COMODO
Creating Trust Online®

Comodo
Cloud Antivirus

Software Version 1.0

User Guide

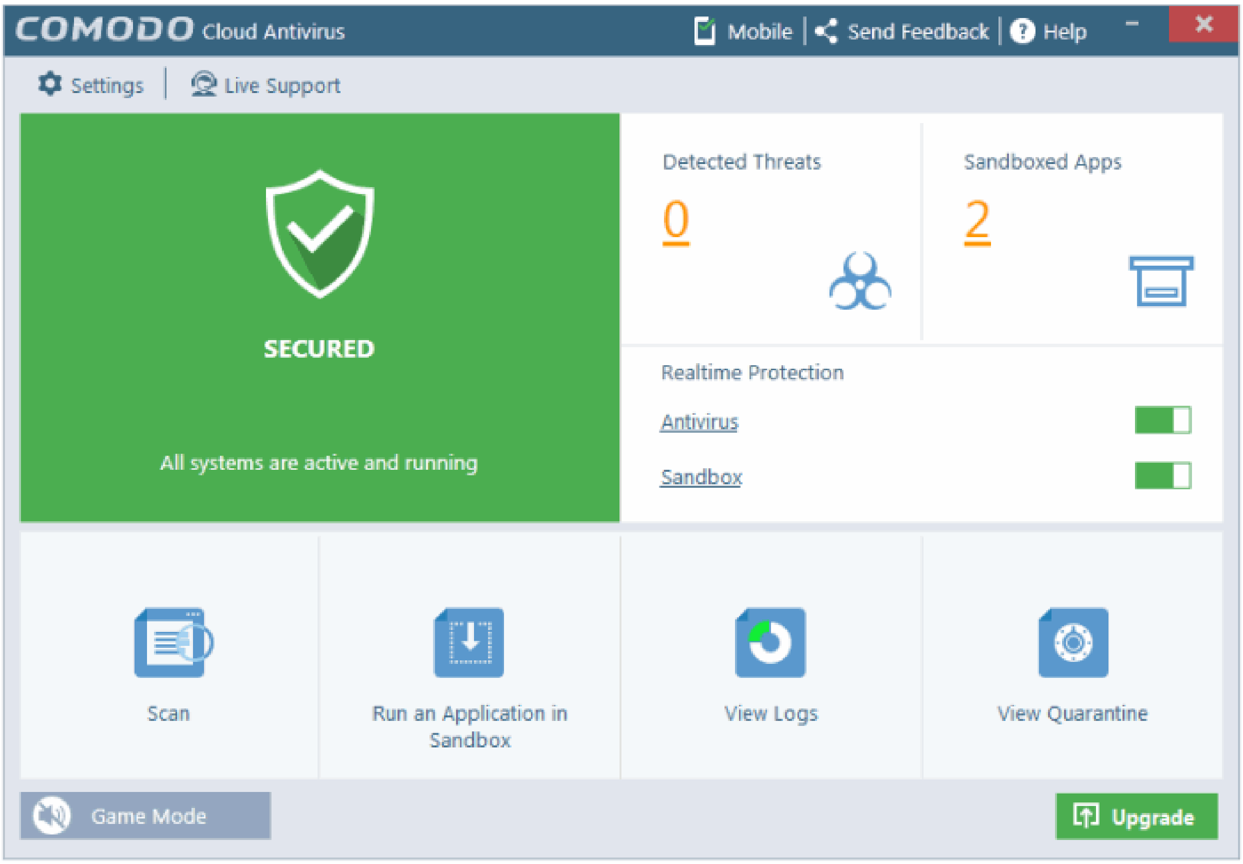
Guide Version 1.0.020516

Comodo Security Solutions
1255 Broad Street
Clifton, NJ, 07013
United States

Table of Contents

1. Introduction to Comodo Cloud Antivirus

Comodo Cloud Antivirus (CCAV) is a lightweight and powerful AV application that utilizes Comodo's auto-containment and real-time cloud scanning to immediately neutralize both known and unknown malware.



SECURED

All systems are active and running

Detected Threats 0

Sandboxed Apps 2

Realtime Protection

Antivirus ●

Sandbox ●

Guide Structure

This guide is intended to take you through the configuration and use of Comodo Cloud Antivirus and is broken down into the following main sections.

1.1. System Requirements

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

Windows 10 Support (Both 32-bit and 64-bit versions) Windows 8 (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)	• 384 MB available RAM • 210 MB hard disk space for both 32-bit and 64-bit versions • CPU with SSE2 support • Internet Explorer Version 5.1 or above
Windows XP (32-bit)	• 256 MB available RAM • 210 MB hard disk space for both 32-bit and 64-bit versions • CPU with SSE2 support • Internet Explorer Version 5.1 or above

Important note: The auto-sandbox is not supported on Windows Server 2003 64 bit.

1.2. Installation

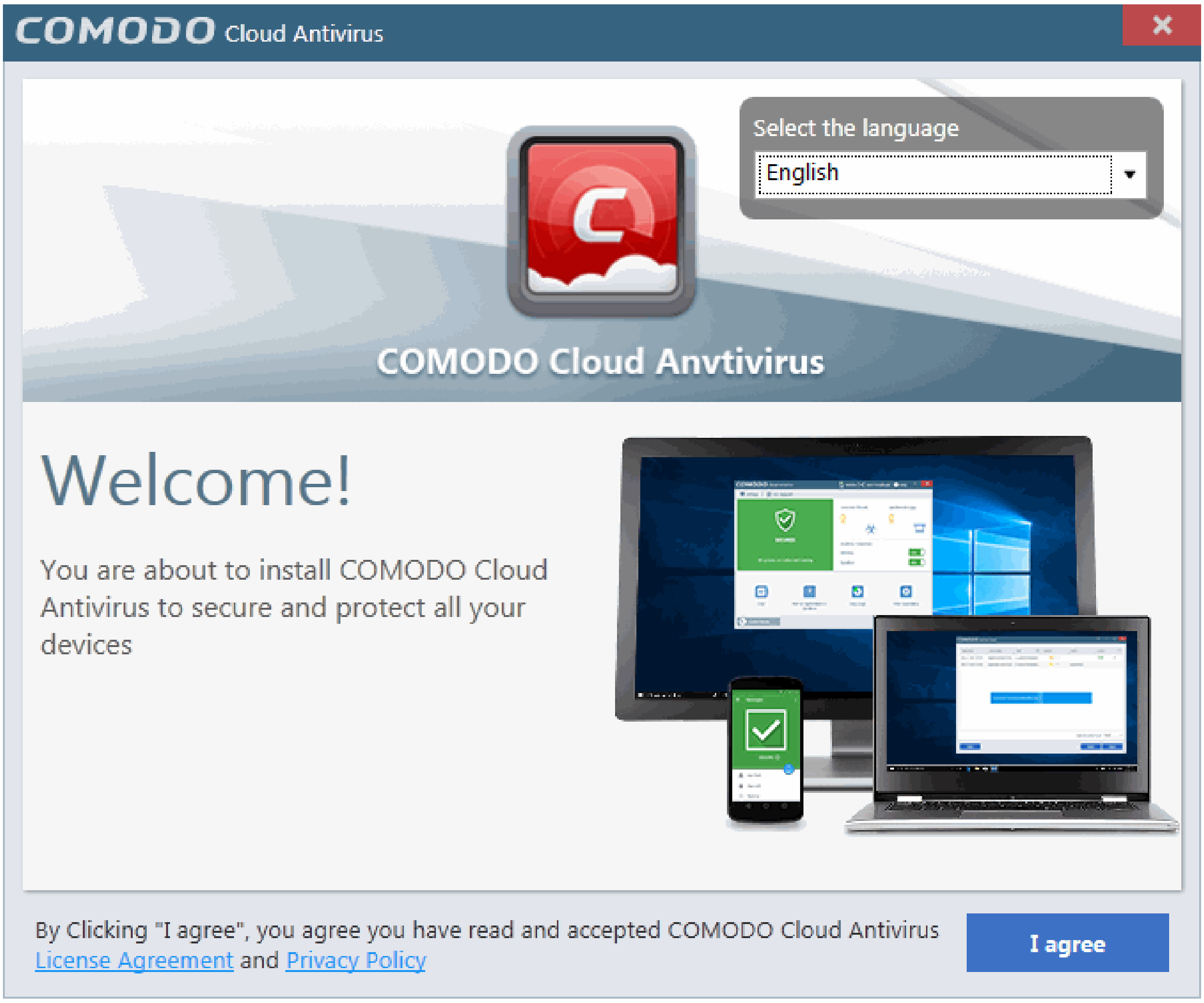
Note - Before beginning installation, please ensure you have uninstalled any other antivirus products and Comodo's CIS/CES that are on your computer. Failure to remove 3rd party AV products and CIS/CES could cause conflicts that mean CCAV will not function correctly. Users should consult their vendor's documentation for precise uninstallation guidelines, however the following steps should help most Windows users:

- Click the Start button to open the Windows Start menu
- Select Control Panel > Programs and Features (Win 10, Win 8, Win 7, Vista) or Control Panel > Add or Remove Programs (XP)
- Select your current antivirus program(s) from the list
- Click Remove/Uninstall button
- Repeat process until all required programs have been removed

To install, download the Comodo Cloud Antivirus setup files to your local drive. (setup file can be downloaded from **http://download.comodo.com/ccav/installers/beta/ccav_installer.exe**)

After downloading the CCAV setup file to your local hard drive, double-click on the ccav_installer file to start the installation wizard.

The language selection dialog will be displayed.



COMODO Cloud Antivirus

Select the language

English

COMODO Cloud Anvtivirus

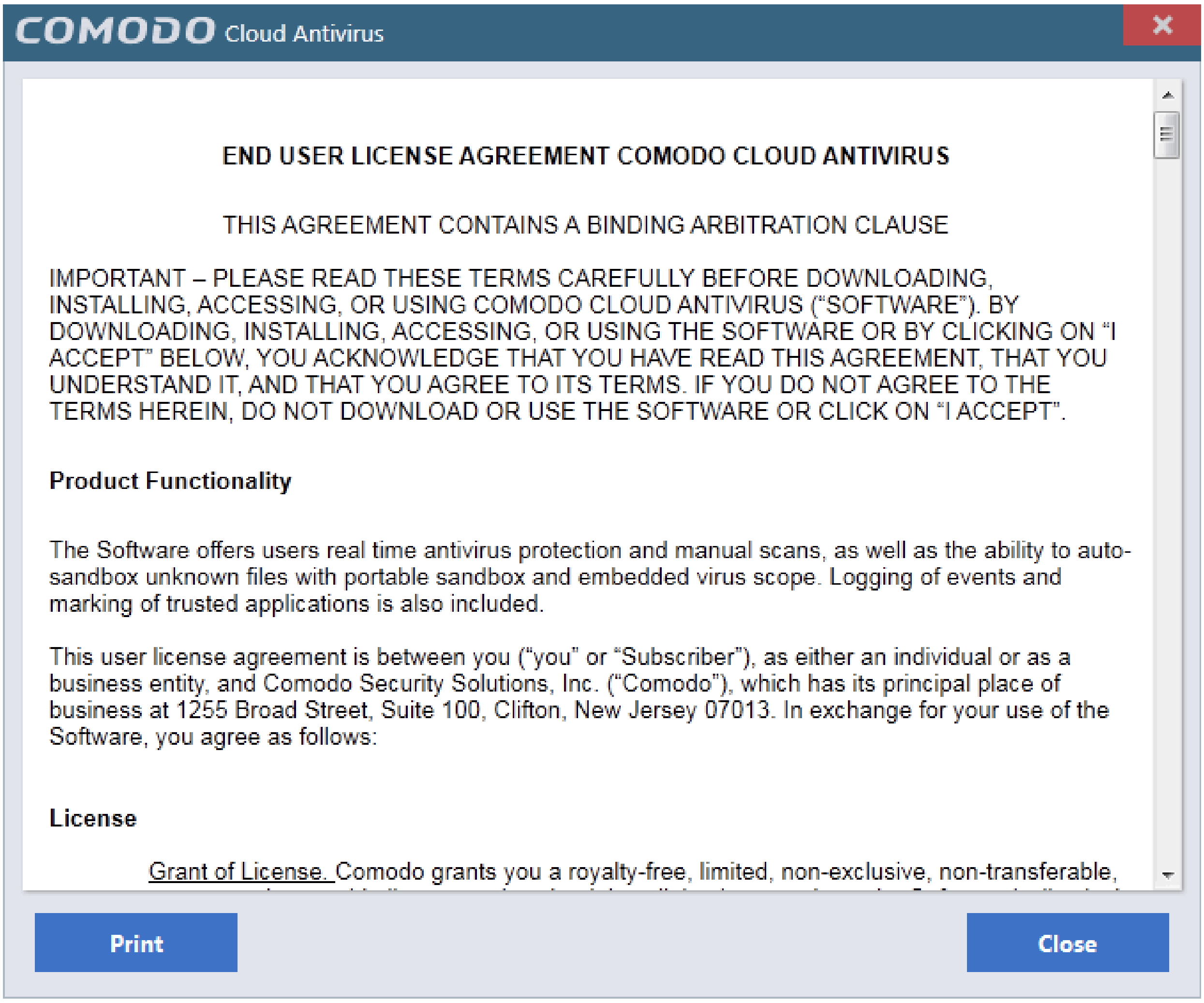
Welcome!

You are about to install COMODO Cloud Antivirus to secure and protect all your devices

By Clicking "I agree", you agree you have read and accepted COMODO Cloud Antivirus License Agreement and Privacy Policy

I agree

- Select the language in which you want CC AV to be installed from the drop-down menu at the right top
- Before proceeding with the installation, read the License Agreement at the bottom of the interface



END USER LICENSE AGREEMENT COMODO CLOUD ANTIVIRUS

THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE

IMPORTANT – PLEASE READ THESE TERMS CAREFULLY BEFORE DOWNLOADING, INSTALLING, ACCESSING, OR USING COMODO CLOUD ANTIVIRUS ("SOFTWARE"). BY DOWNLOADING, INSTALLING, ACCESSING, OR USING THE SOFTWARE OR BY CLICKING ON "I ACCEPT" BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO ITS TERMS. IF YOU DO NOT AGREE TO THE TERMS HEREIN, DO NOT DOWNLOAD OR USE THE SOFTWARE OR CLICK ON "I ACCEPT".

Product Functionality

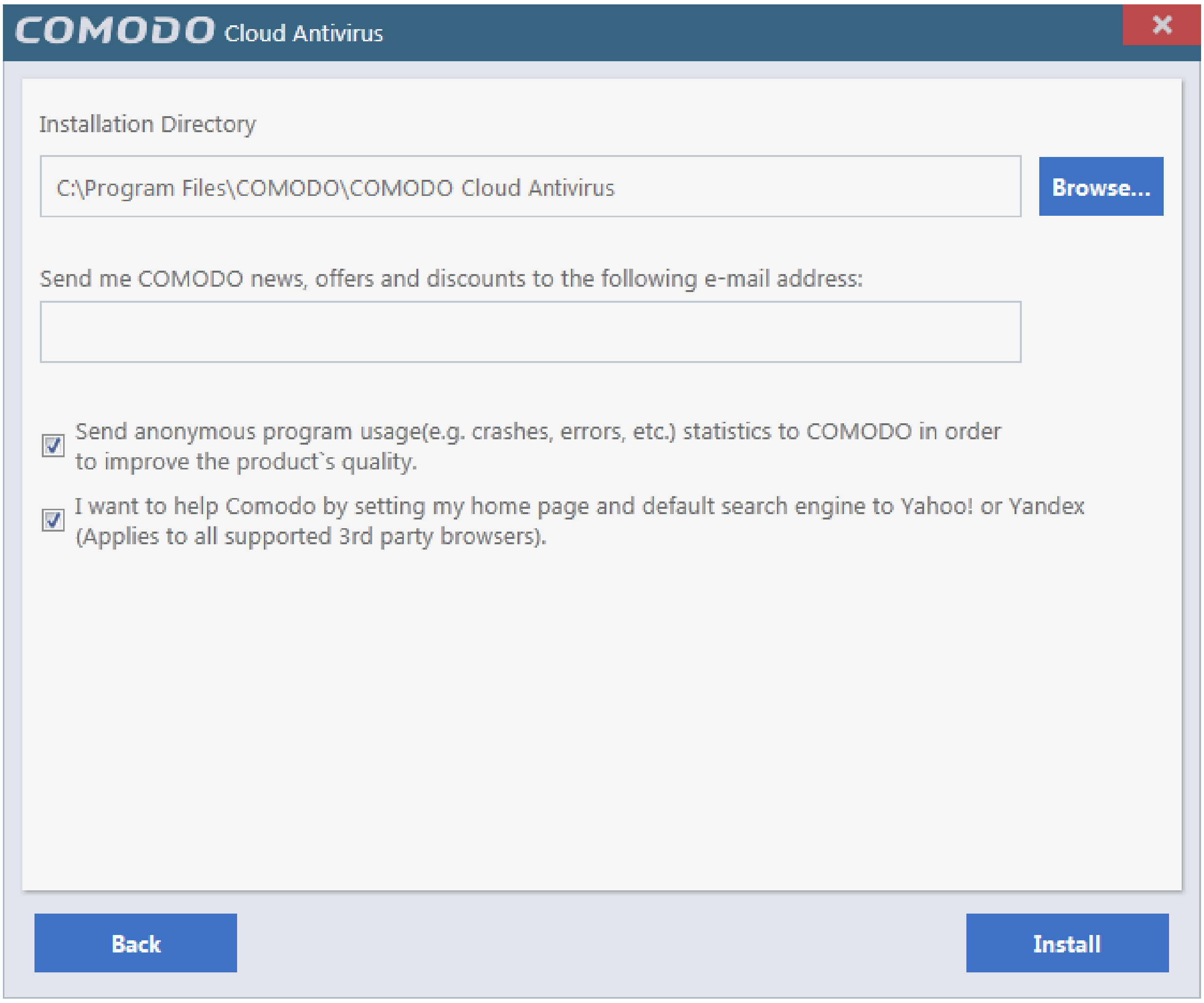
The Software offers users real time antivirus protection and manual scans, as well as the ability to auto-sandbox unknown files with portable sandbox and embedded virus scope. Logging of events and marking of trusted applications is also included.

This user license agreement is between you ("you" or "Subscriber"), as either an individual or as a business entity, and Comodo Security Solutions, Inc. ("Comodo"), which has its principal place of business at 1255 Broad Street, Suite 100, Clifton, New Jersey 07013. In exchange for your use of the Software, you agree as follows:

License

Grant of License. Comodo grants you a royalty-free, limited, non-exclusive, non-transferable,

- Click the 'Close' button to return to the installation configuration screen then click 'I agree' to begin installation wizard.



Installation Directory

C:\Program Files\COMODO\COMODO Cloud Antivirus

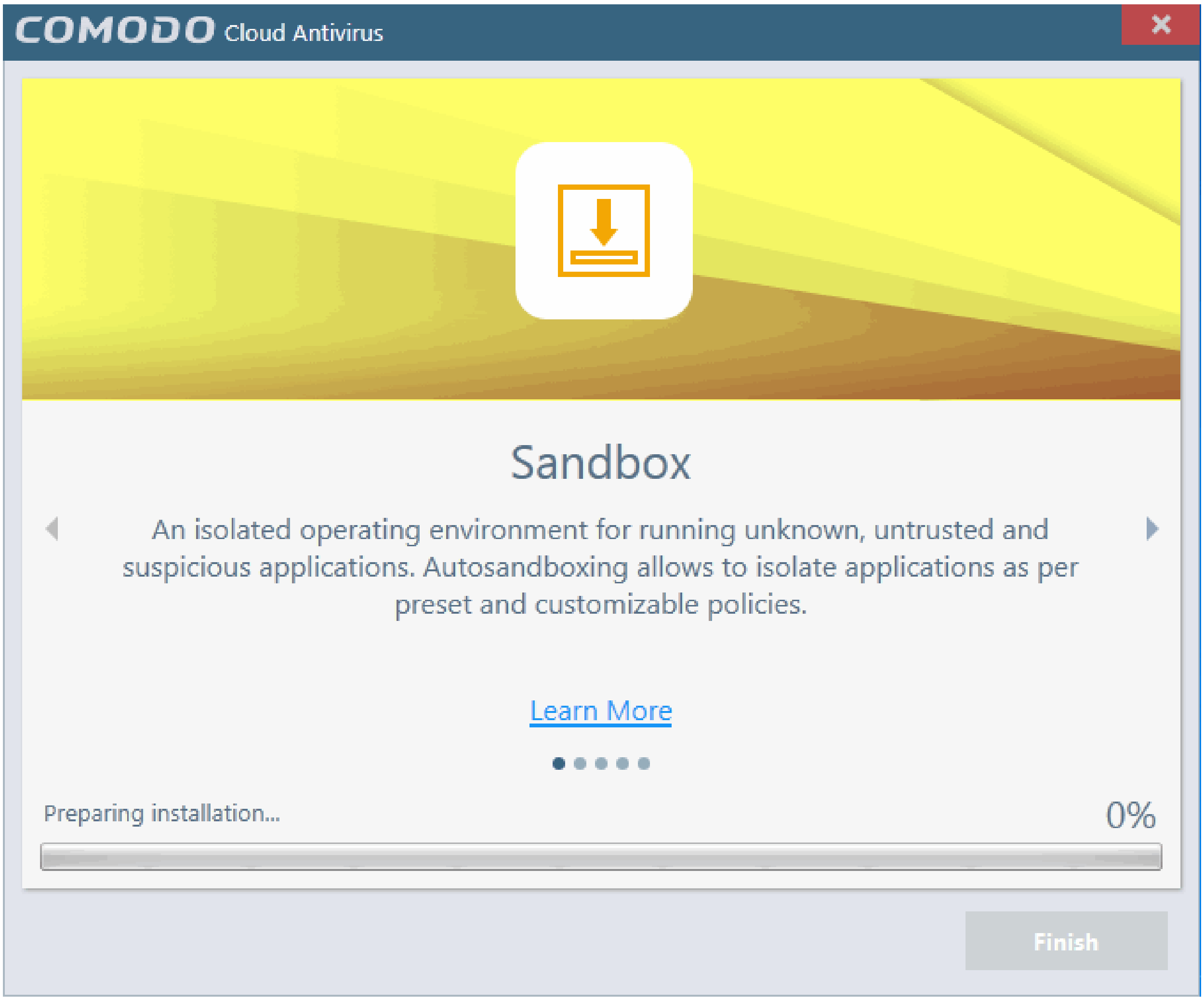
Send me COMODO news, offers and discounts to the following e-mail address:

☑ Send anonymous program usage(e.g. crashes, errors, etc.) statistics to COMODO in order to improve the product`s quality.

☑ I want to help Comodo by setting my home page and default search engine to Yahoo! or Yandex (Applies to all supported 3rd party browsers).

- The default installation location is C:\Program Files\COMODO\COMODO Cloud Antivirus. If you want to change this, click the 'Browse...' button, navigate to the desired location and click 'Open'.
- Enter your email address in the second field if you would like to subscribe for Comodo news and get offers and discounts from Comodo.
- Report errors – Select the check box at the end to send program usage errors such as crashes statics to Comodo.
- 'I want to help Comodo by setting my page and default engine to Yahoo! or Yandex (applies to all supported 3rd party browsers)' means:
  - When you enter a search item into the address bar of a supported browser, the search will be carried out by Yahoo/Yandex
  - A ‘Search with Yahoo' menu entry will be added to the right-click menu of supported browsers.
  - Yahoo!/Yandex will be set as the default search engine in the ‘Search’ box of supported browsers
  - The instant ‘search suggestions’ that you see when you start typing a search item will be provided by Yahoo!/Yandex.
- Click the 'Next' button.

The installation progress will be displayed and on completion...



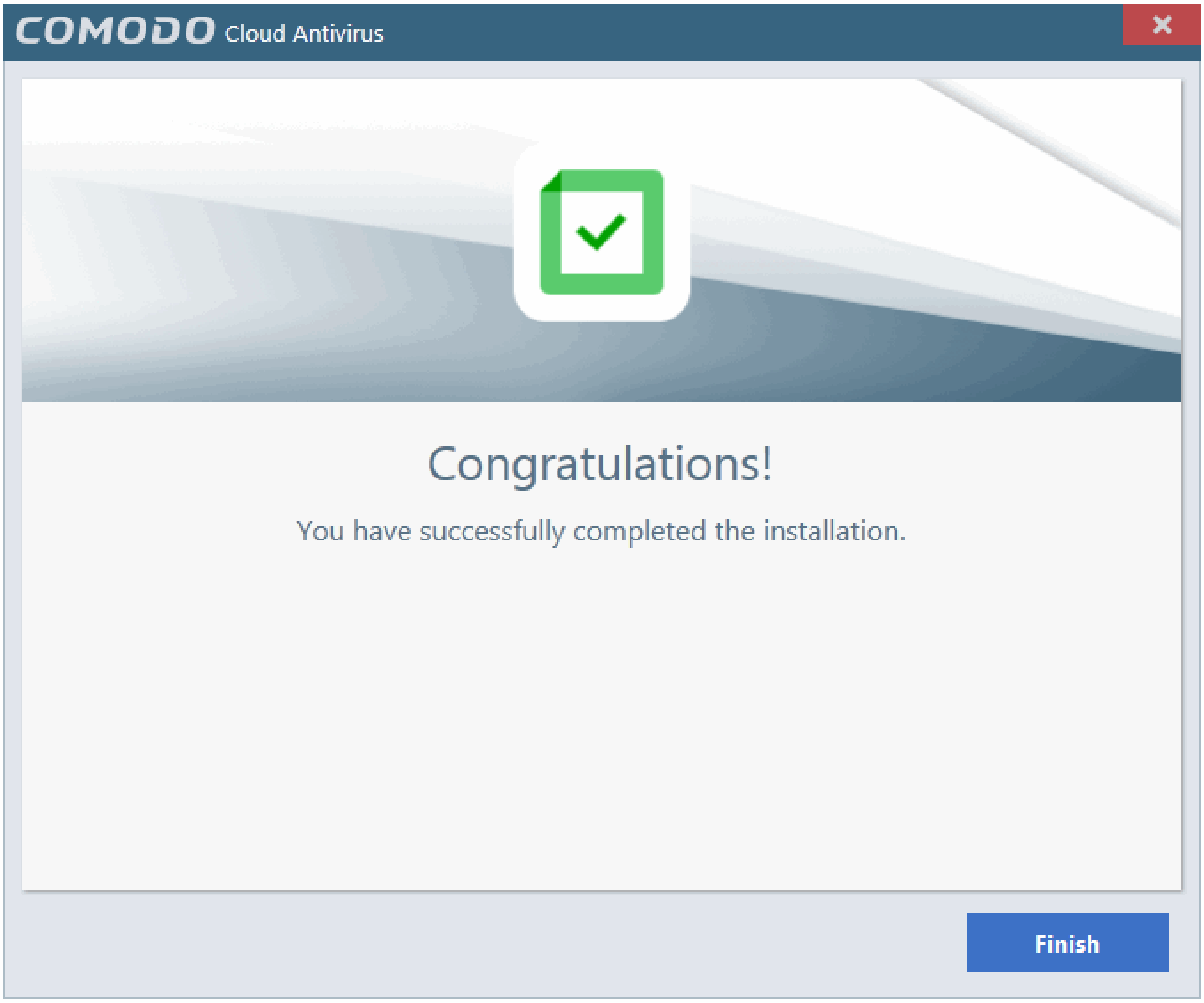
Sandbox

An isolated operating environment for running unknown, untrusted and suspicious applications. Autosandboxing allows to isolate applications as per preset and customizable policies.

Preparing installation...

0%

...the success message will be displayed.



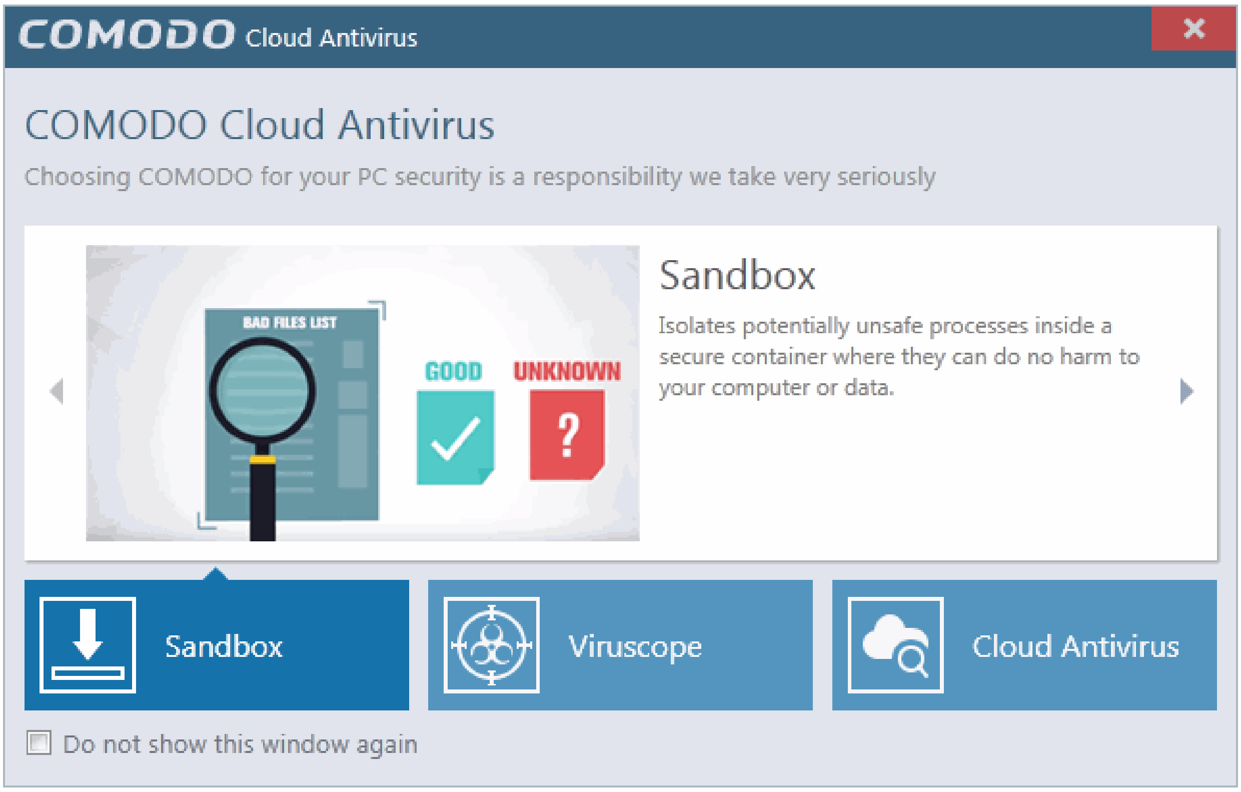
Congratulations!

You have successfully completed the installation.

- Click 'Close'

In order to finalize the installation, your system has to be restarted. Please save any unsaved data and restart the system.

- After restarting your computer CCAV will start automatically and a welcome screen will be displayed.



COMODO Cloud Antivirus

Choosing COMODO for your PC security is a responsibility we take very seriously

Sandbox

Isolates potentially unsafe processes inside a secure container where they can do no harm to your computer or data.

□ Do not show this window again

This screen will appear every time you start your system. If you do not want the screen to be displayed on every start up, select the check box 'Do not show this window again' before closing the window.

1.3. Starting Comodo Cloud Antivirus

After installation, Comodo Cloud Antivirus will automatically start running in the background whenever you start Windows. In order to configure and view settings within CCAV, you need to access the main interface.

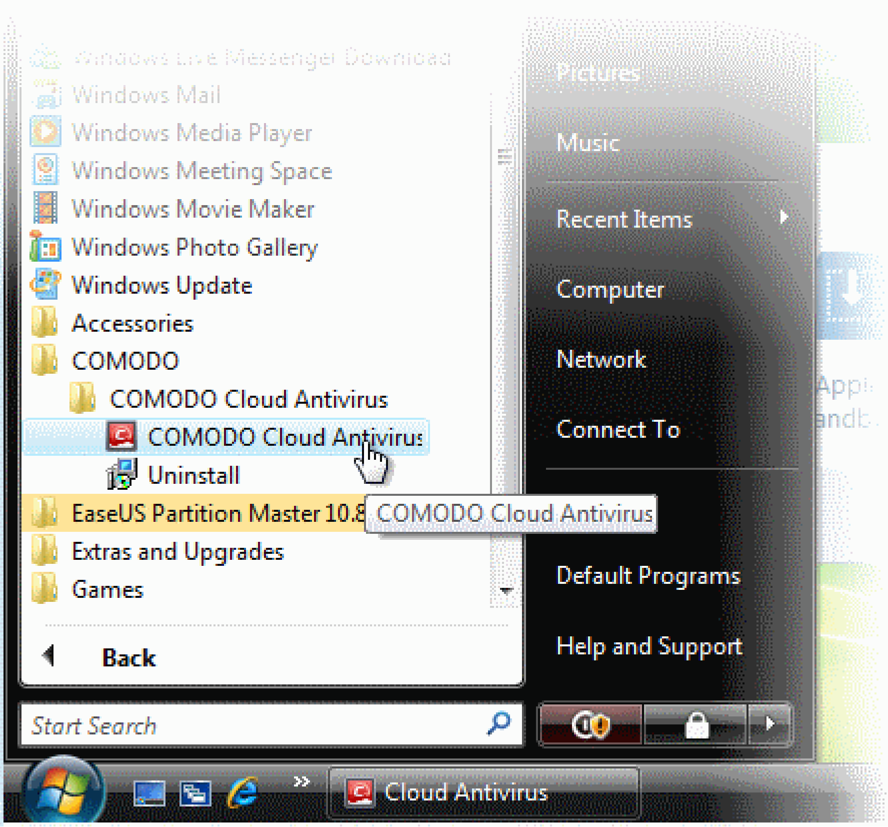
There are 3 different ways to open Comodo Cloud Antivirus:

- **Windows Start Menu**
- **Windows Desktop**
- **System Tray Icon**

Start Menu

You can access Comodo Cloud Antivirus via the Windows Start Menu.

- Click **Start** and select **All Programs** > **COMODO** > **COMODO Cloud Antivirus > COMODO Cloud Antivirus**

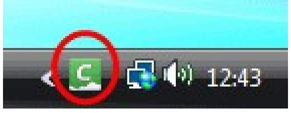


Windows Desktop

- Just double click the 'C' icon in the desktop to start Comodo Cloud Antivirus.

System Tray Icon

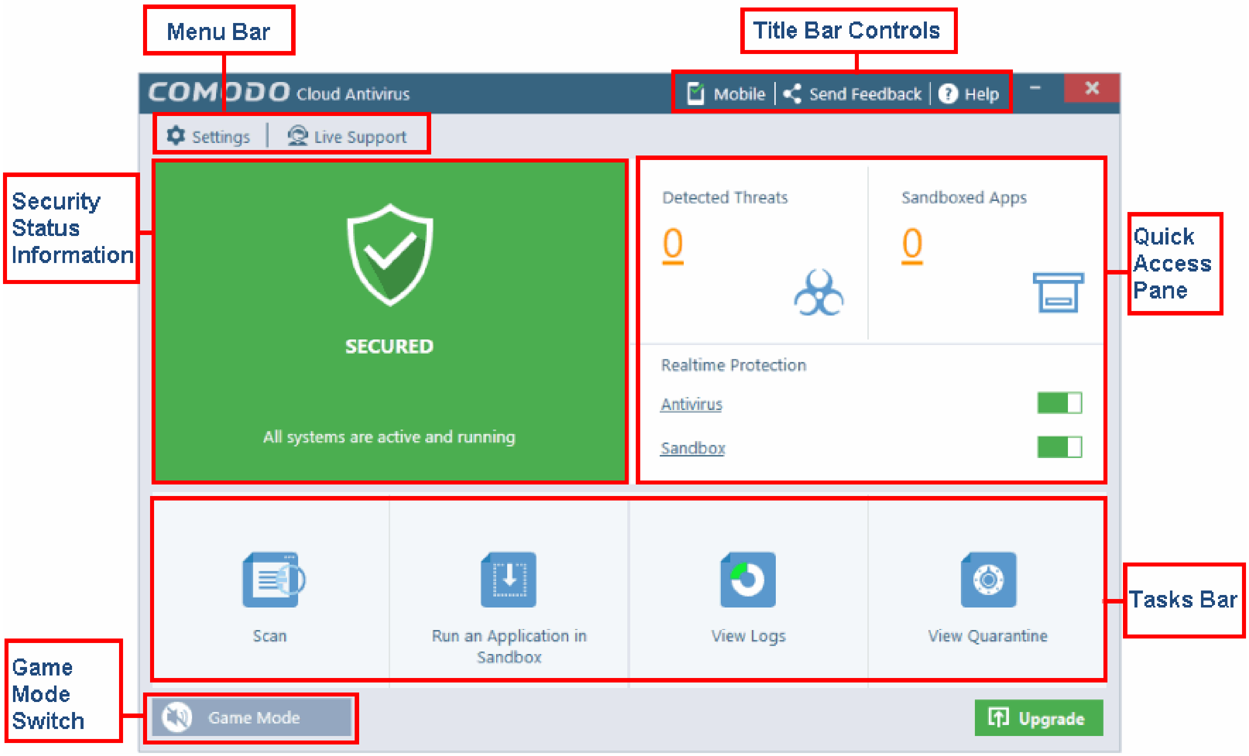
- Just double click the CCAV tray icon to start the main interface.



Right-clicking the tray icon provides quick access to some important settings. These include settings related to the Antivirus, Sandbox, Game Mode options and more. Refer to the section '**The System Tray Icon**' for more details.

1.3.1. The Main Interface

The CCAV interface is designed to be as clean and informative as possible while allowing to you carry out tasks you want with the minimum of fuss.



Menu Bar

- **Settings** – Allows you to configure protection and general settings such as antivirus configuration, sandbox configuration, manage trusted applications and more. Refer to the section '**CCAV Settings**' for more details.
- **Live Support** – Allows you to chat with a Comodo technician for any problems related to the application. Refer to the section '**Comodo Support and About Information**' for more details.

Tasks Bar

- **Scan** – Do a quick AV scan, full computer scan or configure a custom scan. Refer to the section '**Scan and Clean your Computer**' for more details.
- **Run an Application in Sandbox** – Run a browser or any application inside the sandbox for full security. Refer to the section '**Run an Application in the Sandbox**' for more details.
- **View Logs** – Allows you to view the logs of AV, sandbox and setting changes. Refer to the section '**View CCAV Logs**' for more details.
- **View Quarantine** – Manage the quarantined items from this interface. Refer to the section '**View and Manage Quarantined Items**' for more details.

Security Status Information

Indicates whether the protection systems are active or not. Refer to the sections '**Antivirus Configuration**' and '**Sandbox Configuration**' for more details.

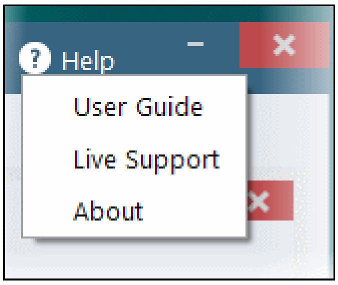
- **Secured** – Indicates the real-time protection is active.
- **At risk** – Indicates one or both the protection system are not active.
- **Game Mode** – Indicates that the 'Game Mode' is switched on.

Title Bar Controls

The title bar (top right) contains shortcuts for:

- **Comodo Mobile Security apps for Android phones and tablets**. - Click 'Mobile' to view and download Comodo mobile security apps such as 'Mobile Security', 'Anti-Theft', 'Back Up' and 'App Lock'. You can also get the apps from our website, **https://m.comodo.com/** or from the 'Google Play' app store.

- **Send Feedback –** Allows you to provide your comments on the product. Clicking on the 'Send Feedback' link will open the default email client in your system for you to provide feedback about CCAV.
- **Get Help** - Click 'Help' for the following options:



  - **User Guide** – Opens the CCAV online help guide at **https://help.comodo.com**
  - **Live Support** – Click this link to chat with our technician for technical help for CCAV.
  - **About** - Displays the product version, details of active Viruscope Recognizers and copyright information.

Quick Access Pane

- **Detected Threats** – Displays the number of threats detected by CCAV during real-time scanning as well as during manual scanning. Clicking on the number opens the 'Detected Threats' interface allowing you to define the threat. Refer to the section '**Managing Detected Threats**' for more details.
- **Sandboxed Apps** – Displays the number of applications that are running in the sandboxed environment. This includes auto-sandboxed applications and manually sandboxed applications. Refer to the section '**Managing Sandboxed Applications**' for more details.
- **Realtime Protection** – The toggle switch allows you a shortcut to switch on/off the antivirus and sandbox protection. Clicking the 'Antivirus' and 'Sandbox' links will open the respective settings screen. Refer to the sections '**Antivirus Configuration**' and '**Sandbox Configuration**' for more details.

Game Mode

Game Mode enables you to play your games without interruptions or alerts. Operations that can interfere with a user's gaming experience are either suppressed or postponed.

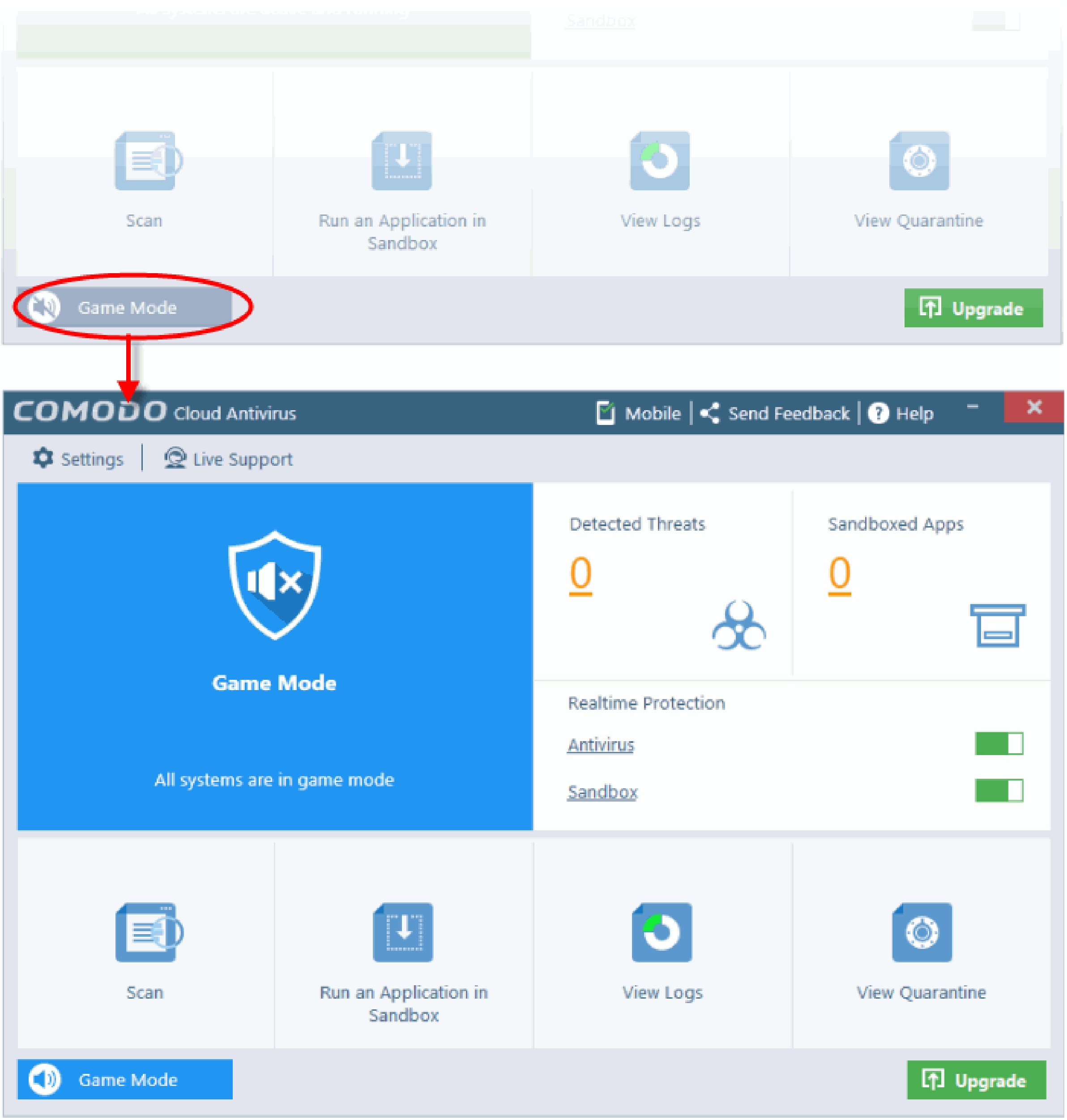
In game mode:

- AV, Viruscope and Sandbox alerts are suppressed.
- Automatic isolation of unknown applications and real-time virus detection are still functional.

To switch to Game mode

- Click the 'Game Mode' switch at the bottom left of the main interface.

The 'Security Status' pane will indicate 'Game Mode' status in blue:



All systems are in game mode

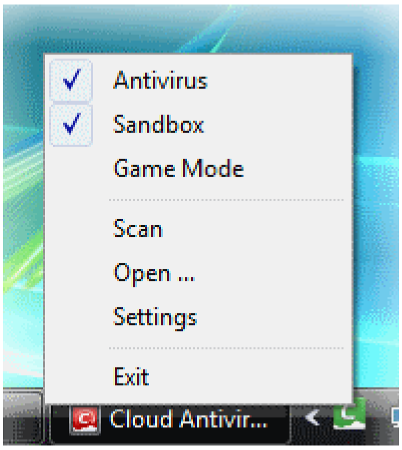
- Deactivate 'Game Mode' to resume alerts and notifications.

Upgrade

Clicking the 'Upgrade' button leads to the purchase page of 'Comodo Internet Security' (CIS), our full featured internet security solution. In addition to the features available in CCAV, CIS also includes a firewall, host intrusion prevention, online backup, 24/7 instant support and more.

1.3.2. The System Tray Icon

Double-clicking the system tray icon will quickly open the CCAV interface. Right-clicking the icon opens a context sensitive menu that allows you to configure various application settings:



- **Antivirus** – Allows you to switch on/off AV protection settings. Tick mark indicates the protection is on.
- **Sandbox** – Allows you to switch the automatic sandbox on or off. Tick mark indicates the protection is on.
- **Game Mode** – Allows to switch on/off 'Game Mode'. Tick mark indicates 'Game Mode' is on.
- **Scan** – Opens the scan dialog. Refer to the section '**Scan and Clean your Computer**' for more details.
- **Open** – Opens the CCAV application.
- **Settings** – Opens the settings interface. Refer to the section '**CCAV Settings**' for more details.
- **Exit** – Closes the CCAV application.

