

**COMODO**  
Creating Trust Online®



# Comodo Cloud Antivirus

Software Version 1.13

## User Guide

Guide Version 1.13.100317

Comodo Security Solutions  
1255 Broad Street  
Clifton, NJ, 07013  
United States [Table of Contents](#)

## Table of Contents

<b>1. Introduction to Comodo Cloud Antivirus.....</b>	<b>5</b>
1.1.System Requirements.....	6
1.2.Installation .....	7
1.3.Starting Comodo Cloud Antivirus.....	16
1.3.1.The Main Interface.....	17
1.3.2.The Widget.....	22
1.3.3.The System Tray Icon.....	24
1.4.'Lucky You' Statistics.....	25
1.5.Understanding CCAV Alerts.....	29
<b>2. Scan and Clean your Computer .....</b>	<b>38</b>
2.1.Run a Quick Scan.....	39
2.2.Run a Full Computer Scan.....	41
2.3.Run a Certificate Scan.....	43
2.4.Run a Custom Scan.....	46
2.4.1.Scan a Folder.....	47
2.4.2.Scan a File.....	50
2.5.Processing Infected Files.....	52
2.6.Managing Detected Threats.....	55
2.7.Viewing Valkyrie Analysis Results.....	57
<b>3. The Sandbox.....</b>	<b>61</b>
3.1.Run an Application or Browser in the Sandbox.....	63
3.2.Manage Sandboxed Items.....	66
<b>4. View CCAV Logs.....</b>	<b>69</b>
4.1.Antivirus Logs.....	71
4.2.Executed Application Logs (Sandbox Logs).....	72
4.3.Setting Changes Logs.....	73
4.4.Scan Actions Logs.....	74
<b>5. View and Manage Quarantined Items.....</b>	<b>75</b>
<b>6. CCAV Settings.....</b>	<b>79</b>
6.1.General Settings.....	81
6.1.1.Customize User Interface.....	82
6.1.2.Configure Program Updates.....	86
6.2. Antivirus Settings.....	88
6.2.1.Antivirus Settings.....	88
6.2.2.Exclusions.....	91
6.3.Sandbox Settings.....	104

6.3.1.Sandbox Settings.....	105
6.3.2.Sandbox Rules.....	108
6.3.3.Protected Files/Folders.....	111
6.4.File Rating Settings .....	114
6.4.1.File Rating Settings.....	115
6.4.2.Trusted Applications.....	116
6.4.3.Submitted Applications.....	120
6.4.4.Trusted Vendors.....	121
6.5.Advanced Protection Settings.....	127
6.5.1.Browser Settings Protection .....	127
<b>7.Getting Live Support.....</b>	<b>130</b>
<b>8. Viruscope - Feature Spotlight.....</b>	<b>131</b>
<b>9. Comodo Internet Security Essentials.....</b>	<b>134</b>
9.1.Understanding Alerts.....	140
<b>10.Comodo Support and About Information.....</b>	<b>144</b>
<b>Appendix 1 - How to Tutorials.....</b>	<b>146</b>
Enable / Disable AV, Sandbox and Game mode.....	147
Run an Antivirus scan on selected items.....	149
Block Incoming / Outgoing Internet connection to sandboxed applications.....	151
Add exclusions by allowing Internet connection to sandboxed applications.....	152
Enable/ Disable Realtime scan.....	153
Run a virus scan on your computer.....	154
Run an Application or Browser in the sandbox.....	160
Run a Certificate Scan.....	162
Configure Antivirus Exclusions.....	165
View lucky you statistics.....	169
Switch Off Automatic Antivirus and Software Updates.....	171
Switch Off Automatic Antivirus and Software Updates.....	171
Enable/ Disable browser settings protection.....	172
Evaluate the behavior of unknown files in the sandbox.....	173
Detect Potentially Unwanted Applications (PUA).....	174
Manually add items to quarantine .....	175
Delete quarantined items .....	176
Restore a quarantined item .....	176
Submit as False Positive.....	177
Configure Proxy and Host Settings.....	177
Enable/ Disable Sandbox indicator.....	178
Enable / Disable viruscope.....	179
Respond to alerts .....	180

View CCAV Logs.....	186
Get instant support.....	191
<b>About Comodo.....</b>	<b>193</b>

## 1. Introduction to Comodo Cloud Antivirus

Comodo Cloud Antivirus (CCAV) is a lightweight and powerful application that uses automatic threat containment and real-time cloud scanning to immediately neutralize both known and unknown malware. The Valkyrie feature automatically analyzes unknown files (those files which could not be classified as either 'Trusted' or 'Malicious') in order to identify zero-day threats.



### 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.

- **Introduction**
  - **System Requirements**
  - **Installation**
  - **Starting Comodo Cloud Antivirus**
  - **Lucky You Statistics**
  - **Understanding CCAV Alerts**
- **Scan and Clean your Computer**

- [Run a Quick Scan](#)
- [Run a Full Computer Scan](#)
- [Run a Certificate Scan](#)
- [Run a Custom Scan](#)
- [Processing Infected Files](#)
- [Managing Detected Threats](#)
- [Viewing Valkyrie Analysis Results](#)
- [Sandbox](#)
  - [Run an Application or Browser in the Sandbox](#)
  - [Manage Sandboxed Items](#)
- [View CCAV Logs](#)
  - [Sandbox Logs](#)
  - [Antivirus Logs](#)
  - [Setting Changes Logs](#)
  - [Scan Actions Logs](#)
- [View and Manage Quarantined Items](#)
- [CCAV Settings](#)
  - [General Settings](#)
  - [Antivirus Settings](#)
  - [Sandbox Settings](#)
  - [File Rating Settings](#)
  - [Advanced Protection Settings](#)
- [Getting Live Support](#)
- [Viruscope - Feature Spotlight](#)
- [Comodo Support and About Information](#)

## 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)	<ul style="list-style-type: none"> <li>• 384 MB available RAM</li> <li>• 210 MB hard disk space for both 32-bit and 64-bit versions</li> <li>• CPU with SSE2 support</li> <li>• Internet Explorer Version 5.1 or above</li> </ul>
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)	
Windows XP (32-bit)	<ul style="list-style-type: none"> <li>• 256 MB available RAM</li> <li>• 210 MB hard disk space for both 32-bit and 64-bit versions</li> <li>• CPU with SSE2 support</li> <li>• Internet Explorer Version 5.1 or above</li> </ul>

**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 that are on your computer, including Comodo CIS/CES. 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 the latest guidelines, however the following steps should help most Windows users:

- Click the Windows 'Start' button
- 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'
- Repeat the 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 <https://antivirus.comodo.com/cloud-antivirus.php>)

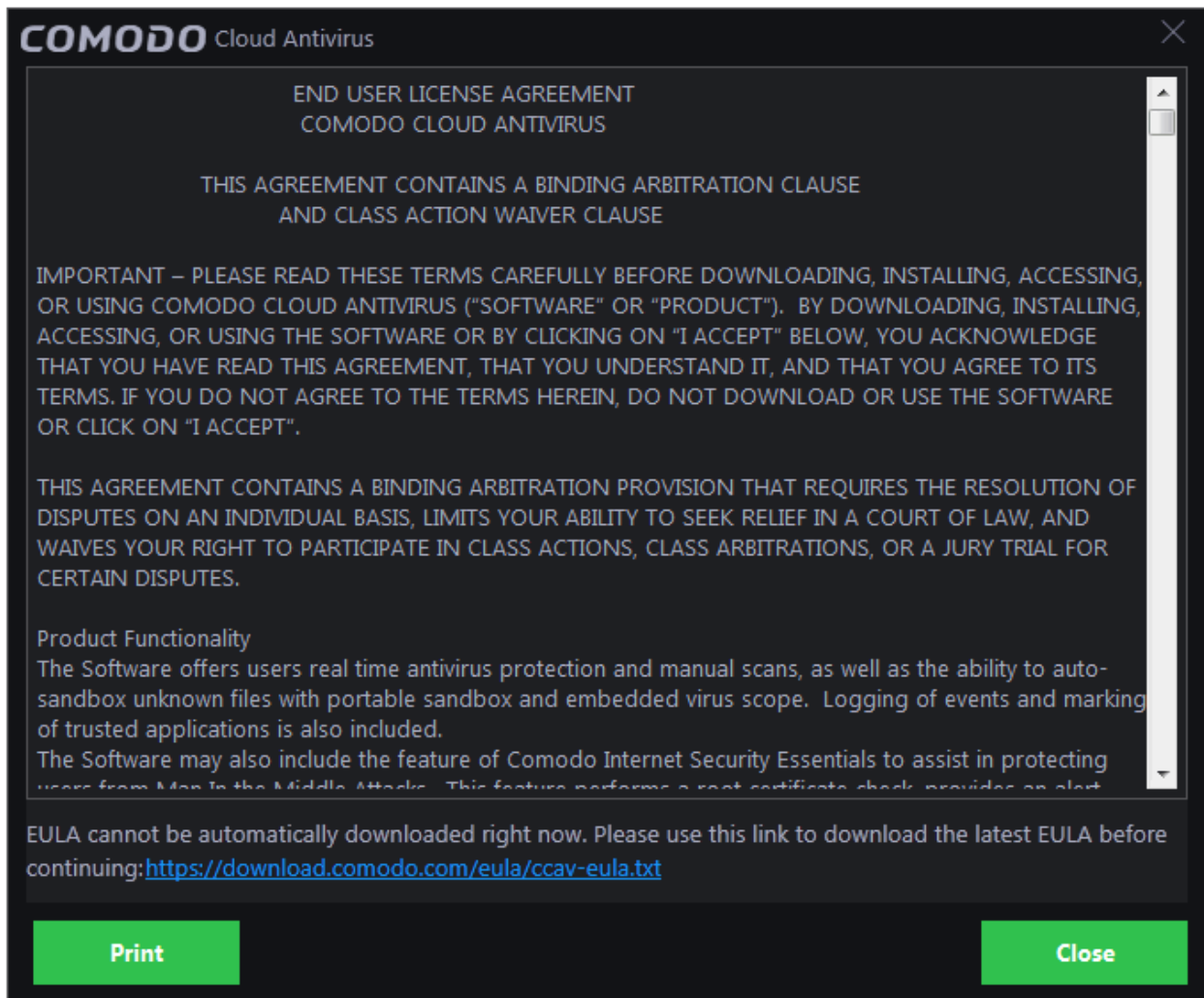
Once download is complete, double-click on the ccav\_installer file  to start the installation wizard:

The language selection dialog will be displayed.

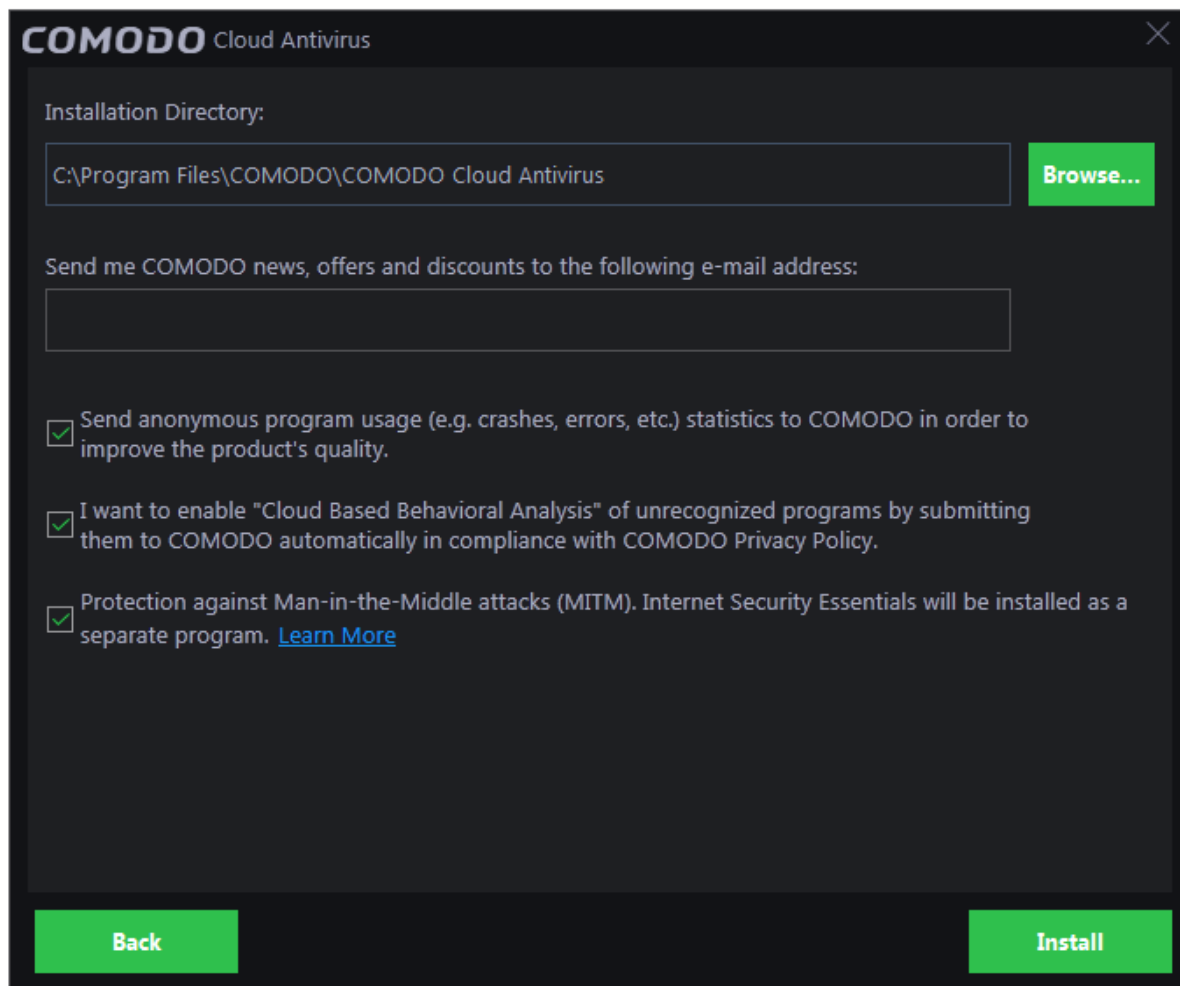


- Select the language in which you want CCAV to be installed from the drop-down menu at the bottom
- Before proceeding with the installation, read and agree to the license agreement at the bottom of the interface



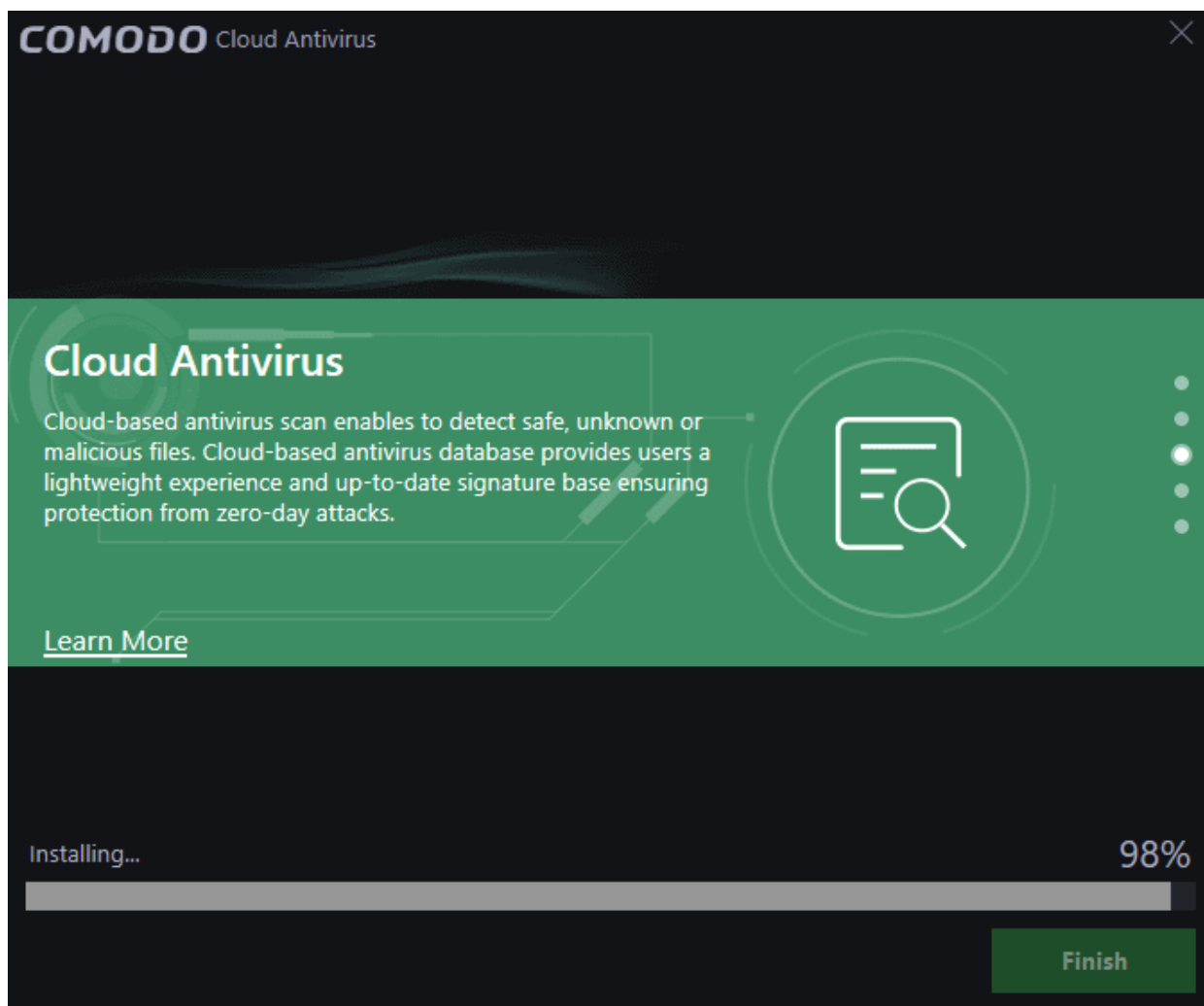


- Click the 'Close' button to return to the installation configuration screen
- Click 'I agree' to begin the installation wizard. This will start the installation of CCAV and, if you do not have it installed already, Comodo Internet Security Essentials (CISE). See **Comodo Internet Security Essentials** to find out more about CISE.

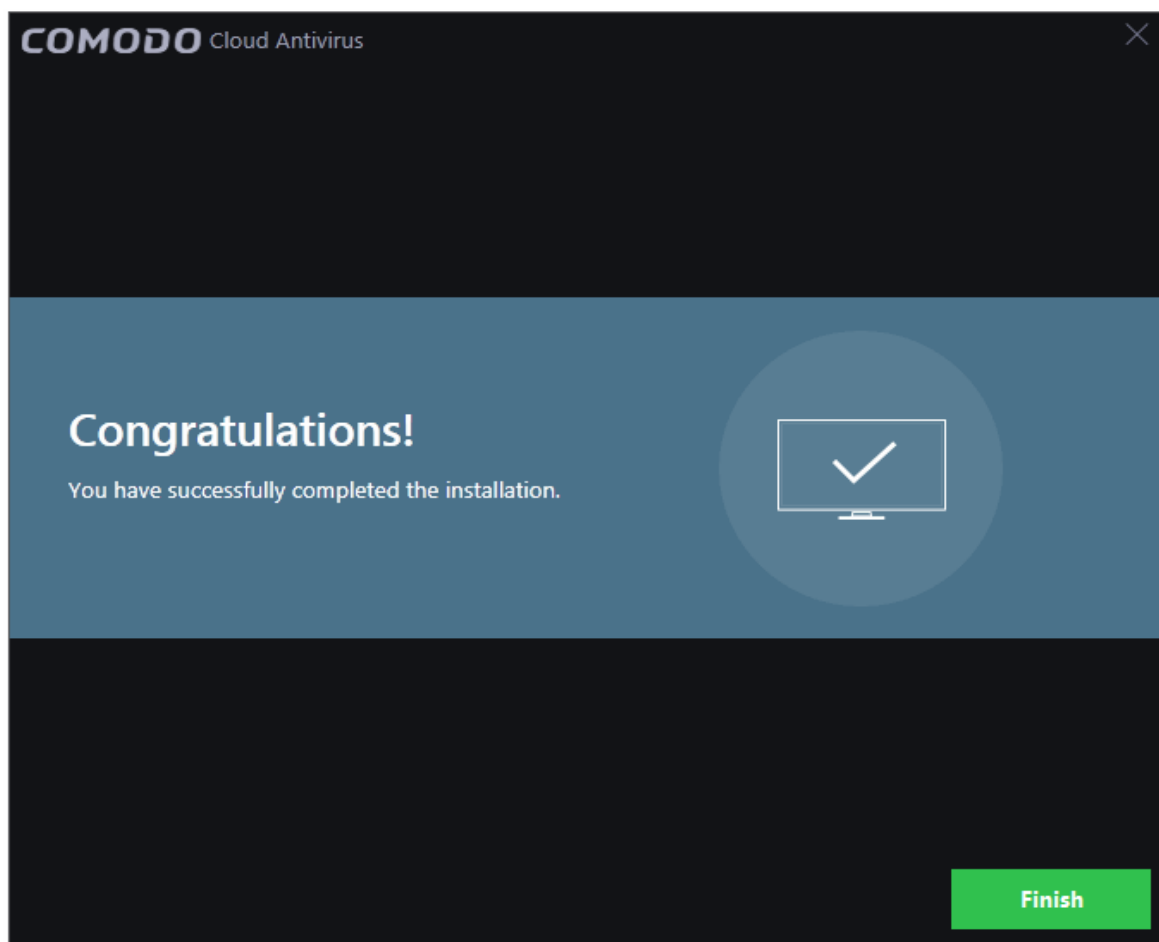


- The default installation location is C:\Program Files\COMODO\COMODO Cloud Antivirus. If you want to change this, click the 'Browse...' button, navigate to the desired location and click 'Open'.
- Enter your email address in the second field if you would like to subscribe for Comodo news and get offers and discounts from Comodo.
- Cloud Based Behavior Analysis. If enabled, any file that is identified as unknown is submitted to Comodo Valkyrie for behavior analysis. Unknown files are subjected to a range of static and dynamic tests to determine whether they behave in a malicious manner. The results will be sent back to your computer in around 15 minutes. Comodo recommends users leave this setting enabled.
- Protection against Man-in-the-Middle attacks (MITM). Will also install Comodo Internet Security Essentials (CISE). CISE protects you online by verifying that the websites you visit are using SSL certificates signed by a trusted CA.
- Click the 'Install' button.

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



...the success message will be displayed.



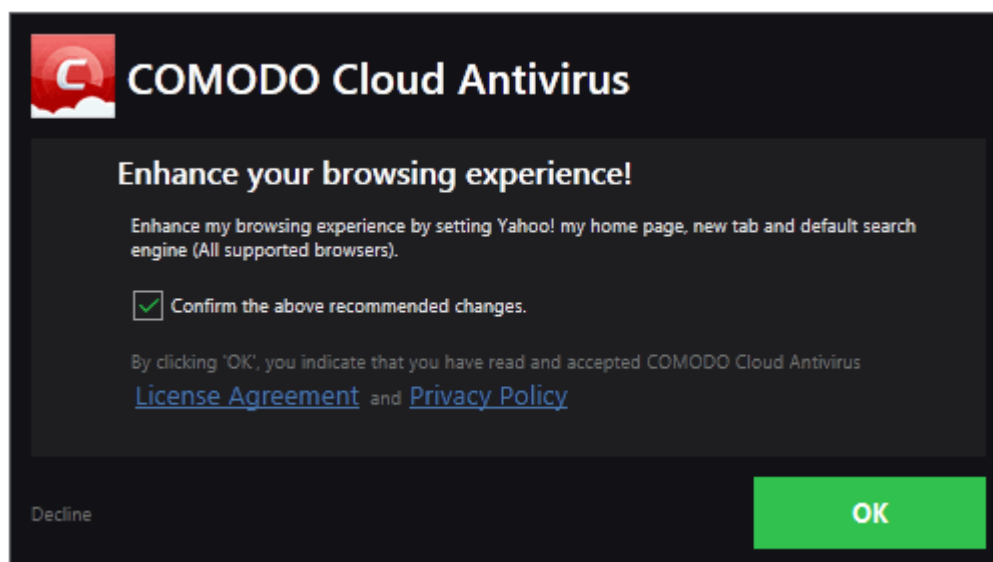
- Click 'Finish'

After successful installation, CCAV will automatically launch a quick virus scan and will display a welcome screen:



The welcome screen will appear every time you start your system. If you do not want to view the screen every start up, select 'Do not show this window again' before closing the window.

You will be offered the opportunity to set your search engine provider to Yahoo:



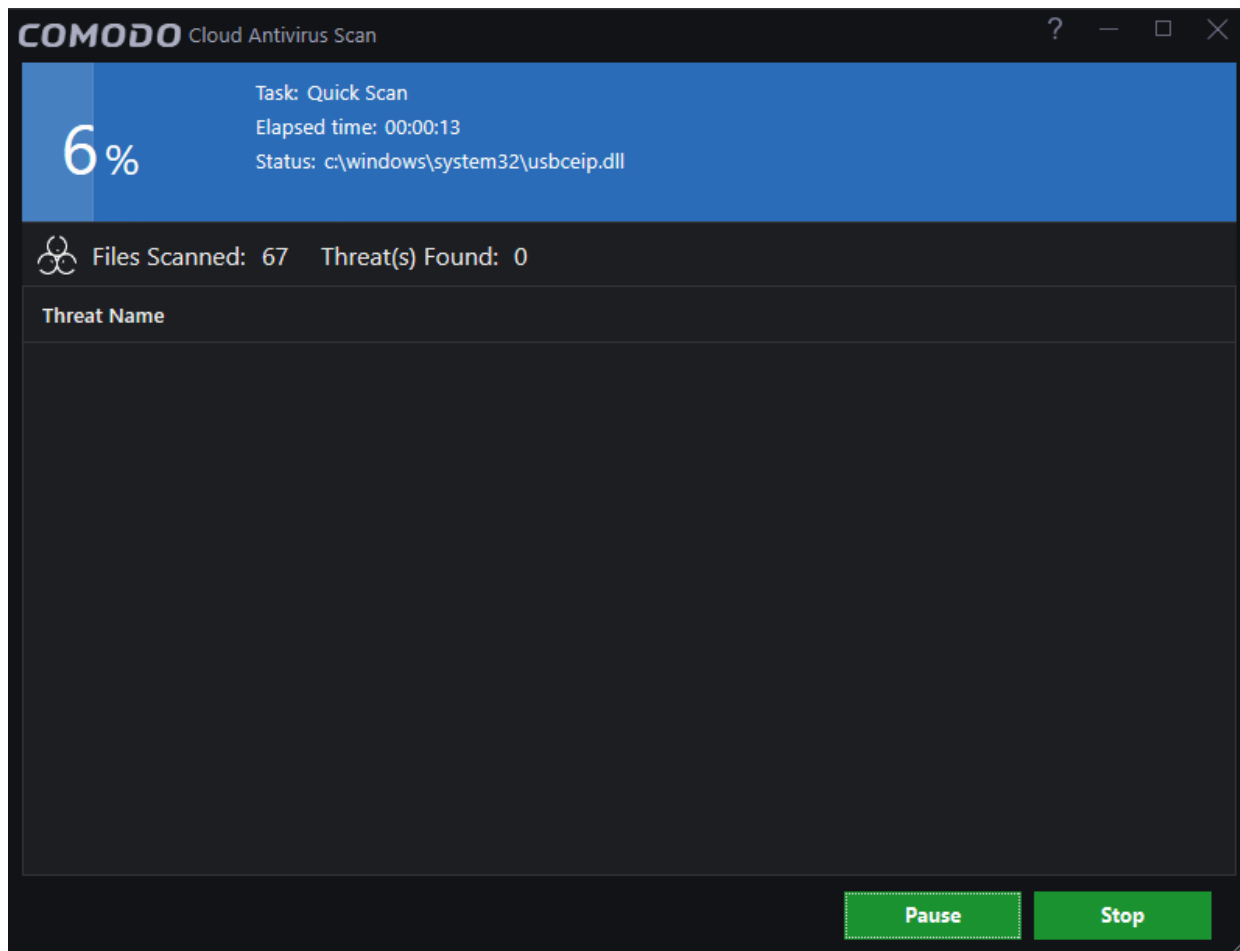
Currently supported browsers are Mozilla Firefox, Google Chrome, Internet Explorer, Comodo Dragon, Comodo IceDragon, Chromodo and Opera.

Making Yahoo! your default search engine means:

- When you enter a search item into the address bar of a supported browser, the search will be carried out by Yahoo
- A 'Search with Yahoo' menu entry will be added to the right-click menu of supported browsers

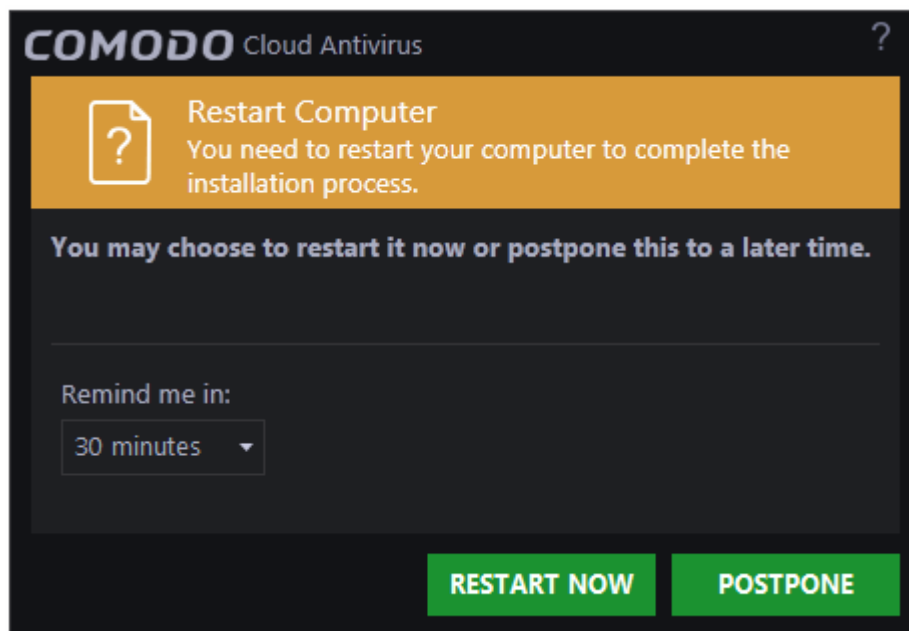
- Yahoo will be set as the default search engine in the 'Search' box of supported browsers
- The instant 'search suggestions' that you see when you start typing a search item will be provided by Yahoo!
- Click 'Decline' to continue using your current search engine and home page.

CCAV will commence a quick scan automatically after the installation. The areas scanned are system memory, auto-run entries, hidden services, boot sectors and other critical areas (including files that could be launched on system startup).



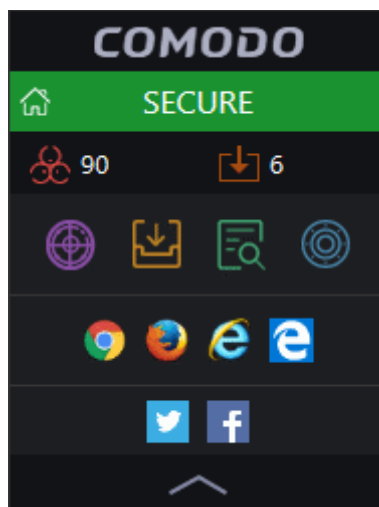
Scan results will be shown once the scan is complete. See ['Processing Infected Files'](#) to learn how to manage infected files.

You will be prompted to restart the system after the scan. Please note that the application will work to its full potential only after the restart.



- If you want to restart the computer immediately, save all your work and click 'Restart Now'
- If you want to restart the computer at a later time, select when you want to be reminded from the drop-down and click 'Postpone'.

The CCAV widget is displayed every time you start your computer. It contains five stripes with shortcuts for executing different CCAV tasks:



- The first stripe displays the current security status of your computer and acts as a shortcut to open the CCAV application.
- The second stripe displays a summary on threats detected by real-time and on-demand scans and applications running currently inside Sandbox.
- The third stripe contains shortcuts for common CCAV tasks:
  - Start a scan
  - Select an application and run it in the Sandbox
  - View logs
  - View quarantine

- The fourth stripe contains shortcuts which will launch your browsers inside the secure container. Browsers running inside the container are isolated from the rest of your computer and your private data, protecting you from online threats.
- The fifth stripe contains shortcuts to social networking sites like Twitter and Facebook.

For more details about the widget, refer to the section [The Widget](#).

## 1.3. Starting Comodo Cloud Antivirus

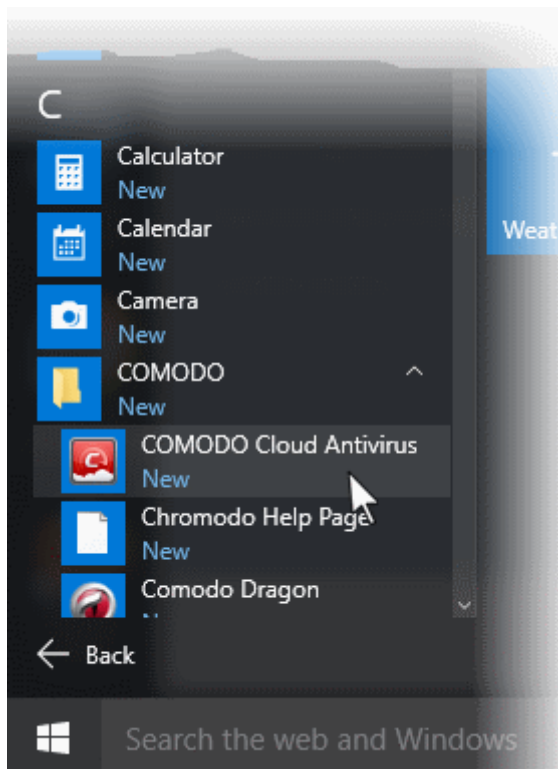
After installation, Comodo Cloud Antivirus will automatically start running in the background whenever you start Windows. In order to configure and view settings within CCAV, you need to open the main interface.

There are 4 different ways to open Comodo Cloud Antivirus:

- [Windows Start Menu](#)
- [Windows Desktop](#)
- [Widget](#)
- [System Tray Icon](#)

### Windows Start Menu

- Click 'Start' and select 'All Programs'/'All Apps' > 'COMODO' > 'COMODO Cloud Antivirus'



### Windows Desktop

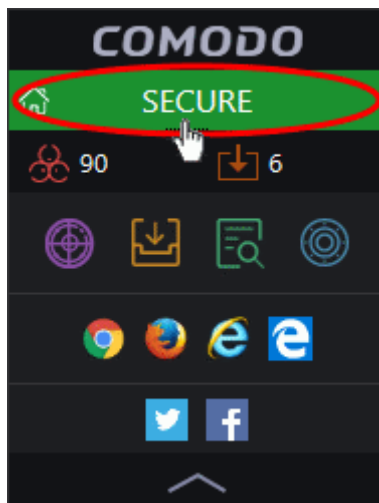
- Double click the 'Comodo Cloud Antivirus' shortcut on your desktop:





## Widget

- Click the information bar on the widget to start CCAV.



You can also view other details in the widget such as current security status, number of threats detected from scans, number of applications currently running in the sandbox, links to social media sites and more. Refer to '[The Widget](#)' for more details.

## System Tray Icon

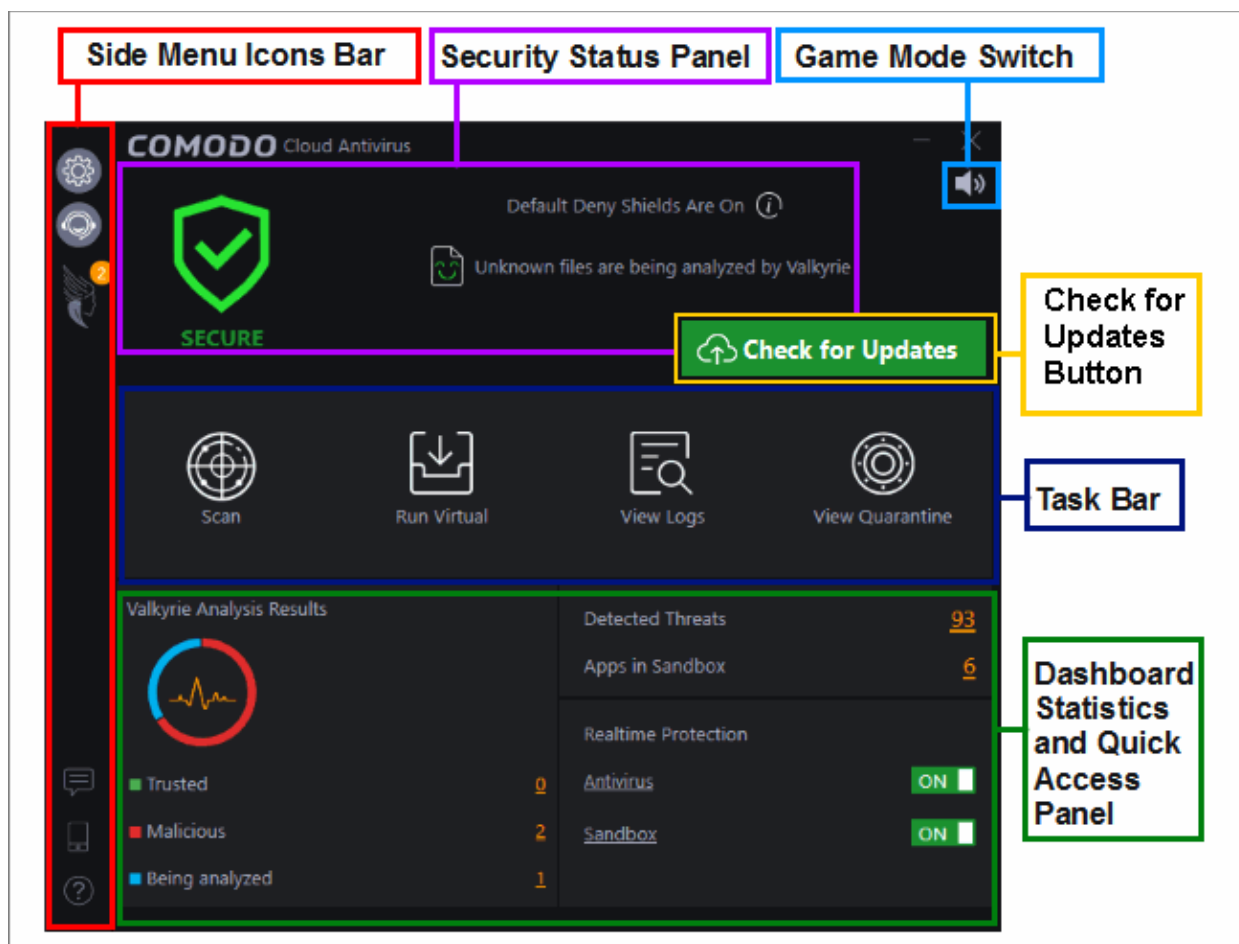
- You can also double click the CCAV tray icon to open the application:









Right-click on the tray icon to quickly access important settings. These include settings related to the Antivirus, Sandbox, Game Mode options and more. Refer to '[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 with the minimum of fuss.



## Side Menu Icons Bar

- Settings**  - Configure protection and general settings, including antivirus configuration, sandbox configuration, manage trusted applications and more. Refer to '**CCAV Settings**' for more details.
- Live Support**  - Chat with a Comodo technician should you have any problems with the application. Refer to '**Getting Live Support**' for more details.
- Lucky You**  - 'Lucky You' files are unknown files discovered on your computer which were subsequently identified as malware by Comodo Valkyrie. The 'Lucky You' description means CCAV detected and blocked the file before any other AV product in the industry viewed it as malicious. Refer to '**Lucky You Statistics**' for more details.
- Send Feedback**  - Allows you to provide comments to Comodo on the product. You can submit feedback over email or by leaving a comment on the Comodo forums.
- Mobile**  - Download Comodo Mobile Security apps for Android phones and tablets. Click 'Mobile' to get Android apps such as 'Comodo Mobile Security', 'Comodo Anti-Theft', 'Comodo Back Up' and 'Comodo App Lock'. You can also get apps from our website, <https://m.comodo.com/> or from the 'Google Play' app store.
- Help**  - Click 'Help' for the following options:
  - User Guide** - Opens the CCAV online help guide at <https://help.comodo.com>

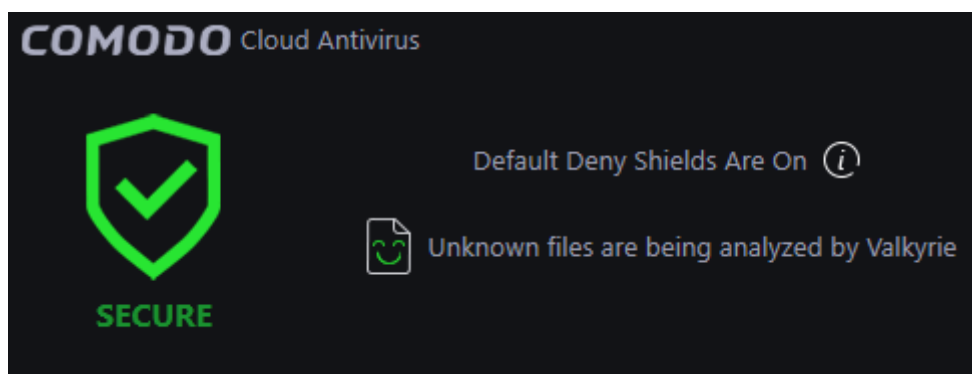
- **Live Support** - Click this link to chat with our technician for technical help for CCAV. Refer to '[Getting Live Support](#)' for more details.
- **Submit File** - Allows you to manually submit a suspicious file from your computer to Valkyrie for analysis. Valkyrie analysis involves automated and manual testing in order to discover whether or not the file is malicious. Note: Valkyrie results only show verdicts for items that have run in the sandbox. The results will be sent back to your computer once the analysis is complete. The results **will be added** to the global whitelist and blacklist to help fellow CCAV users who encounter the same file. Refer to '[Viewing Valkyrie Analysis Results](#)' for more details.
- **Diagnostics Report** - Runs a comprehensive diagnostics report on your system. Reports include items like loaded modules, services, Windows errors, Auto codes, IDE and more.
- **Check for Updates** - Checks for and installs any available CCAV updates. Release notes are available for each major update
- **About** - Displays the product version, details of active Viruscope recognizers, copyright information and release for upcoming updates. Refer to '[Comodo Support and About Information](#)' for more details.

## Tasks Bar

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

## Security Status Pane

The security status pane shows your overall protection levels and messages about individual security modules:



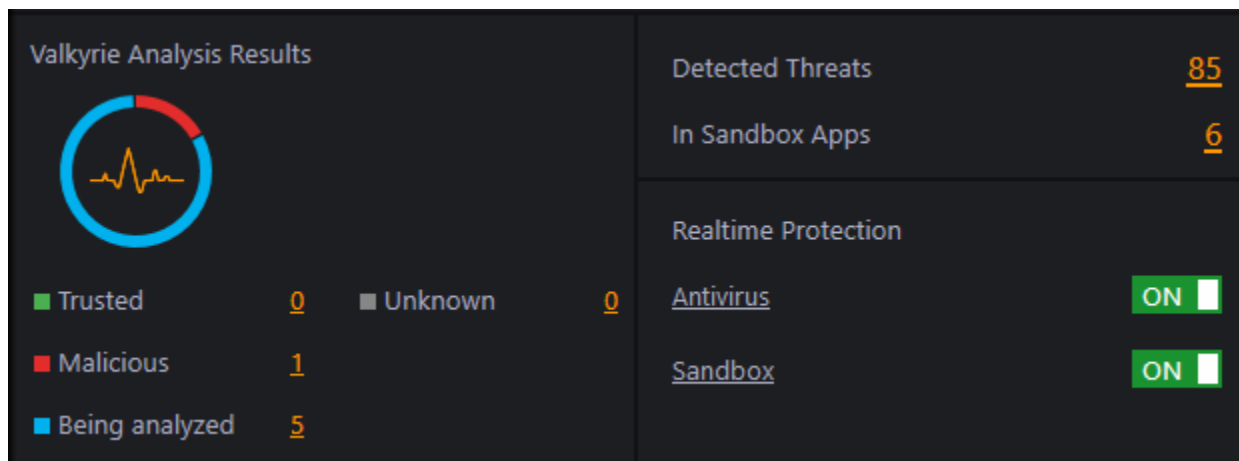
The text below the shield states your current security status. See '[Antivirus Configuration](#)' and '[Sandbox Configuration](#)' for more details.

- **Secure** - Indicates real-time protection is active.
- **At risk** - Indicates one or more protection systems are not active or require updates. Click 'Fix it' to resolve the issue.
- **Game Mode** - Indicates whether the 'Game Mode' is switched on or off

The pane also displays status messages such as from Valkyrie, initial quick scan is running and so on.

## Dashboard Statistics and Quick Access Pane

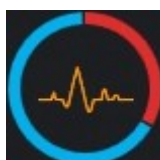
The upper-right pane shows the number of threats detected by the antivirus (all time), and the number of applications currently running in the sandbox. The left-hand pane displays the verdicts on unknown files submitted to Valkyrie for analysis. The 'Unknown' details will be available if the 'I want to enable Cloud Based Behavioral Analysis' check box is disabled in **Sandbox Settings**. The 'Realtime Protection' pane allows you to enable or disable the antivirus and sandbox components.



- **Detected Threats** - Displays the number of threats detected by CCAV during real-time scanning as well as during manual scanning. Click on the number to open the 'Detected Threats' interface to lets you take actions on the threats. Refer to the section '**Managing Detected Threats**' for more details.
- **Sandboxed Apps** - Displays the number of applications that are currently running inside the sandbox environment. This includes automatically sandboxed applications and those which were manually added to the sandbox. Refer to the section '**Managing Sandboxed Applications**' for more details.
- **Valkyrie Analysis** - Summary of verdicts on unknown files submitted to Valkyrie for analysis.
  - The pie-chart shows the comparison of numbers of files with different verdicts with an indication of current Valkyrie detection status.



- Indicates that you need to run a full scan to identify unknown files on your computer.



Indicates that the detected unknown files were submitted to Valkyrie and are currently under analysis after auto-submission. You can also submit unknown files manually for Valkyrie analysis:

- - Refer to the explanation **above** for details on manually submitting files.
  - Refer to the section **Sandbox Settings** for more details on configuring CCAV to automatically submit unknown files for analysis.



- Indicates that all unknown files have been submitted and analyzed by Valkyrie and there is no unknown or pending files left in your computer.

- At the right of the pie chart, the numbers of files with different Valkyrie Analysis status are displayed:
  - Trusted - Number of files identified as trustworthy by Valkyrie Analysis
  - Malicious - Number of identified as malicious by Valkyrie Analysis
  - Being analyzed - Number of files submitted to Valkyrie, but yet to be analyzed
  - Unknown - This will be available if the auto-submission of detected unknown files is disabled in **Sandbox Settings**. Displays the number of unknown files that are to be submitted to Valkyrie for analysis.
- Click the numbers beside 'Trusted', 'Malicious', 'Being analyzed' and 'Unknown' to open the respective results interface.

## To enable/disable real-time protection

- Use the toggle switches under 'Realtime Protection' section to enable or disable real-time 'Antivirus' and 'Sandbox' protection. If disable a protection setting, the status under 'Security Status' icon will show as 'At Risk'
- Click the 'Antivirus' and 'Sandbox' links to open the 'Settings' screen for configuring the respective module

## Game Mode

The '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.

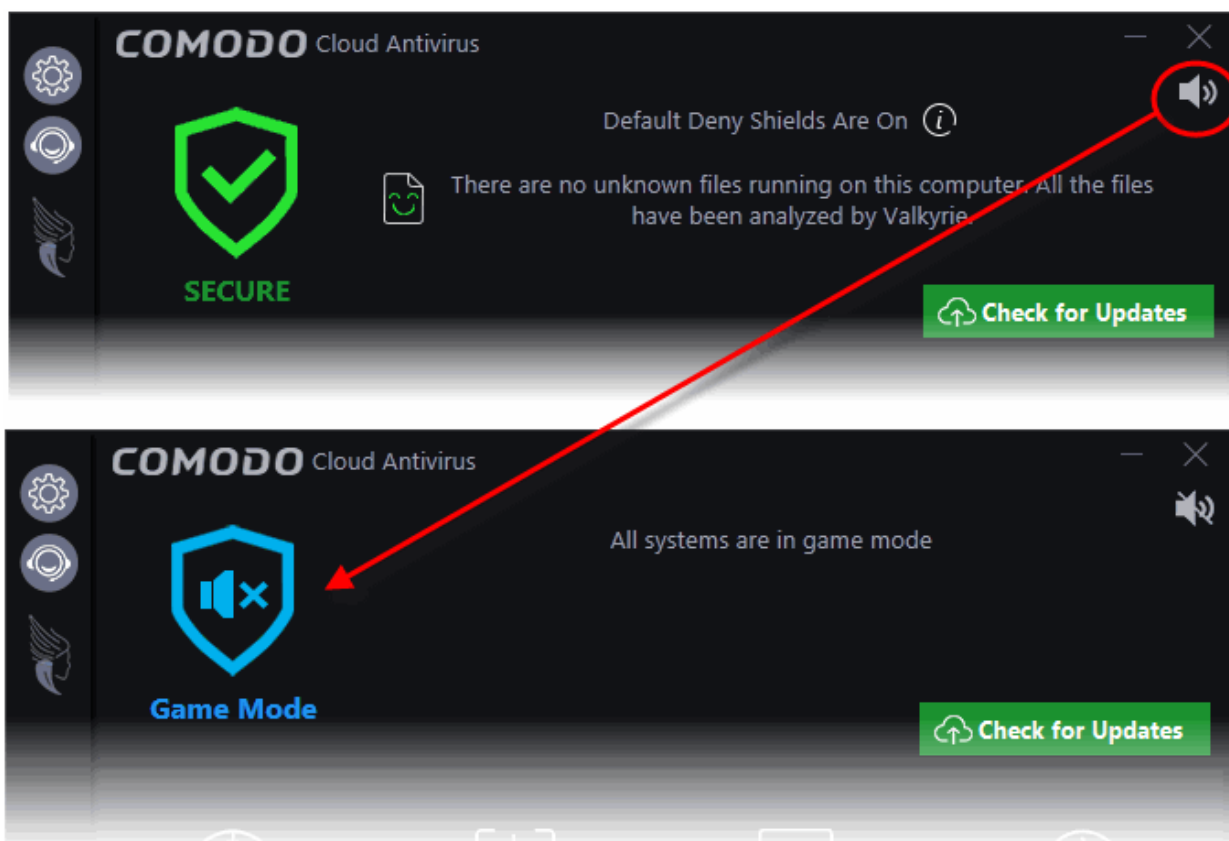
In game mode:

- AV 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 top-right of the main interface.

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



- To return to normal mode and resume alerts and notifications click the 'Game Mode' button again.

## Check for Updates

- Click the 'Check for Updates' button to start the manual search for updates

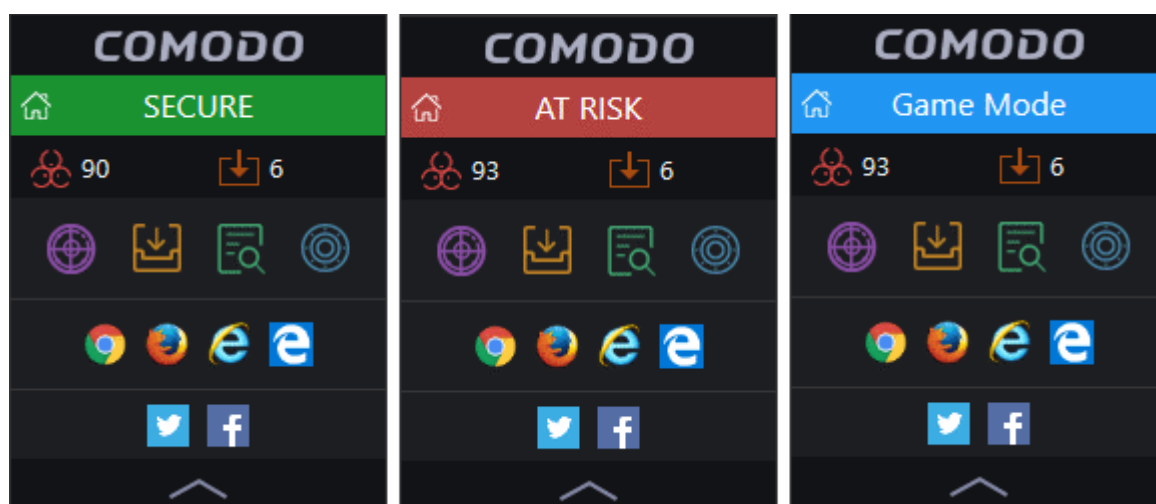
## 1.3.2. The Widget

The CCAV Widget is a handy control that provides at-a-glance information about your overall security, antivirus scans, sandbox status and more.

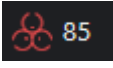

It contains,

- shortcuts for executing common CCAV tasks
- shortcuts for opening browsers in the sandbox
- links to popular social networking sites.

Right-click on the widget to enable or disable CCAV components and to configure various settings. See [The System Tray Icon](#) for more details.



- The color coded row at the top of the widget displays your current security status. Clicking on the top row opens the CCAV main interface.
- The second row displays AV and sandbox statistics:

- The first button  displays the number of threats detected by real-time and manual AV scans. Click the button to open the 'Detected Threats' interface, allowing you to take further actions. Refer to the section **Managing Detected Threats** for more details.
- The second button  displays the number of applications currently running inside the sandbox. Click the button to open the 'Sandboxed Applications' interface, which displays all currently sandboxed applications and allows you to take further actions. Refer to **The Sandbox** for more details.

The statistics row will be shown only if 'Show Statistics Pane' is enabled. This setting can be found by right-clicking on the system tray icon or the widget. Refer to **The System Tray Icon** for more details. (*Default = Enabled*)

- The third row contains shortcuts for the four common tasks (Scan, Run Virtual, View Logs and View Quarantine) available in the task bar in the main interface. Clicking the shortcut on the widget will run the task.

The 'Common Tasks' row is displayed only if 'Show Common Tasks Pane' is enabled under 'Widget' options of the CCAV tray icon or the widget right-click menu. Refer to section **The System Tray Icon** for more details. (*Default = Enabled*)

- The fourth row contains shortcuts for browsers installed on your computer. Click a browser icon to open the browser inside the sandbox for a secure browsing session. The browser window will have a green border around it as it is running inside the sandbox. Refer to **The Sandbox** for more details.


The row is displayed only if 'Show Browsers Pane' is enabled under 'Widget' section of the CCAV tray right-click menu or the widget right-click menu. Refer to the section **The System Tray Icon** for more details. (*Default = Enabled*)

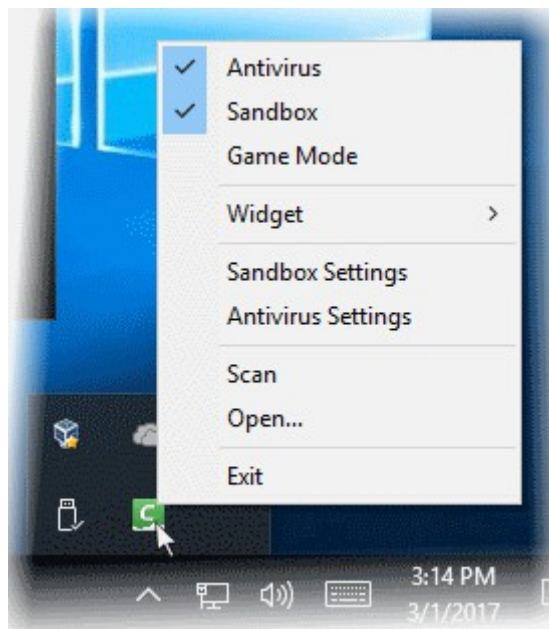
- The last row on the widget provides links to social networking sites.

This row is displayed only if 'Show Connect Pane' is enabled under 'Widget' section of the CCAV tray right-click menu or the widget right-click menu. Refer to the section **The System Tray Icon** for more details. (*Default = Enabled*)

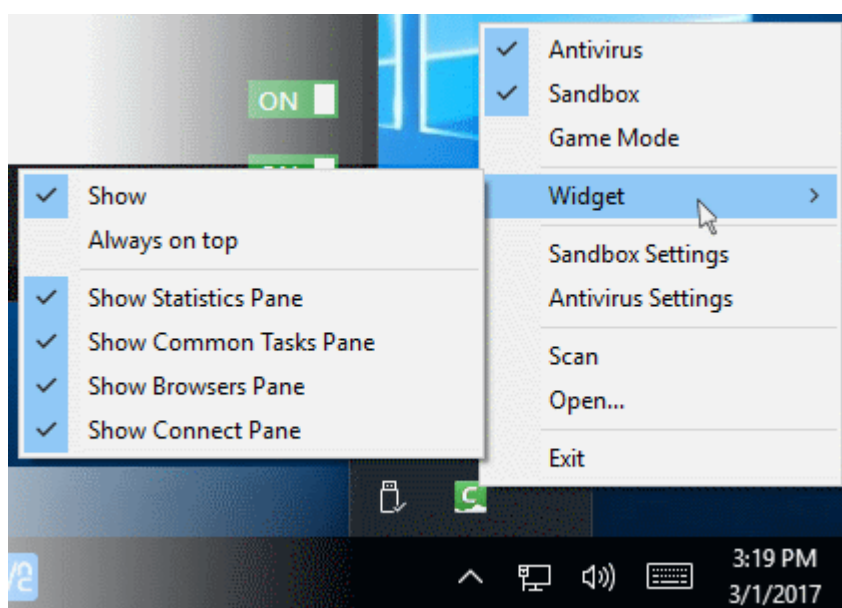
- The up arrow at the bottom allows you to collapse or expand the widget

## 1.3.3. 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. A check mark indicates that protection is on.
- **Sandbox** - Allows you to switch automatic sandboxing on or off. A check mark indicates that it is on.
- **Game Mode** - Allows to switch 'Game Mode' on or off. A check mark indicates that 'Game Mode' is on. Refer to the explanation of **Game Mode** in the previous section for more details.
- **Widget** - Allows you to select whether the Widget is to be displayed and which widget components are included:





- **Sandbox Settings** - Opens the 'Sandbox Settings' interface for configuring the behavior of Sandbox. Refer to the section '**Sandbox Settings**' for more details.
- **Antivirus Settings** - Opens the 'Antivirus Settings' interface for configuring the behavior of Antivirus. Refer to the section '**Antivirus Settings**' for more details.
- **Scan** - Opens the scan dialog. Refer to the section '**Scan and Clean your Computer**' for more details.
- **Open** - Opens the CCAV application.
- **Exit** - Closes the CCAV application.

For more information, see '**Lucky You Statistics**' section.

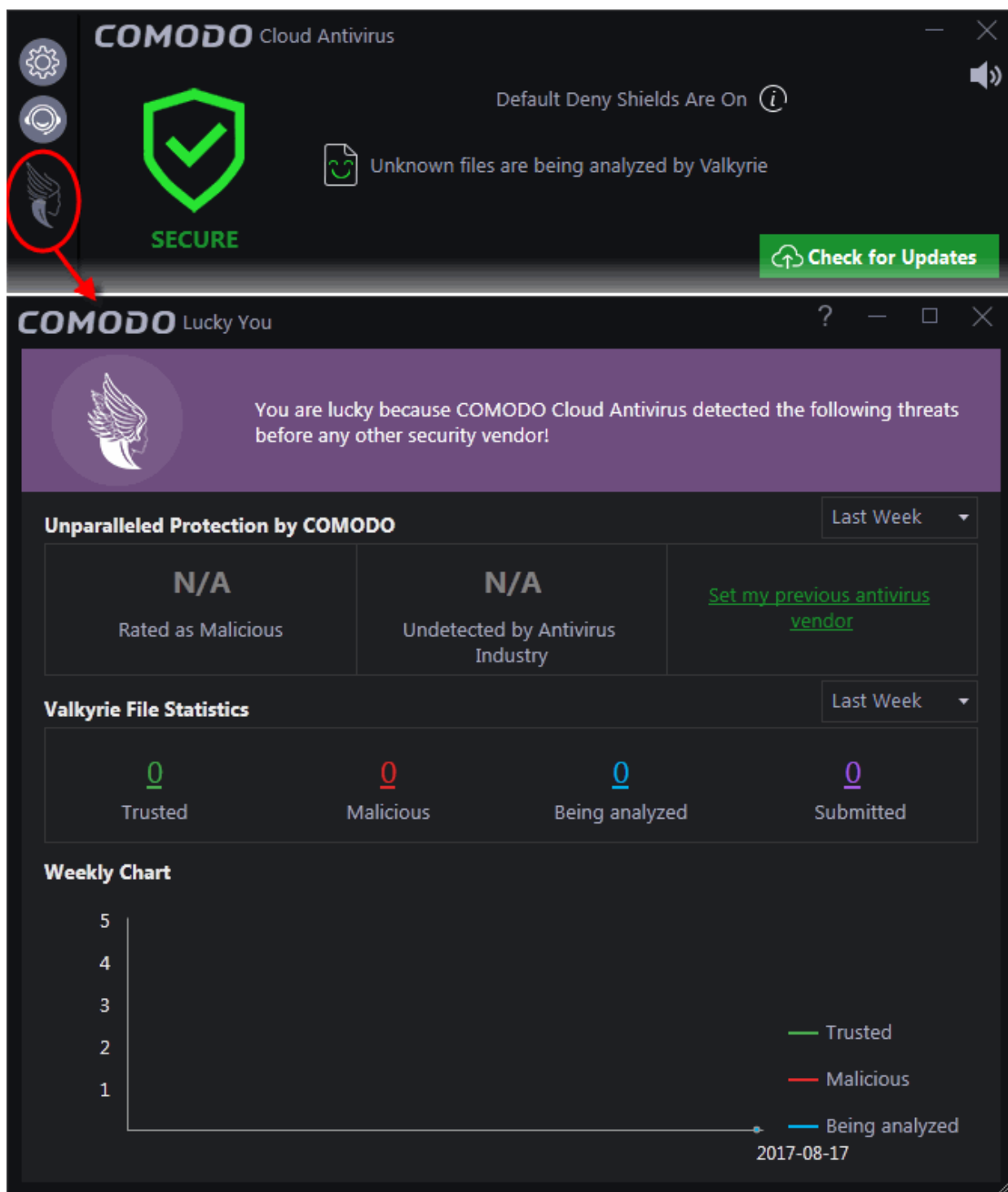
## 1.4. 'Lucky You' Statistics

The 'Lucky You' page displays unknown files found on your computer that were subsequently identified as malware by Comodo Valkyrie - before any other antivirus company detected them as such.

The 'Lucky' part is because traditional antivirus solutions would have allowed this malware to run on your computer. Fortunately, Comodo's Containment and Valkyrie technologies were on hand to protect you throughout. Containment keeps the files locked away in a secure sandbox environment where they can do no harm while Valkyrie tests whether or not the file is trustworthy. Note: Valkyrie results only show verdicts for items that have run in the sandbox.

You can also set your previous antivirus vendor so you can see how many threats were caught by CCAV that would previously have been missed.

- To view your 'Valkyrie Lucky You Statistics' details, click the 'Lucky You' icon on the menu icon bar.

