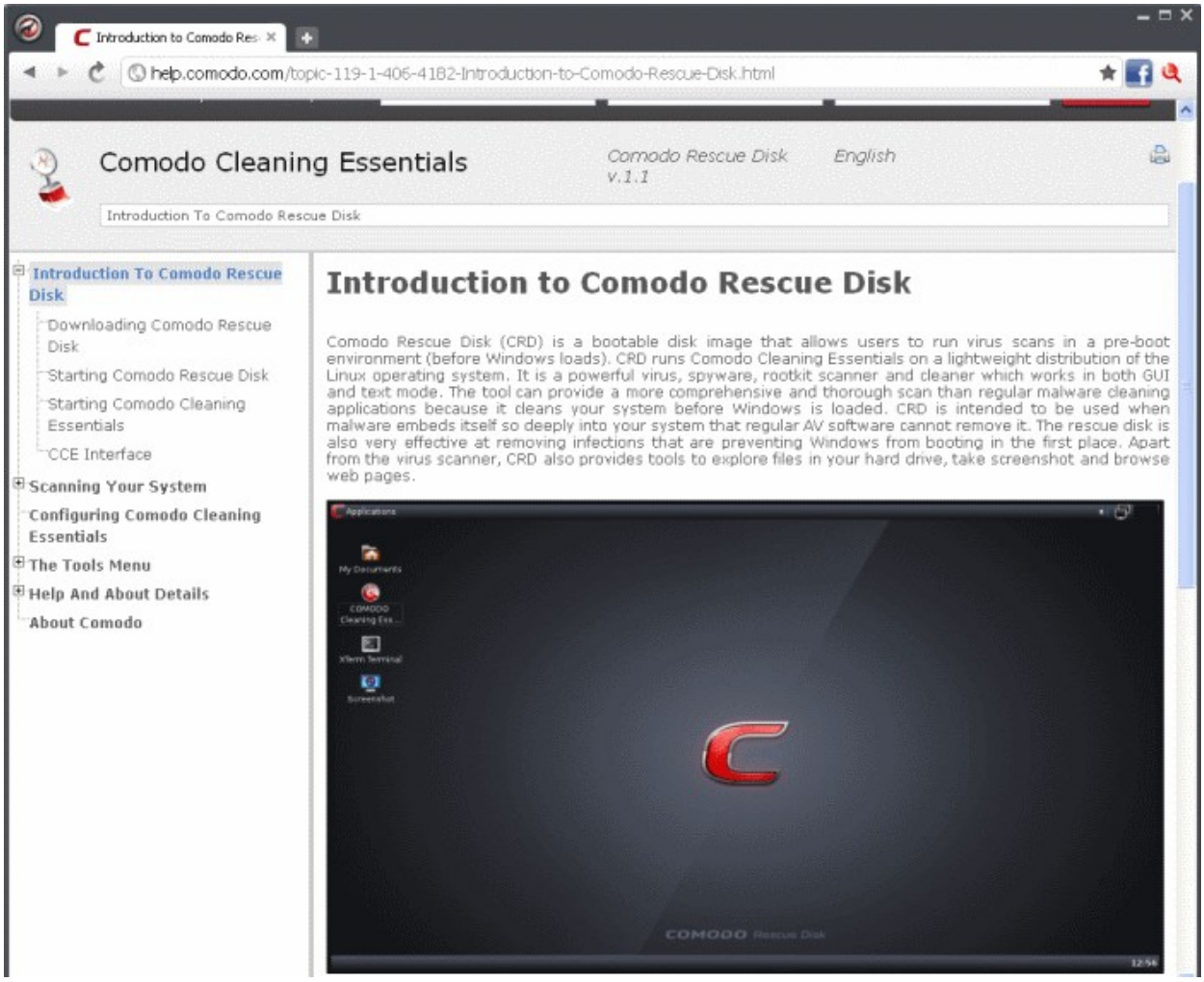
The Help menu at the top right corner of the CCE main interface enables you to access the online help guide and view the About dialog of the application.

Click the links below for more information:

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

5.1. Help

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



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

5.2. About

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

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

About Comodo

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

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

Comodo Security Solutions, Inc.

525 Washington Blvd. Jersey City,

NJ 07310

United States

Tel: +1.888.256.2608

Tel: +1.877.712.1309

Fax: +1.201.963.9003

Email: **EnterpriseSolutions@Comodo.com**

Comodo CA Limited

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

United Kingdom.

Tel : +44 (0) 161 874 7070

Fax : +44 (0) 161 877 1767

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