1.4. Understanding CCAV Alerts

CCAV alerts warn you about security related activities at the moment they occur. Each alert contains information about a particular issue so you can make an informed decision about whether to allow or block it. Alerts also let you specify how CCAV should behave in future when it encounters activities of the same type. The alerts also enable you to reverse the changes made to your computer by the applications that raised the security related event.

Alert Types

Comodo Cloud Antivirus alerts come in three main varieties. Click the name of the alert (at the start of the following bullets) if you want more help with a particular alert type.

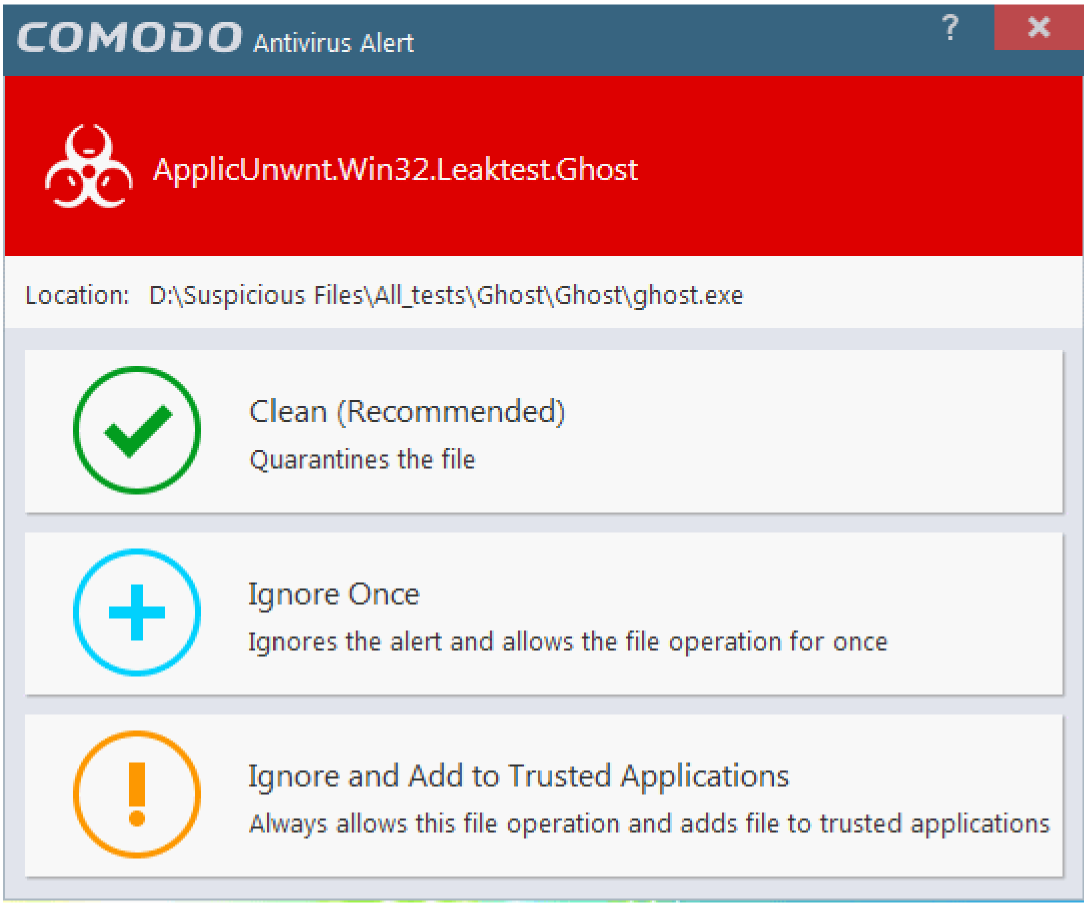
- **Antivirus Alerts** - Shown whenever virus or virus-like activity is detected. AV alerts will be displayed only when 'Enable Realtime Scan' is selected and the option 'Alert' for 'Action when threat is detected' is selected in **Real-time Scanner Settings**.
- **Sandbox Alerts** - Shown whenever an application tries to modify operating system or related files and when the CCAV sandboxes an unrecognizable file. Sandbox Alerts will be displayed only if '**Enable Auto-Sandbox**' is enabled.
- **Viruscope Alerts** - Shown whenever a sandboxed process attempts to take suspicious actions, and when a non-sandboxed installer or updater takes suspicious actions. Viruscope alerts allow you to quarantine the process or let the process continue. Be especially wary if a Viruscope alert pops up 'out-of-the-blue' when you have not made any recent changes to your computer. Viruscope Alerts will be displayed only when **Viruscope is enabled** under Sandbox.

In each case, the alert may contain very important security warnings or may simply occur because you are running a certain application for the first time. Your reaction should depend on the information that is presented at the alert.

Answering an Antivirus Alert

Comodo Cloud Antivirus generates an 'Antivirus' alert whenever a virus or virus-like activity is detected on your computer. The alert contains the name of the virus detected and the location of the file or application infected by it. Within the alert, you are also presented with response-options such as 'Clean', 'Ignore Once' and 'Ignore and Add to Trusted Applications'.

Note: Antivirus alerts will be displayed only when 'Enable Realtime Scan' is selected and the option 'Alert' for 'Action when threat is detected' is selected in **Real-time Scanner Settings**.



COMODO Antivirus Alert

ApplicUnwnt.Win32.Leaktest.Ghost

Location: D:\Suspicious Files\All_tests\Ghost\Ghost\ghost.exe

Clean (Recommended)
Quarantines the file

Ignore Once
Ignores the alert and allows the file operation for once

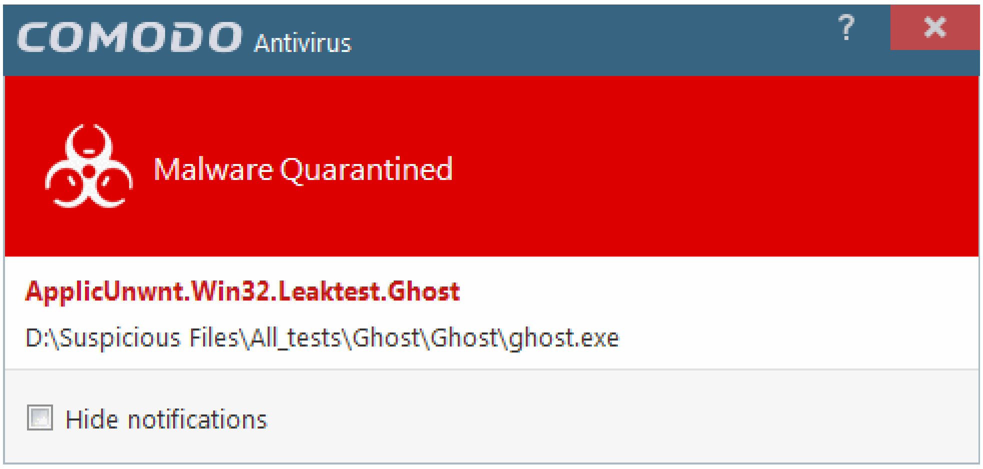
Ignore and Add to Trusted Applications
Always allows this file operation and adds file to trusted applications

The following response-options are available:

- **Clean** - Disinfects the file if a disinfection routine exists. If no routine exists for the file then it will be moved to Quarantine. If desired, you can submit the file/application to Comodo for analysis from the **Quarantine** interface. Refer to **View and Manage Quarantined Items** for more details on quarantined files.
- **Ignore Once** - Allows the process to run and does not attempt to clean the file or move it to quarantine. Only click 'Ignore Once' if you are absolutely sure the file is safe. An alert will generated again for the file if it is run again.
- **Ignore and Add to Trusted Applications** - Allows the process to run and the file will be added to the trusted applications list. Select this option only if you are absolutely sure the file is safe. No alert will be generated for this file in the future.

Antivirus Notification

If you have chosen either 'Block' or 'Quarantine' for the option 'Action when threat is detected' in **Real-time Scanner Settings**,it will be immediately blocked or quarantined and provide you with instant on-screen notification.



COMODO Antivirus

Malware Quarantined

ApplicUnwnt.Win32.Leaktest.Ghost

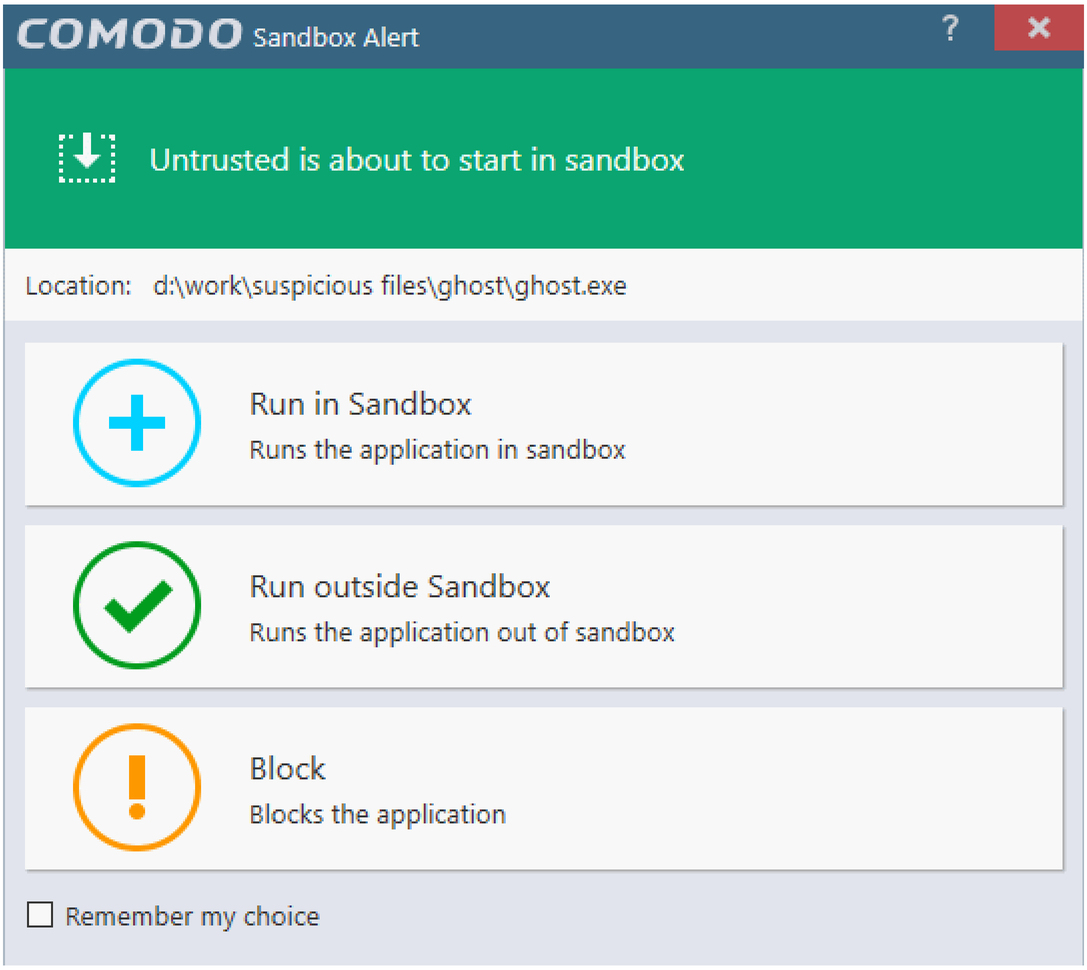
D:\Suspicious Files\All_tests\Ghost\Ghost\ghost.exe

□ Hide notifications

Please note that these antivirus notifications will be displayed only when you have chosen either 'Block' or 'Quarantine' for the option 'Action when threat is detected' in **Real-time Scanner Settings**, *and* 'Show notifications' check box is enabled in **'General Settings'** > '**Customize User Interface**' screen.

Answering a Sandbox Alert

Comodo Cloud Antivirus generates an 'Sandbox' alert whenever an application rated as 'Untrusted' or 'Unknown' is executed. The alert contains the location from which the application is trying to execute. Within the alert, you are also presented with response-options such as 'Run in Sandbox', 'Run outside Sandbox' and 'Block'.



COMODO Sandbox Alert

Untrusted is about to start in sandbox

Location: d:\work\suspicious files\ghost\ghost.exe

Run in Sandbox
Runs the application in sandbox

Run outside Sandbox
Runs the application out of sandbox

Block
Blocks the application

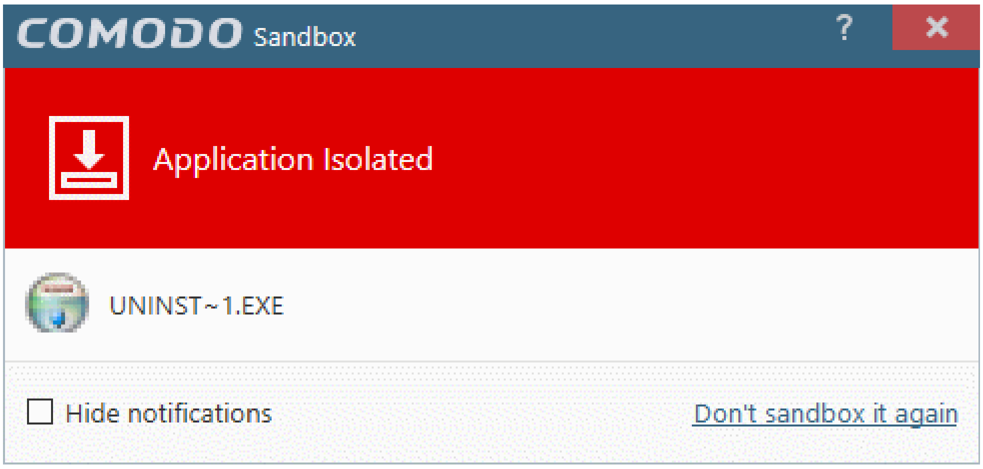
□ Remember my choice

Note: Sandbox alerts will be displayed only when 'Enable Auto-sandbox' is selected and the option 'Alert for untrusted files' is chosen in **Sandbox Settings**.

- **Run in Sandbox** – The application will be run inside the sandbox. This is useful, for example, if you wish to sandbox an application from a trusted vendor. Similarly, you may wish to sandbox your internet browser so that you can surf from within a security hardened environment.
- **Run Outside Sandbox** – The application will be run outside of the sandbox. This is useful, for example, if you wish to create an exception for an application that CCAV considers untrusted. This situation can occur for beta software, unsigned software or applications from relatively new vendors. CCAV will generate alert if you execute the application in future unless you select 'Remember my choice' at the bottom of the alert.
- **Block** – The application will be prevented from running by CCAV.
- If you want CCAV to take the same action as you have chosen for the application in future, select 'Remember my choice' check-box at the bottom of the alert.

Sandbox Notification

If you have chosen 'Sandbox all untrusted files' in the '**Sandbox Settings**' interface any untrusted application that is executed will be automatically sandboxed and a notification will be displayed.



- Clicking 'Don't sandbox it again' assigns 'Trusted' status to the file, so that the application will not be auto-sandboxed in future. Choose this option if you are absolutely sure that the executable is safe.
- If you do not want these notifications to be displayed in future, select 'Hide notifications' checkbox.

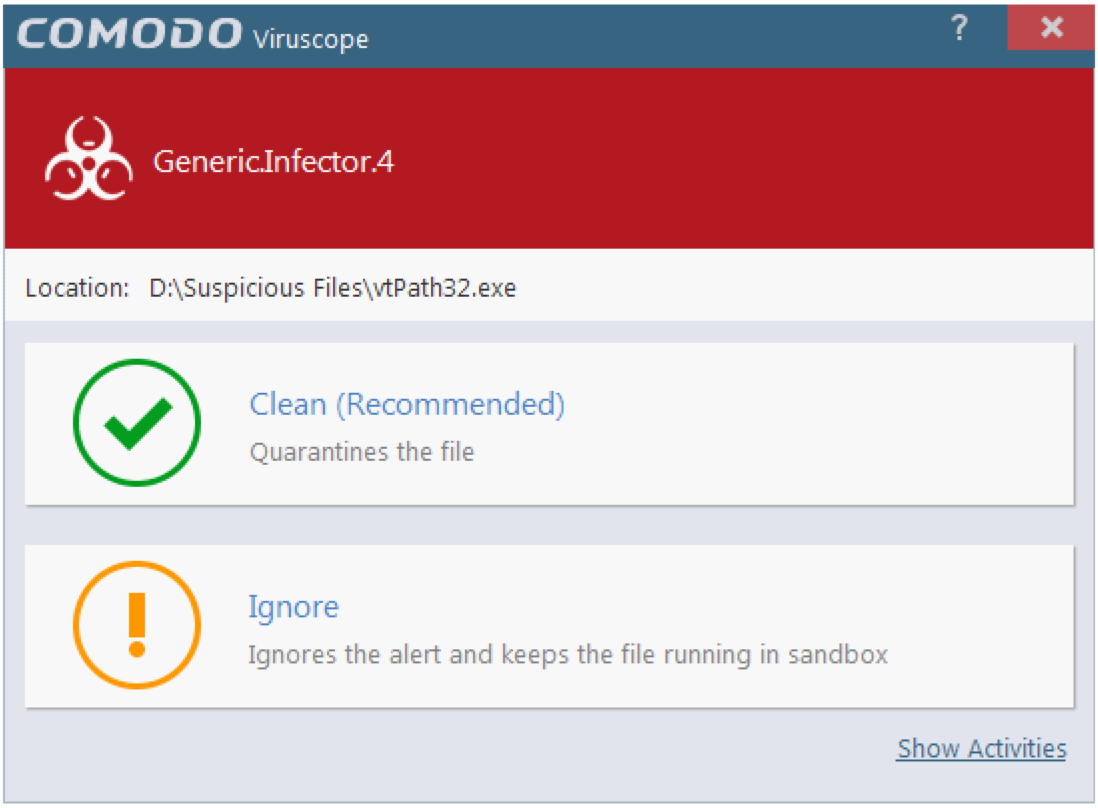
Please note that these 'Sandbox' notifications will be displayed only when you have chosen 'Sandbox all untrusted files' in the '**Sandbox Settings**' interface *and* 'Show notifications' check box is enabled in '**General Settings**' > '**Customize User Interface**' screen.

Answering a Viruscope Alert

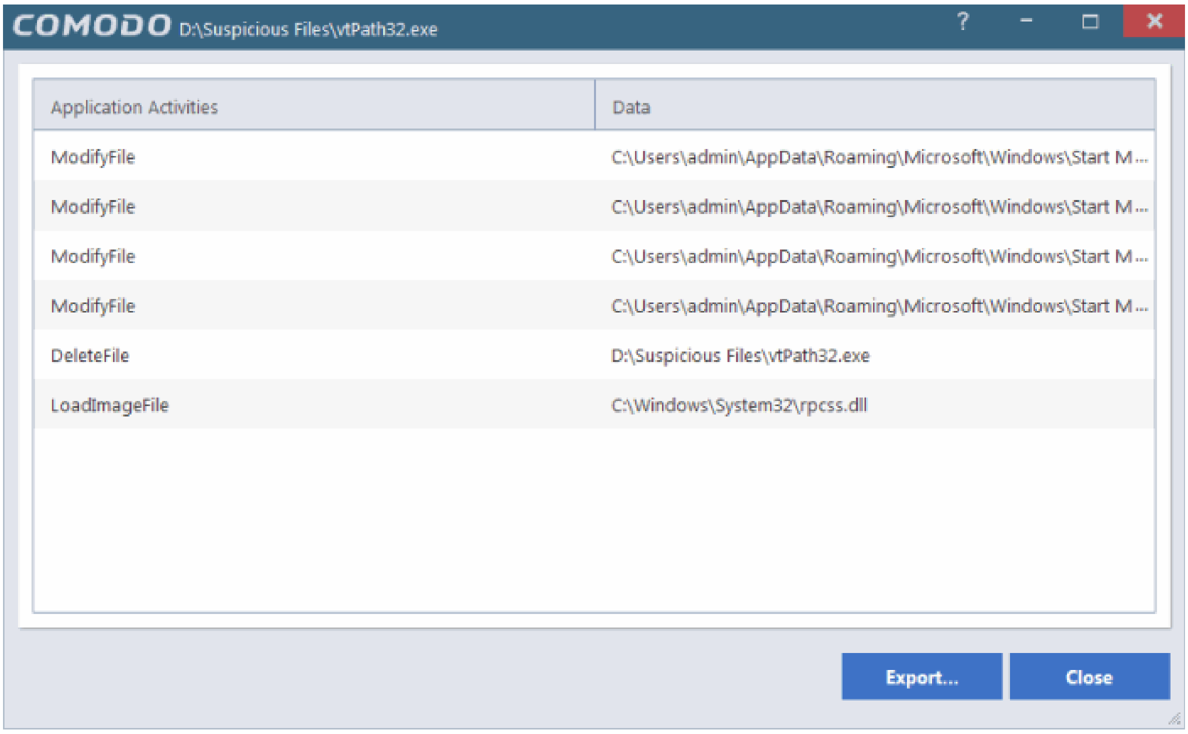
CCAV generates a Viruscope alert if a sandboxed process performs an action that might represent a threat to your privacy and/or security. Please note that Viruscope alerts are not always definitive proof that malicious activity has taken place. Rather, they are an indication that a process has taken actions that you ought to review and confirm because they have the potential to be malicious. You can review all actions taken by clicking the 'Show Activities' link.

Please read the following advice before answering a Viruscope alert:

1. Carefully read the information displayed in the alert.


COMODO Viruscope
Generic.Infector.4
Location: D:\Suspicious Files\vtPath32.exe
Clean (Recommended)
Quarantines the file
Ignore
Ignores the alert and keeps the file running in sandbox
Show Activities

- If you are not sure of the authenticity of the parent application indicated in the 'Location' field, you can move it to quarantine by clicking 'Clean'.
- If it is an application you trust, you can allow the process to run by clicking 'Ignore'.
- To view the activities of the process, click the 'Show Activities' link at the bottom right. The 'Process Activities List' dialog will open with a list of activities exhibited by the process.



Application Activities	Data
ModifyFile	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start M...
ModifyFile	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start M...
ModifyFile	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start M...
ModifyFile	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start M...
DeleteFile	D:\Suspicious Files\vtPath32.exe
LoadImageFile	C:\Windows\System32\rpcss.dll

Column Descriptions

- Application Activities - Displays the activities of each of the processes run by the parent application.

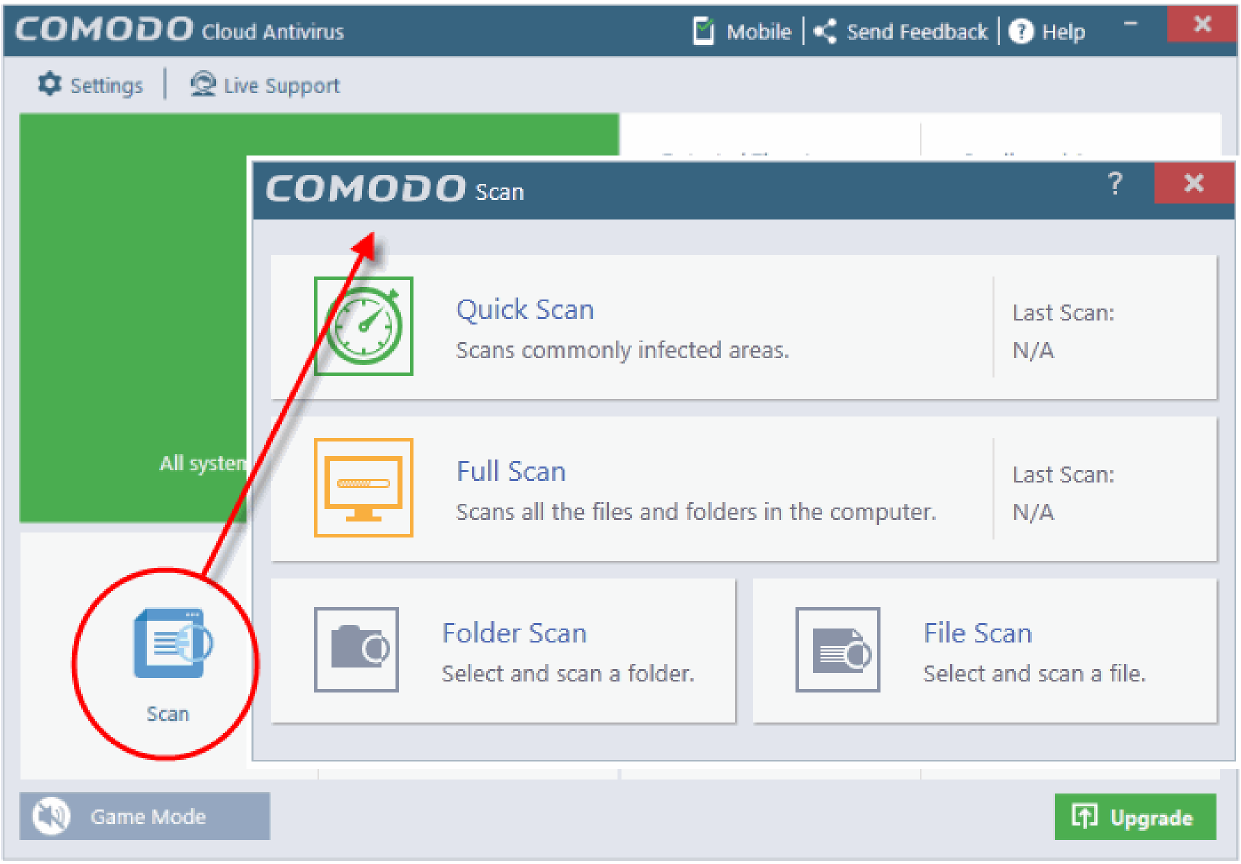
- Data - Displays the file affected by the action.

You can save the activities list for analysis at a later time by clicking the 'Export...' button at the bottom.

2. Scan and Clean your Computer

Comodo Cloud Antivirus leverages multiple technologies, including Real-time/On-Access Scanning and On-Demand Scanning to immediately start removing or quarantining suspicious files from your hard drives, shared disks, emails, downloads and system memory. The application also features full event logging, quarantine and file submission facilities. When you want to run a virus scan on your system, you can launch an **On-Demand Scan** using the **Scan** option. This executes an instant virus scan on the selected item or on the full computer. You can also use the right-click options to run a scan for an entire drive/folder/file.

- To open the 'Scan' interface, click 'Scan' from the 'Tasks Bar'.



There are multiple types of antivirus scans that can be run from the 'Scan' interface. The following sections explain more about each scan type, how to process infected files and manage detected threats.

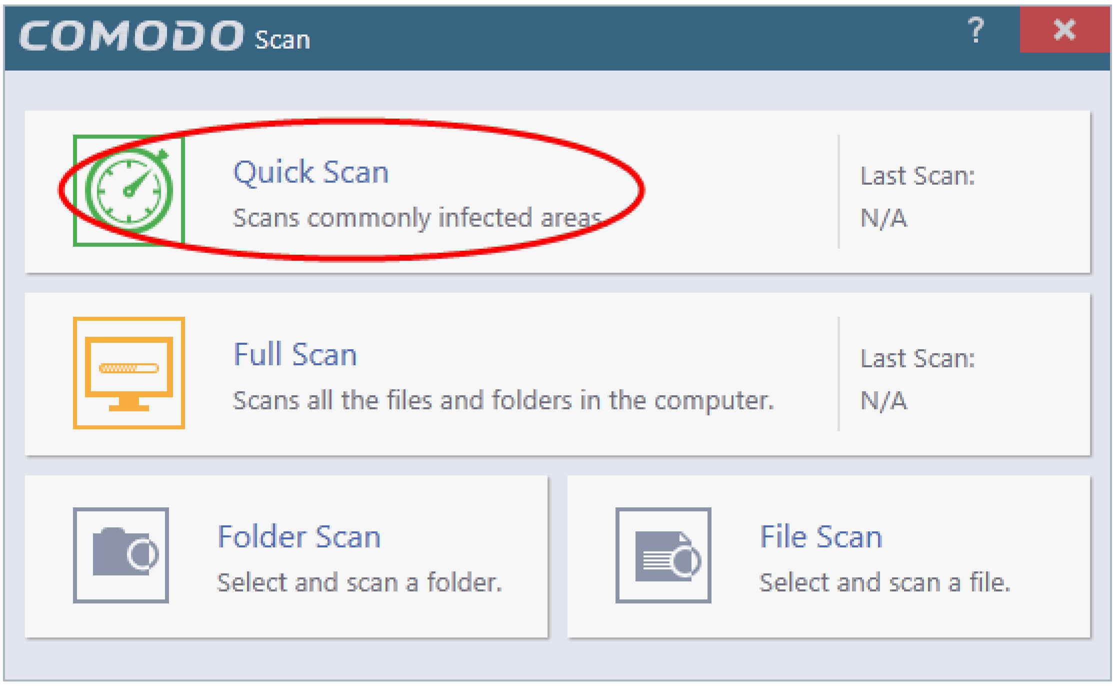
- Run a Quick Scan
- Run a Full Computer Scan
- Run a Custom Scan
  - Scan a Folder
  - Scan a File
- Processing Infected Files
- Managing Detected Threats

2.1. Run a Quick Scan

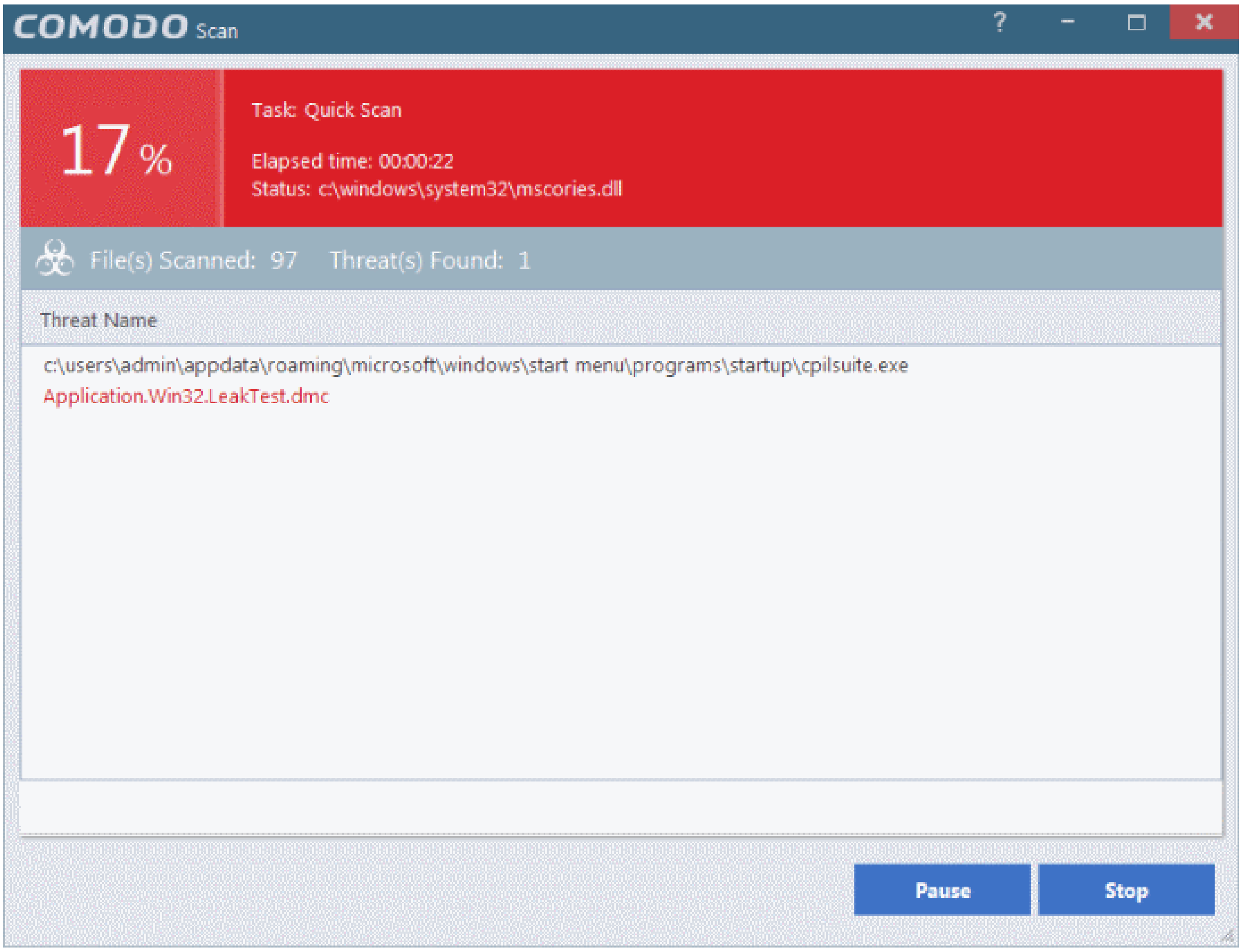
The 'Quick Scan' feature enables you to quickly scan those important areas of your computer which are highly prone to infection. Areas scanned include system memory, auto-run entries, hidden services, boot sectors and other significant areas like important registry keys and system files. These areas are of great importance to the health of your computer so it is essential to keep them free of infection.

To run a Quick Scan

- Click 'Scan' from the 'Tasks Bar' and click 'Quick Scan' from the 'Scan' interface.


COMODO Scan
?
×
Quick Scan
Scans commonly infected areas
Last Scan:
N/A
Full Scan
Scans all the files and folders in the computer.
Last Scan:
N/A
Folder Scan
Select and scan a folder.
File Scan
Select and scan a file.

The scanner will start and the scan progress will be displayed:



Task: Quick Scan

Elapsed time: 00:00:22

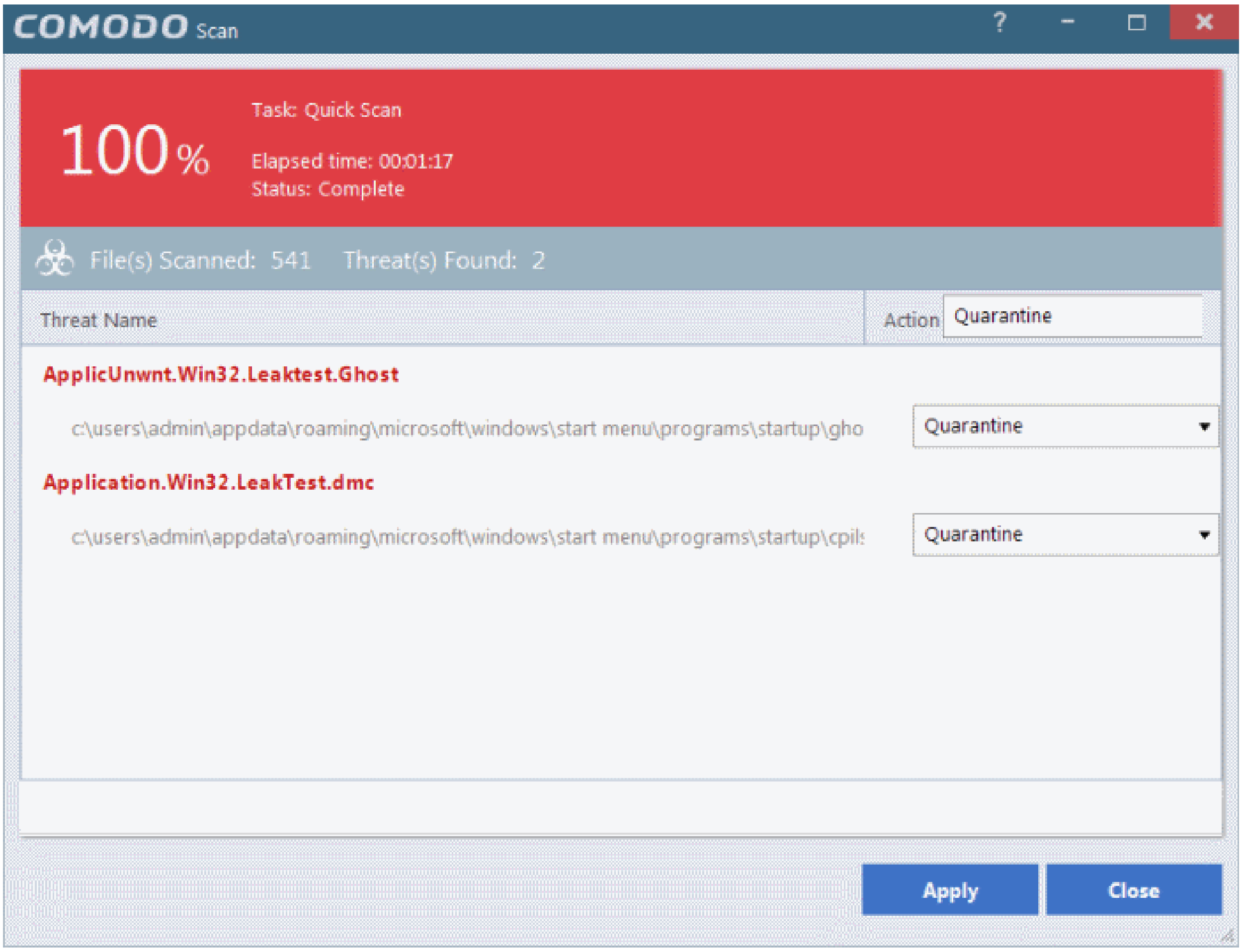
Status: c:\windows\system32\mscories.dll

File(s) Scanned: 97   Threat(s) Found: 1

Threat Name
c:\users\admin\appdata\roaming\microsoft\windows\start menu\programs\startup\cpilsuite.exe Application.Win32.LeakTest.dmc

- You can pause, continue or stop the scan by clicking the appropriate button.

The results window will be displayed after the scanning process is completed.



Task: Quick Scan

Elapsed time: 00:01:17

Status: Complete

File(s) Scanned: 541 Threat(s) Found: 2

Threat Name	Action: Quarantine
ApplicUnwnt.Win32.Leaktest.Ghost c:\users\admin\appdata\roaming\microsoft\windows\start menu\programs\startup\gho	Quarantine
Application.Win32.LeakTest.dmc c:\users\admin\appdata\roaming\microsoft\windows\start menu\programs\startup\cpil:	Quarantine

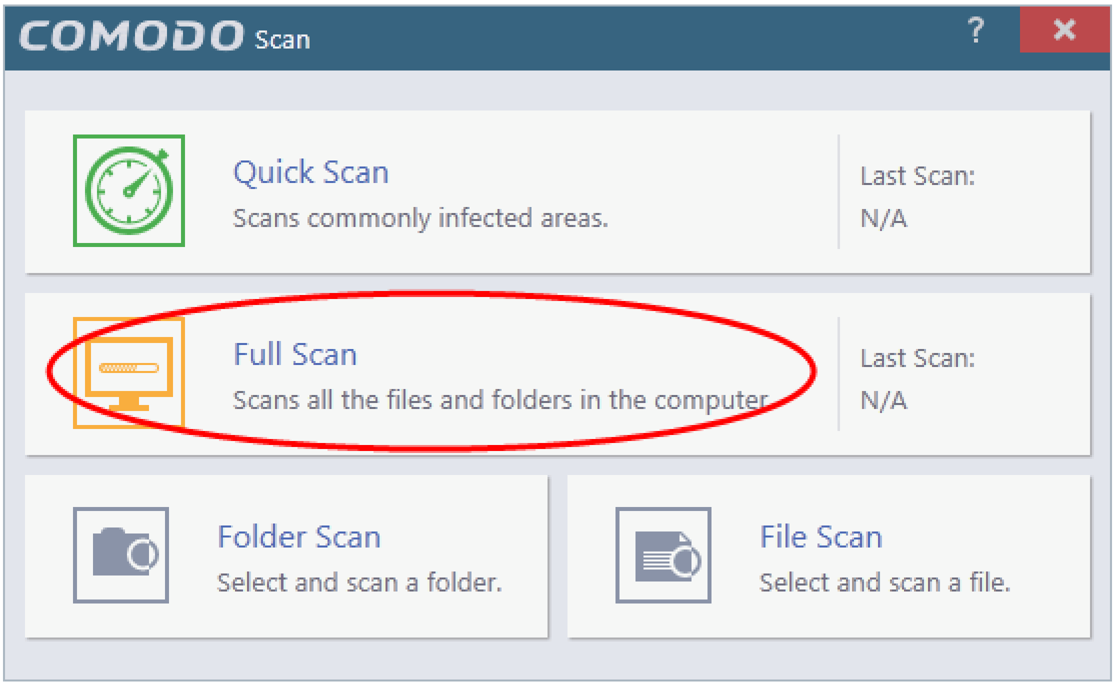
The results window shows the number of objects scanned and the number of threats (Viruses, Rootkits, Malware). Use the drop-down menu to choose whether to clean, move to quarantine or ignore the threat. Refer to **Processing the infected files** for more details.

2.2. Run a Full Computer Scan

A 'Full System Scan' scans every local drive, folder and file on your system. External devices such as USB drives, storage drives and digital cameras will also be scanned.

To run a Full Computer Scan

- Click 'Scan' from the 'Tasks Bar' and click 'Full Scan' from the 'Scan' interface.



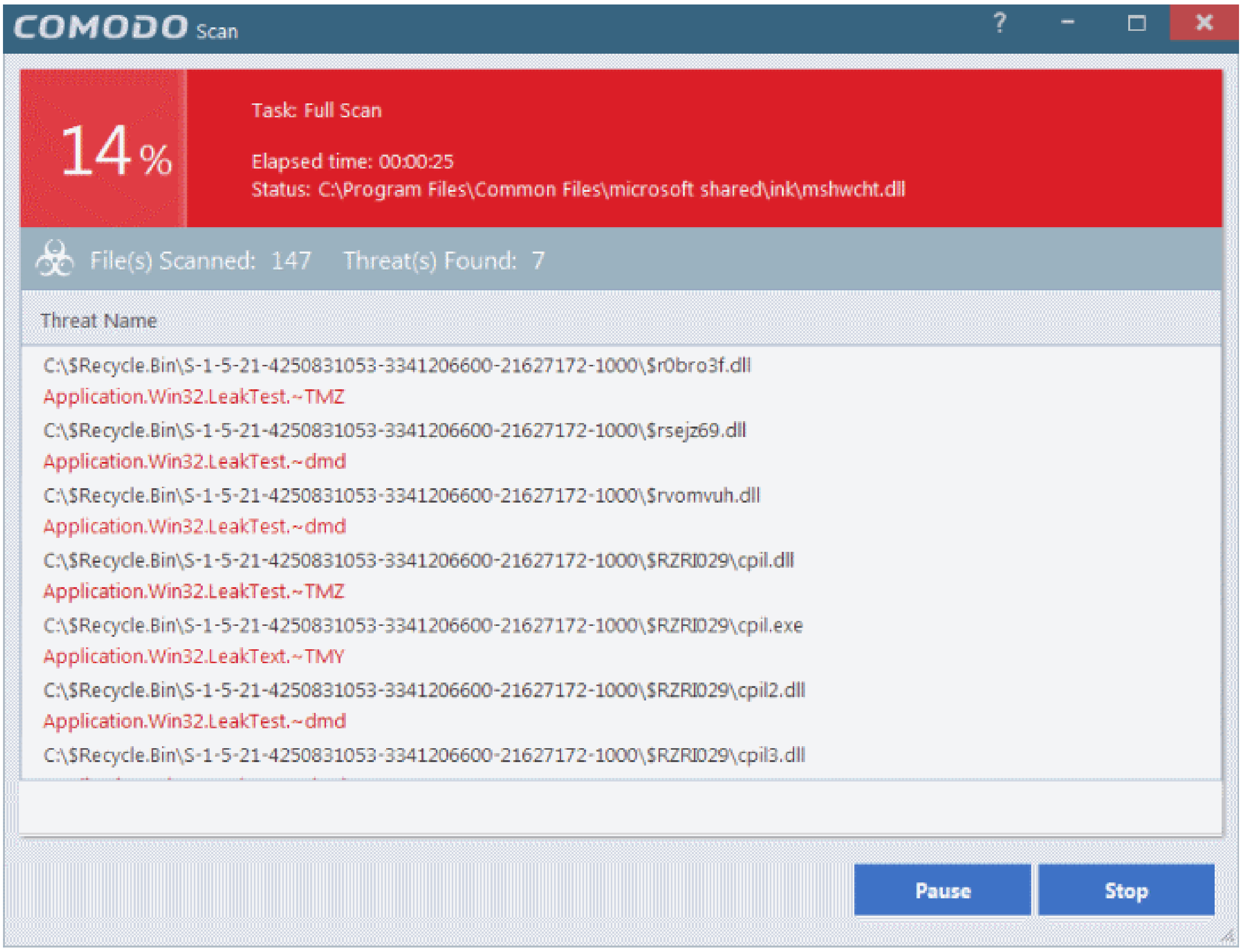
Quick Scan
Scans commonly infected areas.
Last Scan:
N/A

Full Scan
Scans all the files and folders in the computer
Last Scan:
N/A

Folder Scan
Select and scan a folder.

File Scan
Select and scan a file.