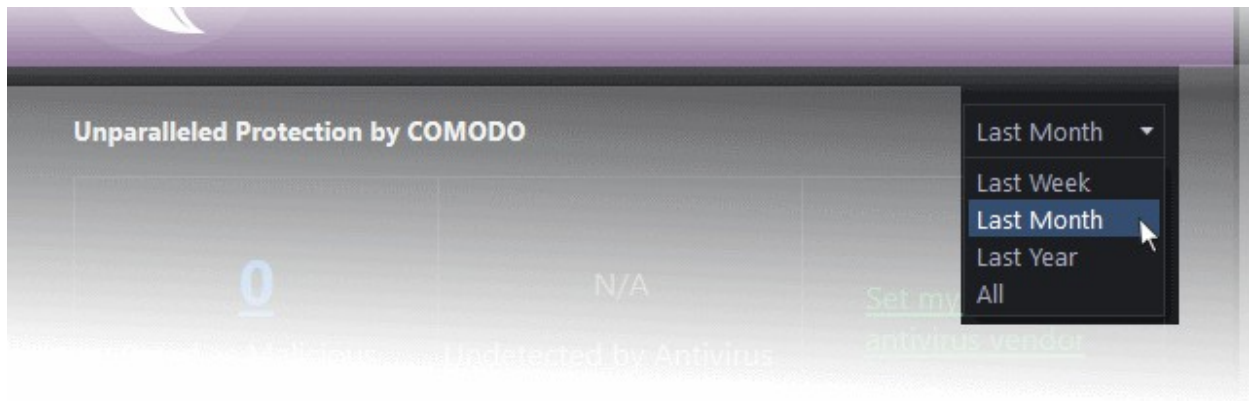


The 'Lucky You' page displays the total number of threats identified by Valkyrie from your computer within a selected period of time, with a comparison of threats that would be missed by other antivirus software vendors and statistics of files uploaded and their verdicts.

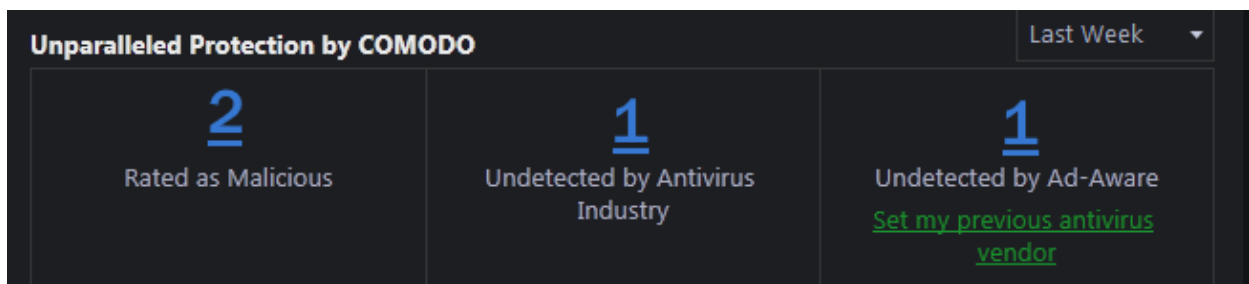
## Protection by Comodo

The first row displays the comparison of numbers of items identified as malicious by CCAV with other AV software, within a selected period of time.

- Choose the time period for which you wish to see the comparison from the drop-down at the left.

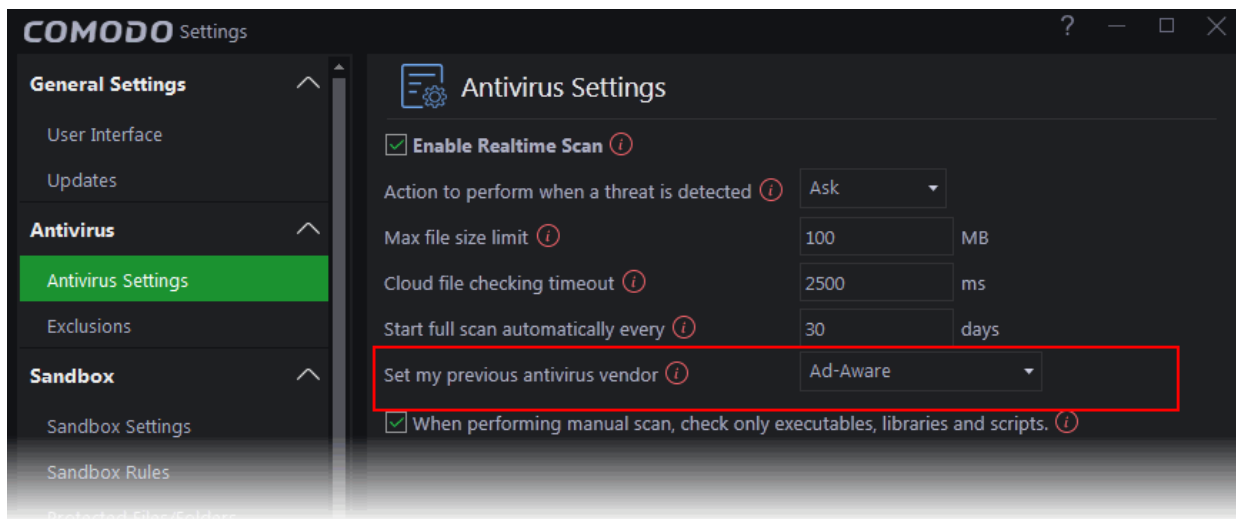


The comparison will be displayed.



- **Rated as Malicious** - Displays the total number of items identified as malicious from your computer by Valkyrie, within the chosen period of time. Click the number to view a list of all files identified as malware.
- **Undetected by Antivirus Industry** - Displays the number of malicious items from your computer, which are zero-day threats, discovered for the first time and have not been discovered yet by all other AV software vendors. Click the number to view a list of files identified as zero-day threats.
- **Undetected by your previous AV vendor** - Displays the number of malicious items identified from computer, which would not have been detected by your previous AV vendor. Click the number to view a list of files identified as threats exclusively by CCAV.

You should have specified your previous vendor to have this comparison from the 'Antivirus Settings' interface. If you haven't done yet, you can click the 'Set my previous antivirus vendor' link to open the 'Antivirus Settings' interface and choose the vendor from the 'Set my previous security vendor' drop-down.

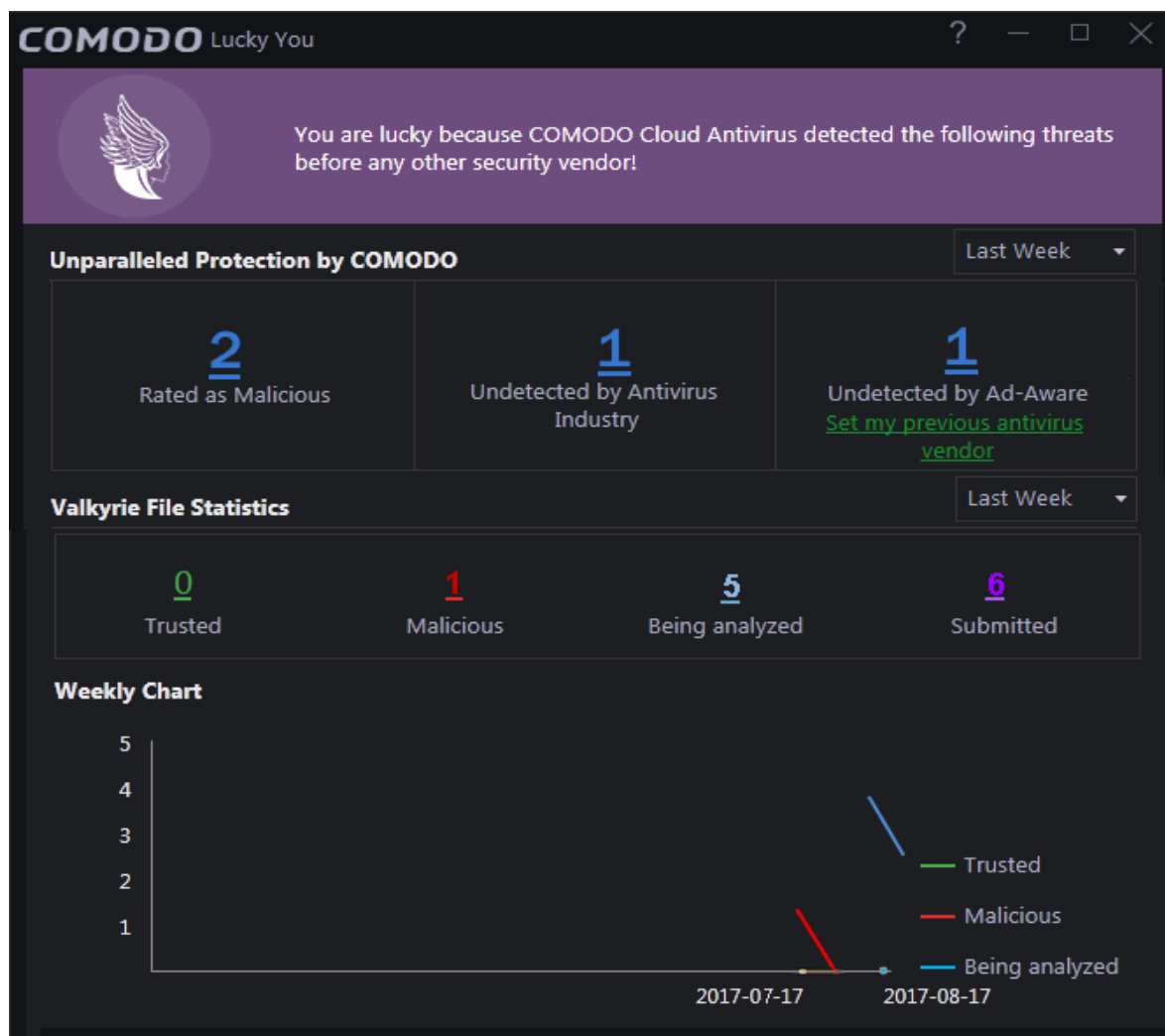


## Valkyrie File Statistics

The file statistics area displays a summary of numbers of items identified as malware, trusted and pending to be analyzed.

- Choose the time period for which you wish to see the comparison from the drop-down on the right.

The statistics for the chosen period will be displayed.



- Click on the numbers to display a list of files identified with respective verdicts.

The graph displays the comparison of statistics on weekly basis.

## 1.5. 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.

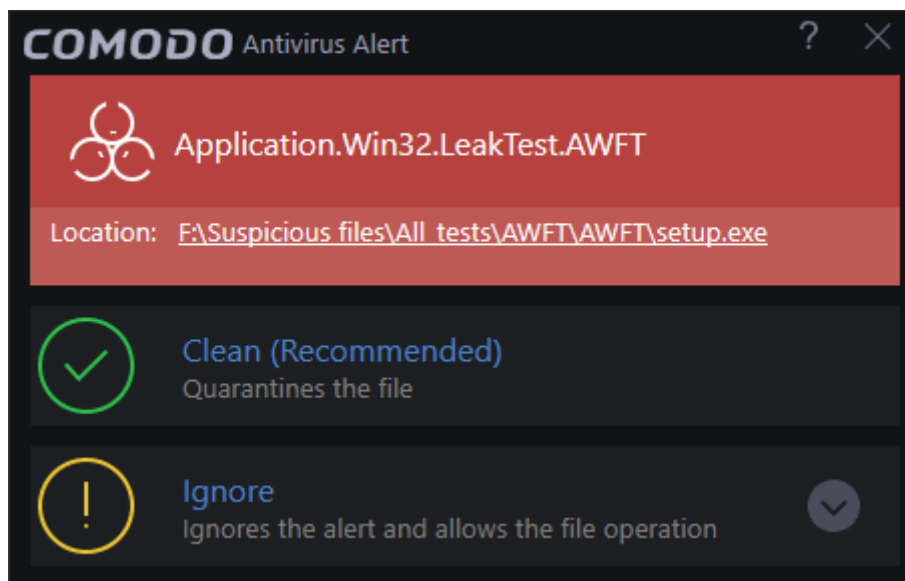
- **Antivirus Alerts** - Shown whenever virus or virus-like activity is detected. AV alerts will be displayed only when 'Enable Realtime Scan' is selected and the option 'Alert' for 'Action when threat is detected' is selected in **Real-time Scanner Settings**.
- **Sandbox Alerts** - Shown whenever an 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.
- **Valkyrie Alert and Notification**- Alerts are shown whenever CCAV receives a verdict on an 'Unknown' file submitted to Valkyrie. A notification will also be displayed if an unknown file is discovered but 'Submit unknown files automatically' is disabled in **Sandbox Settings**.
- **Browser Protection Alert** - Shown when an application attempts to change your browser settings for the first time (e.g. default search engine, home page, privacy setting etc). Browser Protection Alerts will be displayed only if the alert type is enabled under **Browser Settings Protection**.
- **Crash Encountered** - Shown whenever the antivirus module encounters a crash. You can help Comodo rectify the issue by sending the error report to Comodo for analysis.
- **Potentially Unwanted Applications (PUA) Detection** - Shown if you attempt to download a piece of software from a domain that is known to serve potentially unwanted software (PUA). A PUA is a piece of software that a user may not be aware is installed on their computer, and/or may have functionality and objectives that are not clear to the user. Example PUA's include adware and browser toolbars.

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

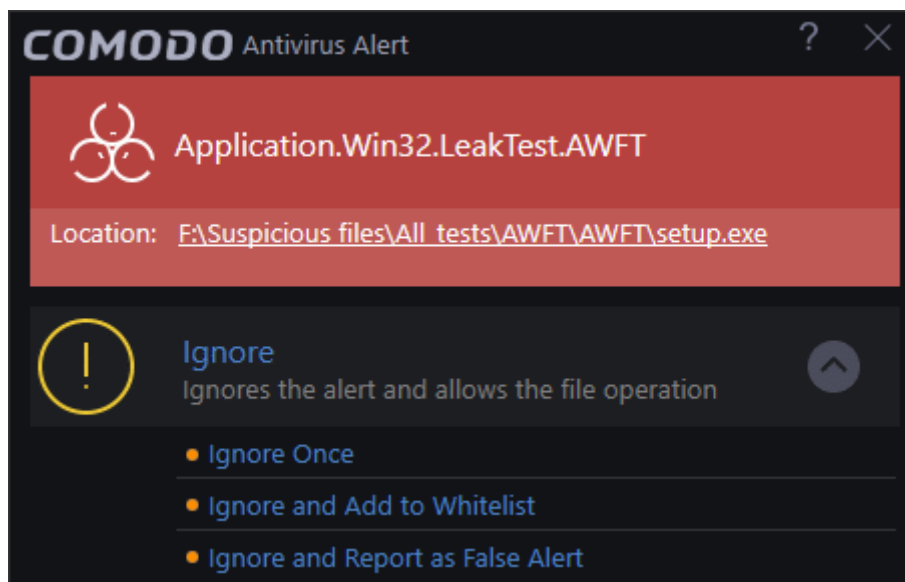
Comodo Cloud Antivirus generates an 'Antivirus' alert whenever a virus or virus-like activity is detected on your computer. The alert contains the name of the virus detected and the location of the file or application infected by it. Within the alert, you are also presented with response-options such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

**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**.



The following response-options are available:

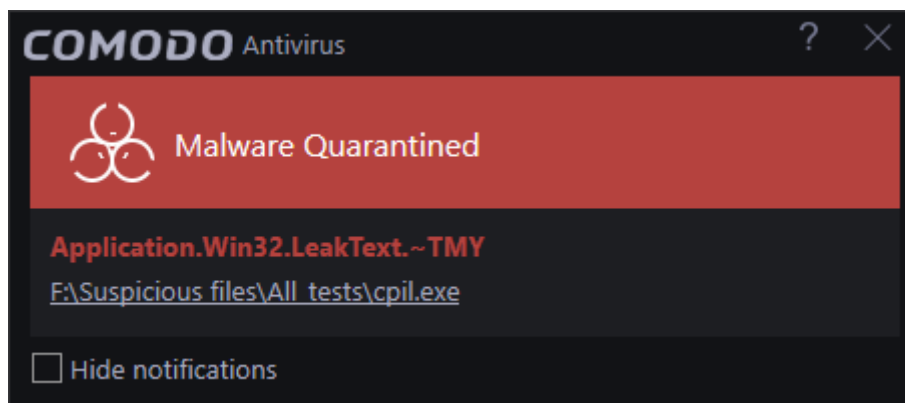
- **Clean** - Disinfects the file if a disinfection routine exists. If no routine exists for the file then it will be moved to Quarantine. If desired, you can submit the file/application to Comodo for analysis from the **Quarantine** interface. Refer to **View and Manage Quarantined Items** for more details on quarantined files.
- **Ignore** - Allows the process to run and does not attempt to clean the file or move it to quarantine. Only click 'Ignore' if you are absolutely sure the file is safe. Clicking 'Ignore' will open three further options:



- **Ignore Once** - The file is allowed to run this time only. Another alert will be shown if the file attempts to execute on future occasions.
- **Ignore and Add to Whitelist** - The file is allowed to run and is added to **Trusted Applications**. - effectively making this the 'Ignore Permanently' choice. No alert is generated if the same application runs again.
- **Ignore and Report as False Alert** - Allows the process to run and the file will be **submitted as false positive** and 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.

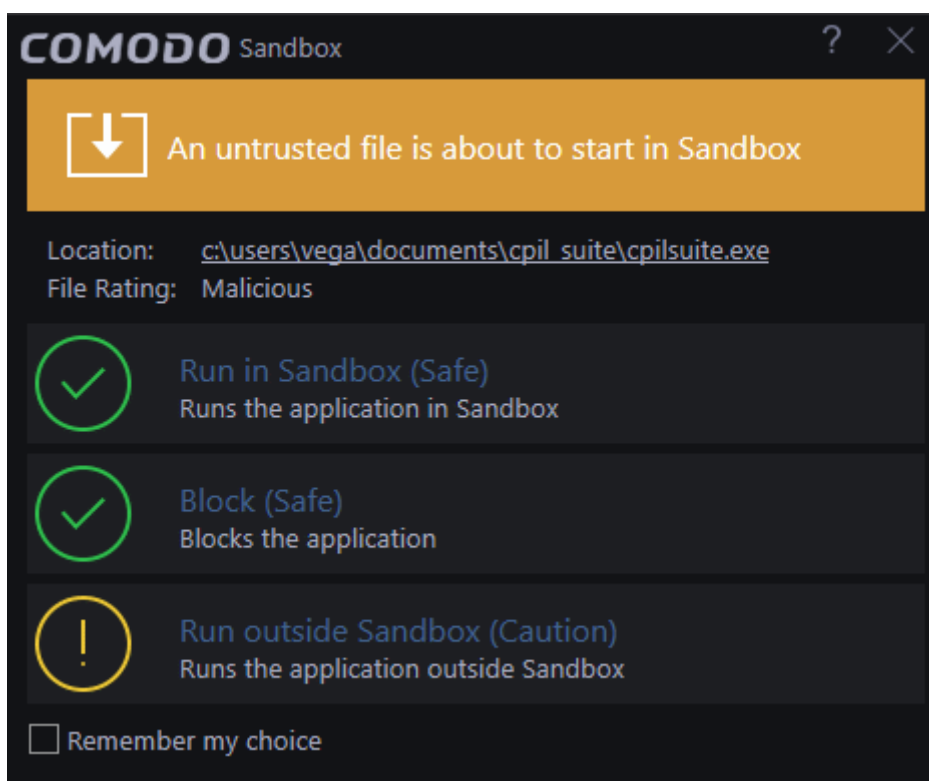


Please note that these antivirus notifications will be displayed only when you have chosen either 'Block' or 'Quarantine' for the option 'Action when threat is detected' in **Real-time Scanner Settings**, and 'Show notifications' check box is enabled in **'General Settings' > 'Customize User Interface'**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

- If you do not want these notifications to be displayed in future, select the 'Hide notifications' checkbox.

## 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'.



**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**.

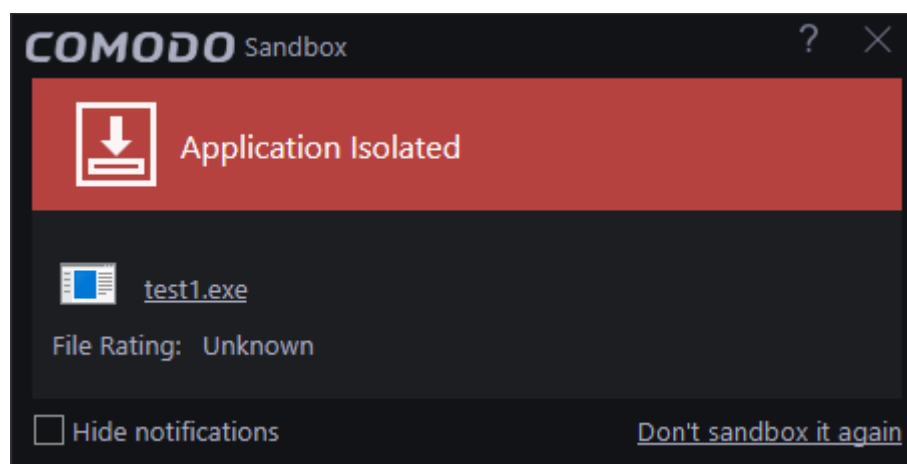
- **Run in Sandbox** - The application will be run inside the sandbox. This is useful, for example, if you wish to

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.

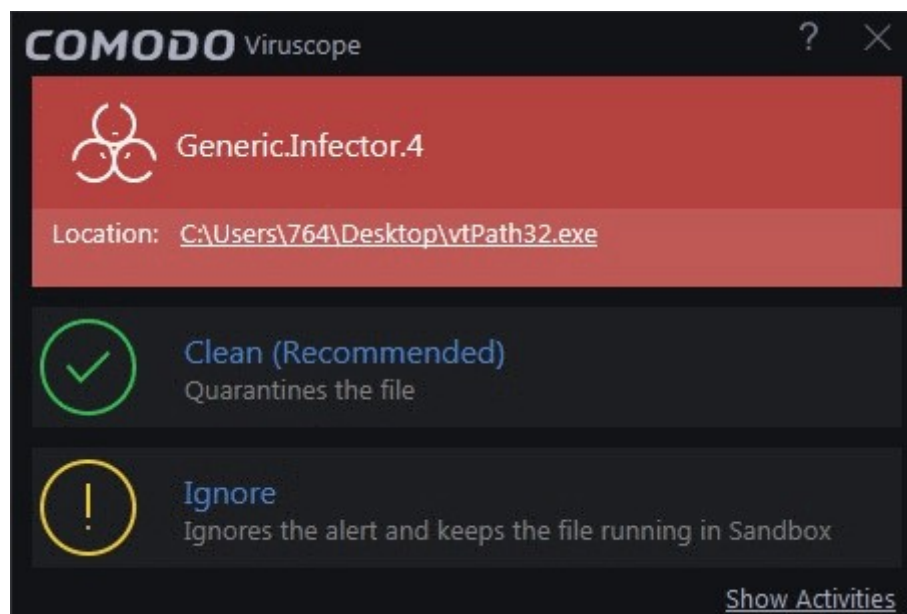
## Answering a Viruscope Alert

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.

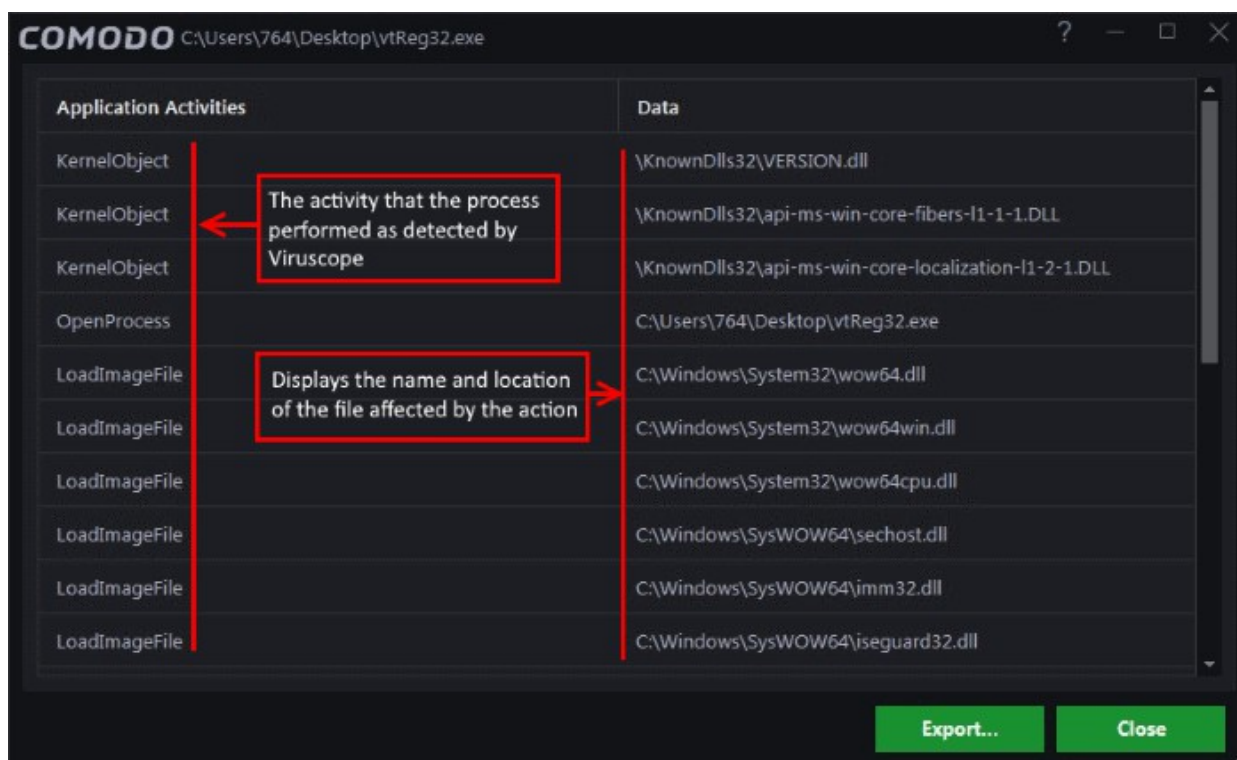
Please read the following advice before answering a Viruscope alert:

1. Carefully read the information displayed in the alert.





- 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.



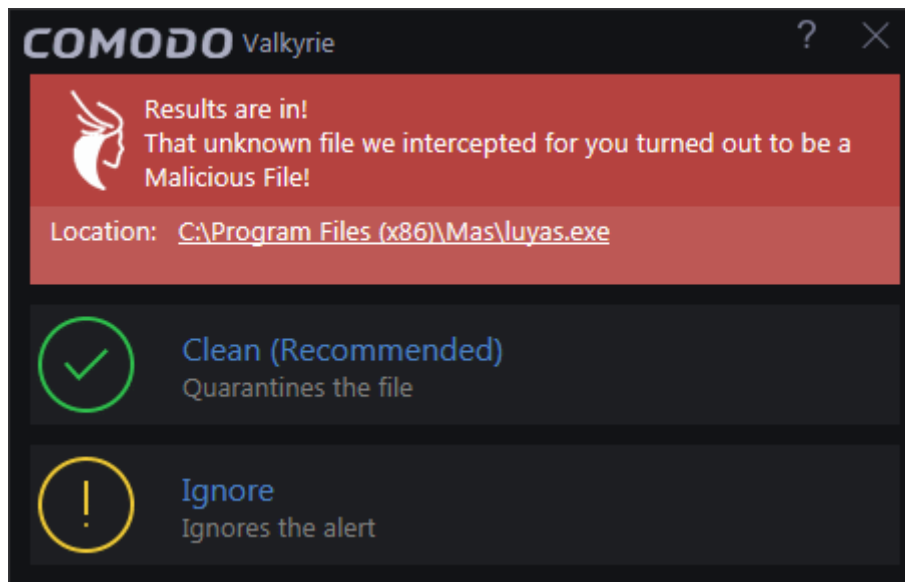
## Column Descriptions

- 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.

## Answering a Valkyrie Alert

These alerts are shown when an unknown file is found to be malicious after analysis by Comodo Valkyrie. Users have the option to automatically upload unknown files which are running in the sandbox. Users can also manually upload files to Valkyrie for analysis.

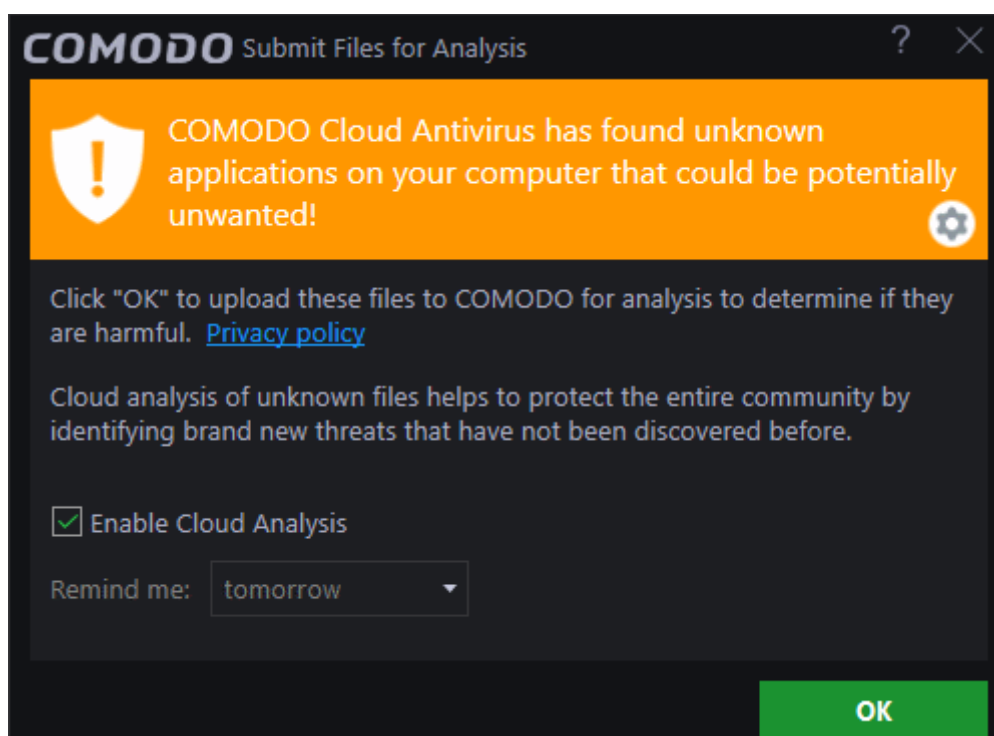


The following response-options are available:

- **Clean** - Moves the file to 'Quarantine'. Refer to [View and Manage Quarantined Items](#) for more details on quarantined files.
- **Ignore** - Allows the file and does not attempt to clean the file or move it to quarantine. The file will be identified as Malicious in the future scans.

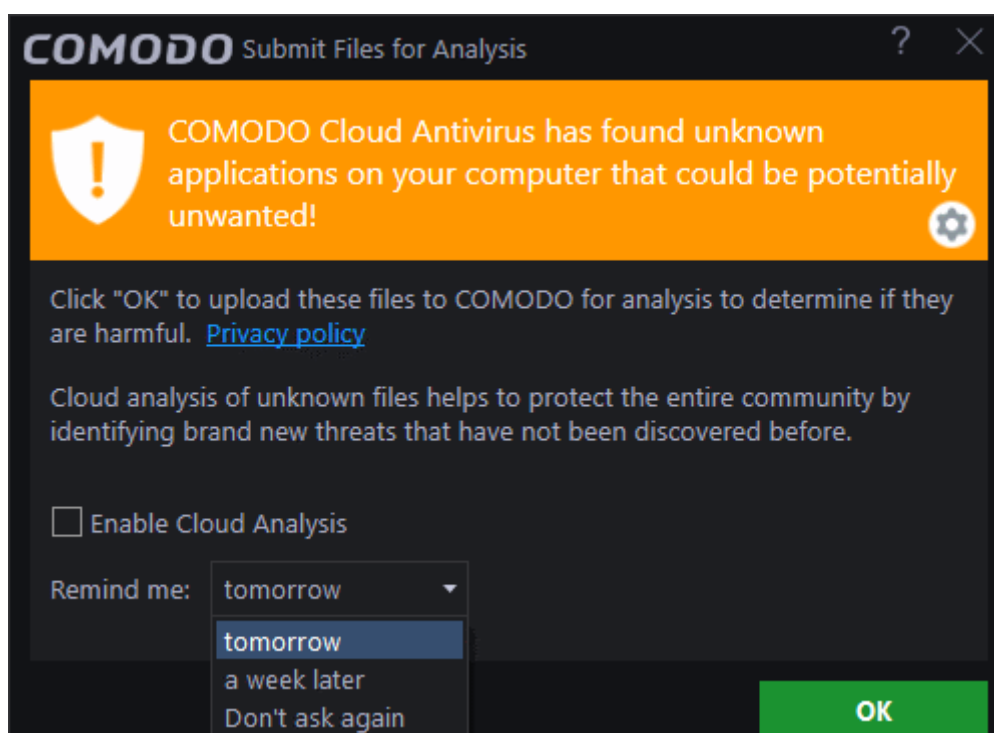
## Valkyrie Notification

The following notification will be displayed if an unknown file is detected but you have chosen to disable 'I want to enable 'Cloud Based Behavioral Analysis' of unrecognized programs ...' in [Sandbox Settings](#).



The 'Enable Cloud Analysis' check box will be enabled by default. If you click 'OK' with this selected then these notifications will no longer be shown and unknown files will be automatically uploaded to Valkyrie in future. The 'I want to enable "Cloud Based Behavioral Analysis" of unrecognized programs...' box in **Sandbox Settings** will be enabled.

If you choose not to enable cloud analysis, you have the option to be reminded daily, once a week or never.

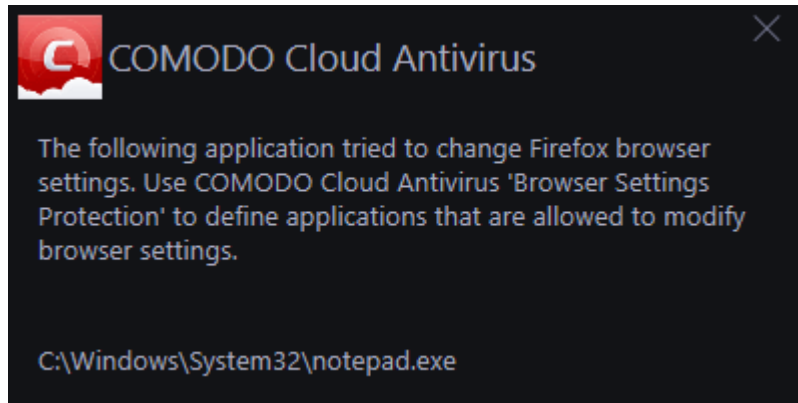


To select an option, deselect 'Enable Cloud Analysis' check box, select the option and click 'OK'. If you select the last option, 'Don't ask again', the notification will not be displayed anymore. If this option is selected then in order to submit unknown files automatically to Valkyrie, you have to enable the option in the **'Sandbox Settings'** interface. Please note you can also submit files manually by right-clicking on a file, then selecting 'Comodo Cloud Antivirus' >

'Submit to Valkyrie' from the context sensitive menu.

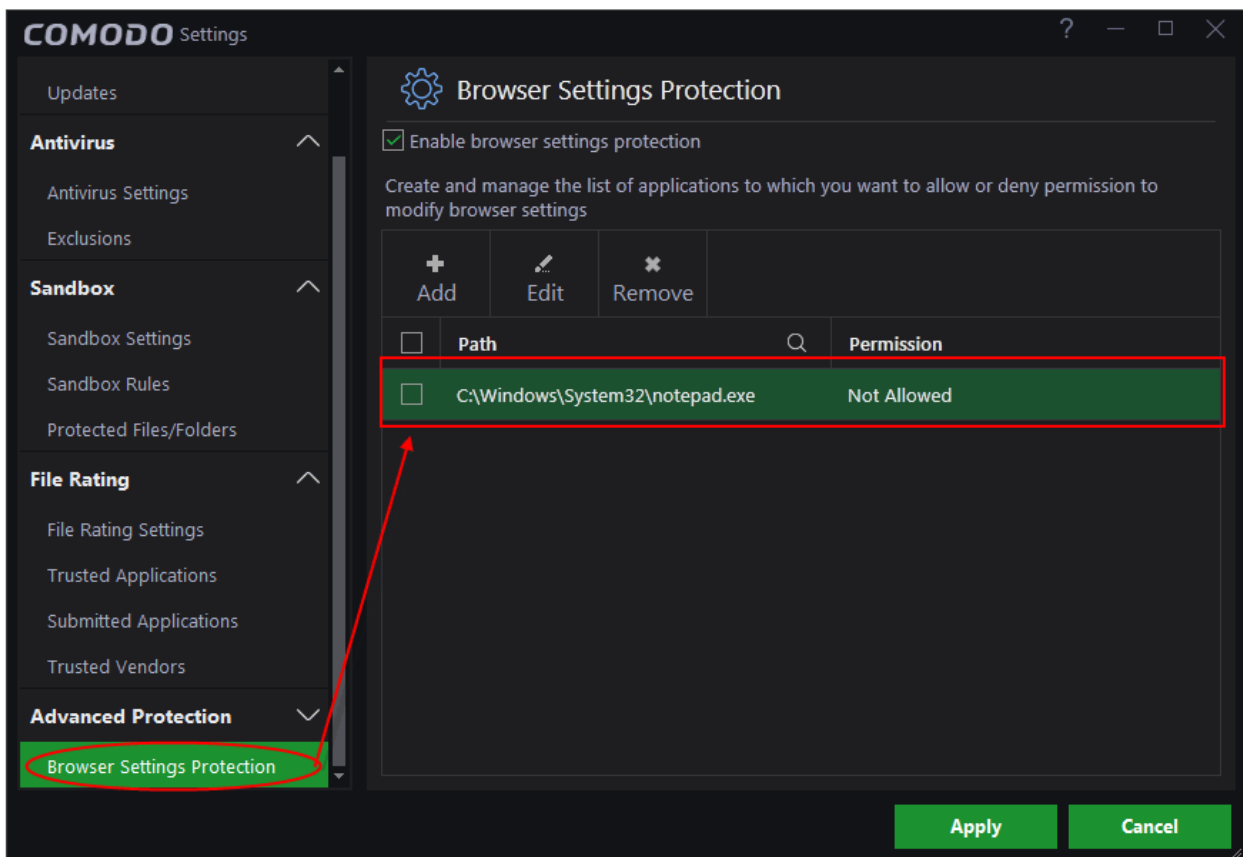
## Browser Protection Alert

CCAV generates a Browser Protection Alert when an application tries to modify your browser settings for the first time. All such attempts by an application will be blocked but the alert message will be shown only for the first attempt for every application.



The alert shows the name of the application that attempted the modification.

Blocked applications will automatically be added to the 'Browser Settings Protection' area of CCAV. You can subsequently change access permissions for each application from this interface. You can also use this interface to manually add applications that you want to restrict.

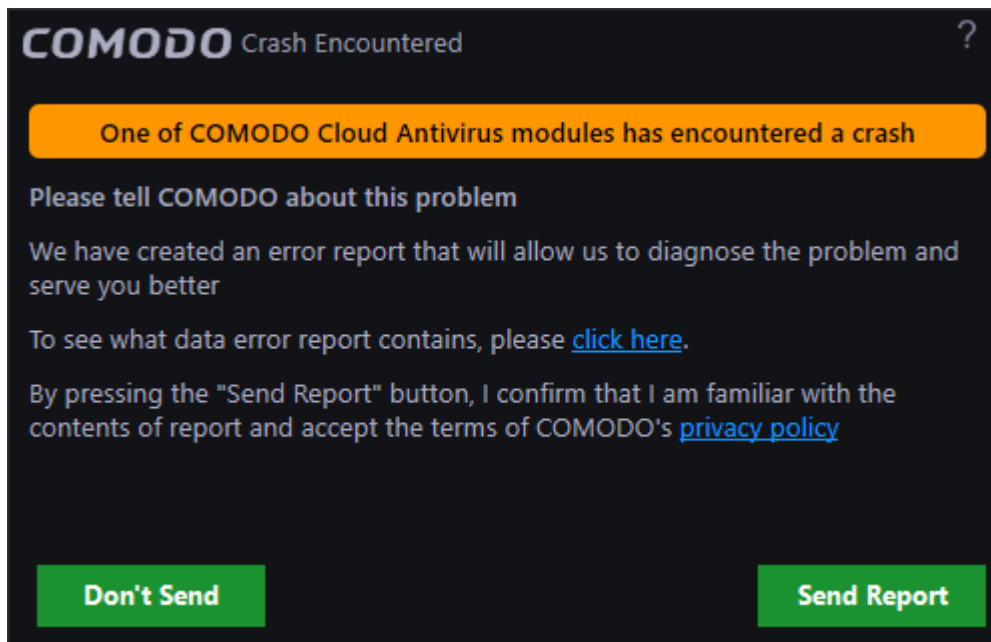


**Note:** Browser Protection Alerts will be displayed only if the option 'Enable browser protection settings' is enabled

under **Browser Settings Protection**.

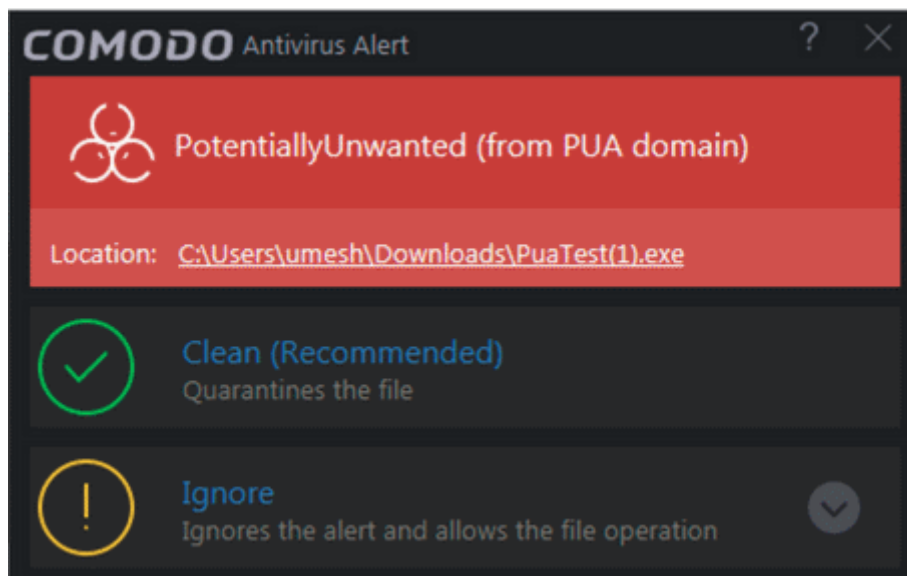
## Answering a Crash Reporting Alert

This alert is shown when one of the CCAV modules encounters a crash. CCAV generates a report that you may choose to send to Comodo to help improve the performance of the application.



## Answering a Potentially Unwanted Application detection Alert

These are alerts that are shown when a potentially unwanted application is detected by CCAV. This option is enabled by default in 'File Rating' settings.



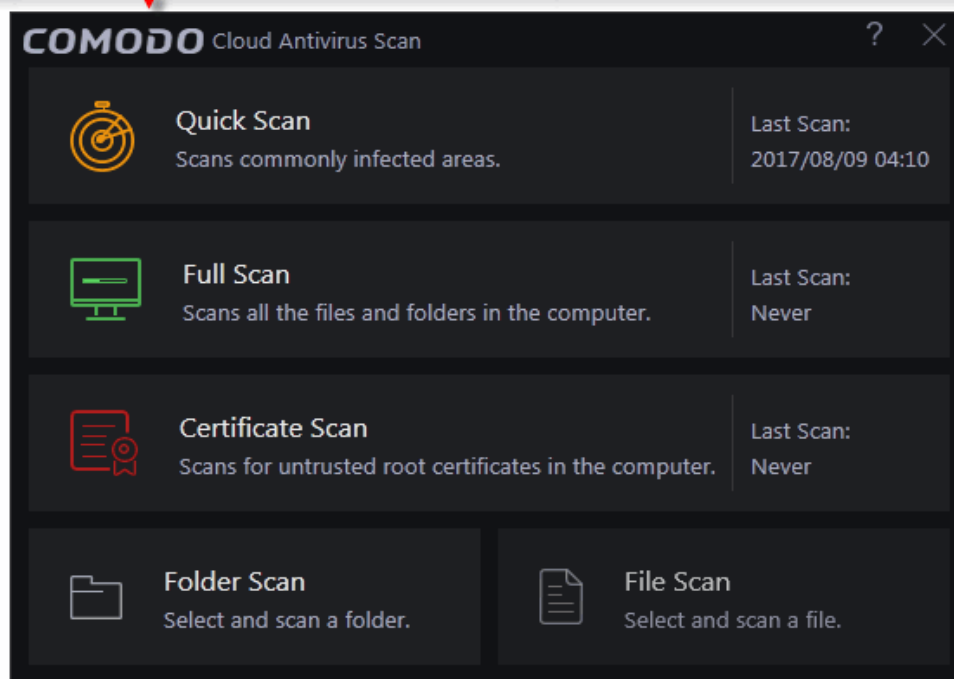
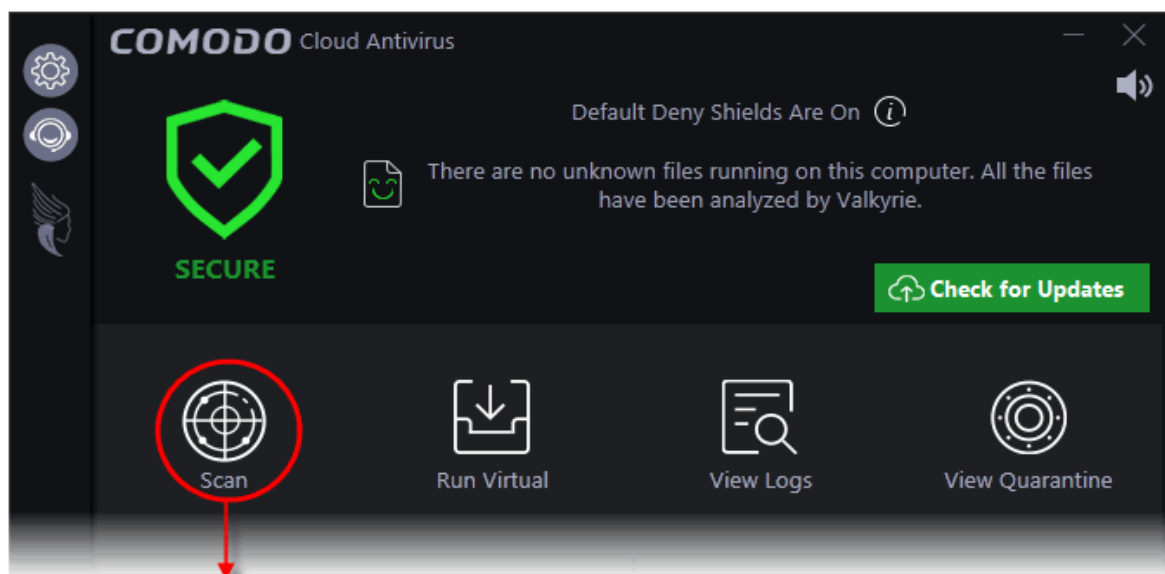
Refer to **File Rating Settings** to find out more.

## 2. Scan and Clean your Computer

Comodo Cloud Antivirus leverages multiple security technologies 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. CCAV scans any file you open and immediately deletes or quarantines it if it is malware. 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 scan individual items.

To open the 'Scan' interface

- Click 'Scan' from the 'Tasks Bar'.



OR

- Click the Scan  shortcut button from the widget

OR

- Right-click on the CCAV system tray icon

There are multiple types of antivirus scans that can be run from the 'Scan' interface. The following sections explain more about each scan type:

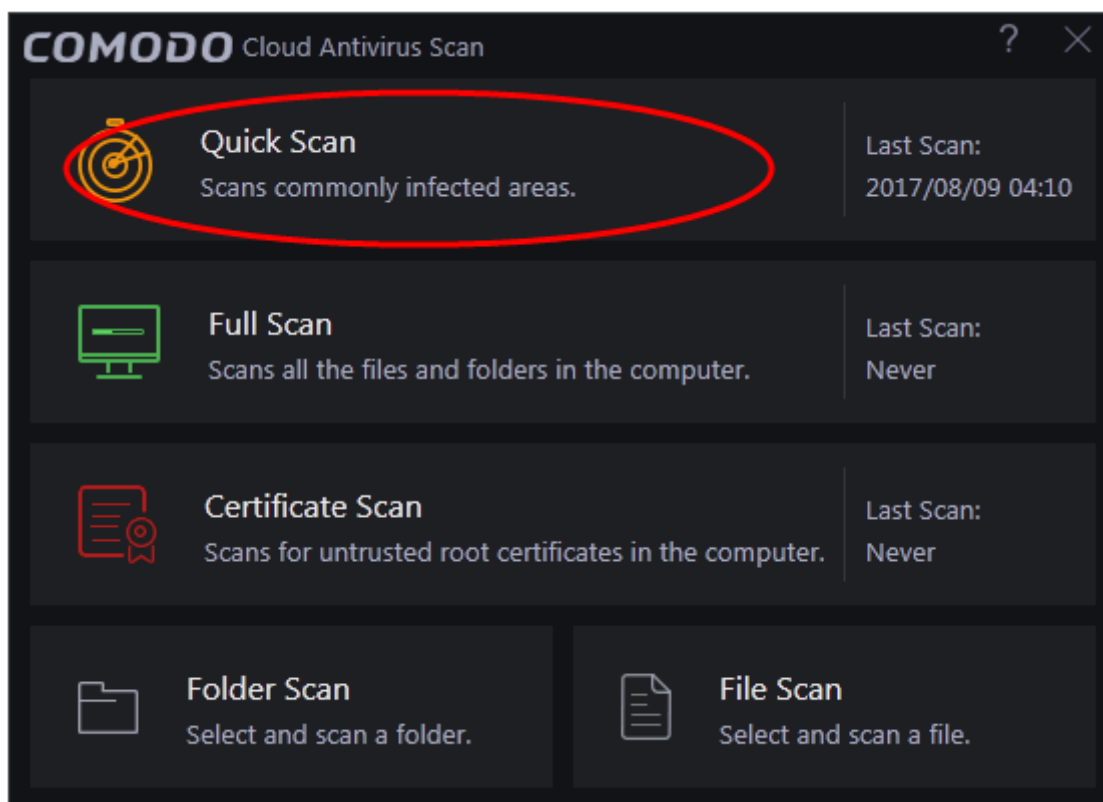
- **Run a Quick Scan**
- **Run a Full Computer Scan**
- **Run a Certificate Scan**
- **Run a Custom Scan**
  - **Scan a Folder**
  - **Scan a File**
- **Processing Infected Files**
- **Managing Detected Threats**
- **Viewing Valkyrie Analysis Results**

## 2.1. Run a Quick Scan

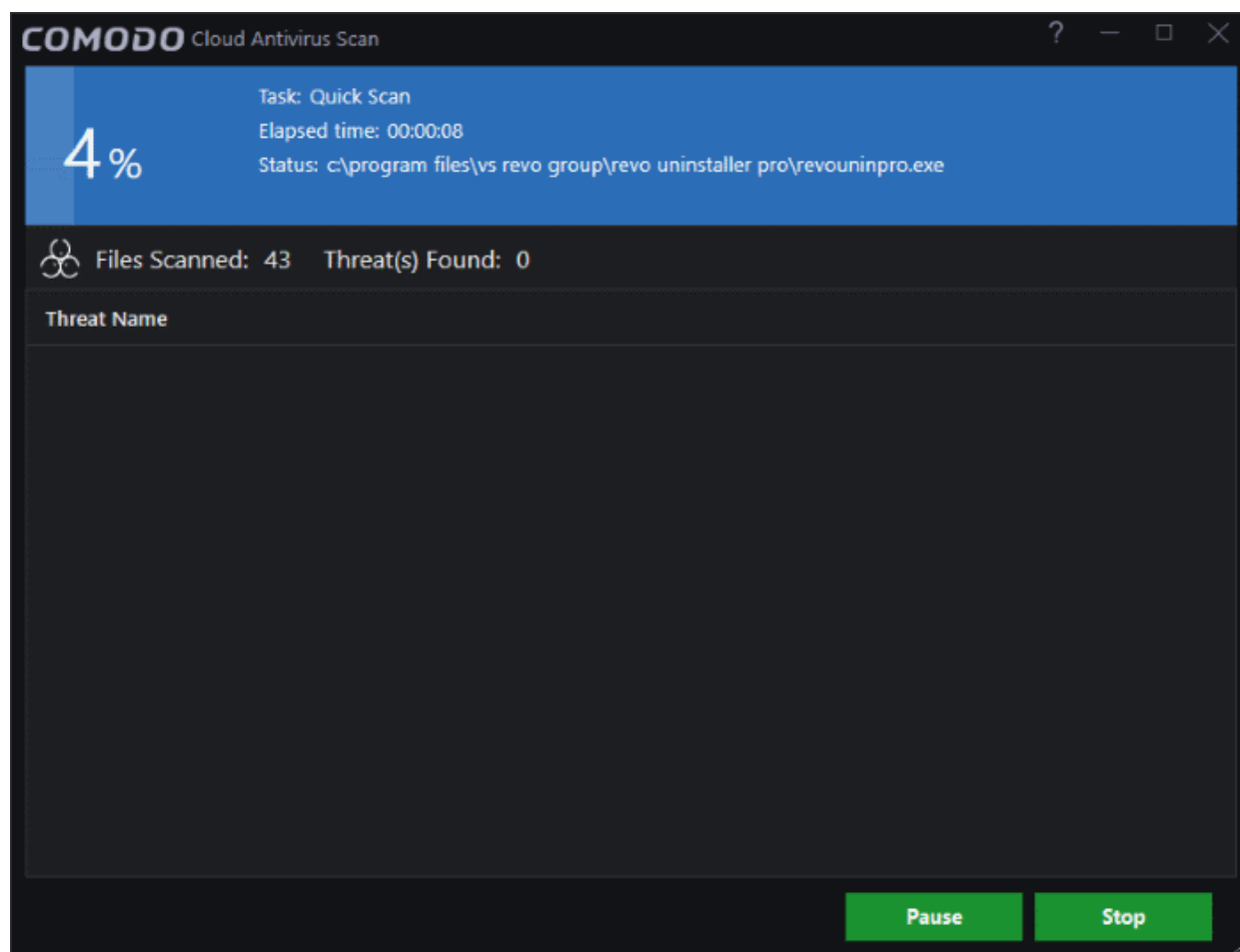
The 'Quick Scan' feature enables you to quickly scan those important areas of your computer which are highly prone to infection. Areas scanned include system memory, auto-run entries, hidden services, boot sectors and other significant areas like important registry keys and system files. These areas 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 'Task bar' or clicking on the scan button from the widget > 'Quick Scan'



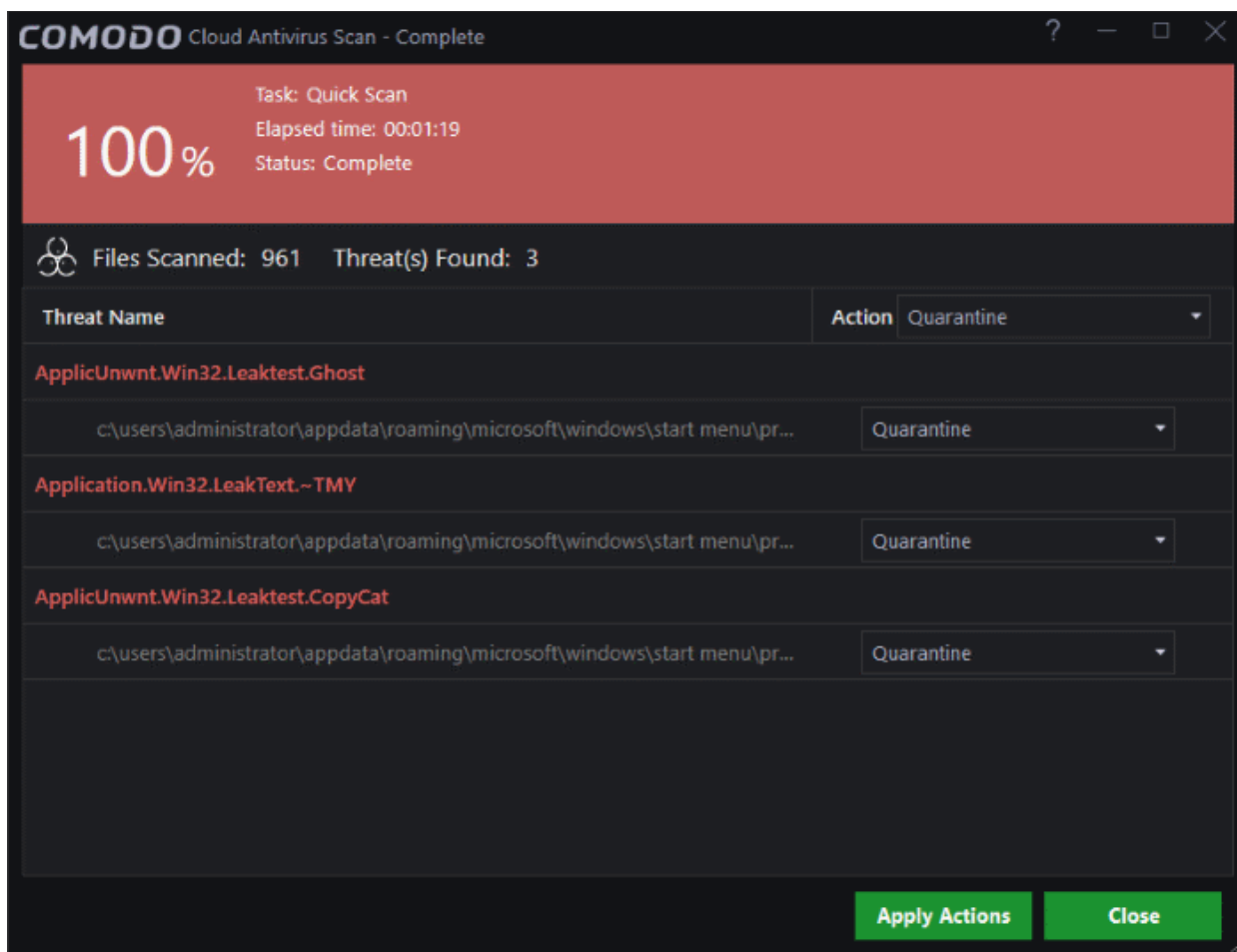
The scanner will start and the scan progress will be displayed:



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

The results window will be displayed on completion of the scanning process.





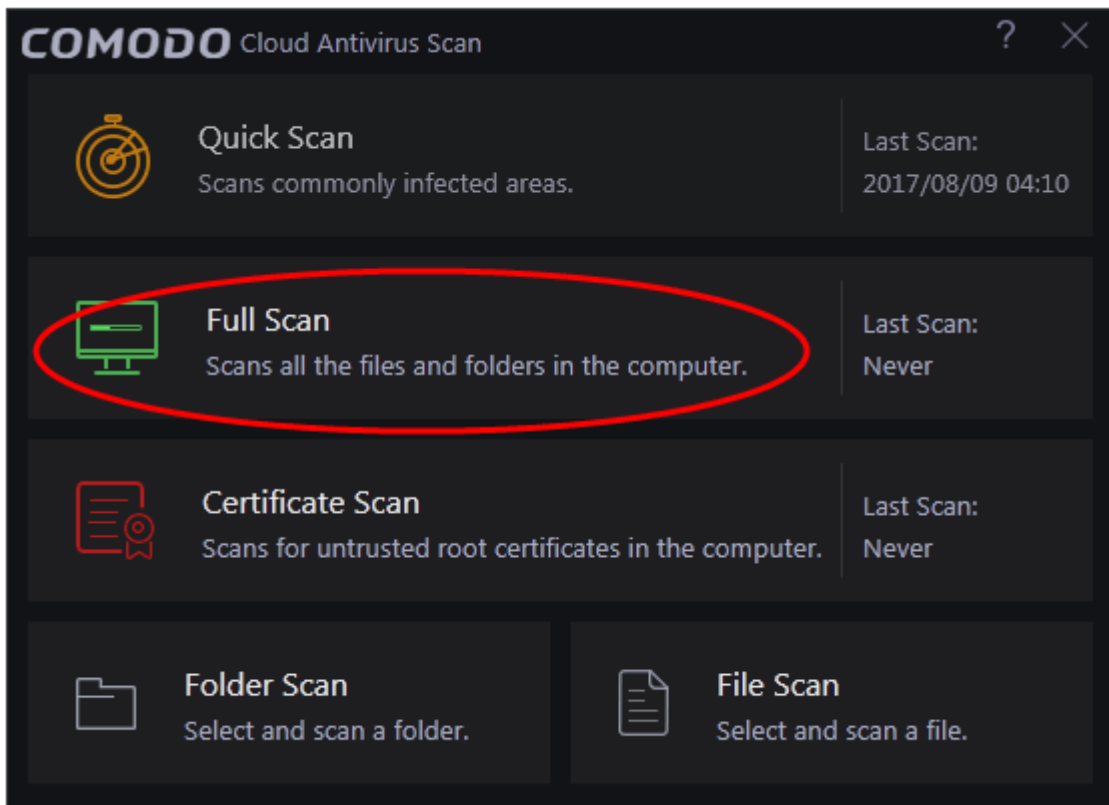
The results window shows the list of objects scanned and the number of threats (Viruses, Rootkits, Malware). Use the drop-down menu to choose whether to clean, quarantine or ignore the threat. Refer to [Processing the infected files](#) for more details.

## 2.2. Run a Full Computer Scan

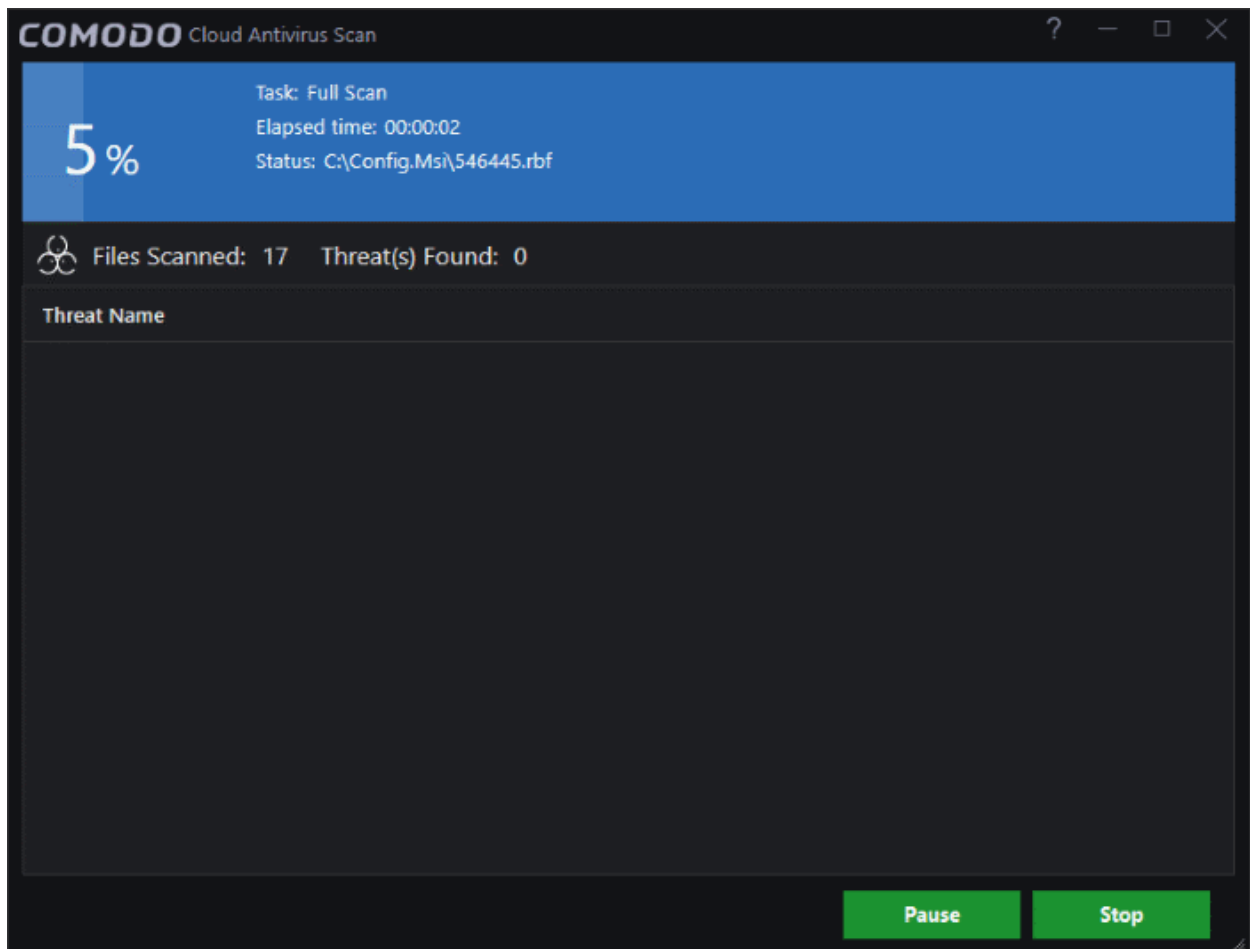
A 'Full System Scan' scans every local drive, folder and file on your system. External devices such as USB drives, storage drives and digital cameras will also be scanned.

### To run a Full Computer Scan

- Open the 'Scan' interface by clicking 'Scan' on the CCAV home screen, or by clicking on the scan button on the widget
- Choose 'Full Scan' from the options:

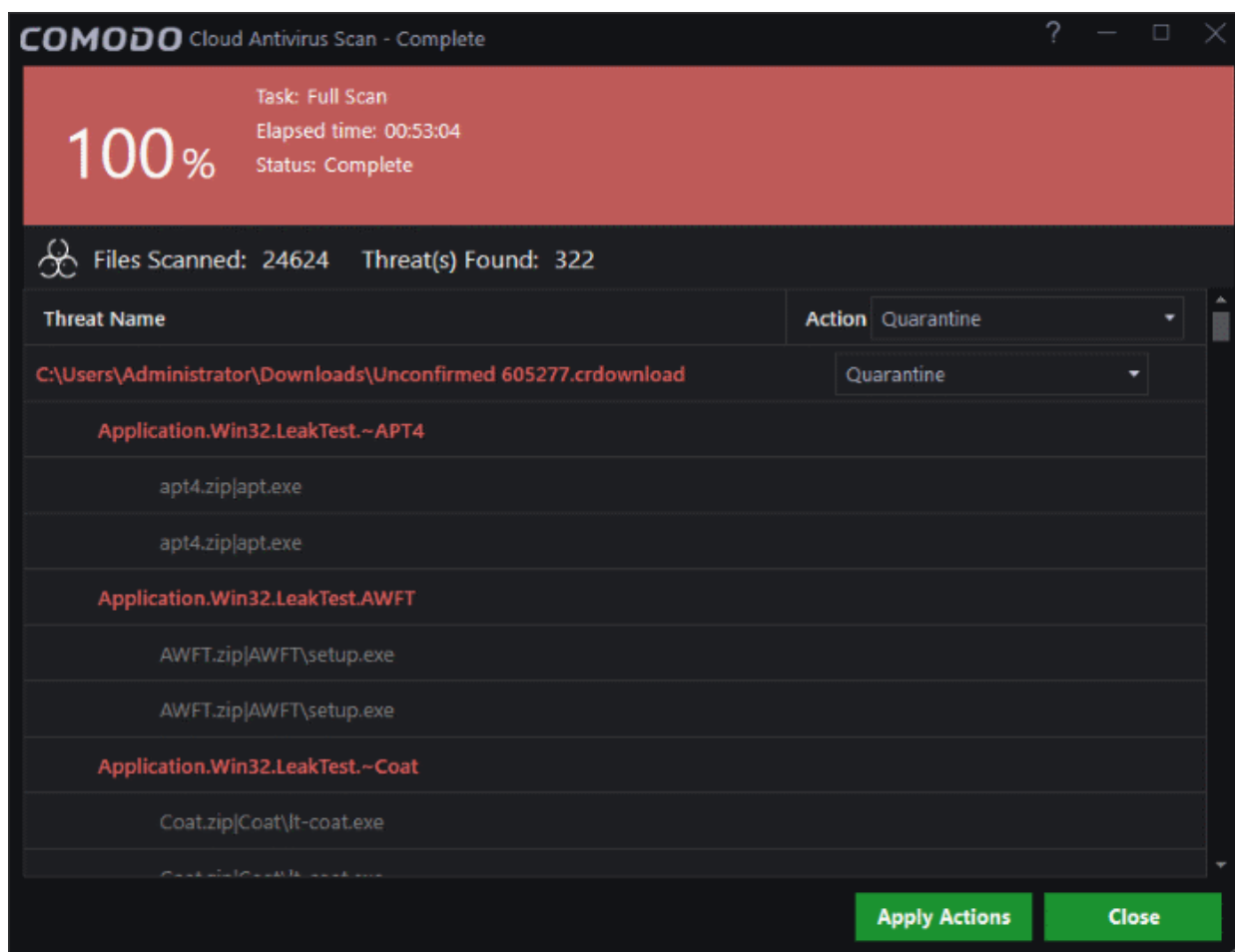


The scanner will start and the scan progress will be displayed:



- 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.



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 quarantine files or ignore the threat based in your assessment. Refer to [Processing the infected files](#) for more details.

## 2.3. Run a Certificate Scan

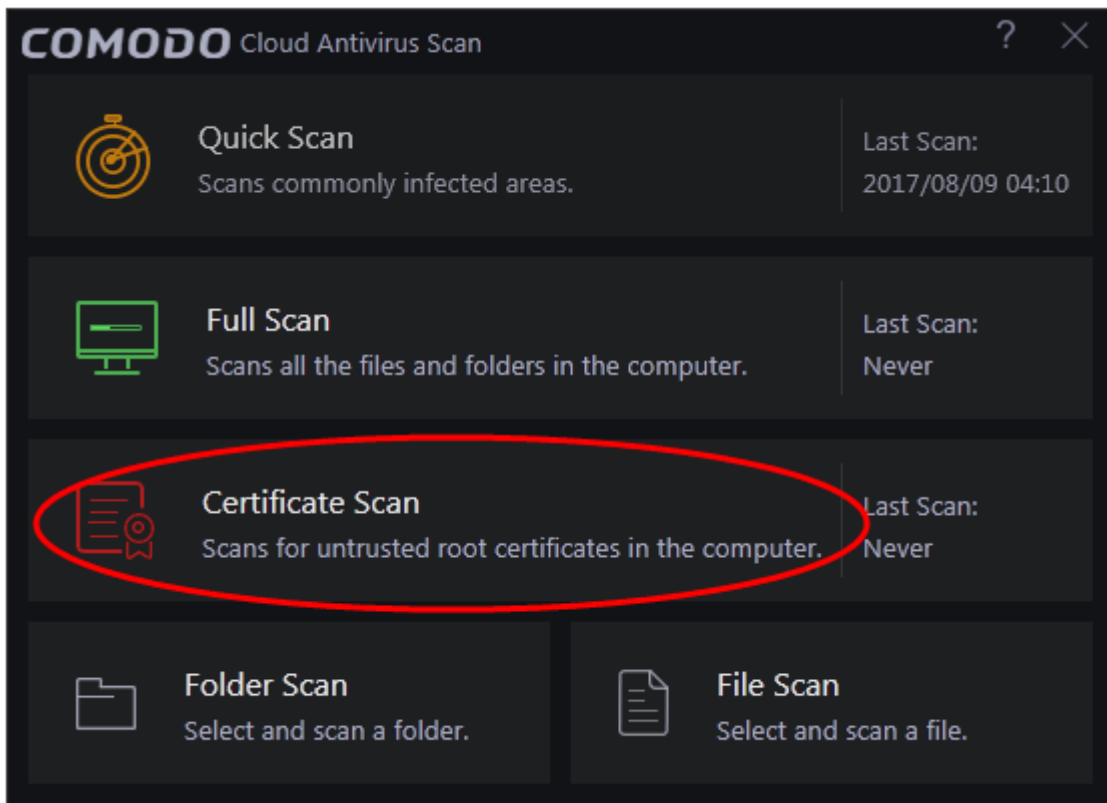
The 'Certificate Scan' feature checks all root SSL certificates on your computer against an internal trusted store of roots.

This helps,

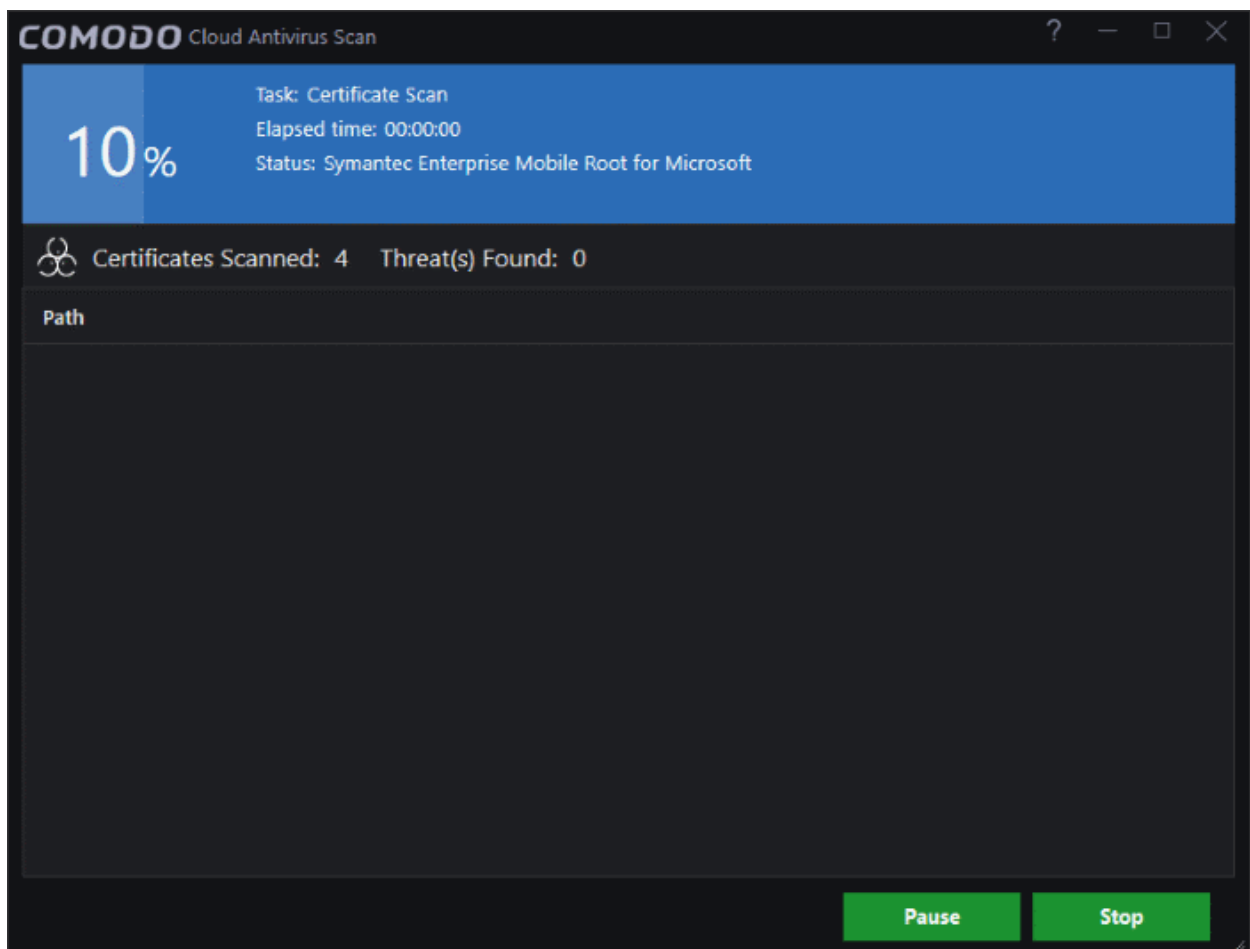
- protect you from malware that installs fraudulent root certificates on your computer in order to trick you into thinking a phishing website is the real site (a man-in-the-middle attack).
- the certificate scan feature performs a check similar to that found in [Comodo Internet Security Essentials](#).

### To run a Certificate scan

- Open the 'Scan' interface by clicking 'Scan' on the CCAV home screen, or by clicking on the scan button on the widget
- Choose 'Certificate Scan' from the options:

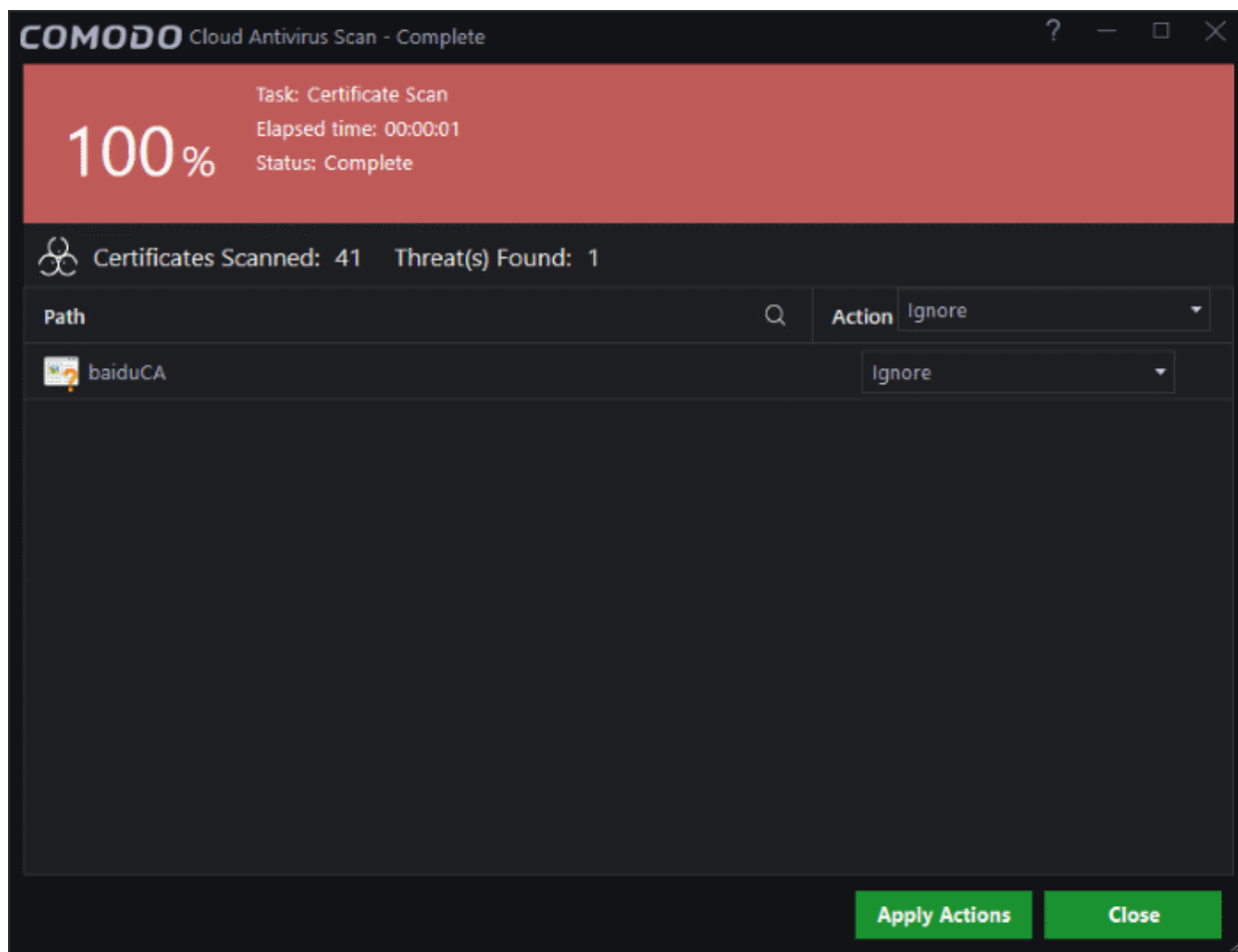


The scanner will start and scan certificates against the list of trusted store of roots:



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

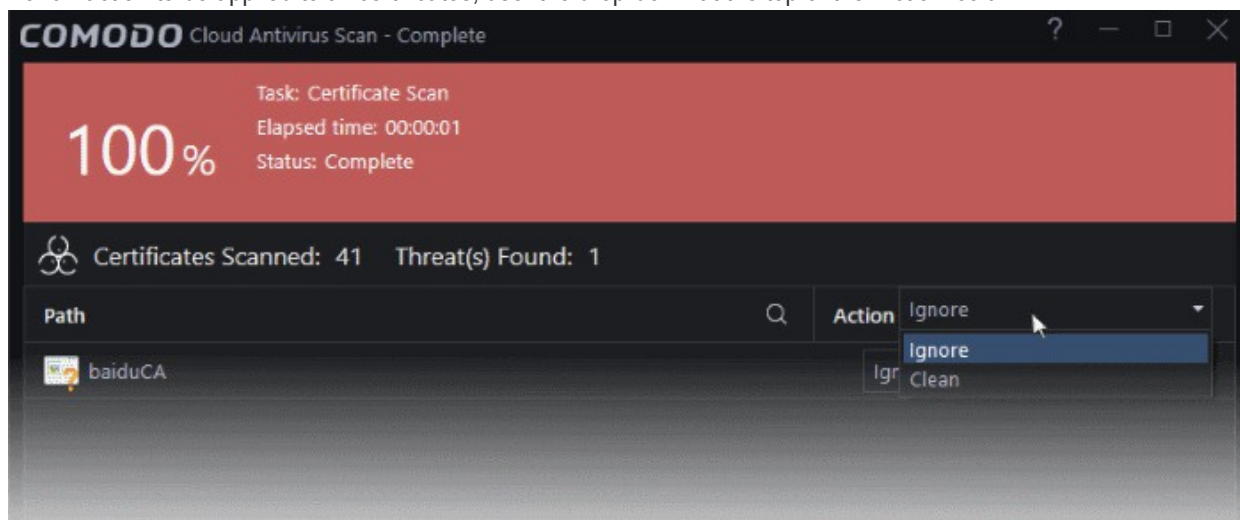
The results window will be displayed when the scan is finished:



The results screen shows the number of certificates scanned and the number of threats detected. In this case, a threat is an untrusted certificate.

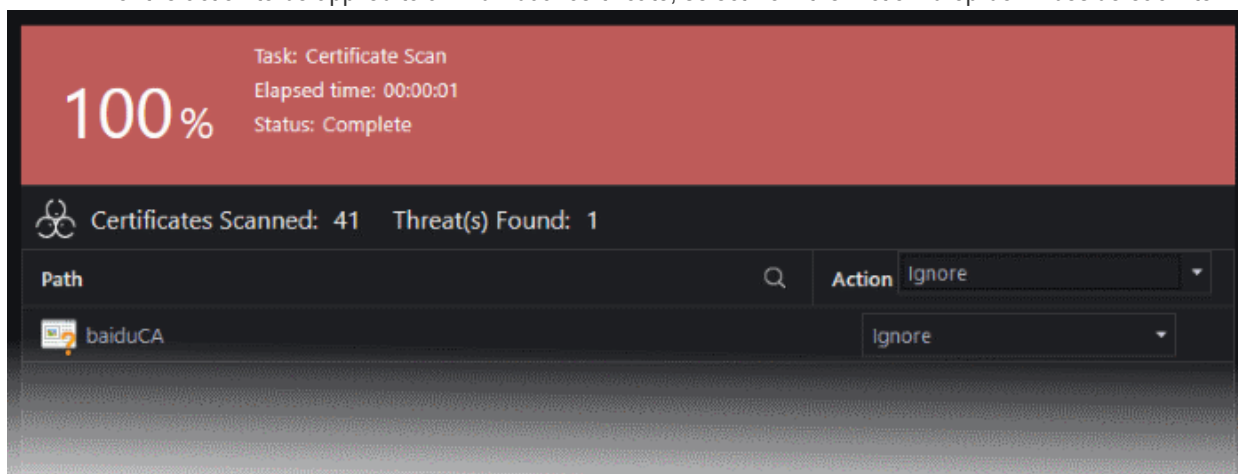
- **Path:** The name of the untrusted certificate.
- **Action:** You can choose to ignore or clean the certificate. Cleaning will remove the certificate from your system.

For an action to be applied to all certificates, use the drop-down at the top of the 'Action' column:

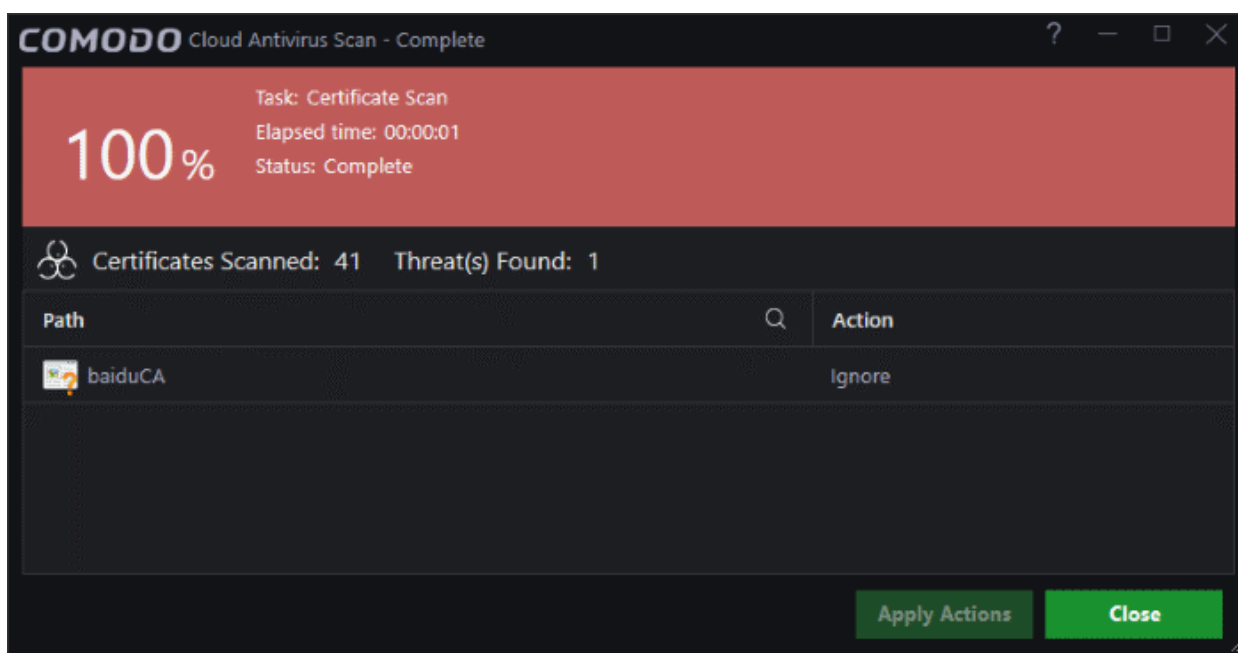


- **Ignore** - If you want to ignore the untrusted certificate, select 'Ignore'. The certificate will be ignored only once and will be reported as untrusted on subsequent scans.
- **Clean** - Comodo Antivirus will delete the certificate.

For the action to be applied to an individual certificate, select from the 'Action' drop-down beside each item:



- Click 'Apply Actions' to implement your choices for the items. The selected actions will be applied.

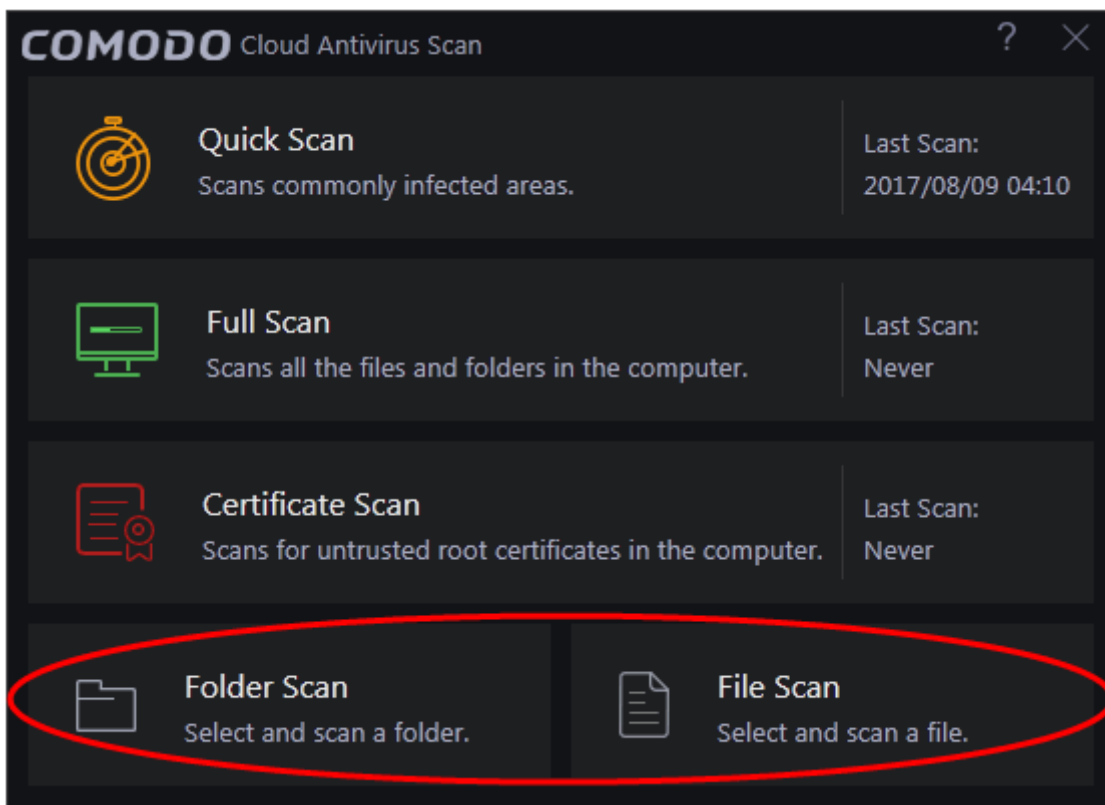


## 2.4. Run a Custom Scan

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

### To run a custom scan

- Open the 'Scan' interface by clicking 'Scan' from the 'Task bar'
- OR
- Click on the scan button from the widget and click 'Folder Scan' or 'File Scan' from the 'Scan' interface.



The following sections explain more on:

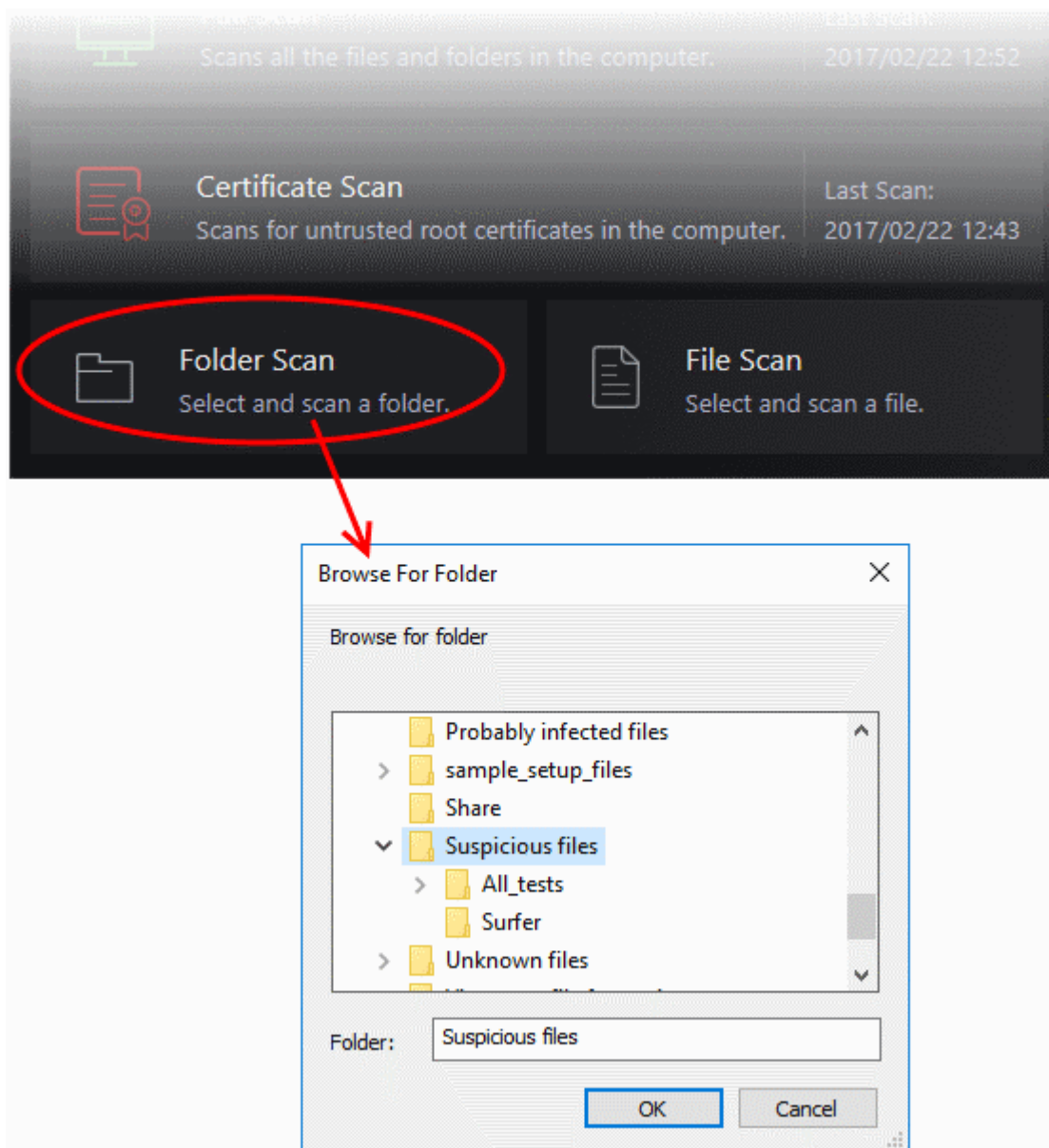
- **Folder Scan** - scan individual folders
- **File Scan** - scan an individual file

## 2.4.1. 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 an external device or downloaded from the internet and want to scan it for threats before you open it.

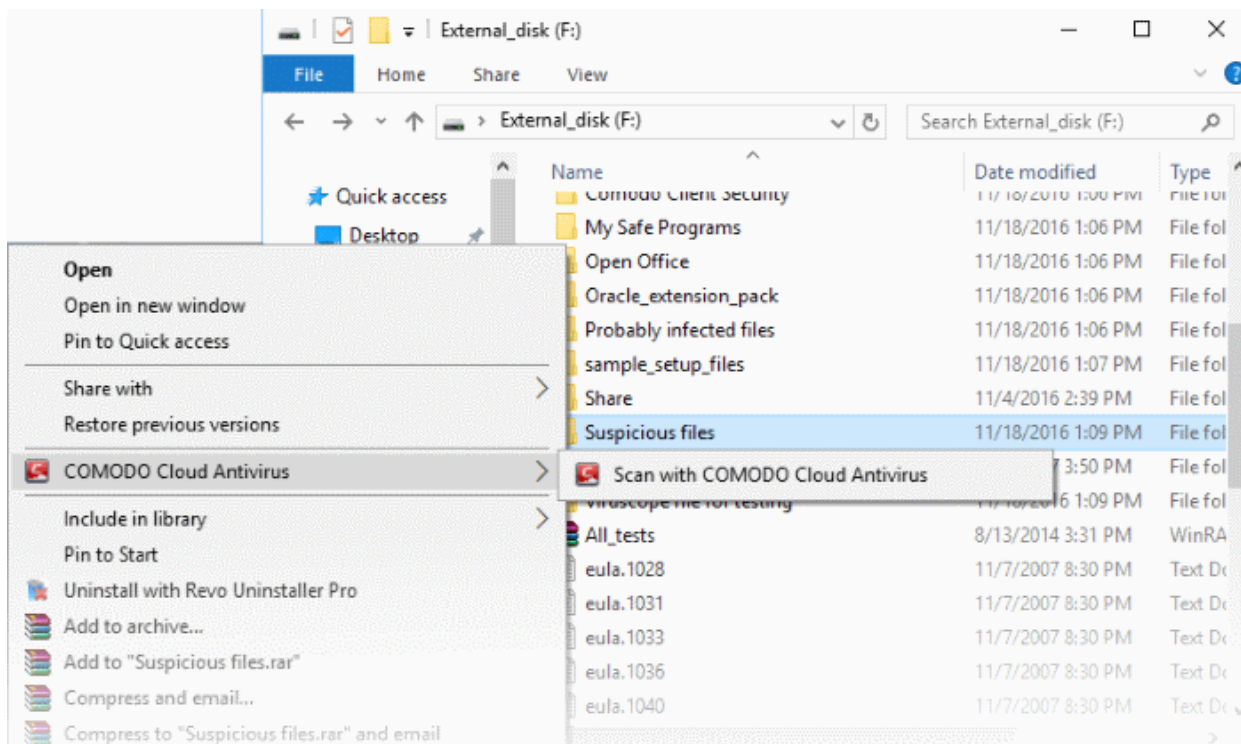
### To scan a specific folder

- Click 'Scan' in the CCAV home screen OR click the scan button on the widget
- Click 'Folder Scan' from the options
- Browse to the folder you want to scan and click 'OK'

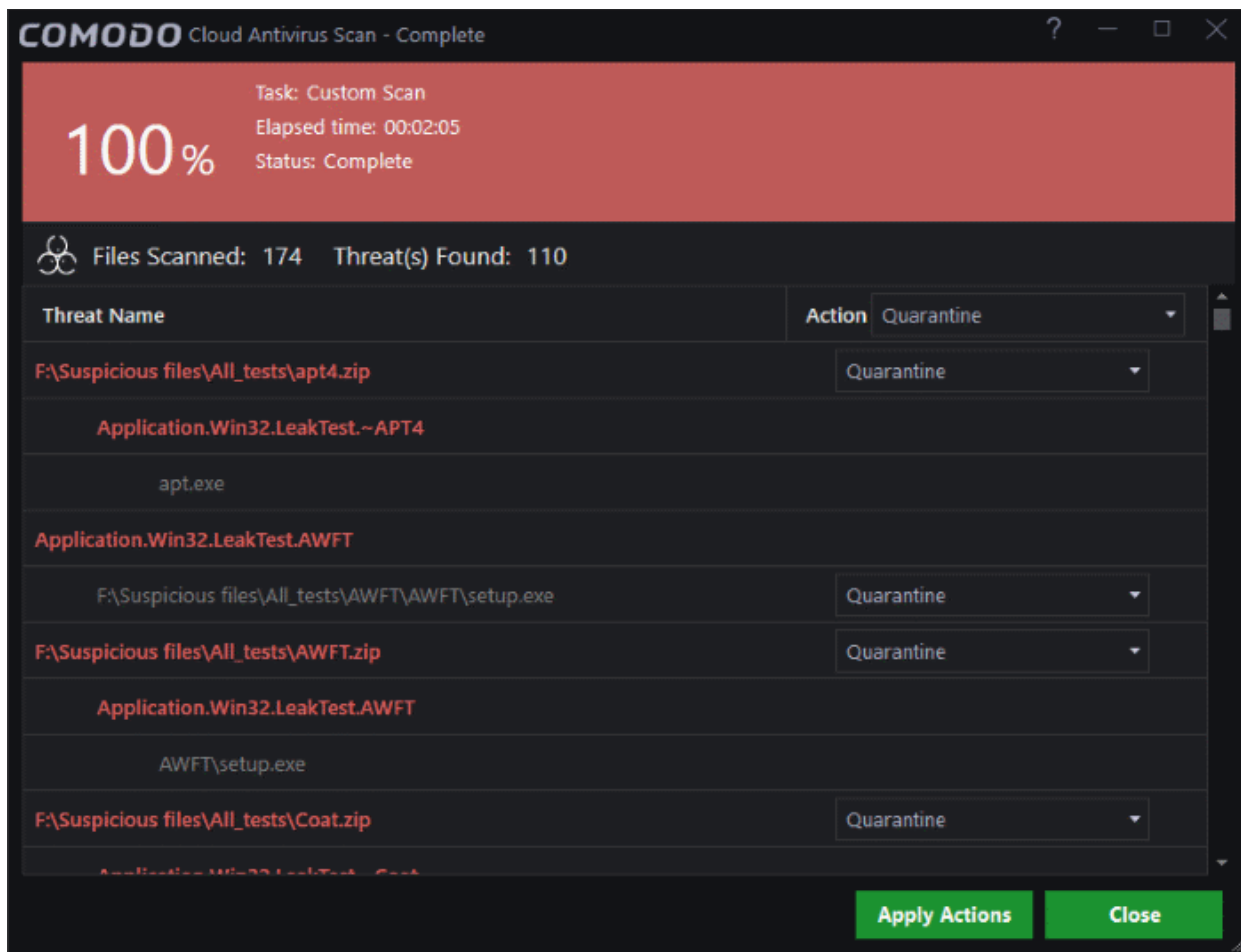


- Alternatively, right-click on a folder and select 'Scan with Comodo Cloud Antivirus' from the context-sensitive menu.





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



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 quarantine files or ignore the threat based in your assessment.

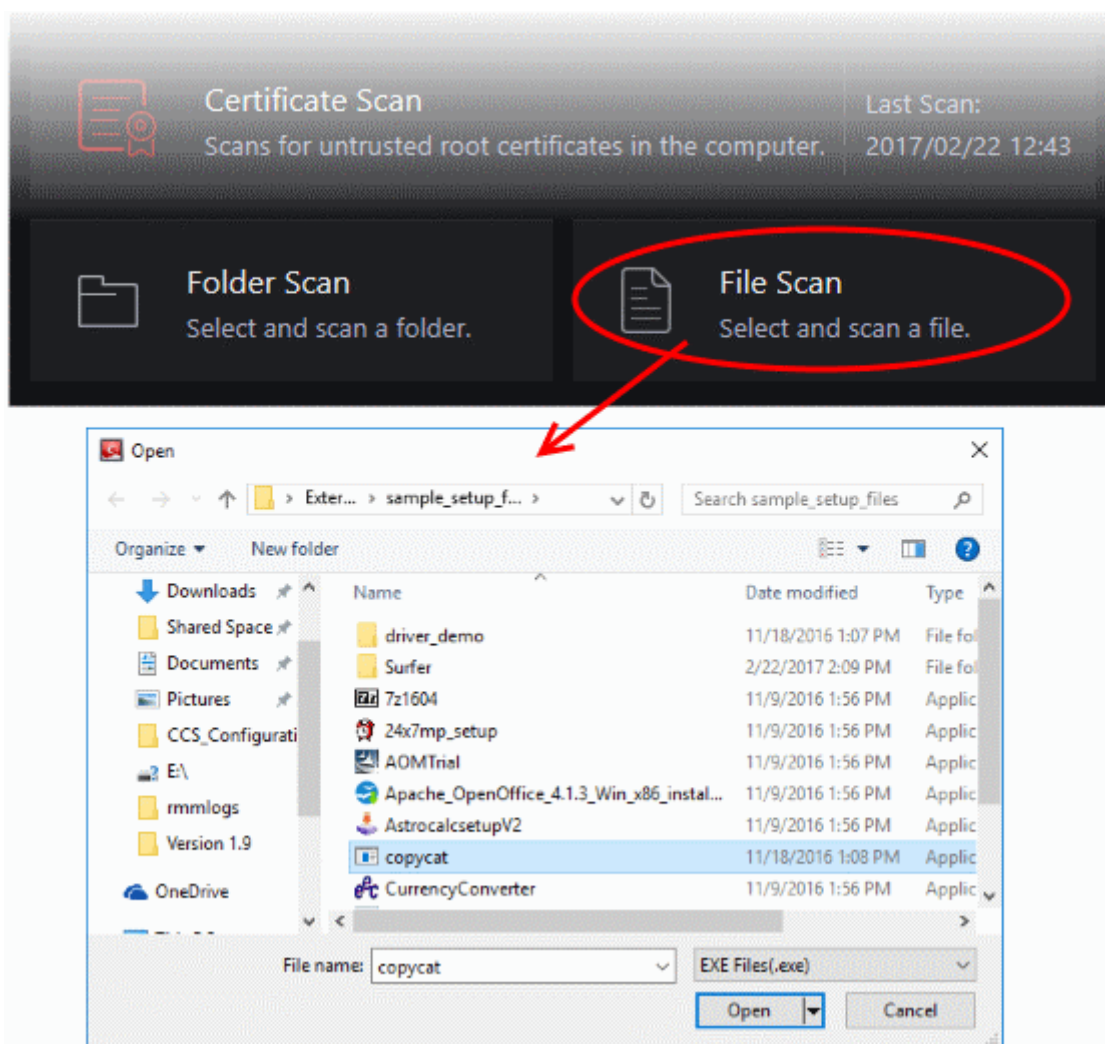
Refer to [Processing the infected files](#) for more details.

## 2.4.2. Scan a File

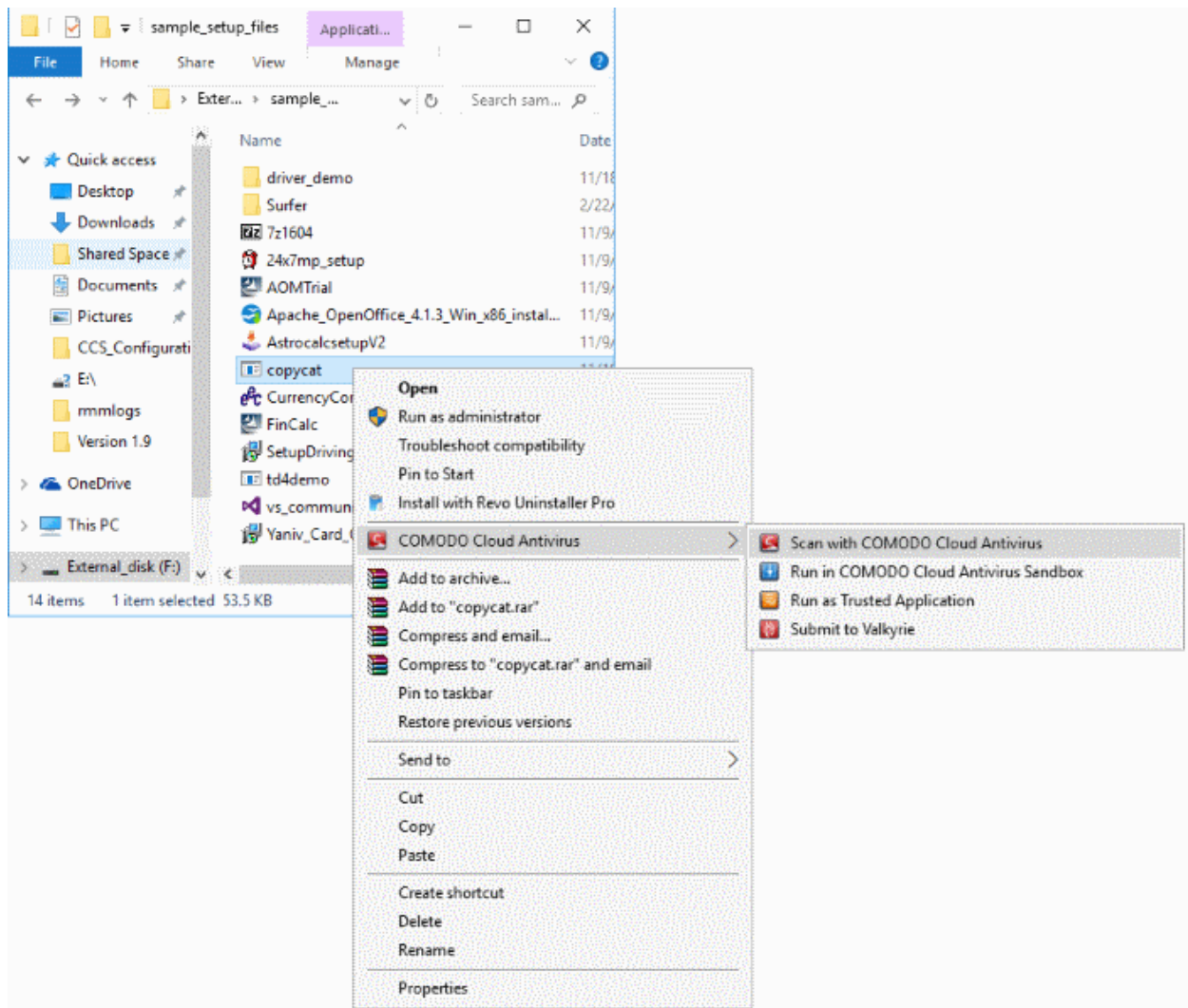
The 'File Scan' option allows you to scan a specific file on your hard drive, CD/DVD or external device. For example, you might have downloaded a file from the internet or dragged an email attachment onto your desktop and want to scan it for threats before you open it.

### To scan a specific file

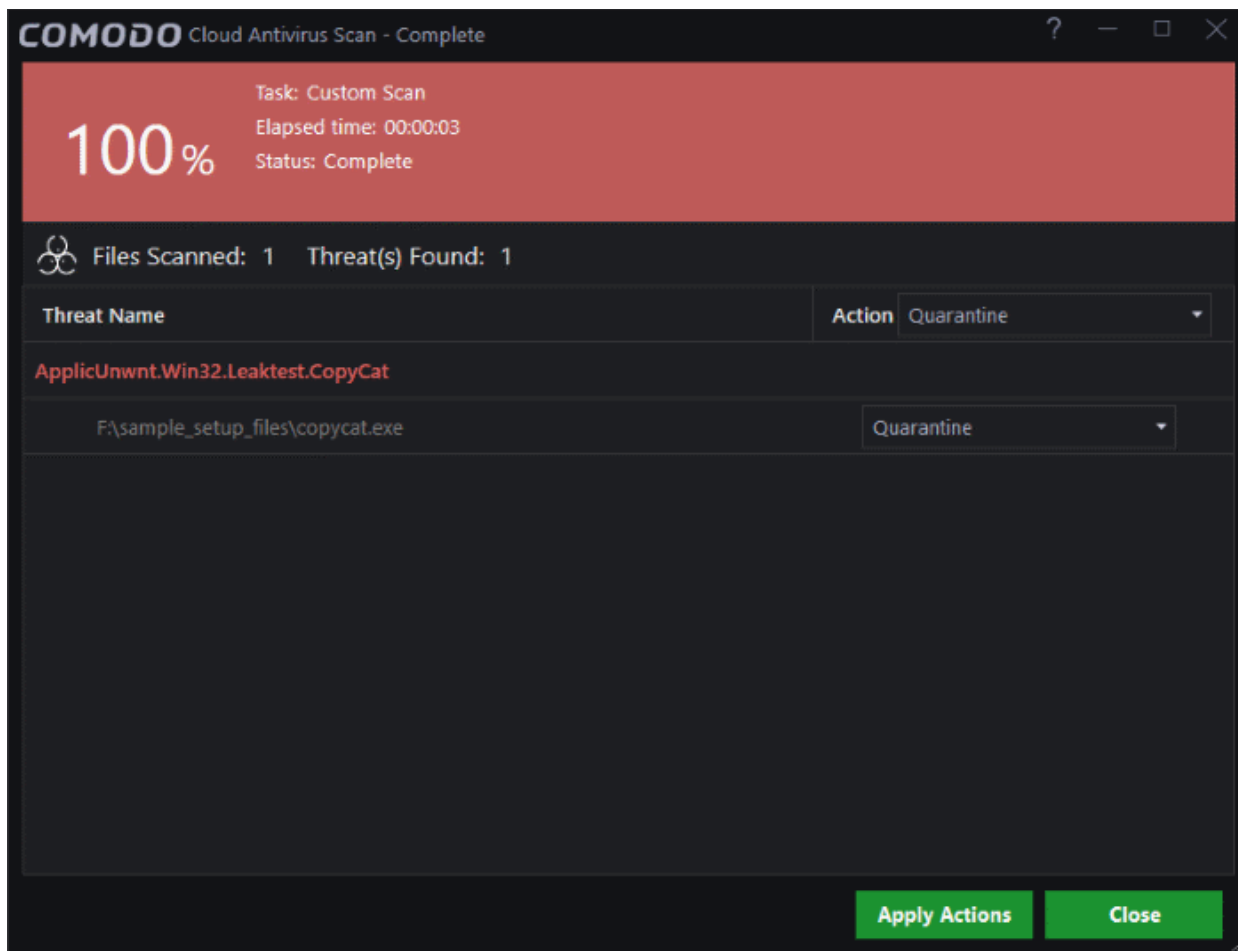
- Click 'Scan' in the CCAV home screen OR click the scan button on the widget.
- Choose 'File Scan', browse to the file you wish to scan then click 'Open':



- 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.

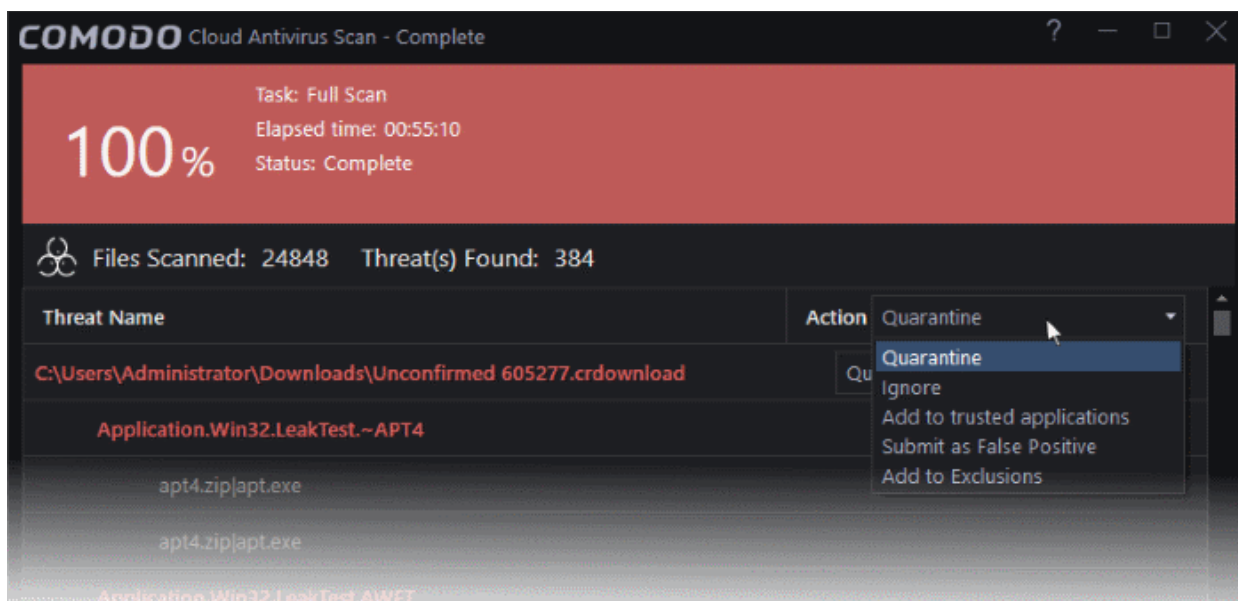


The scan results window displays the number of objects scanned and the number of threats (Viruses, Rootkits, Malware and so on). You can choose to quarantine files or ignore the threat based in your assessment. Refer to [Processing the infected files](#) for more details.

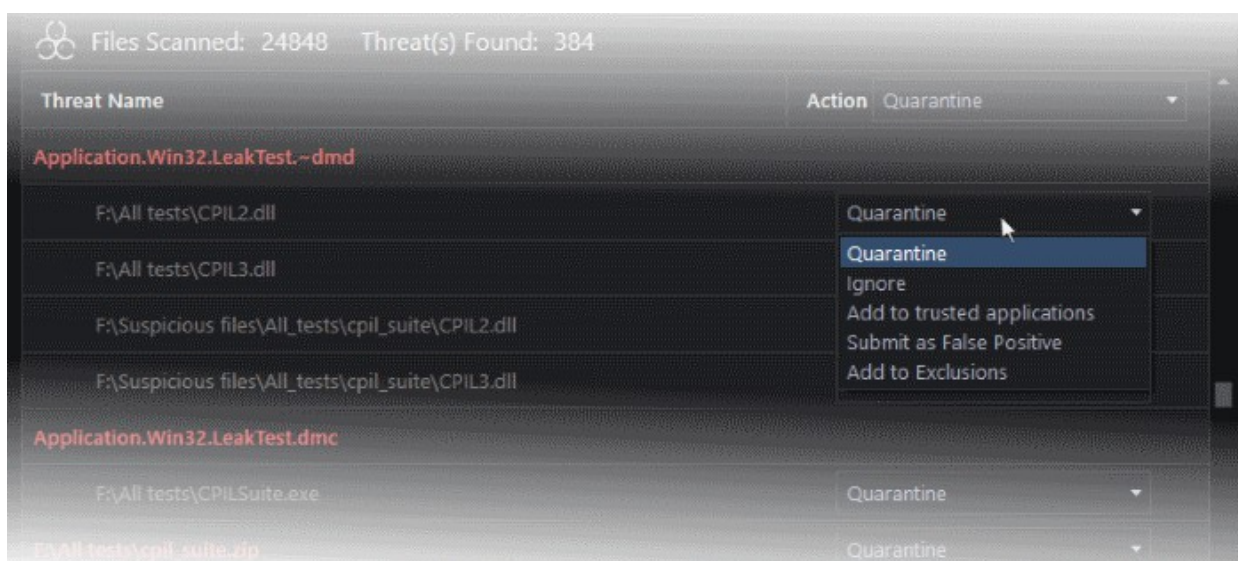
## 2.5. Processing Infected Files

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.

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



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

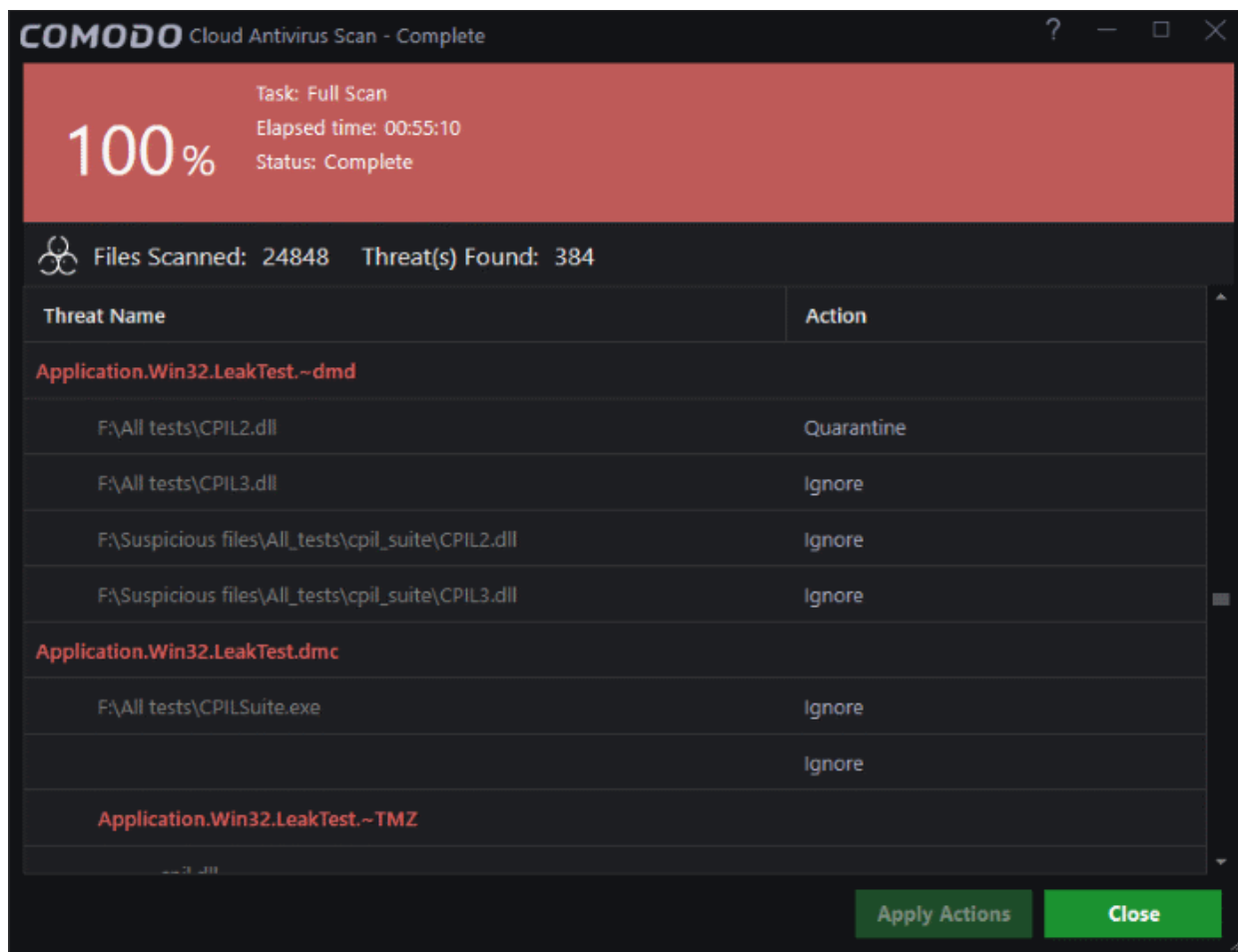


The available actions are:

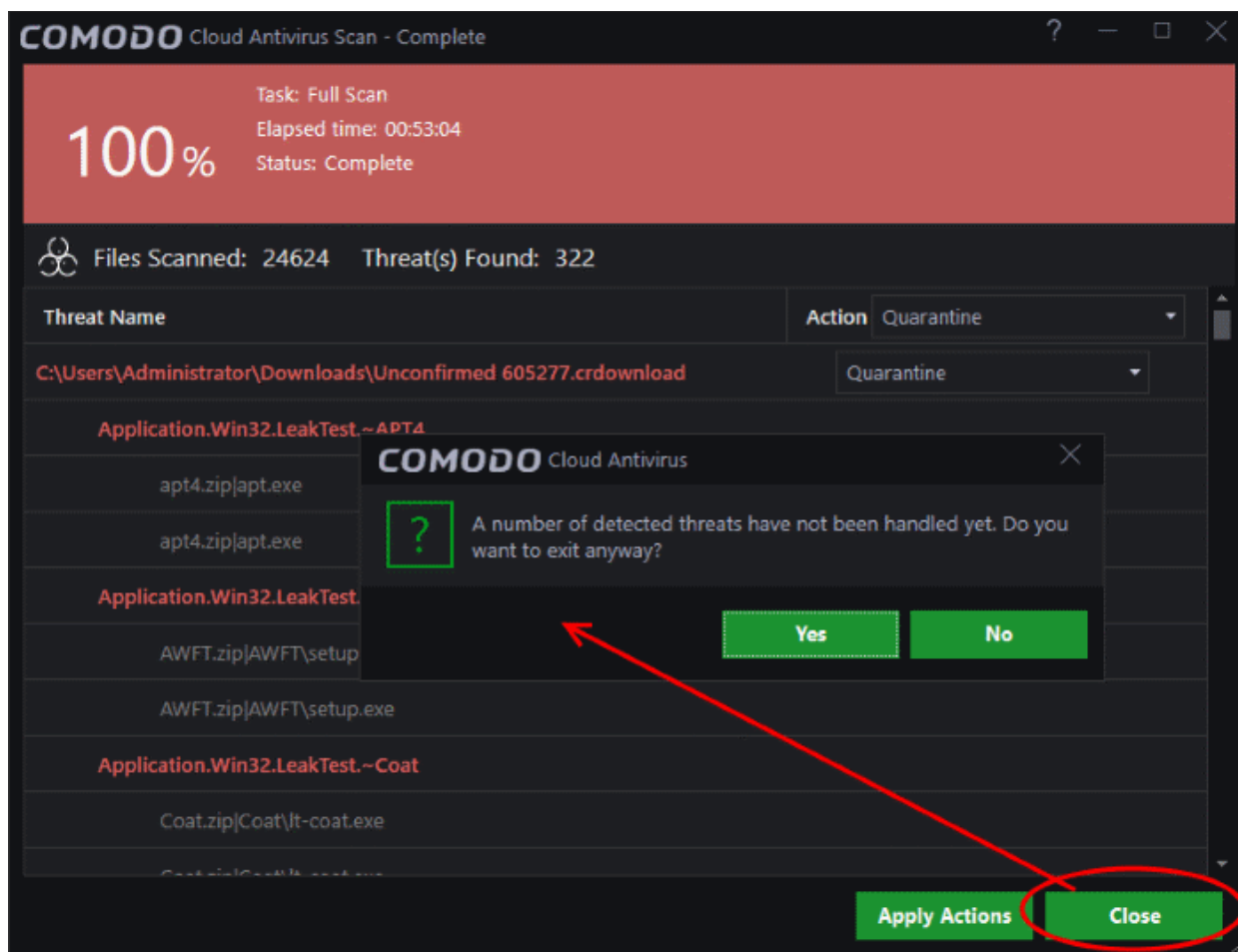
- **Quarantine** - The files will be moved to quarantine. For more details on quarantine feature, refer to the section '**View and Manage Quarantined Items**'.
- **Ignore** - If you want to ignore the threat this time only, select 'Ignore'. The file will be ignored only at that time and if the same application 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.
- **Submit as False Positive** - If you are sure that the file is safe, select 'Submit False Positive'. The file will be sent to Comodo for analysis. If the file is trustworthy it will be added to the Comodo safe list.
- **Add to Exclusions** - The file will be moved to an 'Exclusions' list maintained by CCAV and will not be scanned in future. The alert will not generated if the same application invokes again.
- 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.