The scanner will start and the scan progress will be displayed:



14%

Task: Full Scan

Elapsed time: 00:00:25
Status: C:\Program Files\Common Files\microsoft shared\ink\mshwcht.dll

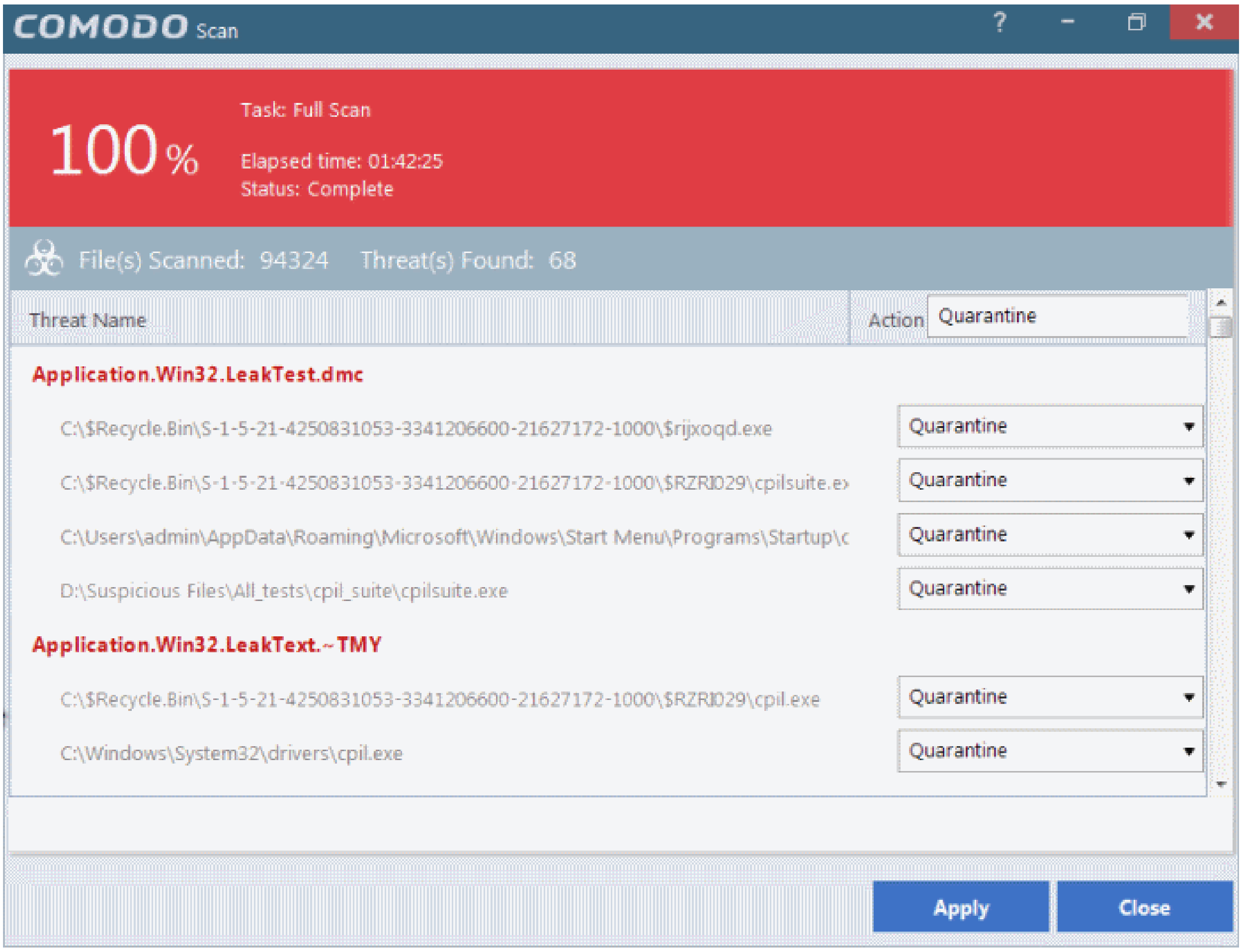
File(s) Scanned: 147 Threat(s) Found: 7

Threat Name

```
C:\$Recycle.Bin\S-1-5-21-4250831053-3341206600-21627172-1000\$r0bro3f.dll
Application.Win32.LeakTest.~TMZ
C:\$Recycle.Bin\S-1-5-21-4250831053-3341206600-21627172-1000\$rsejz69.dll
Application.Win32.LeakTest.~dmd
C:\$Recycle.Bin\S-1-5-21-4250831053-3341206600-21627172-1000\$rvomvuh.dll
Application.Win32.LeakTest.~dmd
C:\$Recycle.Bin\S-1-5-21-4250831053-3341206600-21627172-1000\$RZRI029\cpil.dll
Application.Win32.LeakTest.~TMZ
C:\$Recycle.Bin\S-1-5-21-4250831053-3341206600-21627172-1000\$RZRI029\cpil.exe
Application.Win32.LeakText.~TMY
C:\$Recycle.Bin\S-1-5-21-4250831053-3341206600-21627172-1000\$RZRI029\cpil2.dll
Application.Win32.LeakTest.~dmd
C:\$Recycle.Bin\S-1-5-21-4250831053-3341206600-21627172-1000\$RZRI029\cpil3.dll
```

- You can pause, continue or stop the scan by clicking the appropriate button.

The results window will be displayed after the scanning process is completed.



100 %

Task: Full Scan

Elapsed time: 01:42:25

Status: Complete

File(s) Scanned: 94324 Threat(s) Found: 68

Threat Name	Action: Quarantine
Application.Win32.LeakTest.dmc	
C:\$Recycle.Bin\S-1-5-21-4250831053-3341206600-21627172-1000\$rijxoqd.exe	Quarantine
C:\$Recycle.Bin\S-1-5-21-4250831053-3341206600-21627172-1000\$RZRI029\cpilsuite.ex	Quarantine
C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\c	Quarantine
D:\Suspicious Files\All_tests\cpil_suite\cpilsuite.exe	Quarantine
Application.Win32.LeakText.~TMY	
C:\$Recycle.Bin\S-1-5-21-4250831053-3341206600-21627172-1000\$RZRI029\cpil.exe	Quarantine
C:\Windows\System32\drivers\cpil.exe	Quarantine

The scan results window displays the number of objects scanned and the number of threats detected (viruses, rootkits, malware and so on). You can choose to move the files to quarantine or ignore the threat based in your assessment. Refer to **Processing the infected files** for more details.

2.3. Run a Custom Scan

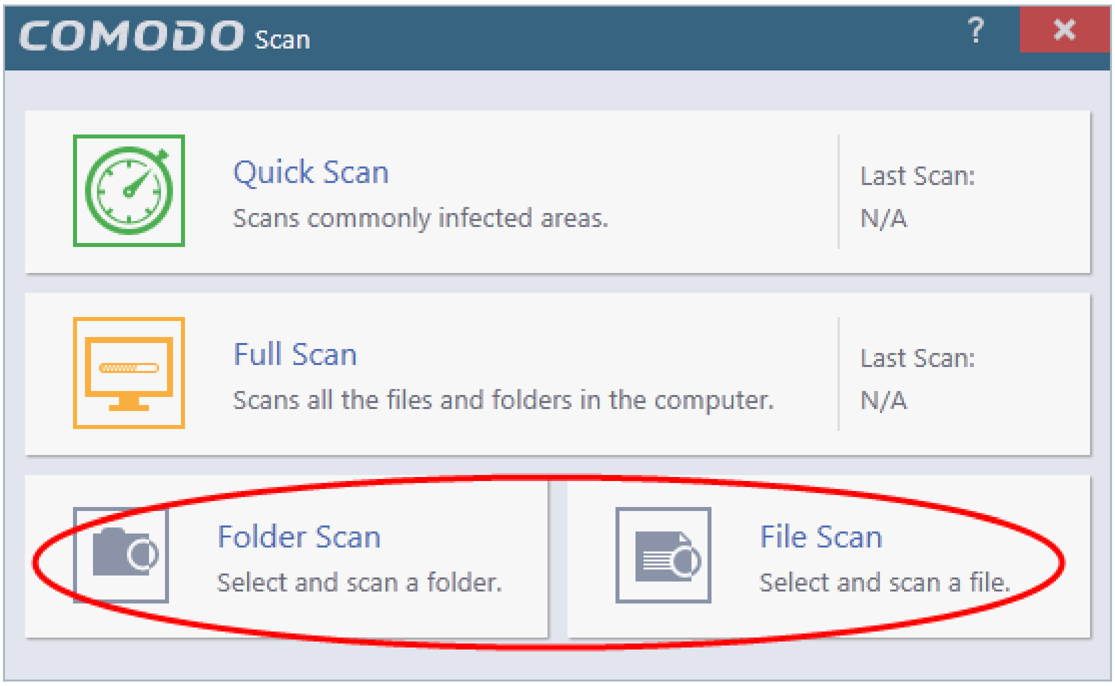
Comodo Cloud Antivirus allows you to scan specific areas, drives, folders or files in your computer.

To run a custom scan

- Click 'Scan' from the 'Tasks Bar' and then click 'Folder Scan' or 'File Scan' from the 'Scan' interface.

Click the following links to find out more about each type:

- **Folder Scan** - scan individual folders
- **File Scan** - scan an individual file

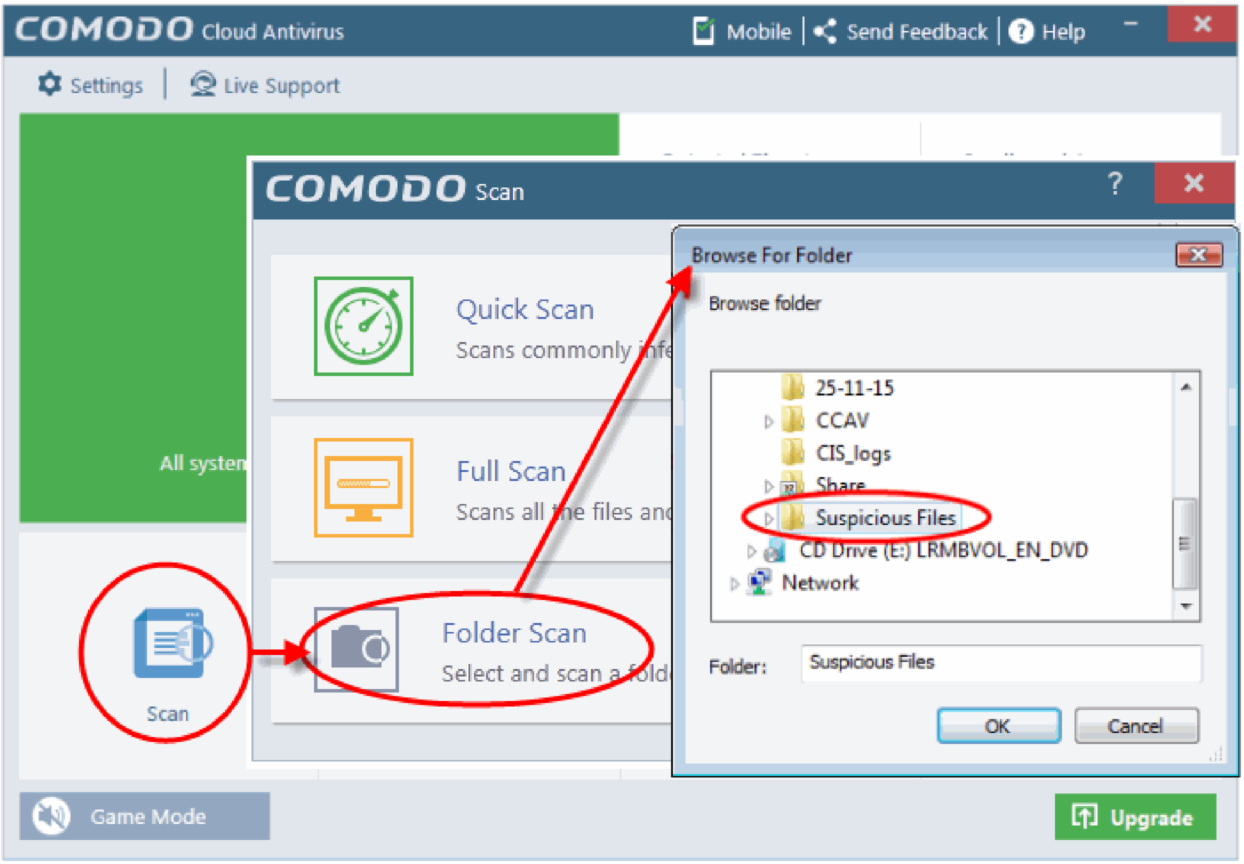

COMODO Scan
?
✕
Quick Scan
Scans commonly infected areas.
Last Scan:
N/A
Full Scan
Scans all the files and folders in the computer.
Last Scan:
N/A
Folder Scan
Select and scan a folder.
File Scan
Select and scan a file.

2.3.1. Scan a Folder

The 'Folder Scan' option allows you to scan a specific folder on your hard drive, CD/DVD or external device. For example you might have copied a folder from another computer in your network, an external device or downloaded from Internet and want to scan it for viruses and other threats before you open it.

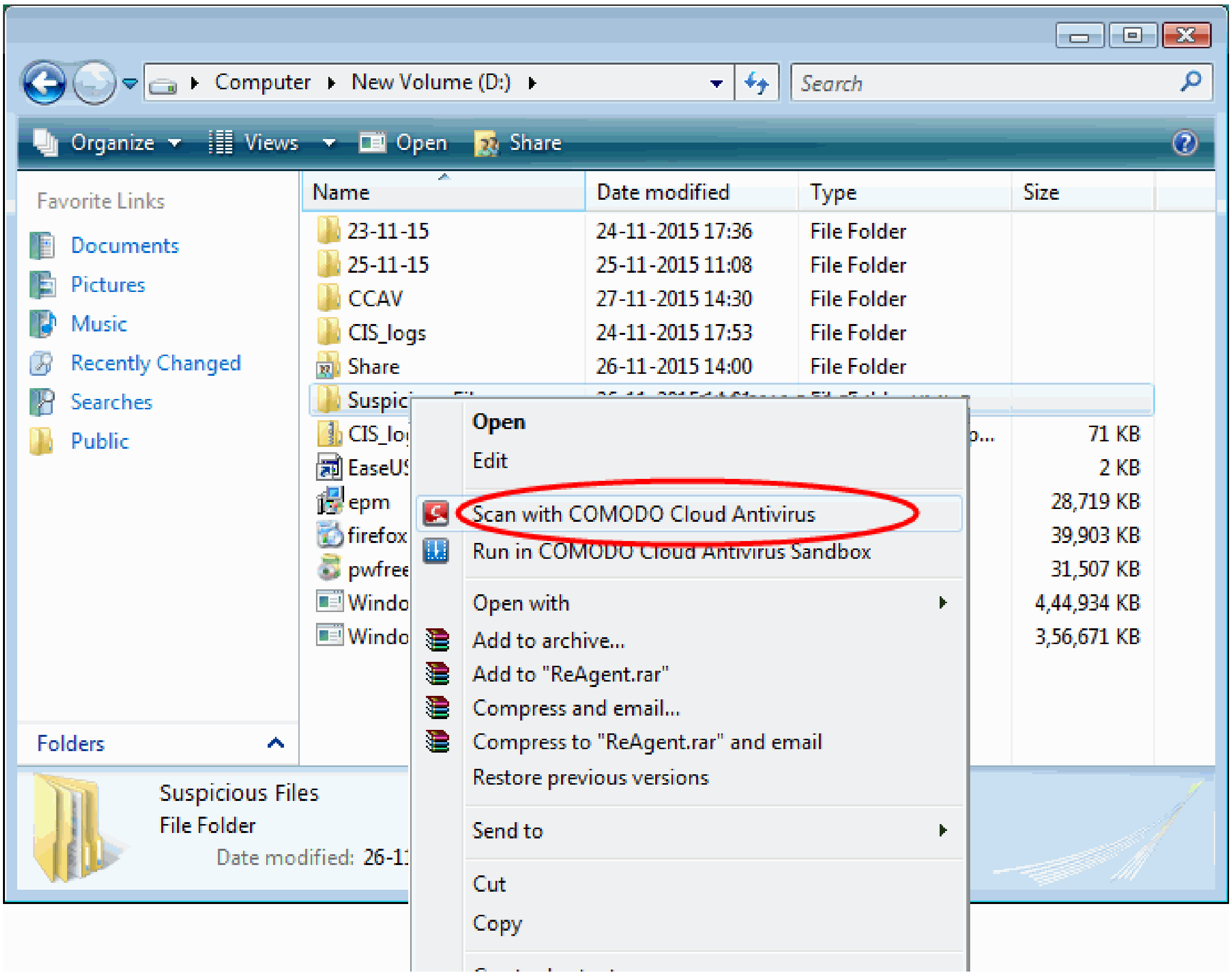
To scan a specific folder

- Click 'Scan' from the 'Tasks Bar' and click 'Folder Scan' from the 'Scan' interface.
- Navigate to the folder to be scanned in the 'Browse for Folder' window and click 'OK'.

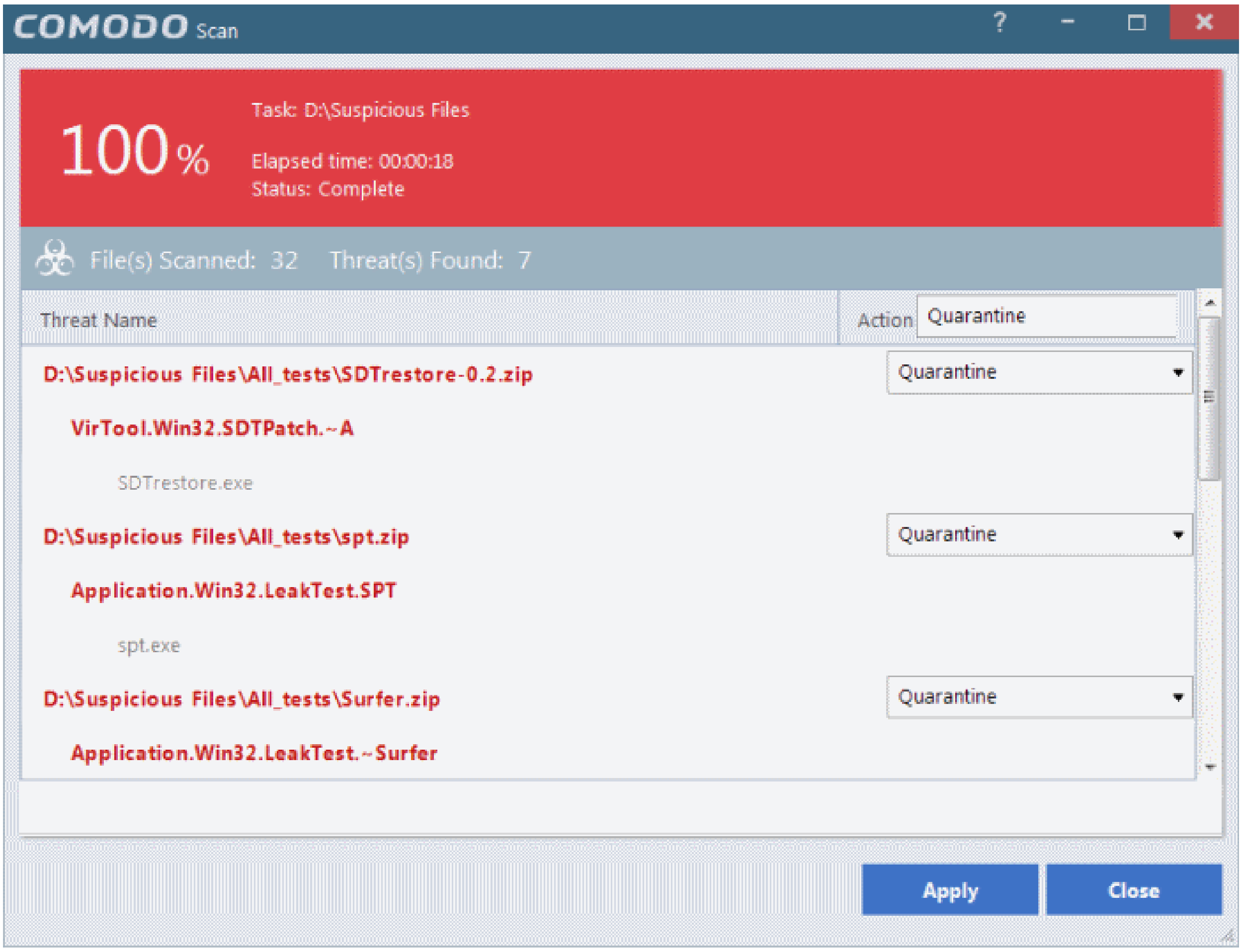


Folder: Suspicious Files

Alternatively, right-click on the folder and select 'Scan with Comodo Cloud Antivirus' from the context-sensitive menu.



The folder will be scanned instantly and the results will be displayed with a list of any identified infections.



Task: D:\Suspicious Files

Elapsed time: 00:00:18

Status: Complete

File(s) Scanned: 32   Threat(s) Found: 7

Threat Name	Action: Quarantine
D:\Suspicious Files\All_tests\SDTrestore-0.2.zip	Quarantine
VirTool.Win32.SDTPatch.~A	
SDTrestore.exe	
D:\Suspicious Files\All_tests\spt.zip	Quarantine
Application.Win32.LeakTest.SPT	
spt.exe	
D:\Suspicious Files\All_tests\Surfer.zip	Quarantine
Application.Win32.LeakTest.~Surfer	

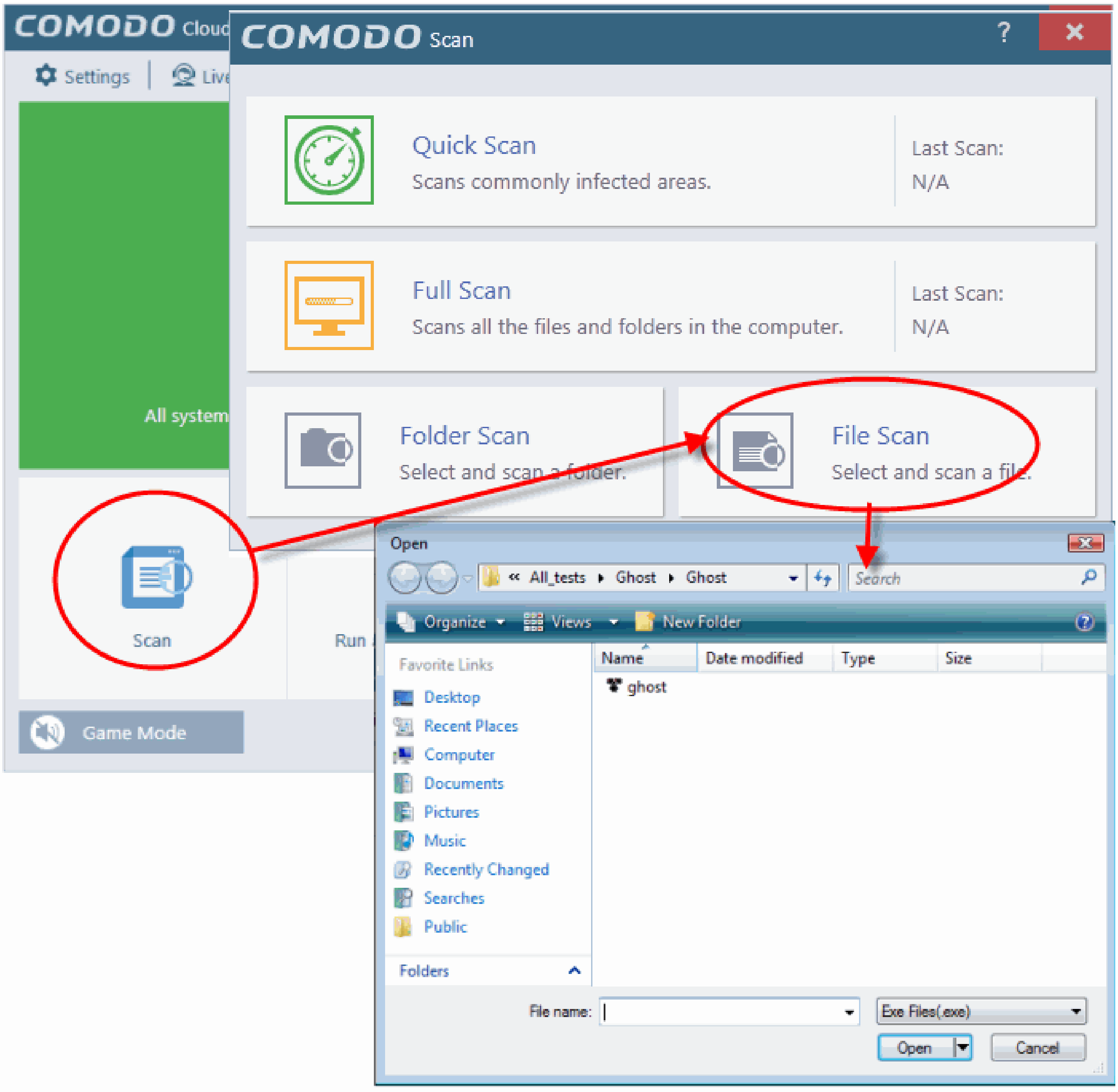
The scan results window displays the number of objects scanned and the number of threats detected (viruses, rootkits, malware and so on). You can choose to move the files to quarantine or ignore the threat based in your assessment. Refer to **Processing the infected files** for more details.

2.3.2. Scan a File

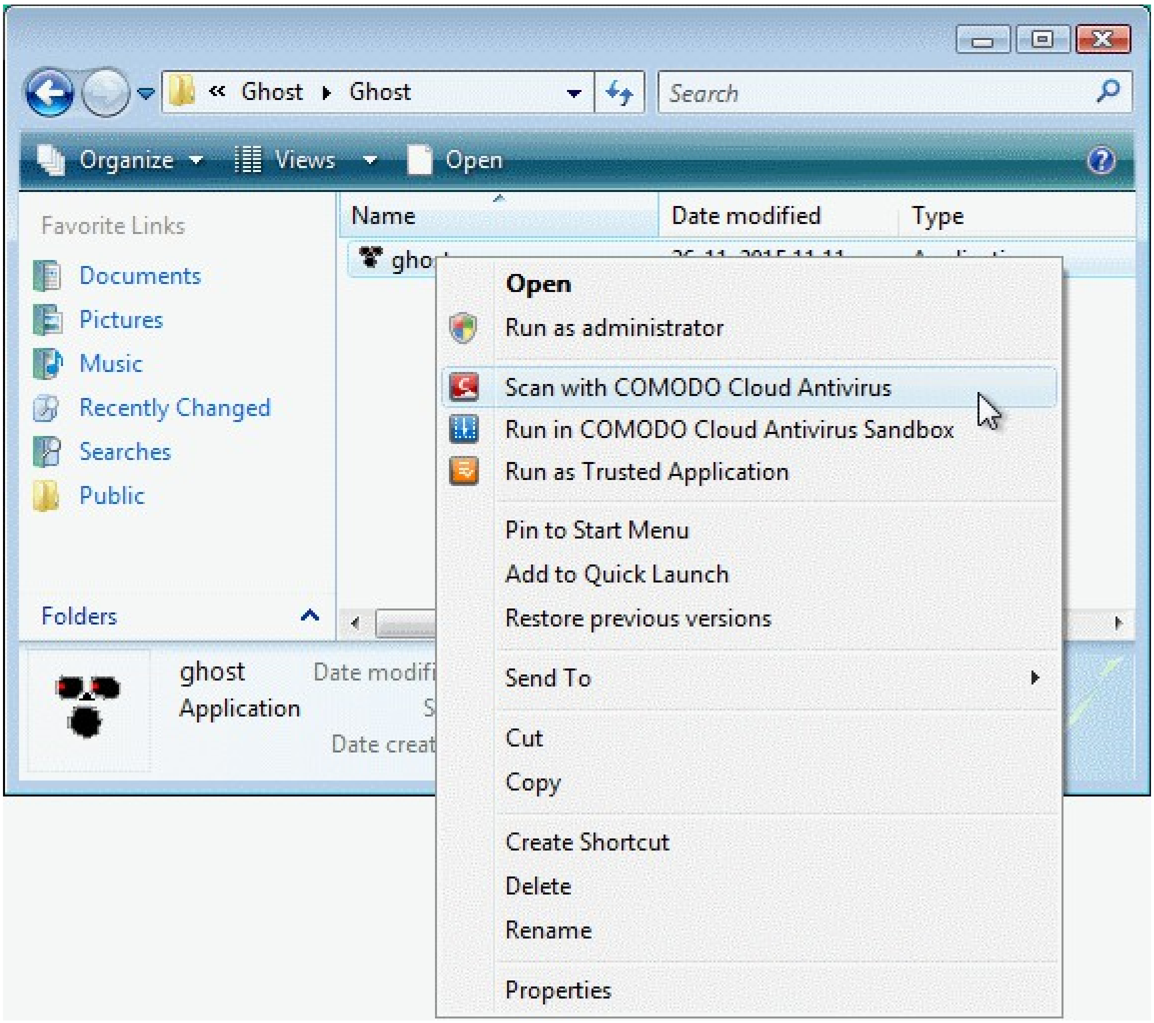
The 'File Scan' option allows you to scan a specific file on your hard drive, CD/DVD or external device. For example, you might have downloaded a file from the internet or dragged an email attachment onto your desktop and want to scan it for threats before you open it.

To scan a specific file

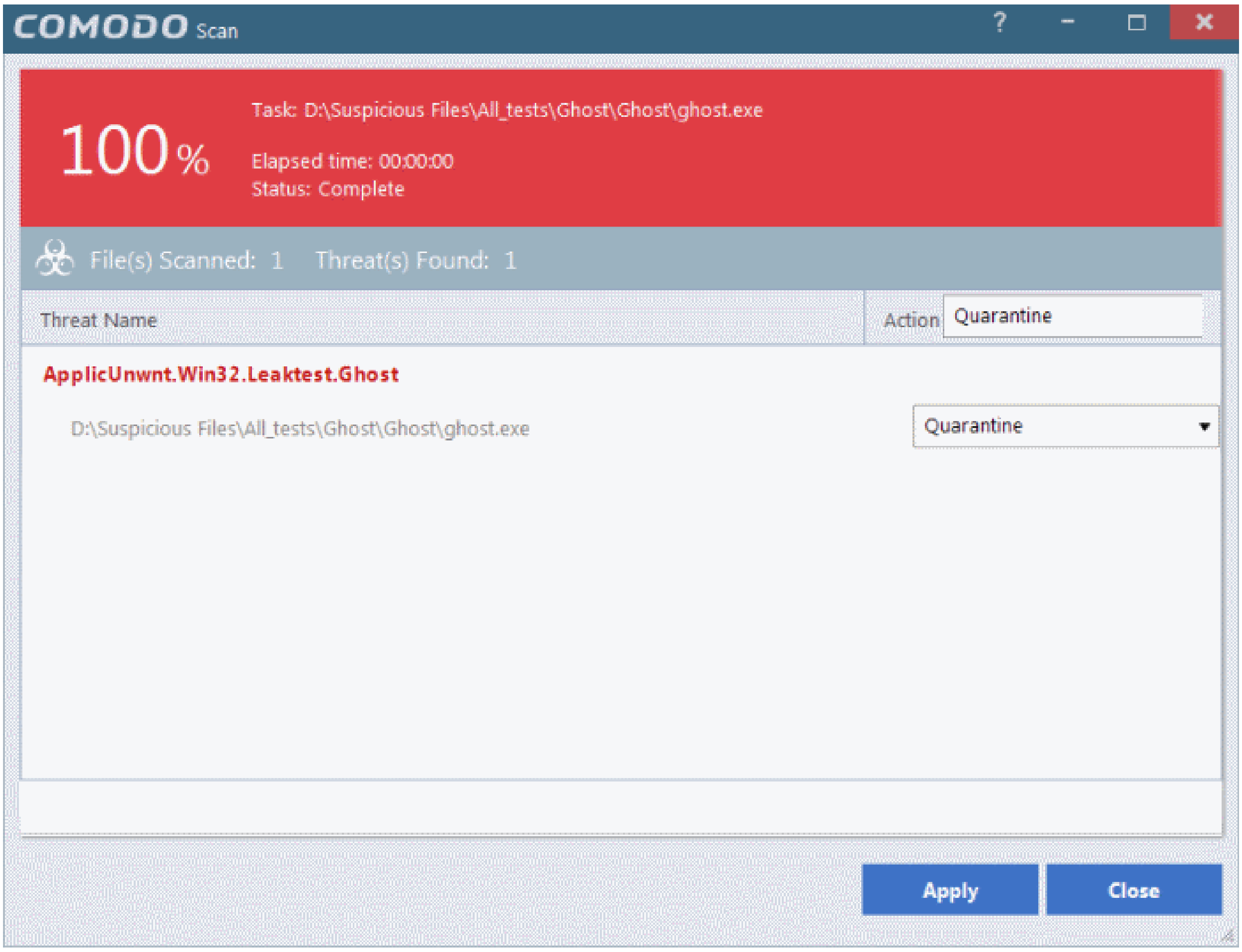
- Click 'Scan' from the 'Tasks Bar' and click 'Folder Scan' from the 'Scan' interface.
- Navigate to the location and select the file to be scanned and click 'OK'.



Alternatively, right-click on the file and select 'Scan with Comodo Cloud Antivirus' from the context-sensitive menu.



The file will be scanned instantly and the result will be displayed.



Task: D:\Suspicious Files\All_tests\Ghost\Ghost\ghost.exe

Elapsed time: 00:00:00

Status: Complete

File(s) Scanned: 1 Threat(s) Found: 1

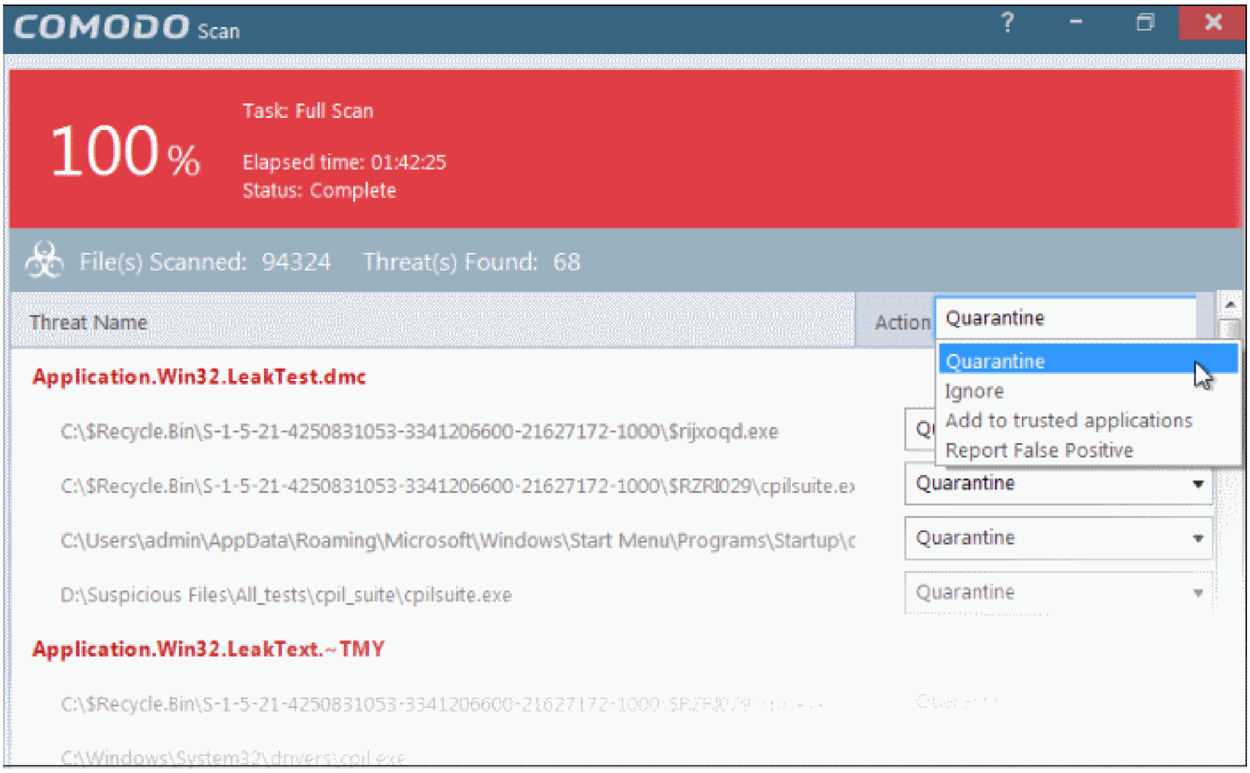
Threat Name	Action: Quarantine
ApplicUnwnt.Win32.Leaktest.Ghost	
D:\Suspicious Files\All_tests\Ghost\Ghost\ghost.exe	Quarantine

The scan results window displays the number of objects scanned and the number of threats (Viruses, Rootkits, Malware and so on). You can choose to move the file to quarantine or ignore the threat based in your assessment. Refer to **Processing the infected files** for more details.

2.4. Processing Infected Files

The scan results screen lists all detected threats and allows you to take appropriate actions. You can quarantine the file, ignore the alert, trust the file or report it as a false positive.

- You can choose an action to be taken on all threats from the 'Action' drop-down at top right:



100 %

Task: Full Scan

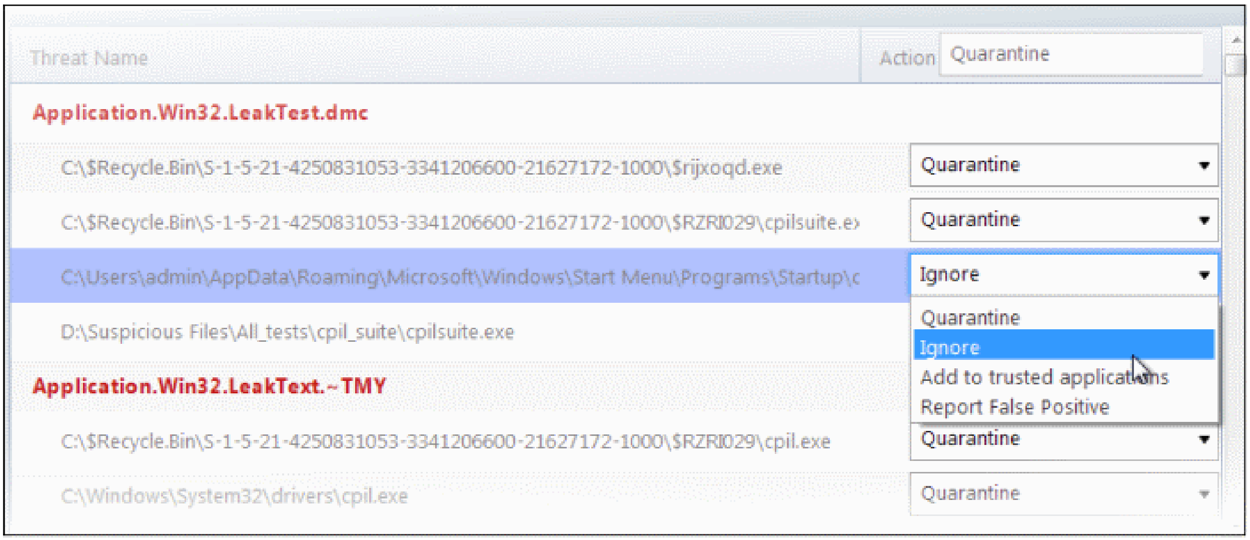
Elapsed time: 01:42:25

Status: Complete

File(s) Scanned: 94324 Threat(s) Found: 68

Threat Name	Action Quarantine
Application.Win32.LeakTest.dmc	
C:\$Recycle.Bin\S-1-5-21-4250831053-3341206600-21627172-1000\$rijxoqd.exe	Q
C:\$Recycle.Bin\S-1-5-21-4250831053-3341206600-21627172-1000\$RZRI029\cpilsuite.e›	Quarantine
C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\c	Quarantine
D:\Suspicious Files\All_tests\cpil_suite\cpilsuite.exe	Quarantine
Application.Win32.LeakText.~TMY	
C:\$Recycle.Bin\S-1-5-21-4250831053-3341206600-21627172-1000\$RZRI029\c...	Quar...
C:\Windows\System32\drivers\cpil.exe	

… or choose an action to be applied to individual items from the drop-down beside each item:



Threat Name	Action Quarantine
Application.Win32.LeakTest.dmc	
C:\$Recycle.Bin\S-1-5-21-4250831053-3341206600-21627172-1000\$rijxoqd.exe	Quarantine
C:\$Recycle.Bin\S-1-5-21-4250831053-3341206600-21627172-1000\$RZRI029\cpilsuite.e›	Quarantine
C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\c	Ignore
D:\Suspicious Files\All_tests\cpil_suite\cpilsuite.exe	
Application.Win32.LeakText.~TMY	
C:\$Recycle.Bin\S-1-5-21-4250831053-3341206600-21627172-1000\$RZRI029\cpil.exe	Quarantine
C:\Windows\System32\drivers\cpil.exe	Quarantine

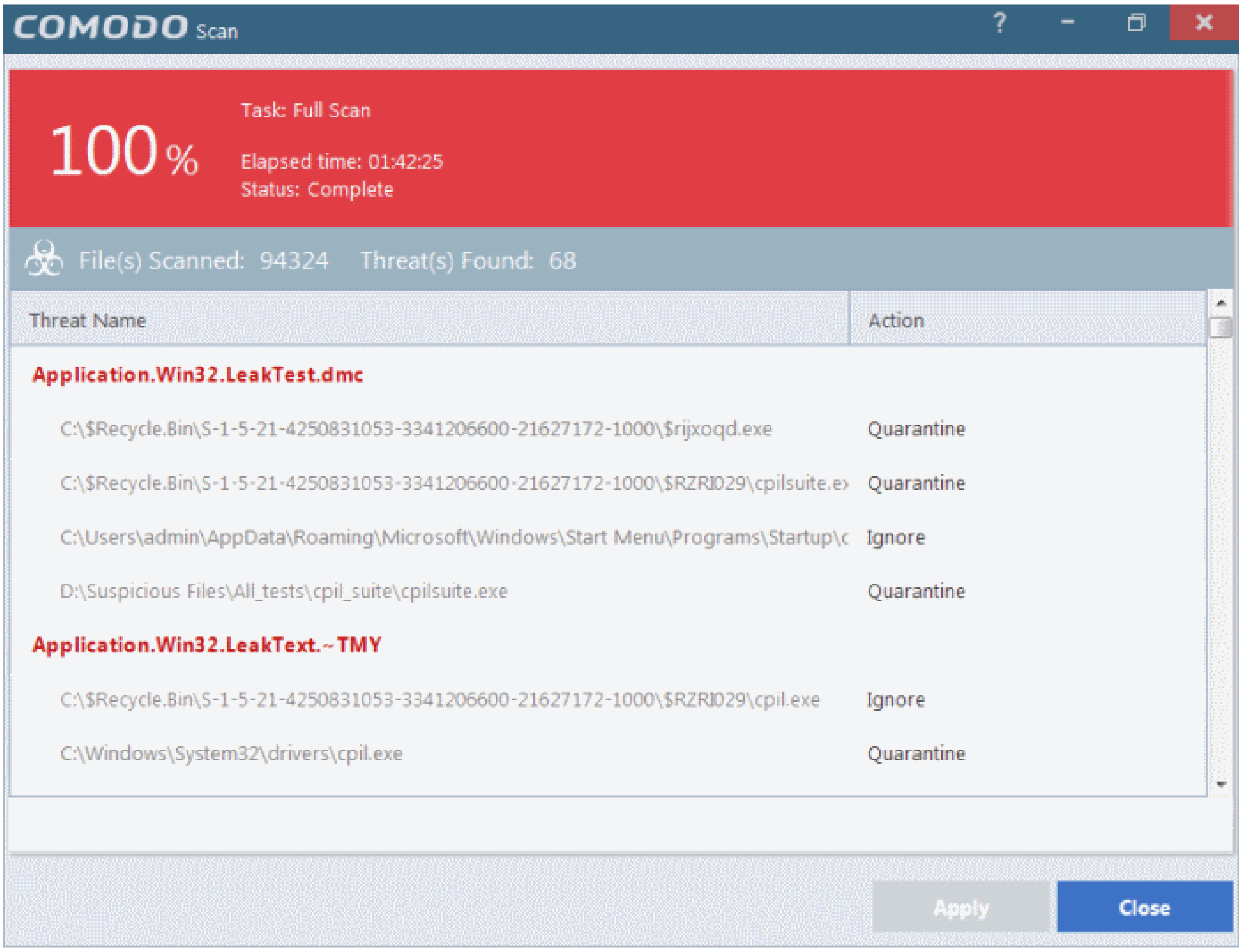
The available actions are:

- **Quarantine** – The files will be moved to quarantine. For more details on quarantine feature, refer to the section 'View and Manage Quarantined Items'.
- **Ignore** – If you want to ignore the threat the threat this time only, select 'Ignore'. The file will be ignored only at that time and if the same application invokes again, the AV scanner will report it as a threat.

- **Add to trusted applications** - If you trust the file, select 'Add to trusted applications'. The file will be assigned 'Trusted' status in the '**Trusted Applications**'. The alert will not generated if the same application invokes again.
- **Report as false positive** - If you are sure that the file is safe, select 'Report False Positive'. The Antivirus will send the file to Comodo for analysis. If the file is trustworthy, it is added to the Comodo safe list.

- After selecting the action(s) to be applied, click 'Apply'. The files will be treated as per the action selected and the progress will be displayed.

On completion the action taken against each threat will be displayed.



100 %

Task: Full Scan

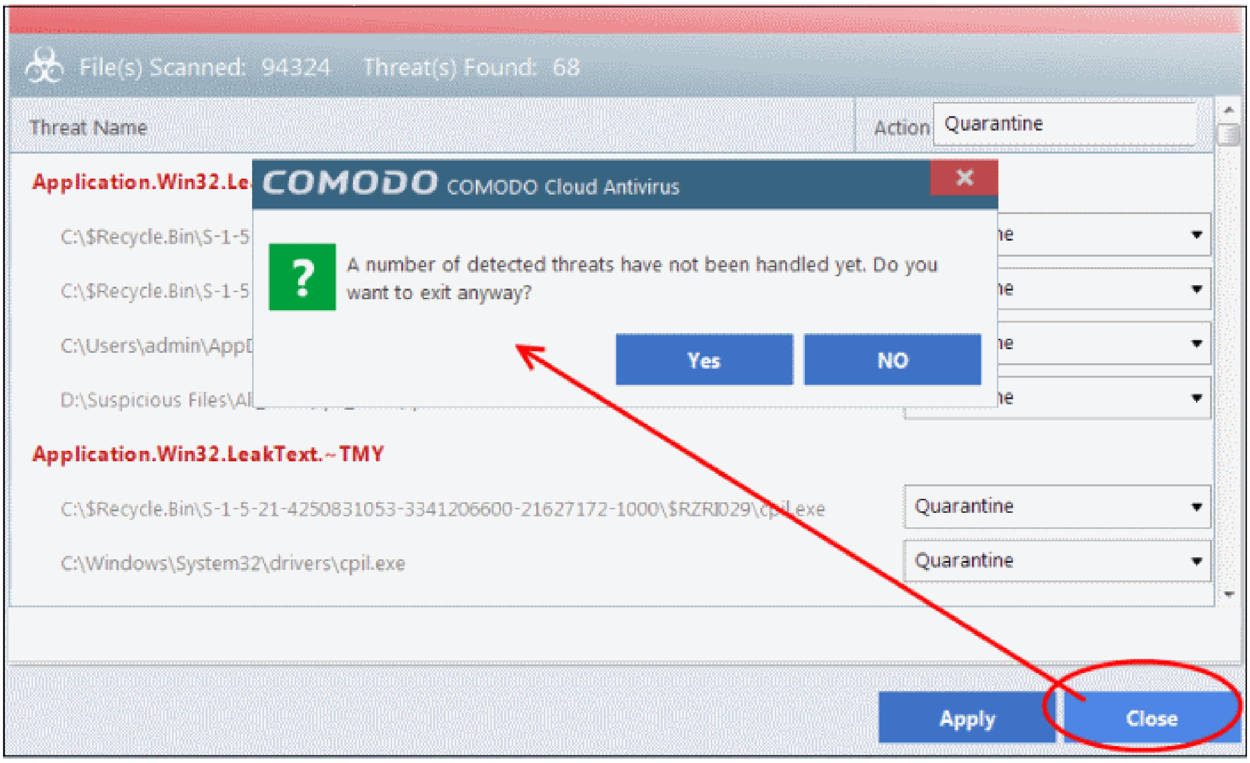
Elapsed time: 01:42:25

Status: Complete

File(s) Scanned: 94324 Threat(s) Found: 68

Threat Name	Action
Application.Win32.LeakTest.dmc	
C:\$Recycle.Bin\S-1-5-21-4250831053-3341206600-2627172-1000\$rijxoqd.exe	Quarantine
C:\$Recycle.Bin\S-1-5-21-4250831053-3341206600-2627172-1000\$RZRI029\cpilsuite.e›	Quarantine
C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\c	Ignore
D:\Suspicious Files\All_tests\cpil_suite\cpilsuite.exe	Quarantine
Application.Win32.LeakText.~TMY	
C:\$Recycle.Bin\S-1-5-21-4250831053-3341206600-2627172-1000\$RZRI029\cpil.exe	Ignore
C:\Windows\System32\drivers\cpil.exe	Quarantine

If you choose to close the results window without taking any action, the threats will be added to the 'Detected Threats' list.

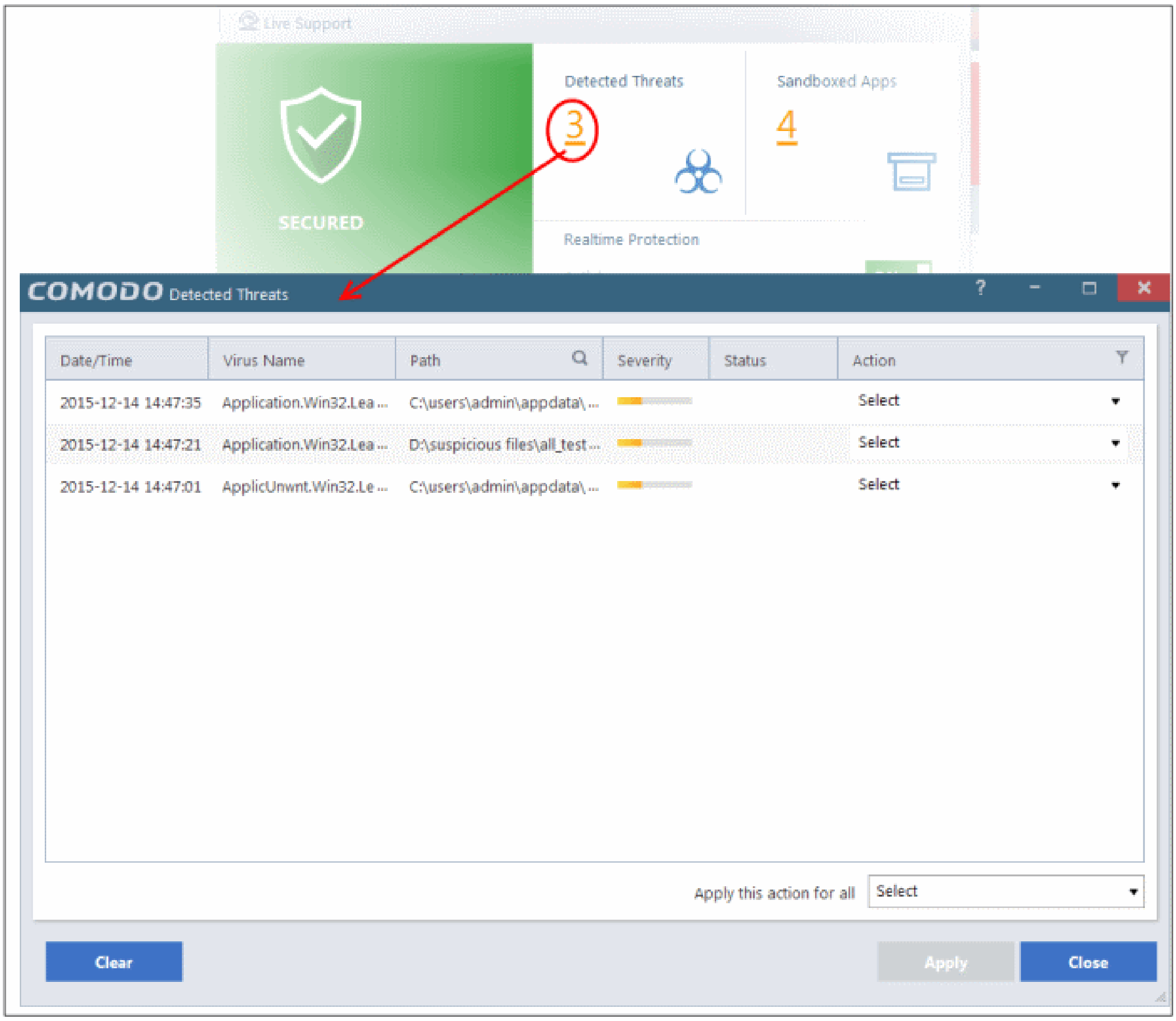

File(s) Scanned: 94324 Threat(s) Found: 68
Threat Name
Action
Quarantine
Application.Win32.Le
C:\$Recycle.Bin\S-1-5
C:\$Recycle.Bin\S-1-5
C:\Users\admin\AppD
D:\Suspicious Files\Al
Application.Win32.LeakText.~TMY
C:\$Recycle.Bin\S-1-5-21-4250831053-3341206600-21627172-1000\$RZRI029\cpil.exe
C:\Windows\System32\drivers\cpil.exe
Quarantine
Quarantine
COMODO COMODO Cloud Antivirus
Yes
NO
Apply
Close

A number of detected threats have not been handled yet. Do you want to exit anyway?

The 'Detected Threats' interface allows you to take action such as 'Quarantine', 'Trust' or 'Trust and Report False Positive' later on. Refer to the section '**Managing Detected Threats**' for more details.

2.5. Managing Detected Threats

You can view the list of items identified as malware by real-time scans by clicking the number under 'Detected Threats' in the home screen of CCAV.



Date/Time	Virus Name	Path	Severity	Status	Action
2015-12-14 14:47:35	Application.Win32.Lea ...	C:\users\admin\appdata\ ...			Select
2015-12-14 14:47:21	Application.Win32.Lea ...	D:\suspicious files\all_test ...			Select
2015-12-14 14:47:01	ApplicUnwnt.Win32.Le ...	C:\users\admin\appdata\ ...			Select

Column Descriptions:

- **Date/Time** – The date and time at which the threat was detected
- **Virus Name** – The name of the malware contained in the application detected as threat
- **Path** – The location of the application in the system
- **Severity** – Indicates the risk level presented by the activity or request of the detected threat
- **Status** – Indicates the status of the action taken. It can be either 'Quarantine', 'Trust' and 'Trust and Report False Positive'.
- **Action** - Displays a drop-down with options for handing the item:

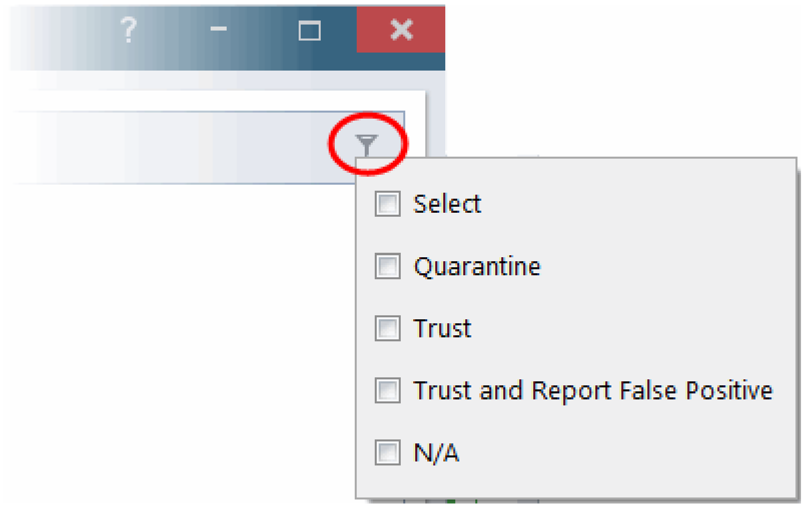
  The available actions are:

  - **Quarantine** – Item will be moved to Quarantine and saved in an encrypted manner. You can analyze the item at a later time and:
    - Restore it to the original location if it is trustworthy or
    - Delete the item from your computer if it is a malware

    from the Quarantine interface. Refer to the section **View and Manage Quarantined Items** for more details.
  - **Trust –** The item will be added to the Trusted Applications and will be excluded from the future scans. Choose this option only if the item is trustworthy.
  - **Trust and Report False Positive** - The item will be added to the Trusted Applications and will be excluded from the future scans. Also it will be submitted to Comodo for analysis. If the file is found harmless by our experts, it will be added to global safelist.

  - **N/A** – No action will be taken on the item.

- To search for specific application, click the search icon beside the 'Path' column header and enter the name of the application in part of full.
- To filter the entries based on the action chosen to be executed on them, click the funnel icon beside the 'Action' table header and choose the action.



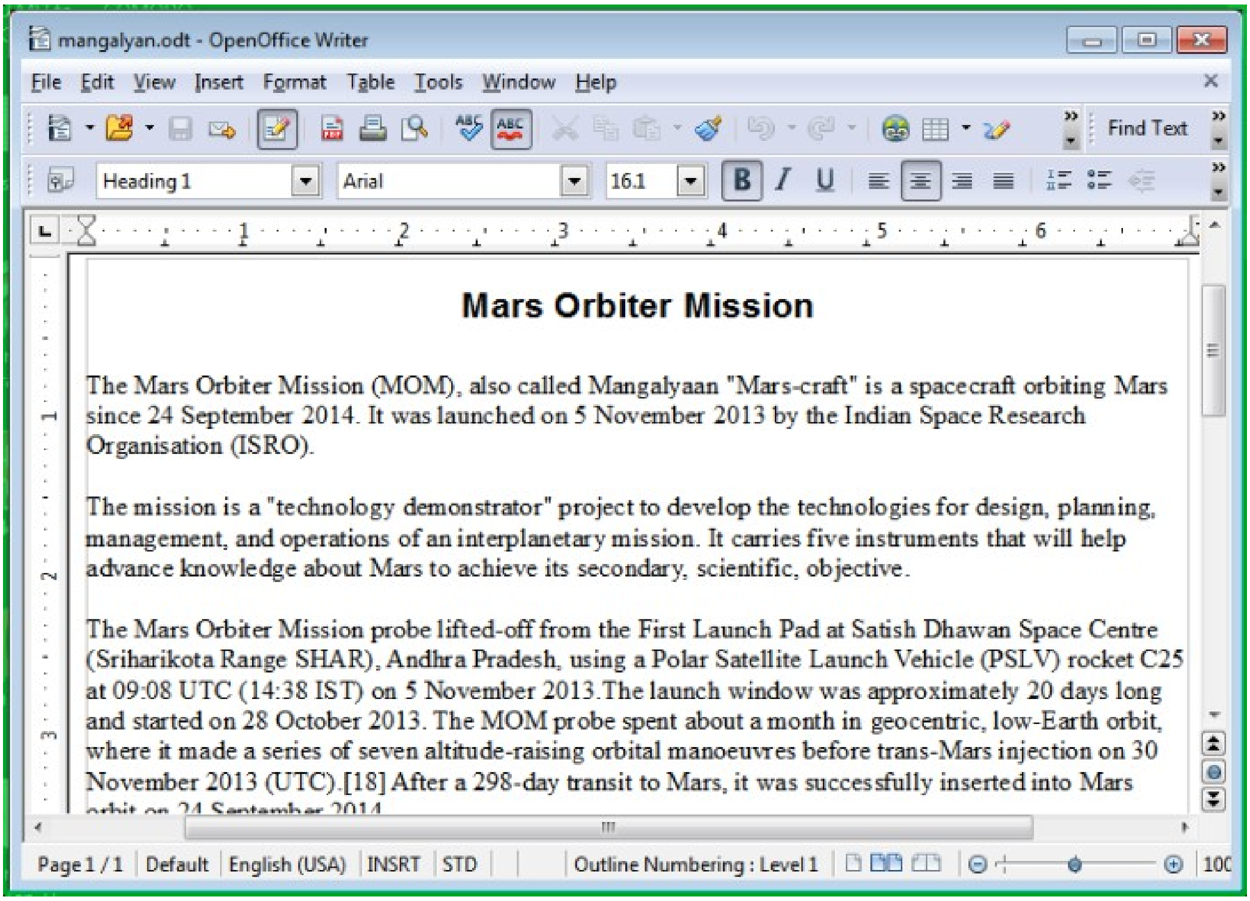
  - To move a malicious item to quarantine choose 'Quarantine' from the 'Action' drop-down in the item row.
  - To exclude an item from future scans, choose 'Trust' from the 'Action' drop-down in the item row
  - To submit an harmless item identified as malware by CCAV by mistake for analysis by Comodo, choose 'Trust and Report False Positive' from the 'Action' drop-down in the item row

- Click 'Apply' for your actions to take effect.

3. The Sandbox

The sandbox is a security hardened operating environment for unknown applications (those that are neither trusted/safe nor definitely malware). A sandboxed application has no opportunity to damage your computer because it is run isolated from your operating system and your files. Sandboxed items have greatly restricted access privileges and write to a virtual file system and registry. This delivers a smooth user experience by allowing unknown applications to run and operate as they normally would while denying them the potential to cause damage.

By default, all 'unknown' applications detected by CCAV will be automatically run in the sandbox environment. Applications in the sandbox have a green border around them. For example, this is how Open Office Writer looks in the sandbox:


mangalyan.odt - OpenOffice Writer
File Edit View Insert Format Table Tools Window Help
Find Text
Heading 1
Arial
16.1
Page 1 / 1
Default
English (USA)
INSRT
STD
Outline Numbering : Level 1
100

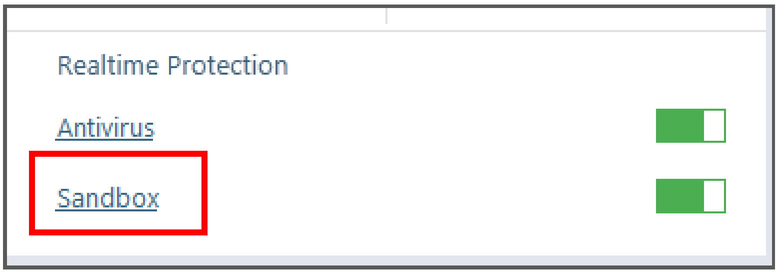
Mars Orbiter Mission

The Mars Orbiter Mission (MOM), also called Mangalyaan "Mars-craft" is a spacecraft orbiting Mars since 24 September 2014. It was launched on 5 November 2013 by the Indian Space Research Organisation (ISRO).

The mission is a "technology demonstrator" project to develop the technologies for design, planning, management, and operations of an interplanetary mission. It carries five instruments that will help advance knowledge about Mars to achieve its secondary, scientific, objective.

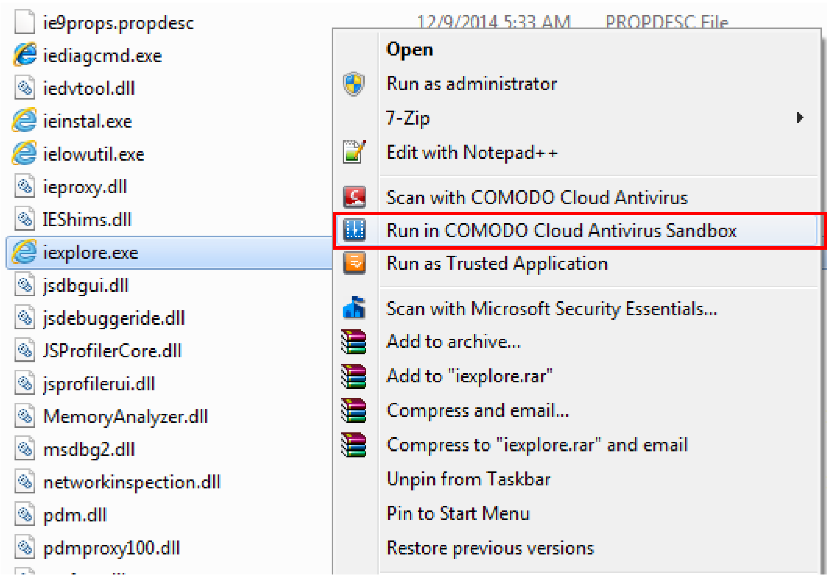
The Mars Orbiter Mission probe lifted-off from the First Launch Pad at Satish Dhawan Space Centre (Sriharikota Range SHAR), Andhra Pradesh, using a Polar Satellite Launch Vehicle (PSLV) rocket C25 at 09:08 UTC (14:38 IST) on 5 November 2013.The launch window was approximately 20 days long and started on 28 October 2013. The MOM probe spent about a month in geocentric, low-Earth orbit, where it made a series of seven altitude-raising orbital manoeuvres before trans-Mars injection on 30 November 2013 (UTC).[18] After a 298-day transit to Mars, it was successfully inserted into Mars orbit on 24 September 2014

- You can configure **sandbox settings** by clicking the 'Sandbox' link on the home screen:

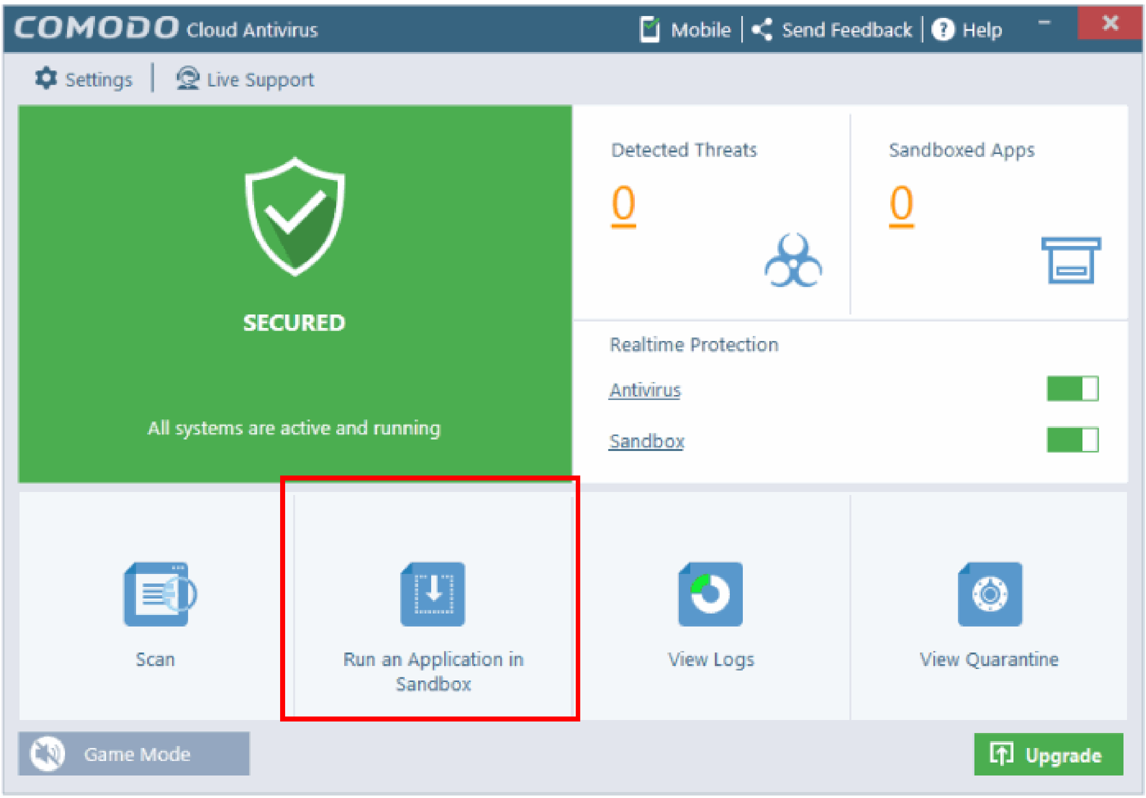


- You can create specific sandbox rules for any application or file. See '**Sandbox Rules** for more details.
- You can also apply rules for categories of software in the 'Application Categories' area. See '**Sandbox Categories**' for more details.
- You can quickly run an application or file in the sandbox using one of the following methods:

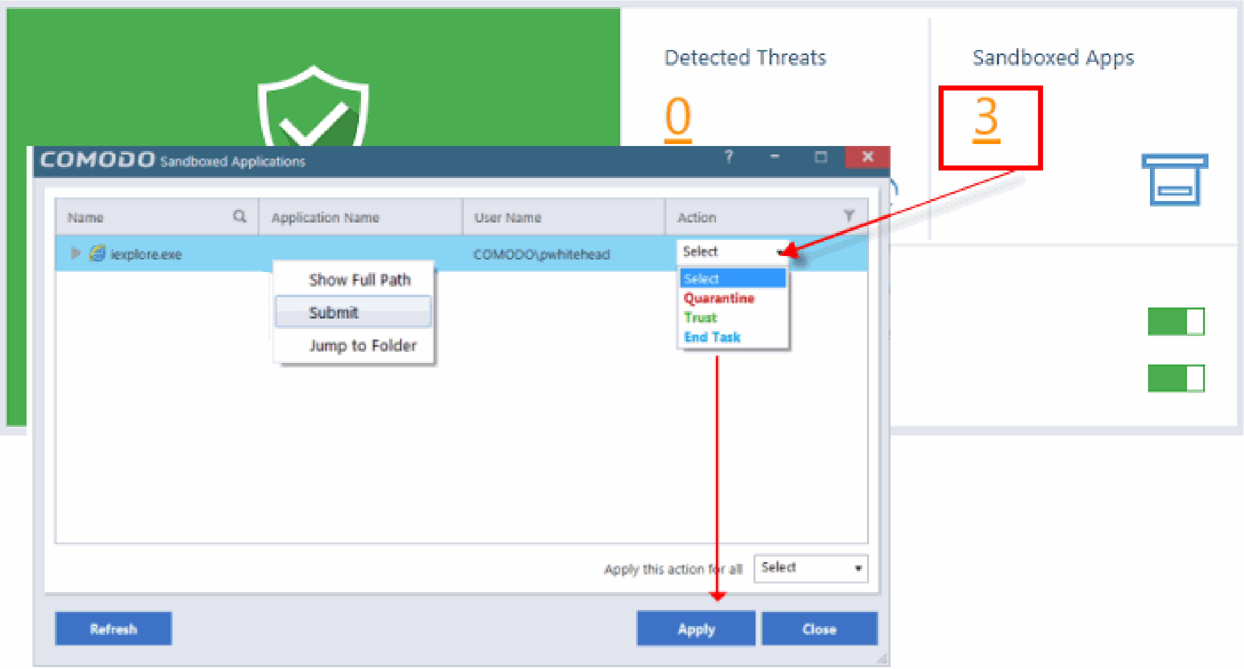
- Right-click on a file then choose 'Run in Comodo Cloud Antivirus Sandbox' from the context sensitive menu:



- Click 'Run an Application in the Sandbox' on the home screen then browse to the file:



- You can view and apply actions to programs which are running in the sandbox by clicking the number in the 'Sandboxed Apps' area.



The drop-down list allows you to apply the following actions to sandboxed applications:

- **Quarantine** – Will block the file and place it in **quarantine**
- **Trust** – Will add the application to the trusted applications list and allow it to run outside the sandbox next time.
- **End Task** – Will close the selected application

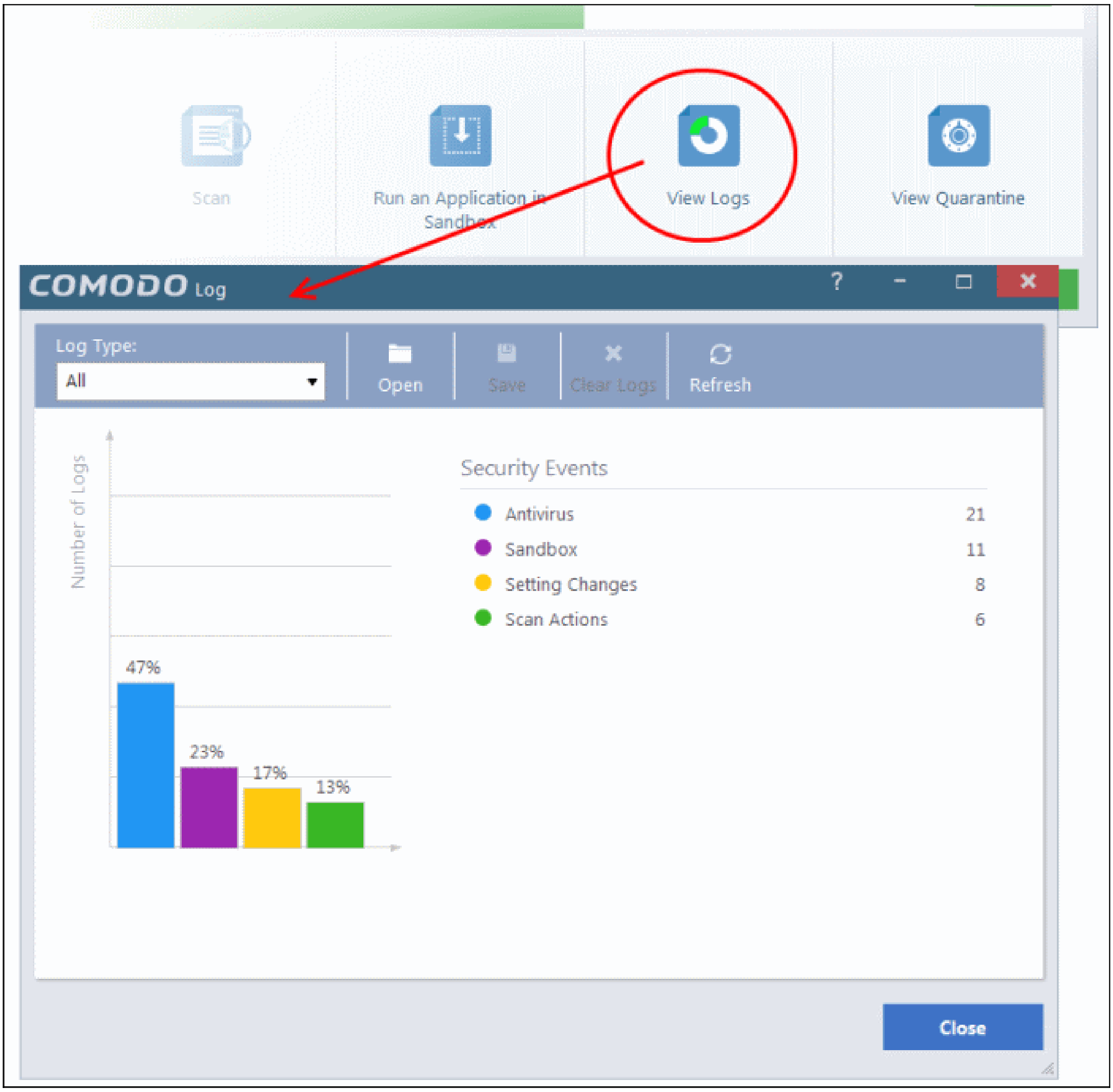
If you select an item and right-click you can perform the following actions:

- **Show full Path** – Will display the exact location of the folder in which the executable resides
- **Submit** – Will submit the file to Comodo for analysis. Comodo Labs will run behavior analysis on the file to determine whether it is trustworthy or malicious.
- **Jump to Folder** – Will open the file location in Windows Explorer.

- Also see **Sandbox Configuration** and **Sandbox Logs**.

4. View CCAV Logs

CCAV logs are records of all antivirus events, sandbox events, configuration changes and user initiated actions. You can open the log viewer interface by clicking the 'View Logs' icon on the home screen:



Security Events

●	Antivirus	21
●	Sandbox	11
●	Setting Changes	8
●	Scan Actions	6

By default, a summary of logs from all events is displayed. The drop-down at the top allows you to choose specific log types.

The interface allows you to save logs from individual modules, open saved log files and clear log files. This is helpful if you want to backup/archive your log files or clear the log module periodically to save disk space.

- To save/archive a log, choose the log type from the drop-down menu and click the 'Save' icon.
- To open a stored log file, click the 'Open log file' button and browse to the location where the log file is saved.
- To clear a log, choose the log type from drop-down and click 'Clear Logs'.
- To refresh the logs, click the 'Refresh' button

The following sections contain more information about:

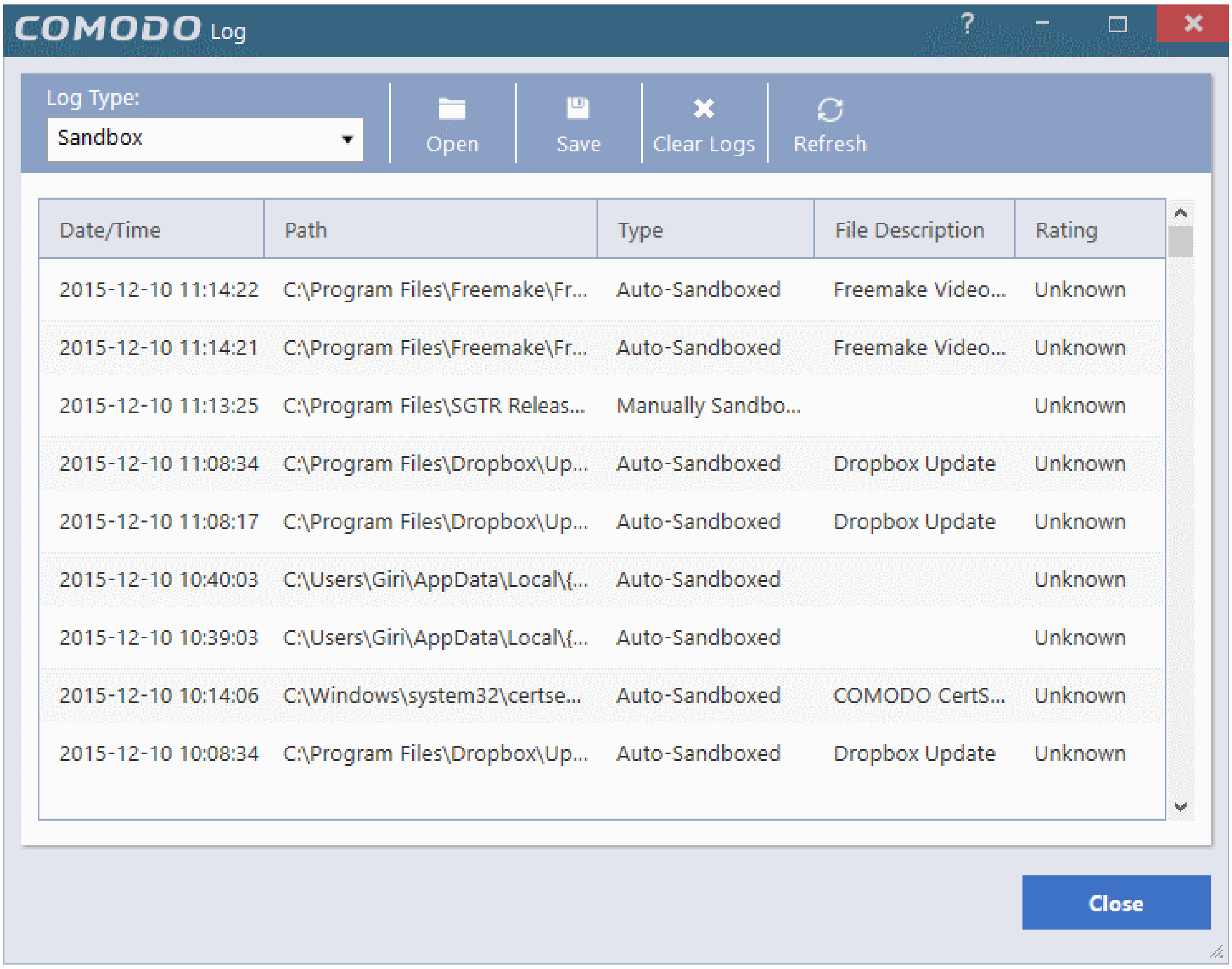
- **Sandbox Logs**
- **Antivirus Logs**
- **Setting Changes Logs**

- Scan Actions Logs

4.1. Sandbox Logs

Comodo Cloud Antivirus records a history of all actions taken by the 'Sandbox' module. For example, logs are created whenever CCAV auto-sandboxes a file and when a file is manually sandboxed by the user.

'Sandbox' logs can be viewed by choosing 'Sandbox' from the 'Log Type' drop-down:



Log Type: Sandbox

Date/Time	Path	Type	File Description	Rating
2015-12-10 11:14:22	C:\Program Files\Freemake\Fr...	Auto-Sandboxed	Freemake Video...	Unknown
2015-12-10 11:14:21	C:\Program Files\Freemake\Fr...	Auto-Sandboxed	Freemake Video...	Unknown
2015-12-10 11:13:25	C:\Program Files\SGTR Releas...	Manually Sandbo...		Unknown
2015-12-10 11:08:34	C:\Program Files\Dropbox\Up...	Auto-Sandboxed	Dropbox Update	Unknown
2015-12-10 11:08:17	C:\Program Files\Dropbox\Up...	Auto-Sandboxed	Dropbox Update	Unknown
2015-12-10 10:40:03	C:\Users\Giri\AppData\Local\{...	Auto-Sandboxed		Unknown
2015-12-10 10:39:03	C:\Users\Giri\AppData\Local\{...	Auto-Sandboxed		Unknown
2015-12-10 10:14:06	C:\Windows\system32\certse...	Auto-Sandboxed	COMODO CertS...	Unknown
2015-12-10 10:08:34	C:\Program Files\Dropbox\Up...	Auto-Sandboxed	Dropbox Update	Unknown

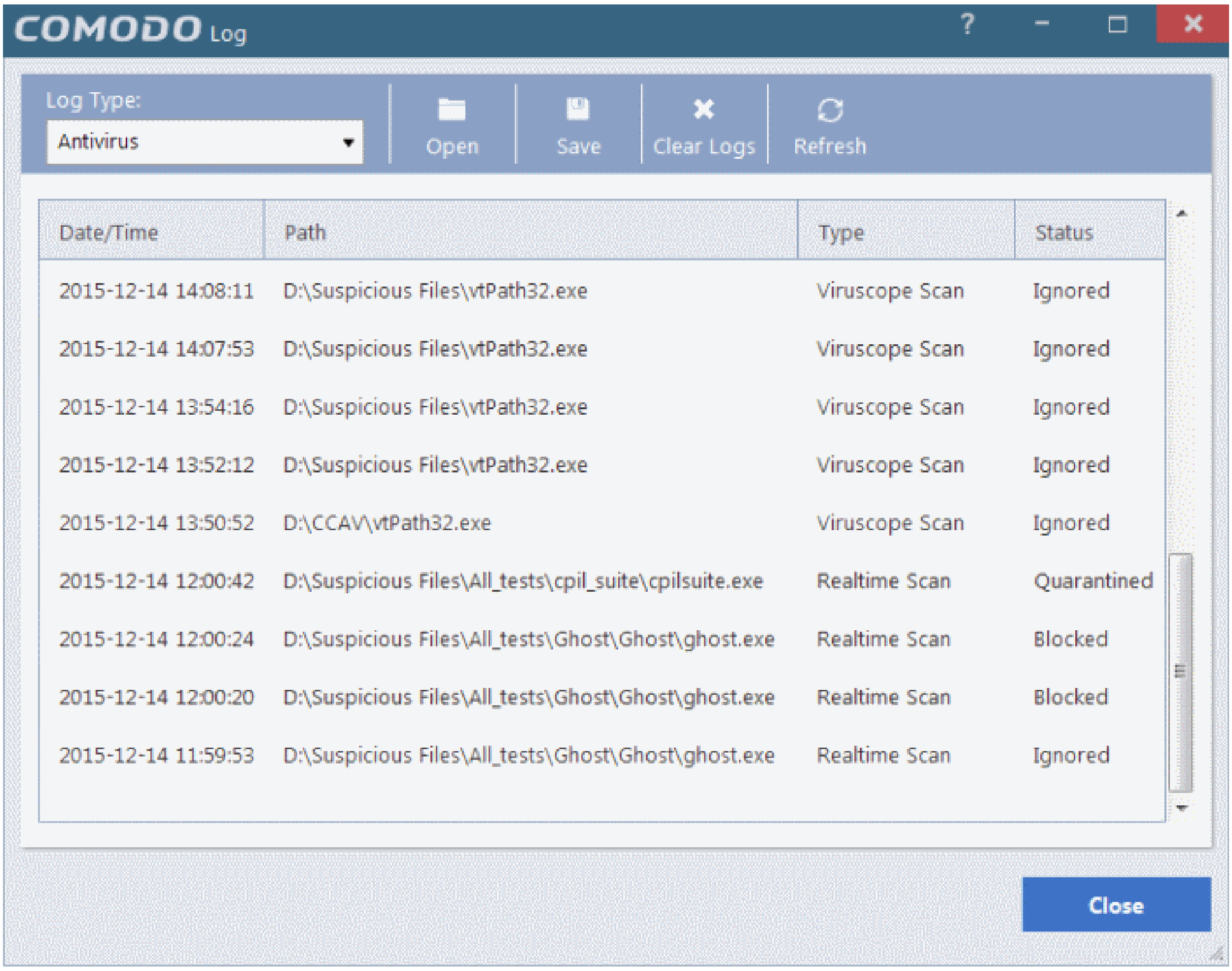
Column Descriptions

1. **Date/Time** – The date and time of the event
2. **Path –** The location the file or application that was run in the sandbox
3. **Type** – Indicates how the application was sandboxed - whether it was sandboxed automatically due to its trust rating or manually sandboxed by the user
4. **File Description** – The name of the file that generated the event
5. **Rating** - Indicates the rating of the file, whether malicious or unknown

- To export the logs as a '.log' file, click the 'Save' button
- To open a stored log file, click the 'Open log file' button
- To update the list with the latest events, click the 'Refresh' button
- To clear the 'Sandbox' logs, click the 'Clear logs' button.

4.2. Antivirus Logs

CCAV keeps a history of all items identified as malware by the virus scanner. Antivirus logs can be viewed by selecting 'Antivirus' from the 'Log Type' drop-down of the log viewer interface:



Date/Time	Path	Type	Status
2015-12-14 14:08:11	D:\Suspicious Files\vtPath32.exe	Viruscope Scan	Ignored
2015-12-14 14:07:53	D:\Suspicious Files\vtPath32.exe	Viruscope Scan	Ignored
2015-12-14 13:54:16	D:\Suspicious Files\vtPath32.exe	Viruscope Scan	Ignored
2015-12-14 13:52:12	D:\Suspicious Files\vtPath32.exe	Viruscope Scan	Ignored
2015-12-14 13:50:52	D:\CCAV\vtPath32.exe	Viruscope Scan	Ignored
2015-12-14 12:00:42	D:\Suspicious Files\All_tests\cpil_suite\cpilsuite.exe	Realtime Scan	Quarantined
2015-12-14 12:00:24	D:\Suspicious Files\All_tests\Ghost\Ghost\ghost.exe	Realtime Scan	Blocked
2015-12-14 12:00:20	D:\Suspicious Files\All_tests\Ghost\Ghost\ghost.exe	Realtime Scan	Blocked
2015-12-14 11:59:53	D:\Suspicious Files\All_tests\Ghost\Ghost\ghost.exe	Realtime Scan	Ignored

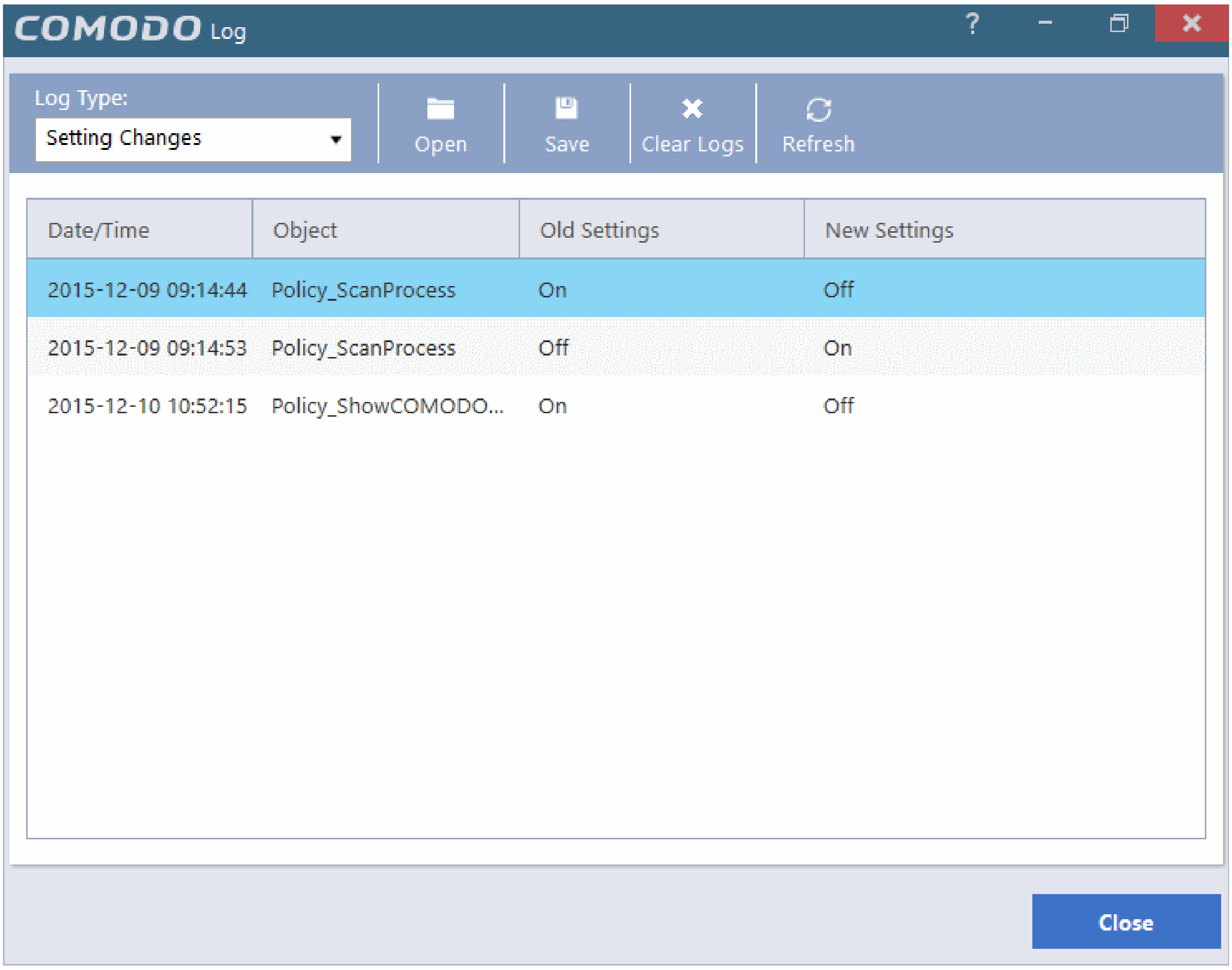
Column Descriptions

1. **Date/Time** – The date and time of the event
2. **Path –** The installation/storage path of the file identified as malware
3. **Type** – Indicates the type of scan from which the item was identified
4. **Status** - Gives the status of the action taken. It can be either 'Ignored', 'Blocked' or 'Quarantined'

- To export the logs as a '.log' file, click the 'Save' button
- To open a stored log file, click the 'Open log file' button
- To update the list with the latest antivirus events, click the 'Refresh' button
- To clear the antivirus logs, click the 'Clear logs' button.

4.3. Setting Changes Logs

CCAV records all software configuration changes that you make in the 'Setting Changes' log. You can view this log by choosing 'Settings Changes' from the 'Log Type' drop-down at the top of the log interface:



Date/Time	Object	Old Settings	New Settings
2015-12-09 09:14:44	Policy_ScanProcess	On	Off
2015-12-09 09:14:53	Policy_ScanProcess	Off	On
2015-12-10 10:52:15	Policy_ShowCOMODO...	On	Off

Column Descriptions

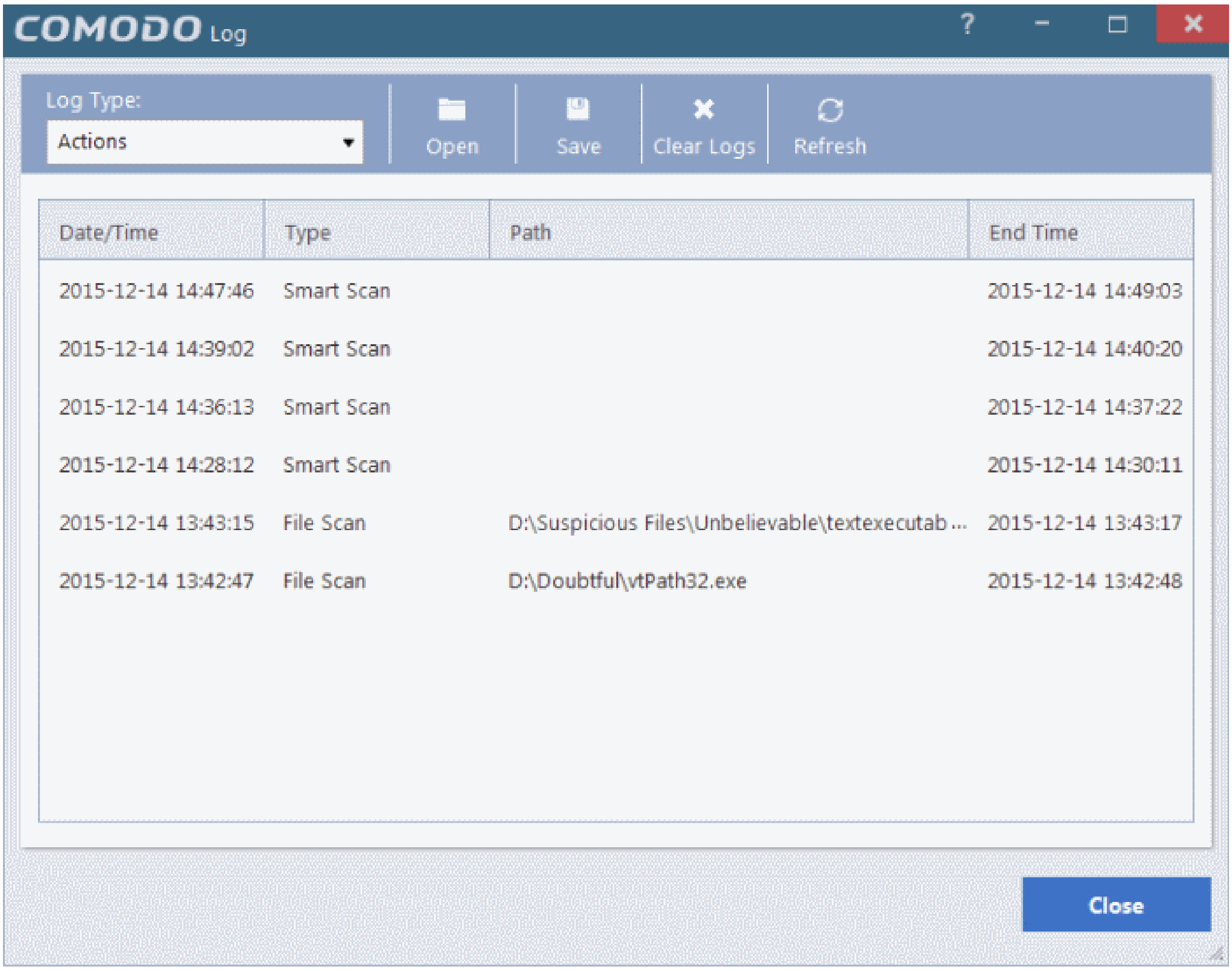
1. **Date/Time** – The date and time of the configuration change
2. **Object –** The configuration parameter or setting that was modified
3. **Old Settings** – The value of the parameter/setting before the change
4. **New Settings** – The value of the parameter/setting after the change

- To export the logs as a '.log' file, click the 'Save' button
- To open a stored log file, click the 'Open log file' button
- To update the list with the latest events, click the 'Refresh' button
- To clear the 'Setting Changes' logs, click the 'Clear logs' button.