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



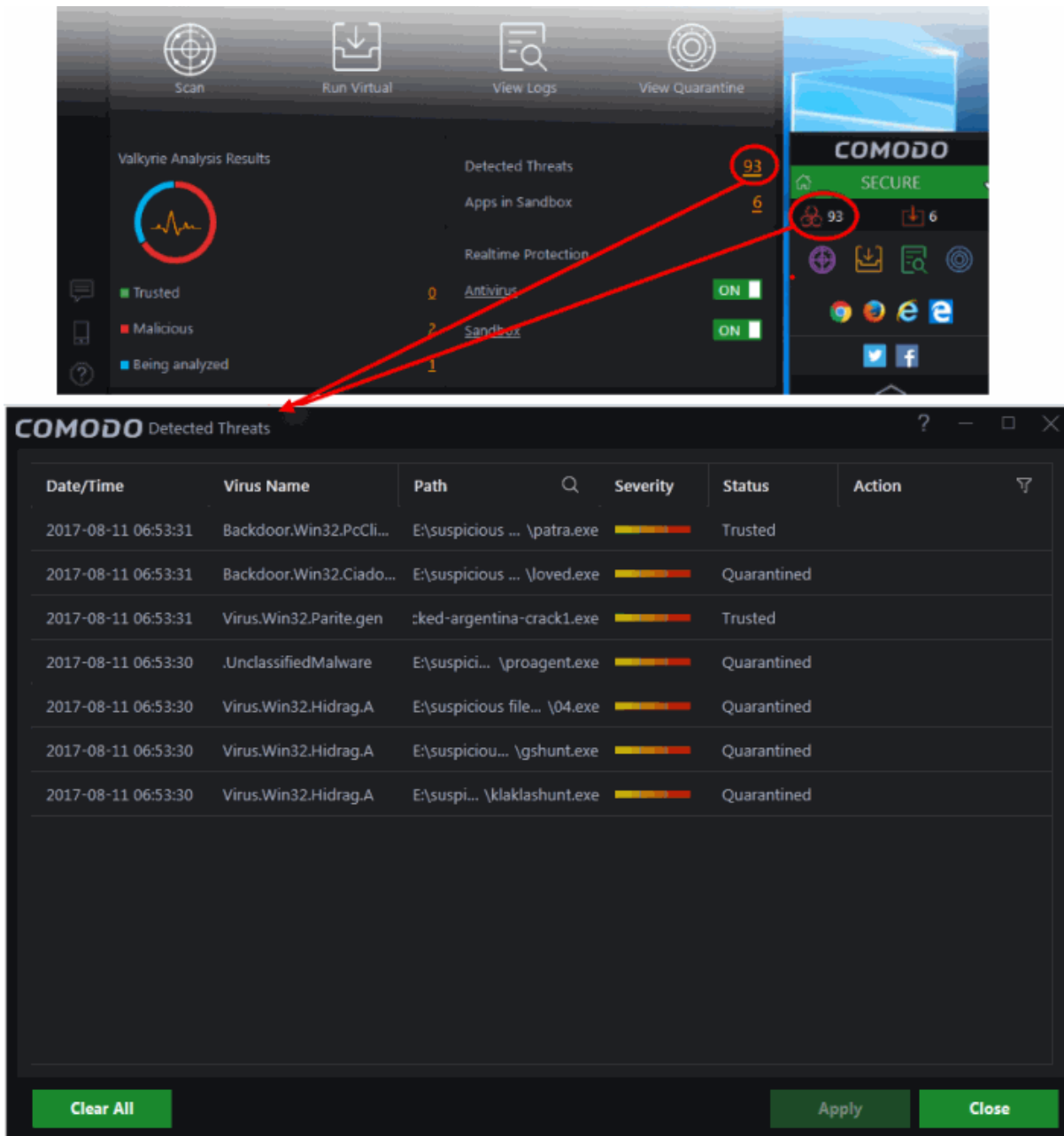
The 'Detected Threats' interface allows you to take action such as 'Quarantine', 'Trust' or 'Trust and Report False Positive' later on. Refer to the section '[Managing Detected Threats](#)' for more details.

## 2.6. Managing Detected Threats

The 'Detected Threats' interface shows items identified as malicious, but which have yet to be processed. The interface also displays the current status of each item - whether it is quarantined, removed, trusted or submitted as a false positive to Comodo. You can also apply additional actions like moving the detected threats to 'Quarantine', 'Trusted files' list or 'Submit as False Positive' to Comodo.

### To open the 'Detected Threats' interface

- Click the number under 'Detected Threats' in the CCAV home screen.
- Alternatively, click the 'Detected Threats' icon on the widget.




## Column Descriptions:

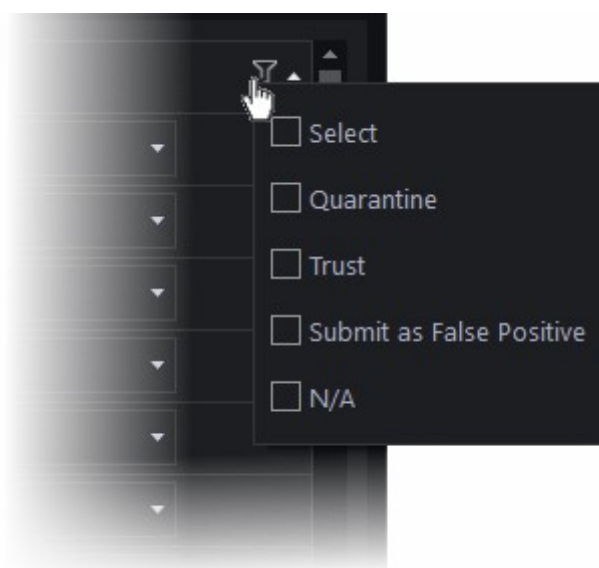
- **Date/Time** - The date and time at which the threat was detected
- **Virus Name** - The name of the malware contained in the application detected as threat
- **Path** - The location of the application in the system
- **Severity** - Indicates the risk level presented by the activity or request of the detected threat
- **Status** - Indicates the status of the action taken. It can be either 'Quarantined', 'Removed' and 'Trusted'
- **Action** - Displays a drop-down with options for handling 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.
- **Submit as 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 the global safe-list.
- To search for a specific application, click the search icon  beside the 'Path' column header and enter the name of the application in part of full.
- To filter items by the action to be executed on them, click the funnel icon beside the 'Action' header and select an action:



- To move an 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 'Submit as False Positive' from the 'Action' drop-down in the item row
- Click 'Apply' for your actions to take effect

## 2.7. Viewing Valkyrie Analysis Results

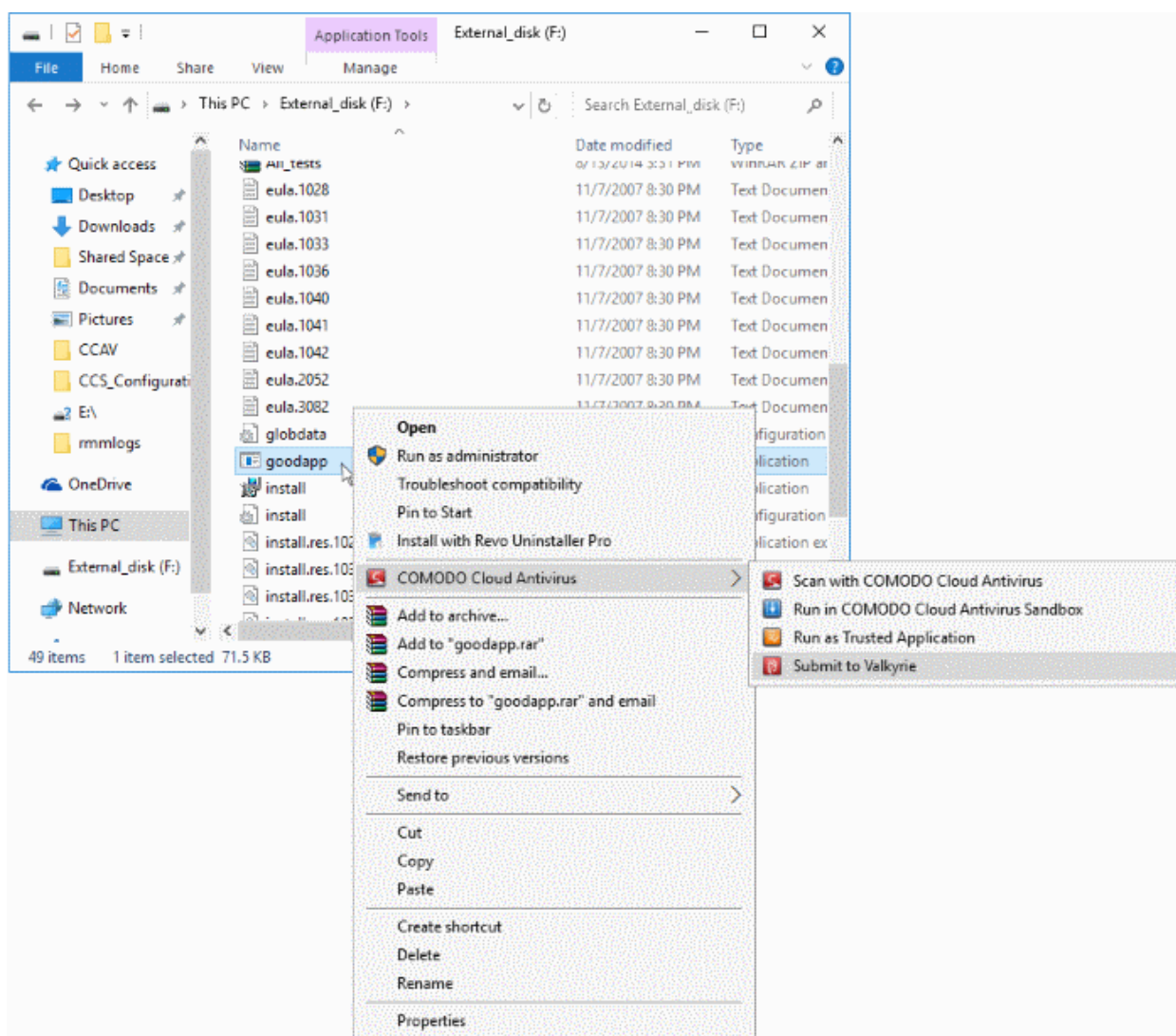
Valkyrie is an online file verdict system that tests unknown files with a range of static and behavioral checks in order to identify those that are malicious. Valkyrie is very effective at detecting zero-day threats missed by the signature-based detection systems of classic antivirus products.

- Unknown files running in the sandbox will be automatically submitted to Valkyrie for analysis if auto-submission is enabled in 'Sandbox Settings' (refer to [Sandbox Settings](#) for more details on this). If not enabled, the results screen of each full scan allows you to manually upload unknown files. Refer to [Running a Full Scan](#) for more details.
- You can also manually upload files to Valkyrie by right-clicking on a file. For example, you could upload an

executable that you recently downloaded from the internet to establish its trustworthiness.

## To manually submit a file

- Right-click on the file you want to upload and select 'COMODO Cloud Antivirus' > 'Submit to Valkyrie'
- OR
- Select 'Submit File' from the 'Help' icon on the side menu icon bar



Submitted files will undergo a series of automated and manual behavioral tests. The results will be sent back to your CCAV installation once the analysis is complete.

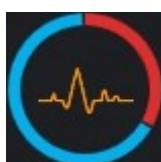
The 'Valkyrie Analysis Results' pane on the home screen displays statistics and messages from Valkyrie.



The icons show verdicts on unknown files on your computer.




- Indicates that you need to run a Full scan to identify unknown files on your computer.



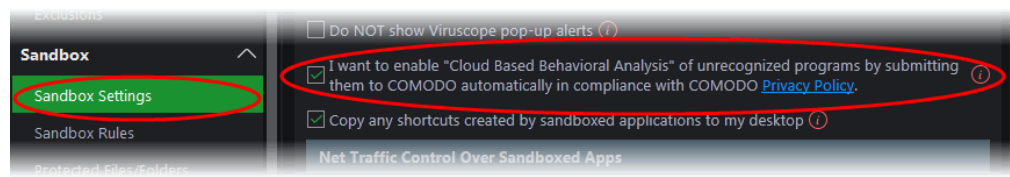
- Unknown files were detected, automatically submitted to Valkyrie, and are currently undergoing analysis. The circle also provides a rough indication of Valkyrie results. A red section indicates that Valkyrie returned a malicious verdict on some files. Green sections mean that the files were found to be safe. The exact quantities of each are shown in the legend under the circle.

- See the explanation **above** for details on how to manually submit files.
- To enable automatic submission of unknown files:



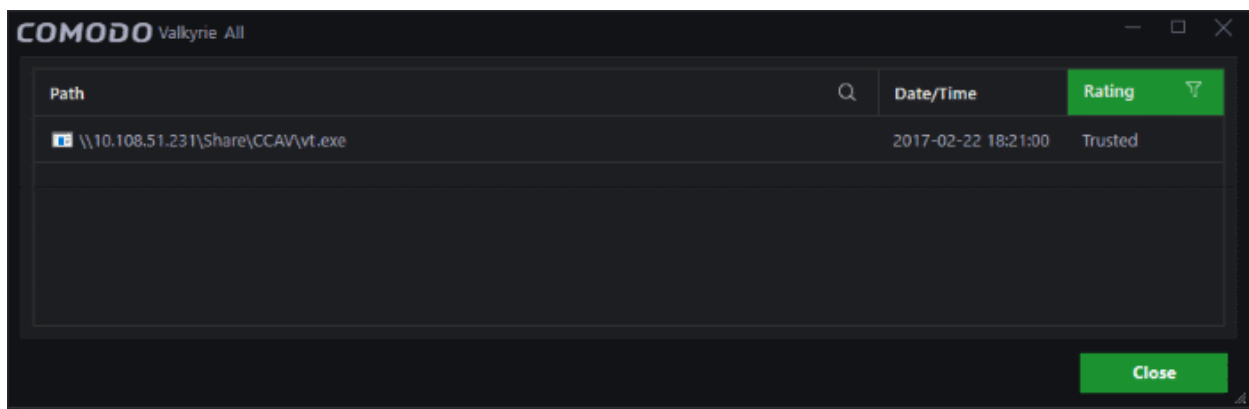
- Click the 'Settings' button  at the top of the left menu to open the 'Settings' interface
- Click 'Sandbox' > 'Sandbox Settings'
- Enable the checkbox labeled: 'I want to enable 'Cloud based Behavioral Analysis of unrecognized programs by submitting them to Comodo

automatically in compliance with Comodo Privacy Policy'

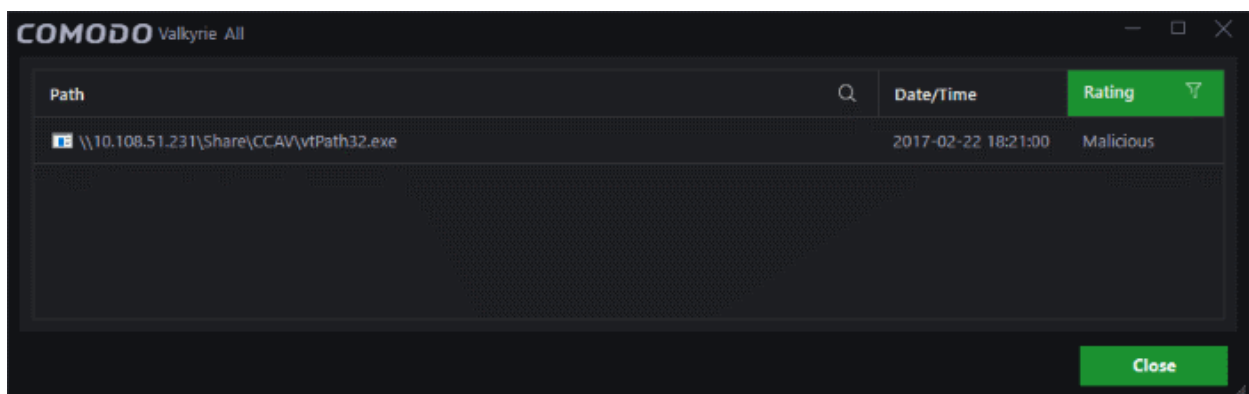


- There are no unknown files on your computer. All unknowns have been submitted and analyzed by Valkyrie and there are no pending files.

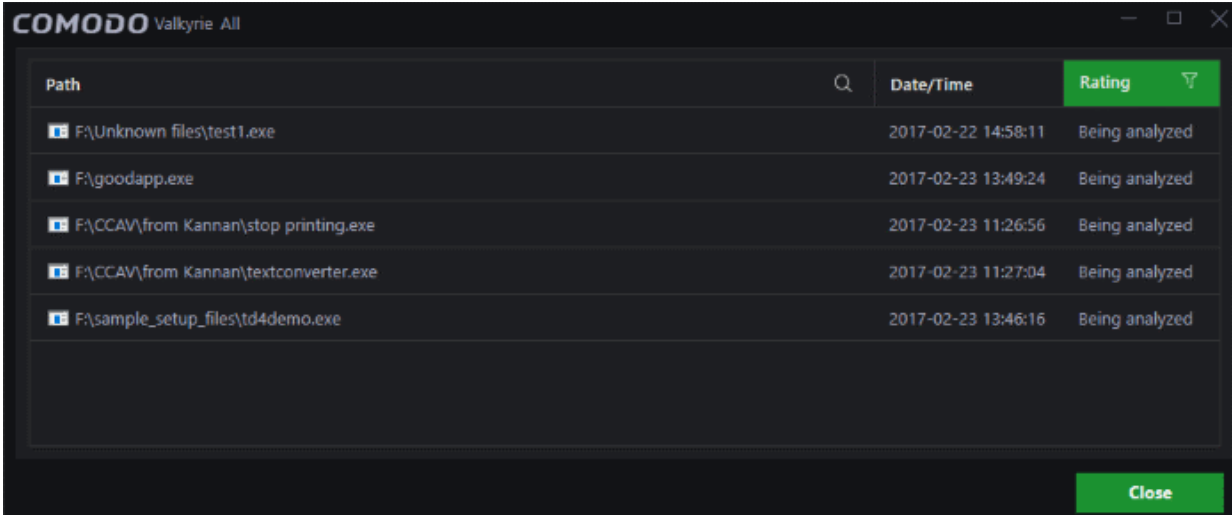
- **Trusted** - Displays the number of files uploaded from your computer and identified as 'Trusted' by Valkyrie Analysis.
  - Click the number to see the list of files identified as 'Trusted'



- **Malicious** - The number of files uploaded from your computer that Valkyrie found to malware.
  - Click the number to view a list of 'Malicious' files



- **Being Analyzed** - Displays the number of files uploaded from your computer which are currently being examined by Valkyrie. The verdicts on these files will be returned to your computer once the analysis is complete.
  - Click the number to view the list of pending files



The screenshot shows the Comodo Valkyrie All interface with a table of files being analyzed. The table has three columns: Path, Date/Time, and Rating. The Rating column is highlighted in green. A green 'Close' button is visible at the bottom right of the window.

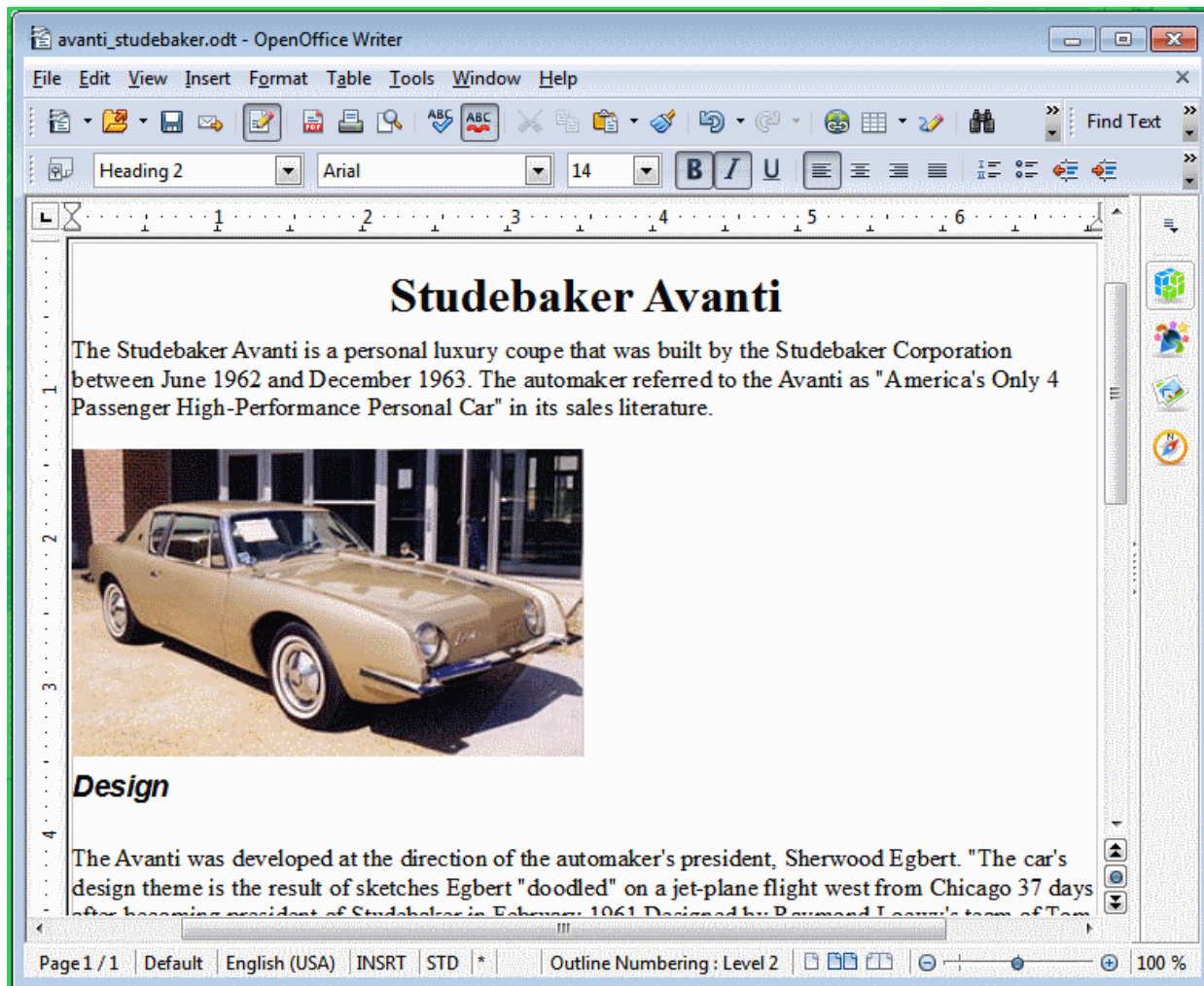
Path	Date/Time	Rating
F:\Unknown files\test1.exe	2017-02-22 14:58:11	Being analyzed
F:\goodapp.exe	2017-02-23 13:49:24	Being analyzed
F:\CCAV\from Kannan\stop printing.exe	2017-02-23 11:26:56	Being analyzed
F:\CCAV\from Kannan\textconverter.exe	2017-02-23 11:27:04	Being analyzed
F:\sample_setup_files\td4demo.exe	2017-02-23 13:46:16	Being analyzed

- **Unknown** - This will be available when the auto-submission of unknown files to Valkyrie is disabled in the **Sandbox Settings**. Displays the number of files that are detected as 'Unknown' and awaiting manual submission. Refer to the explanation **above** for details on manually submitting files.

## 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. You can create specific sandbox rules for any application or file. See '**Sandbox Rules**' for more details.

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:



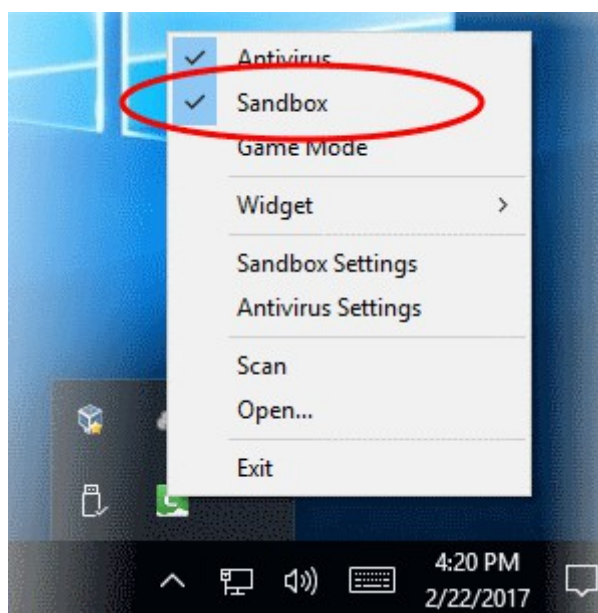
All executables identified as 'Unknown' will automatically run inside the sandbox by default. You can enable/disable auto-sandboxing from the CCAV home screen, from the widget, or by right-clicking on the system tray icon:

- **Main interface.** Use the 'Sandbox' switch to enable/disable auto-sandboxing



- Click the 'Sandbox' link to open the 'Sandbox Settings' interface. Refer to **Sandbox Settings** for more details.
- **Tray Icon/ Widget.** Right-click on the CCAV tray icon or widget. Enable or disable the sandbox as shown

below:



Following sections explain more on:

- [Running an Application or Browser in the Sandbox](#)
- [Managing Sandboxed Items](#)

## 3.1. Run an Application or Browser in the Sandbox

You can also manually run applications and internet browsers in the CCAV sandbox. For example, you may want to test beta or new software in the sandbox where they cannot impact the rest of your computer. Running your browser in the sandbox makes for a more secure online experience as all downloaded files (and potential threats) will automatically sandboxed.

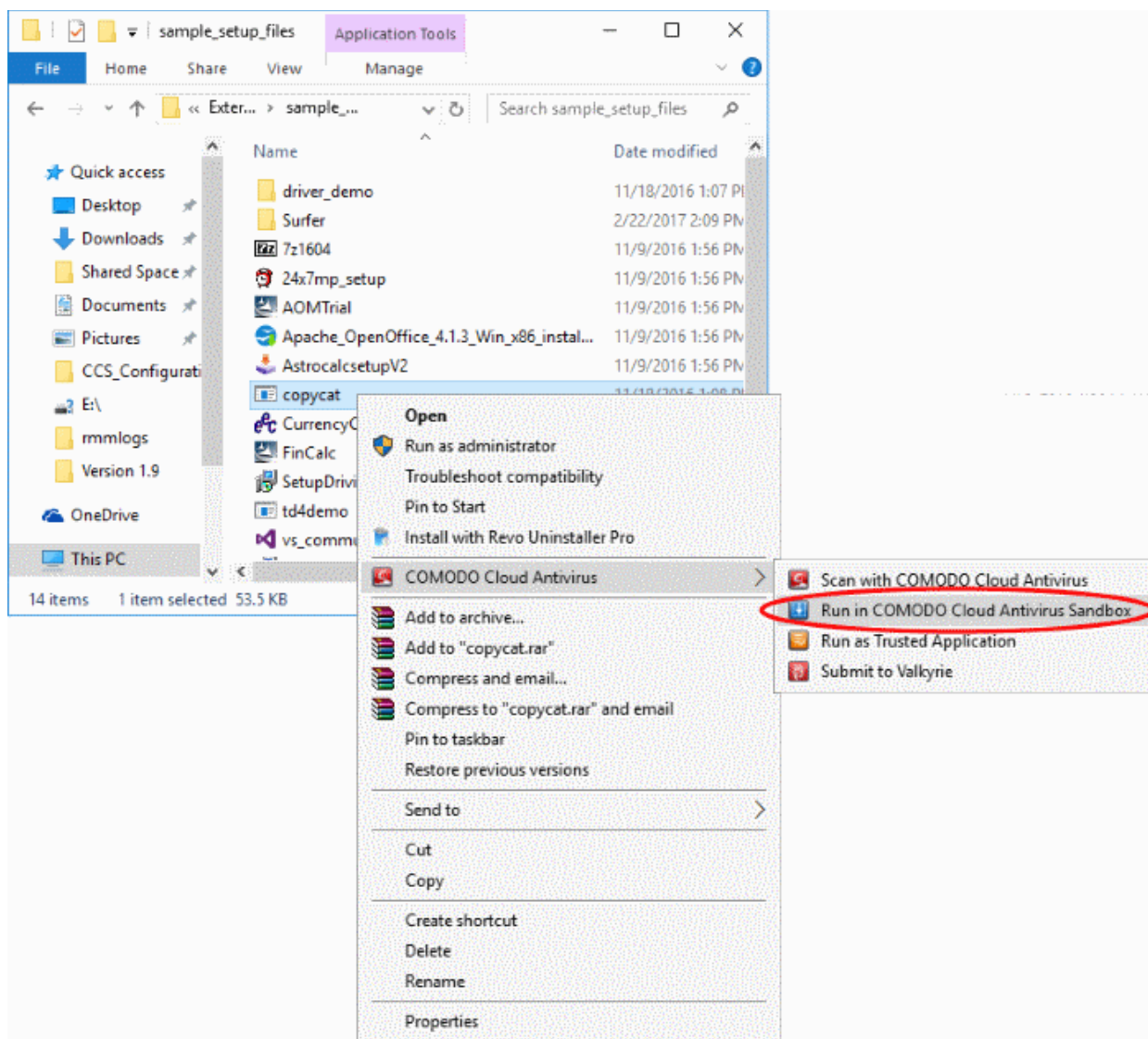
There are various methods you can use to manually run applications/browsers inside the sandbox:

- [Running an application from context sensitive menu](#)
- [Adding an application to Sandbox](#)
- [Running Browsers from shortcuts in the Widget](#)

### Run an Application from the Context Sensitive Menu

You can quickly run an application or file in the sandbox by right-clicking on it.

- Locate the file/application you wish to run in the sandbox
- Right-click on the item and choose 'COMODO Cloud Antivirus' > 'Run in COMODO Cloud Antivirus Sandbox' from the context sensitive menu.



## Add and Run Applications in Sandbox

You can add applications and browsers to CCAV sandbox, allowing you to run those applications from CCAV home screen, inside the sandbox.

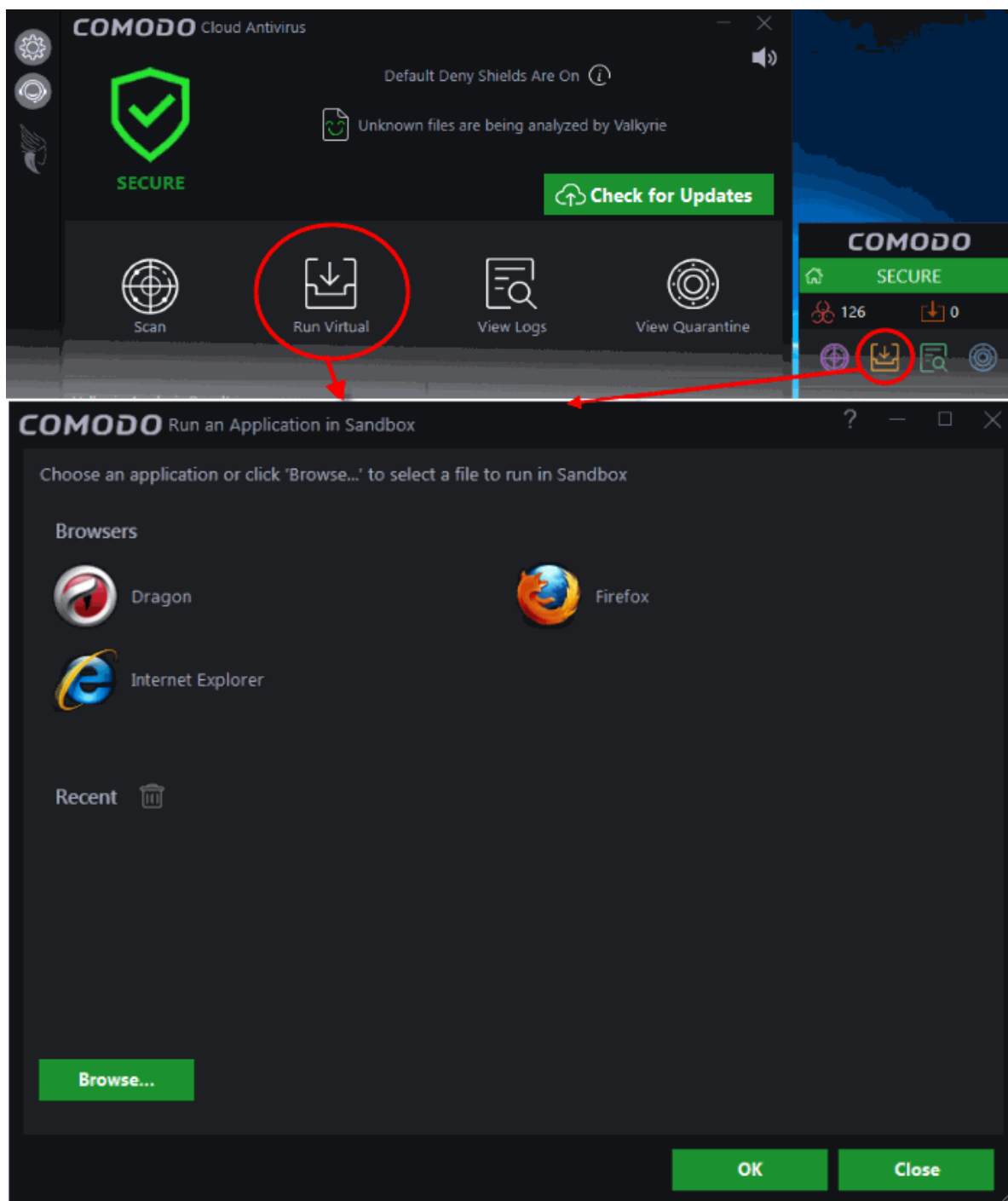
### To add an application to the sandbox

- Click 'Run Virtual' from CCAV main interface

OR

- Click the 'Select an application and run it in Sandbox' button  from the CCAV desktop widget





The 'Run an Application in Sandbox' interface will open:

The interface contains shortcuts to open all browsers installed on your computer inside the sandbox. It also allows you to add applications to the list.

- Click 'Browse' navigate to the location of the executable and click 'Open'
- Click 'OK'

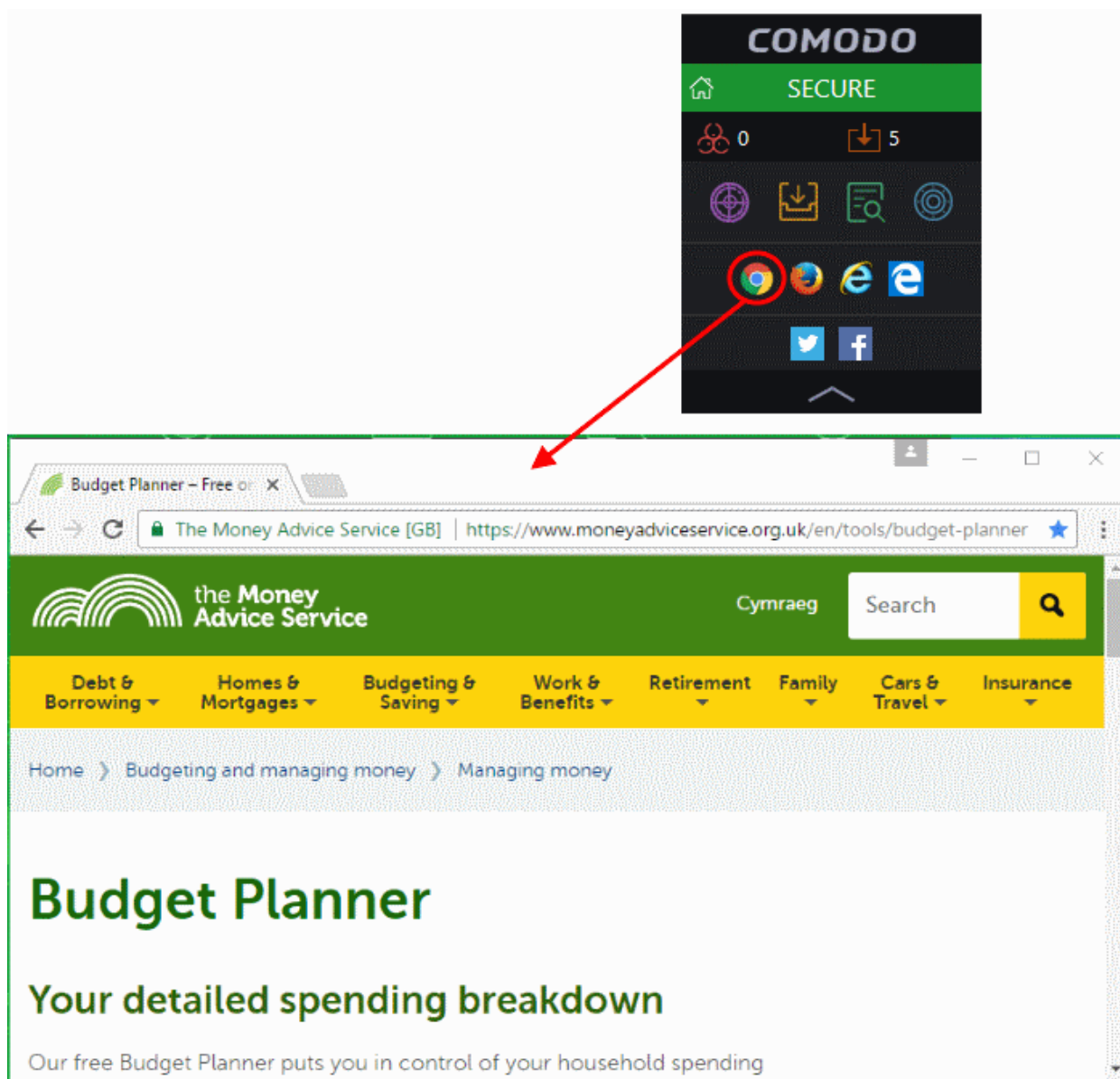
The application will start and run within the sandbox.

The application will also be listed under 'Recent' in the 'Run an Application in Sandbox' interface. For subsequent execution of the same application inside the sandbox, you can open the 'Run an Application in Sandbox' interface by clicking 'Run Virtual' from the CCAV main interface and clicking on the application.

## Run Browsers from Shortcuts in the Widget

The CCAV desktop widget displays shortcuts to the browsers you have installed:

- To start a secure browsing session inside the sandbox, click on a browser icon.



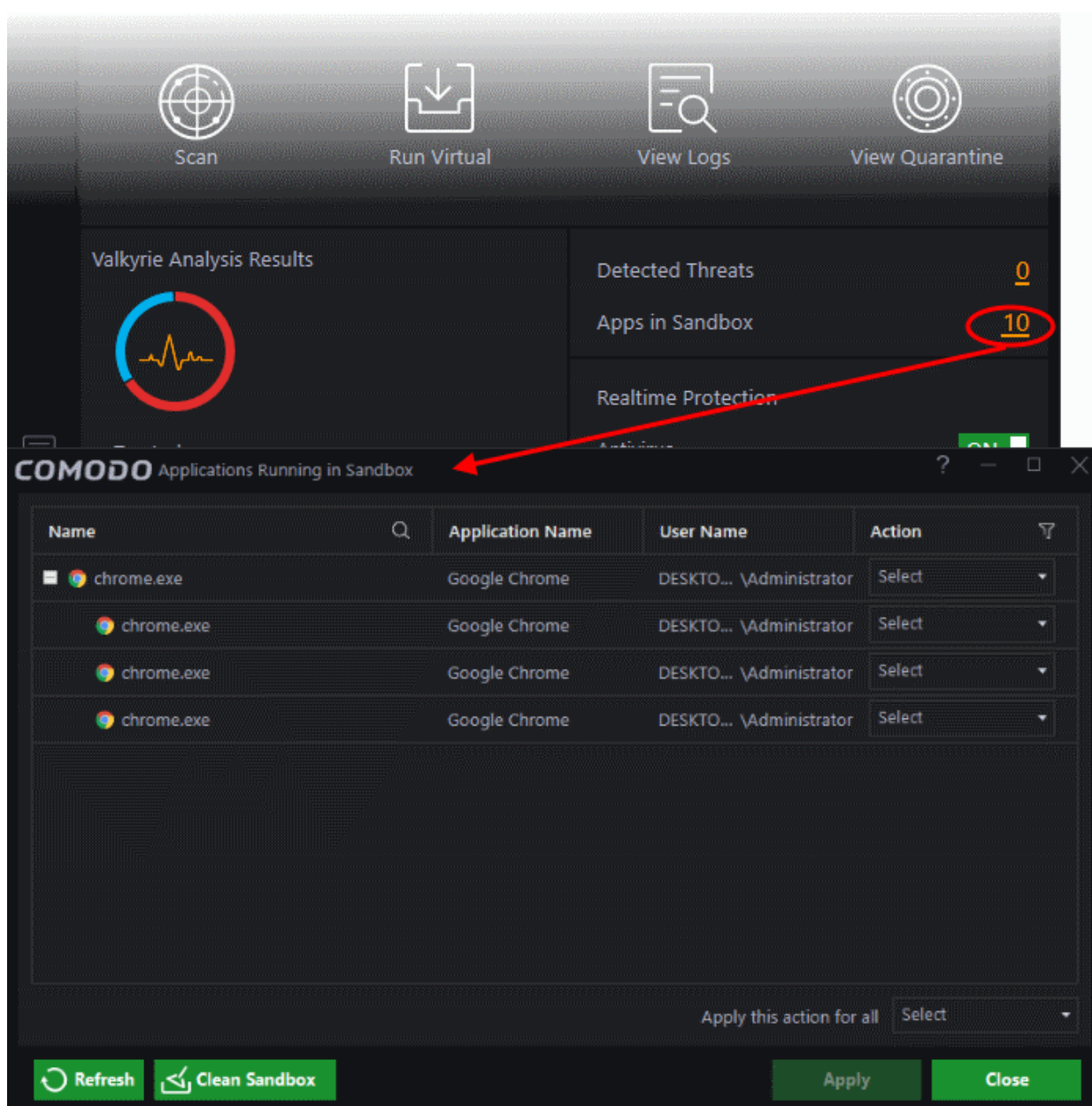
The browser will be started and executed inside the sandbox at 'Fully Virtualized' level. If 'Show highlight frame for virtualized programs' is enabled in **Sandbox Settings** then CCAV displays a green border around the sandboxed browser.

**Tip:** You can also start a browser inside the sandbox by clicking 'Run Virtual' from the main interface and selecting the browser from the 'Run an application inside Sandbox' interface.

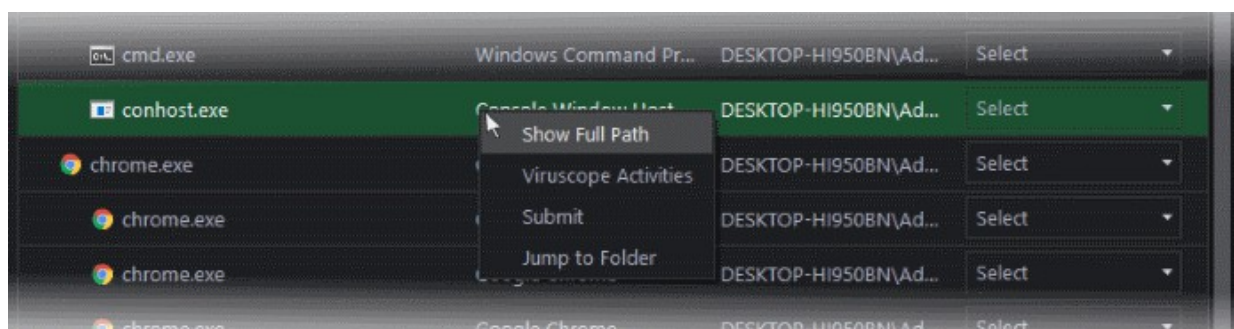
## 3.2. Manage Sandboxed Items

The number of currently sandboxed applications is shown in the 'Sandboxed Apps' area of the CCAV home screen. This figure includes both auto-sandboxed and manually sandboxed applications.

- To view and manage sandboxed applications, click the number in the 'Sandboxed Apps' section:



- To view more details about an application, right-click on it and choose an option from the context sensitive menu.

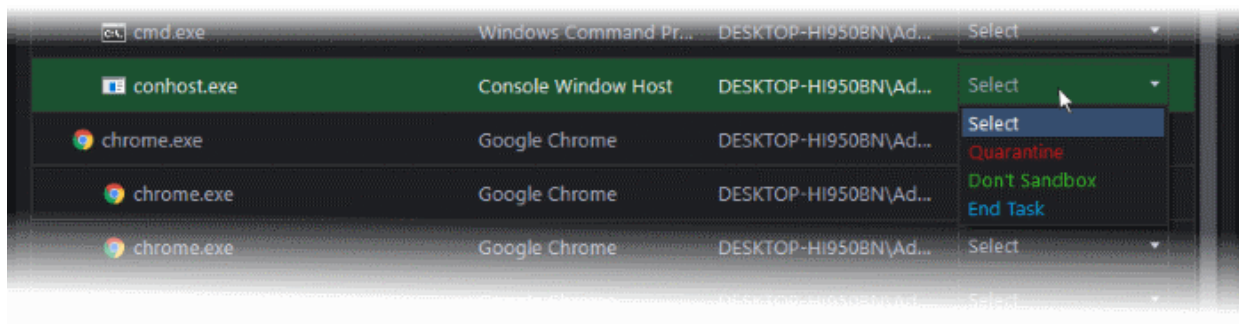


- Show full Path** - Will display the exact storage location in which the executable resides
- Viruscope Activities** - Displays the list of malicious activities, if any, as detected by Viruscope. For more details, refer to the section **Viruscope - Feature Spotlight**.

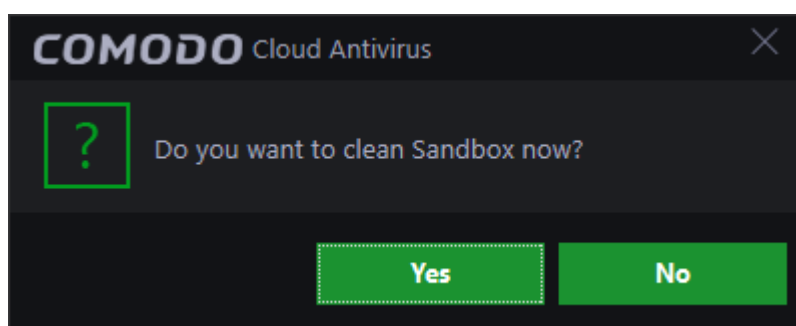
- **Submit** - Will submit the file to Comodo for analysis. Comodo Labs will run behavior analysis on the file to determine whether it is trustworthy or malicious and add it to the global whitelist or blacklist.
- **Jump to Folder** - Will open the file location in Windows Explorer.

Depending on the nature of the file, you can release it from the sandbox, quarantine it or terminate the process.

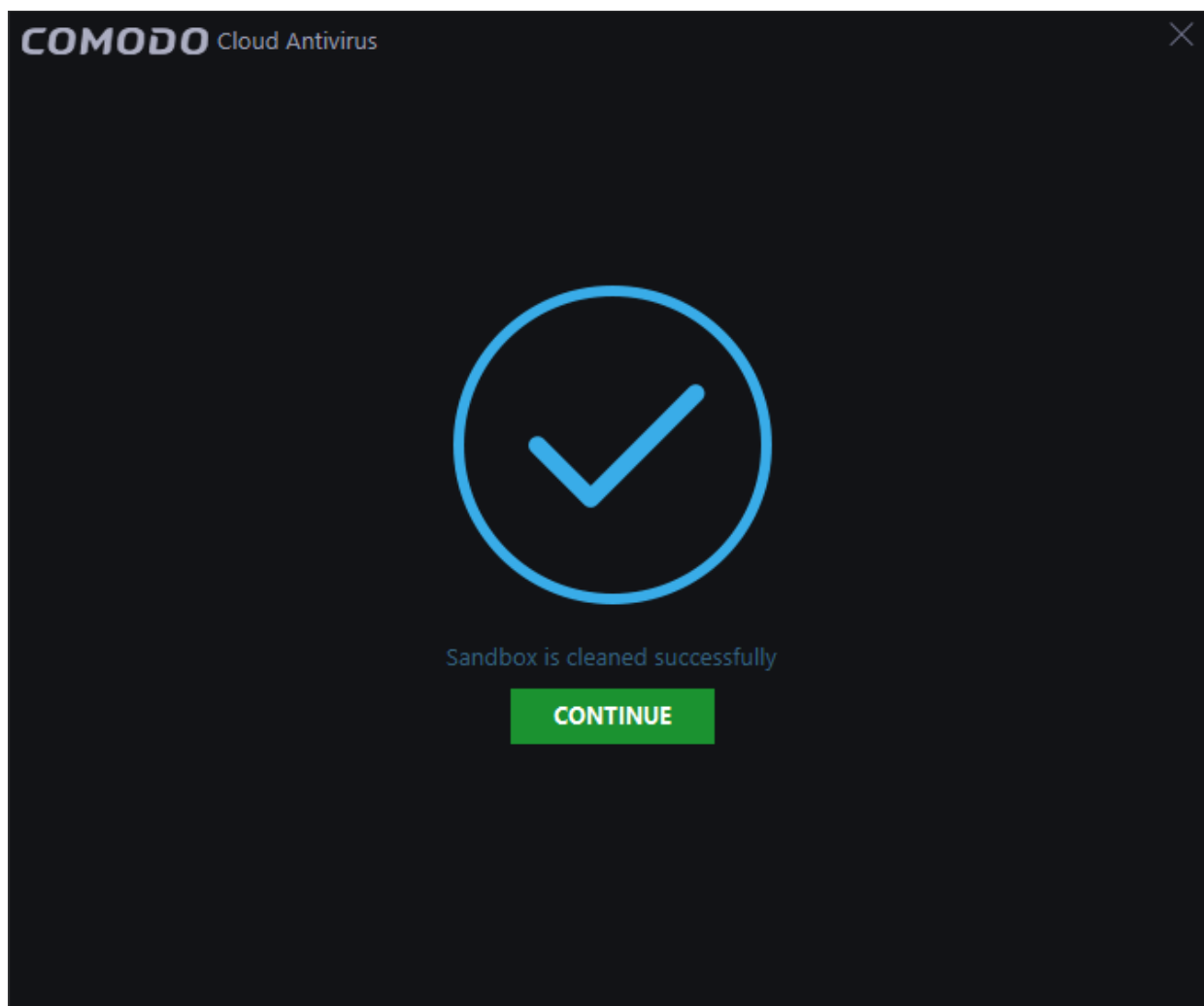
- To apply an action to a sandboxed item, choose it from the 'Action' drop-down beside the item. The available actions are:



- **Quarantine** - Stops execution of the file and adds it to Quarantine. Refer to the section [View and Manage Quarantined Items](#) for more details
  - **Don't Sandbox** - Stops execution of the file inside the sandbox and allows you to start the application normally. From the next execution the application will not be auto-sandboxed
  - **End Task** - Terminates the application
- To apply same action to all applications choose the action from the 'Apply this action for all' drop-down at the bottom right
  - After selecting the action(s) to be applied, click 'Apply'. The files will be treated as per the action selected
  - To reload the dialog with the latest data, click 'Refresh'
  - To remove all applications from the sandbox, click the 'Clean Sandbox' button.



- Click "Yes" to confirm the removal:



Also see [Sandbox Configuration](#) and [Sandbox Logs](#).


## 4. View CCAV Logs

CCAV logs are records of all antivirus events, sandbox events, configuration changes and other user initiated actions. The 'Log' interface allows you to view and manage the logs.

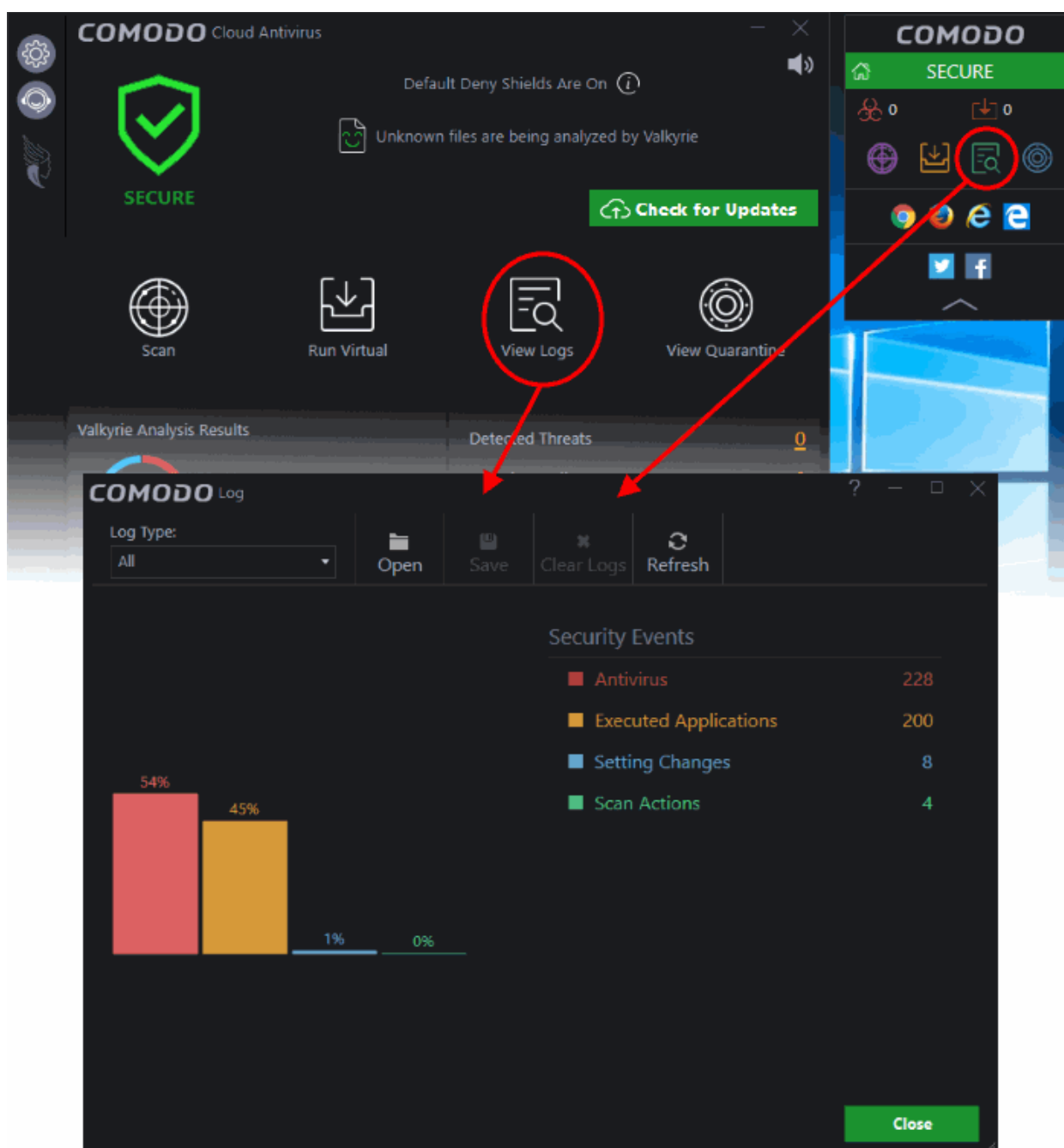
### To open the 'Log' interface

- Click 'View Logs' from the 'Tasks Bar' of the CCAV main interface

OR

- Click the 'View Logs' shortcut button  from the widget





By default, a summary displays logs of all events. 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:

- **Antivirus Logs**

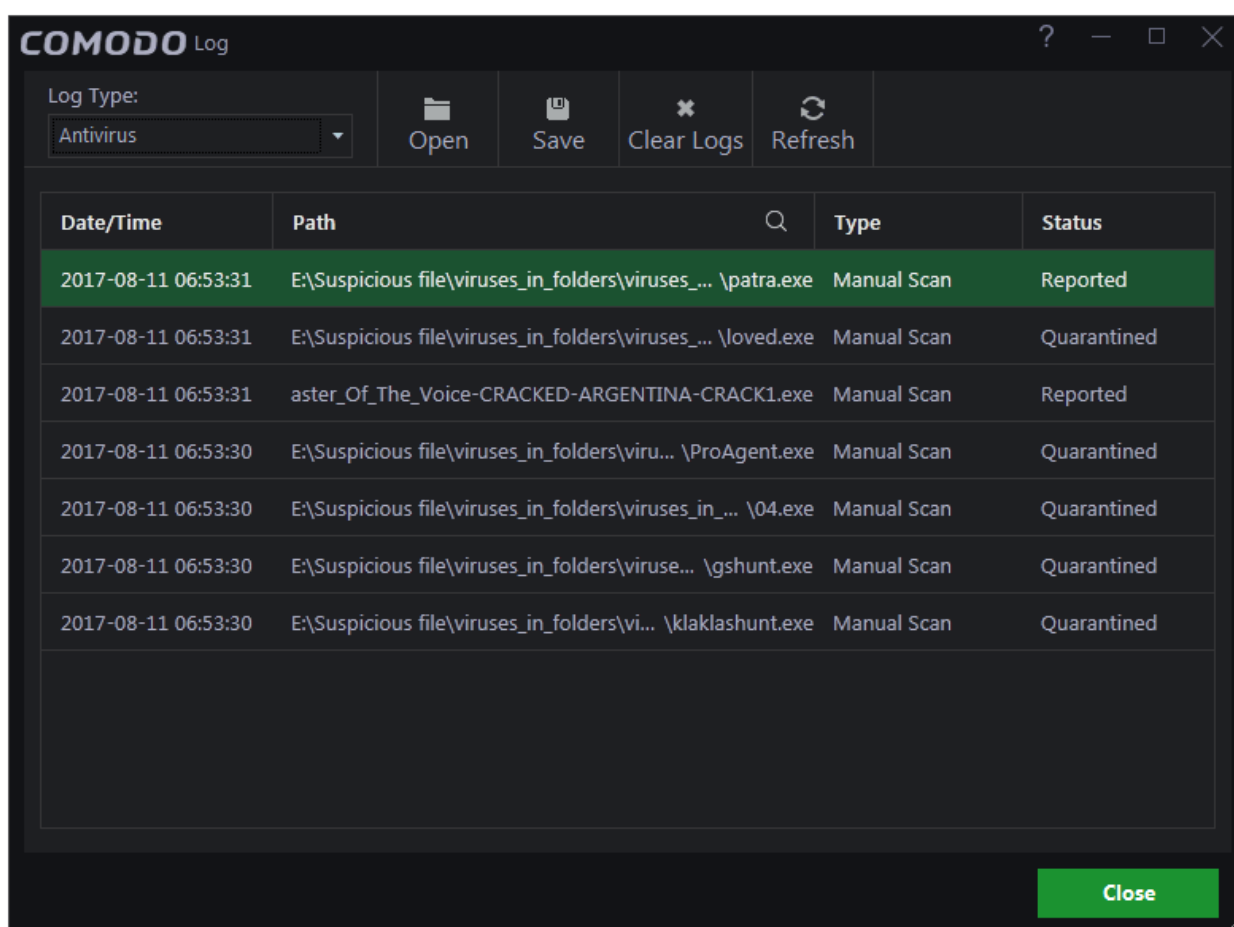
- [Executed Applications Logs \(Sandbox Logs\)](#)
- [Setting Changes Logs](#)
- [Scan Actions Logs](#)

## 4.1. Antivirus Logs

CCAV keeps a history of all items identified as malware by the virus scanner from the real-time scans, manual scans run by the user and files identified as malicious by Valkyrie analysis.

### To view Antivirus logs

- Click 'View Logs' on the CCAV home screen OR click the 'View Logs' button on the widget
- Select 'Antivirus' from the 'Log Type' drop-down at the top left



The screenshot shows the 'COMODO Log' window. At the top, there is a 'Log Type' dropdown menu set to 'Antivirus'. To the right of the dropdown are four buttons: 'Open', 'Save', 'Clear Logs', and 'Refresh'. Below these is a table with the following columns: 'Date/Time', 'Path', 'Type', and 'Status'. The table contains seven rows of scan results. The first row is highlighted in green. At the bottom right of the window is a green 'Close' button.

Date/Time	Path	Type	Status
2017-08-11 06:53:31	E:\Suspicious file\viruses_in_folders\viruses_... \patra.exe	Manual Scan	Reported
2017-08-11 06:53:31	E:\Suspicious file\viruses_in_folders\viruses_... \loved.exe	Manual Scan	Quarantined
2017-08-11 06:53:31	aster_Of_The_Voice-CRACKED-ARGENTINA-CRACK1.exe	Manual Scan	Reported
2017-08-11 06:53:30	E:\Suspicious file\viruses_in_folders\viru... \ProAgent.exe	Manual Scan	Quarantined
2017-08-11 06:53:30	E:\Suspicious file\viruses_in_folders\viruses_in_... \04.exe	Manual Scan	Quarantined
2017-08-11 06:53:30	E:\Suspicious file\viruses_in_folders\viruse... \gshunt.exe	Manual Scan	Quarantined
2017-08-11 06:53:30	E:\Suspicious file\viruses_in_folders\vi... \klaklashunt.exe	Manual Scan	Quarantined

### Column Descriptions

1. **Date/Time** - The precise date and time of the antivirus 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', 'Quarantined' or 'Reported' ('Reported' appears when a user select "Submit as False Positive" for action to be taken)
- To export the logs as a '.log' file, click the 'Save' button
  - To open a stored log file, click the 'Open' log file button



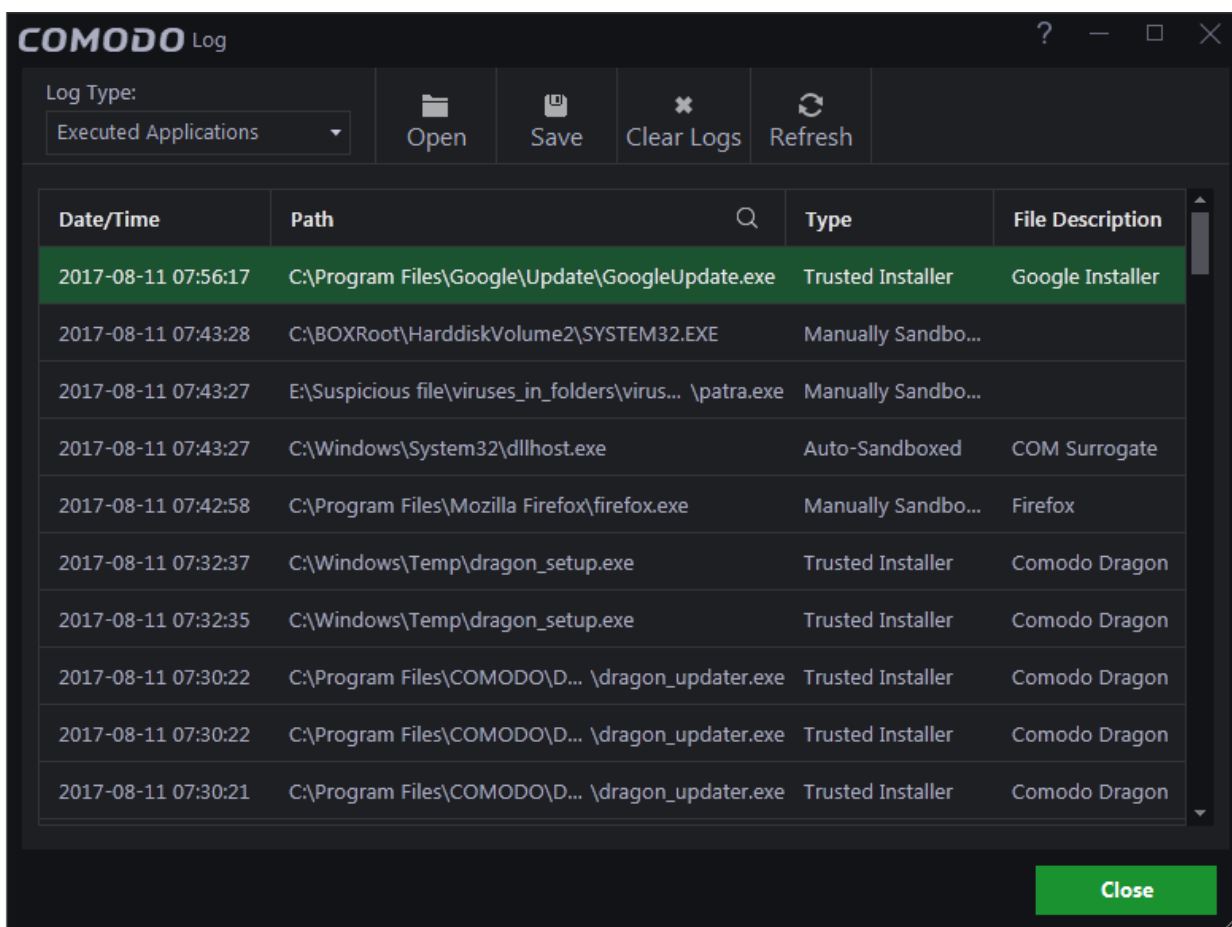
- To update the list with the latest antivirus events, click the 'Refresh' button
- To clear the antivirus logs, click the 'Clear Logs' button.