4.4. Scan Actions Logs

CCAV keeps a record of all manually initiated virus scans. This includes scans started by clicking the 'Scan' button on the home screen, and those started by right clicking on an item and choosing 'Scan with Comodo Cloud Antivirus'.

The 'Scan Actions' logs can be viewed by choosing 'Actions' from the 'Log Type' drop-down of the log viewer interface.



Date/Time	Type	Path	End Time
2015-12-14 14:47:46	Smart Scan		2015-12-14 14:49:03
2015-12-14 14:39:02	Smart Scan		2015-12-14 14:40:20
2015-12-14 14:36:13	Smart Scan		2015-12-14 14:37:22
2015-12-14 14:28:12	Smart Scan		2015-12-14 14:30:11
2015-12-14 13:43:15	File Scan	D:\Suspicious Files\Unbelievable\textexecutab ...	2015-12-14 13:43:17
2015-12-14 13:42:47	File Scan	D:\Doubtful\vtPath32.exe	2015-12-14 13:42:48

Column Descriptions

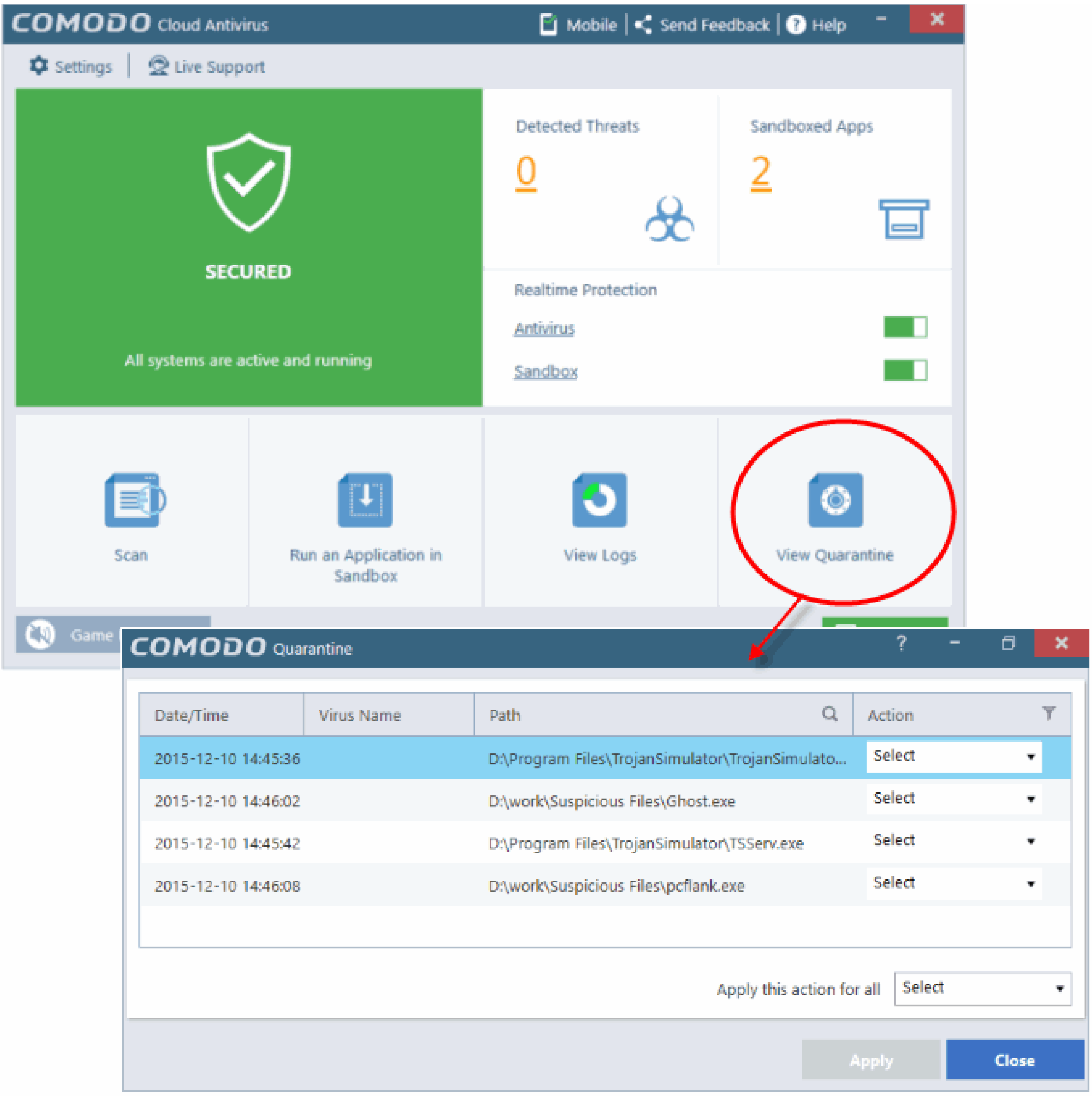
1. **Date/Time** – The date and time of the event
2. **Type –** The type of scan profile
3. **Path** – The location scanned. This will be available for 'File', 'Folder' and 'Custom' scan.
4. **End Time** – Date and time at which the scan was completed

- To export the logs as a '.log' file, click the 'Save' button
- To open a stored log file, click the 'Open log file' button
- To update the list with the latest events, click the 'Refresh' button
- To clear the scan logs, click the 'Clear logs' button

5. View and Manage Quarantined Items

The 'Quarantine' interface displays a list of files which have been isolated by Comodo Cloud Antivirus to prevent them from infecting your system. Items are generally placed in quarantine as a result of an on-demand or real time antivirus scan. Any files transferred to quarantine are encrypted - meaning they cannot be run or executed. You can also manually quarantine items you believe are suspicious. Conversely, you can restore a file to its original location if you think it has been quarantined in error, and/or submit files as false positives to Comodo for analysis.

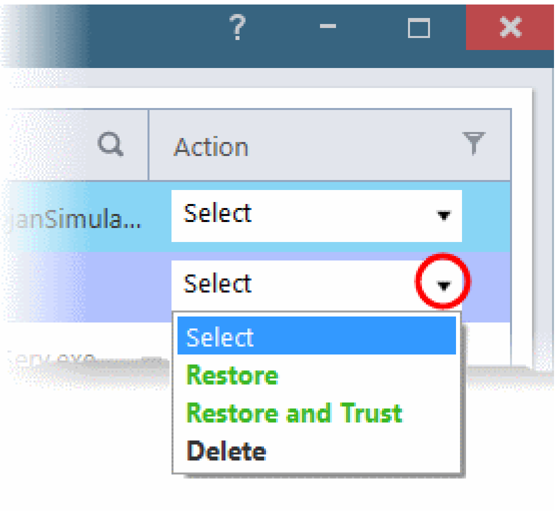
The 'Quarantine' interface can be accessed by clicking 'View Quarantine' from the home screen.



Date/Time	Virus Name	Path	Action
2015-12-10 14:45:36		D:\Program Files\TrojanSimulator\TrojanSimulato...	Select
2015-12-10 14:46:02		D:\work\Suspicious Files\Ghost.exe	Select
2015-12-10 14:45:42		D:\Program Files\TrojanSimulator\TSServ.exe	Select
2015-12-10 14:46:08		D:\work\Suspicious Files\pcflank.exe	Select

Column Descriptions

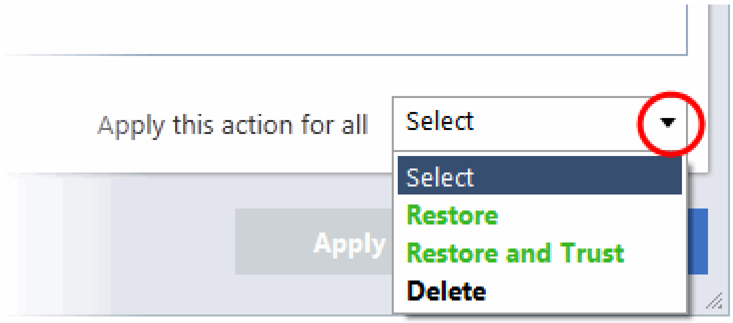
- **Date/Time** – The precise date and time at which the item was moved to quarantine
- **Virus Name** – The file name of the quarantined file
- **Path** – The location where the file was discovered
- **Action** - Displays a drop-down with options for handing the item.



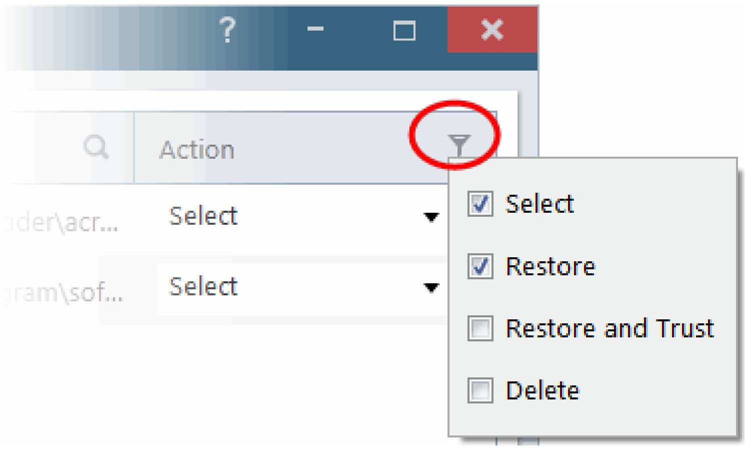
The available actions are:

- **Restore** – The item will be restored to its original location. However, subsequent scans will still identify it as malicious and will quarantine the file.
- **Restore and Trust** – The item will be restored to its original location and will be added to Trusted Applications list in your local file list. The file will be excluded from future scans.
- **Delete** – The item will be removed from your computer.

You can also apply an action to all quarantined items at once using the 'Apply this action for all' drop-down at bottom right:



- To filter items based on the actions to be executed on them, click the funnel icon in the 'Action' column:



The 'Quarantine' interface also allows you to:

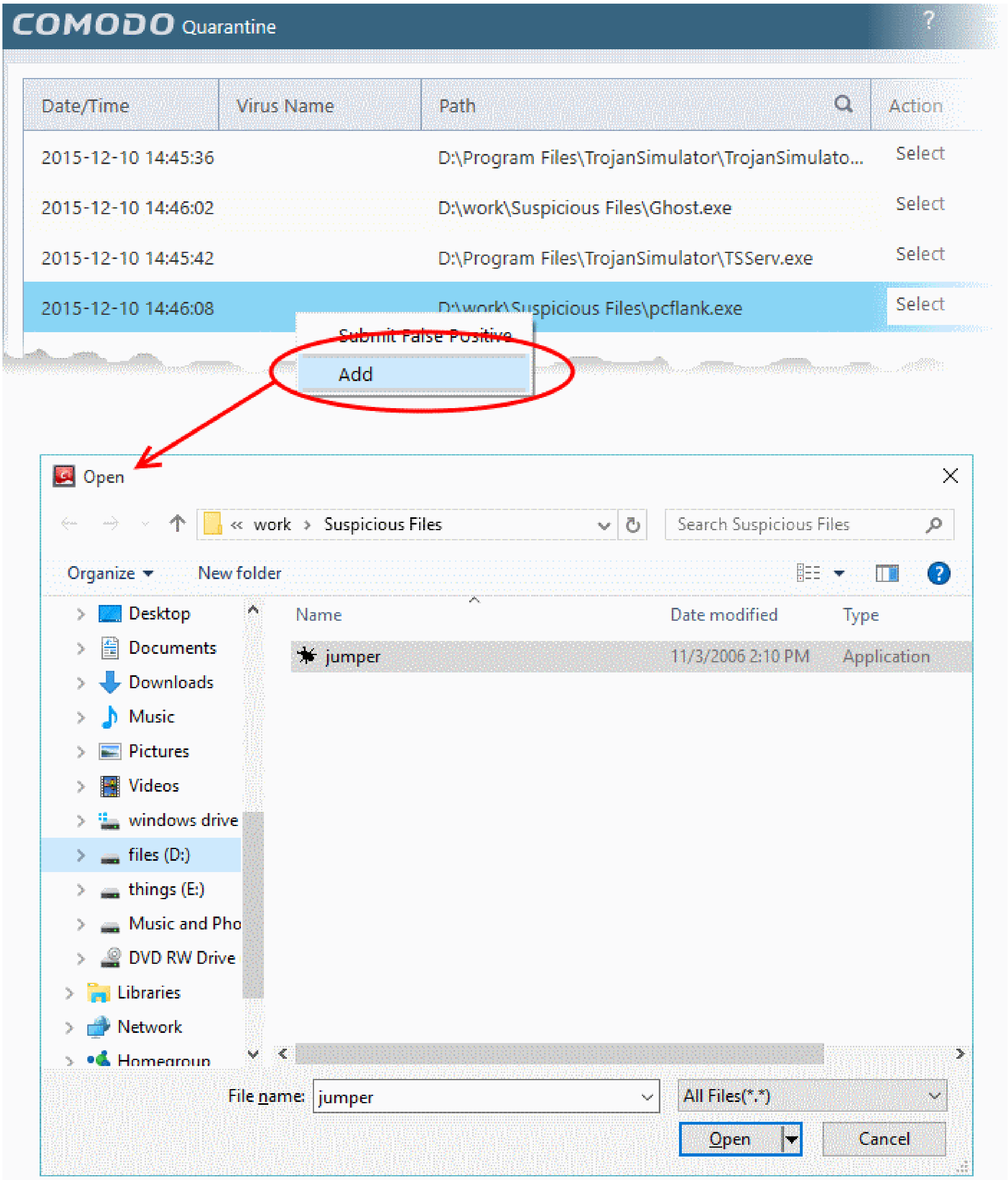
- **Manually add items to quarantine**
- **Delete quarantined items**
- **Restore a quarantined item to its original location**
- **Submit false positives to Comodo for analysis**

Manually add items to quarantine

If you have a file, folder or drive that you suspect may contain a virus which has not been detected by the scanner, then you have the option to isolate that item in quarantine.

To manually add a Quarantined Item

- Right click any where inside the Quarantine interface and choose 'Add'
- Navigate to the file you want to add to quarantine and click 'Open'.



Date/Time	Virus Name	Path	Action
2015-12-10 14:45:36		D:\Program Files\TrojanSimulator\TrojanSimulato...	Select
2015-12-10 14:46:02		D:\work\Suspicious Files\Ghost.exe	Select
2015-12-10 14:45:42		D:\Program Files\TrojanSimulator\TSServ.exe	Select
2015-12-10 14:46:08		D:\work\Suspicious Files\pcflank.exe	Select

Name	Date modified	Type
jumper	11/3/2006 2:10 PM	Application

File name: jumper

- Click 'Apply' to quarantine the file

To delete quarantined item(s)

- To delete a single item, choose 'Delete' from the 'Action' drop-down in the item row.
- To delete all quarantined items at once, choose 'Delete' from the drop-down beside 'Apply this action to all' at the bottom right of the interface.
- Click 'Apply' for your changes to take effect

The file(s) will be deleted from the system permanently.

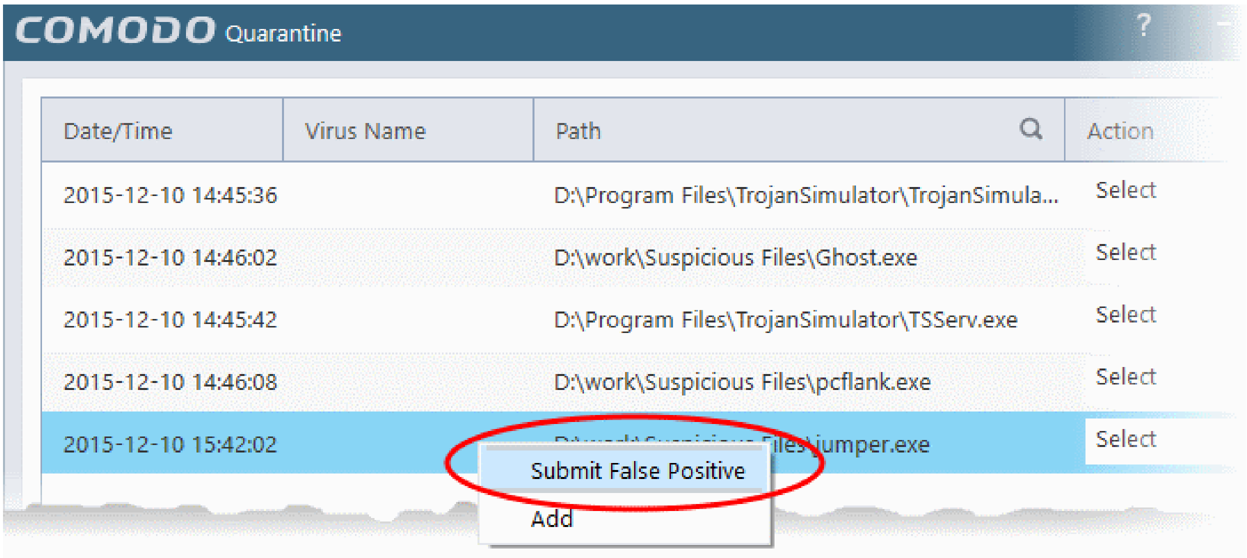
To restore quarantined item(s) to its/their original location(s)

- To restore a single item, choose 'Restore' from the 'Action' drop-down in the item row.
- To restore a single item and exclude it from future scans, choose 'Restore and Trust' from the 'Action' drop-down in the item row.
- To restore all items, choose 'Restore' from the 'Apply this action to all' drop-down at bottom right.
- To restore all items and exclude them from future scans, choose 'Restore and Trust' from the 'Apply this action to all' drop-down at bottom right.
- Click 'Apply' for your changes to take effect

Any restored files will be moved back to their original locations.

To submit a selected quarantined item to Comodo for analysis

- Select the item from the 'Quarantine' interface, right click on it and choose 'Submit False Positive' from the options.



Date/Time	Virus Name	Path	Action
2015-12-10 14:45:36		D:\Program Files\TrojanSimulator\TrojanSimula...	Select
2015-12-10 14:46:02		D:\work\Suspicious Files\Ghost.exe	Select
2015-12-10 14:45:42		D:\Program Files\TrojanSimulator\TSServ.exe	Select
2015-12-10 14:46:08		D:\work\Suspicious Files\pcflank.exe	Select
2015-12-10 15:42:02		D:\work\Suspicious Files\jumper.exe	Select

- Click 'Apply' for your changes to take effect

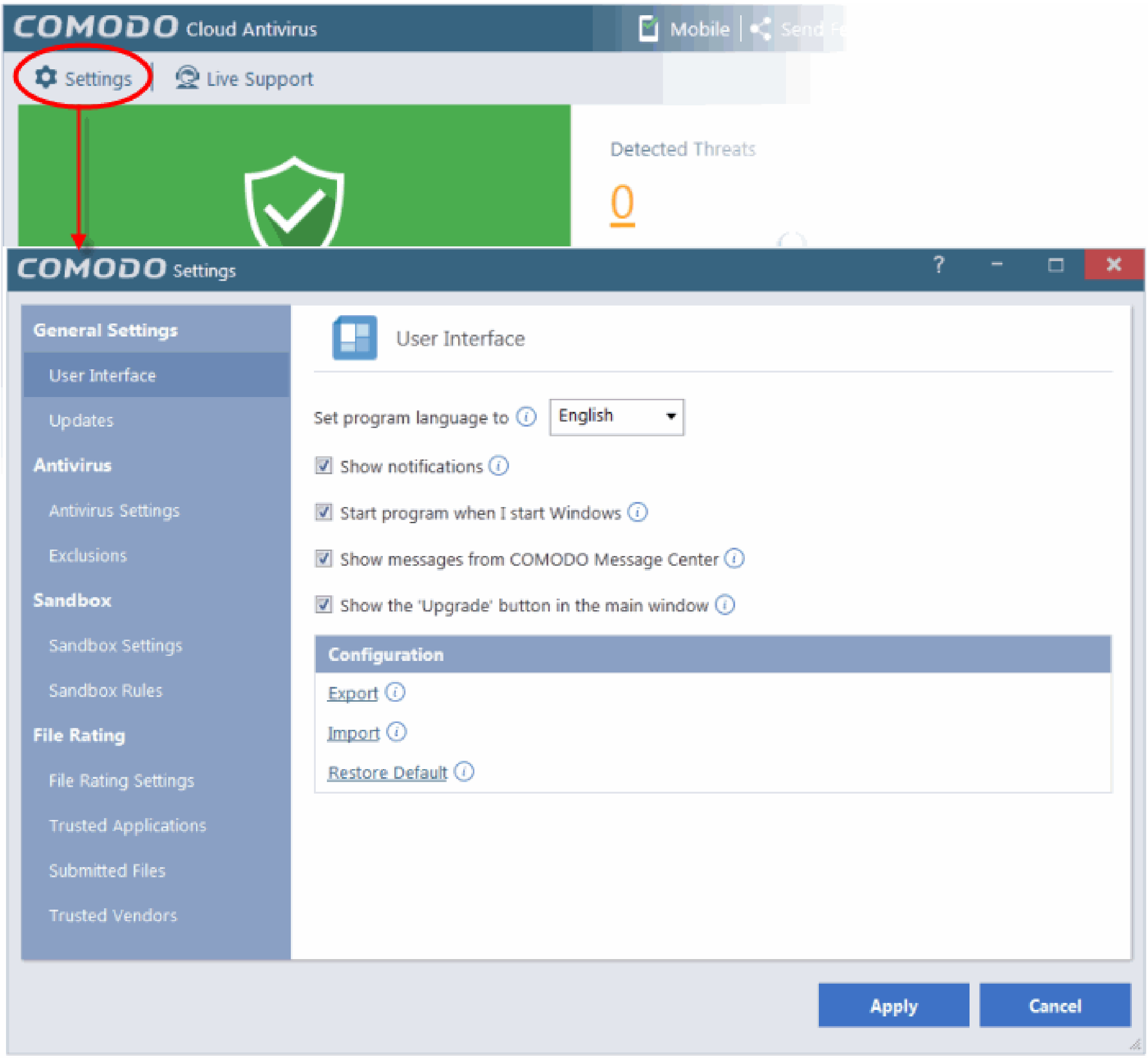
You can submit suspicious files to Comodo for deeper analysis. You can also submit files which you think are safe but have been identified as malware by CCAV (false positives). Comodo will analyze all submitted files. If they are found to be trustworthy, they will be added to the Comodo safe list (whitelisted). Conversely, if they are found to be malicious then they will be added to the database of virus signatures (blacklisted).

Note: Quarantined files are strongly encrypted, cannot be executed and do not constitute any danger to your computer.

6. CCAV Settings

The 'Settings' interface allows you to configure every aspect of the operation, behavior and appearance of Comodo Cloud Antivirus (CCAV). The 'General Settings' section lets you specify top-level preferences regarding the interface and the updates. The 'General Settings' section lets advanced users delve into granular configuration of the 'Antivirus', and the 'Sandbox' modules. For example, the 'Antivirus Settings' area allows you to enable/disable real-time scanning, configure detection actions, create exclusions and more. The 'Sandbox Settings' area allow you to configure the behavior of the Sandbox, add programs which should always run inside the sandbox and more. The 'File Rating' settings allows you to add Trusted files to be excluded from scans and monitoring, view files submitted to Comodo for analysis, and view and manage 'Trusted Vendors' list.

To open the 'Settings' interface, click 'Settings' from the top menu:



Set program language to: English

☑ Show notifications

☑ Start program when I start Windows

☑ Show messages from COMODO Message Center

☑ Show the 'Upgrade' button in the main window

Tip: Alternatively, you can open the 'Settings' interface by right-clicking on the CCAV system tray ion and choosing 'Settings'.

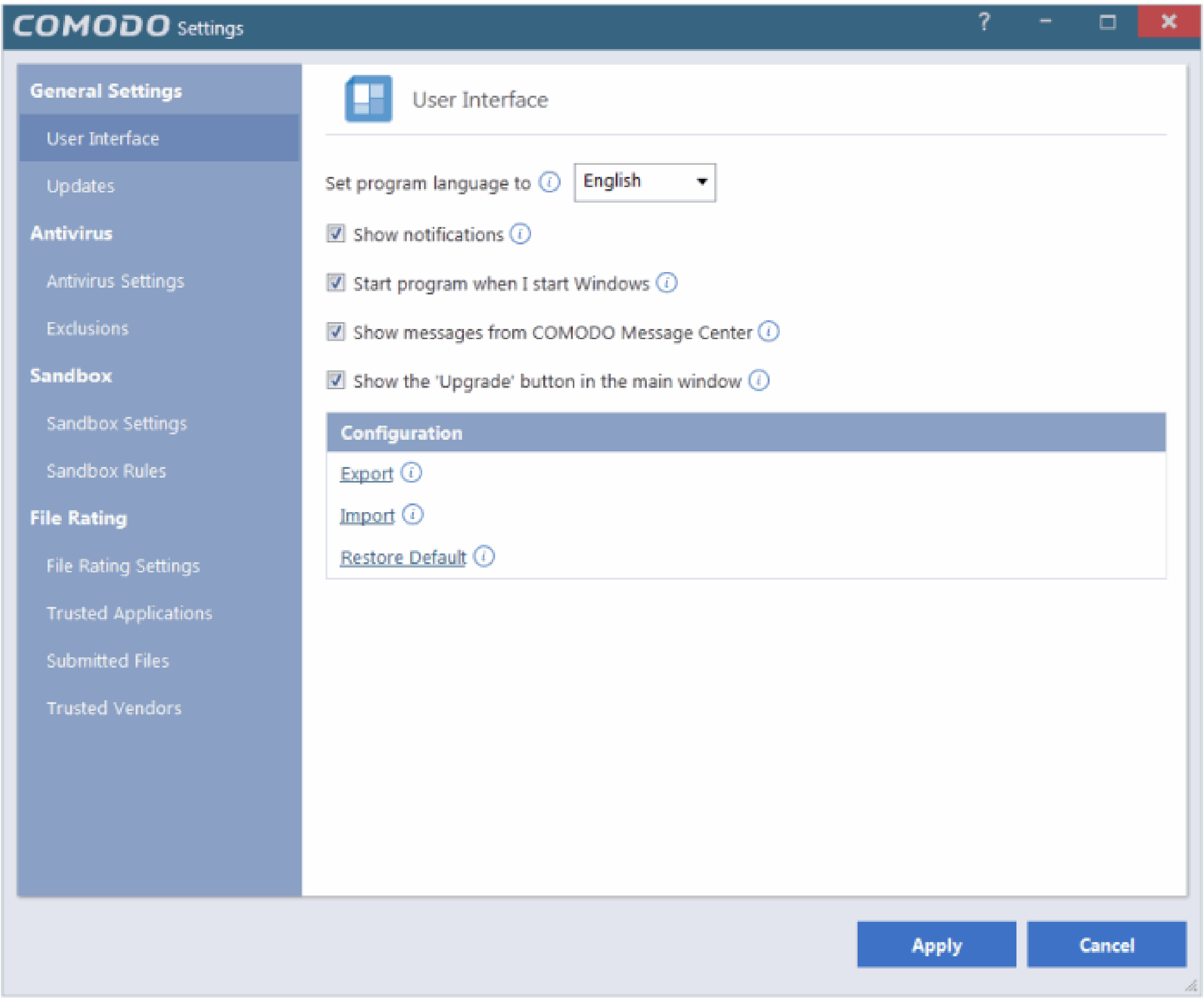
The following sections in this guide explain the various settings areas in more detail:

- **General Settings** – Allows you to configure the appearance and behavior of the application
  - **Customize User Interface**
  - **Configure Program and Updates**
- **Antivirus** – Allows you to configure the 'Antivirus' module
  - **Antivirus Settings**

  - Exclusions
- Sandbox - Allows you to configure the 'Sandbox' module
  - Sandbox Settings
  - Sandbox Rules
- File Rating – Allows you to view and manage Trusted applications list, files submitted to Comodo and Trusted Vendors list
  - File Rating Settings
  - Trusted Applications
  - Submitted Files
  - Trusted Vendors List

6.1. General Settings

The 'General Settings' area enables you to customize the appearance and overall behavior of Comodo Cloud Antivirus. You can configure general properties like the interface language, notification messages, automatic updates and more.



User Interface

Set program language to: English

☑ Show notifications

☑ Start program when I start Windows

☑ Show messages from COMODO Message Center

☑ Show the 'Upgrade' button in the main window

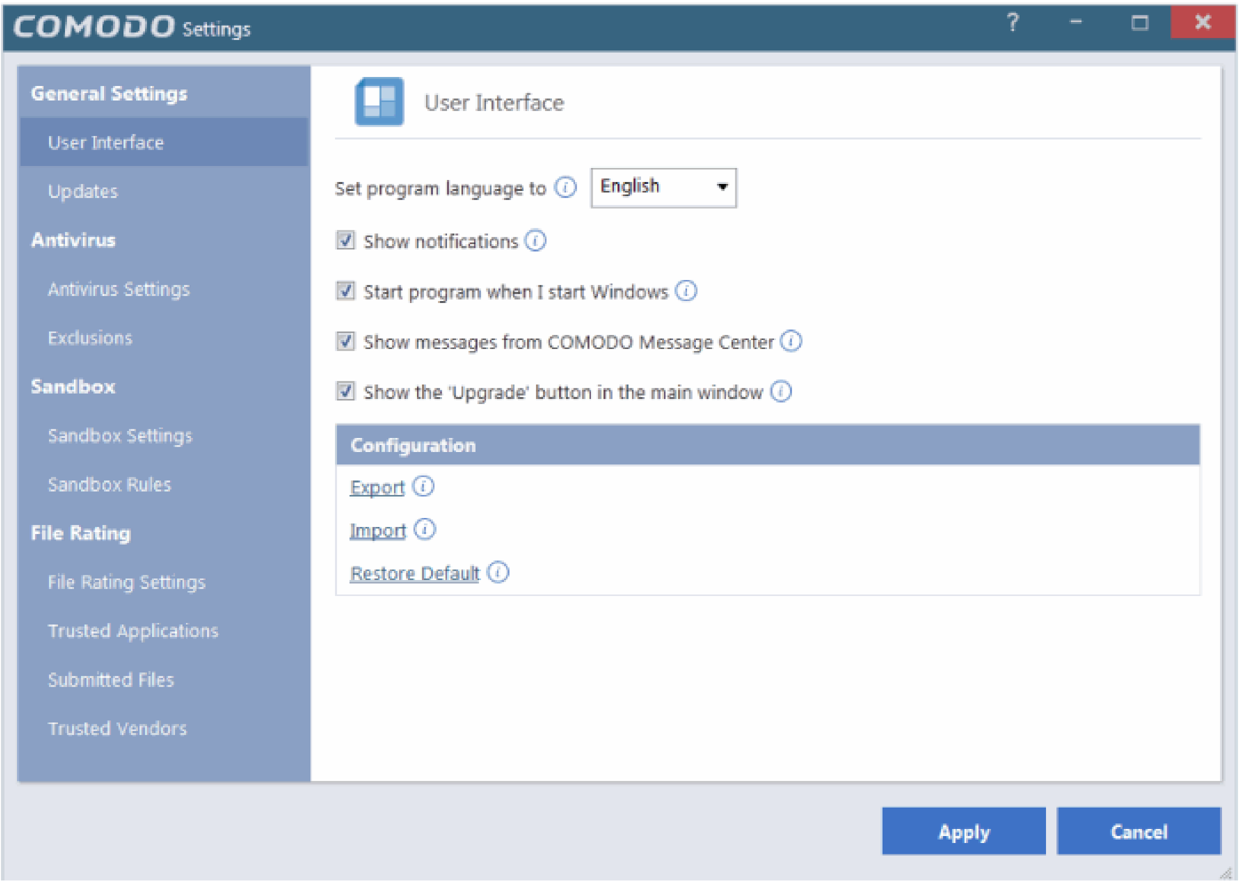
The category has the following sections:

- User Interface
- Updates

6.1.1. Customize User Interface

The 'User Interface' settings area lets you choose the interface language, how to start the application and to configure how messages are to be displayed. You can export your current CCAV configuration as an XML file, allowing you import the configuration to other computers, or to quickly re-implement your settings if you uninstall then re-install the application.

To open 'User Interface' settings, click 'User Interface' under 'General Settings' on the left of the 'Settings' interface.



Set program language to English

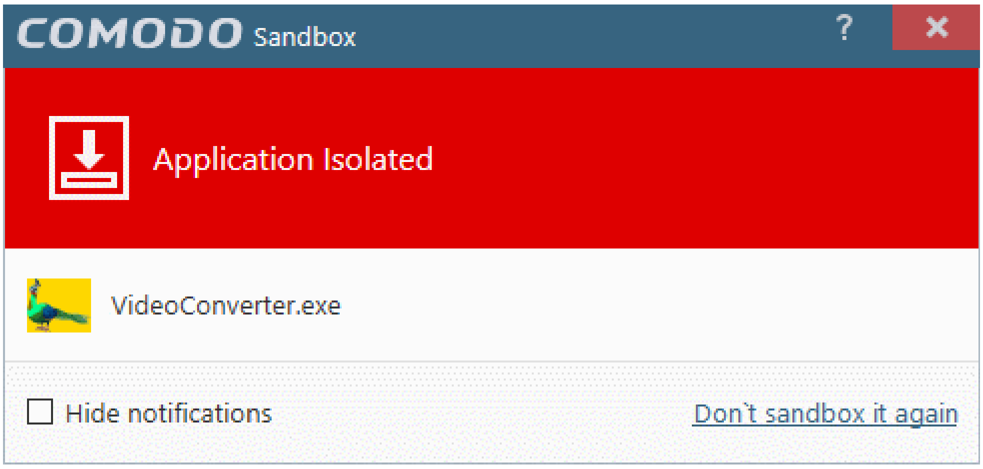
☑ Show notifications

☑ Start program when I start Windows

☑ Show messages from COMODO Message Center

☑ Show the 'Upgrade' button in the main window

- **Language Settings** - Comodo Cloud Antivirus is available in multiple languages. You can choose the language in which the interface is to be displayed, from the 'Set program language to' drop-down menu (***Default = English***).
- **Show Notifications** – CCAV displays notifications at the bottom right corner of your screen to inform you about the actions that it is taking and any CIS status updates. For example, notifications are displayed when CCAV automatically quarantines a file after a real-time scan or when it runs a program inside the sandbox. An example is shown below.



Application Isolated

VideoConverter.exe

☐ Hide notifications

Antivirus notifications will also be displayed if you have selected 'Quarantine' or 'Block' in the 'Action when threat is detected' setting in the 'Antivirus' settings screen.

- Clear this check box if you do not want to see these system messages (***Default = Enabled***).

Tip: Selecting 'Hide notifications' in any alert will automatically disable this setting.

- **Start program when I start Windows** – By default, CCAV will start automatically every time you start your computer in order to provide continuous protection. Clear this setting if you do not want the application to load when you start Windows. (***Default = Enabled***)
- **Show messages from COMODO Message Center** – If enabled, Comodo Message Center messages will periodically appear to keep you abreast of news in the Comodo world. An example is shown below. (***Default = Enabled***)

- Click 'Apply' for your changes to take effect

Exporting your Security Configuration - CCAV allows you to import and export your current CCCA configuration to a .xml file, and to reset CCAV configuration back to factory settings. This is especially useful if you are a network administrator looking to roll out a standard security configuration across multiple computers. If you are upgrading your system and there is a need to uninstall and re-install CCAV then it can be great time-saver to export your configuration settings beforehand. After re-installation, you can import your previous settings and avoid having to configure everything over again.

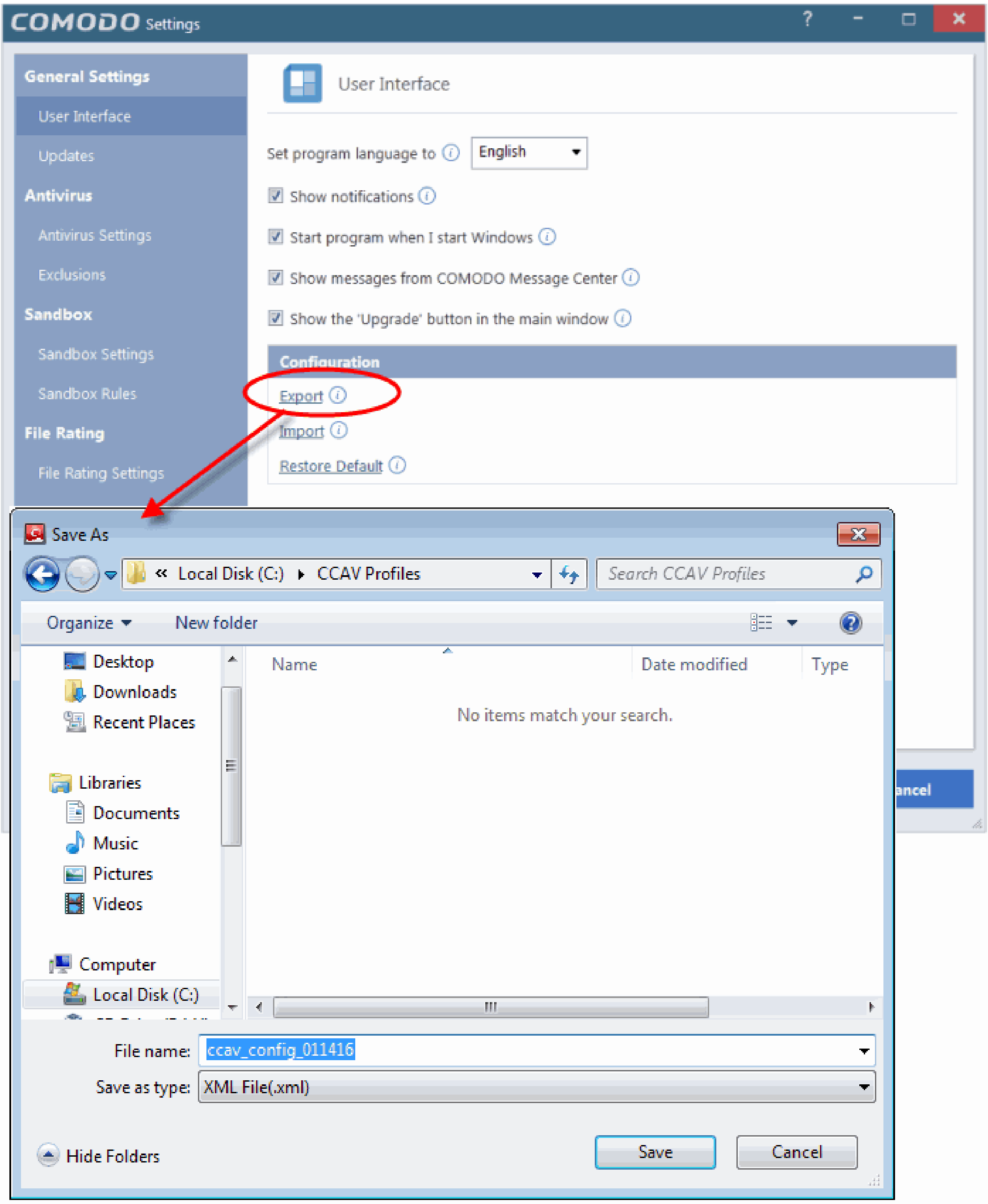
The following explains more about:

- **Export a configuration to a file**
- **Import a saved configuration from a file**
- **Reset to default a configuration setting**

To export your current configuration

- Click the 'Export' link in the 'User Interface' settings area

The 'Save As' dialog will open:



Set program language to: English

☑ Show notifications

☑ Start program when I start Windows

☑ Show messages from COMODO Message Center

☑ Show the 'Upgrade' button in the main window

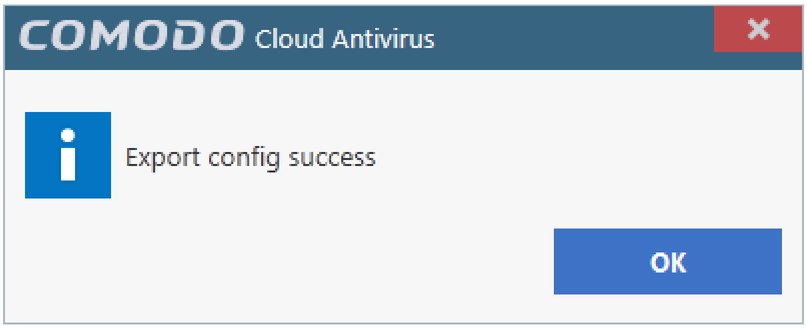
No items match your search.

File name: ccav_config_011416

Save as type: XML File(.xml)

- Navigate to the location where you want to save the configuration file, type a name (e.g., 'ccav_config') for the file and click 'Save'.

A confirmation dialog will appear indicating the successful export of the profile.

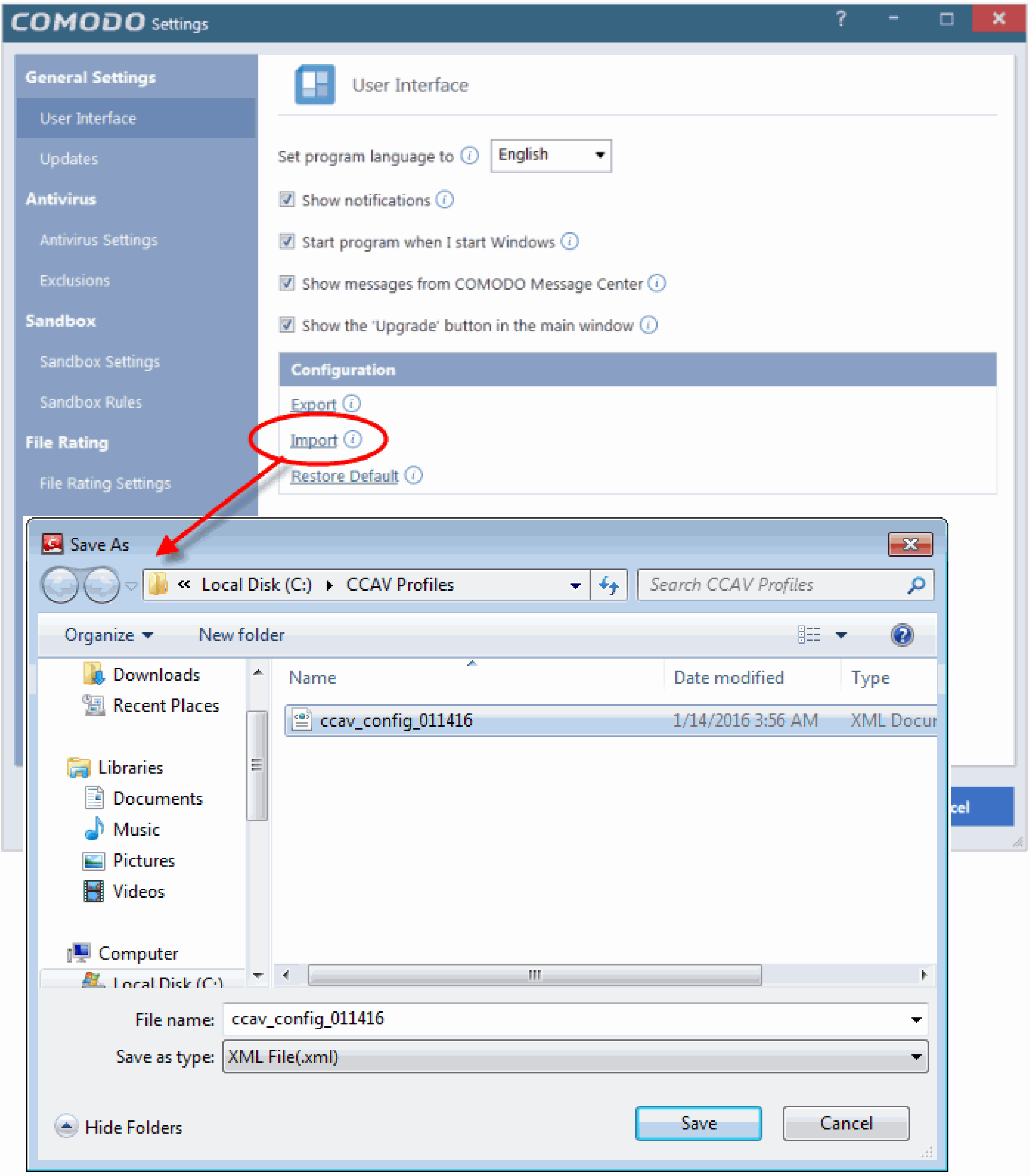


Export config success

Import a saved configuration from a file

- Click the 'Import' link in the 'User Interface' settings area

The 'Save As' dialog will open:



Set program language to: English

☑ Show notifications

☑ Start program when I start Windows

☑ Show messages from COMODO Message Center

☑ Show the 'Upgrade' button in the main window

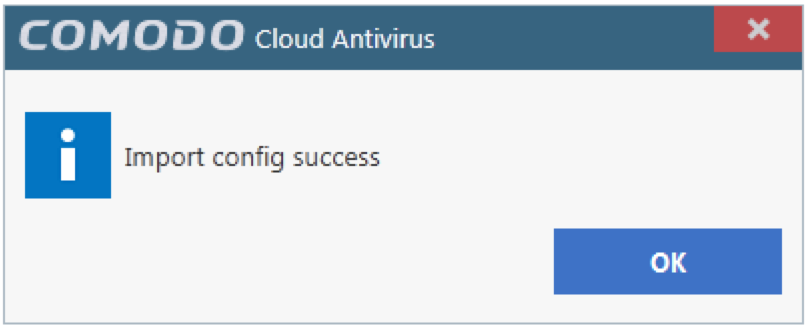
Name	Date modified	Type
ccav_config_011416	1/14/2016 3:56 AM	XML Docu

File name: ccav_config_011416

Save as type: XML File(.xml)

- Navigate to the location of the saved profile and click 'Save' .