## 4.2. Executed Application Logs (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.

### To view Executed Applications Logs (Sandbox logs)

- Click 'View Logs' on the home screen OR click the 'View Logs' button on the widget
- Choose 'Executed Applications' from the 'Log Type' drop-down at top left:



Date/Time	Path	Type	File Description
2017-08-11 07:56:17	C:\Program Files\Google\Update\GoogleUpdate.exe	Trusted Installer	Google Installer
2017-08-11 07:43:28	C:\BOXRoot\HarddiskVolume2\SYSTEM32.EXE	Manually Sandbo...	
2017-08-11 07:43:27	E:\Suspicious file\viruses_in_folders\virus... \patra.exe	Manually Sandbo...	
2017-08-11 07:43:27	C:\Windows\System32\dlhhost.exe	Auto-Sandboxed	COM Surrogate
2017-08-11 07:42:58	C:\Program Files\Mozilla Firefox\firefox.exe	Manually Sandbo...	Firefox
2017-08-11 07:32:37	C:\Windows\Temp\dragon_setup.exe	Trusted Installer	Comodo Dragon
2017-08-11 07:32:35	C:\Windows\Temp\dragon_setup.exe	Trusted Installer	Comodo Dragon
2017-08-11 07:30:22	C:\Program Files\COMODO\D... \dragon_updater.exe	Trusted Installer	Comodo Dragon
2017-08-11 07:30:22	C:\Program Files\COMODO\D... \dragon_updater.exe	Trusted Installer	Comodo Dragon
2017-08-11 07:30:21	C:\Program Files\COMODO\D... \dragon_updater.exe	Trusted Installer	Comodo Dragon

### Column Descriptions

1. **Date/Time** - The precise date and time of the sandbox 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. **Cloud Rating** - Indicates the rating of the file, whether malicious, unknown or safe
- To export the logs as a '.log' file, click the 'Save' button

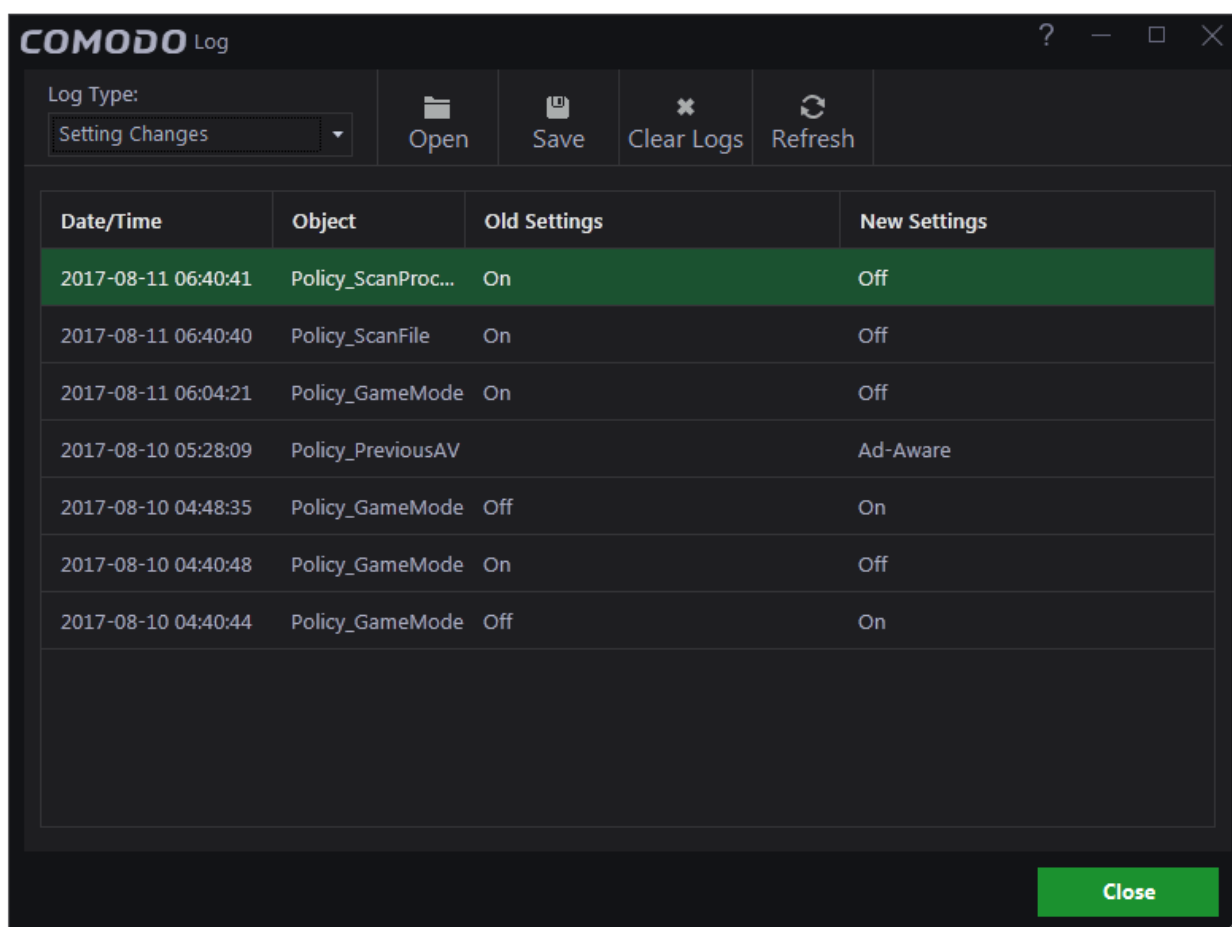
- To open a stored log file, click the 'Open' log file button
- To update the list with the latest events, click the 'Refresh' button
- To clear the 'Executed Application' logs, click the 'Clear Logs' button.

## 4.3. Setting Changes Logs

Setting changes logs are a record of all software configuration changes that you make.

To view 'Setting Changes' logs:

- Click 'View Logs' on the home screen OR click the 'View Logs' button on the widget
- Choose 'Setting Changes' from the 'Log Type' drop-down at the top left of the 'Log' interface



The screenshot shows the 'COMODO Log' window. At the top, there is a 'Log Type:' dropdown menu set to 'Setting Changes'. To the right of the dropdown are four buttons: 'Open', 'Save', 'Clear Logs', and 'Refresh'. Below this is a table with the following columns: 'Date/Time', 'Object', 'Old Settings', and 'New Settings'. The table contains several rows of log entries. A 'Close' button is located at the bottom right of the window.

Date/Time	Object	Old Settings	New Settings
2017-08-11 06:40:41	Policy_ScanProc...	On	Off
2017-08-11 06:40:40	Policy_ScanFile	On	Off
2017-08-11 06:04:21	Policy_GameMode	On	Off
2017-08-10 05:28:09	Policy_PreviousAV		Ad-Aware
2017-08-10 04:48:35	Policy_GameMode	Off	On
2017-08-10 04:40:48	Policy_GameMode	On	Off
2017-08-10 04:40:44	Policy_GameMode	Off	On

### Column Descriptions:

1. **Date/Time** - The precise 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

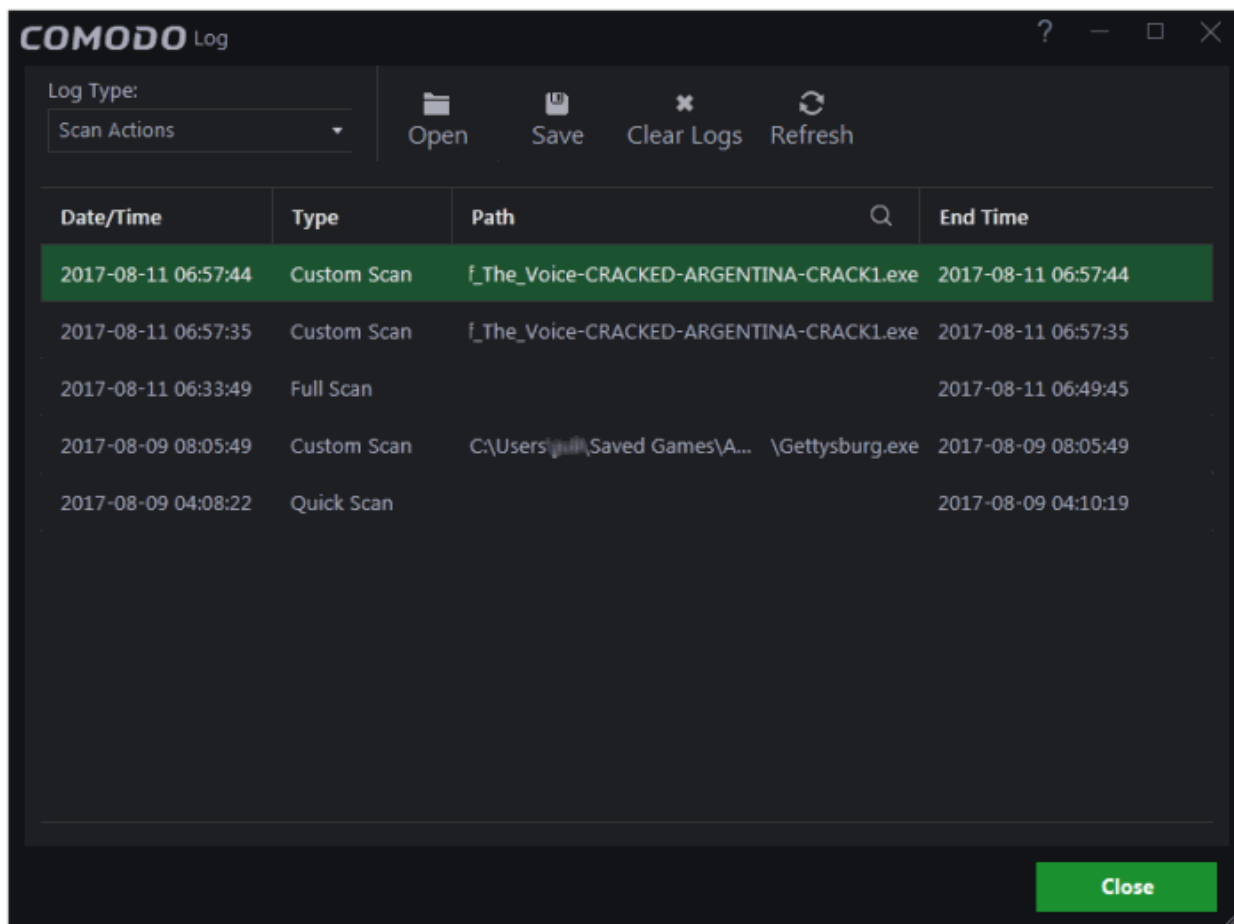
- To clear the 'Setting Changes' logs, click the 'Clear Logs' button.

## 4.4. Scan Actions Logs

CCAV keeps a record of all manually initiated virus scans. This includes manual full scans, quick scans, certificate scans and custom scans. Refer to [Scan and Clean your Computer](#) to read more about running a scan.

To view 'Actions' logs

- Click 'View Logs' on the home screen OR click the 'View Logs' button on the widget
- Choose 'Scan Actions' from the 'Log Type' drop-down at the top left of the 'Log' interface




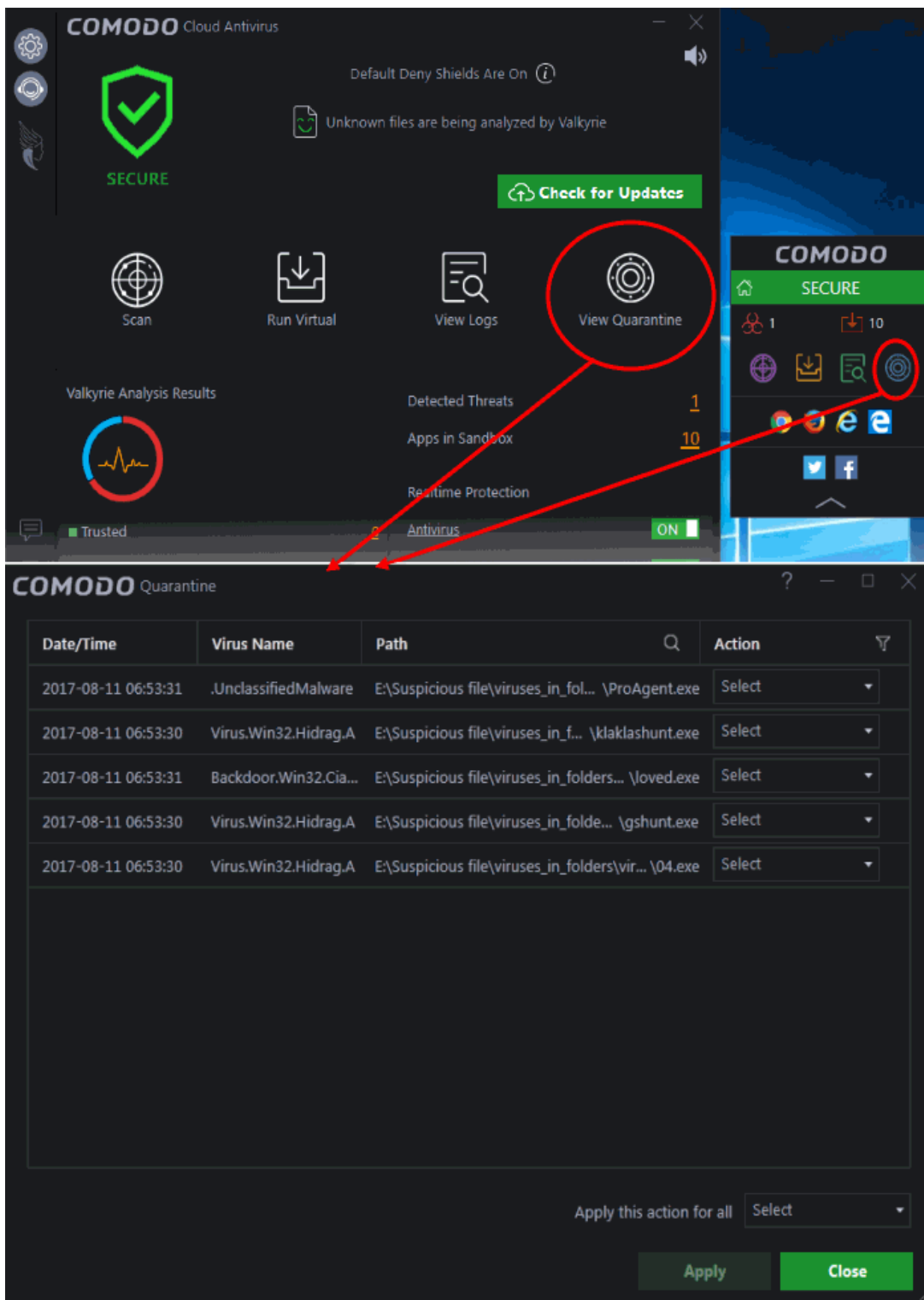
### Column Descriptions

1. **Date/Time** - The precise date and time of the scan
  2. **Type** - The type of scan
  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

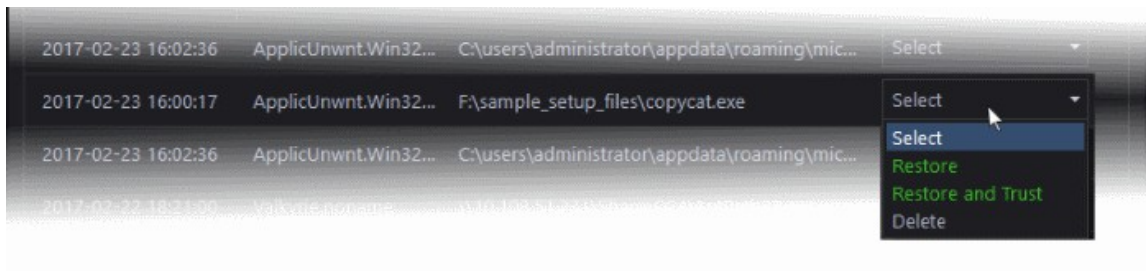
The 'Quarantine' interface displays a list of files which have been isolated by Comodo Cloud Antivirus to prevent them from infecting your system. Items are generally placed in quarantine as a result of an on-demand or real time antivirus scan. Any files transferred to quarantine are encrypted - meaning 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.

- Click 'View Quarantine' on the main interface
- OR
- Click the 'Quarantine' icon  on the CCAV desktop widget



## Column Descriptions

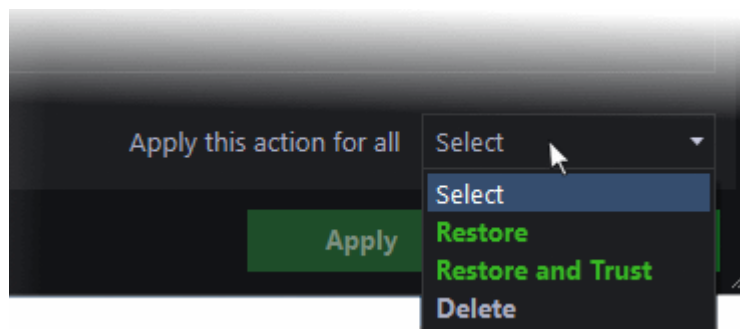
- **Date/Time** - The precise date and time at which the item was moved to quarantine
- **Virus Name** - The name of the malware that was quarantined
- **Path** - The location where the file was discovered
- **Action** - Displays a drop-down with options for handling the item.



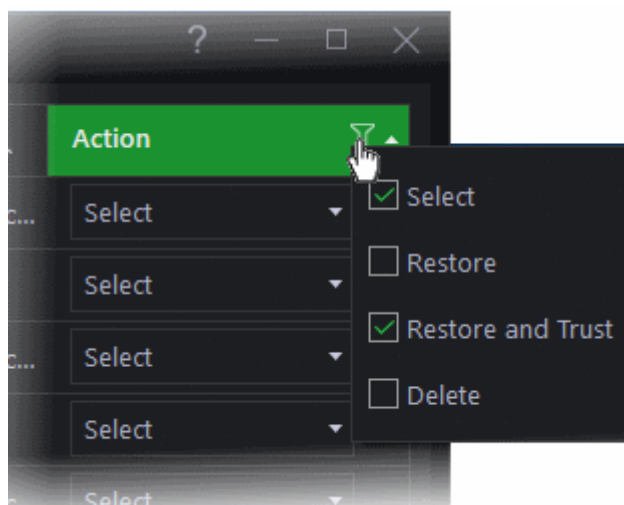
The available actions are:

- **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:

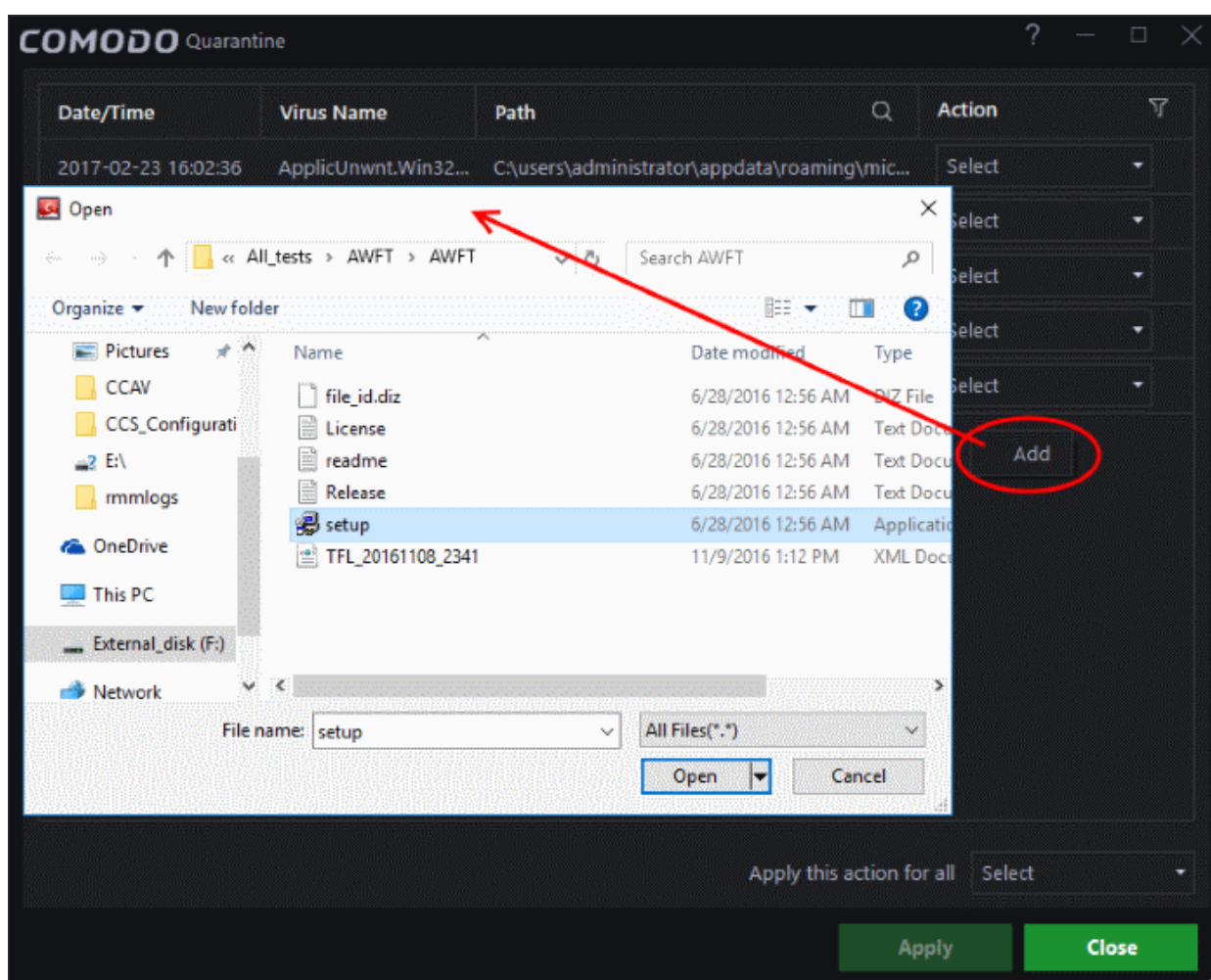
- **Manually add items to quarantine**
- **Delete quarantined items**
- **Restore a quarantined item to its original location**
- **Submit false positives to Comodo for analysis**

## Manually add items to quarantine

Files or folders that you are suspicious of can be manually moved to quarantine:

### To manually add a Quarantined Item

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



- 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.

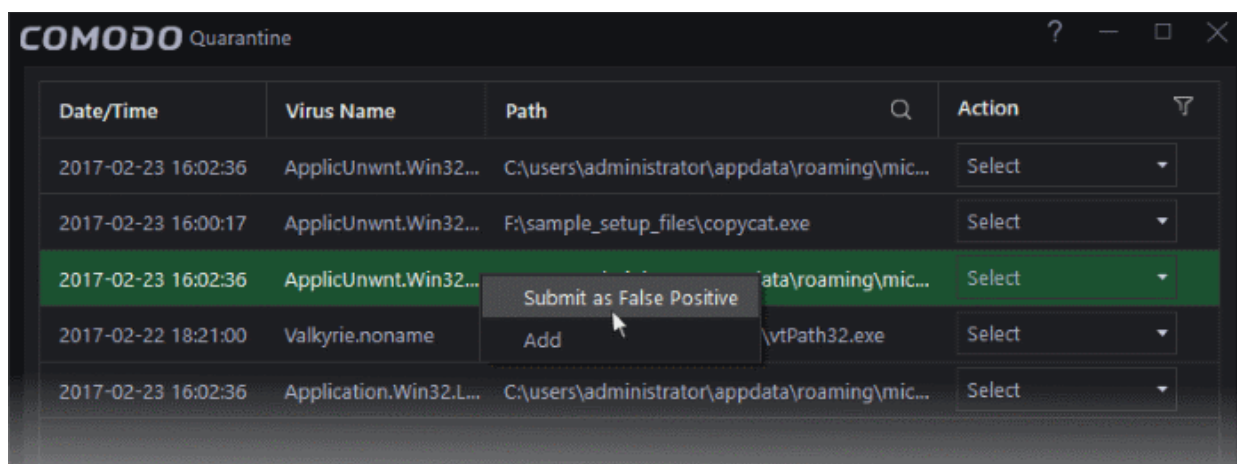
## To restore quarantined item(s) to its/their original location(s)

- 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.



- 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.

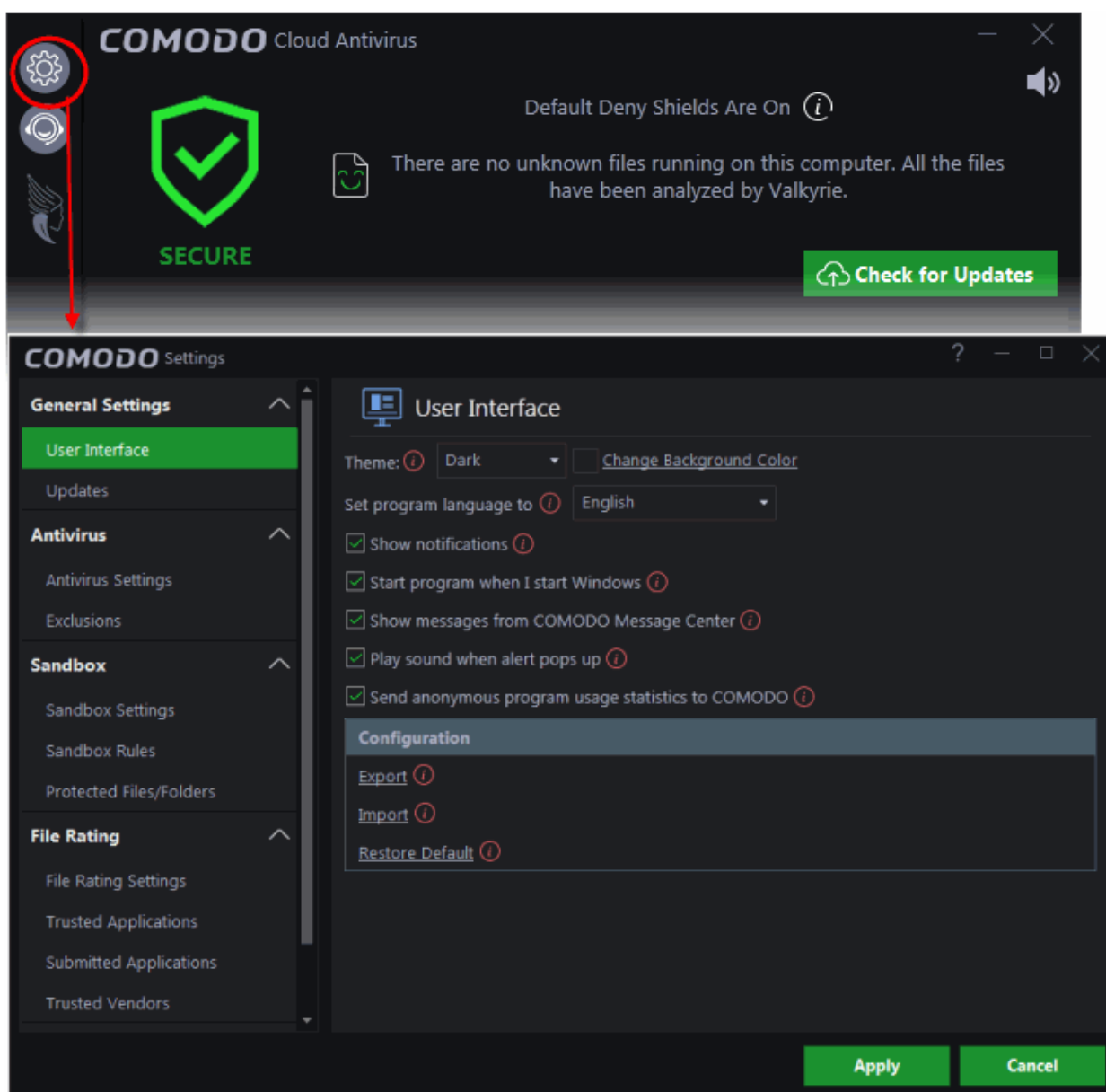
## 6. CCAV Settings

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 updates.
- The other sections let advanced users delve into granular configuration of the 'Antivirus', 'Sandbox', 'File Rating' and 'Advanced Protection' modules:



- The 'Antivirus' settings area lets you enable/disable real-time scanning, configure detection actions, create exclusions and more.
- The 'Sandbox' settings' area lets you configure the behavior of the Sandbox, add programs which should always run inside the sandbox and more.
- 'File Rating' settings lets you add trusted files to be excluded from scans and monitoring, view files submitted to Comodo for analysis and to manage the 'Trusted Vendors' list.
- The 'Advanced Protection' area lets you configure whether 3rd party applications are allowed to modify browser settings.
- To open the 'Settings' interface, click 'Settings' from the top menu



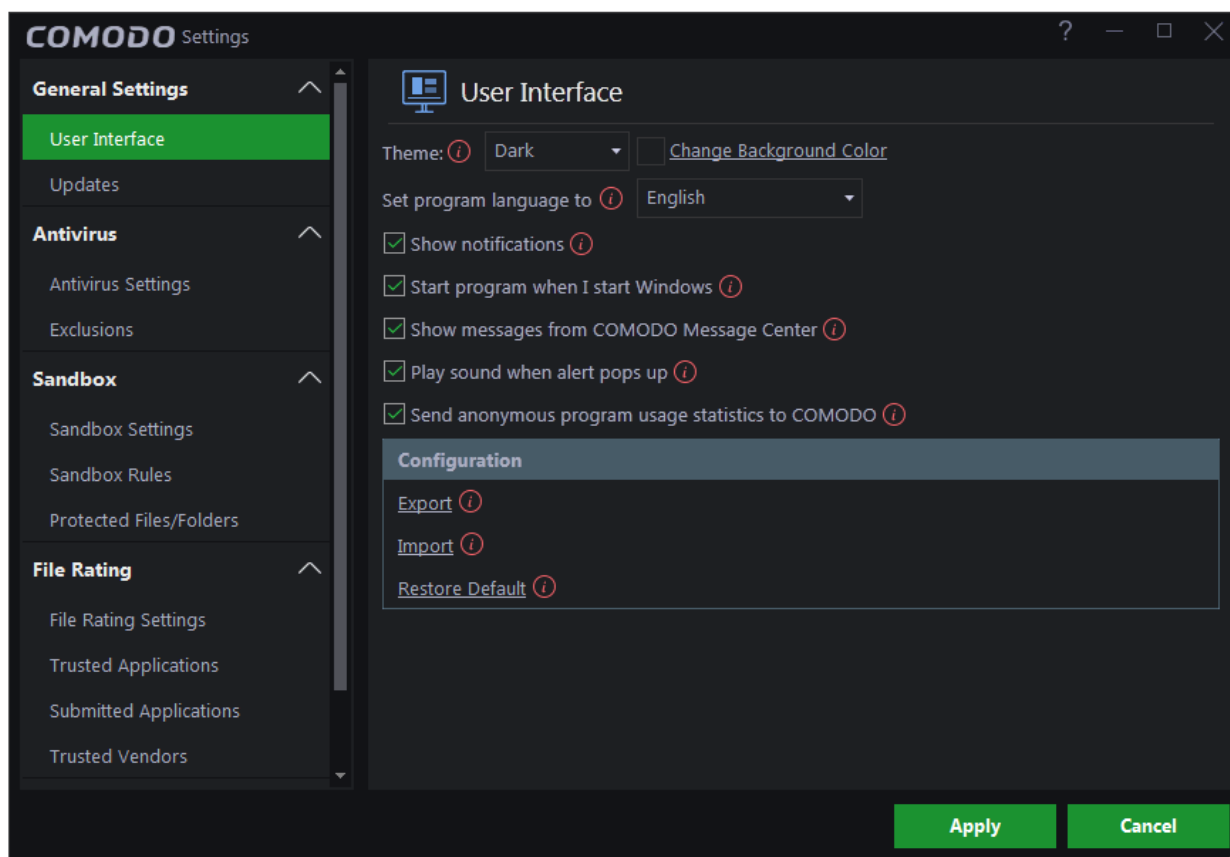
The following sections explain the various settings areas in more detail:

- **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**
  - **Protected Data Folders**
- **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 Applications**
  - **Trusted Vendors**
- **Advanced Protection** - Allows you to configure whether applications are allowed or blocked from modifying browser settings.
  - **Browser Settings Protection**

## 6.1. General Settings

The 'General Settings' area enables you to customize the appearance, theme, background color and overall behavior of Comodo Cloud Antivirus. You can configure general properties like the interface language, notification messages, automatic updates and more. Also, you can export the current CCAV configuration as an XML file and import configurations when needed.



The category has the following sections:

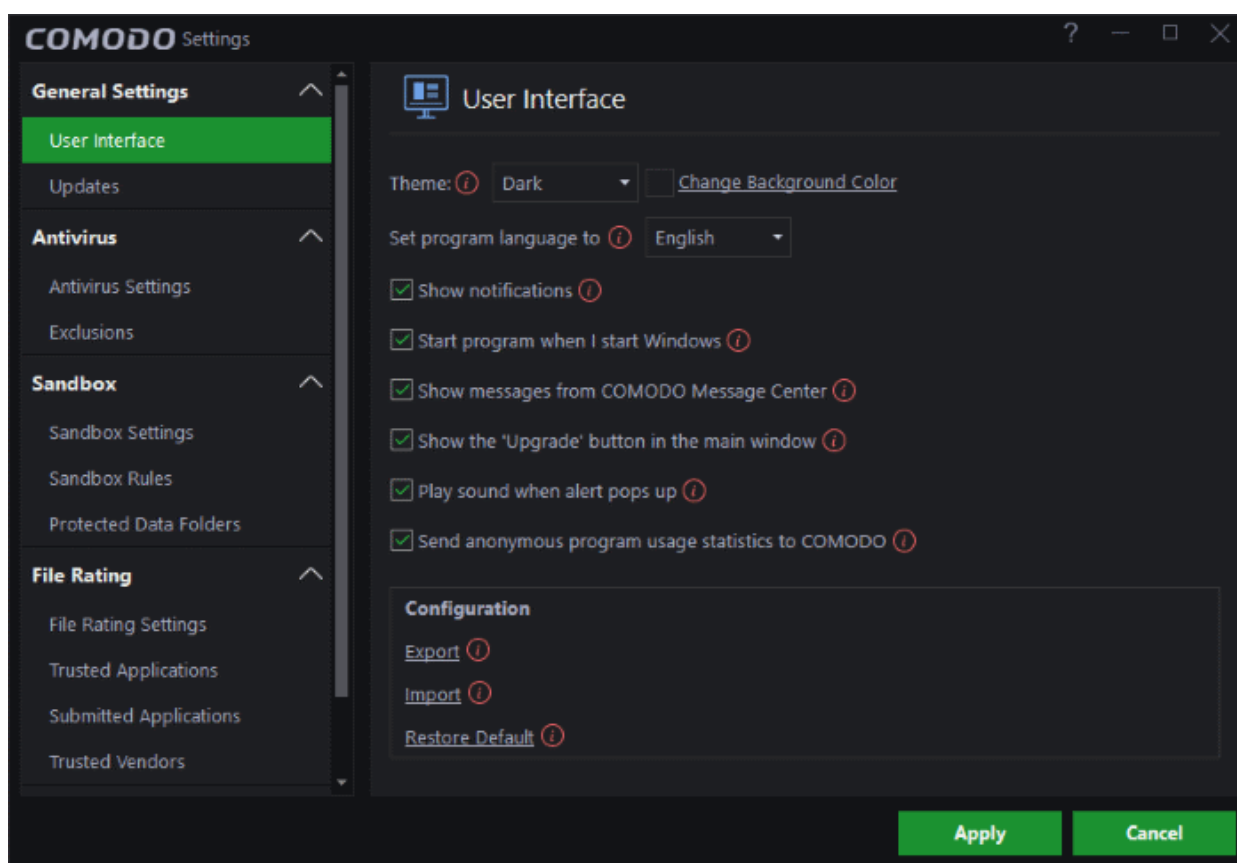
- **User Interface**
- **Updates**

## 6.1.1. Customize User Interface

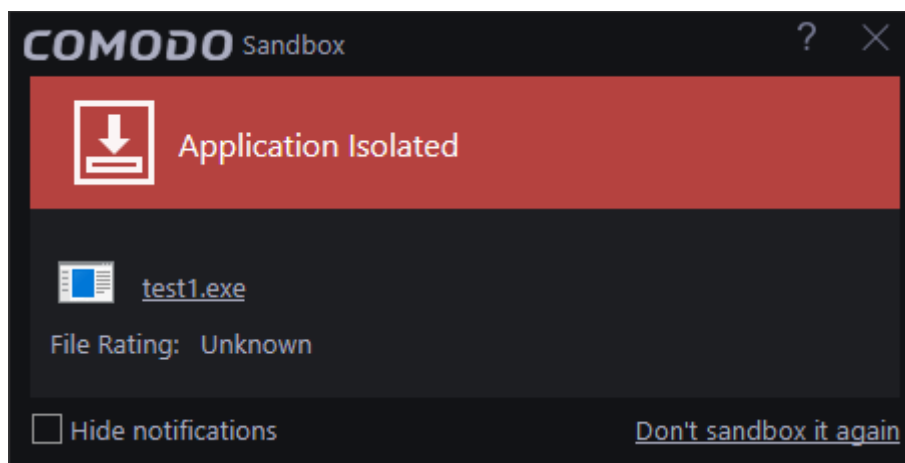
The 'User Interface' settings area lets you choose the interface language, theme, background color, startup options and how messages should be displayed. You can export your current CCAV configuration as an XML file, allowing you to import the configuration to other computers, or to quickly re-implement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

To open 'User Interface' settings,

- Click the 'Settings' icon on the left of the home screen
- Click 'User Interface' under 'General Settings' on the left:



- **Theme Settings** - The 'Themes' drop-down allows you to choose colors and appearance of the GUI as you prefer. (*Default = Dark theme and background color*)
- **Language Settings** - Comodo Cloud Antivirus is available in multiple languages. You can choose the language which is displayed in the interface from the 'Set program language to' drop-down. (*Default = English*)
- **Show notifications** - CCAV displays notifications at the bottom-right corner of your screen to inform you about actions that it is taking and about any CCAV 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.



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*)



- **Play sound when alert pops up** - CCAV generates a chime whenever it raises a security alert to grab your attention. If you do not want the sound to be generated, clear this check box. (*Default = Enabled*)
  - **Send anonymous program usage statistics to COMODO** - If enabled, CCAV will periodically send anonymous program usage statistics to Comodo servers through a secure and encrypted channel. This data is useful to Comodo as it helps us identify the areas of the program which need to be improved. Disable this option if you do not want to send usage statistics (*Default = Enabled*)
- Click 'Apply' for your changes to take effect

**Exporting your Security Configuration** - Allows you to export your current CCAV configuration, including your custom Antivirus settings, Sandbox settings, Sandbox rules etc. to an XML file, and to reset CCAV configuration back to factory settings. You can also import configurations from a saved .XML file. This is especially useful if you are a network administrator looking to roll out a standard security configuration across multiple computers. Exporting your

settings can also be a great time-saver if you get a new computer. After re-installing CCAV you can import your previous settings to avoid having to configure everything over again.

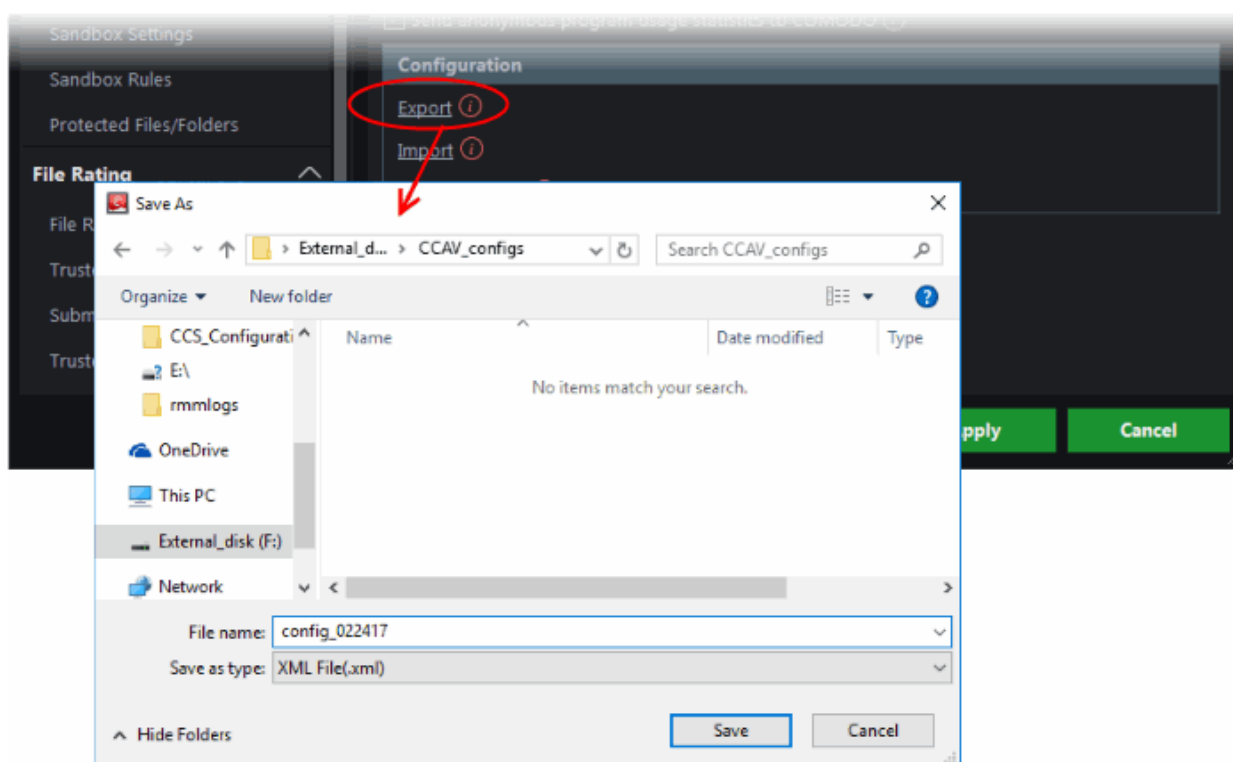
The following sections explain how to:

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

## To export your current configuration

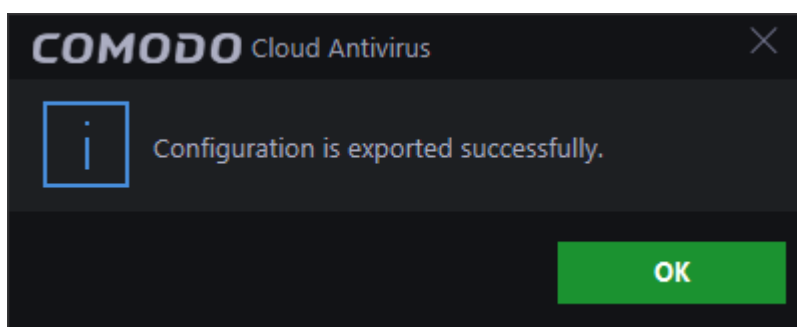
- Click the 'Export' link in the 'User Interface' settings area

The 'Save As' dialog will open:



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

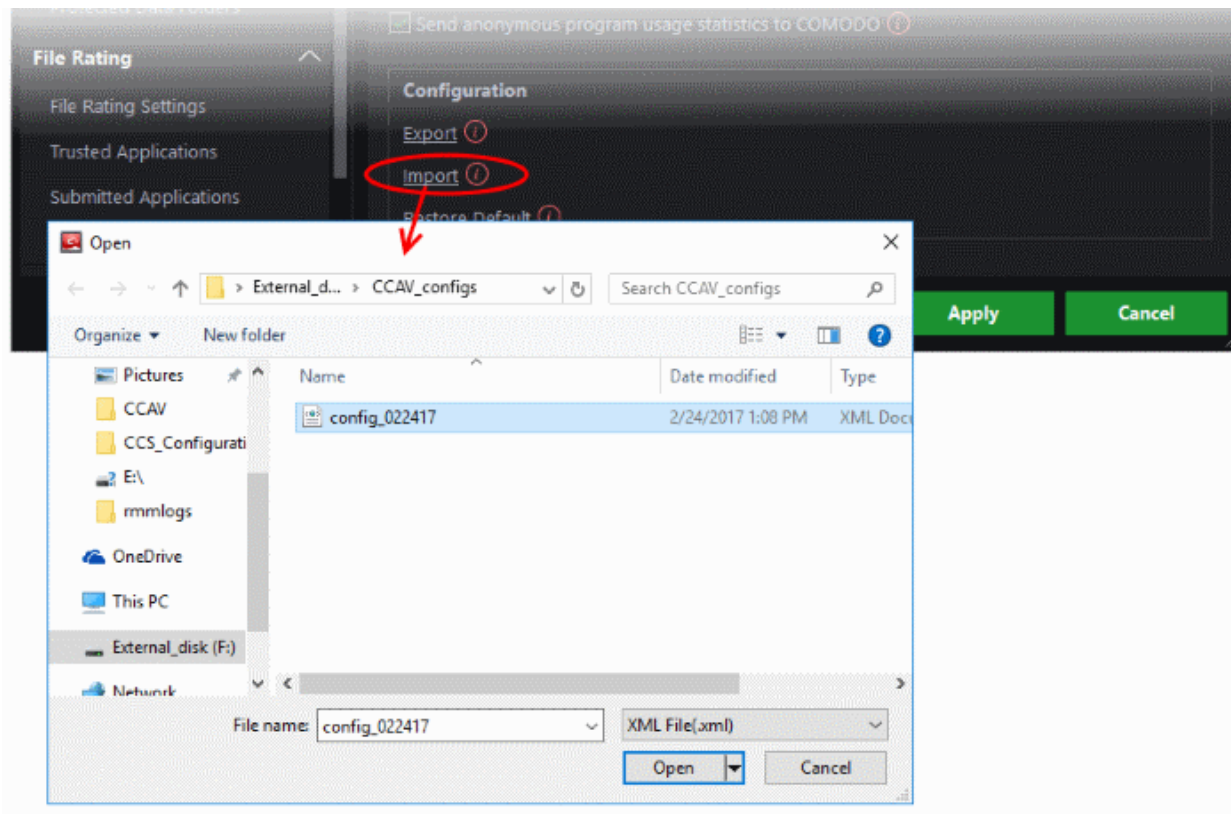
A confirmation dialog will appear indicating the successful export of the profile.



## Import a saved configuration from a file

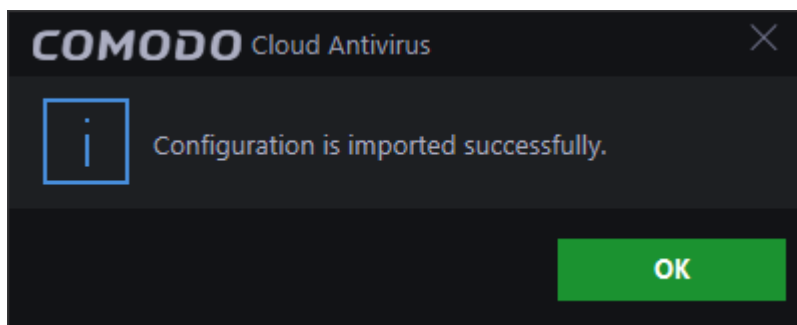
- Click the 'Import' link in the 'User Interface' settings area

The 'Open' dialog will open:



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

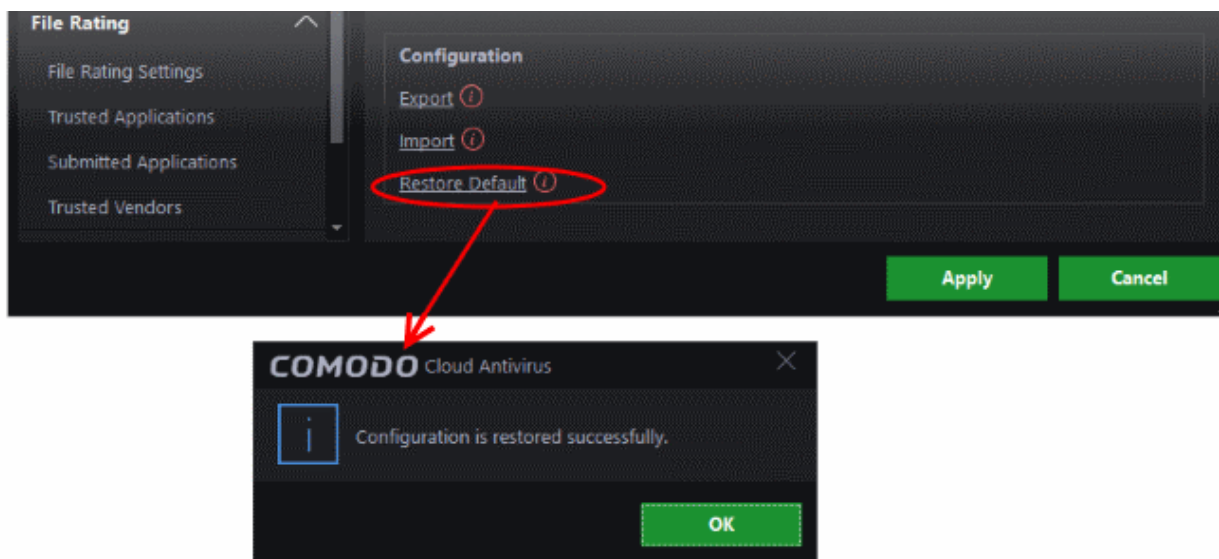
A confirmation dialog will appear indicating the successful import of the profile:



## Restore your CCAV installation to Factory Default settings

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

A dialog box confirming the theme and settings changes will be shown:

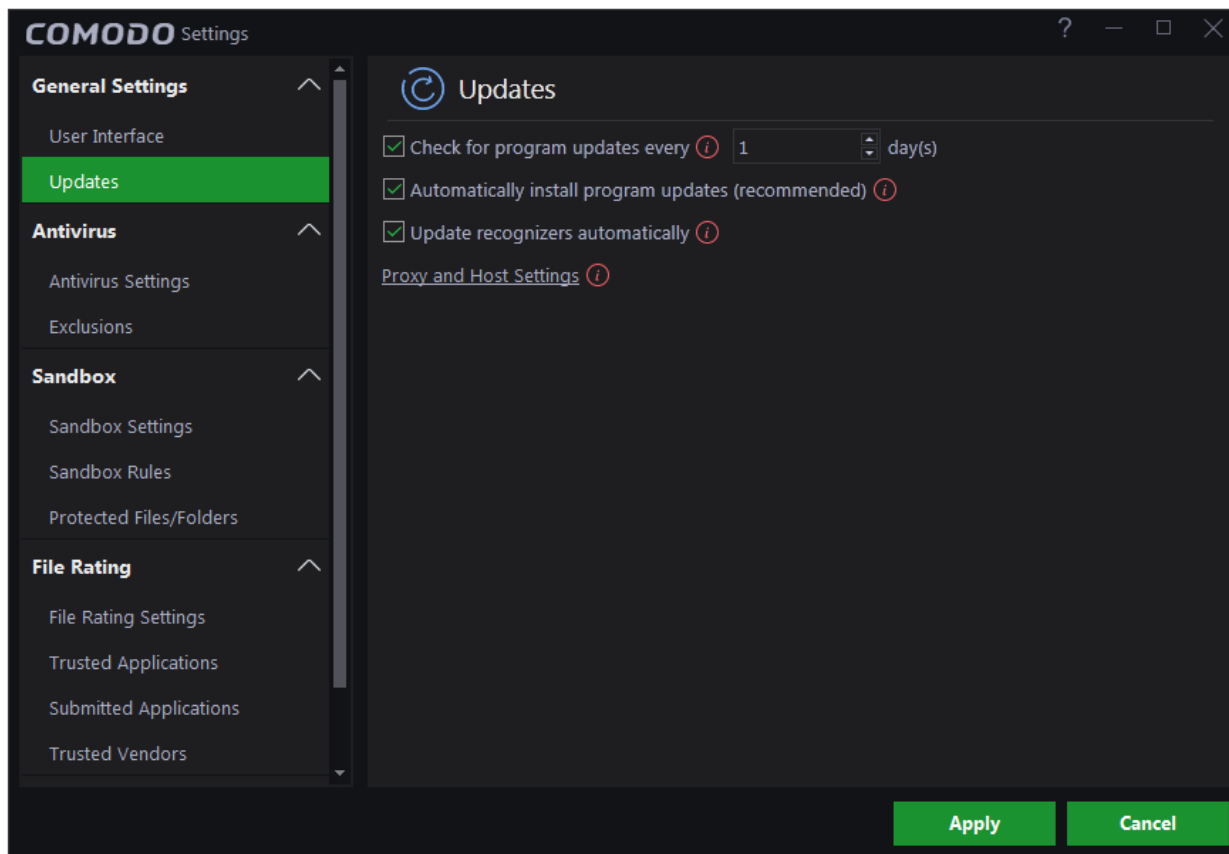


## 6.1.2. Configure Program Updates

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

To open update settings:

- Click the 'Settings' icon on the left of the home screen
- Click 'Updates' under 'General Settings' on the left:



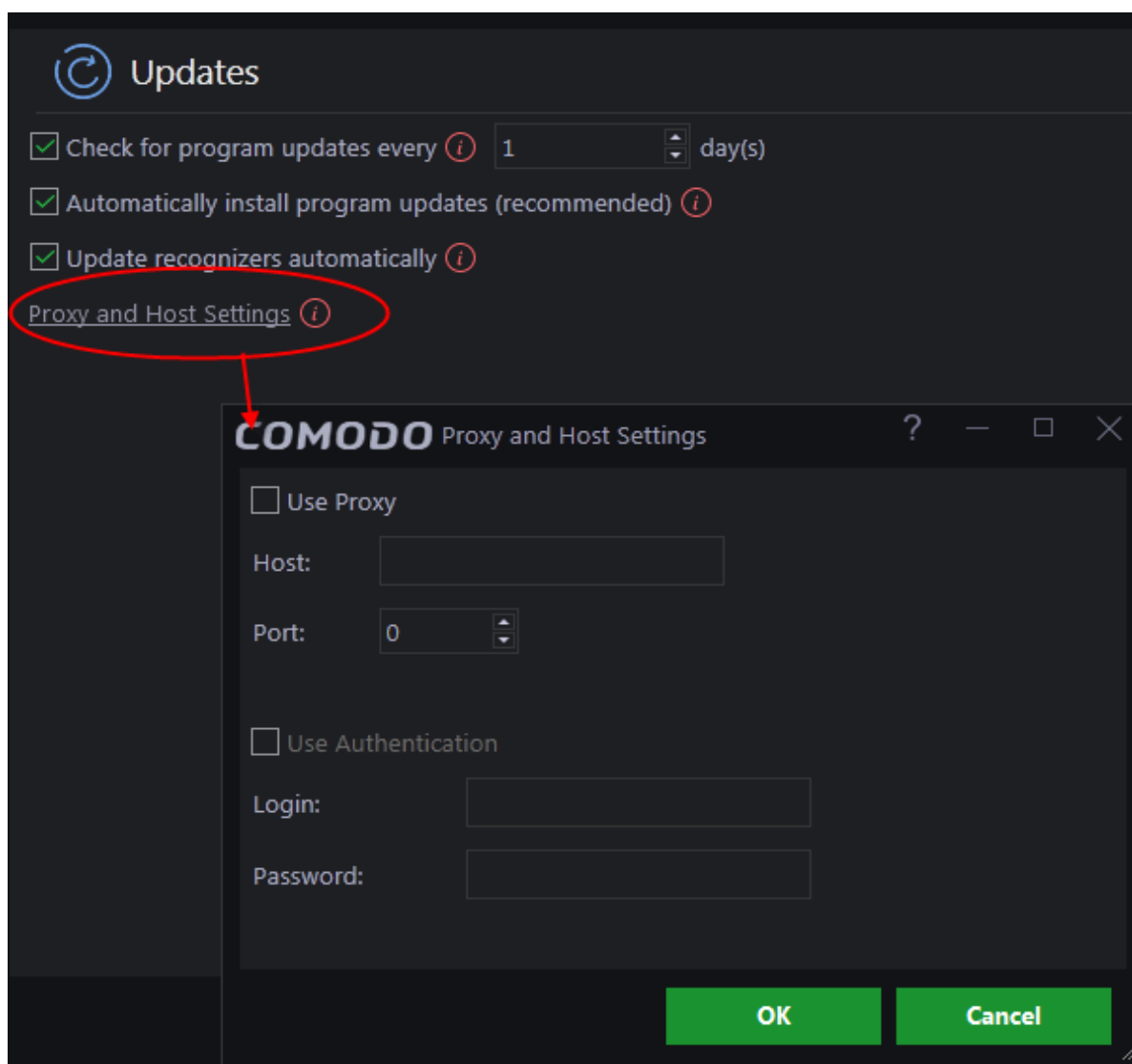
- **Check program updates every NN day(s)** - Enables you to specify the interval at which CCAV will check Comodo servers for the availability of new versions and program updates. Set the time

interval (in days) from the drop-down combo box. (*Default = 1 day*)

- **Automatically install program updates (recommended)** - CCAV automatically downloads and installs program updates as soon as they are available. (*Default=Enabled*)
- **Update recognizers automatically** - If enabled, CCAV will automatically download and implement any new recognizers which become available. (*Default = Enabled*)
- **Proxy and Host Settings** - Allows you to select the host from which updates are downloaded. By default, CCAV downloads updates from Comodo servers. However, advanced users and network admins may wish to first download updates to a proxy/staging server and have individual CCAV installations collect the updates from there. The 'Proxy and Host Settings' interface allows you to point CCAV at this proxy/staging server. This helps to conserve bandwidth and accelerate the update process when a large number of endpoints are involved.

### To configure updates via proxy server

- Click 'Proxy and Host Settings' link. The 'Proxy and Host Settings' interface will open:



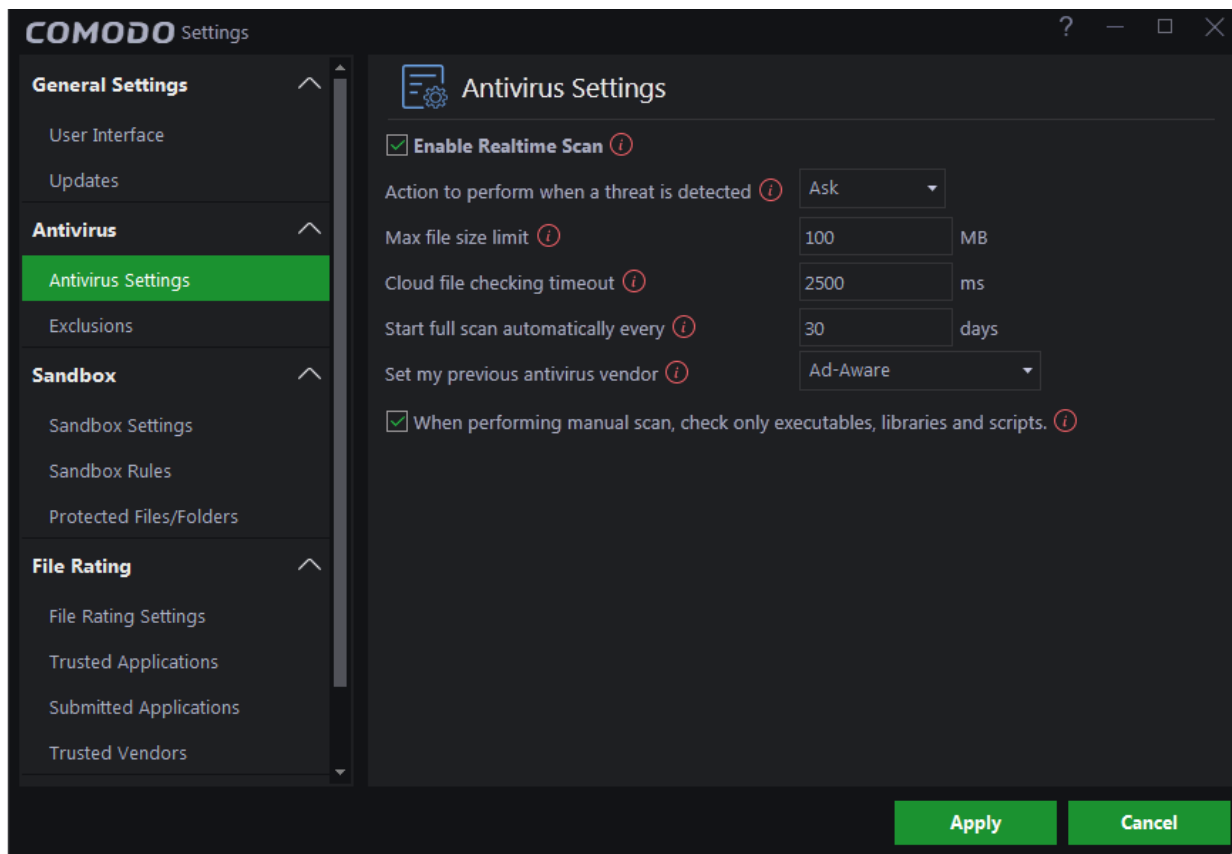
- Enable the 'Use Proxy' check-box.
- Enter the host name and port numbers. If the proxy server requires access credentials, select the 'Use Authentication' check-box and enter the login / password accordingly.
- Click 'OK' for your settings to take effect.



- 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.



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

- [Antivirus Settings](#)
- [Exclusions](#)

### 6.2.1. Antivirus Settings

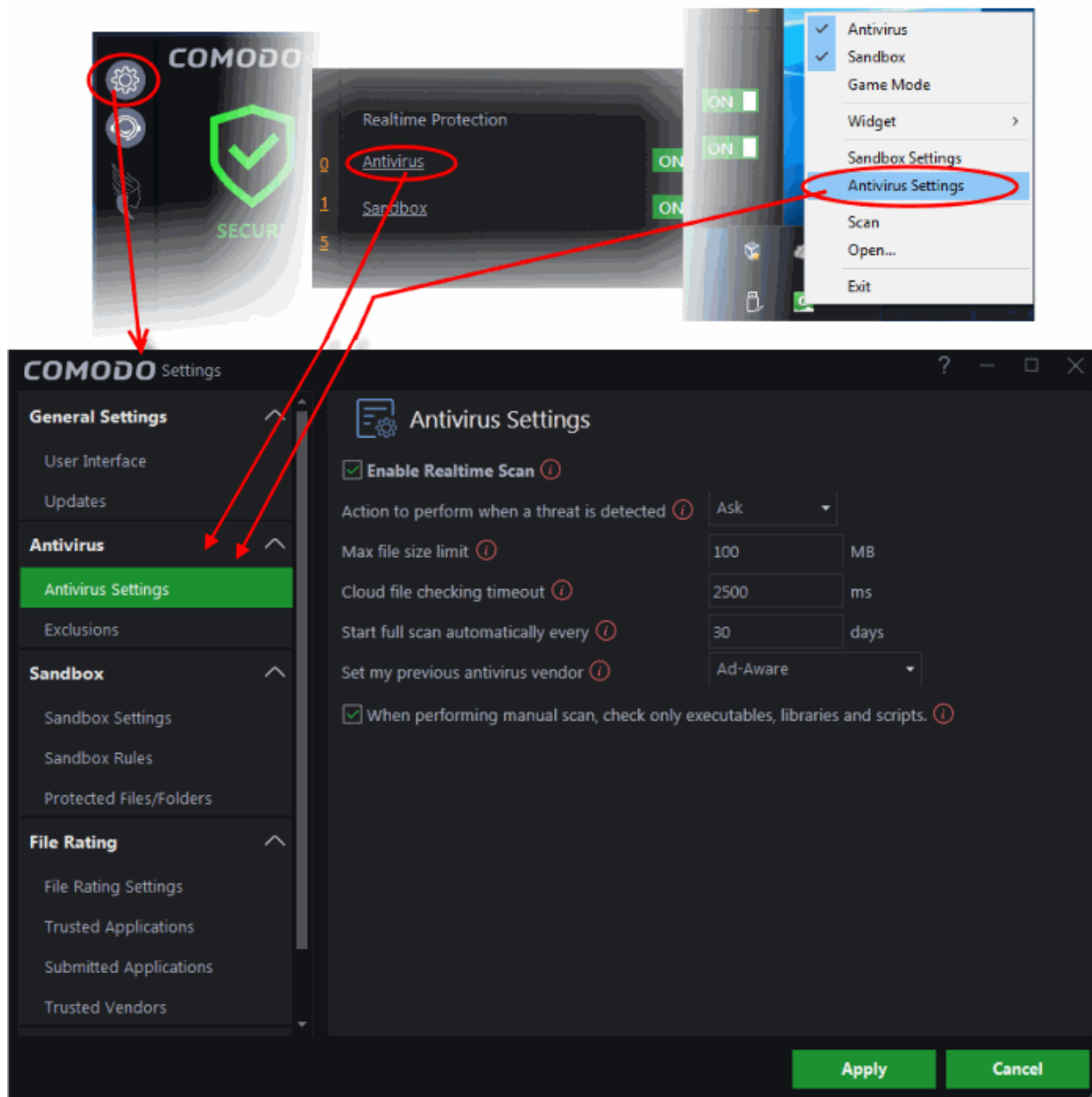
CCAV's real-time scanner constantly monitors all files and processes on your computer for potential threats. If you launch a program or a file which poses a threat, then the scanner blocks it and alerts you immediately. The Antivirus settings interface allows you to enable/disable the real-time scanner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

#### To open the 'Antivirus Settings' area

This can be done in three ways:

1. Click the 'Settings' icon on the left then 'Antivirus' > 'Antivirus Settings'  
OR
2. Click the 'Antivirus' link under 'Realtime Protection'  
OR

3. Right-click the CCAV system tray icon (or the widget) and choose 'Antivirus Settings' from the options.



- **Enable Realtime Scan** - Enable or disable Real-time virus monitoring. It is strongly recommended you leave this option selected. (*Default = Enabled*)

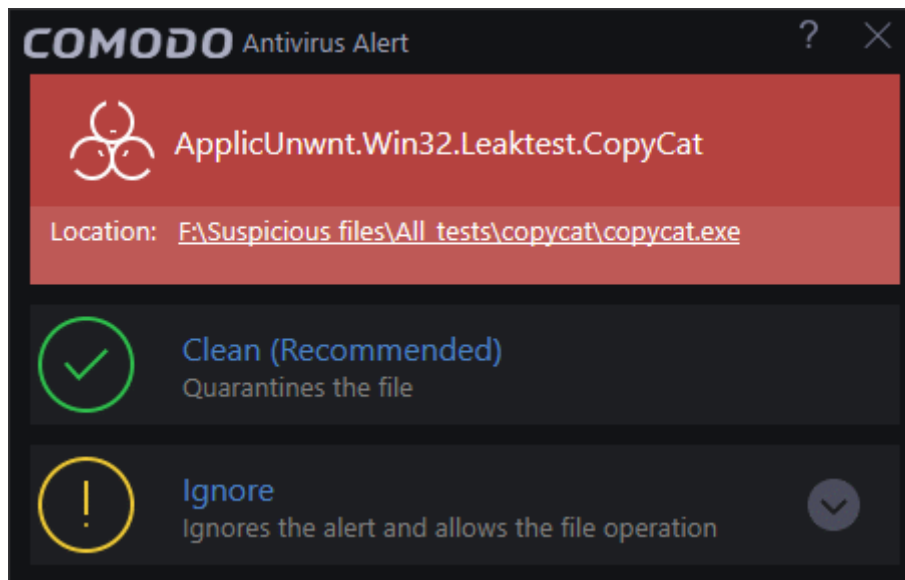
**Background Note:** The real-time scanner (aka 'On-Access Scan') is always ON and checks files in real time when they are created, opened or copied (as soon as you interact with a file, Comodo Cloud Antivirus checks it). This instant detection of viruses assures you, the user, that your system is perpetually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

- **Action to perform when a threat is detected** - Configure how CCAV should react when malware is detected by the real-time protection engine (*Default = Alert*).

The available options are:

- **Ask** - An alert will be displayed whenever a malware is identified. An example of antivirus alert is shown below:



You can choose to clean, ignore, submit the file as false alert or add the file to trusted files list. If you need more details about these 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 the 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 scanned. (*Default = 100 MB*)
- **Cloud file checking timeout** - Allows you to configure 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 will be skipped (*Default = 2500 Ms*)
- **Start full scan automatically every** - Allows you to schedule a full scan to run automatically after a set number of days. (*Default = 30 days*)
- **Set my previous antivirus vendor** - Allows you to specify your previous antivirus software vendor for the 'Lucky You' statistics page. Once set, the 'Lucky You' page will show you how many threats have been blocked by CCAV that would have been allowed by your previous vendor. See **'Lucky You' Statistics** for more details.
- **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 details on on-demand/manual scans, refer to the section **Scan and Clean your Computer**. (*Default = Enabled*)

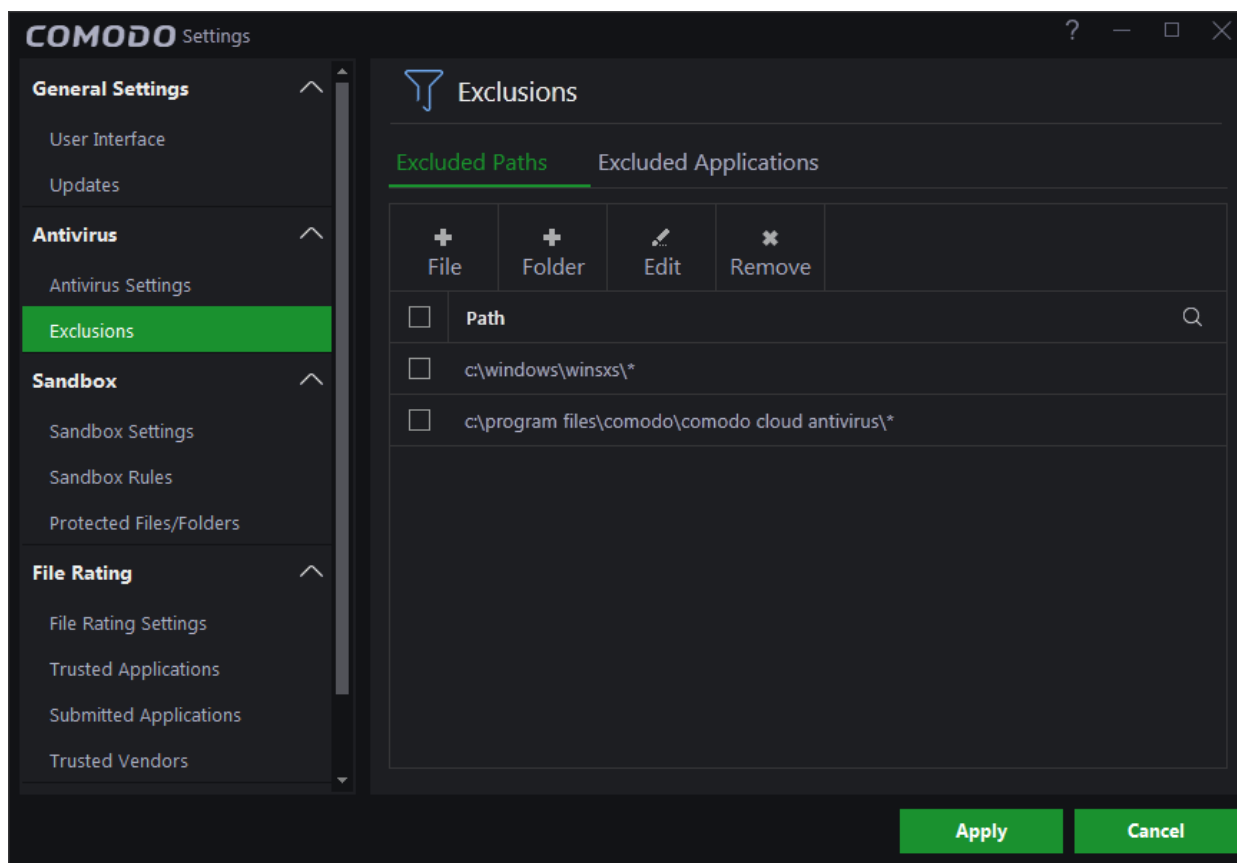
## 6.2.2. Exclusions

CCAV allows you to create a list of files and folders that should be excluded from antivirus scans. This list also includes files for which you have selected '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

- Click the 'Settings' icon on the left of the home screen
- Select 'Antivirus' then 'Exclusions'



The 'Exclusions' panel has two tabs:

- **Excluded Paths** - Displays a list of paths/folders/files on 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 applications which are excluded from real-time antivirus scans. Items can be excluded by clicking 'Ignore' in the virus **Scan Results** or by clicking 'Ignore' at an **Antivirus Alerts**, or by excluding it manually. Note - excluded items are skipped by the real-time scanner but will be scanned during on-demand scans. Refer to **Excluding Programs/Applications from real-time scans** for more details on manually adding and removing exclusions.

### Excluding Drives/Folders/Files from all types of scans

You can exclude items from any type of virus scan by adding them to 'Excluded Paths'.

#### To add file to excluded paths

- Click the 'Excluded Paths' tab from the 'Exclusions' interface

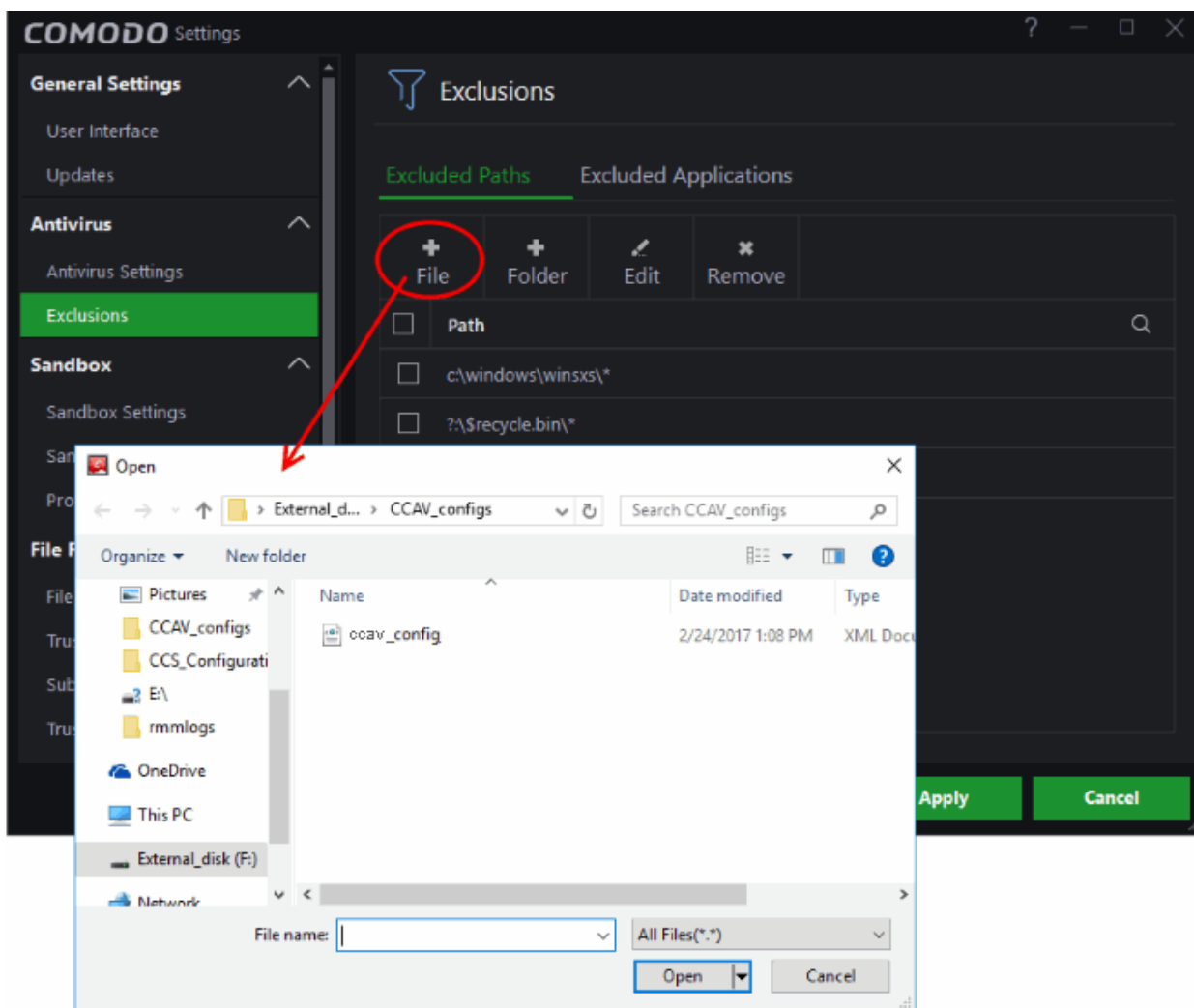
You can add a:

- **An individual File**
- OR
- **Drive partition/Folder**

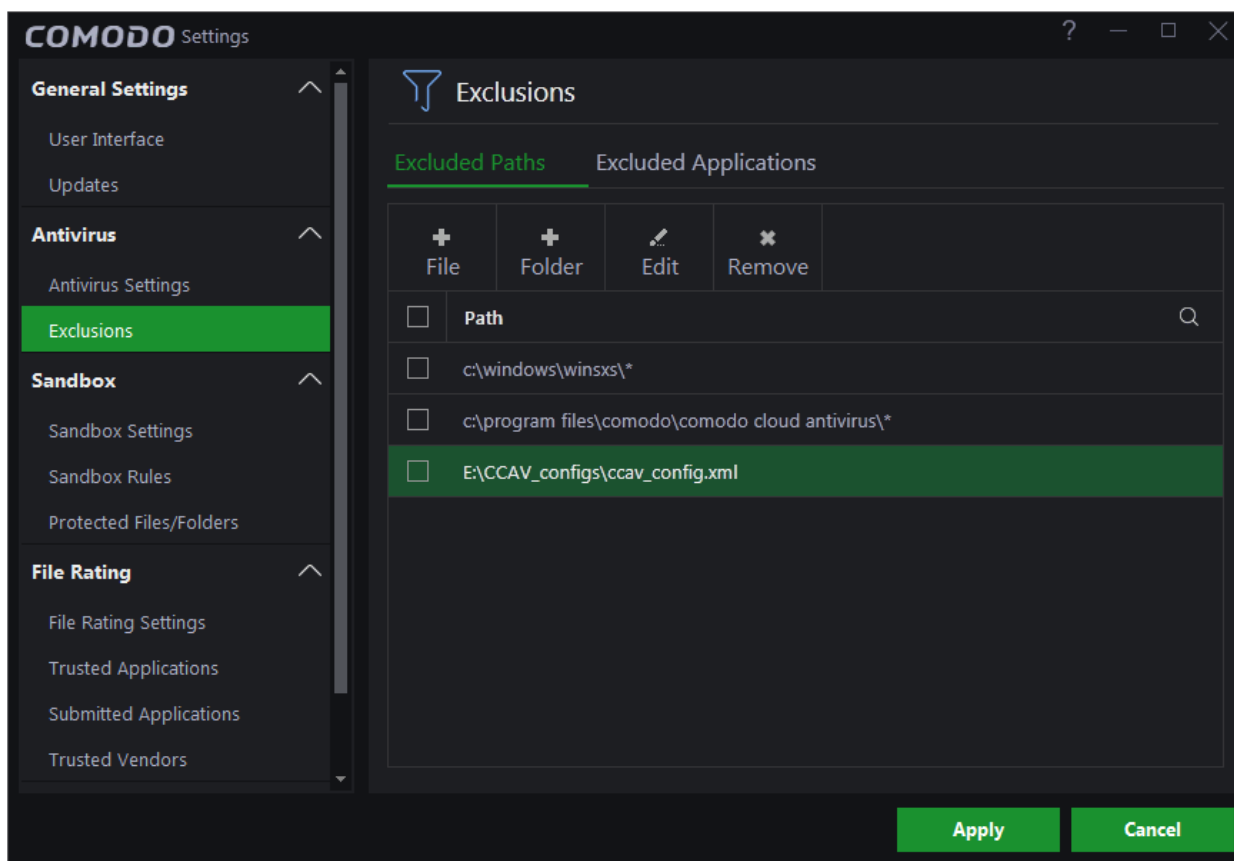
## Adding an individual File

You can specify individual files as excluded path.

- Click 'Settings' on the CCAV home screen
- Click 'Antivirus' > 'Exclusions'
- Choose 'File' at the top



- Navigate to the file you want to add to excluded paths and click 'Open'.

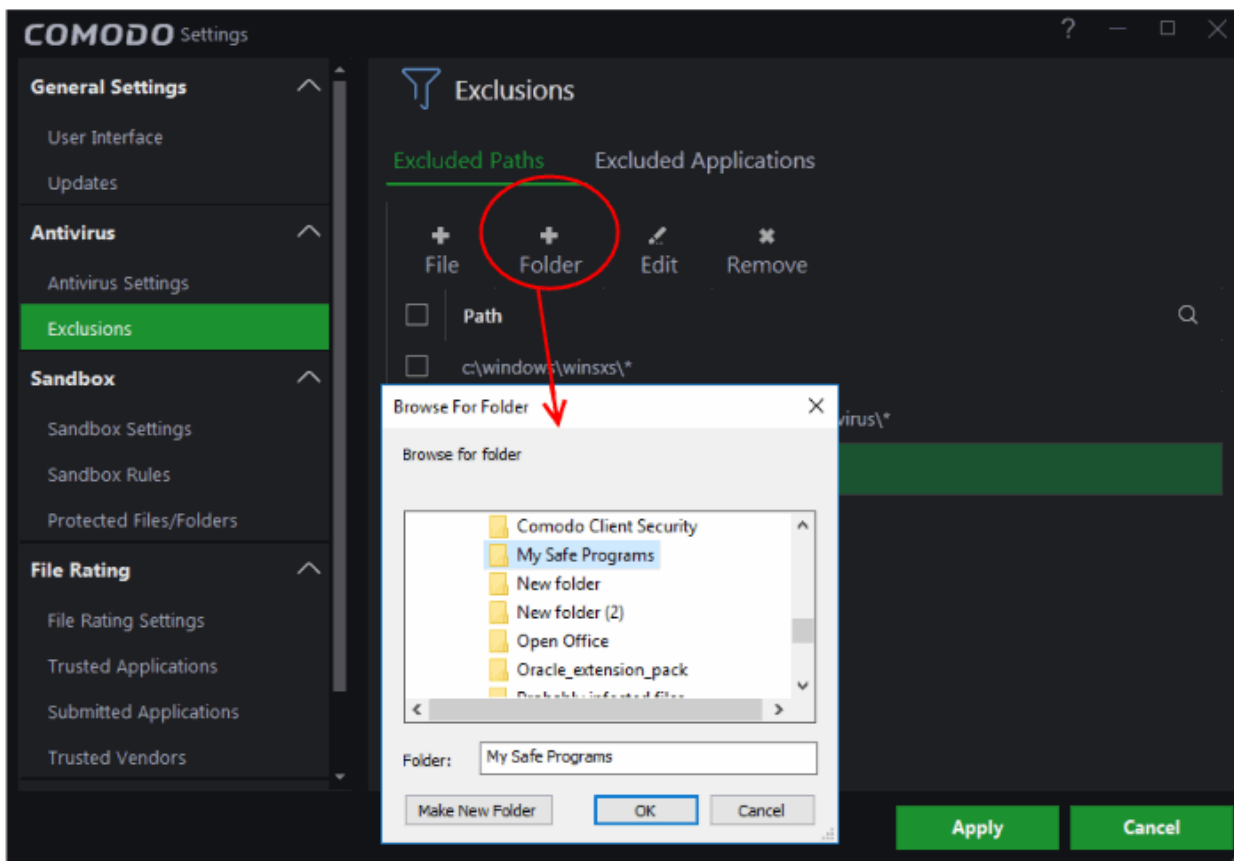


The file will be added to excluded paths.

- Repeat the process to add more paths.
- Click 'Apply' for your settings to take effect. Items added to 'Excluded Paths' will be omitted from all types of virus scan in the future.

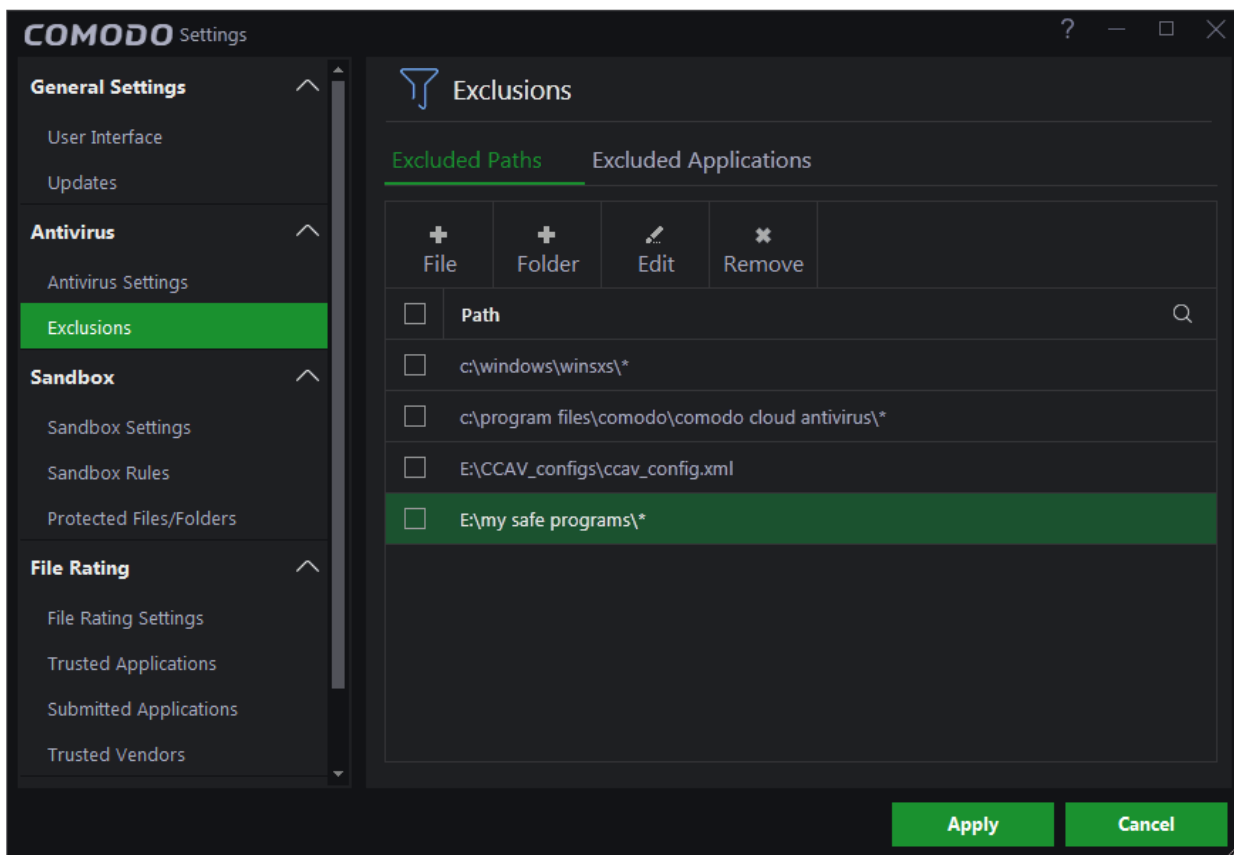
### Adding a Drive Partition/Folder

- Click 'Settings' on the CCAV home screen
- Click 'Antivirus' > 'Exclusions'
- Select 'Excluded Paths'
- Choose 'Folder' at 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'.

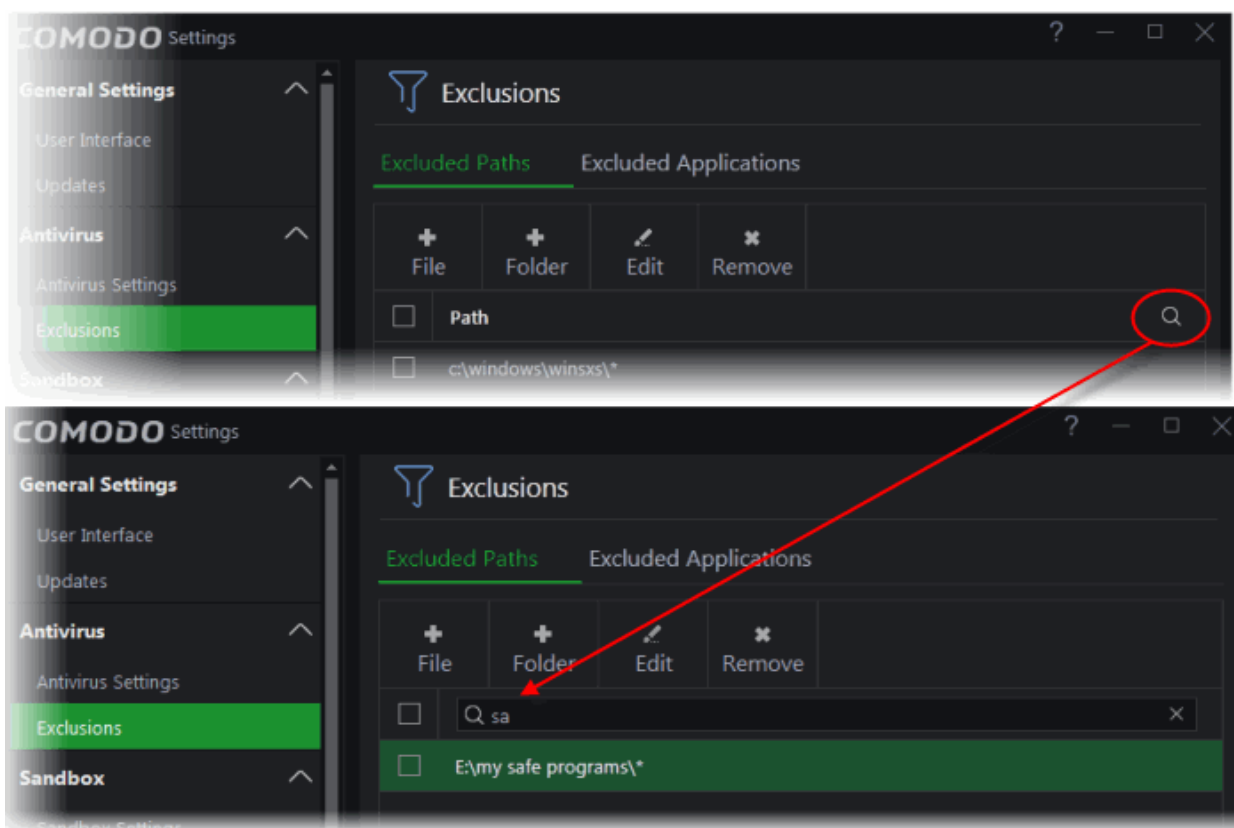


The folder/partition will be added to the list of excluded items:

- Repeat process to add more folders
- Click 'Apply' for your settings to take effect. Items added to 'Excluded Paths' will be omitted from all types of antivirus scans in future.

## Search Options

You can use the search option to find a specific excluded path, folder or file from the list by clicking the search icon at the top right.

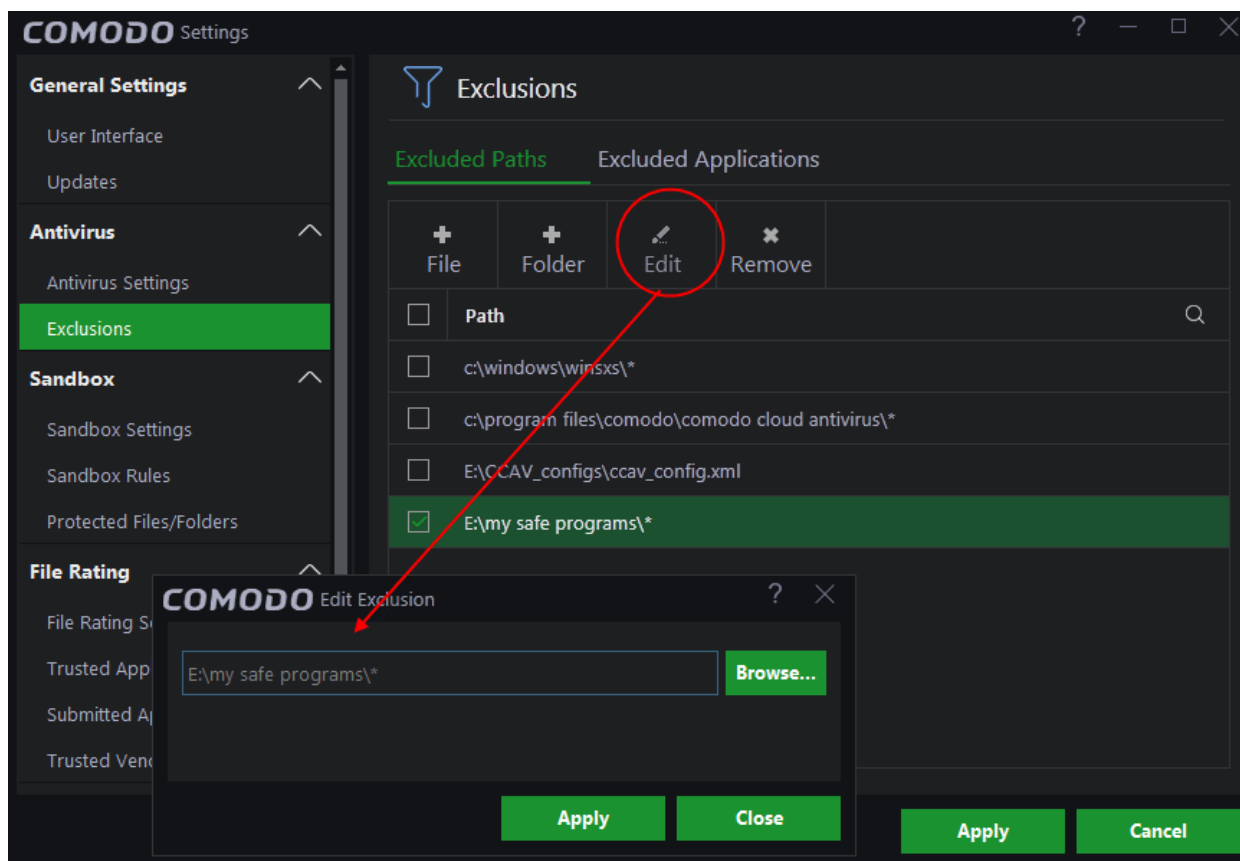


- Enter the path, folder name or file name to be searched in full or part in the search field.
- The search results will be displayed.
- Click the icon 'X' in the search field to close the search option.

## To edit the path of an added item

- Double click on the item
- OR
- Select the target item and click 'Edit at the top'

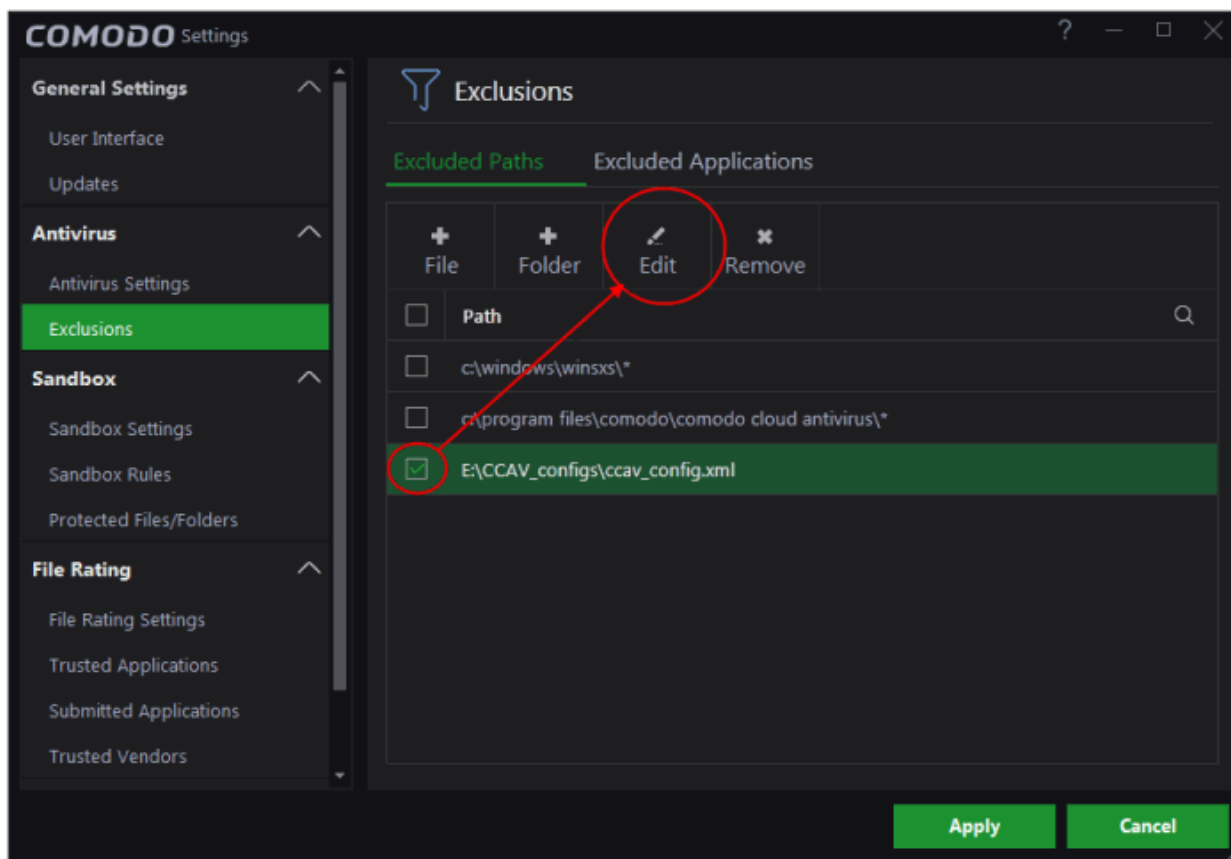




- Next, click the 'Browse...' button and navigate to the file you want to modify or make the required changes for the file path in the 'Edit Exclusion' dialog and click 'Apply'.

## To remove item(s) from Excluded Paths

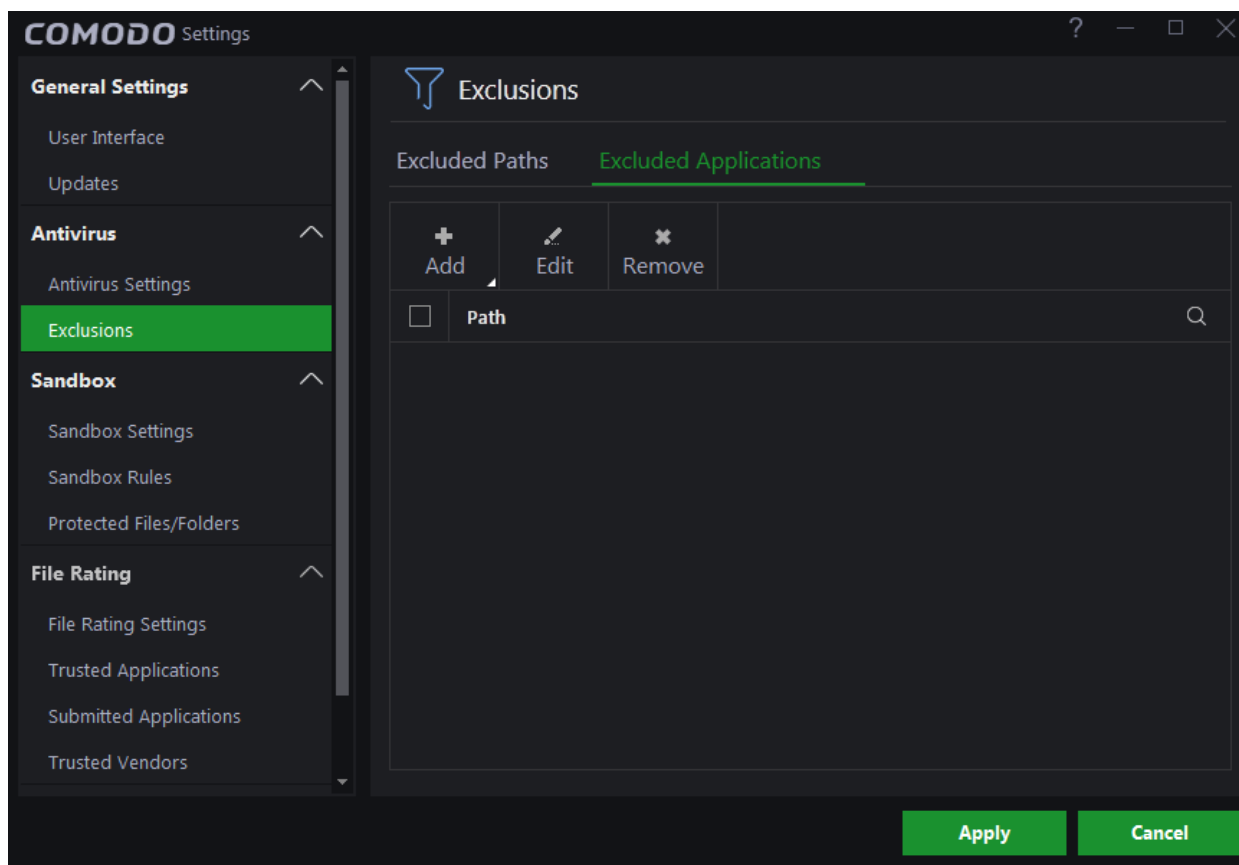
- Select the target item(s) and click 'Remove' at the top:



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

## Excluding Programs/Applications from Real-time Scans

- The 'Excluded Applications' screen lets you exclude programs from real-time virus scans.
- Applications which you chose to 'Ignore' in an antivirus alert or in the **Scan Results** window are automatically added to this list.
- You can manually add and remove programs to/from the list as required

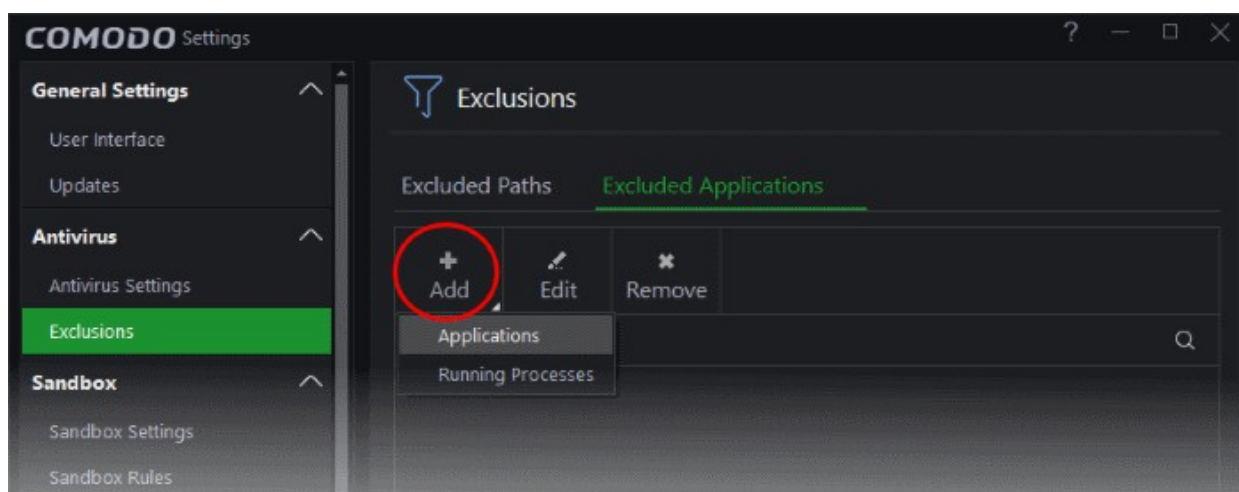


## Manually adding applications to the 'Exclusions' list

You can add applications to be excluded, by selecting the applications installed on your computer or by choosing a currently running process.

### To add an item to Excluded Applications

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



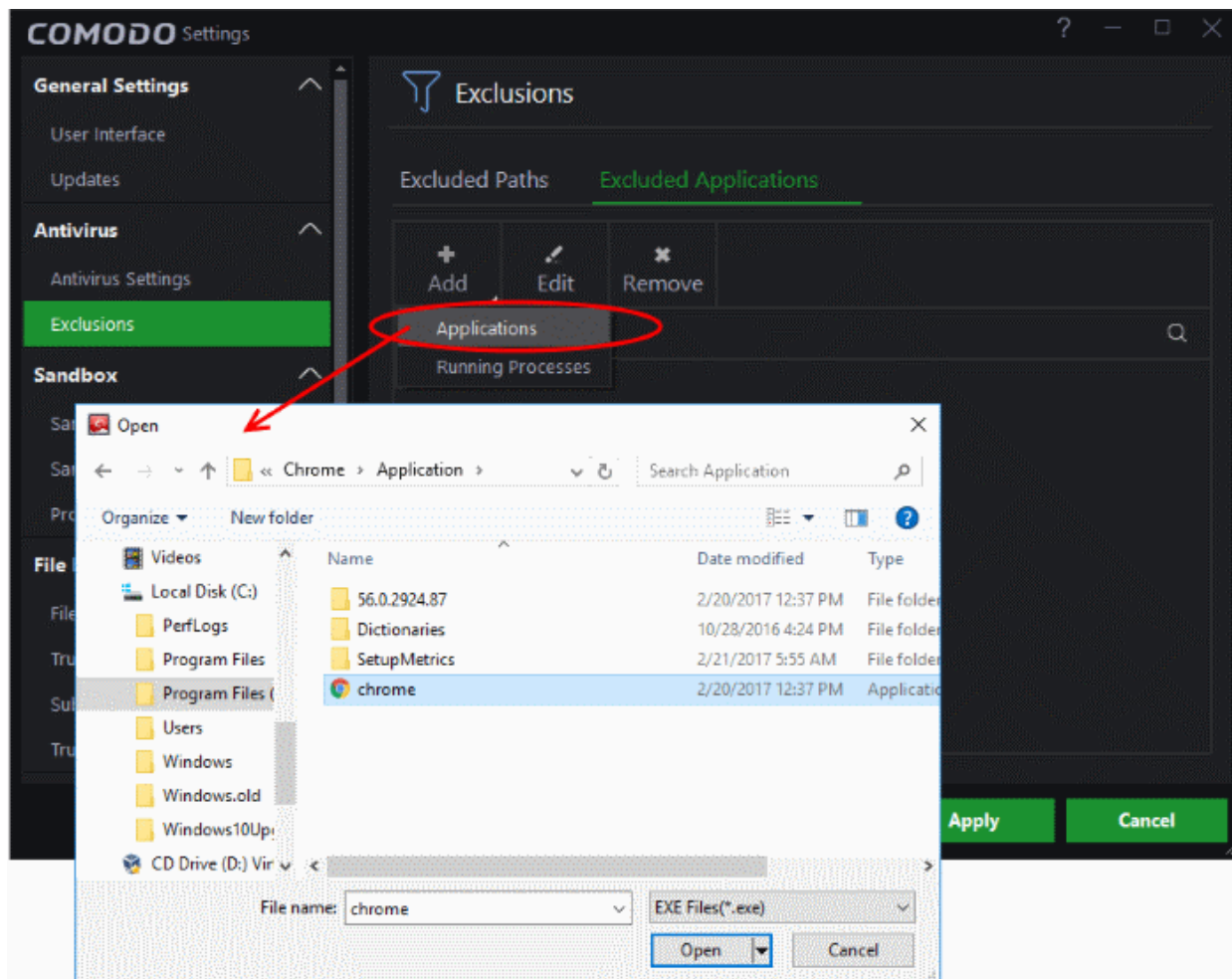
You can choose to add an application by:

- **Browsing your computer for the application** - This option is the easiest for most users and simply allows you to browse the files which you want to exclude from a virus scan.
- **Selecting it from the running processes** - This option allows you to browse to the files which you want to

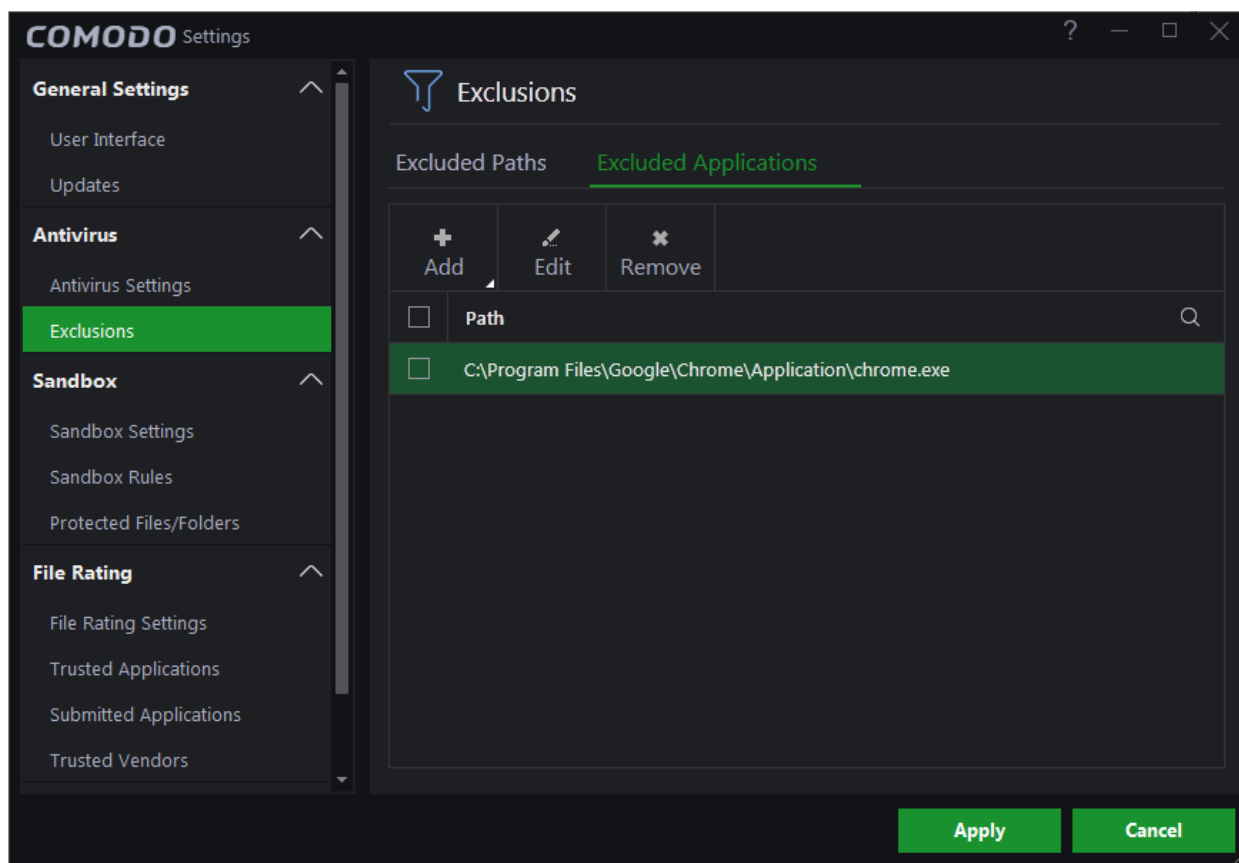
exclude.

## Browsing to the Application

- Choose 'Applications' from the 'Add' drop-down
- Navigate to the file you want to exclude and click 'Open'.



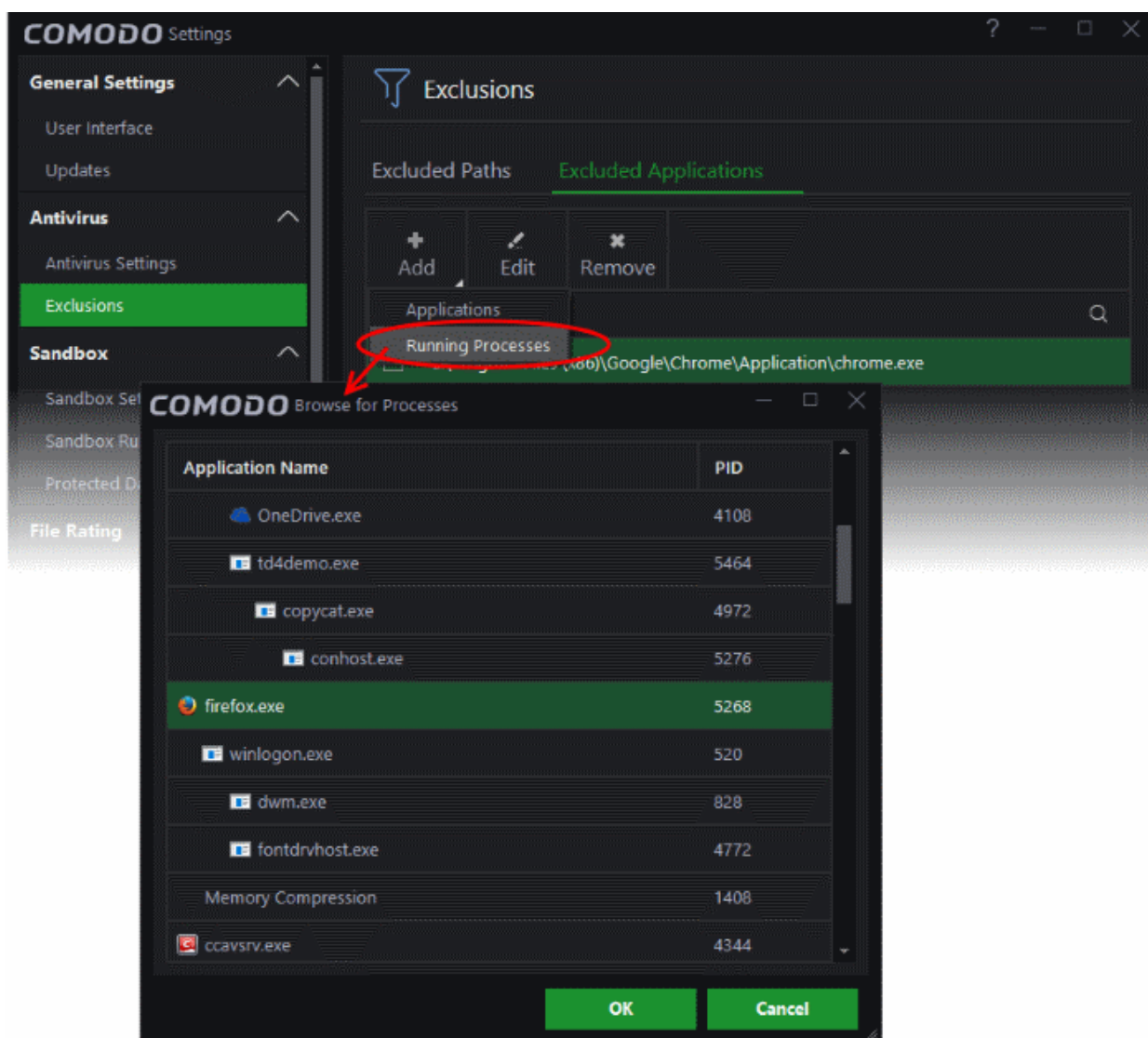
The file will be added to excluded applications.



- Repeat process to add more items.
- Click 'Apply' for saving your settings. Excluded items will be skipped from future real-time scans.

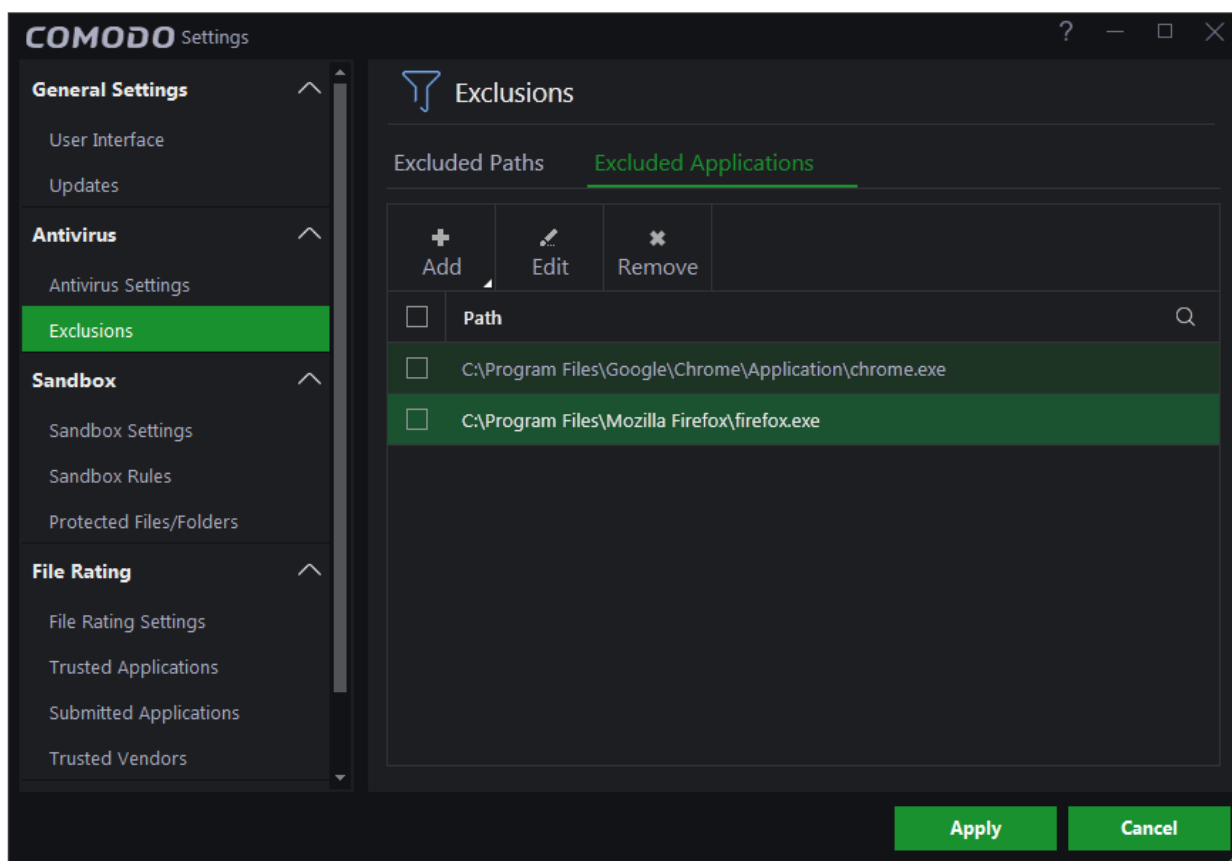
### Adding application from running processes

- Choose 'Running Processes' from the 'Add' drop-down



A list of currently running processes in your computer will be displayed.

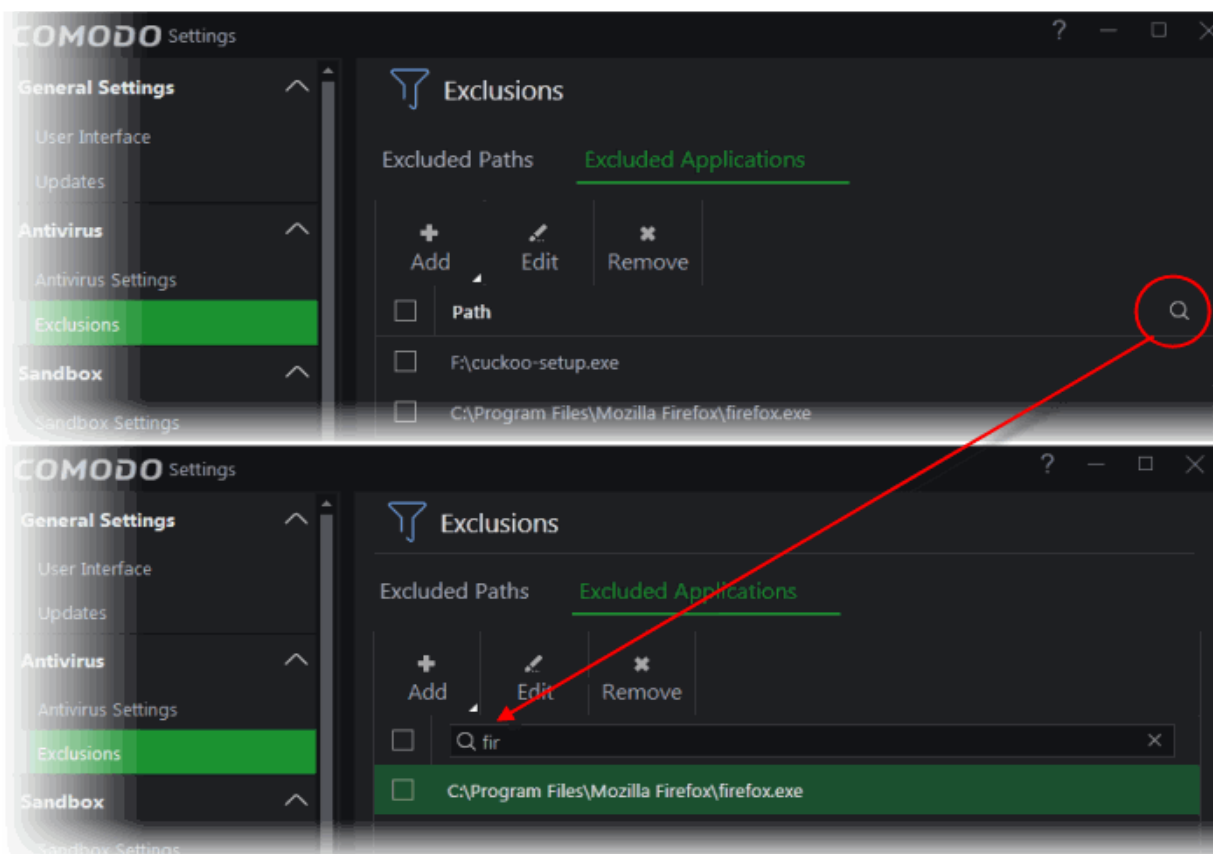
- Select the process whose target application you wish to exclude and click 'OK'.



- Repeat the process to add more items
- Click 'Apply' for saving your settings. The applications will be skipped from future real-time scans

## Search Options

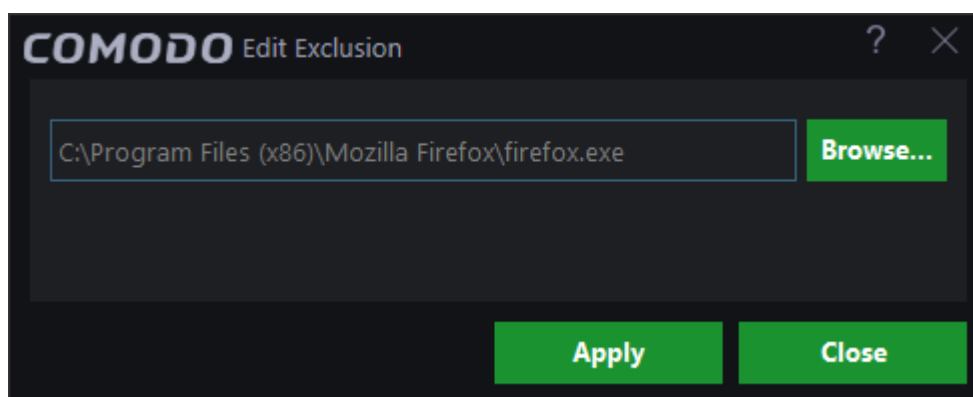
You can use the search option to find a specific excluded application from the list by clicking the search icon at top-right.



- Enter the name of the application in full or part in the search field
- The search results will be displayed
- Click the icon 'X' in the search field to close the search option

### To edit the path of the application added to Excluded Application

- Double-click on the item
- OR
- Checkbox the application and click 'Edit' at the top

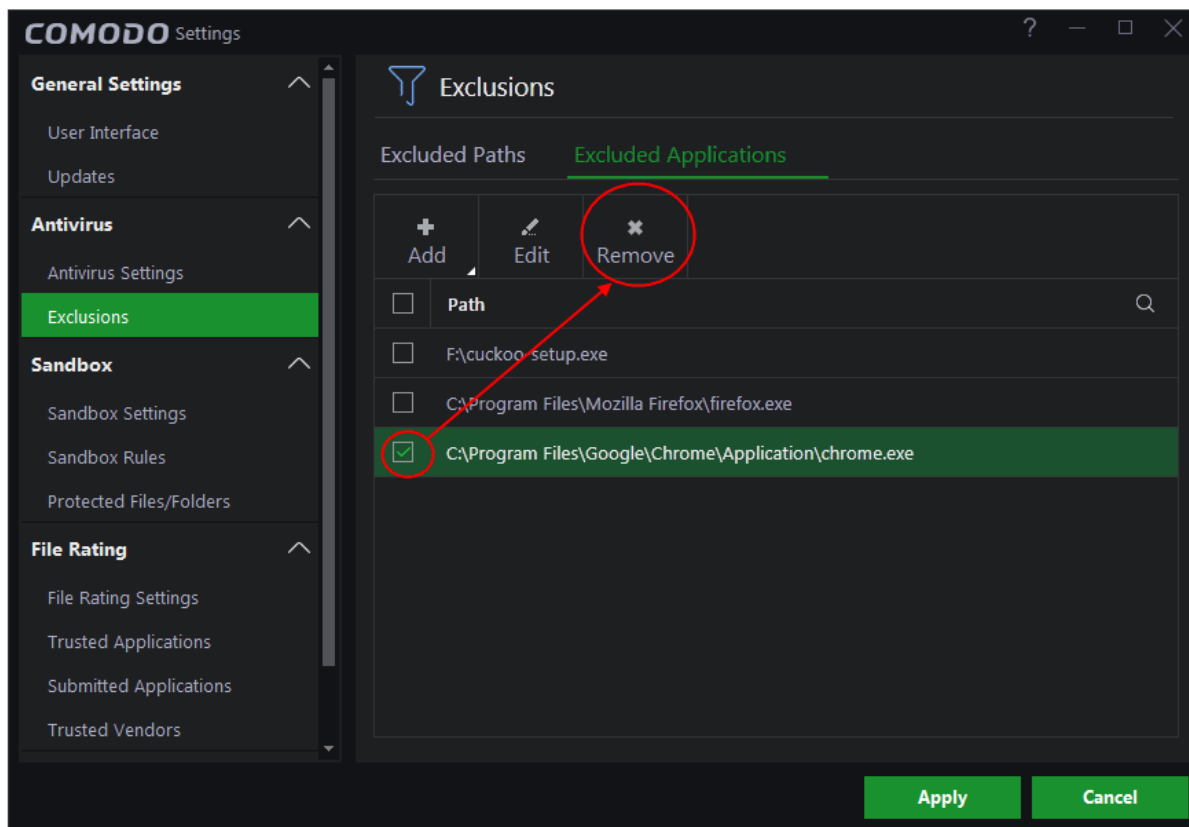


- Next, click the 'Browse...' button, navigate to the file you want to modify and click 'Apply'. Alternatively, type the file path into the field and click 'Apply'.

### To remove item(s) from the Excluded Applications

- Select the item(s) and click 'Remove' from the top.