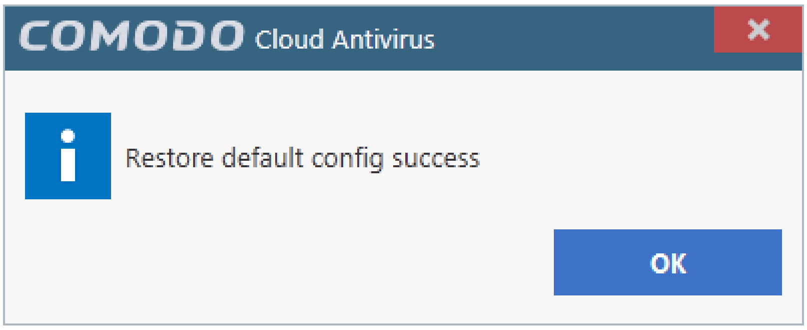
A confirmation dialog will appear indicating the successful import of the profile:


COMODO Cloud Antivirus

Import config success

- Click the 'Restore Default' link to reset CCAV to factory settings:

A confirmation dialog will appear indicating successful restoration:

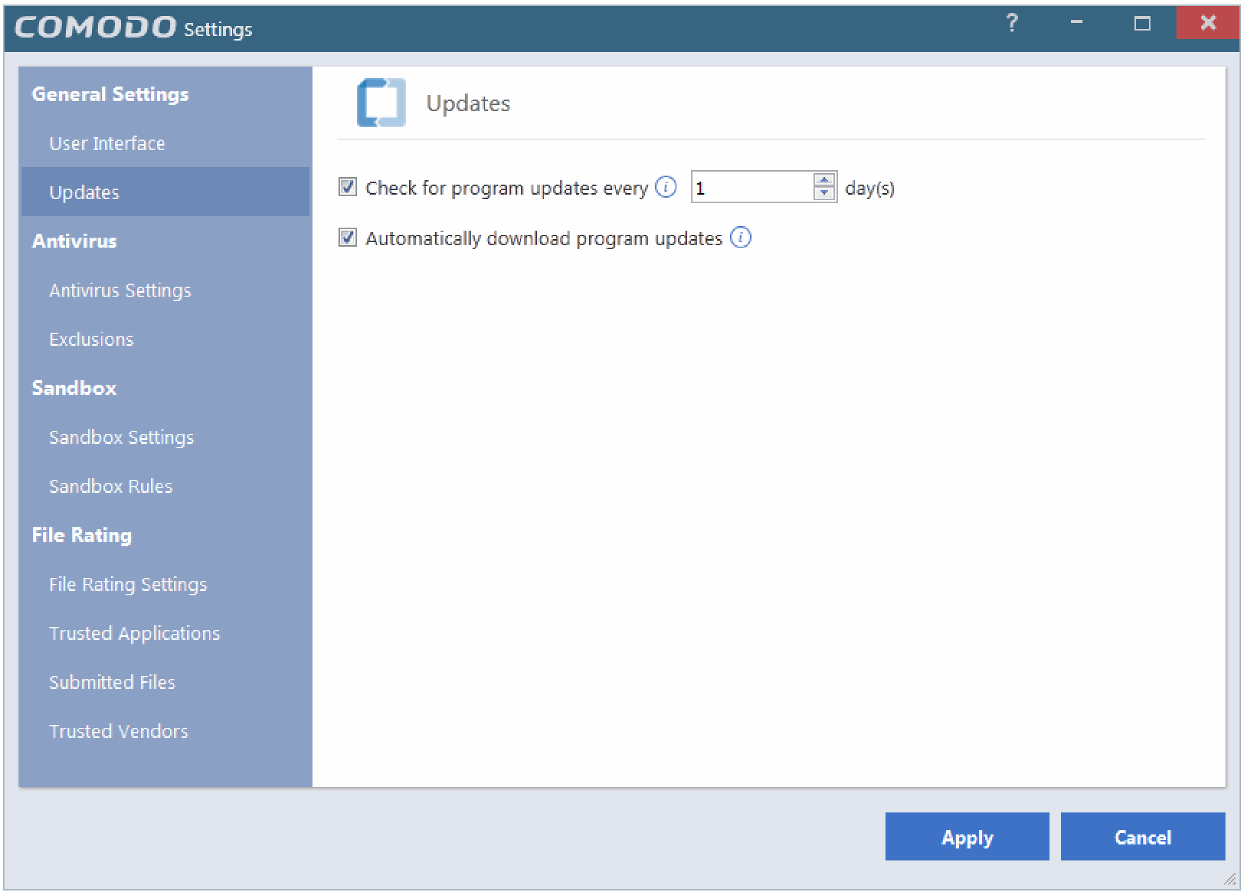

COMODO Cloud Antivirus

Restore default config success

6.1.2. Configure Program Updates

The 'Updates' area allows you to configure settings that govern CCAV program updates.

To open the area, click 'Updates' under 'General Settings' on the left of the 'Settings' interface:



Updates

☑ Check for program updates every 1 day(s)

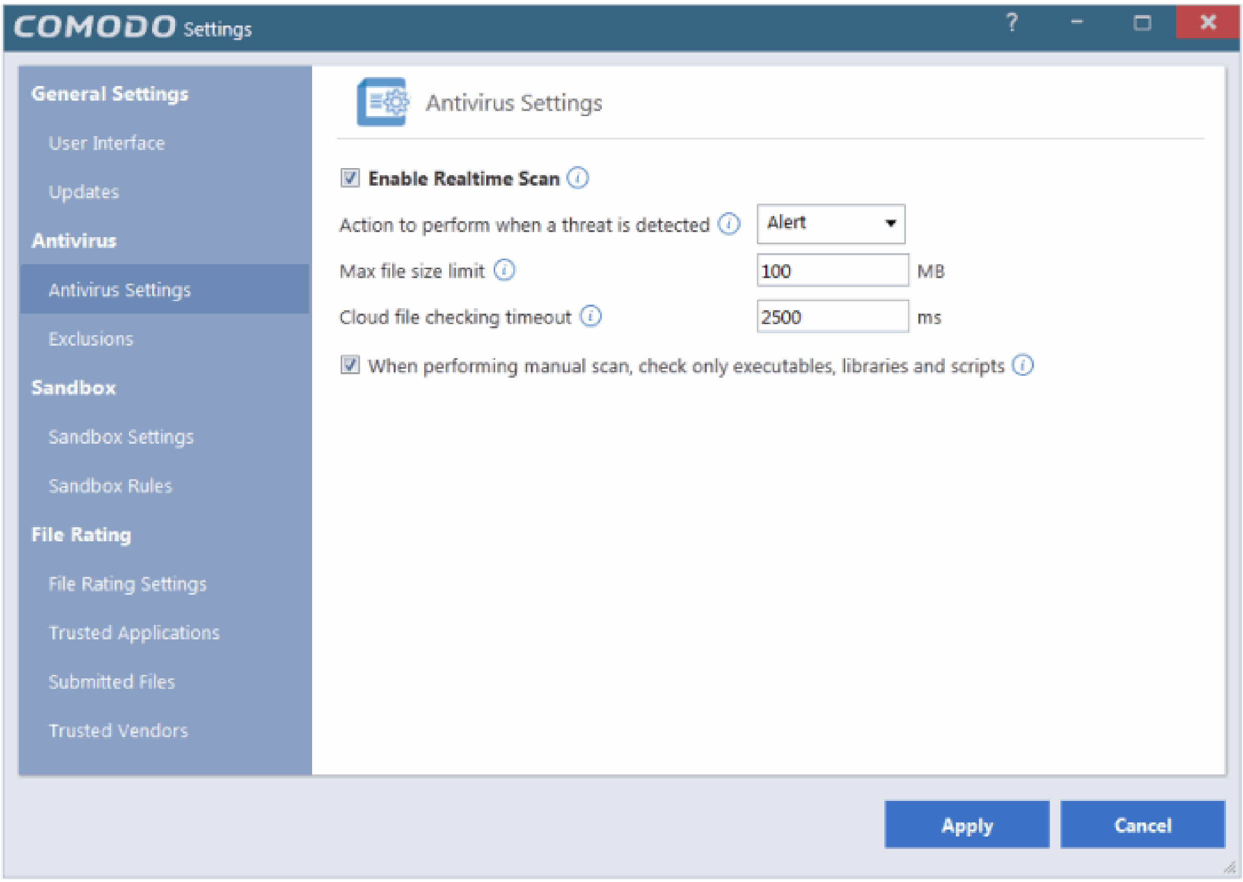
☑ Automatically download program updates

- **Check program updates every NN day(s)** - Enables you to specify the interval at which CCAV will check for availability of new version of the program updates from the Comodo servers. Set the time interval (in days) from the drop-down combo box. **(Default = 1 day)**
- **Automatically download program updates** - Instructs CCAV to automatically download program updates as soon as they are available. **(Default=Enabled)**

- Click 'Apply' for your changes to take effect.

6.2. Antivirus Settings

The 'Antivirus' settings area allows you to enable or disable antivirus protection, and to configure file size limits, time-out periods and scan exclusions:



☑ Enable Realtime Scan

Action to perform when a threat is detected: Alert

Max file size limit: 100 MB

Cloud file checking timeout: 2500 ms

☑ When performing manual scan, check only executables, libraries and scripts

There are two sub-sections – please click on the following links to find out more about each:

- **Antivirus Settings**
- **Exclusions**

6.2.1. Antivirus Settings

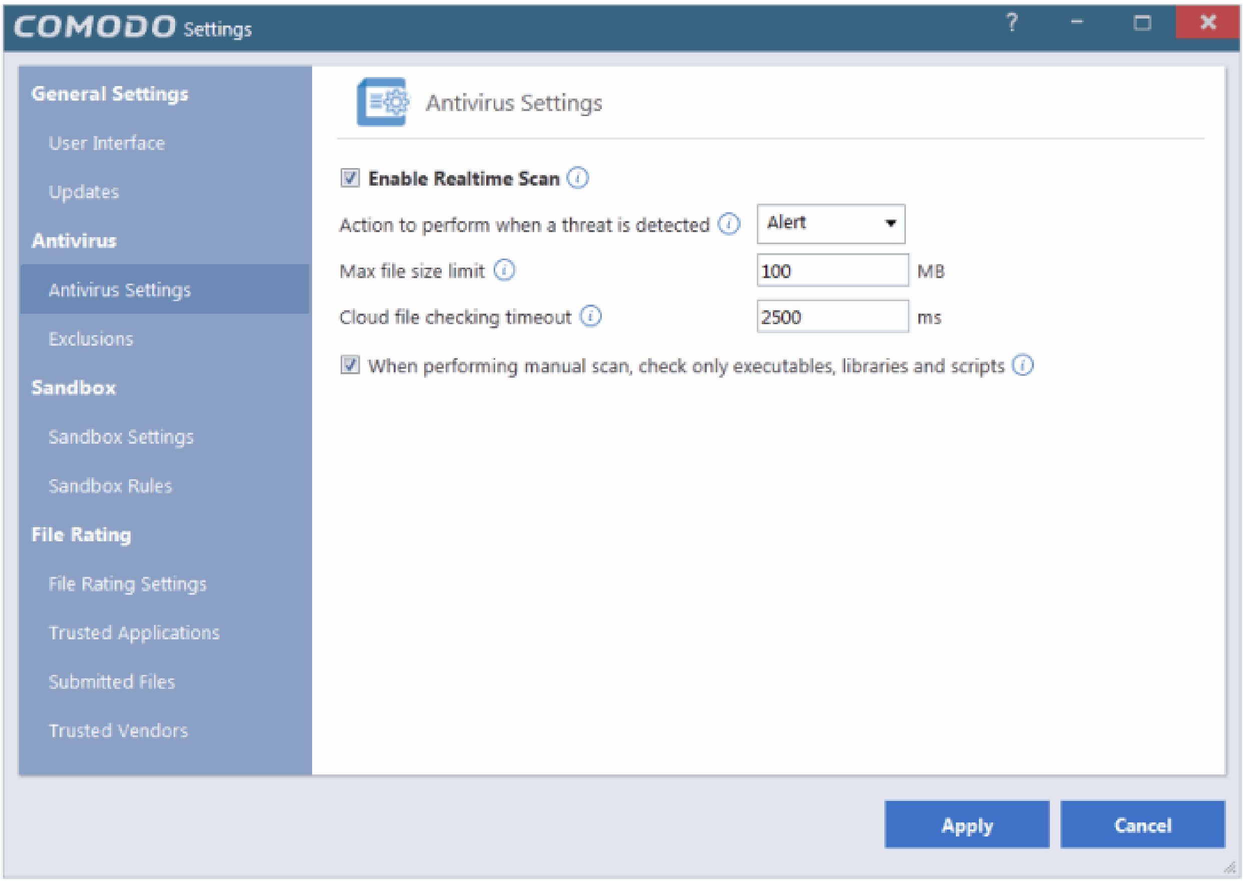
CCAV's real-time scanner checks files constantly monitors all files and processes on your computer for potential threats. If you launch a program or file which creates destructive anomalies, then the scanner blocks it and alerts you immediately. The Antivirus settings interface allows you to enable/disable the real-time scanner and to configure scan parameters.

To open the 'Antivirus Settings' area

- Click the Antivirus link on the CCAV home screen

  OR

- Click 'Settings' at the top left of the home screen then select 'Antivirus Settings'



Antivirus Settings

☑ Enable Realtime Scan

Action to perform when a threat is detected: Alert

Max file size limit: 100 MB

Cloud file checking timeout: 2500 ms

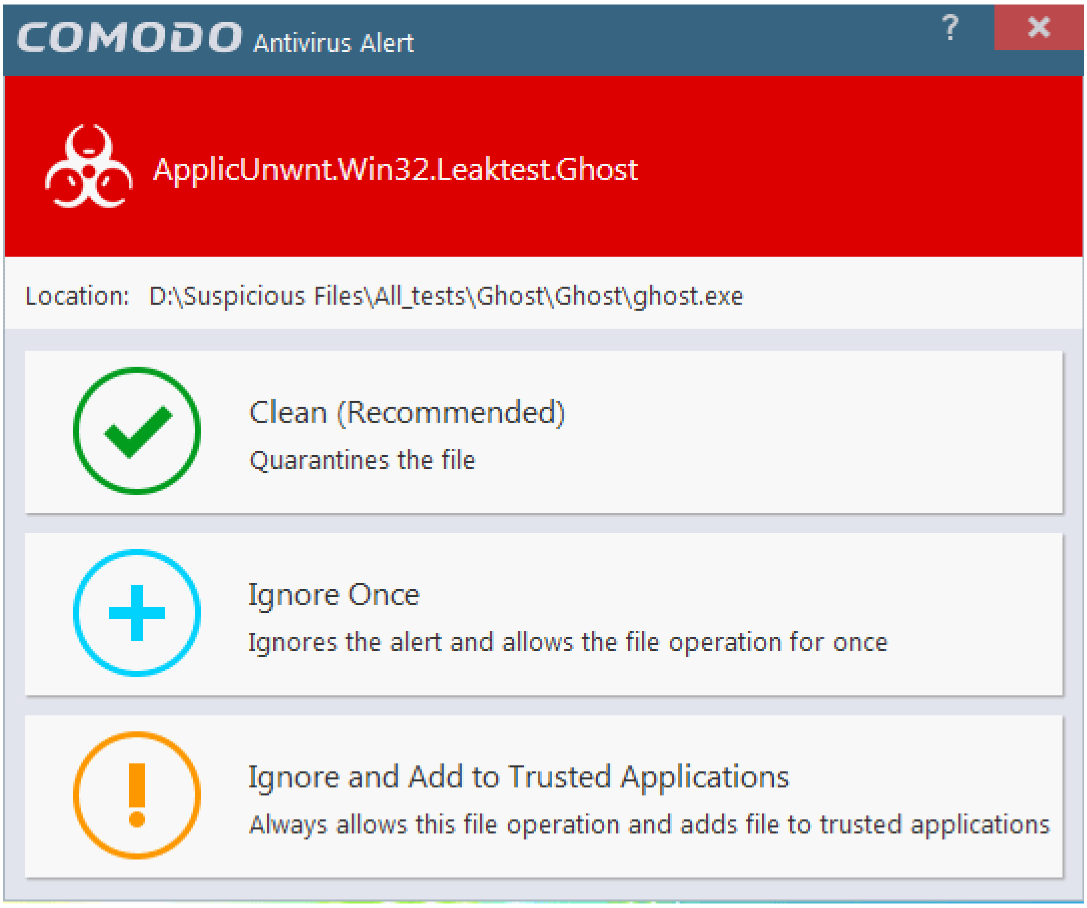
☑ When performing manual scan, check only executables, libraries and scripts

- **Enable Real-time Scan** – Allows you to enable or disable Real-time virus monitoring. It is recommended that you leave this option selected. (***Default = Enabled***)

Background Note: The real-time scanner (aka 'On-Access Scan') is always ON and checks files in real time when they are created, opened or copied (as soon as you interact with a file, Comodo Cloud Antivirus checks it). This instant detection of viruses assures you, the user, that your system is perpetually monitored for malware and enjoys the highest level of protection.

The real-time Scanner also scans system memory on start. If you launch a program or file which creates destructive anomalies, then the scanner blocks it and alerts you immediately. Should you wish, however, you can specify that CCAV does not show you alerts if viruses are found but automatically deals with them (choice of auto-quarantine or auto-block). It is highly recommended that you leave the Real Time Scanner enabled to ensure your system remains continually free of infection.

- **Action when a threat is detected** – Allows you to configure how CCAV should react when a malware is detected by the real-time protection engine (***Default = Alert***). The available options are:
  - **Alert** – An alert will be displayed whenever a malware is identified. An example of Antivirus Alert is shown below:



COMODO Antivirus Alert

ApplicUnwnt.Win32.Leaktest.Ghost

Location: D:\Suspicious Files\All_tests\Ghost\Ghost\ghost.exe

Clean (Recommended)
Quarantines the file
Ignore Once
Ignores the alert and allows the file operation for once
Ignore and Add to Trusted Applications
Always allows this file operation and adds file to trusted applications

You can choose to clean, ignore or add the file to trusted files list. If you need more details about this options, refer to **Antivirus Alerts** in **Understanding CCAV Alerts**. Choosing not show antivirus alerts in favor of automatically quarantining or blocking will minimize disturbances but at some loss of user awareness.

  - **Quarantine** – The detected threat(s) will be automatically moved to quarantine for your later assessment and action. Refer to the section **View and Manage Quarantined Items** for more details.
  - **Block** - Stops the application or file from execution.

- **Max file size limit** - Allows you to set the maximum size of a file that CCAV should scan. Files larger than the size specified here will not be not scanned. (***Default = 100 MB***)
- **Cloud file checking timeout** – Allows you to the maximum time for which CCAV can run an antivirus scan on a single file over the cloud. If CCAV has not completed scanning a particular file by the end of this time period then the file is skipped (***Default = 2500 Ms***)
- **When performing manual scan, check only executables, libraries and scripts** – Allows you to limit the file types to be scanned during an on-demand/manual scan. By default, CCAV scans only executable files, library files (e.g. .dll files) and scripts in the target location. This helps save time because, statistically, those file types are far more likely to contain malware. If you want to scan every file in a location then clear this check-box. For more derails on on-demand/manual scans, refer to the section **Scan and Clean your Computer**.

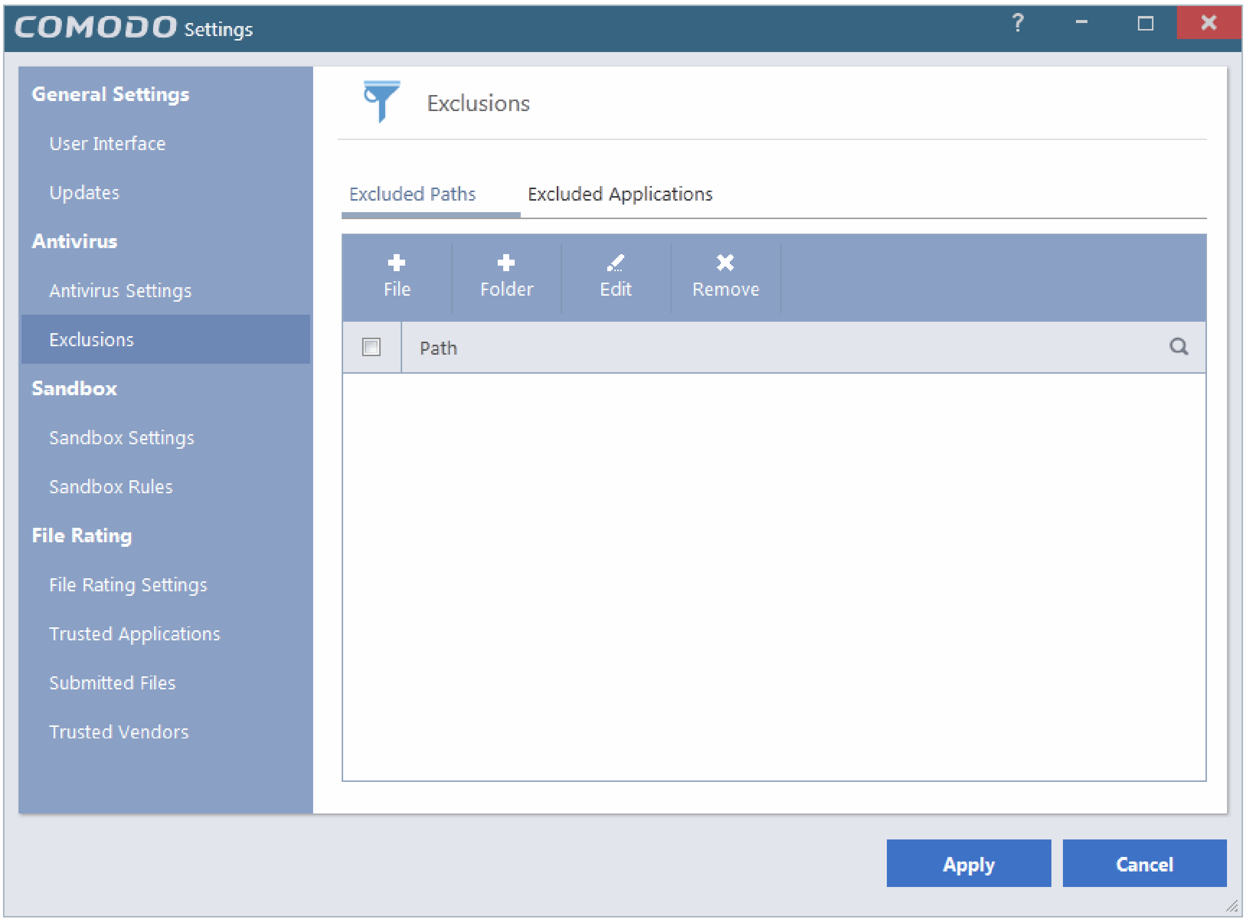
6.2.2. Exclusions

CCAV allows you to create a list of files and folders that should be excluded from antivirus scans. This list also includes the files which you chose to '**Ignore** ' from the **Scan Results** window.

The 'Exclusions' panel displays all currently excluded items and allows you to manually add or remove items.

To open the Exclusions panel

- Open the 'Advanced Settings' interface by clicking 'Settings' link from the top left of the CCAV interface
- Click on 'Antivirus' from and choose 'Exclusions'



The 'Exclusions' panel has two tabs:

- **Excluded Paths** - Displays a list of paths/folders/files in your computer which are excluded from real-time, on-demand and scheduled antivirus scans. Refer to the section **Excluding Drives/Folders/Files from all types of scans** for more details on adding and removing exclusion items in this interface.
- **Excluded Applications** - Displays a list of programs/applications in your computer which are excluded only from real-time antivirus scans. Items are included on this list by clicking 'Ignore' from the **Scan Results** window of various scans and **Antivirus Alerts**, or by adding items manually. Please note that these items are excluded only from real-time sans but will be scanned during an on-demand scan. Refer to **Excluding Programs/Applications from real-time scans** later in this section for more details.

Excluding Drives/Folders/Files from all types of scans

You can exclude a drive partition, a folder or a file from the real-time scan by adding them to 'Excluded Paths'.

To add file to excluded paths

- Click 'File' from the top, under the 'Excluded Paths' tab

You can choose to add a:

- an individual File

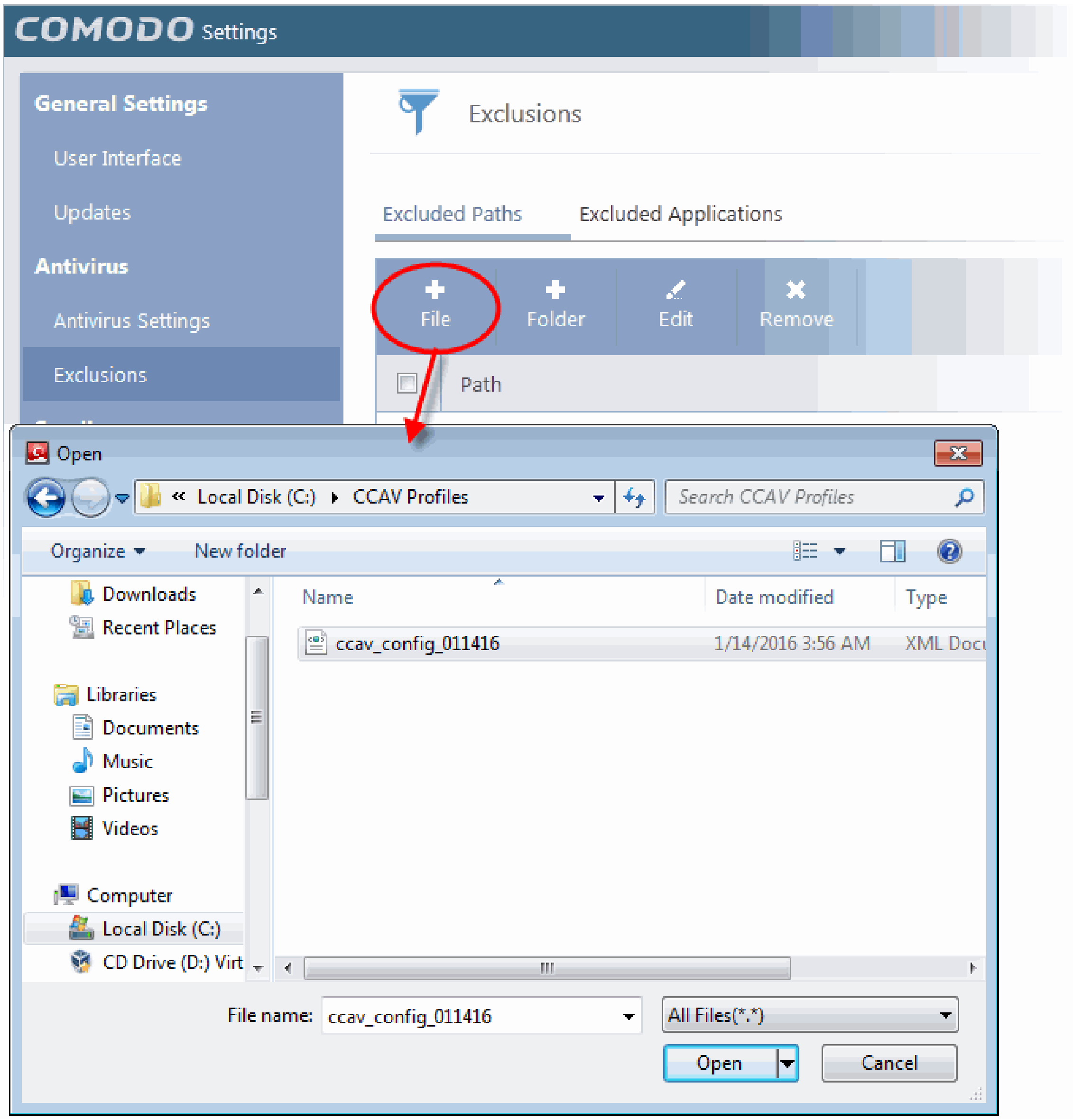
  OR

- Drive partition/Folder

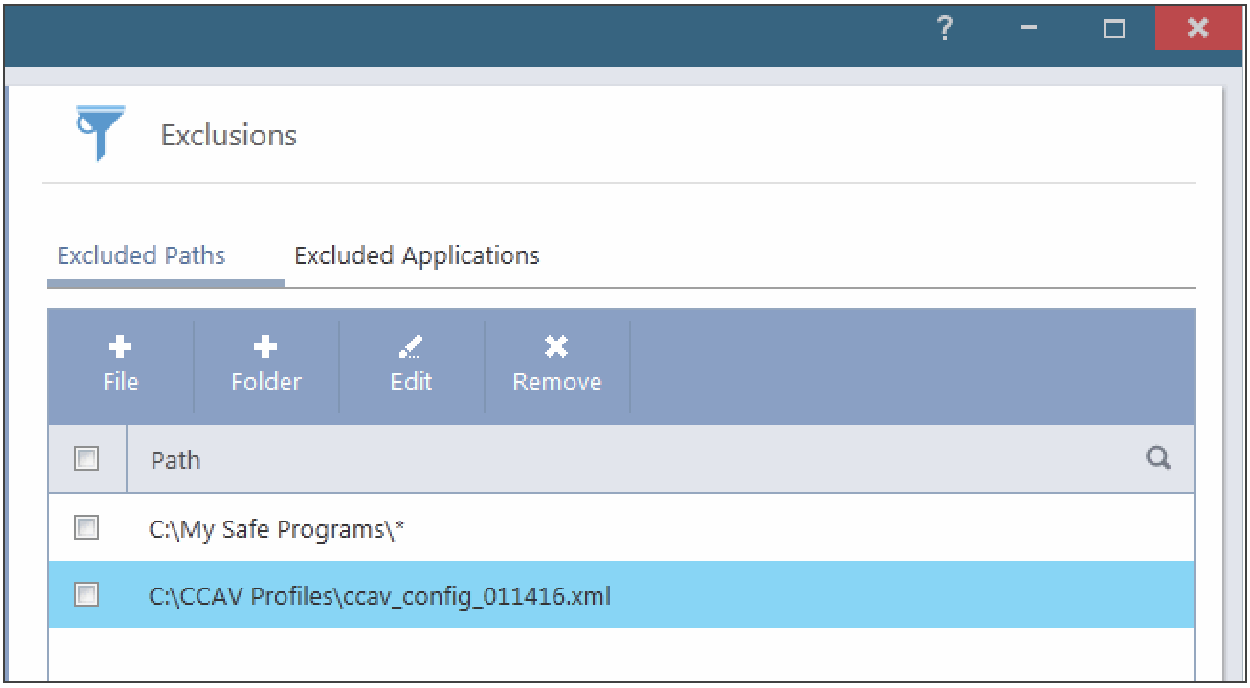
Adding an individual File

You can specify individual files as excluded path.

- To add a file, choose 'File' from the top



- Navigate to the file you want to add to Excluded Paths in the 'Open' dialog and click 'Open'



□ Path

	Path
□	C:\My Safe Programs*
□	C:\CCAV Profiles\ccav_config_011416.xml

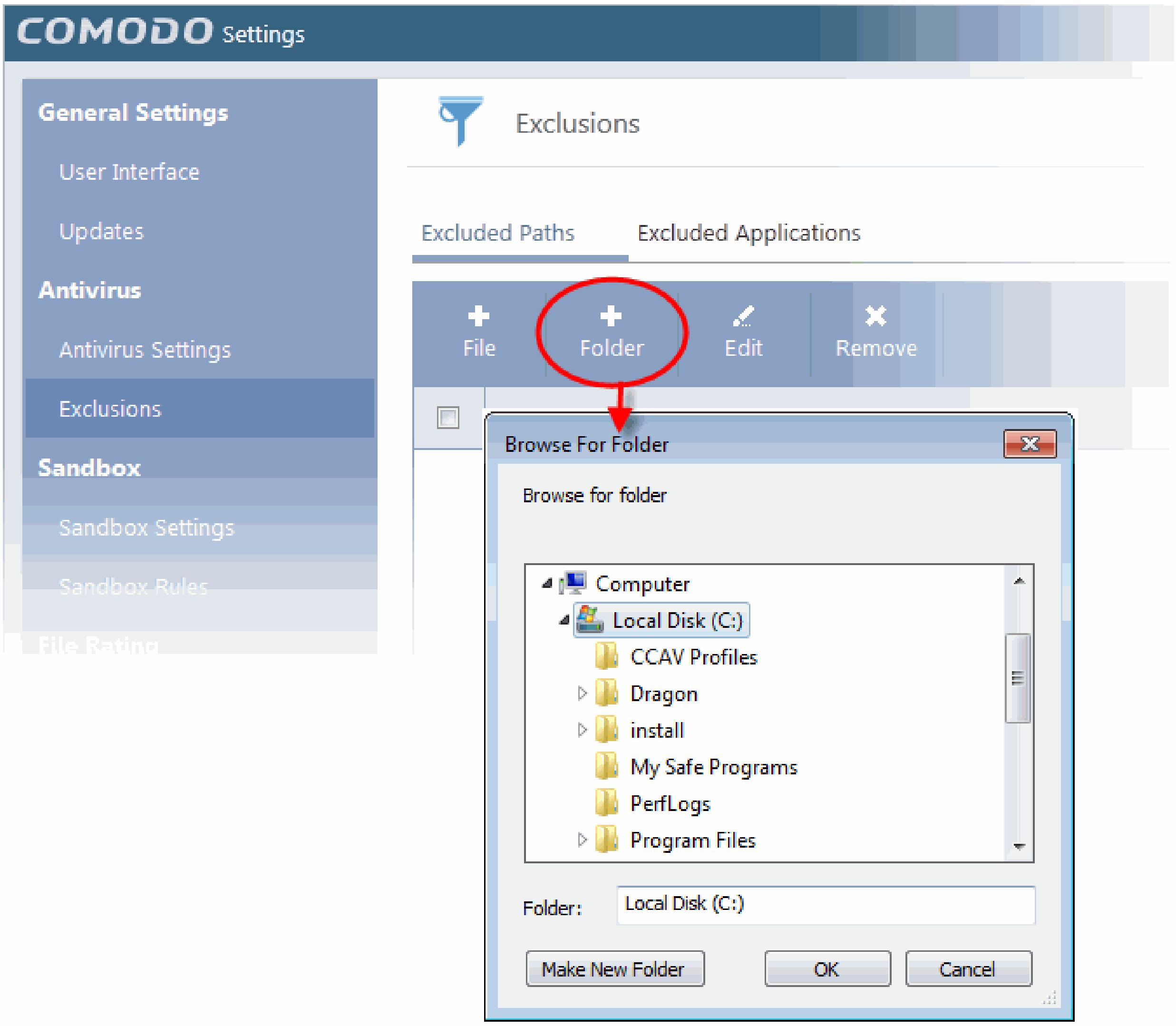
The file will be added to Excluded Paths.

- Repeat the process to add more paths. The items added to the Excluded Paths will be omitted from all types of future antivirus scans.

Adding a Drive Partition/Folder

Choosing 'Folder' allows you to specify drive partitions and/or folders as excluded paths. All the sub-folders and files within the chosen partition/folder will be excluded from all types of antivirus scans.

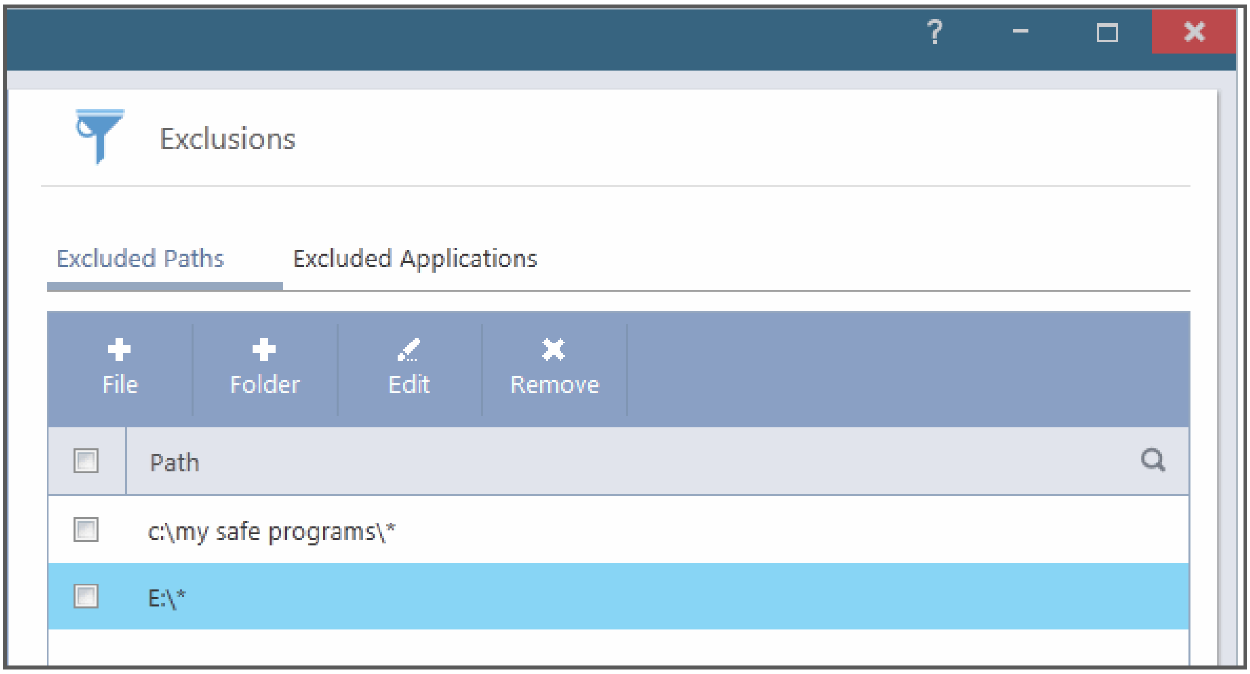
- To add a folder, choose 'Folder' from the top



The 'Browse for folder' dialog will appear.

- Navigate to the drive partition or folder you want to add to excluded paths and click 'OK'.

The drive partition/folder will be added to Excluded Paths.



□	Path
□	c:\my safe programs*
□	E:\*

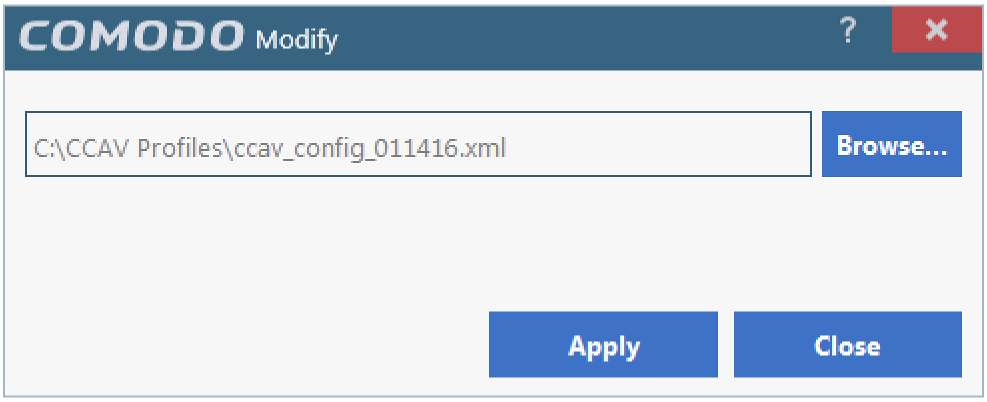
- Repeat process to add more folders. The items added to the 'Excluded Paths' will be omitted from all types of future antivirus scans.

To edit the path of an added item

- Double click on the item

  OR

- Select the item and click 'Edit' from the top.



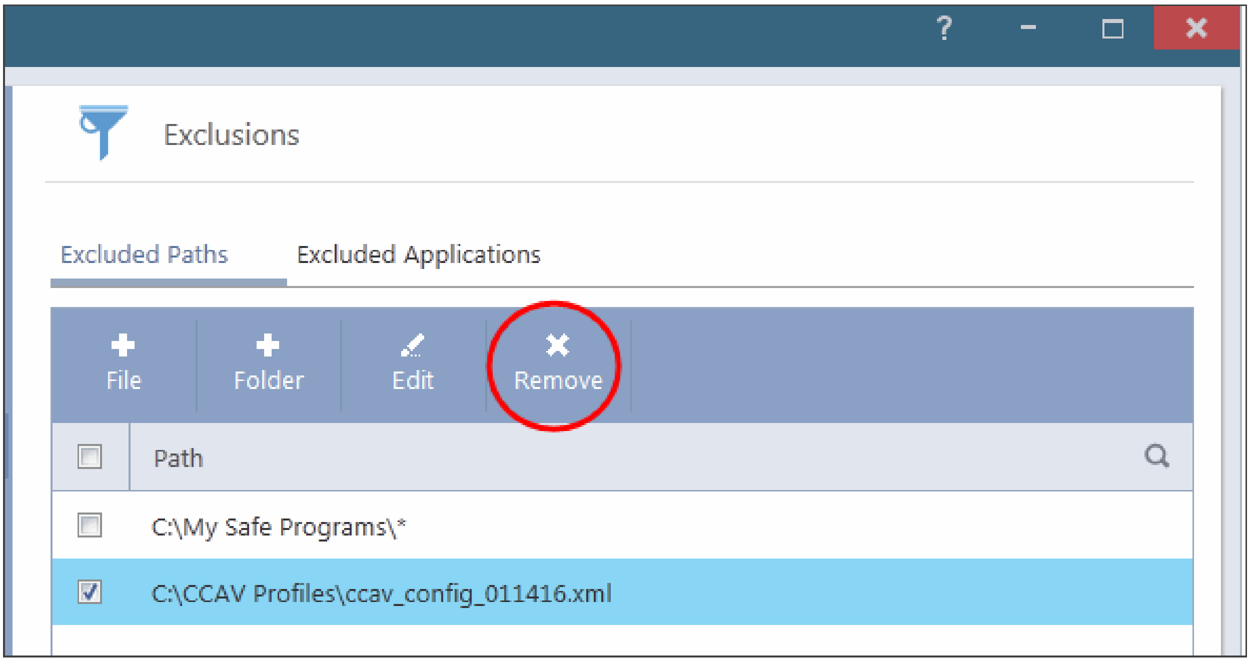
C:\CCAV Profiles\ccav_config_011416.xml

Next, click the 'Browse...' button and navigate to the file to which you want to modify.

- Make the required changes for the file path in the 'Modify' dialog and click 'Apply'.

To remove an item from the Excluded Paths

- Select the item and click 'Remove' from the top.

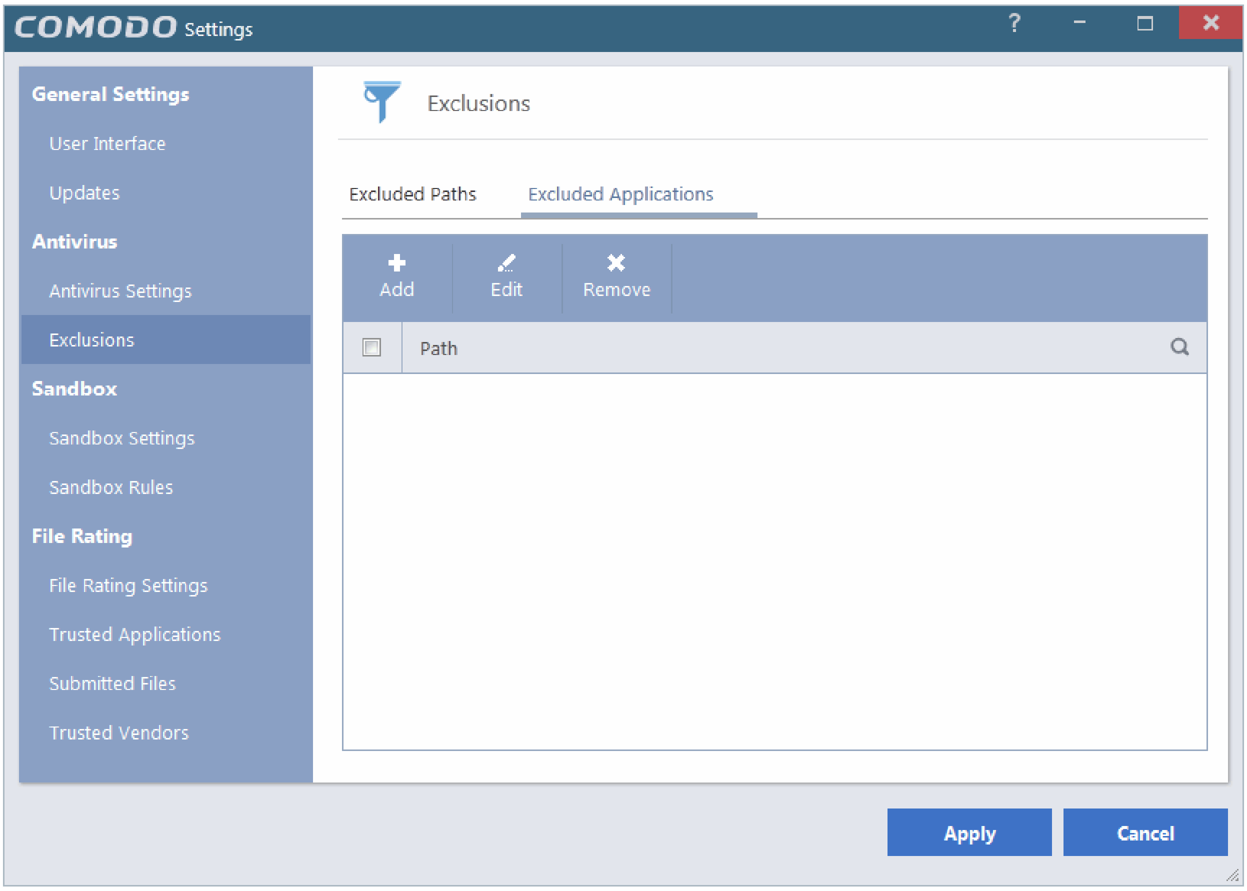


	Path
☐	C:\My Safe Programs*
☑	C:\CCAV Profiles\ccav_config_011416.xml

- Click 'Apply' in the 'Settings' dialog for your settings to take effect.

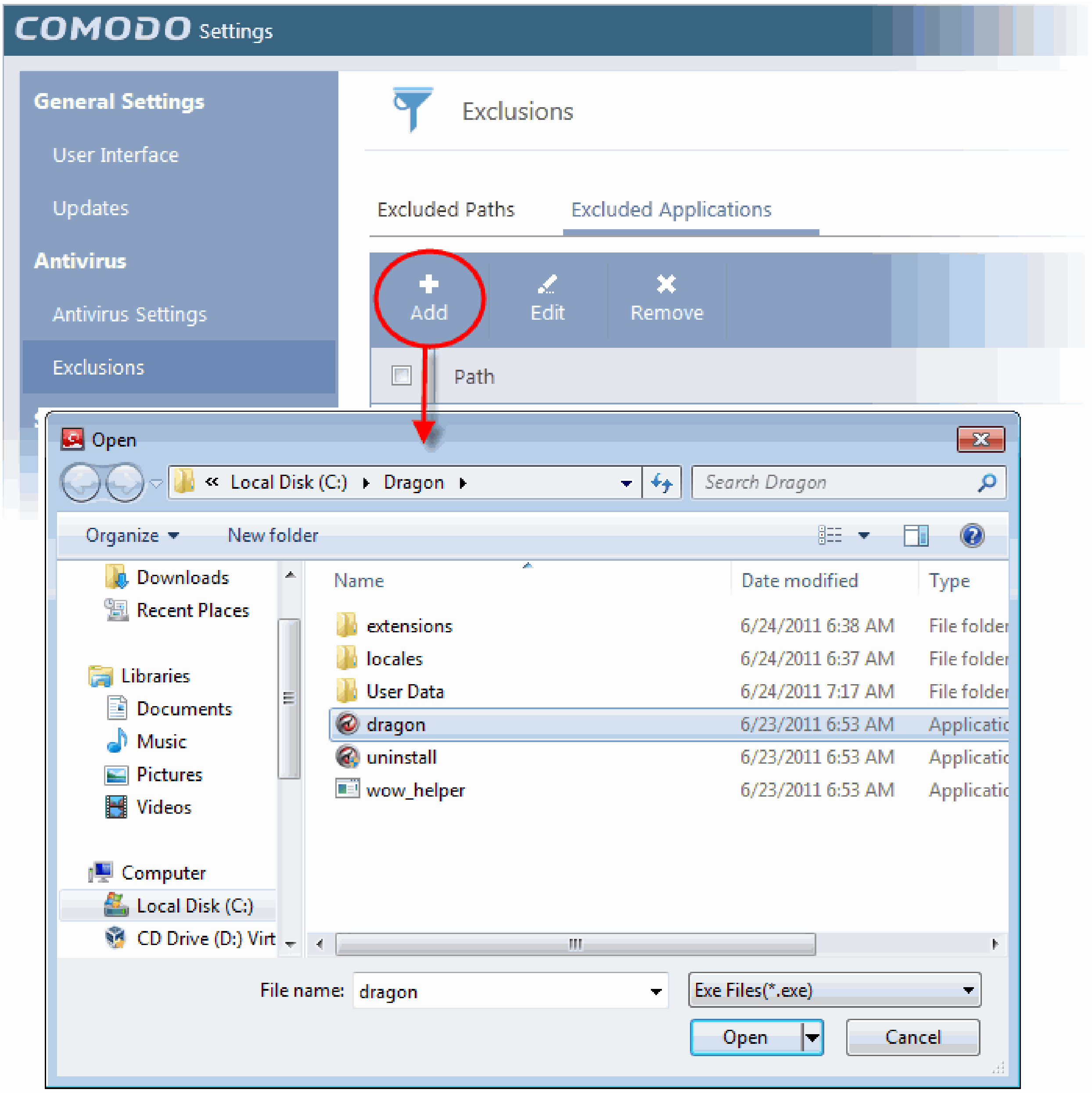
Excluding Programs/Applications from Real-time Scans

The 'Excluded Applications' tab displays the list of applications/files that are excluded only from real-time antivirus scans. The applications/files for which you have selected '**Ignore** ' from the antivirus alert or the **Scan Results** window of various scans are automatically added to this list. You can manually add programs/applications to the 'Excluded Applications' list and can remove items that were added by mistake.



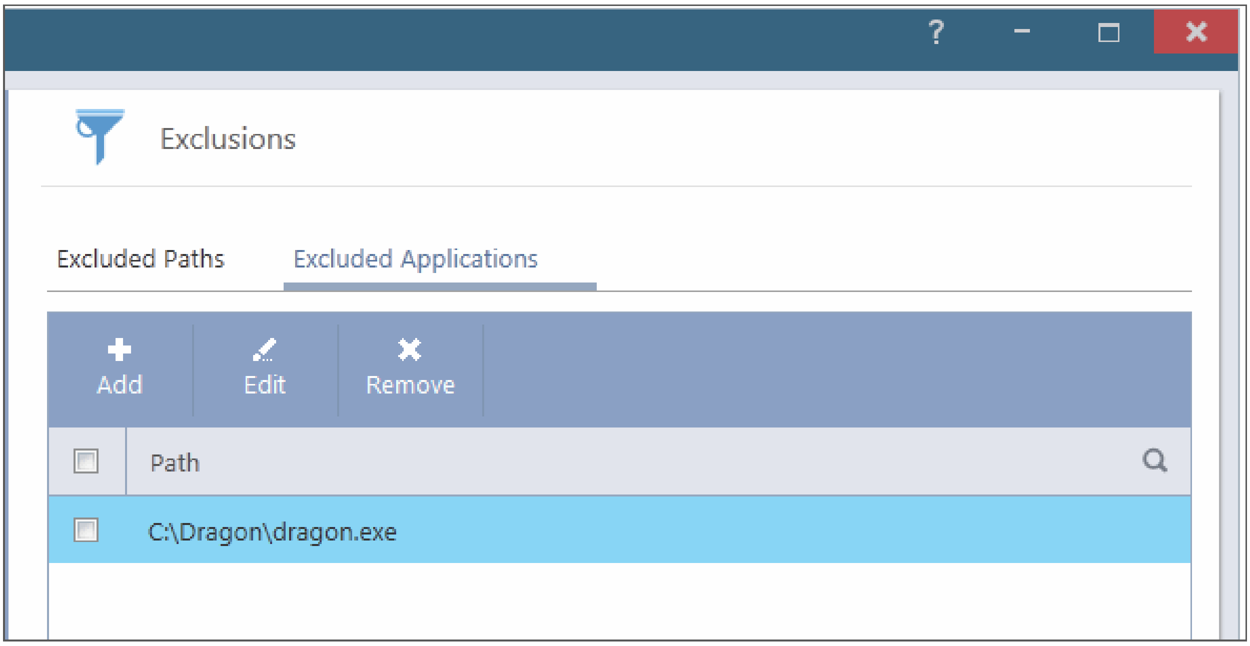
To add an item to Excluded Applications

- Click 'Add' at the top of the 'Excluded Applications' pane.



- Navigate to the file you want to add to Excluded Applications in the 'Open' dialog and click 'Open'.

The file will be added to 'Excluded Applications'.



□ C:\Dragon\dragon.exe

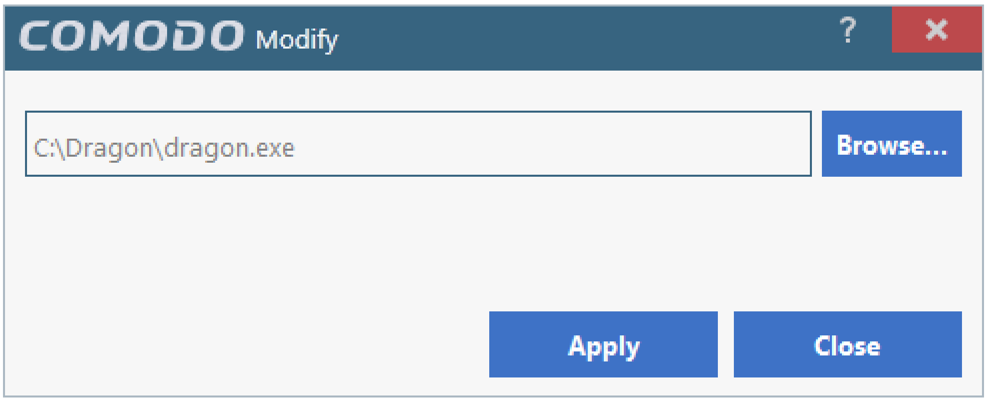
- Repeat process to add more items. The items will be skipped from future real-time scans.

To edit the path of the application added to Excluded Application

- Double click on the item

  OR

- Select the application and click 'Edit' from the top.
- Make the required changes for the file path in the 'Modify' dialog.

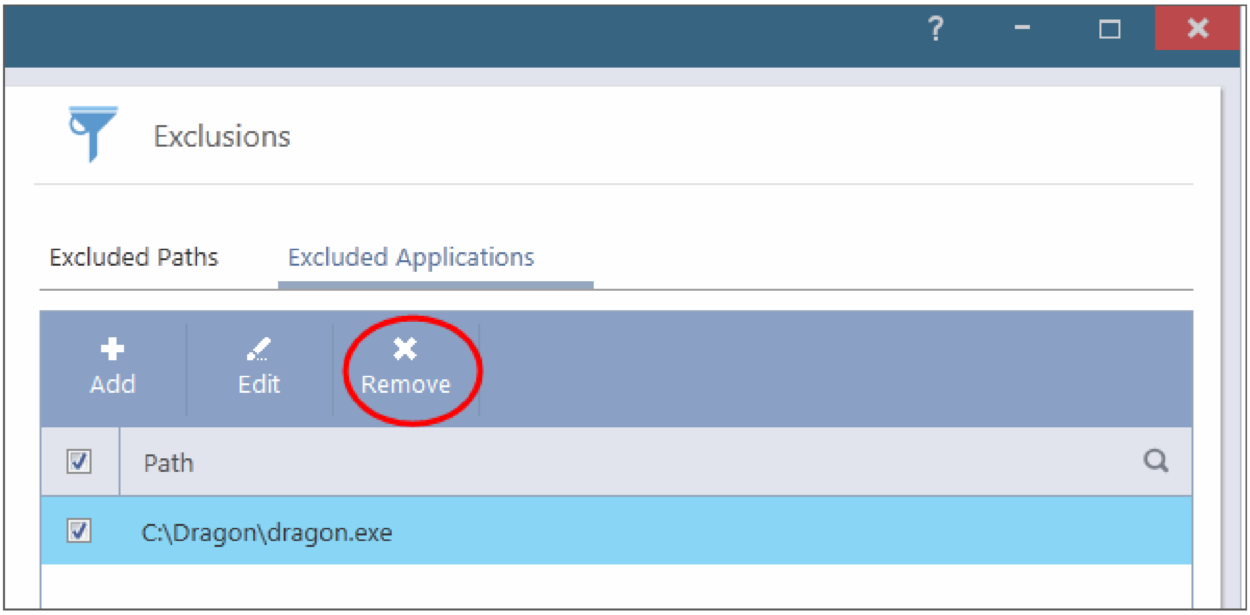


C:\Dragon\dragon.exe

Next, click the 'Browse...' button and navigate to the application to which you want to modify.

To remove an item from the Excluded Applications

- Select the item and click 'Remove' from the top.

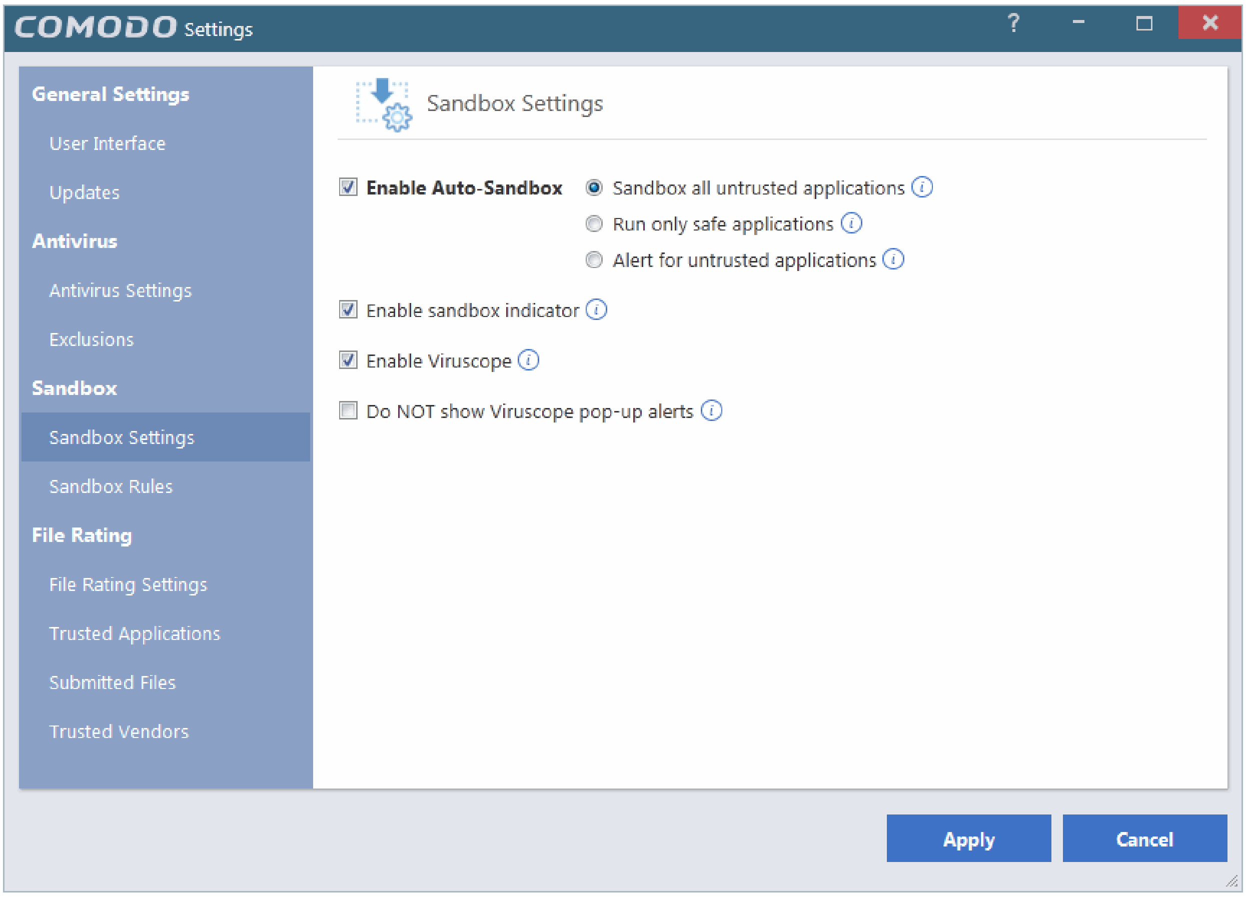


☑ C:\Dragon\dragon.exe

- Click 'Apply' in the 'Settings' dialog for your settings to take effect.

6.3. Sandbox Settings

If CCAV encounters a file that has a trust status of 'Unknown' then you have the option to automatically run that file in the sandbox. Files running in the sandbox are isolated from the rest of your computer and your data to prevent them causing damage. The sandbox configuration section allows you define how unknown files should be handled and to configure sandbox rules.



☑ **Enable Auto-Sandbox** ● Sandbox all untrusted applications
○ Run only safe applications
○ Alert for untrusted applications

☑ Enable sandbox indicator

☑ Enable Viruscope

□ Do NOT show Viruscope pop-up alerts

Refer to the following sections for more details:

- **Sandbox Settings**
- **Sandbox Rules**

6.3.1. Sandbox Settings

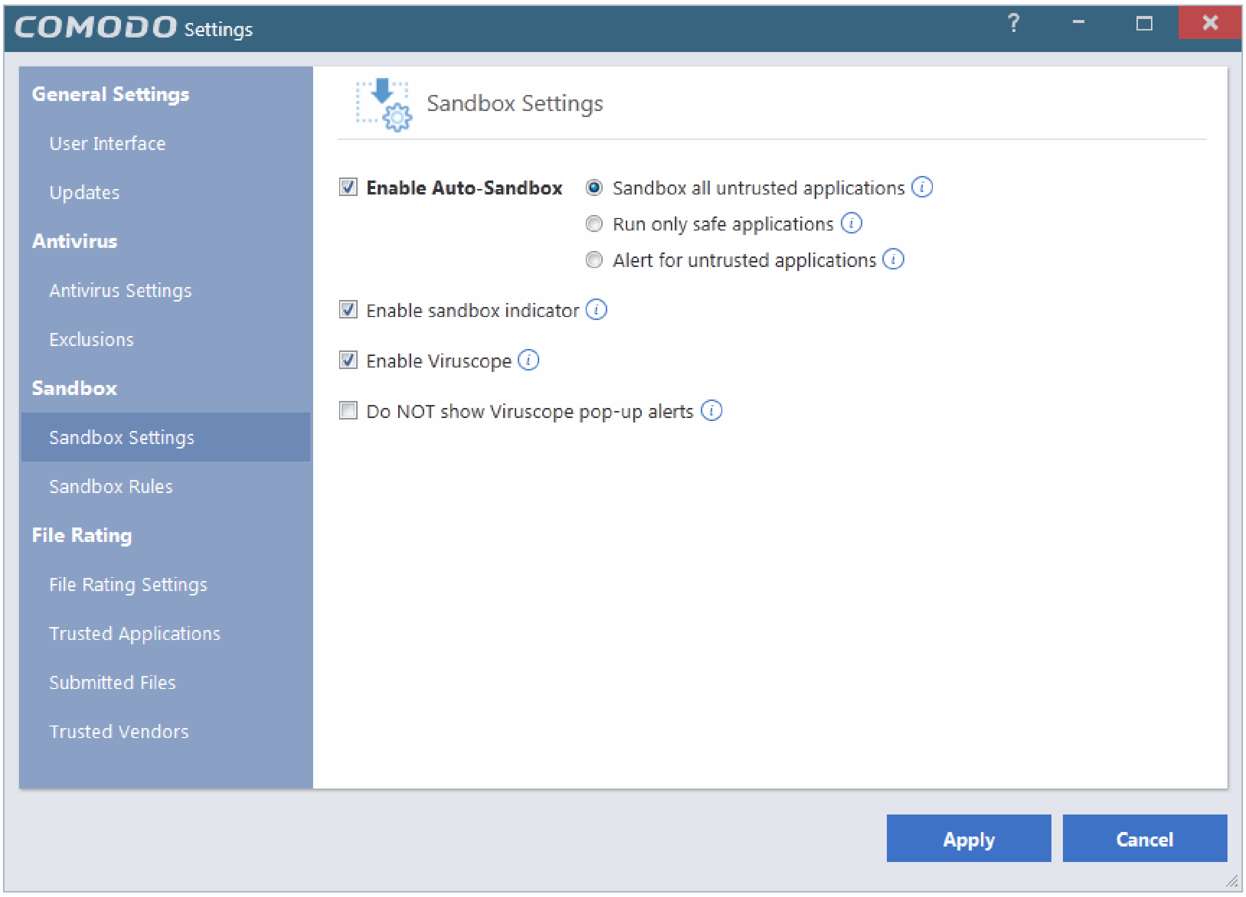
The sandbox settings area allows you to configure your overall sandbox policy.

To open sandbox settings

- Click the Sandbox link on the CCAV home screen

  OR

- Click the 'Settings' button on the home screen then choose 'Sandbox Settings' under 'Sandbox'



Sandbox Settings

☑ **Enable Auto-Sandbox** ● Sandbox all untrusted applications ○ Run only safe applications ○ Alert for untrusted applications

☑ Enable sandbox indicator

☑ Enable Viruscope

□ Do NOT show Viruscope pop-up alerts

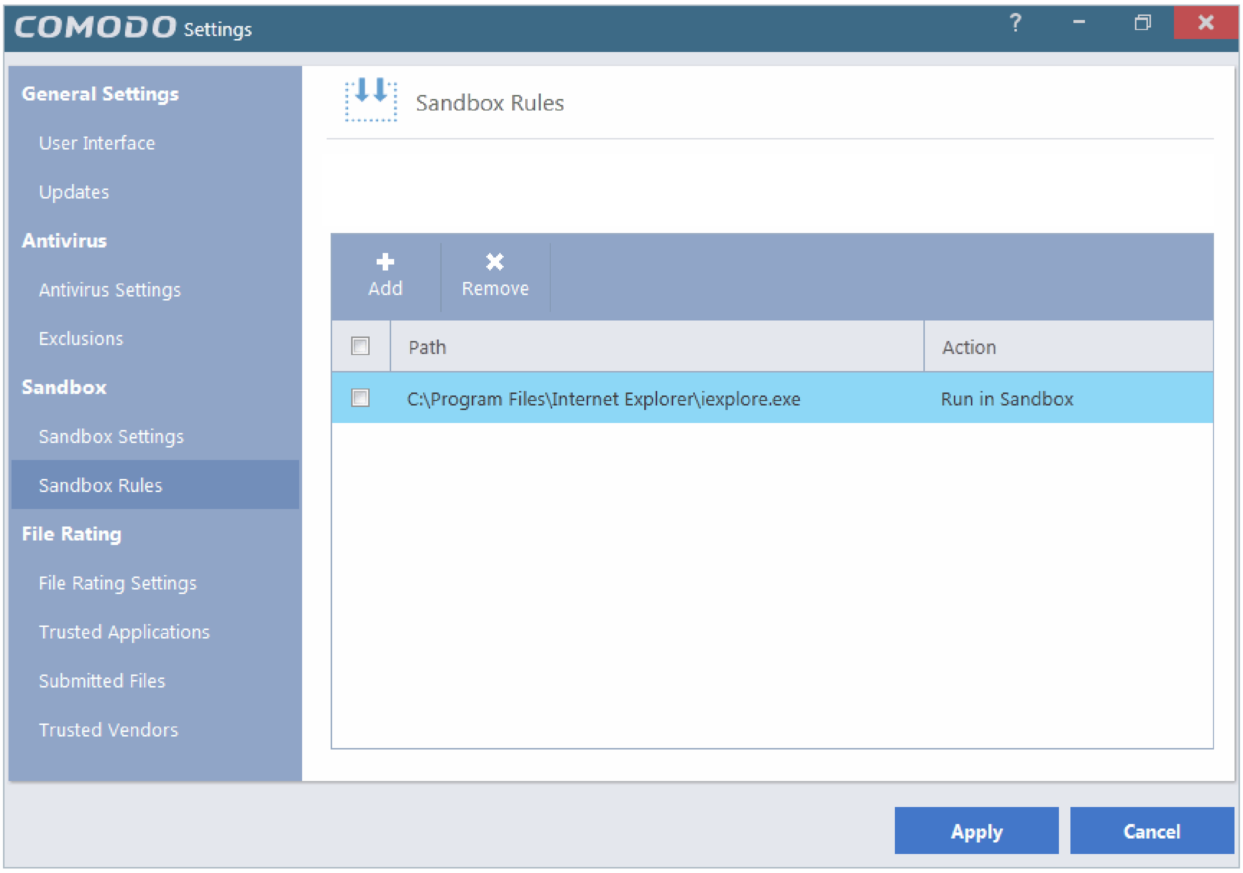
- **Enable Auto-Sandbox -** Switch automatic sandboxing on or off. If you disable the sandbox, then any sandbox rules that you have created will be disregarded. If you enable the sandbox, you have the following options:
  - Sandbox all untrusted files - CCAV will automatically run 'unknown' files and applications in the sandbox. A file can have one of three trust statuses – Trusted, Untrusted or Unknown. 'Trusted' files are those that are either on the Comodo white-list of known-good applications, or have been trusted by the user. Trusted files and are allowed to run outside the sandbox. 'Untrusted' files are usually viruses and other forms of malware and will be quarantined by the antivirus scanner. 'Unknown' files are those which are neither 'Trusted' nor 'Untrusted'. As their precise intentions are not yet known, we run these applications in the sandbox. If they later transpire to be malicious, they will not have been able to cause damage to your computer or data because they were sandboxed.
  - Run only safe applications - Only applications from **Trusted Vendors** or those in your list of **Trusted Applications** will be allowed to run on your computer. All other applications will be blocked.

  - Alert for untrusted files - Instead of automatically sandboxing unknown files, CCAV will instead show you an alert and offer you the choice of sandboxing the application or running it normally.

- **Enable sandbox indicator -** CCAV will display a green border around an application if it is running in the sandbox. Disable this setting if you do not want to see this border.
- **Enable Viruscope** - Viruscope monitors the activities of processes running on your computer and alerts you if they take actions that could potentially threaten your privacy and/or security. Viruscope alerts give you the opportunity to quarantine the process & reverse its changes or to let the process continue. Viruscope forms another layer of security on top of the core antivirus protection and helps CCAV to control and evaluate the behavior of sandboxed applications.
- **Do not show Viruscope pop-up alerts** - Allows you to configure whether or not CCAV should show an alert if Viruscope detects a suspicious activity. Choosing 'Do not show' will minimize disturbances but at some loss of user awareness. If you choose not to show alerts then detected threats are automatically quarantined and their activities are reversed.
- Click 'Apply' for your settings to take effect.

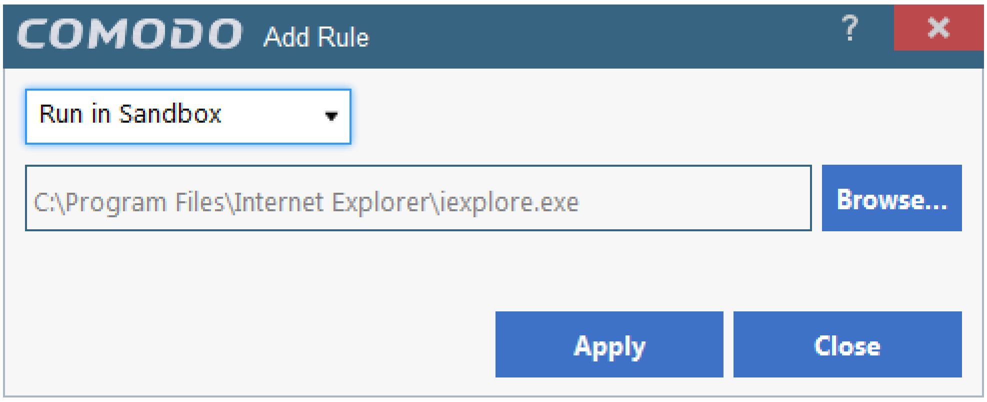
6.3.2. Sandbox Rules

The 'Sandbox Rules' interface allows you to add custom sandboxing rules for particular applications. This can be useful, for example, for creating exceptions to your overall sandbox policy. To open the rules interface, click the 'Sandbox Rules' tab in the lower half on the sandbox settings interface:



□	Path	Action
□	C:\Program Files\Internet Explorer\iexplore.exe	Run in Sandbox

- Existing rules will be listed in the lower pane, along with the application path and the sandbox action associated with it.
- To remove a rule, select the check-box next to the rule name and click 'Remove'.
- Double-click a rule to edit it.
- To add a new rule for an application, first click the 'Add' button to open the rule configuration dialog:



C:\Program Files\Internet Explorer\iexplore.exe

Next, choose the type of rule you wish to apply from the drop-down menu. The choices are:

- **Run in Sandbox** – The application you choose will always run in the sandbox. This is useful, for example, if you wish to sandbox an application from a trusted vendor. Similarly, you may wish to sandbox your internet browser so that you can surf from within a security hardened environment.
- **Run Outside Sandbox** – The application you choose will always run outside of the sandbox. This is useful, for example, if you wish to create an exception for an application that CCAV considers untrusted. This situation can occur for beta software, unsigned software or applications from relatively new vendors.
- **Block** – The application you choose will be prevented from running by CCAV.

Next, click the 'Browse...' button and navigate to the application or file to which you want to apply the rule. The example above shows a rule for 'Internet Explorer' browser. Click 'Apply' in the dialog then 'Apply' in the settings interface to implement your rule.

Note 1. You must enable the sandbox in 'Sandbox Settings' if you want to implement rules. If you disable the sandbox, then rules will be disregarded anyway.

Note 2. If the sandbox is enabled, then CCAV prioritizes rules as follows:

1. Sandbox rules for a particular application have top priority.
2. Sandbox settings have 2nd priority (the radio buttons next to 'Enable Auto-Sandbox')

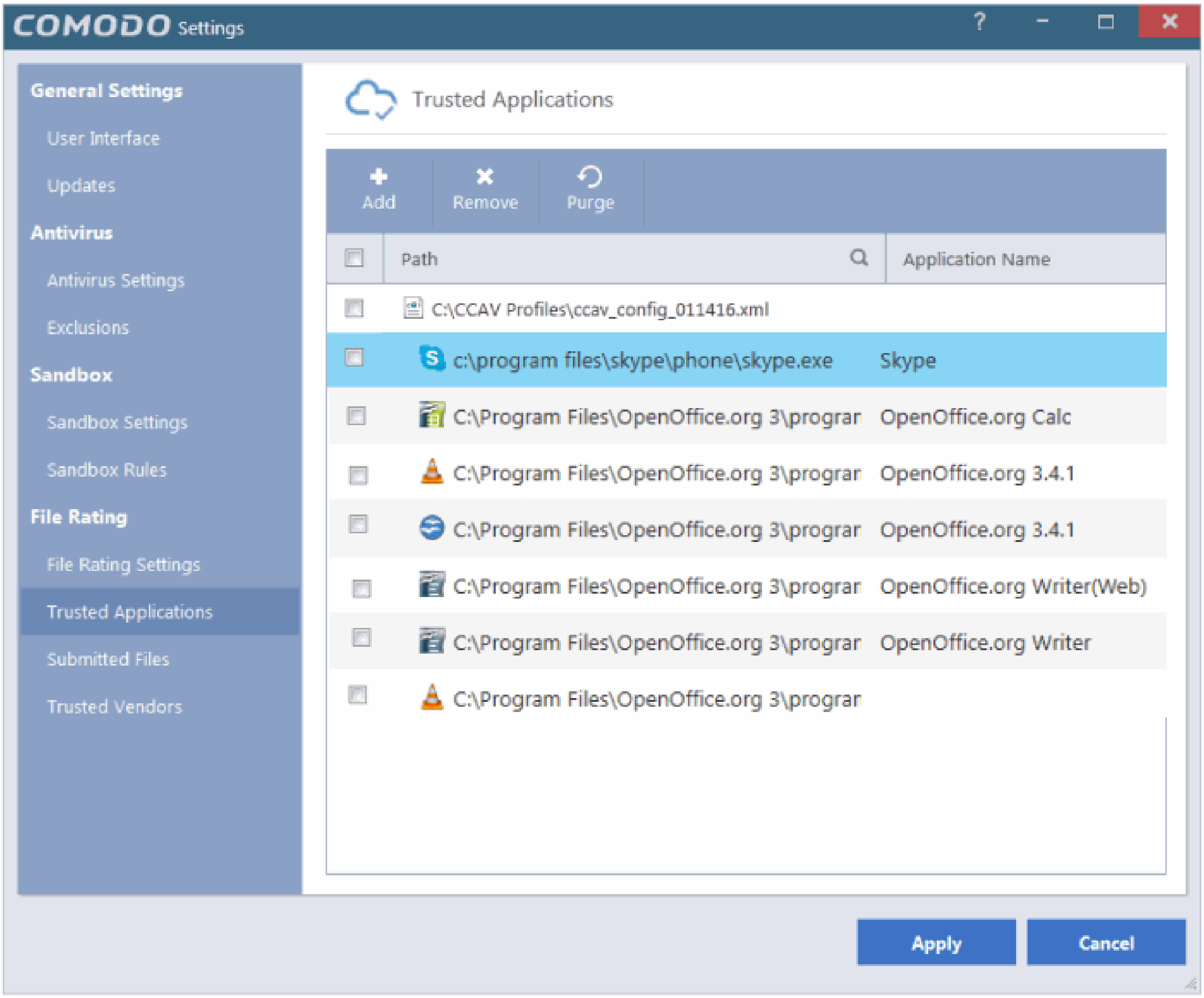
6.4. File Rating Settings

The CCAV file rating system is a cloud-based file look-up service (FLS) that attempts to ascertain the reputation of files on your computer by consulting a global database. Whenever a file is first accessed, CCAV will check the file against our master whitelist and blacklists and will award it trusted status if:

- The application/file is included in the local Trusted Applications list
- The application is from a vendor included in the Trusted Vendors list
- The application is included in the extensive and constantly updated Comodo safelist

Trusted applications are excluded from monitoring by Auto-Sandbox - reducing hardware and software resource consumption.

The 'File Rating' area allows you to view and manage the list of Trusted Applications and Trusted Vendors and to view the files submitted to Comodo for analysis.



□	Path	Application Name
□	C:\CCAV Profiles\ccav_config_011416.xml	
□	c:\program files\skype\phone\skype.exe	Skype
□	C:\Program Files\OpenOffice.org 3\prograr	OpenOffice.org Calc
□	C:\Program Files\OpenOffice.org 3\prograr	OpenOffice.org 3.4.1
□	C:\Program Files\OpenOffice.org 3\prograr	OpenOffice.org 3.4.1
□	C:\Program Files\OpenOffice.org 3\prograr	OpenOffice.org Writer(Web)
□	C:\Program Files\OpenOffice.org 3\prograr	OpenOffice.org Writer
□	C:\Program Files\OpenOffice.org 3\prograr	

Click the following links to jump to the section you need help with:

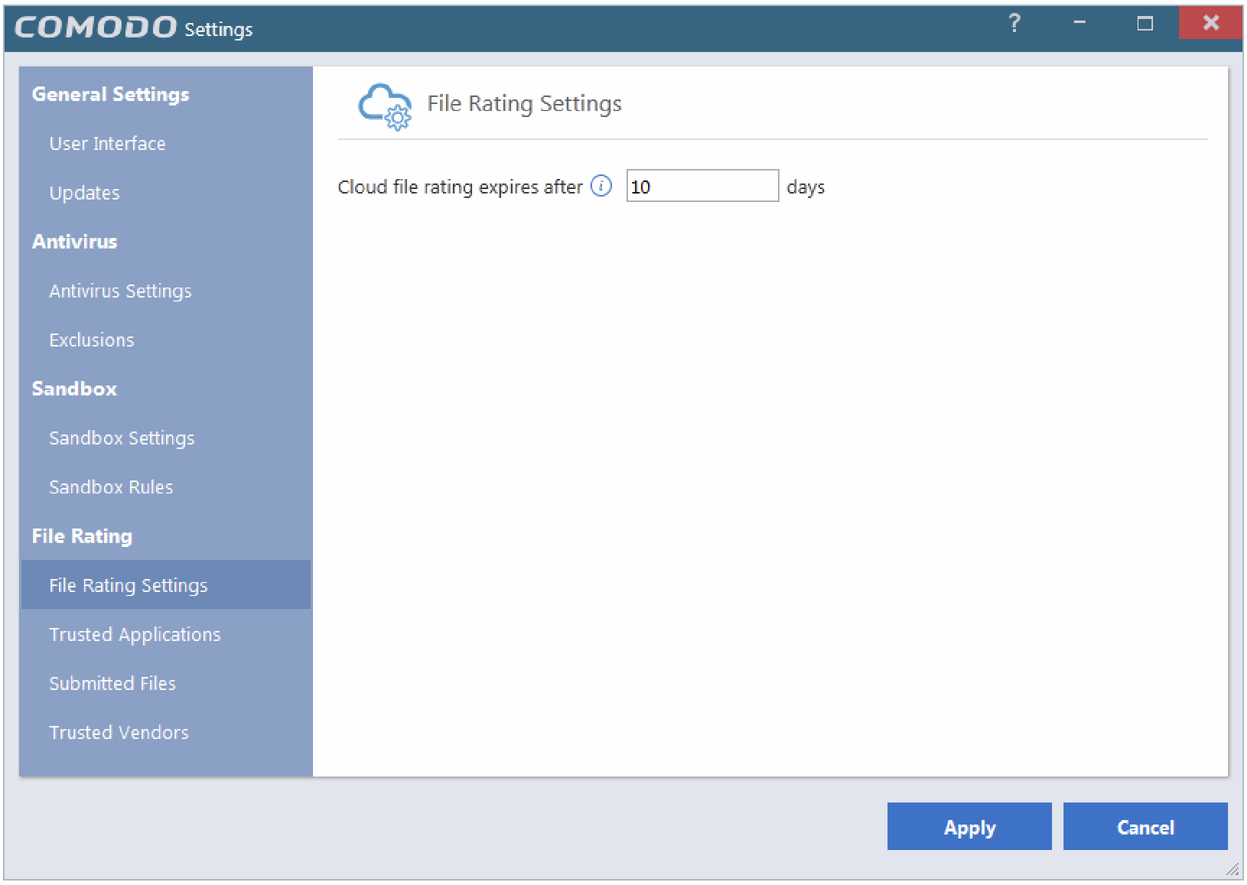
- **File Rating Settings** - Configure settings that govern the overall behavior of file rating.
- **Trusted Applications** – Add and manage applications to local Trusted Applications list.
- **Submitted Files** - View any files already submitted to Comodo for analysis.
- **Trusted Vendors** - View the list of trusted software vendors and manually add vendors.

6.4.1. File Rating Settings

The 'File Ratings Settings' area allows you to configure the period for which file ratings obtained from the Cloud server are valid.

To open the 'File Rating Settings' interface

- Click 'Settings' from the top left of the CCAV home screen to open the 'Settings' interface
- Choose 'File Rating Settings' under 'File Rating' from the left, in the 'Settings' interface



Cloud file rating expires after 10 days

- **Cloud file rating expires after NN days** – In order to determine its run-time privileges, CCAV consults a file's rating whenever you access the file. This rating is obtained from Comodo's cloud-based file ratings server and is then cached locally to speed-up subsequent executions. This settings allows you to specify the number of days for which a cached rating should be considered valid ***(Default = 10 days)***. When this period has elapsed, CCAV obtains updated ratings from the cloud server.

- Click 'Apply' for your settings to take effect.

6.4.2. Trusted Applications

Files with 'Trusted' rating are automatically allowed to run outside the sandbox. Using a combination of online lookups and locally stored information, files are identified as trusted in the following ways:

- The application is from a vendor included in the Trusted Software Vendors list;
- The application is included in the extensive and constantly updated Comodo safelist.
- User Rating – You can provide 'Trusted' status to your executables by adding it to the Trusted Applications list.

For the files assigned with 'Trusted' status by the user, CCAV generates a hash or a digest of the file using a pre-defined algorithm and saves in its database. On access to any file, its digest is created instantly and compared against the list of stored hashes to decide on whether the file has 'Trusted' status. By this way, even if the file name is changed later, it will retain its 'Trusted' status as the hash remains same.

By granting 'Trusted' status to executables you can reduce the amount of alerts that Sandbox generates whilst maintaining a high level of security. This is particularly useful for developers that are creating new applications that, by their nature, are as yet unknown to the Comodo safe list.

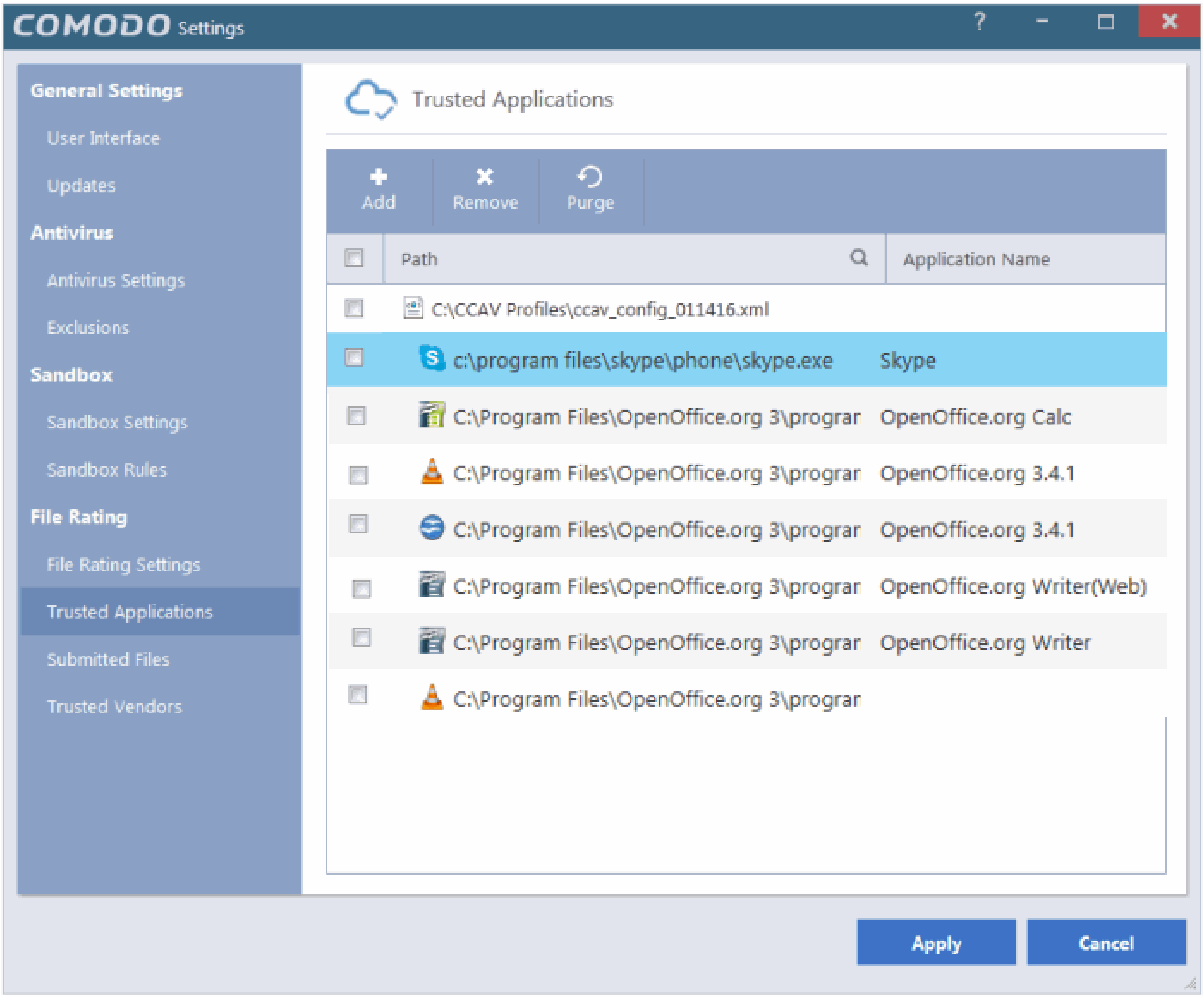
Creating your own list of 'Trusted Files' allows you to define a personal safe list of files to complement the default Comodo safe list.

The Trusted Applications interface allows you to add and manage files to 'Trusted Applications' list.

To open the 'Trusted Applications' interface

- Click 'Settings' from the top left of the CCAV home screen to open the 'Settings' interface

- Choose 'Trusted Applications' under 'File Rating' from the left, in the 'Settings' interface



□	Path	Application Name
□	C:\CCAV Profiles\ccav_config_011416.xml	
□	c:\program files\skype\phone\skype.exe	Skype
□	C:\Program Files\OpenOffice.org 3\prograr	OpenOffice.org Calc
□	C:\Program Files\OpenOffice.org 3\prograr	OpenOffice.org 3.4.1
□	C:\Program Files\OpenOffice.org 3\prograr	OpenOffice.org 3.4.1
□	C:\Program Files\OpenOffice.org 3\prograr	OpenOffice.org Writer(Web)
□	C:\Program Files\OpenOffice.org 3\prograr	OpenOffice.org Writer
□	C:\Program Files\OpenOffice.org 3\prograr	

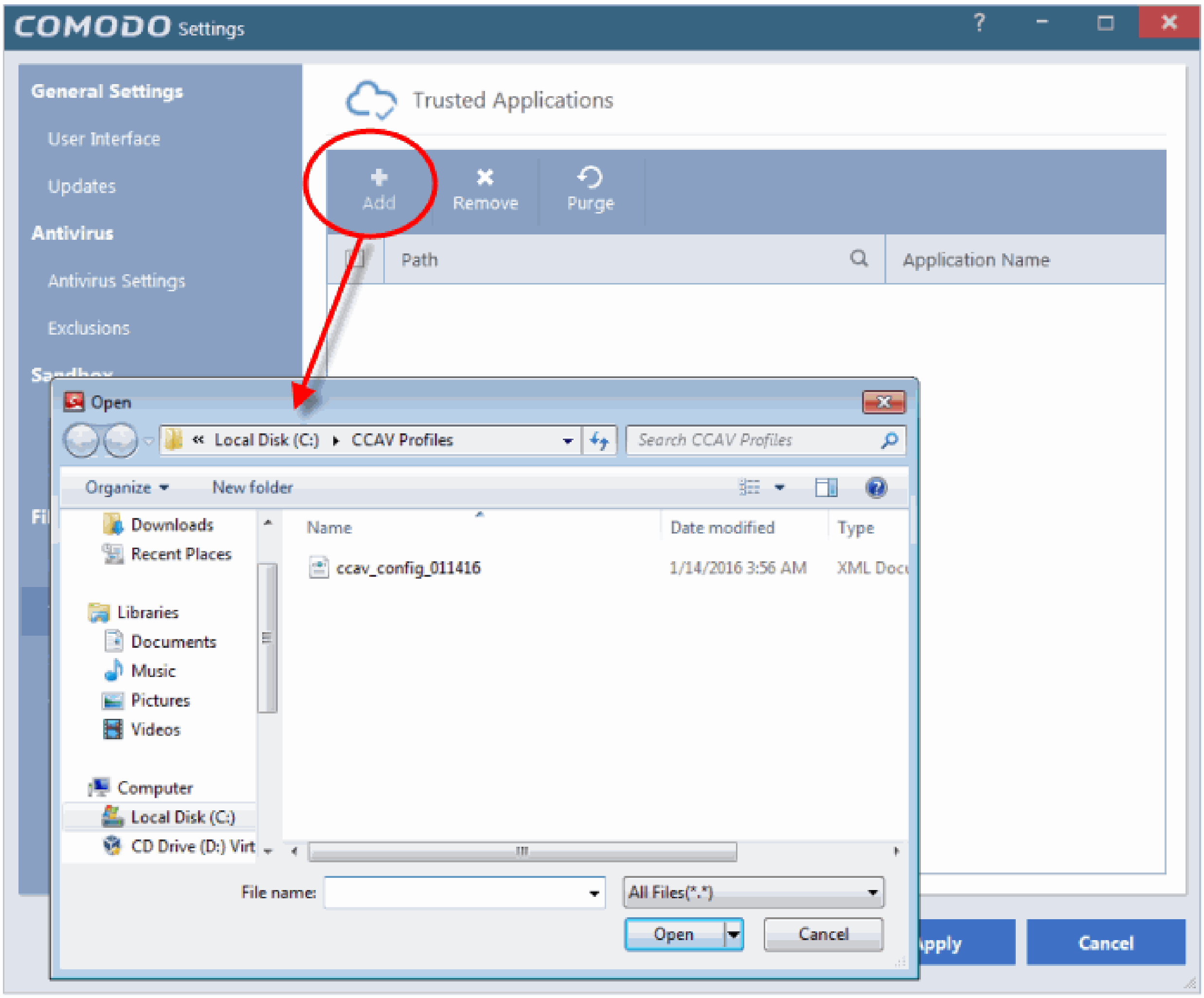
The interface displays a list of files added as 'Trusted Applications' with the following details:

- **Path** – The installation path of the application/executable file
- **Application Name** – The name of the application/executable file

You can search for specific application(s) from the list by clicking the search icon 🔍 in the table header and entering the name of the application in part or full.