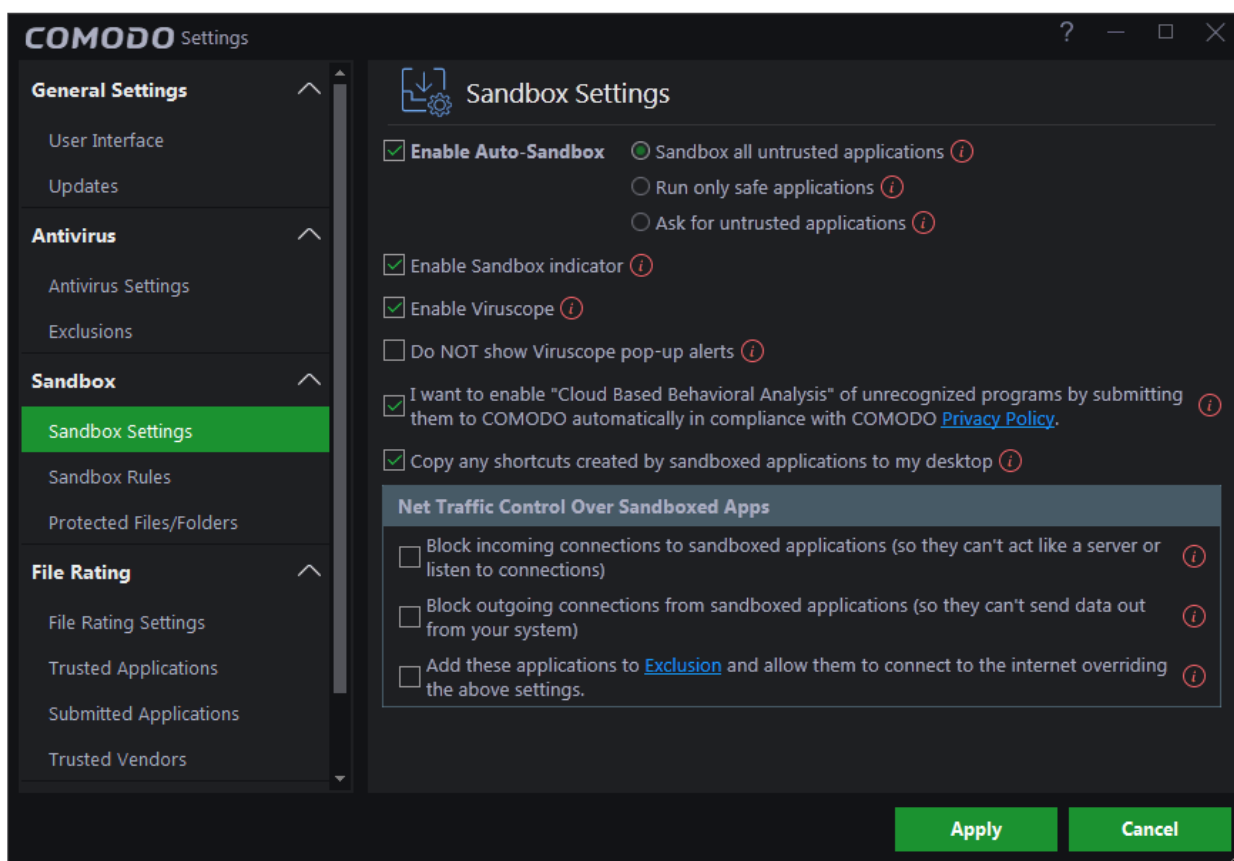




- Click 'Apply' in the 'Settings' dialog for your settings to take effect.

## 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 from causing damage. The sandbox configuration section allows you define how unknown files should be handled and to configure sandbox rules.



Refer to the following sections for more details:

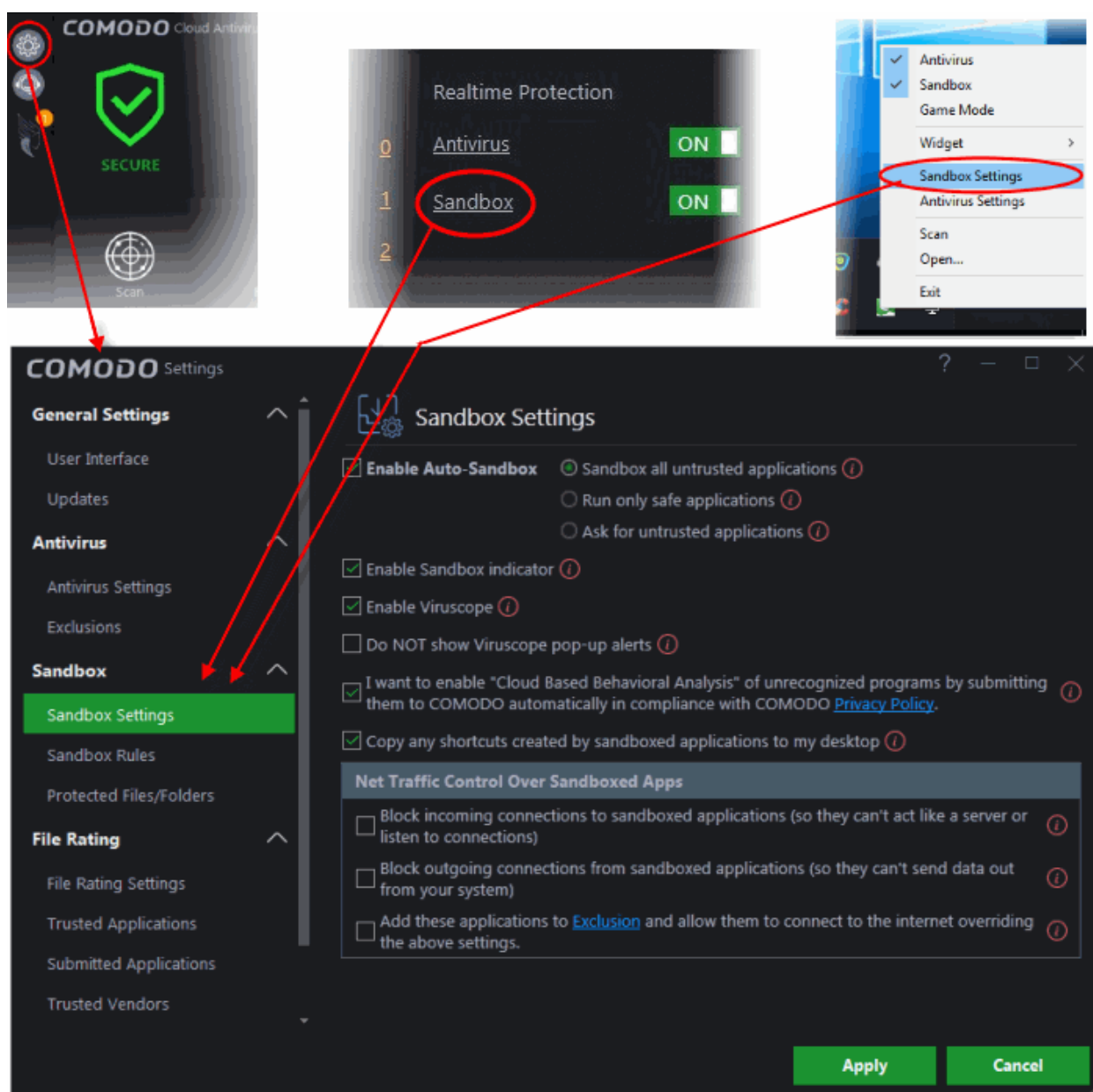
- [Sandbox Settings](#)
- [Sandbox Rules](#)
- [Protected Files/Folders](#)

## 6.3.1. Sandbox Settings

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

### To open sandbox settings

- Click the 'Settings' icon on the left then 'Sandbox' > 'Sandbox Settings'  
OR
- Click the 'Sandbox' link under 'Realtime Protection' on the home screen  
OR
- Right-click on the CCAV system tray icon (or the widget) and choose 'Sandbox Settings' from the options.

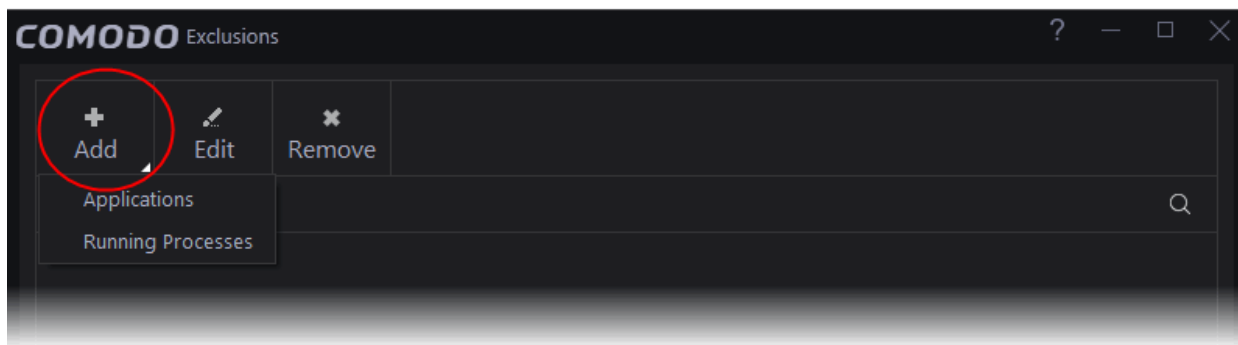


- **Enable Auto-Sandbox** - Switch automatic sandboxing on or off. Default = On.
- If you disable the sandbox then any sandbox rules you have created will be disregarded.
- If you enable the sandbox, you have the following options:
  - **Sandbox all untrusted applications** - CCAV will automatically 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 manually trusted by the user. Trusted files 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.

- Ask for untrusted files - Instead of automatically sandboxing unknown files, CCAV will 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.
- **I want to enable 'Cloud based Behavioral Analysis of unrecognized programs by submitting them to Comodo automatically in compliance with Comodo Privacy Policy'** - Any file that is identified as unknown is sent to the Cloud server for behavior analysis. Each file is executed in a virtual environment on Comodo servers and tested to determine whether it contains any malicious code. The results will be sent back to your computer in around 15 minutes. Comodo recommends users leave this setting enabled. If you disable this setting, an alert to submit unknown files will be displayed. Refer to '[Understanding CCAV Alerts](#)' for more details.
- **Copy any shortcuts created by sandboxed applications to my desktop** - Will place a duplicate of any shortcuts created by sandboxed applications onto the desktop of your local machine. This allows you to open the application faster and also alerts you to the fact that the application created a shortcut. Clicking the local shortcut will run the application in the sandbox.
- Net Traffic Control Over Sandbox Apps
  - **Block incoming connections to sandboxed applications (so they can't act like a server or listen for connections)** - Will prevent sandboxed applications from accepting TCP internet connections from external sources. This stops potentially malicious applications from receiving instructions from their control server.
  - **Block outgoing connections from sandboxed applications (so they can't send data out of your system)** - Will prevent sandboxed applications from making TCP internet connections to external sources. This stops potentially malicious applications from broadcasting your confidential data without your knowledge.
  - **Add these applications to [Exclusion](#) and allow them to connect to the internet by overriding the above settings** - Specify applications that will be allowed incoming or outgoing connections to the internet, even if sandboxed.

#### To define exclusions for items

- Click the 'Exclusion' link. The 'Exclusions' dialog will contain 'Applications' and 'Running Processes' options available at top-right:



- **Applications** - Specify applications that will be added to the exclusion
- **Running Processes** - Allows you to select an application from the list of currently running processes, so that the parent application of the chosen process will be added to the exclusion.
- To edit an exception, select it from the list, click the 'Edit' at the top or double-click on it
- Change an application location path and click 'Apply' to implement your settings

**Note:** Sandboxed applications will not have access to the clipboard. This is to prevent apps from transferring potentially malicious content outside the sandbox.

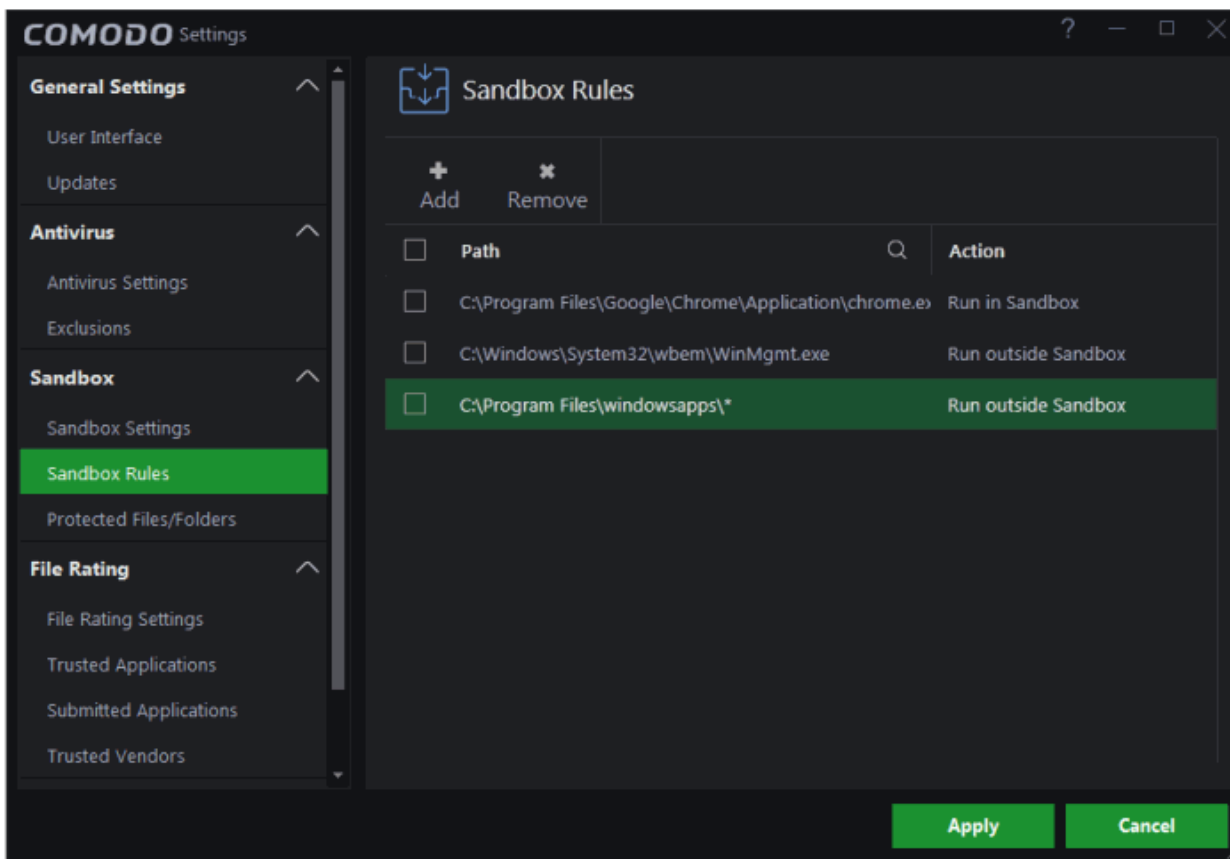
- Click 'Apply' for your settings to take effect.

## 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 'Sandbox Rules' interface

- Click the 'Settings' icon on the left of the home screen
- Click 'Sandbox' > 'Sandbox Rules'



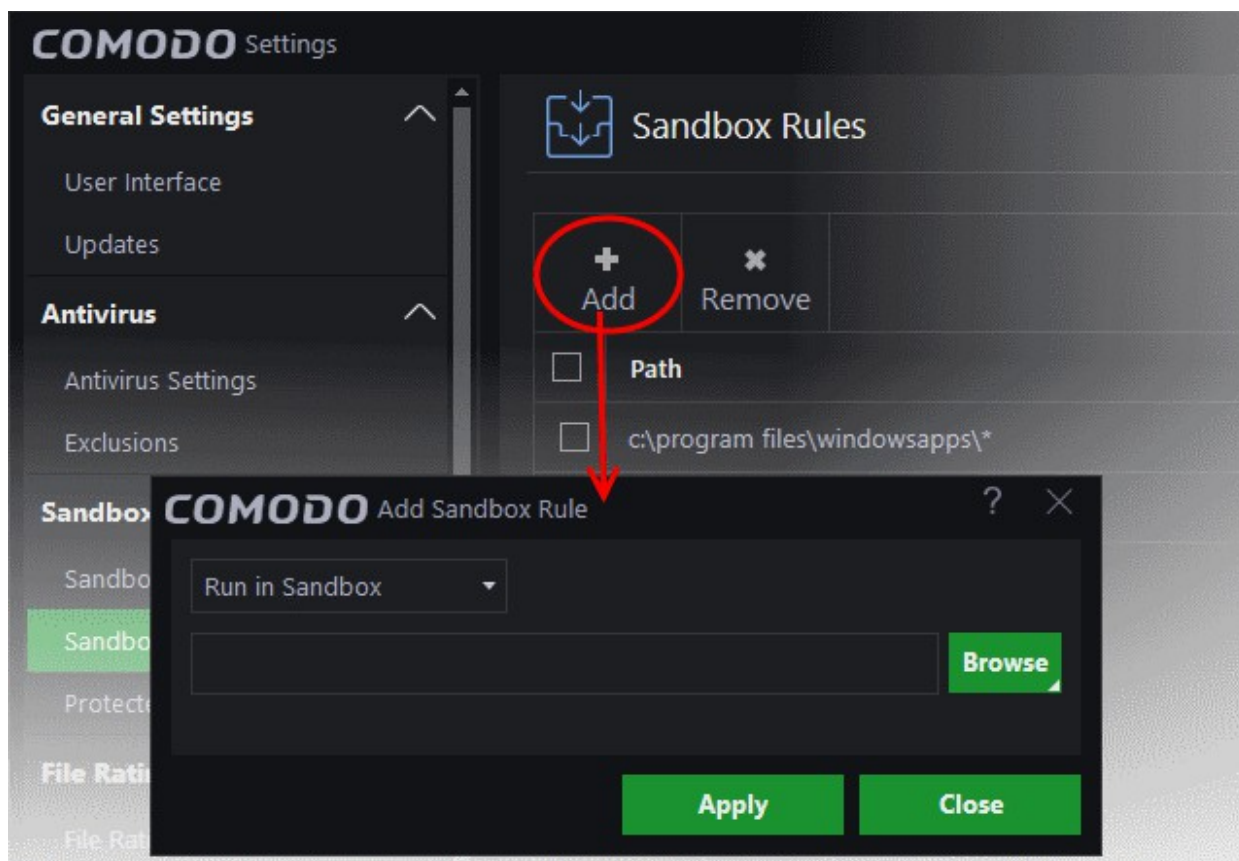
The interface displays a list of existing rules along with the application path and the sandbox action associated with it.

## Adding a new rule

You can add new sandbox rules by specifying an application and the sandbox actions that should be applied to it.

### To add a sandbox rule

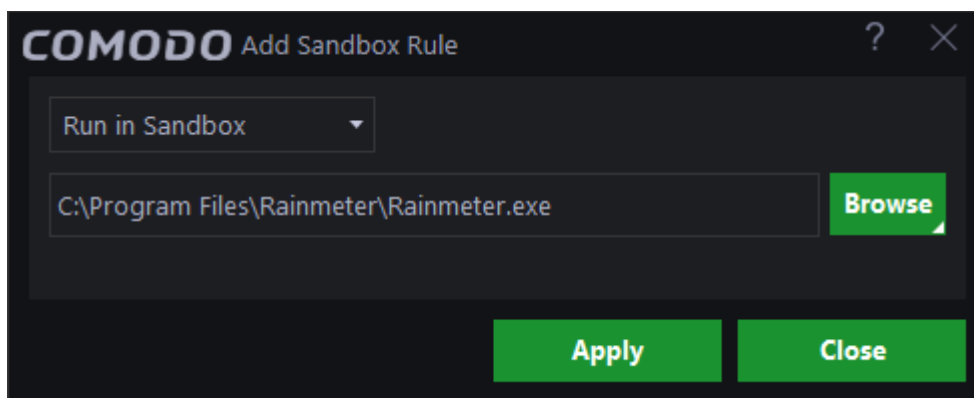
- Click 'Add' at the top of the 'Sandbox Rules' interface to open the 'Add Sandbox Rule' dialog.



- Choose the action to be applied from the drop-down at the top. The available 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 an untrusted 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, specify the application or folder to which the rule should apply. You have the following options:
  - **Enter the path of the application \ folder directly** - Type or paste the full path of the in the field provided.
  - **Browse your computer for the application \ folder** - Click the 'Browse' button and select 'Application' or 'Folder'
  - **Select an application from running processes** - Click the 'Browse' button and choose 'Running Processes' to select an application from processes which are currently running on your PC.
- After choosing your application/folder, click 'Apply' in the 'Settings' dialog for your rules to take effect.
- Repeat the process to add more rules.
- Click 'Apply' from the 'Settings' dialog for your rules to take effect.

## Editing a rule

- To edit a rule, double click on it.



The edit dialog is similar to the 'Add Sandbox Rule' dialog. Refer to the explanation [above](#) for more details.

- To remove a rule, select the check-box next to the rule name and click 'Remove'.

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

**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 2<sup>nd</sup> priority (the check-boxes next to 'Enable Auto-Sandbox');

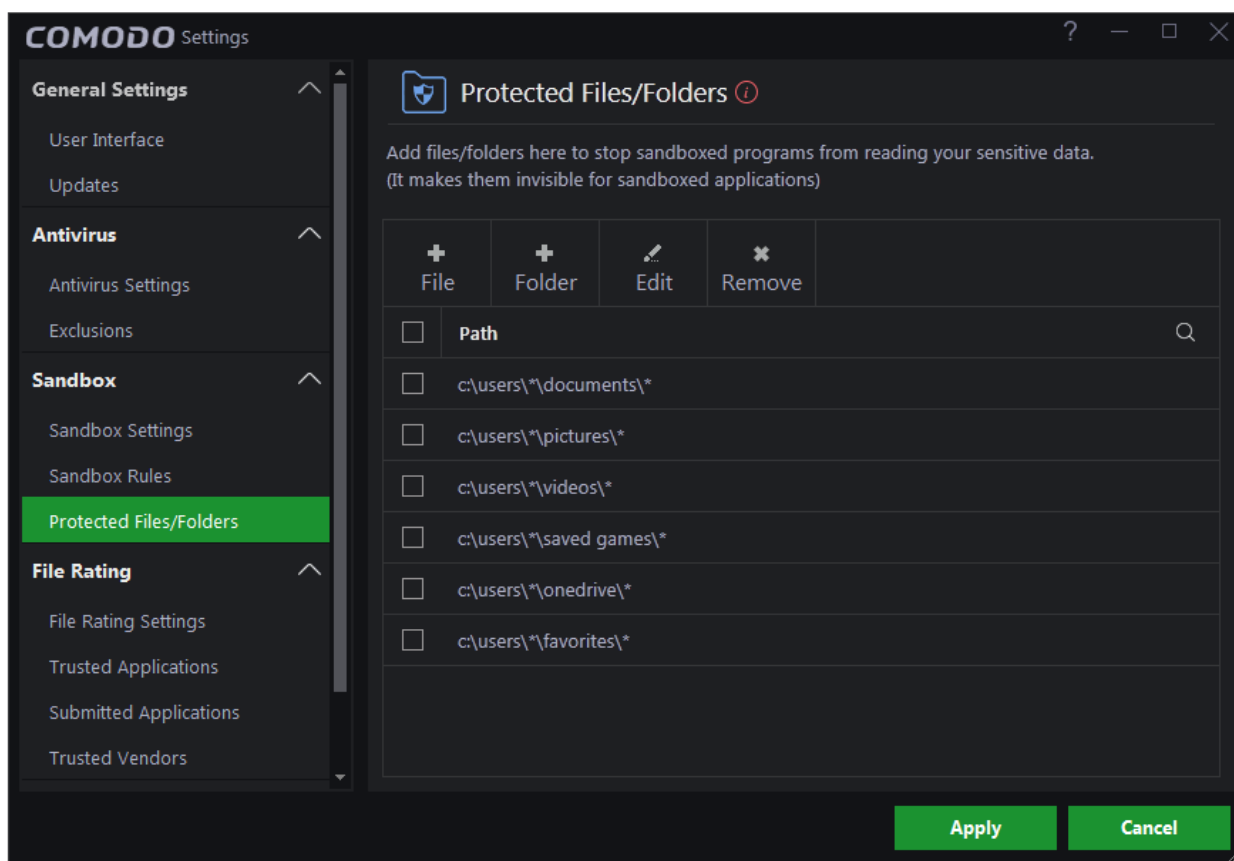
### 6.3.3. Protected Files/Folders

Protected files and folders cannot be seen, accessed or modified by any application running inside the sandbox. The protected file/folders area lets you define the paths of the items you wish to protect.

**To open the "Protected Data Files/Folders" area**

- Click the 'Settings' icon on the left of the home screen
- Select 'Sandbox' > 'Protected Files/Folders'

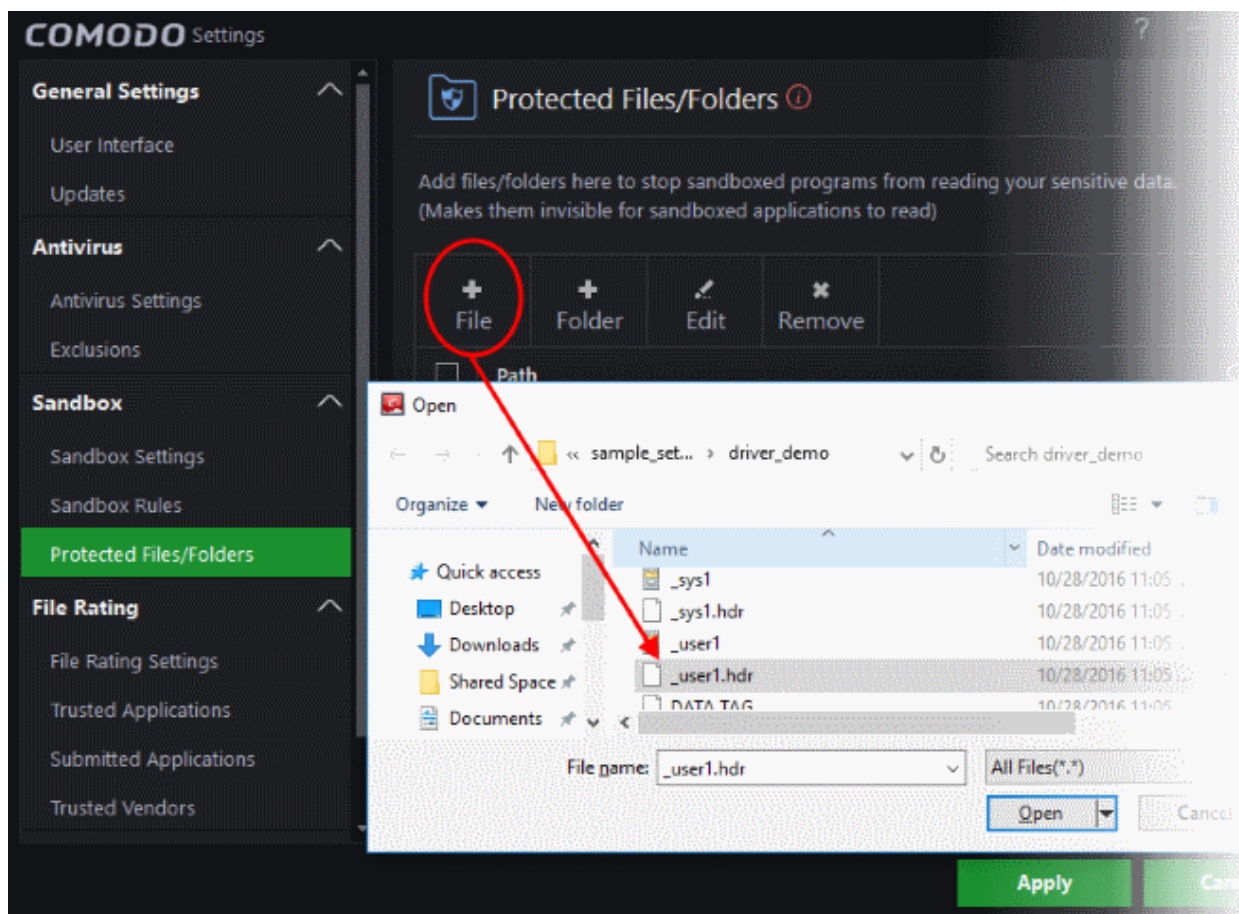




The interface displays a list of protected files or folders and their paths.

### To add a new file/folder

- Click the 'File' or 'Folder' at the top of the 'Protected Files/Folders' interface
- Browse to the file or folder you wish to protect
- Click 'OK'/'Open':

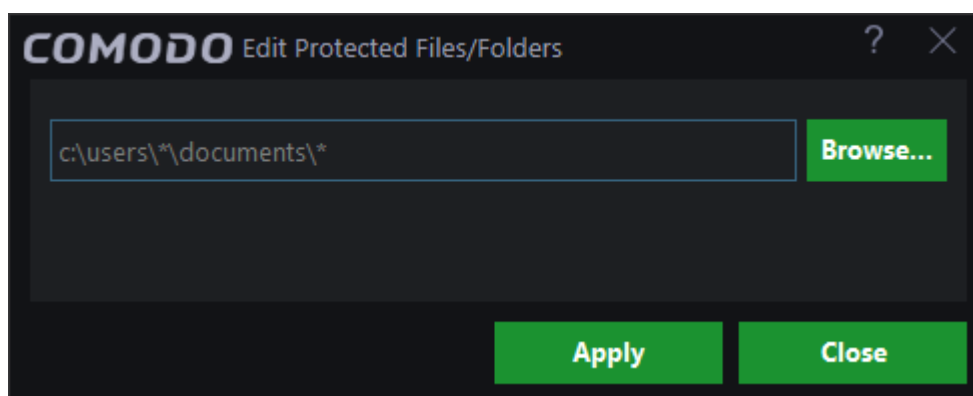


The file/folder will be added to the 'Protected File/Folder' list.

- Repeat the process to add more files or folders
- Click 'Apply' from the 'Settings' dialog for your settings to take effect

## To edit a folder

- Select the folder you wish to edit
- Click the 'Edit' button (or simply double click on it).
- The 'Edit Protected File/Folder' dialog will appear:



- Click 'Browse' to change the file or folder path

- Click 'Apply' to save your changes
- Click 'Apply' in the 'Settings' dialog for your rules to take effect.

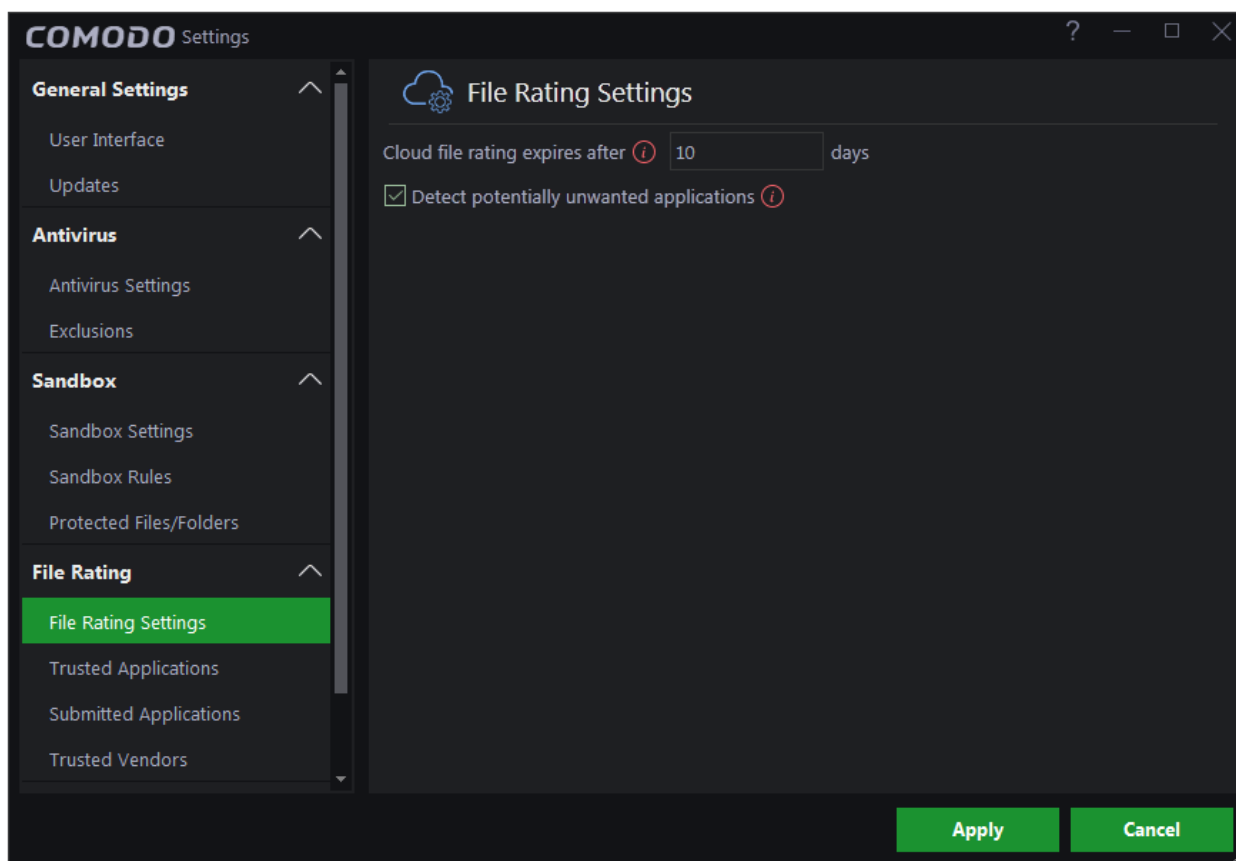
## 6.4. File Rating Settings

The file rating system is a cloud-based file look-up service (FLS) that ascertains 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.



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

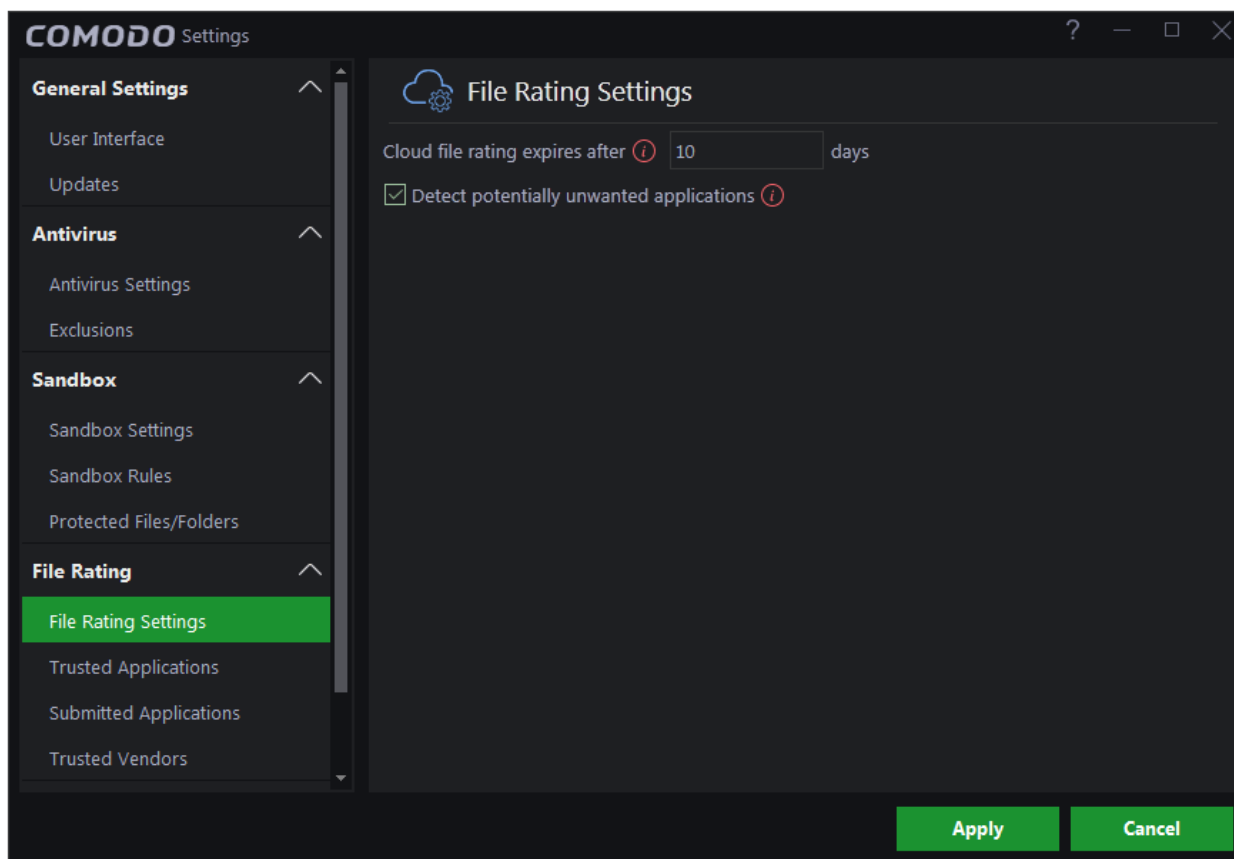
- [File Rating Settings](#) - Configure settings that govern the overall behavior of file rating.
- [Trusted Applications](#) - Add and manage applications to local 'Trusted Applications' list.
- [Submitted Files](#) - View any files already submitted to Comodo for analysis.
- [Trusted Vendors](#) -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

## 6.4.1. File Rating Settings

The 'File Ratings Settings' area lets you configure the length of time that file ratings from the cloud server are considered valid.

To open the 'File Rating Settings' interface

- Click the 'Settings' icon at the top left of the CCAV home screen
- Click 'File Rating' > 'File Rating Settings' on the left



- **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.
- **Detect potentially unwanted applications** - When this check box is selected, CCAV also scans for applications that (i) a user may or may not be aware is installed on their computer and (ii) may functionality and objectives that are not clear to the user. Example PUA's include adware and browser toolbars. PUA's are often installed as an additional extra when the user is installing an unrelated piece of software. Unlike malware, many PUA's are 'legitimate' pieces of software with their own EULA agreements. However, the 'true' functionality of the software might not have been made clear to the end-user at the time of installation. For example, a browser toolbar may also contain code that tracks a user's activity on the Internet. (**Default = Enabled**)
- Click 'Apply' for your settings to take effect.

## 6.4.2. Trusted Applications

Files with a 'Trusted' rating are automatically allowed to run outside the sandbox. Files are given 'trusted' status if:

- 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.
- The application has been added to the 'Trusted Applications' list.

For files assigned '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. When you open a file, a new digest is instantly created for it and compared with the database of hashes belonging to trusted files. So, even if the file name is changed later, it will retain its 'Trusted' status as the hash remains same.

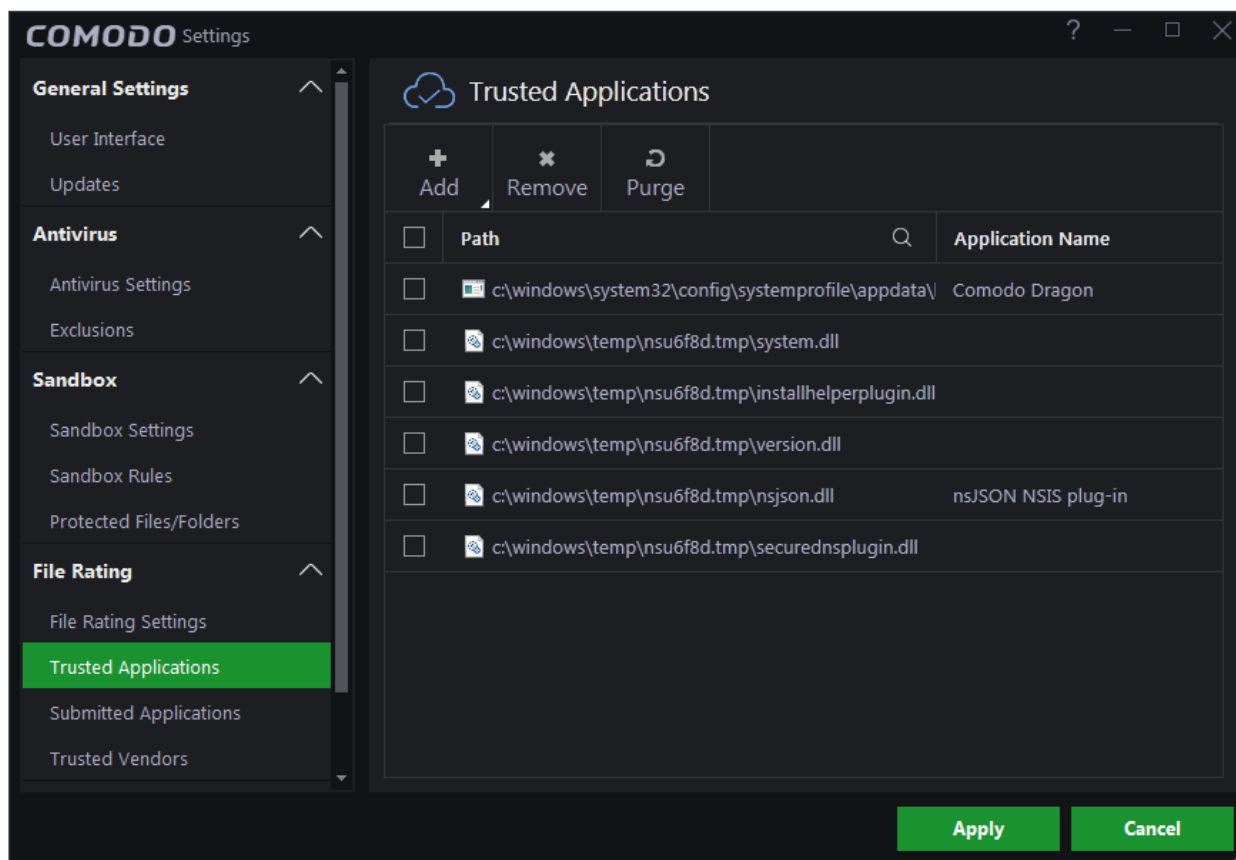
By granting 'Trusted' status to executables you can reduce the amount of alerts that the sandbox generates while maintaining a high level of security. This is particularly useful for developers that are creating new applications that are unknown to the Comodo safe list.

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 the 'Settings' icon at the top left of the CCAV home screen
- Choose 'Trusted Applications' under 'File Rating' on the left



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

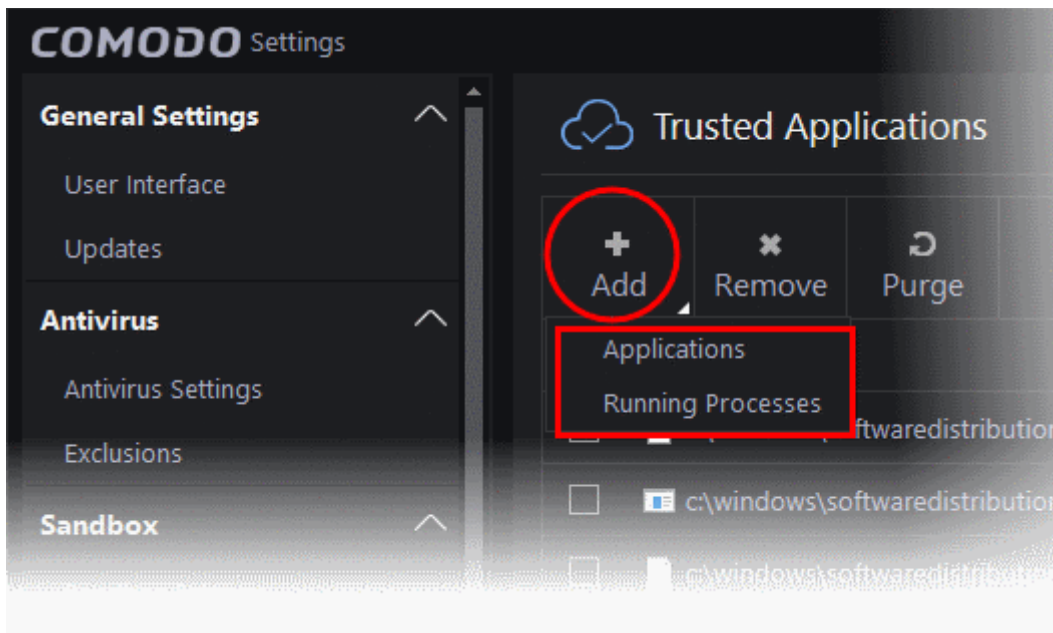
- **Path** - The installation path of the application/executable file

- **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

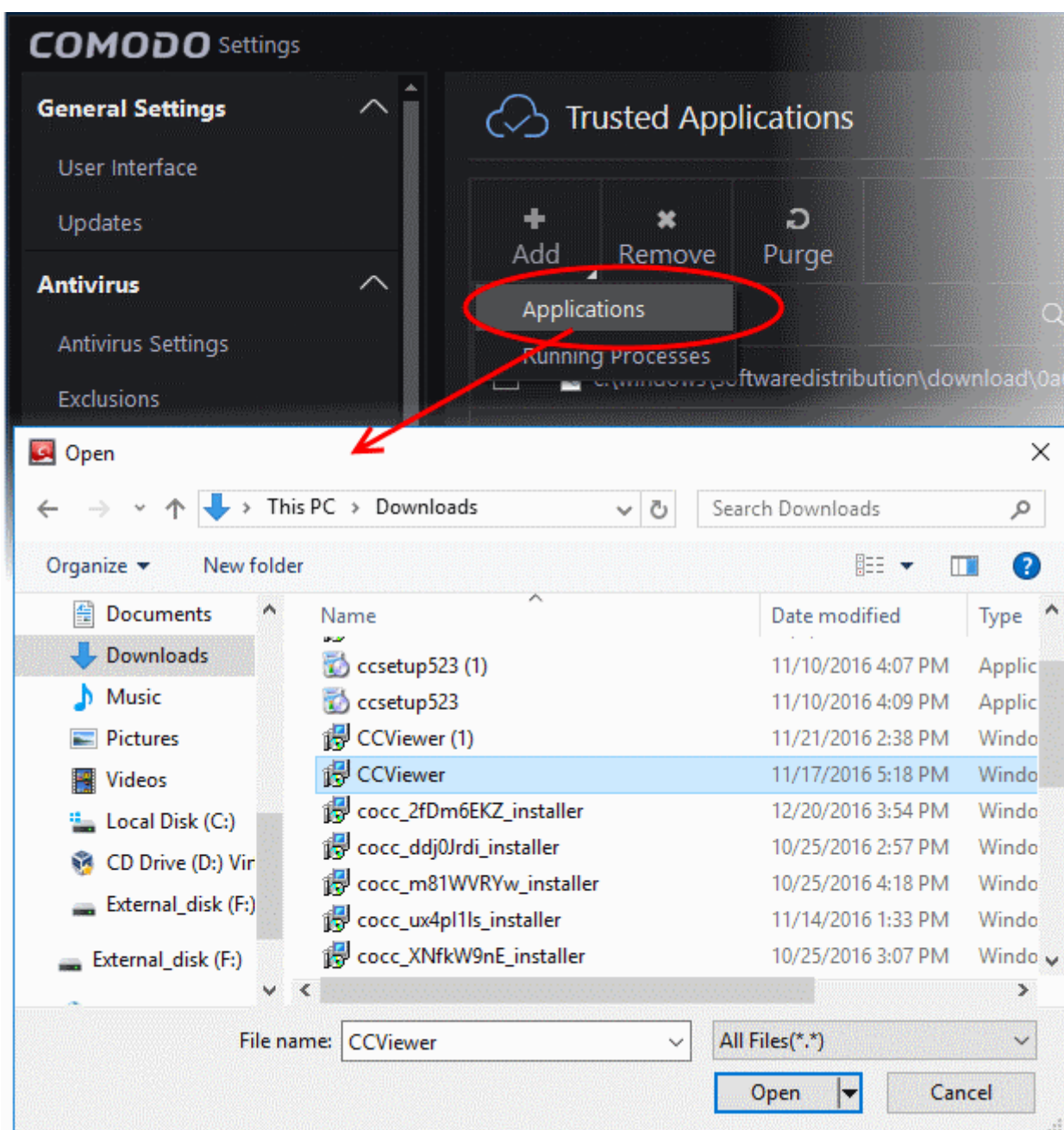


You can add an application by :

- **Browsing your computer** - Enables you to select files on your hard drive(s) that you want to add to your list of trusted applications.
- **Selecting from running processes** - Enables you to choose files from processes which are currently running on your system.

### To add an application from your computer

- Choose 'Applications' from 'Add' drop-down
- Navigate to the file you want to add to 'Trusted Applications' in the 'Open' dialog and click 'Open'.

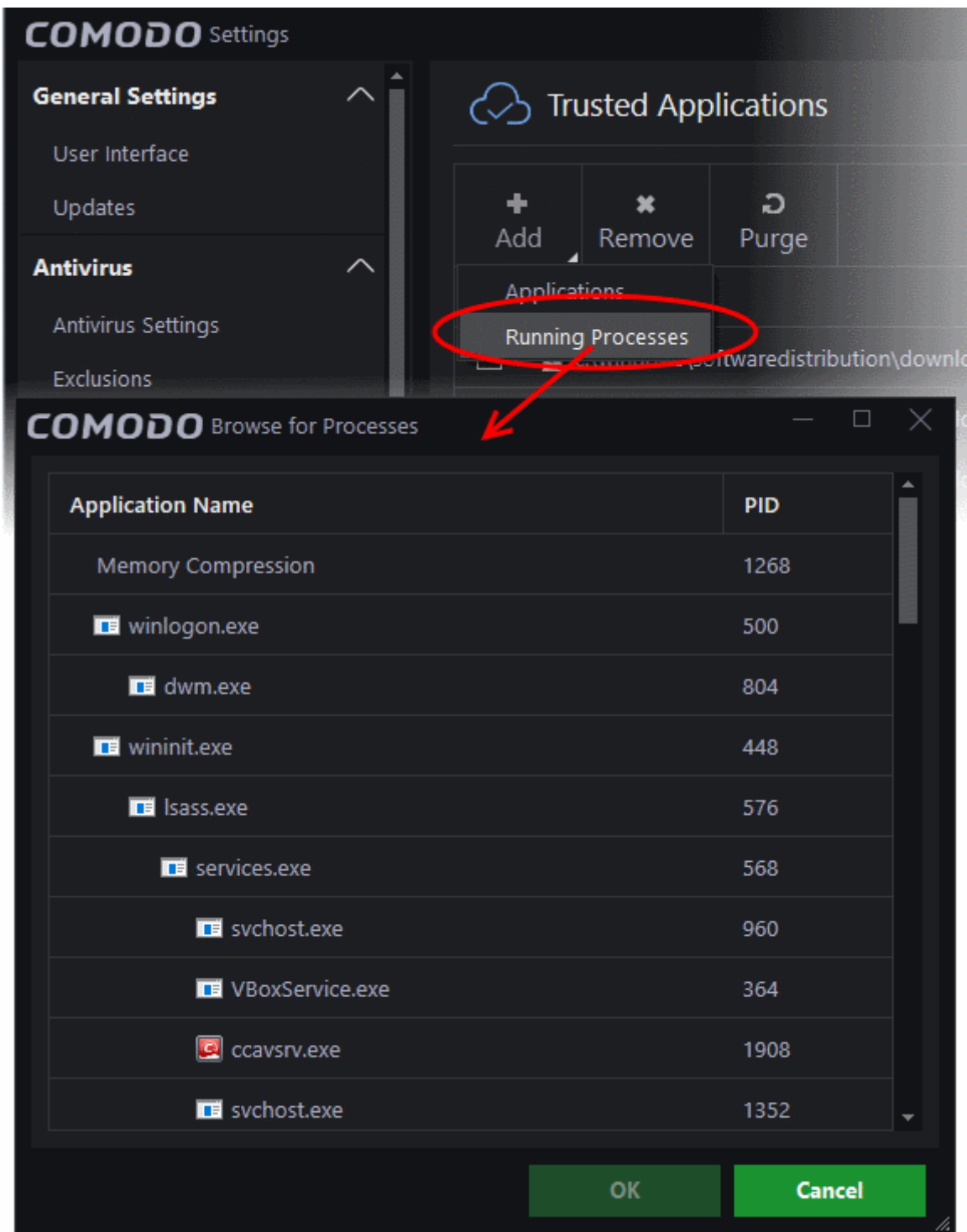


This file will now be added to the trusted applications list.

- Repeat the process to add more items.
- Click 'Apply' to save your settings.

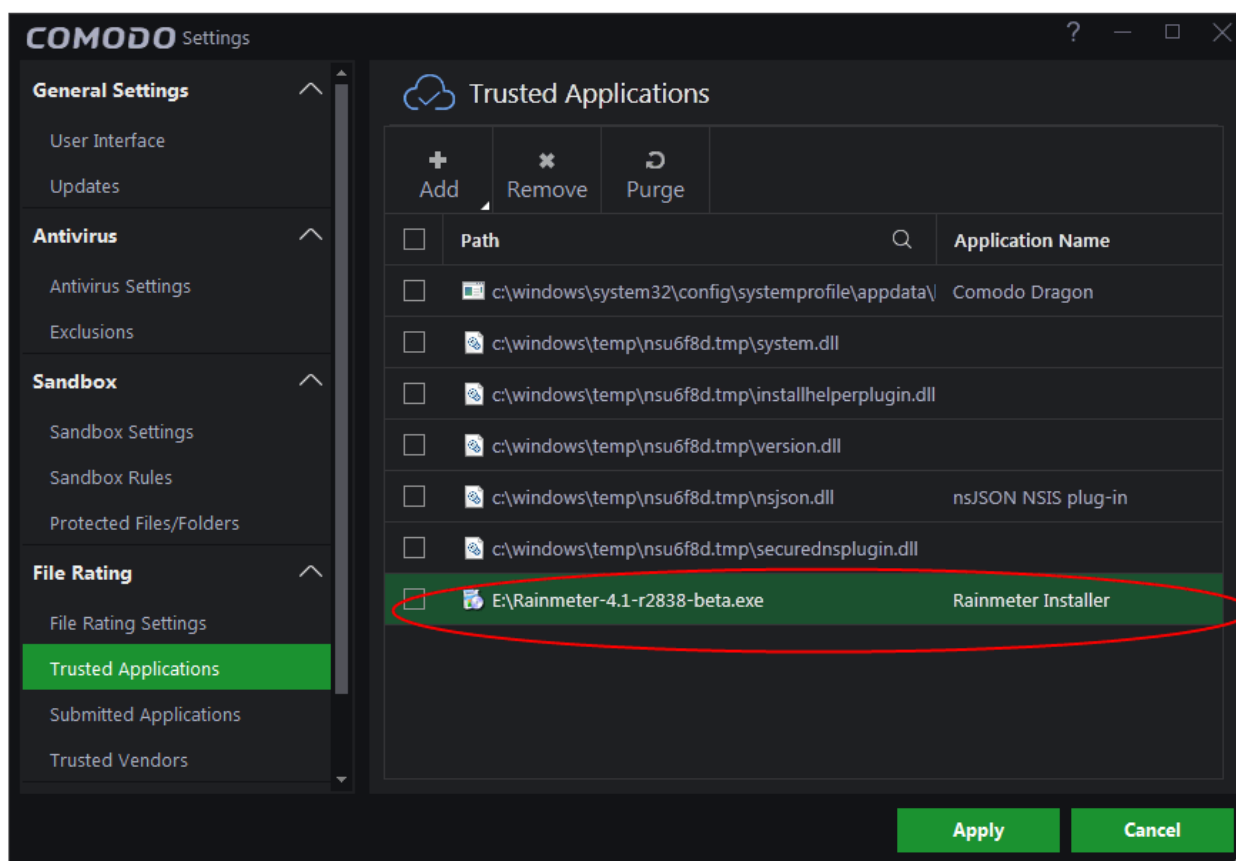
#### To add applications from Running processes

- Choose 'Running Processes' from the 'Add' drop-down.



- Select the application from the running process you wish to add to trusted applications and click 'OK'. The selected applications will be added to the 'Trusted Applications' list.





- Repeat the process to add more items.
- Click 'Apply' to save your settings.

#### To remove item(s) from the Trusted Applications list

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

#### To Purge item(s) from the Trusted Applications list

- Click 'Purge'

CCAV will verify that all files in the list are actually installed on your computer at the paths specified. If not, the file will be removed ('purged') from the list.

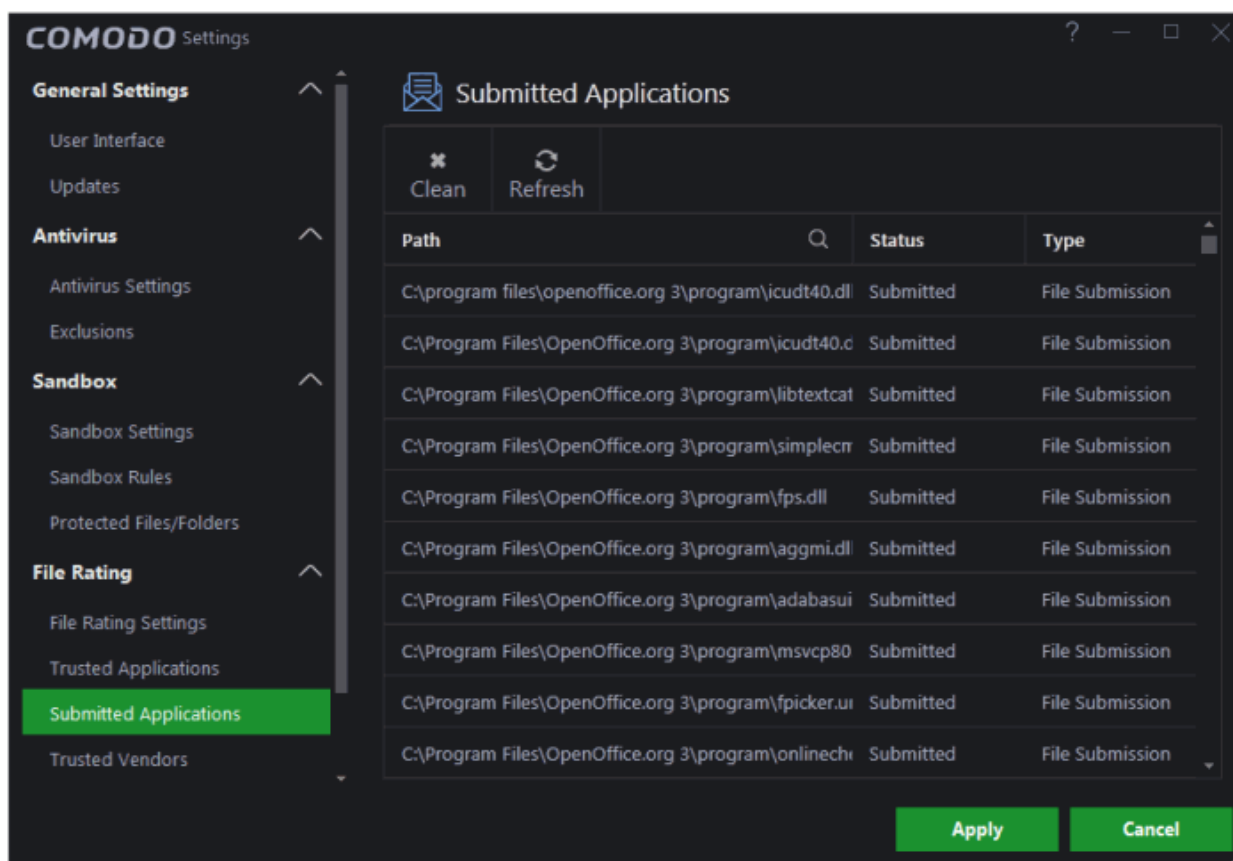
### 6.4.3. Submitted Applications

Files identified as 'unknown' or 'malicious' are uploaded to Comodo for Analysis. You can submit files that 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 Applications' area allows you to view files you have submitted for analysis to Comodo.

#### To open the 'Submitted Applications' interface

- Click the 'Settings' at the top left of the CCAV home screen to open the 'Settings' interface
- Click 'Submitted Applications' under 'File Rating' on the left



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

- **Path** - Indicates the location of the file on your computer
- **Status** - The precise status of the file submitted
- **Type** - Indicates the type of submit. This can include false positives and file submissions to Valkyrie. To see the latest file verdict, scan the file again.

There are two available statuses on completion:

- **In progress:** The file is in queue, yet to be submitted
- **Submitted:** File has been submitted successfully

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

## 6.4.4. Trusted Vendors

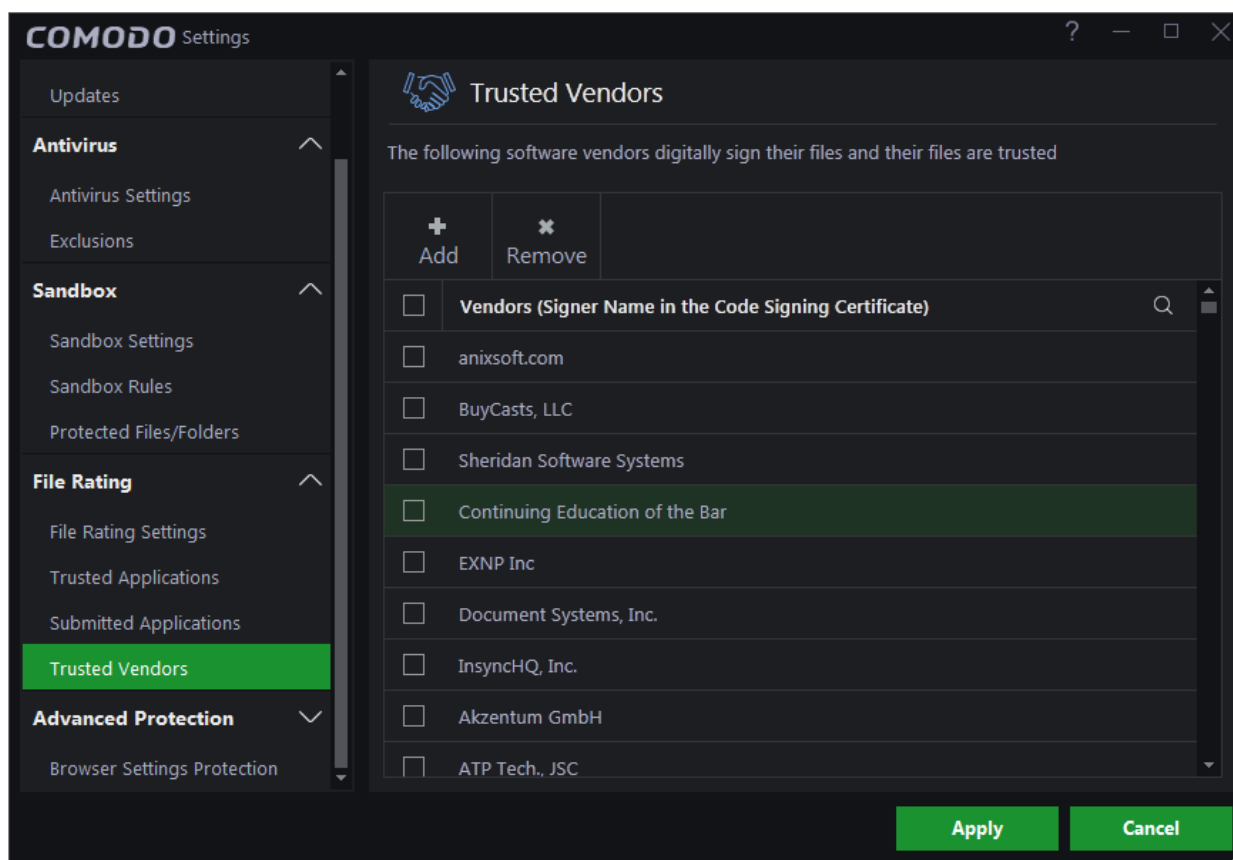
There are three basic methods in which an application can be treated as safe. Either it has to be part of the Comodo 'Safe List' (of known-safe software), or the application is signed by one of the vendors in the 'Trusted Software Vendor List', or the file is added to 'Trusted Applications' list by the 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 the 'Settings' at the top left of the CCAV home screen to open the 'Settings' interface
- Choose 'Trusted Vendors' under 'File Rating' on the left



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:

- Content Source:** The software they are downloading and are about to install *really comes from the publisher that signed it.*
- Content Integrity:** That the software they are downloading and are about to install *has not be modified or corrupted since it was signed.*

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

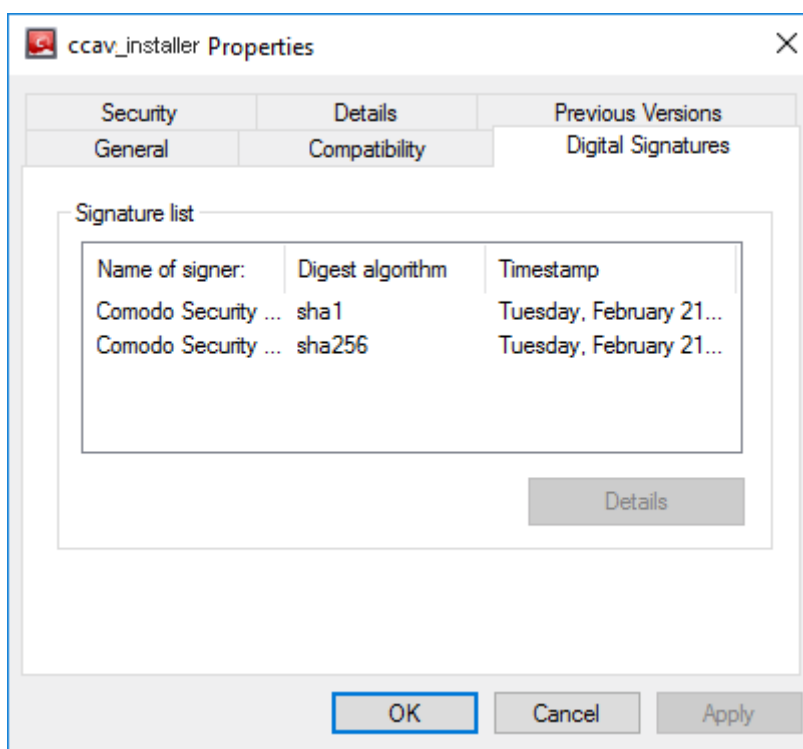
'Symantec' are two examples of a Trusted CA's and are authorized to counter-sign 3rd party software. This counter-signature is critical to the trust process and a Trusted CA only counter-signs a vendor's certificate after it has conducted detailed checks that the vendor is a legitimate company.