To add an item to the Trusted Applications list

- Click the 'Add' button at the top of the 'Trusted Applications' interface



- Navigate to the file to be added as Trusted Application and click 'Open'.

The item will be added to the list and rated as Trusted.

- Click 'Apply' for your changes to take effect

To remove item(s) from the Trusted Applications list

- Select the items to be removed from the Trusted Applications list interface and click the 'Remove' button from the top.
- Click 'Apply' for your changes to take effect

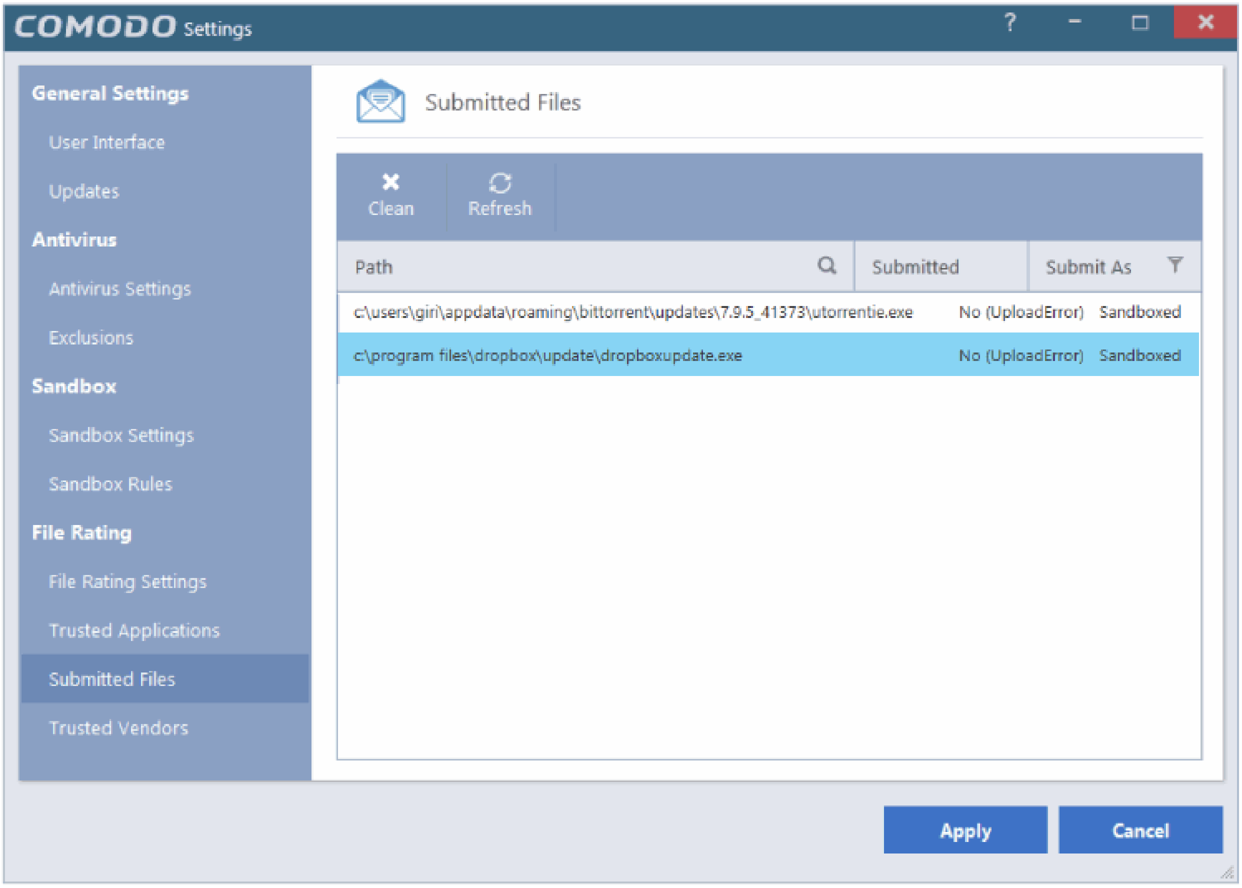
6.4.3. Submitted Files

Files identified as 'unknown' or 'malicious' are queued for submission to Comodo for Analysis. You can also submit files you suspect of being 'false positives' (those files that you feel CCAV has incorrectly identified as malware). Once uploaded, the files will undergo a series of automated tests to establish whether or not they are trustworthy. After manual classification by Comodo Labs, they will be added to global white or black list accordingly.

The 'Submitted Files' area in the 'Settings' interface allows you to view the list of files you have submitted so far for analysis to Comodo.

To open the 'Submitted Files' interface

- Click 'Settings' from the top left of the CCAV home screen to open the 'Settings' interface
- Choose 'Submitted Files' under 'File Rating' from the left, in the 'Settings' interface



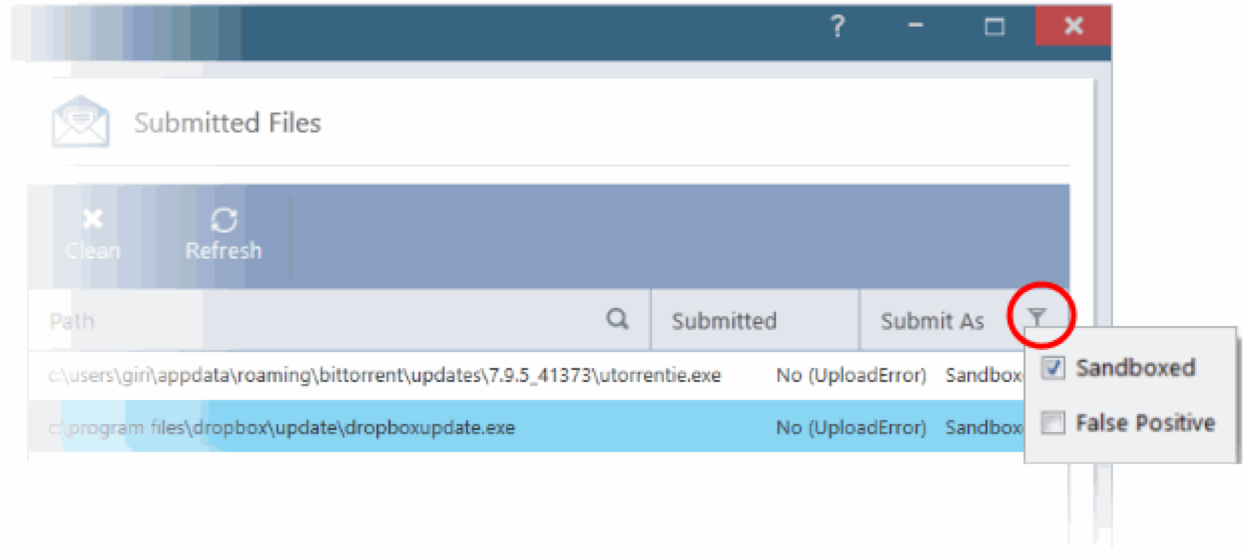
Path	Submitted	Submit As
c:\users\giri\appdata\roaming\bittorrent\updates\7.9.5_41373\utorrentie.exe	No (UploadError)	Sandboxed
c:\program files\dropbox\update\dropboxupdate.exe	No (UploadError)	Sandboxed

The list of submitted file will be displayed with their details:

- **Path** – The installation path of the application/executable file
- **Submitted** – The precise date and time at which the file wwas submitted
- **Submitted As** - Indicates whether the file was submitted as an auto-sandboxed file or as a false positive, from the result of Antivirus scan.

You can search for specific application(s) from the list by clicking the search icon 🔍 in the table header and entering the name of the application in part or full.

You can filter the results to show only the items submitted as Sandboxed or False Positives by clicking the funnel icon beside the Submitted As column header and choosing the filter criteria.



Path	Submitted	Submit As
c:\users\giri\appdata\roaming\bittorrent\updates\7.9.5_41373\utorrentie.exe	No (UploadError)	Sandbox
c:\program files\dropbox\update\dropboxupdate.exe	No (UploadError)	Sandbox

- To remove all the items from the list, click 'Clean'
- To refresh the list to view the latest items, click 'Refresh'

6.4.4. Trusted Vendors

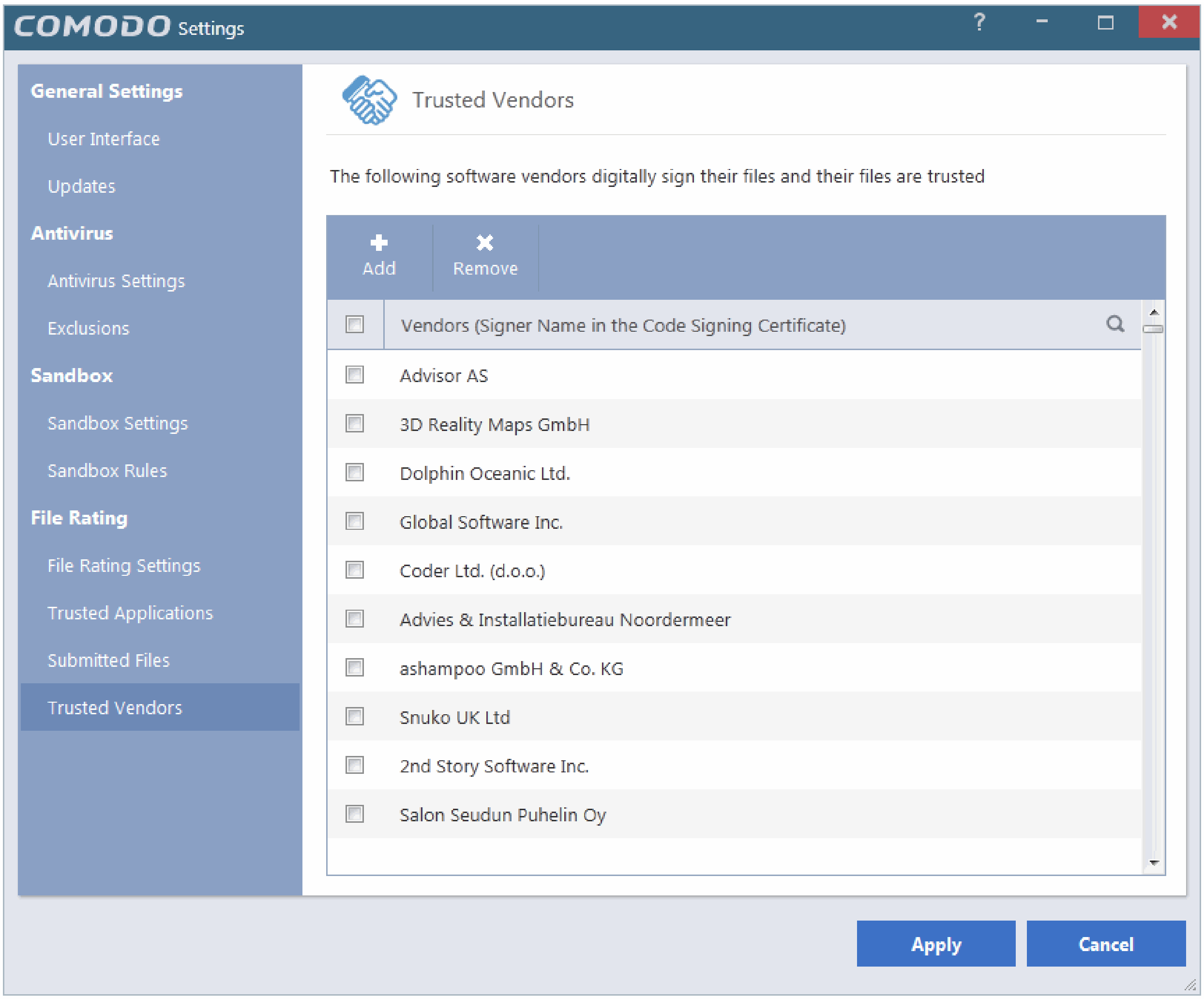
In Comodo Cloud Antivirus, there are three basic methods in which an application can be treated as safe. Either it has to be part of the Comodo 'Safe List' (of known-safe software), or the application is signed by one of the vendors in the 'Trusted Software Vendor List', or the file is added to the list of Trusted Applications by the user.

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 with CCAV. Details about this can be found at the foot of this page.

The 'Trusted Vendors' area in the settings interface allows you to view the list of Trusted Vendors added to CCAV by default and allows you to add or remove Trusted Vendors.

To open the 'Trusted Vendors' interface

- Click 'Settings' from the top left of the CCAV home screen to open the 'Settings' interface
- Choose 'Trusted Vendors' under 'File Rating' from the left, in the 'Settings' interface



Trusted Vendors

The following software vendors digitally sign their files and their files are trusted

□	Vendors (Signer Name in the Code Signing Certificate)
□	Advisor AS
□	3D Reality Maps GmbH
□	Dolphin Oceanic Ltd.
□	Global Software Inc.
□	Coder Ltd. (d.o.o.)
□	Advies & Installatiebureau Noordermeer
□	ashampoo GmbH & Co. KG
□	Snuko UK Ltd
□	2nd Story Software Inc.
□	Salon Seudun Puhelin Oy

You can search for specific vendor(s) from the list by clicking the search icon 🔍 in the table header and entering the name of the vendor in part or full.

- **Click here to read background information on digitally signing software**
- **Click here to learn how to Add / Define a user-trusted vendor**
- **Software Vendors - click here to find out about getting your software added to the list**

Background

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

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

ii. **Content Integrity**: That the software they are downloading and are about to install ***has not be modified or corrupted since it was signed.***

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

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

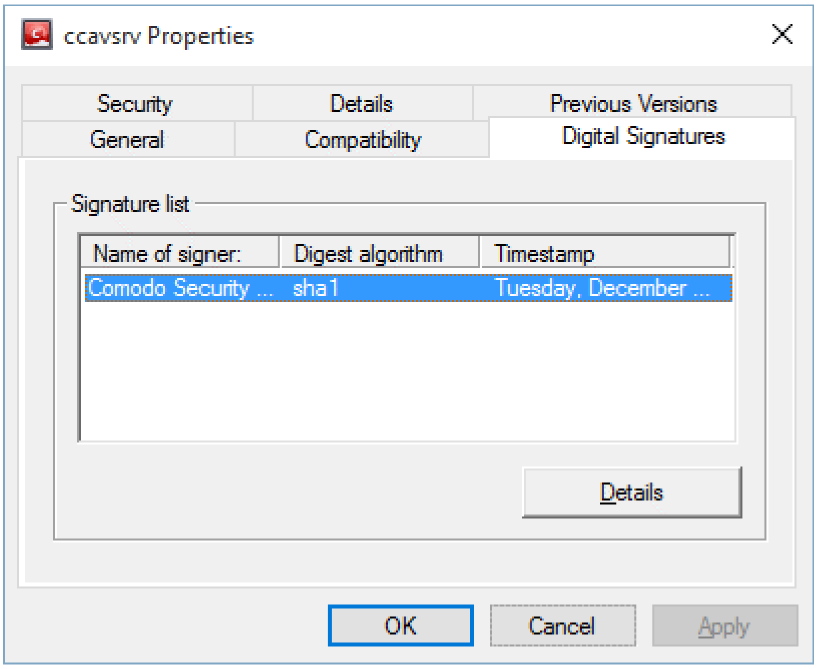
However, companies can't just 'sign' their own software and expect it to be trusted. This is why each code signing certificate is counter-signed by an organization called a 'Trusted Certificate Authority'. 'Comodo CA Limited' and 'Verisign' are two examples of a Trusted CA's and are authorized to counter-sign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

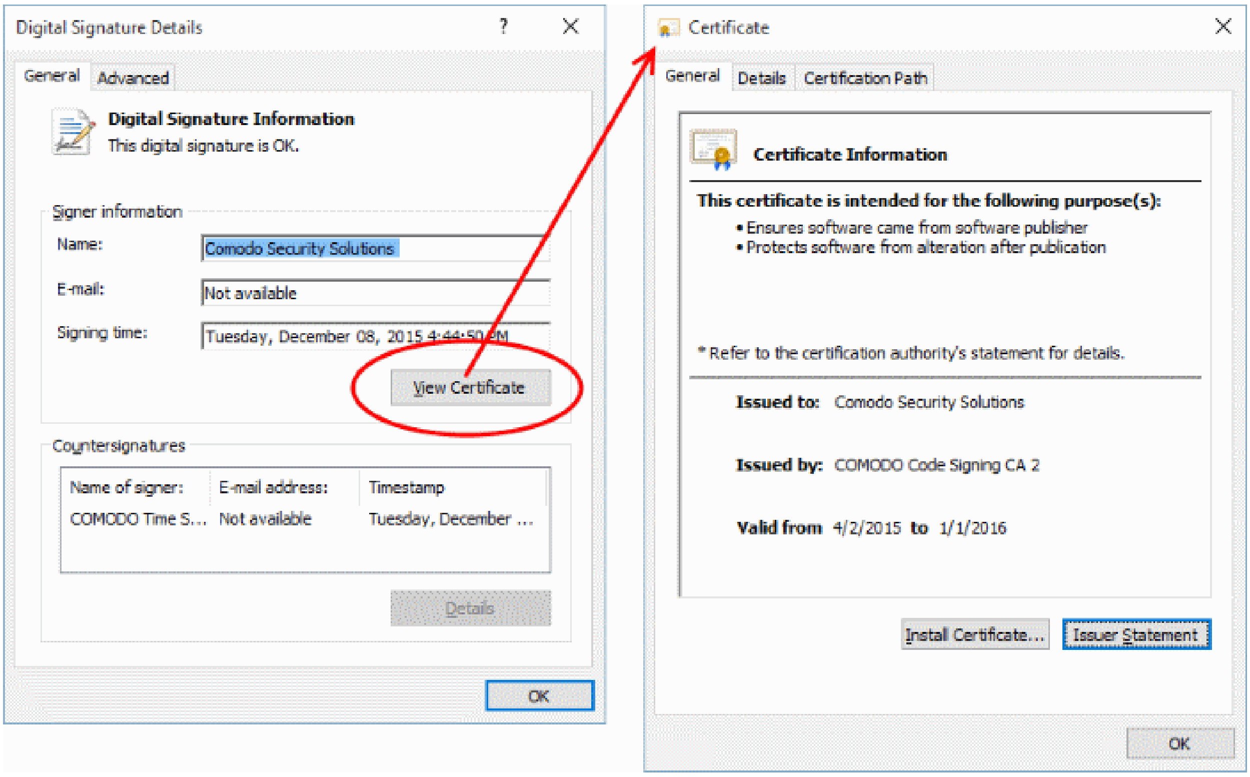
- Browse to the (default) installation directory of CCAV.
- Right click on the file 'ccavsrv.exe'.
- Select 'Properties' from the menu.
- Click the tab 'Digital Signatures (if there is no such tab then the software has not been signed).

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



Name of signer:	Digest algorithm	Timestamp
Comodo Security ...	sha1	Tuesday, December ...

- 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

E-mail: Not available

Signing time: Tuesday, December 08, 2015 4:44:50 PM

Countersignatures

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

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

Issued by: COMODO Code Signing CA 2

Valid from 4/2/2015 **to** 1/1/2016

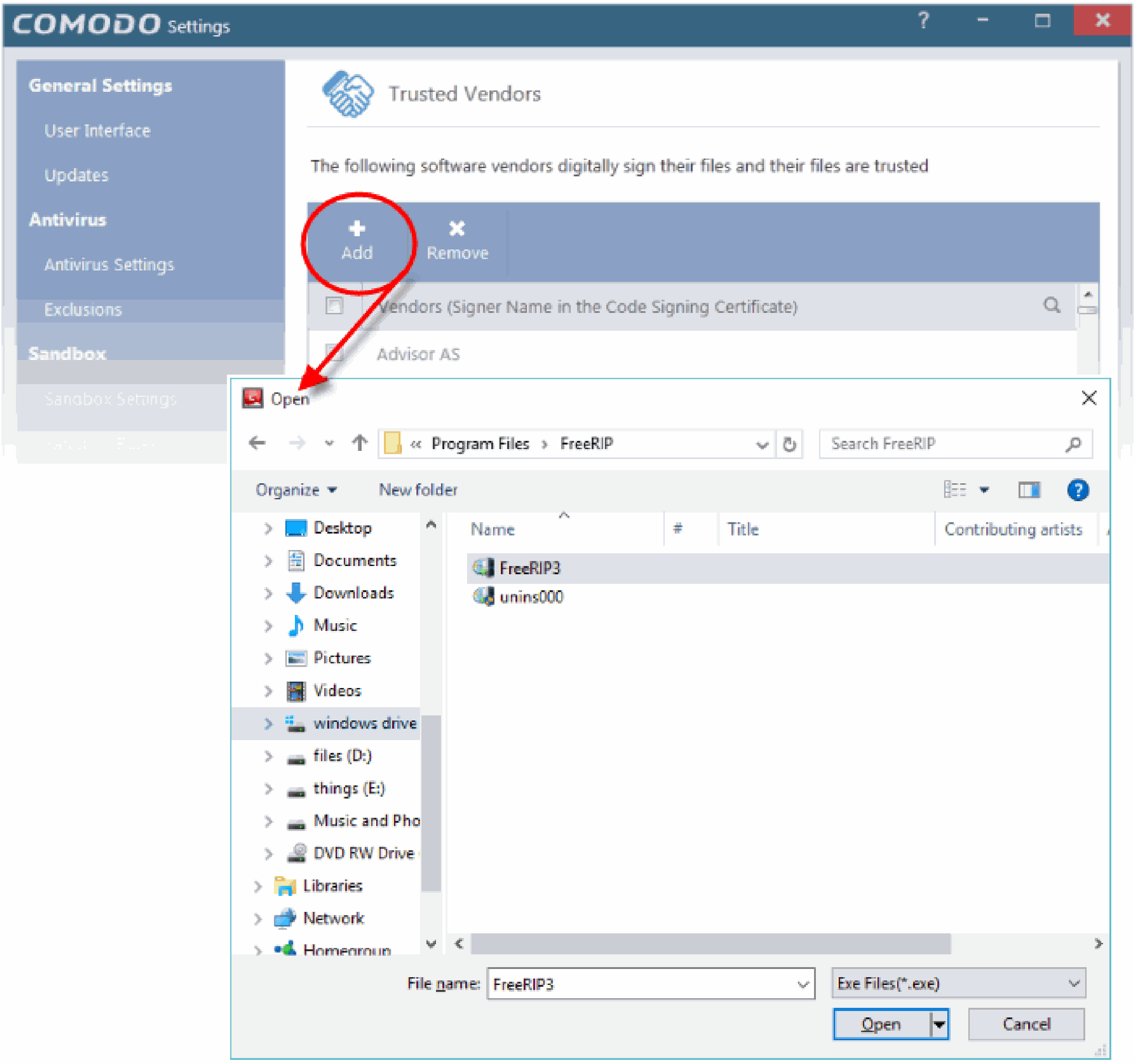
It should be noted that the example above is a special case in that Comodo, as creator of 'ccavsrv.exe', is both the signer of the software and, as a trusted CA, it is also the counter-signer (see the 'Countersignatures' box). In the vast majority of cases, the signer or the certificate (the vendor)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

Adding and Defining a User-Trusted Vendor

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

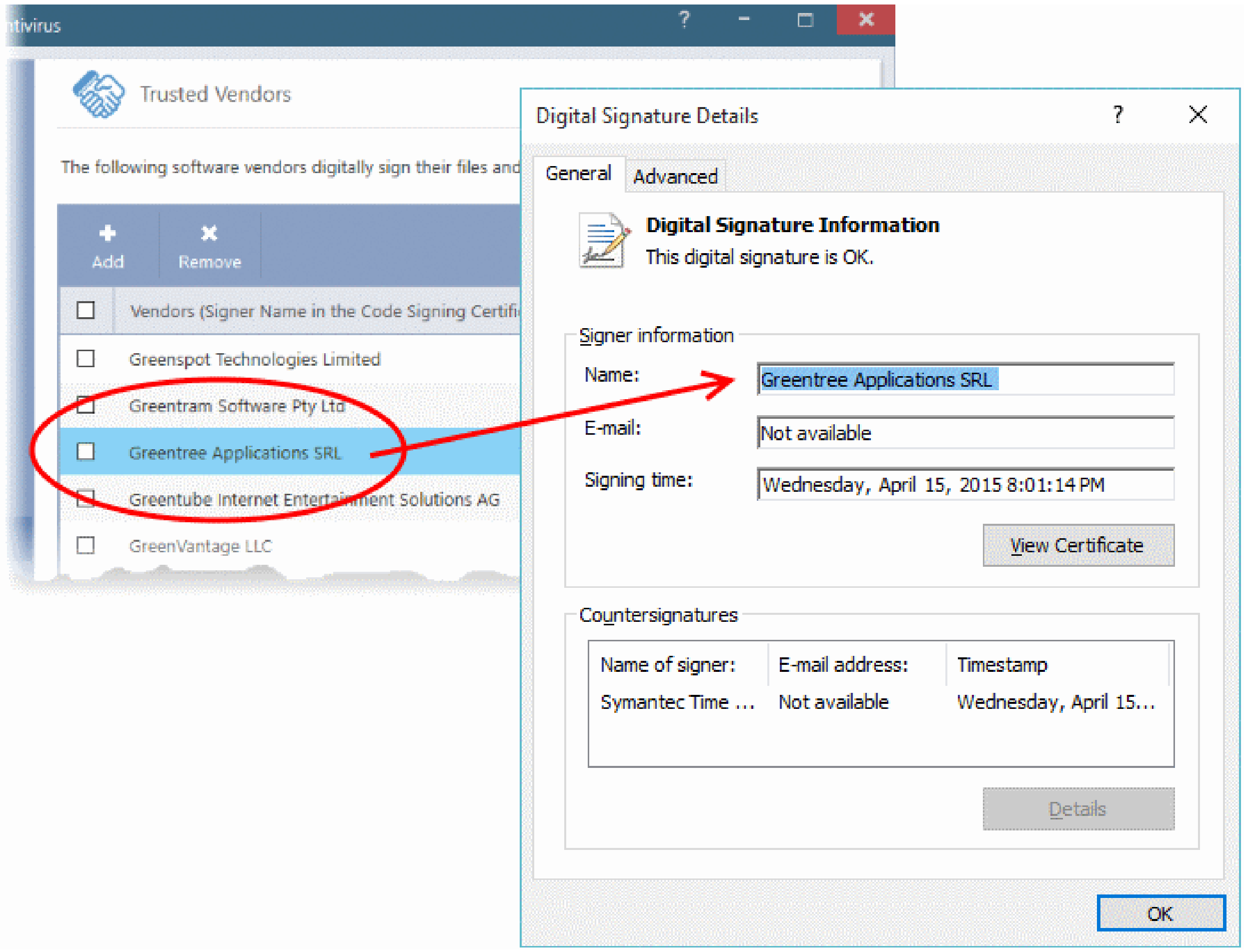
To add a trusted vendor

- Click the 'Add' button from the Trusted Vendors interface



- Navigate to the location of the executable your local drive. In the example above, we are adding the executable 'FreeRIP3.exe'.
- Click 'Apply' for your settings to take effect.

On clicking 'Open', CCAV 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):



The following software vendors digitally sign their files and

□	Vendors (Signer Name in the Code Signing Certifi
□	Greenspot Technologies Limited
□	Greentram Software Pty Ltd
□	Greentree Applications SRL
□	Greentube Internet Entertainment Solutions AG
□	GreenVantage LLC

Digital Signature Information
This digital signature is OK.

Signer information

Name: Greentree Applications SRL

E-mail: Not available

Signing time: Wednesday, April 15, 2015 8:01:14 PM

Countersignatures

Name of signer:	E-mail address:	Timestamp
Symantec Time ...	Not available	Wednesday, April 15...

In the example above, CCAV was able to verify and trust the vendor signature on FreeRIP3.exe because it had been counter-signed by the trusted CA 'Symantec'. The software signer 'Greentree Applications SRL' is now a 'Trusted Software Vendor' and is added to the list. All future software that is signed by the vendor 'Greentree Applications SRL' is automatically added to the Comodo Trusted Vendor list.

If CCAV cannot verify that the software certificate is signed by a Trusted CA then it does not add the software vendor to the list of 'Trusted Vendors'.

Note: The 'Trusted Software Vendors' list displays two types of software vendors:

- User defined trusted software vendors - As the name suggests, these are added by the user by the method outlined earlier. These vendors can be removed by the user by selecting and clicking the 'Remove' button.
- Comodo defined trusted software vendors - These are the vendors that Comodo, in it's capacity as a Trusted CA, has independently validated as legitimate companies. If the user needs to remove any of these vendors from the list, it can be done by selecting the vendor, clicking 'Remove' and restarting the system. Please note that the removal will take effect only on restarting the system.

The Trusted Vendor Program for Software Developers

Software vendors can have their software added to the default 'Trusted Vendor List' that is shipped with Comodo Cloud Antivirus. 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, CCAV 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 CCAV.

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

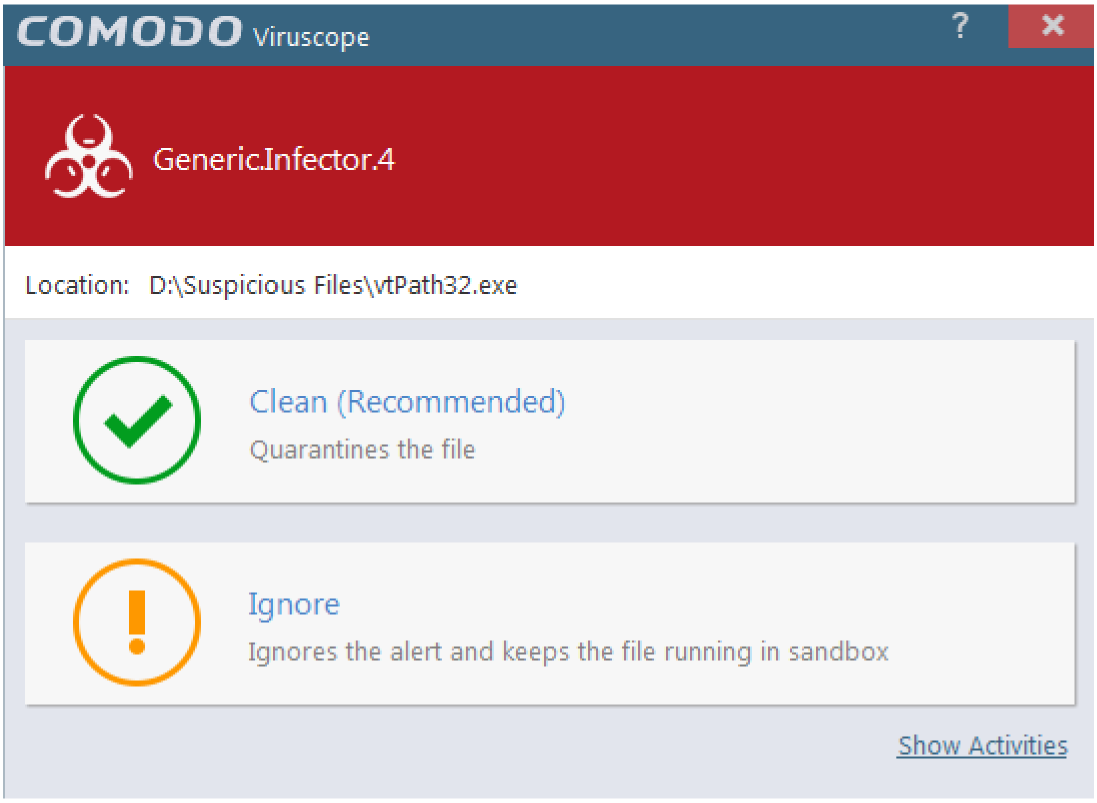
7. Viruscope – Feature Spotlight

Comodo Cloud Antivirus (CCAV) provides unrivalled protection against new malware by automatically running unknown files inside a sandbox. Unknown files are those that are neither definitely bad (blacklisted malware) nor definitely good (whitelisted). If the file is harmless it will run as normal. If the file turns out to be malicious, it will not have been able to cause damage because it was denied access to your data and the underlying operating system.

But what do we do to evaluate the behavior of unknown files in the sandbox? Enter Viruscope.

Viruscope is a behavior analysis technology built into CCAV that monitors the activities of sandboxed processes and installers and alerts you if they take actions that could threaten your security.

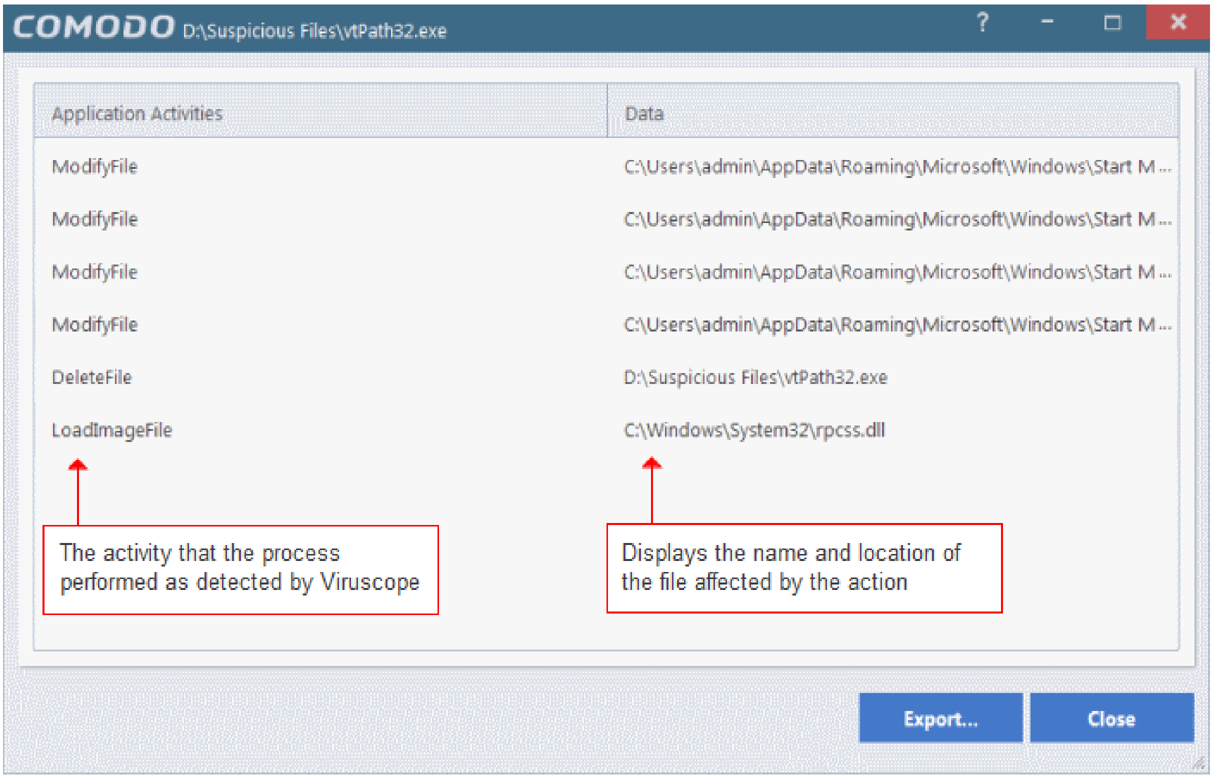
You will see an alert if Viruscope discovers a sandboxed process or an installer/updater is behaving in a suspicious manner:



Generic.Infector.4

Location: D:\Suspicious Files\vtPath32.exe

- If you are not sure of the authenticity of the parent application indicated in the 'Location' field, you can move it to quarantine by clicking 'Clean'.
- If it is an application you trust, you can allow the process to run by clicking 'Ignore'.
- To view the activities of process, click the 'Show Activities' link at the bottom right of the alert:



COMODO D:\Suspicious Files\vtPath32.exe

Application Activities	Data
ModifyFile	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start M...
ModifyFile	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start M...
ModifyFile	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start M...
ModifyFile	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start M...
DeleteFile	D:\Suspicious Files\vtPath32.exe
LoadImageFile	C:\Windows\System32\rpcss.dll

The activity that the process performed as detected by Viruscope

Displays the name and location of the file affected by the action

To implement this, Viruscope uses a set of sophisticated set of behavior ‘Recognizers’, each of which contains algorithms which detect actions typical of a malicious application.

What are behavior recognizers?

Viruscope behavior recognizers detect suspicious activities in multiple functional areas. Recognizers monitor the following activity events:

File activities:

- Create/Modify/Rename/Delete file.
- Set file attributes.
- Set file time to past.

Registry activities:

- Create/Rename/Delete registry key.
- Set/Delete registry key value.

Process activities:

- Create/Terminate process.
- Load file image.
- Other process activities.

Technically, the core Viruscope technology contains the following items:

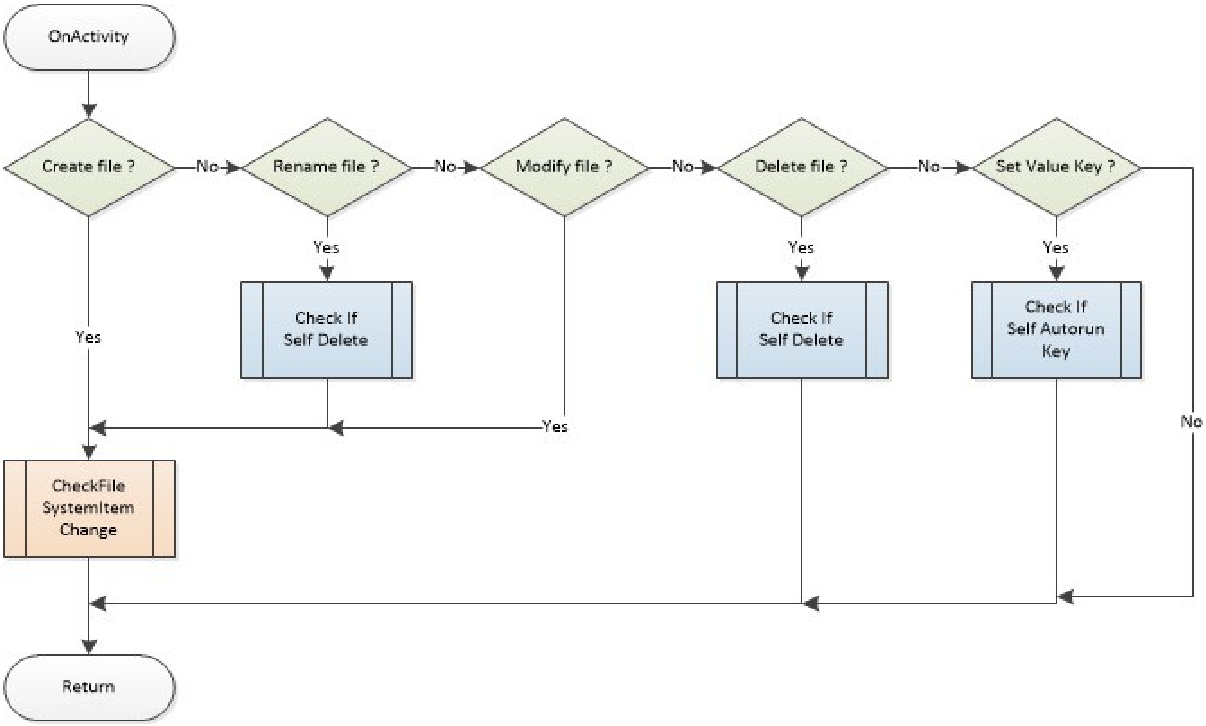
- Tree of all active processes. This tree includes all processes-tracked or not.
- Queue of activities. IO threads receive activities from a target application and pushes them to a queue. These activities are then processed sequentially by a worker thread.
- Per-process activity list. Each process has a list of activities which belong to it. A Viruscope worker thread audits all activities executed by a running process and adds them to the activity list for this particular process.

It will use these items to execute the following tasks:

- After queing the activities of each process, the worker thread will sequentially send each one to the behavior recognizers for analysis.

- A recognizer may traverse the entire process tree and activity list created by Viruscope.
- A recognizer may build its own process tree (the default recognizer uses this technique) and/or queue of activities (the default recognizer doesn't use a cache of activities)

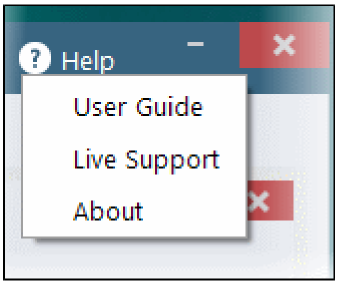
This flowchart describes the activity inspection process of a sample Viruscope recognizer:



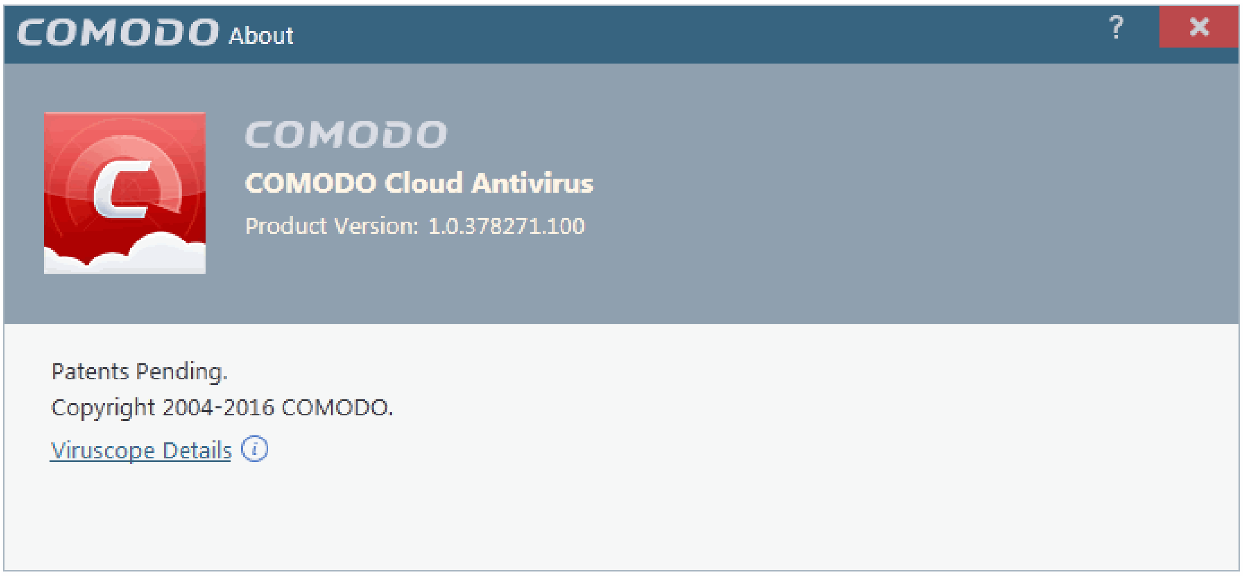
Viruscope is another key layer of security in the CCAV arsenal, taking our protection beyond that found in any other antivirus product. Our real-time virus monitor protects you against known threats, while auto-sandboxing protects you against unknown threats. With Viruscope on top, you also get proactive warnings about brand new malware.

8. Comodo Support and About Information

You can view the online help guide for Comodo Cloud Antivirus, start a chat support session with a technician at Comodo and view the About dialog by clicking the Help link in the title bar.



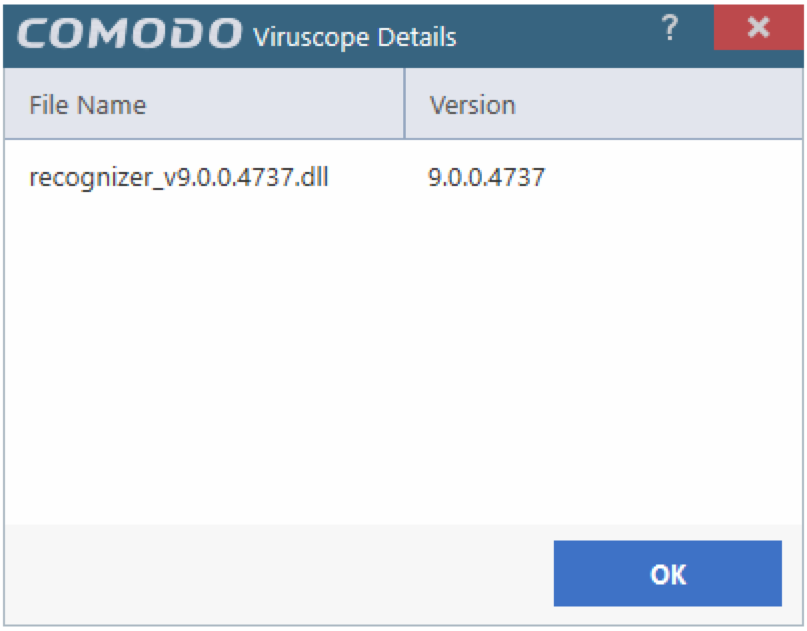
- **User Guide** – Opens the CCAV online help guide at **https://help.comodo.com**
- **Live Support** – Choose this option to chat with our technician for technical help for CCAV. A chat session will start in your browser window and you will be connected to a Microsoft certified support technician at Comodo. The expert support is available 24/7.
- **About** - Displays the product version, details of active Viruscope Recognizers and copyright information.



Product Version: 1.0.378271.100

Patents Pending.
Copyright 2004-2016 COMODO.

- To view the Viruscope Recognizer version installed on your computer, click the 'Viruscope Details' link.



File Name	Version
recognizer_v9.0.0.4737.dll	9.0.0.4737

About Comodo

The Comodo organization is a global innovator and developer of cyber security solutions, founded on the belief that every single digital transaction deserves and requires a unique layer of trust and security. Building on its deep history in SSL certificates, antivirus and endpoint security leadership, and true containment technology, individuals and enterprises rely on Comodo's proven solutions to authenticate, validate and secure their most critical information.

With data protection covering endpoint, network and mobile security, plus identity and access management, Comodo's proprietary technologies help solve the malware and cyber-attack challenges of today. Securing online transactions for thousands of businesses, and with more than 85 million desktop security software installations, Comodo is Creating Trust Online®. With United States headquarters in Clifton, New Jersey, the Comodo organization has offices in China, India, the Philippines, Romania, Turkey, Ukraine and the United Kingdom.

Comodo Security Solutions, Inc.

1255 Broad Street

Clifton, NJ, 07013

United States

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.**