If a file is signed by a 'Trusted Software Vendor' then it will be automatically trusted by Comodo Cloud Antivirus (if you would like to read more about code signing certificates, see <http://www.instantssl.com/code-signing/>).

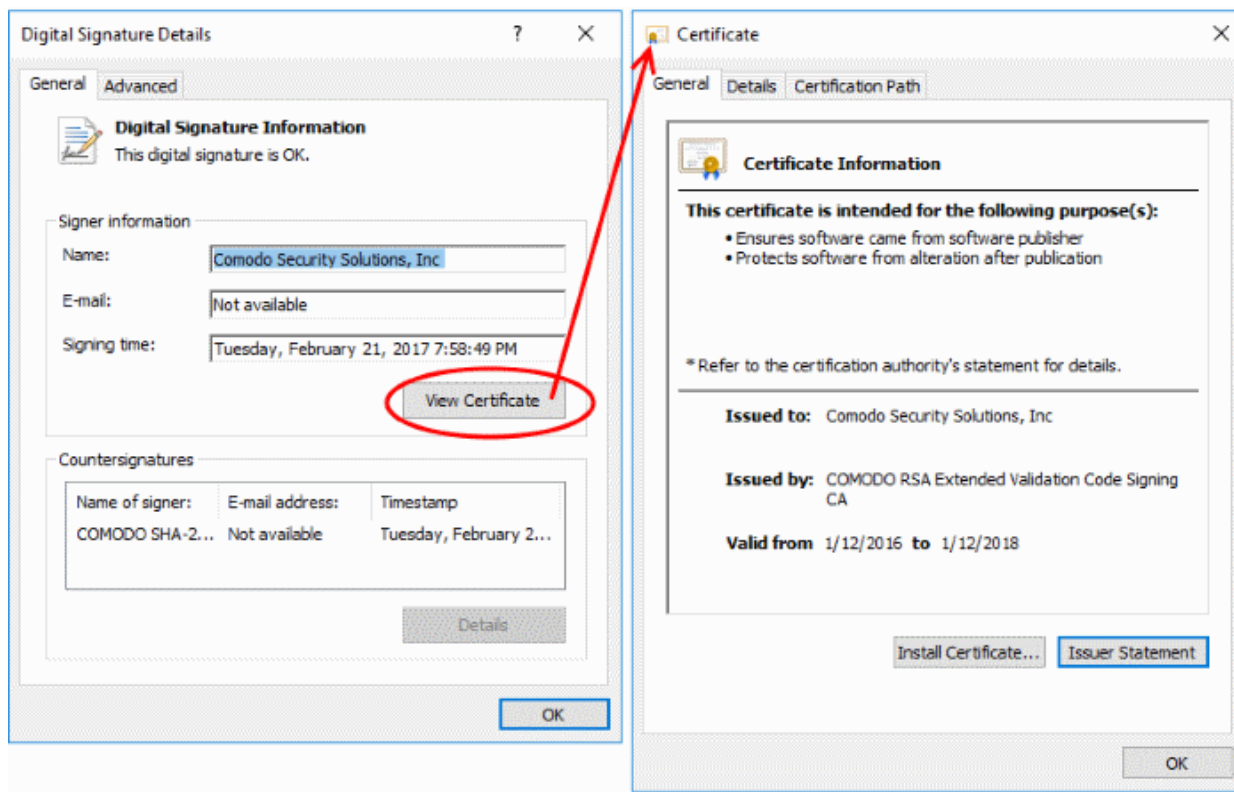
One way of telling whether an executable file has been digitally signed is checking the properties of the .exe file in question. For example, the main program executable for Comodo Cloud Antivirus is called 'ccav.exe' and has been digitally signed.

- Browse to the (default) installation directory of CCAV.
- Right-click on the file 'ccav\_installer.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:



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



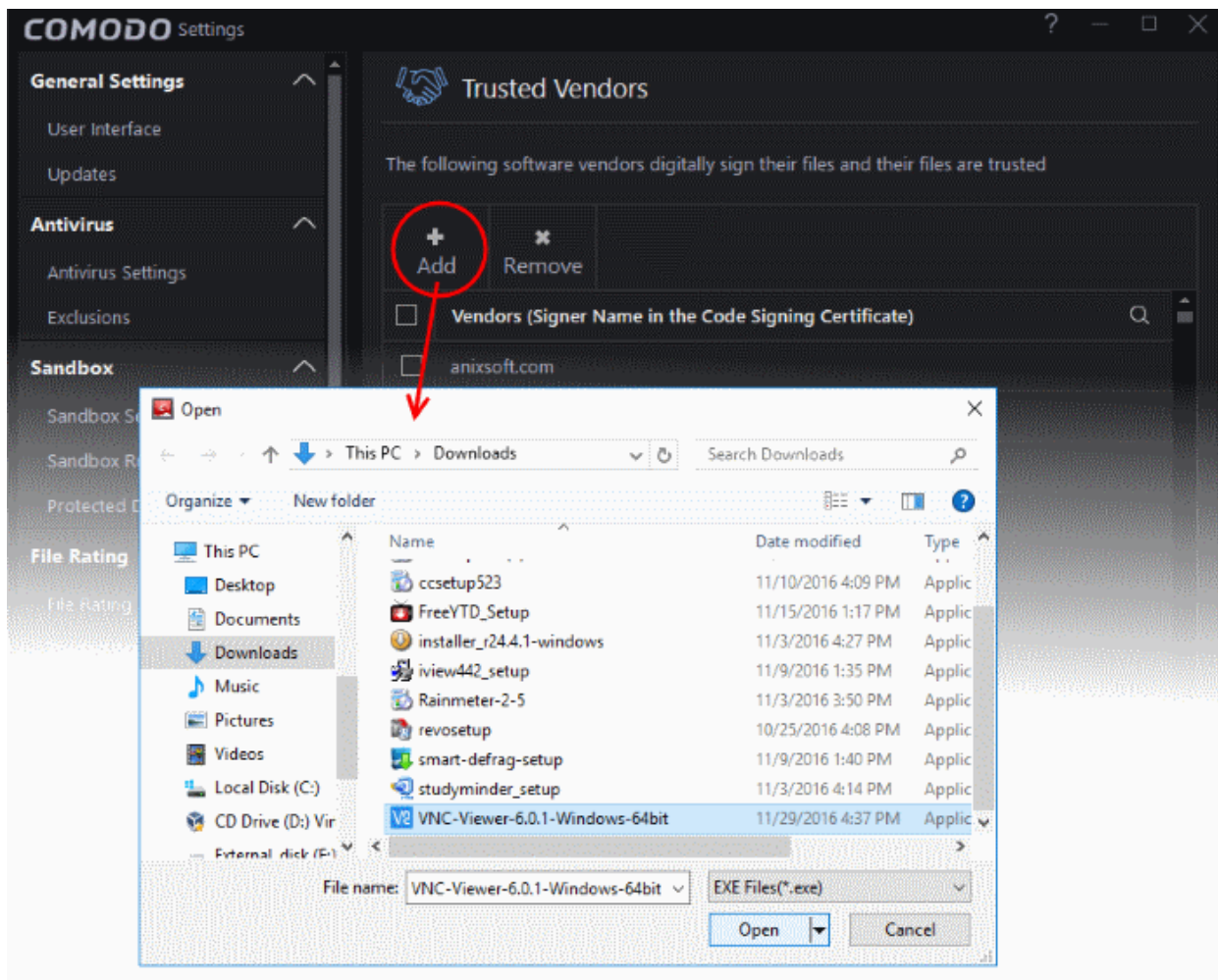
It should be noted that the example above is a special case in that Comodo, as creator of 'ccav\_installer.exe', is both the signer of the software and, as a trusted CA, it is also the counter-signer (see the 'Countersignatures' box). In the vast majority of cases, the signer or the certificate (the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

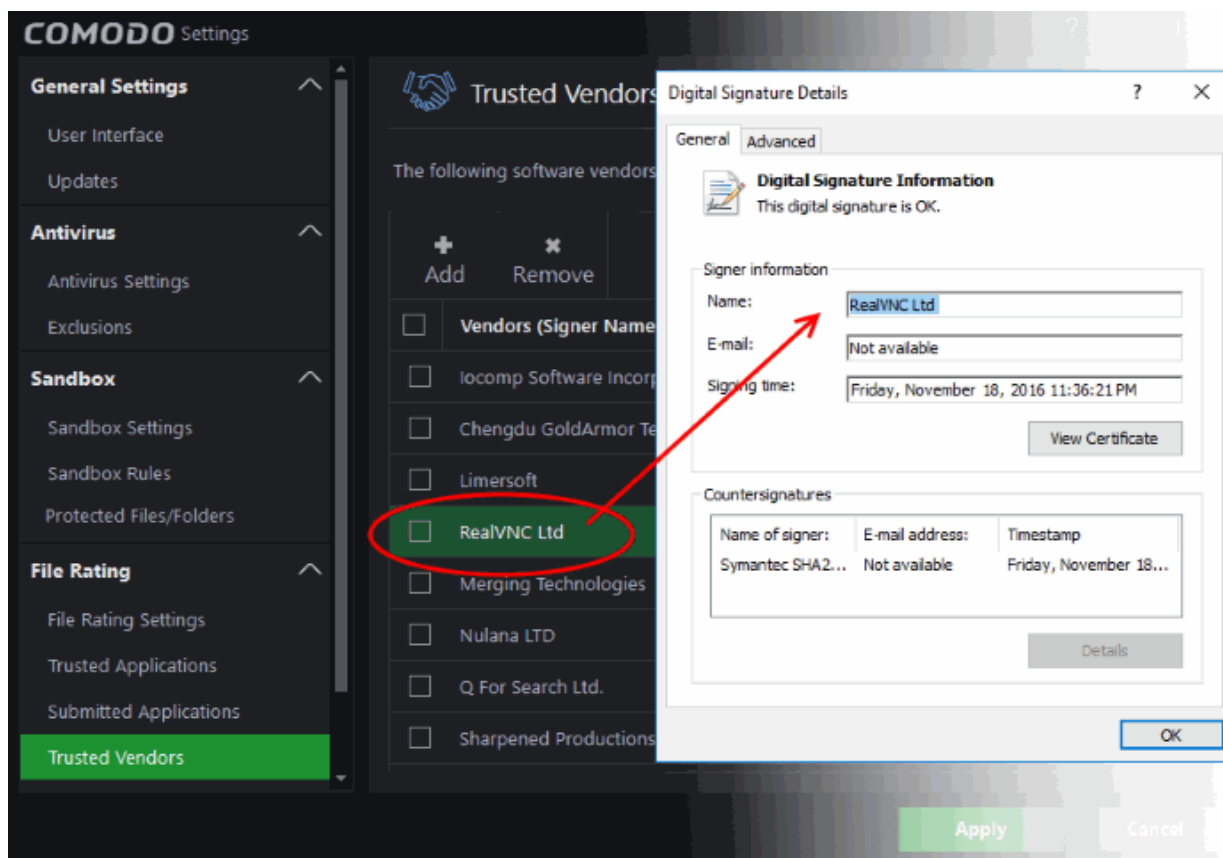
### To add a trusted vendor

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



- Navigate to the location of the executable your local drive. In the example above, we are adding the executable 'VNC-Viewer-6.2.0-Windows-64bit.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 Vendors list (TVL):



In the example above, CCAV was able to verify and trust the vendor signature on 'VNC-Viewer-6.2.0-Windows-64bit.exe' because it had been counter-signed by the trusted CA 'Symantec'. The software signer 'RealVNC LTD' is now a 'Trusted Software Vendor' and is added to the list. All future software that is signed by the vendor 'RealVNC LTD' 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 its 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:

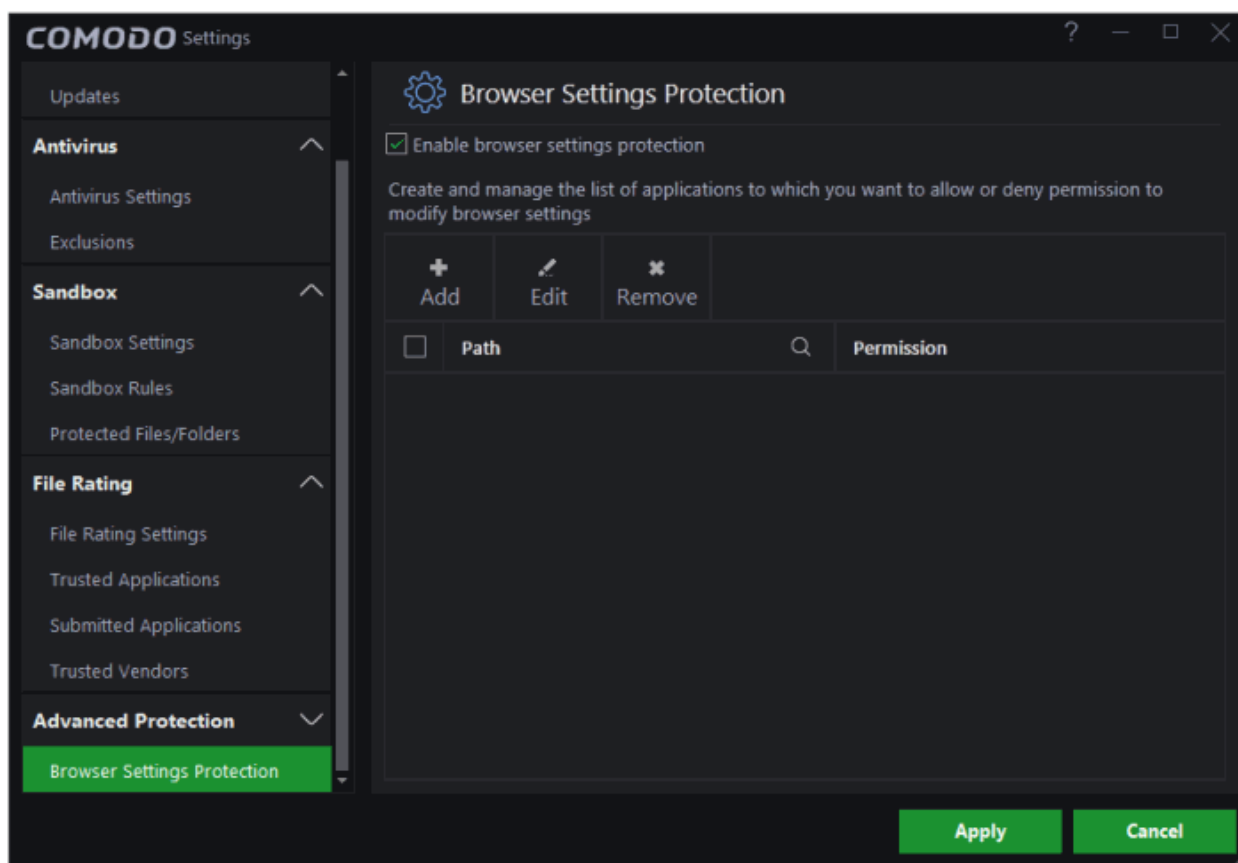
- The software is signed with a valid code signing certificate from a trusted CA;
- The software does not contain any threats that harm a user's PC;

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>.

## 6.5. Advanced Protection Settings

The 'Advanced Protection' section allows you to view and configure whether 3rd party applications are allowed to modify browser settings.



Refer to the following section for more details:

- **Browser Settings Protection**

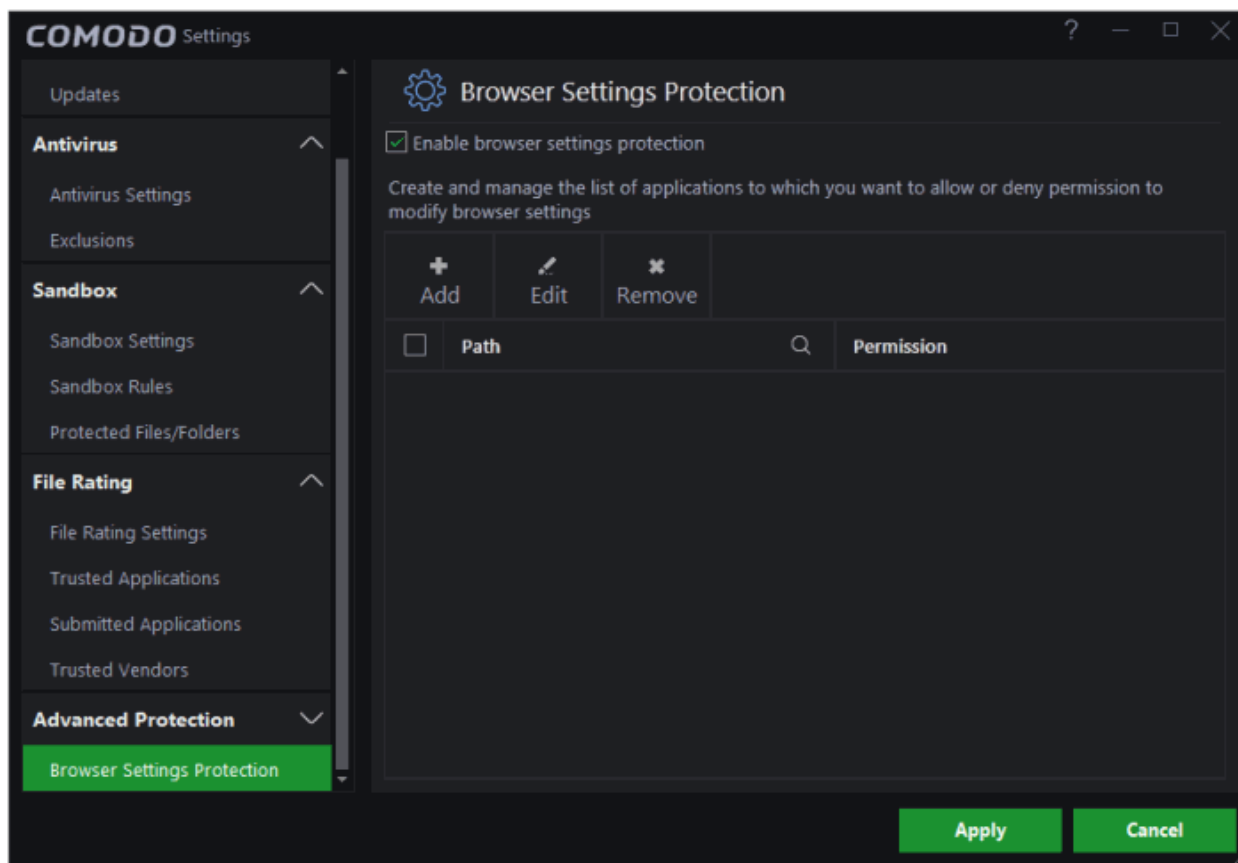
### 6.5.1. Browser Settings Protection

Browsers that are protected include IE, Comodo Dragon, Ice Dragon, Firefox, Chrome and Chromodo. If protection is switched on, the blocked apps will be automatically added to the list. You can also manually add individual apps and configure their browser access settings.

**To open the 'Browser Settings Protection' interface**

- Click the 'Settings' at the top left of the CCAV home screen to open the 'Settings' interface
- Choose 'Browser Settings Protection' under 'Advanced Protection' on the left






- **Enable browser settings protection** - Switch browser protection on or off.
  - If disabled, any protection that you have created will be disregarded.
  - If the protection is switched on, the blocked apps will be automatically added to the list.

The interface displays a list of applications added with the following details:

- **Path** - The installation path of the application
- **Permission** - Indicates whether 3<sup>rd</sup> party applications are allowed to alter the browser settings or not

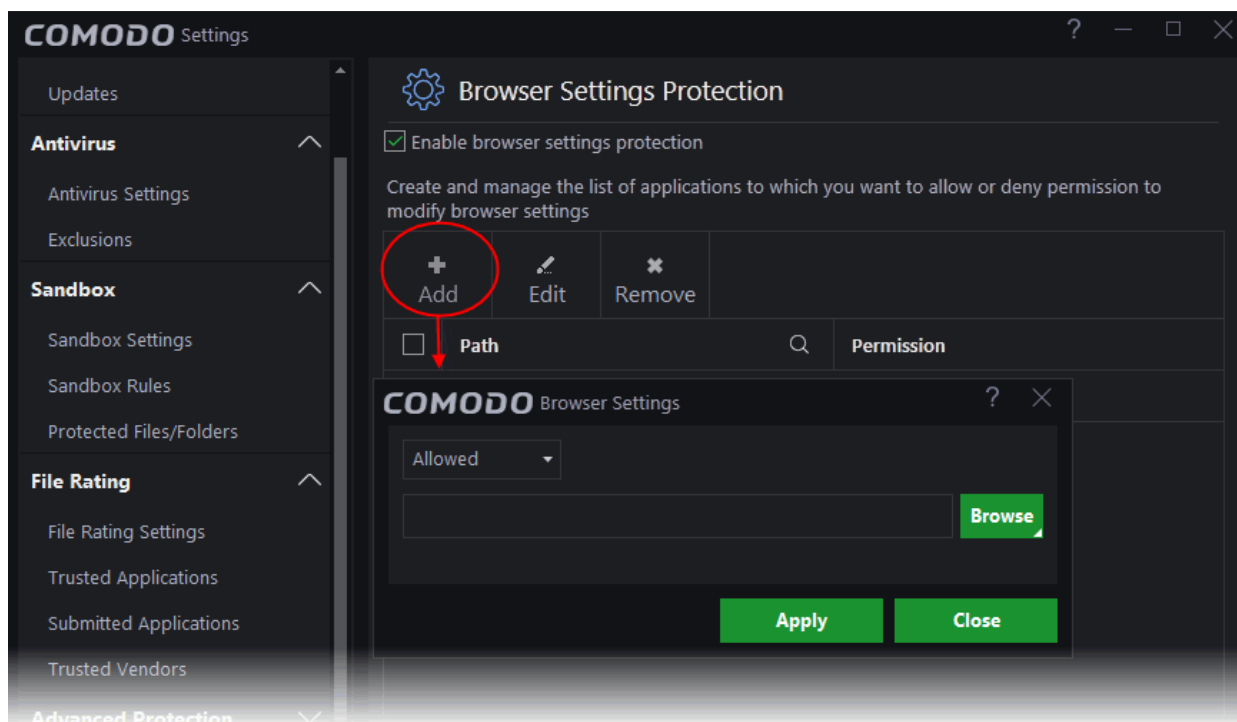
You can search for specific applications(s) from the list by clicking the search icon  in the table header and entering the name of the browser in part or full.

## Adding an application

You can add new a application and the protection status that should be applied to it.

### To add applications to the protection list

- Click 'Add' at the top of the 'Settings' interface to open the 'Browser Settings' dialog.



- Choose the action to apply from the drop-down at the top.

The available choices are:

- Allowed - Browsers in the system will allow 3<sup>rd</sup> party applications to modify the settings, for example, to gather information by accessing cookies to analyze your browsing habits and so on.
- Not Allowed - CCAV will block 3<sup>rd</sup> party applications from altering browsers' settings and provide an alert.
- Next, specify the application for which the settings should apply.

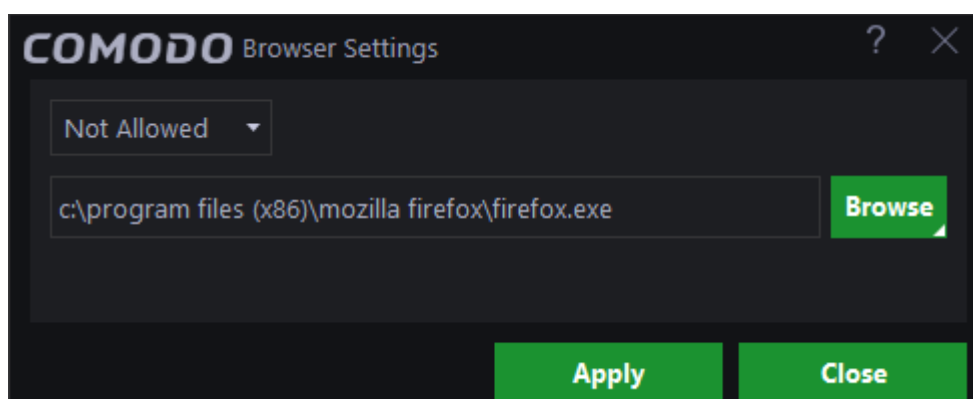
You have the following options:

- Enter the path of the application - Type or paste the full path of the application in the field provided.
- Browse your computer for the application - Click the 'Browse' button and select 'Application', navigate to the application and click 'Open'
- Select an application from running processes - Click the 'Browse' button and choose 'Running Processes' to select an application's processes which are currently running on your PC.
- After choosing your application, click 'Apply' for your settings to take effect.
- Repeat the process to add more applications.
- Click 'Apply' from the 'Settings' dialog for your protection settings to take effect.

If you feel that a safe application is blocked from modifying the browsers' settings, you can edit the settings to allow it.

## Editing browser settings

- Select and click the 'Edit' button at the top or simply double-click on it.



The edit dialog is same as 'Browser Settings' dialog. Refer to the explanation [above](#) for more details.

- To remove an application from the list, select the check-box next to the application's name and click 'Remove'.


An example of the alert for a protected browser is shown below:



## 7. Getting Live Support

Comodo GeekBuddy is a personalized computer support service provided by friendly computer experts at Comodo. GeekBuddy technicians can help solve most computer issues through web-based chat sessions. Do you need help to get rid of a particularly nasty virus? Has your computer slowed down to a crawl for no apparent reason? Are you having trouble setting up that wireless router you just bought? GeekBuddy techs can offer you expert guidance and, with your permission, can even remote-desktop into your computer and fix your problems while you sit back and watch. No longer do you need to make time consuming calls to impatient help desk support staff. Instead, just sit back and relax while our friendly technicians do the work for you.

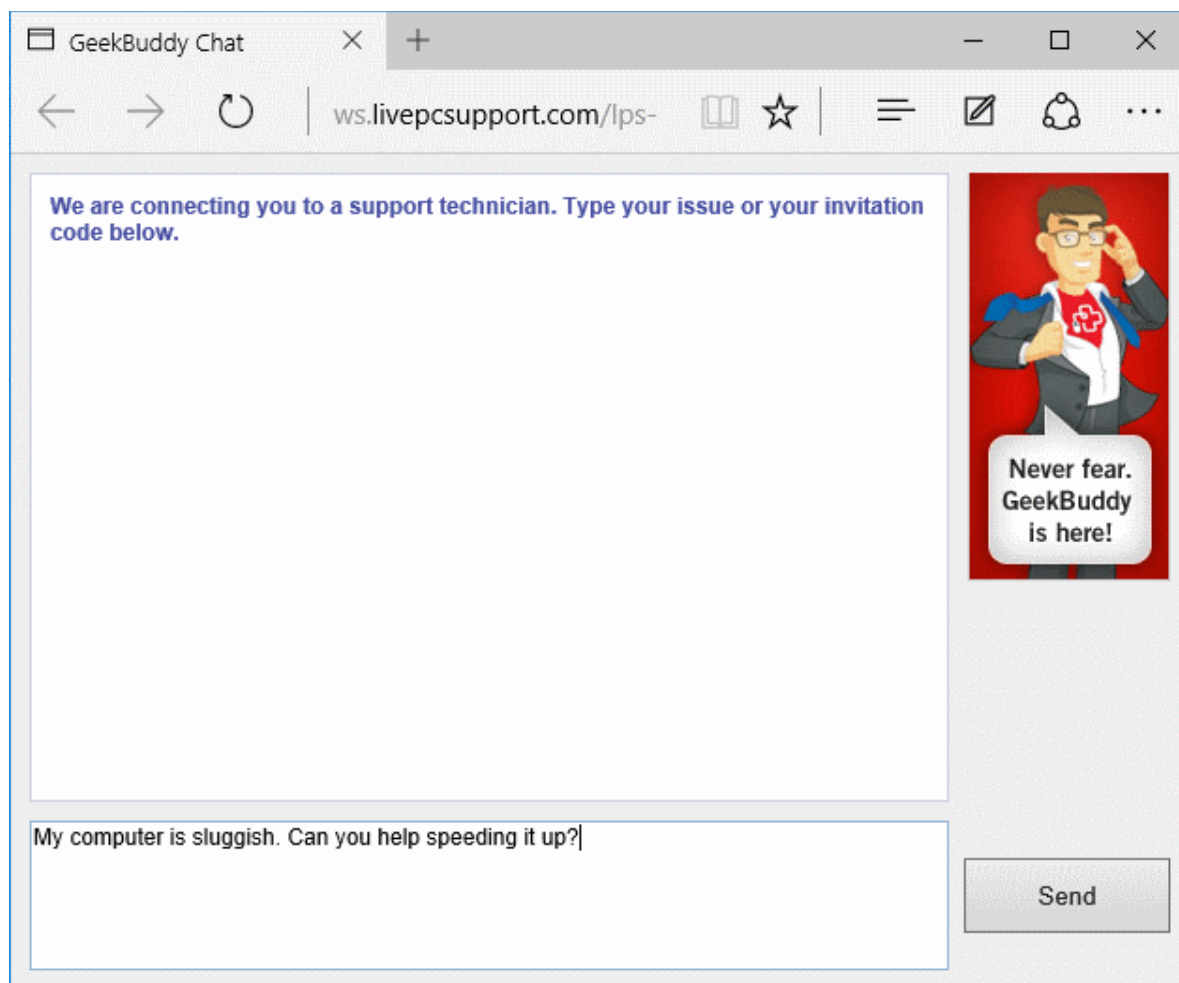
### To get instant support

- Click the 'Live Support' icon  on the menu icon bar

OR

- Click the 'Help' icon at the top right of the interface and choose 'Live Support'

A web based chat will start on your default browser. You will be connected to a Geekbuddy technician.



Chat away! Ask for help with any issue that you are experiencing with your PC. The technician will assess your problem, offer advice, work with you to fix issues, and can even connect to your PC and perform system maintenance.

Visit <https://www.geekbuddy.com/> for more details.

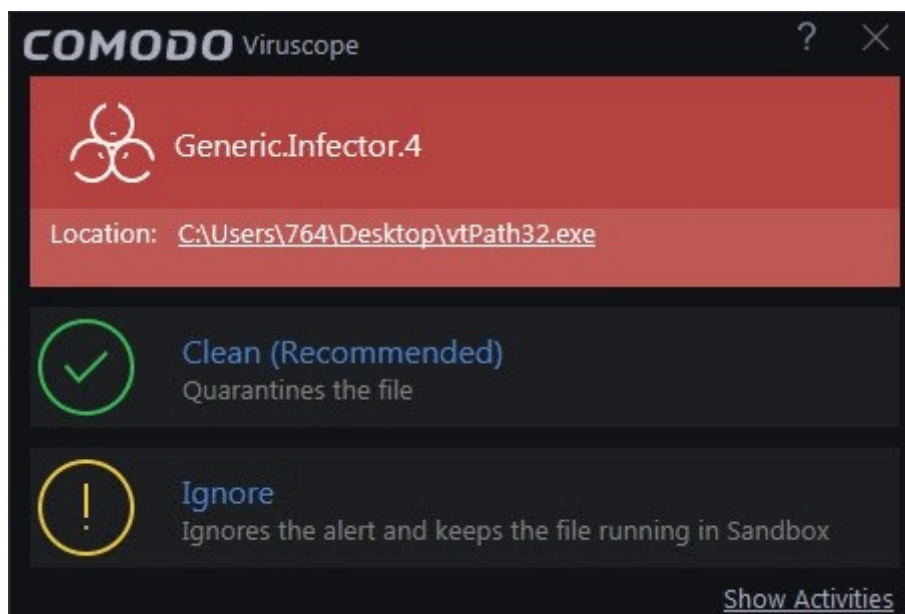
## 8. Viruscope - Feature Spotlight

Comodo Cloud Antivirus (CCAV) provides unrivaled 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.

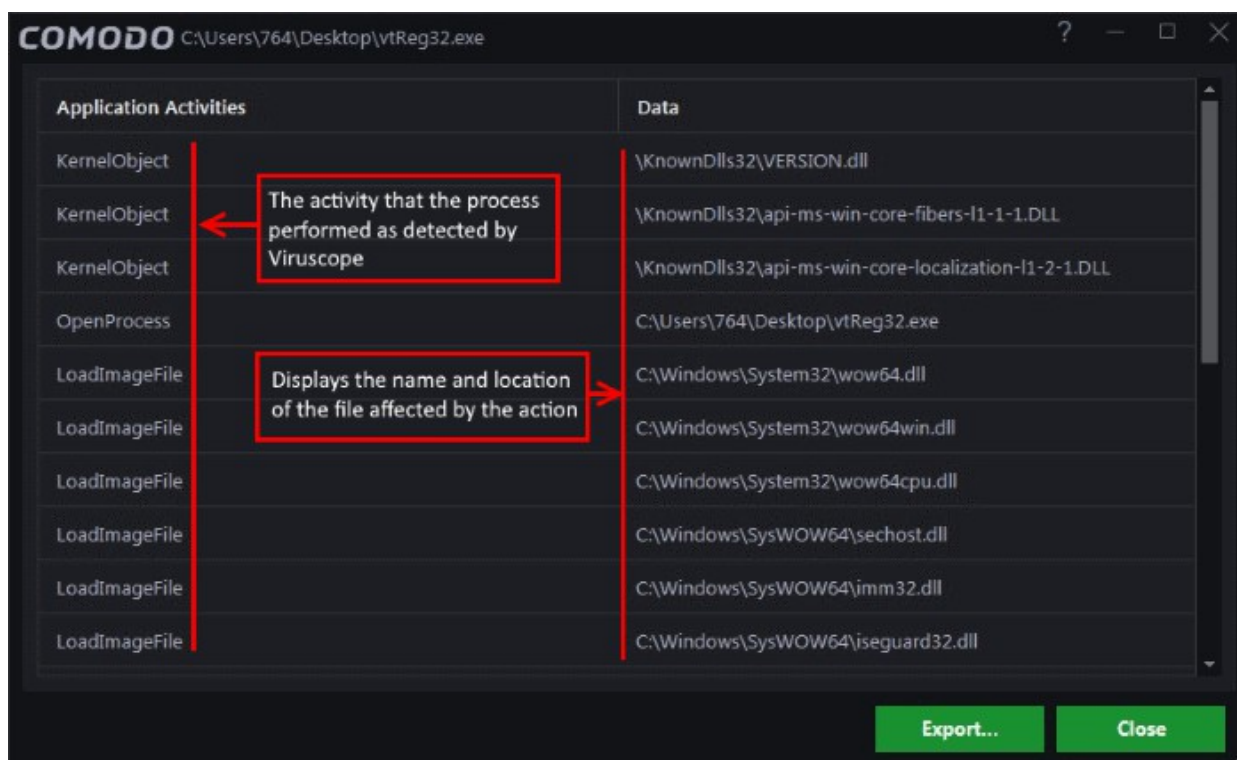
But what do we do to evaluate the behavior of unknown files in the sandbox? Enter Viruscope.

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:



- 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:



Viruscope identifies zero-day malware by using a sophisticated set of behavior 'Recognizers', each of which can 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.

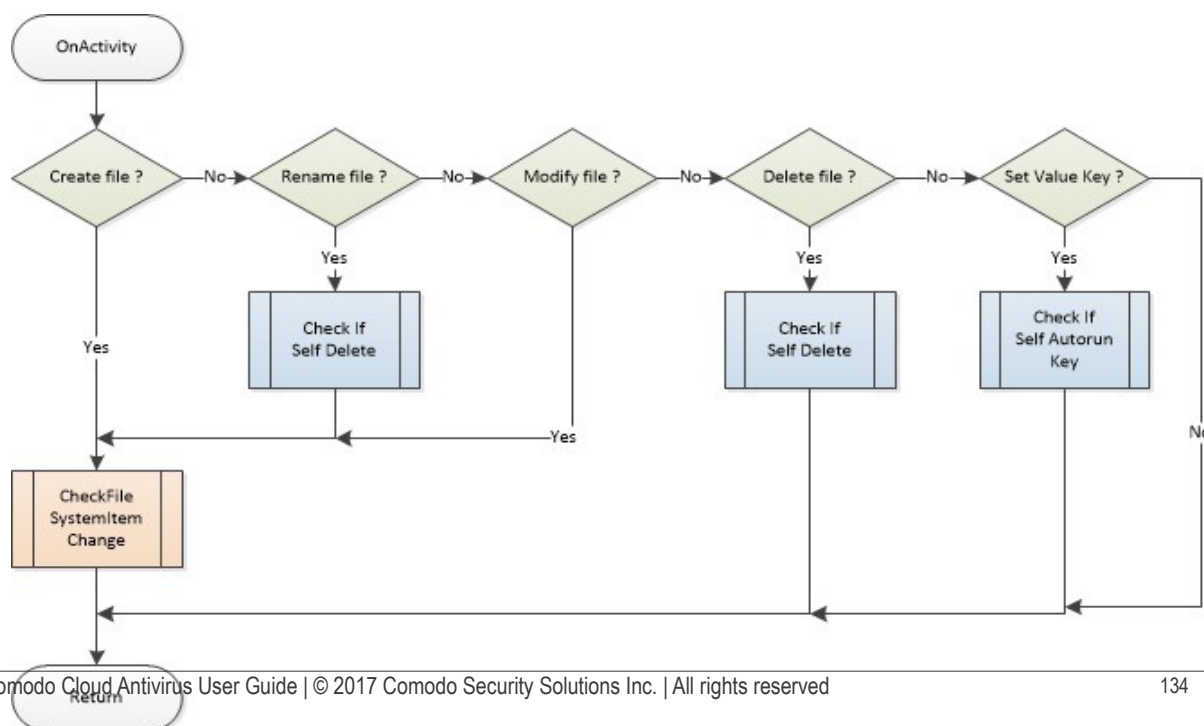
Technically, the core Viruscope technology contains the following items:

- 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 queuing 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:



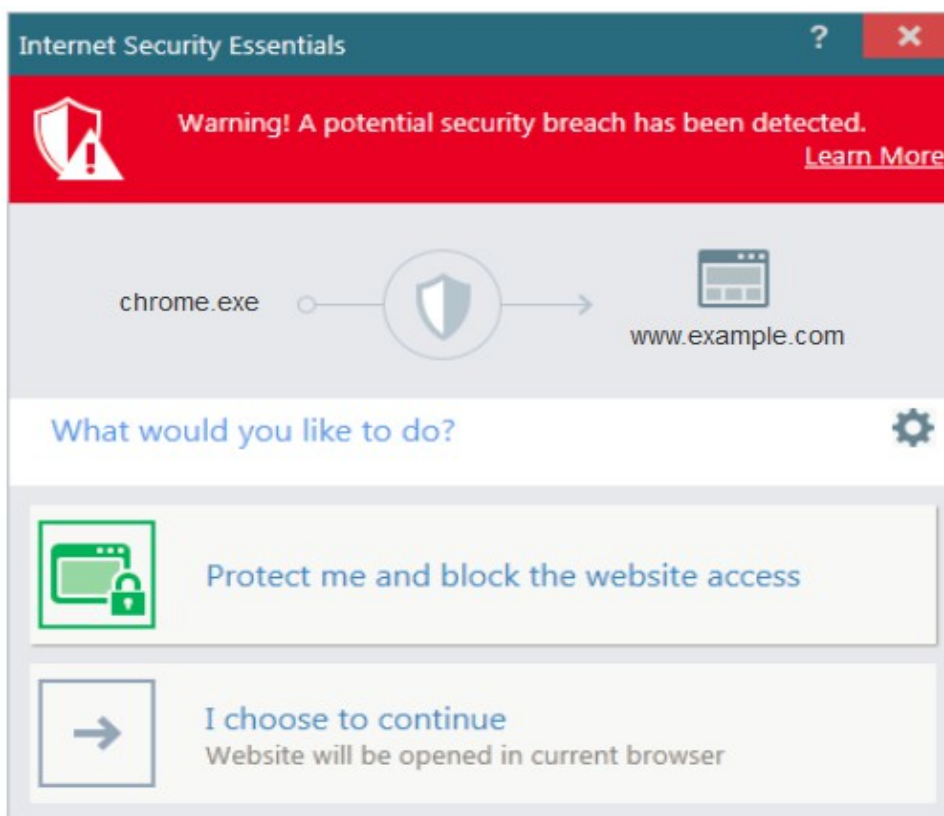
Viruscope is another key layer of security in the CCAV arsenal, taking our protection beyond that found in any other antivirus product. Our real-time virus monitor protects you against known threats, while auto-sandboxing protects you against unknown threats. With Viruscope on top, you also get proactive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

## 9. Comodo Internet Security Essentials

### What is Comodo Internet Security Essentials?

Comodo Internet Security Essentials (CISE) protects you from man-in-the-middle attacks during online banking and shopping sessions by verifying that sites you connect to are using a trusted SSL certificate.

CISE runs as a background process and will alert you if a site uses a potentially malicious certificate. You will have the option to discontinue the connection (recommended) or to continue.

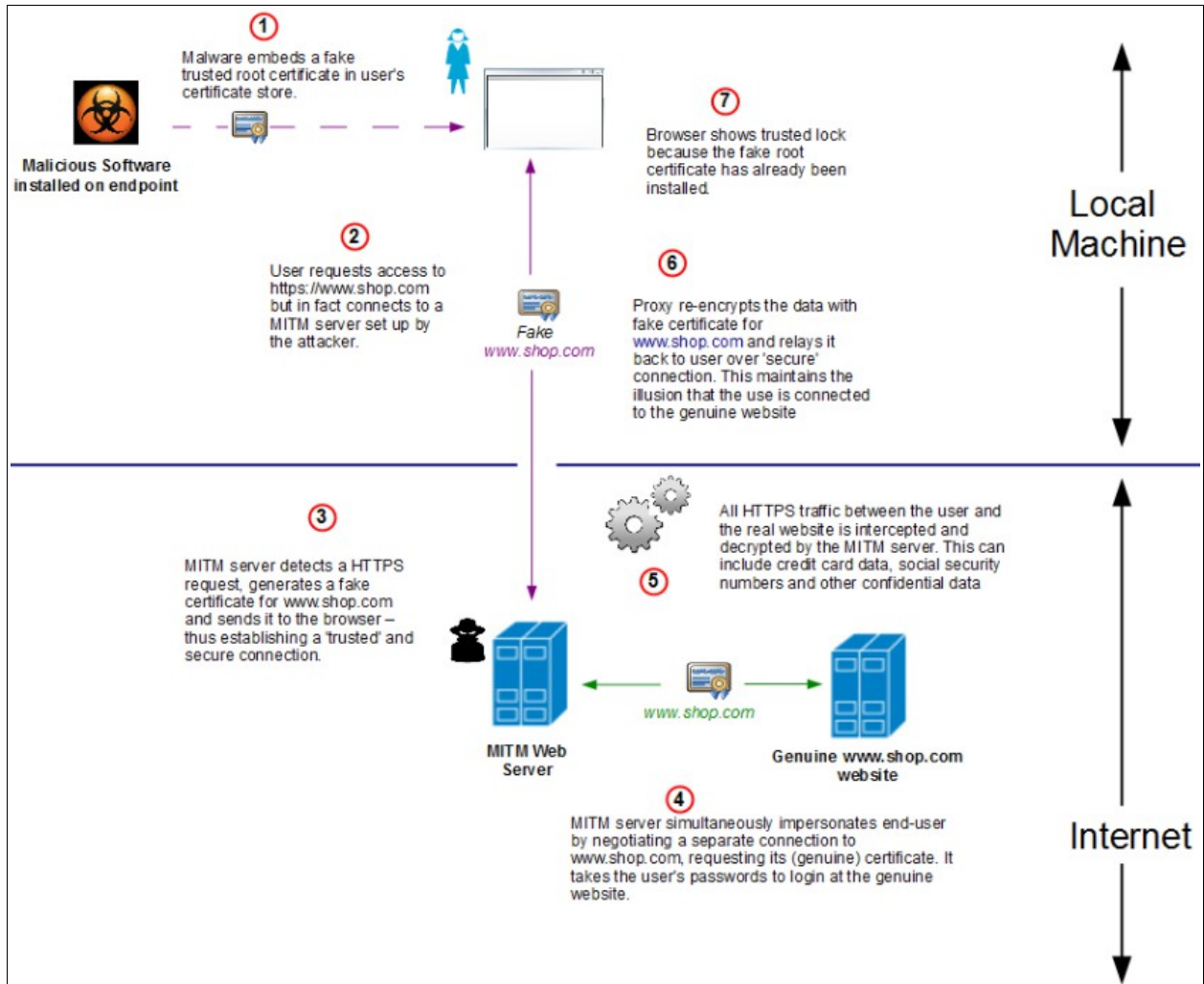


CISE blocks man-in-the-middle attacks attempts by verifying certificates against Comodo's trusted root certificate list. This functionality is especially important if you are accessing sensitive websites while on a public Wi-Fi such as those found in an cafe, park or airport.

### What is a man-in-the-middle attack?

Man-in-the-middle attacks occur when an attacker forces a client to connect to a server other than the one that the client intended to connect.

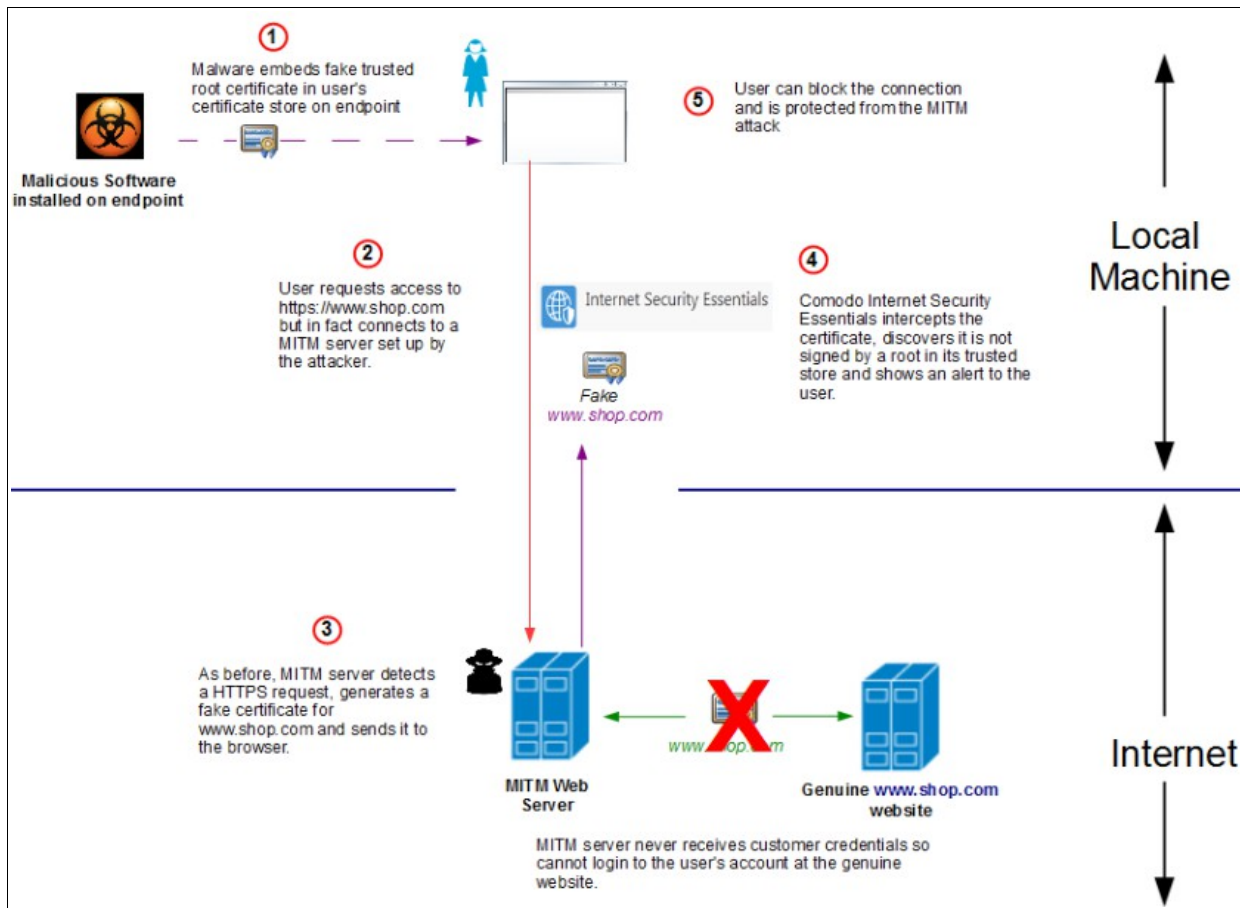
By injecting a fake root certificate into the Windows certificate store, malicious actors can often fool browsers into trusting a connection to a server operated by an attacker. This is known as certificate root poisoning and is the most commonly used technique for launching man-in-the-middle attacks. If successful, all data sent from your browser would be routed through the attacker's server. The following diagram shows a typical man-in-the-middle attack:



## How does Comodo Internet Security Essentials protect me from a man-in-the-middle attack?

Comodo Internet Security Essentials blocks these attacks by independently verifying all certificates used for secure connections against an internal, verified list of trusted root certificates. The following diagram shows how CISE will thwart a man-in-the-middle attack:





## What is the install location of Comodo Internet Security Essentials?

By default, Comodo Internet Security Essentials is installed at:

C:\Program Files (x86)\Comodo\Internet Security Essentials

## How do I remove Comodo Internet Essentials?





Internet Security Essentials installs as a standalone program and must be removed separately. Uninstalling the application that CISE was bundled with will not remove nor deactivate the program.

To remove Comodo Internet Security Essentials:

- Open the Windows control panel then open 'Programs and Features' (or 'Add/Remove Programs' on older versions of Windows)
- Select 'Internet Security Essentials' in the list of programs
- Click 'Uninstall'

## Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

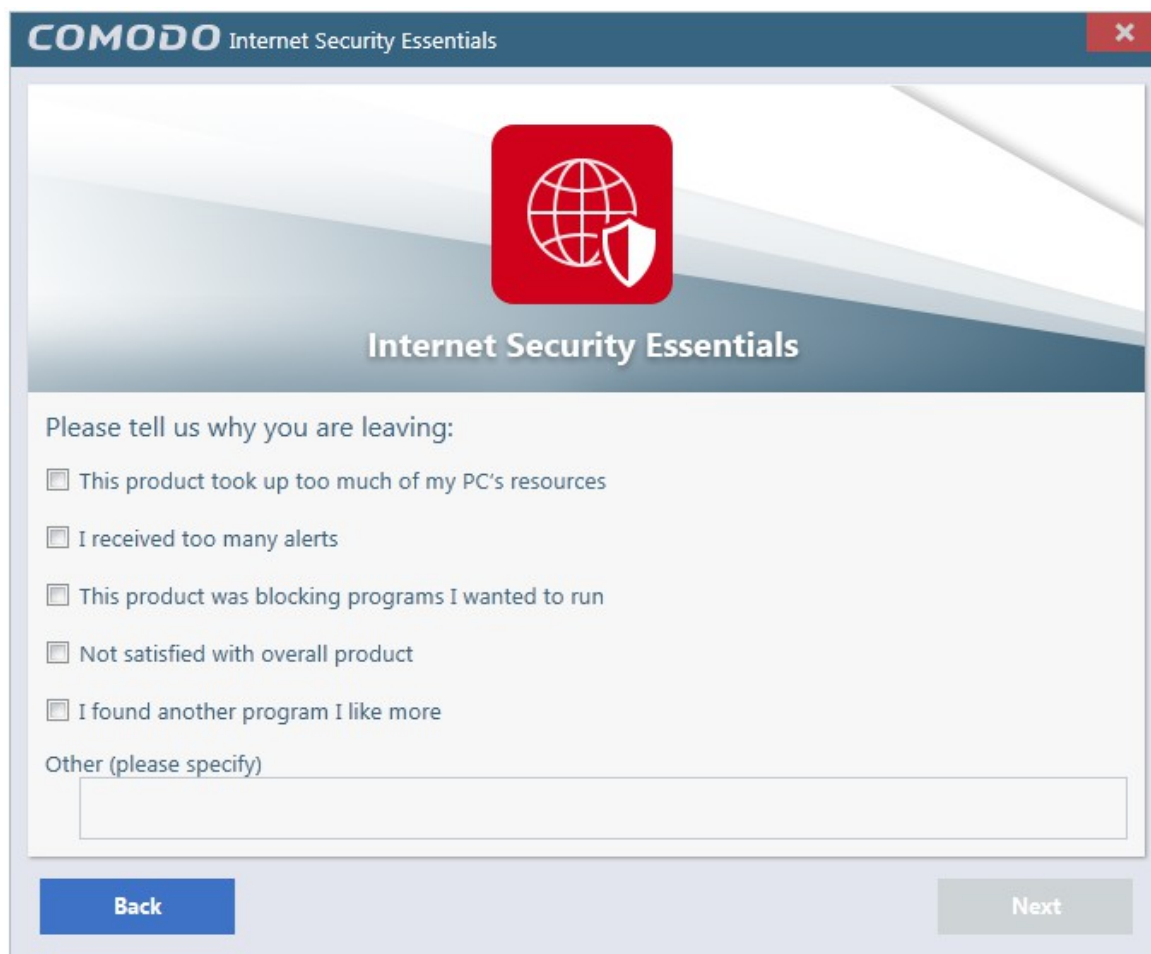
Organize ▾ Uninstall	
Name	Publisher
 Intel® USB 3.0 eXtensible Host Controller Driver	Intel Corporation
 Internet Security Essentials	Comodo
 Java 8 Update 77	Oracle Corporation
 Lenovo Auto Scroll Utility	

- The uninstallation wizard will start. Click 'Uninstall' to remove the program:

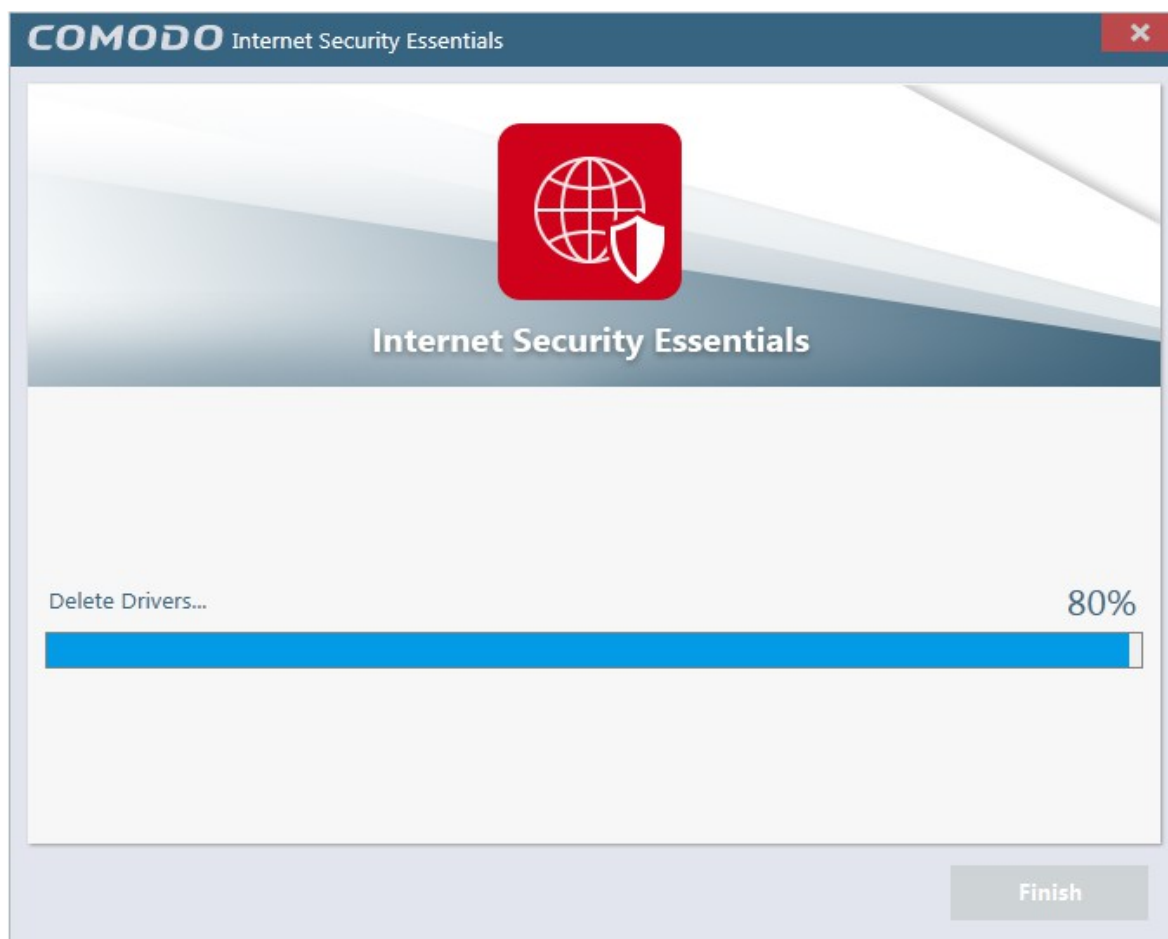




- Please provide us with valuable feedback by specifying the reason that you are uninstalling Comodo Internet Security Essentials:



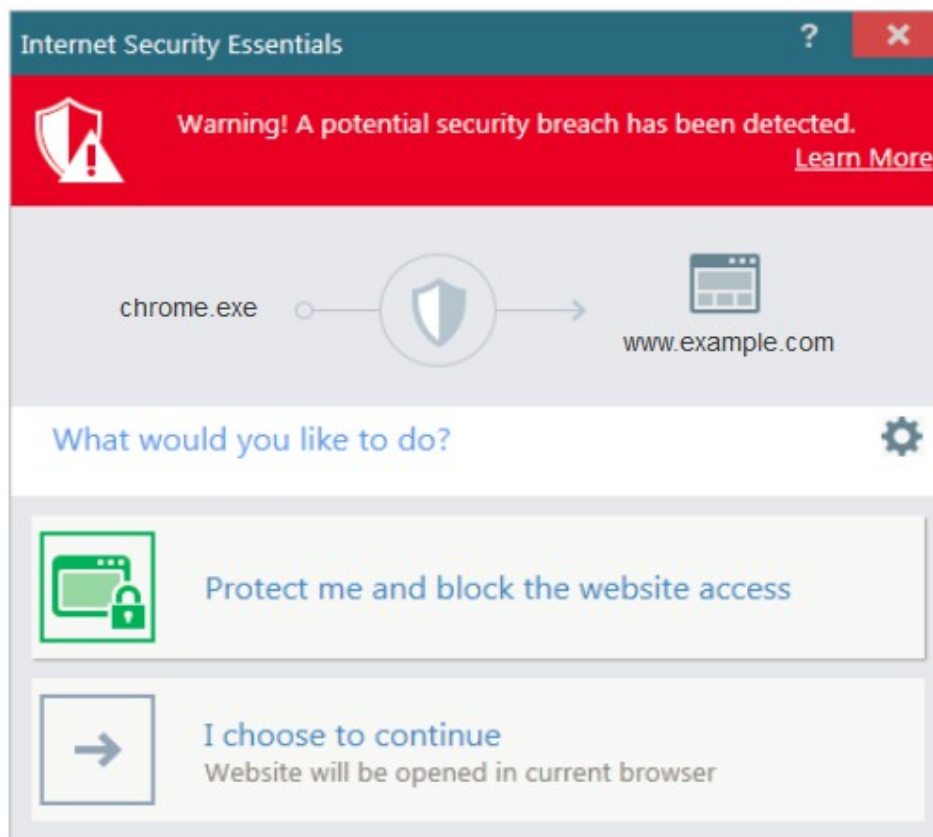
- Click 'Next' to complete the uninstall:



That's it! Click 'Finish' to close the program.

## 9.1. Understanding Alerts

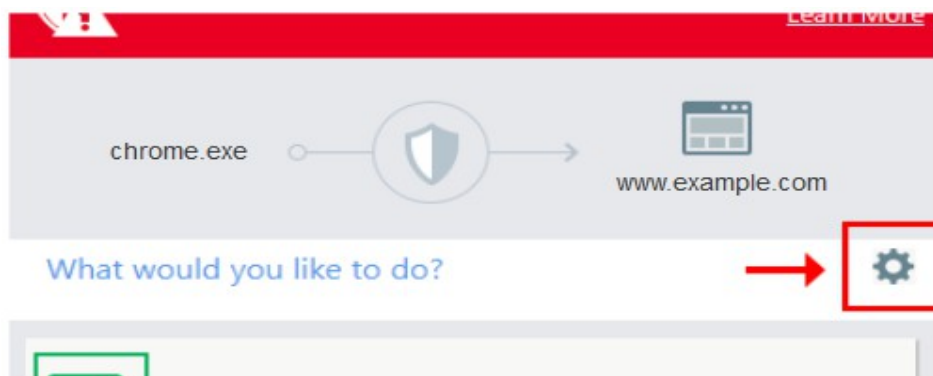
If Comodo Internet Security Essentials (CISE) detects that a website is potentially using a fraudulent certificate, it will present you with an alert similar to the following:



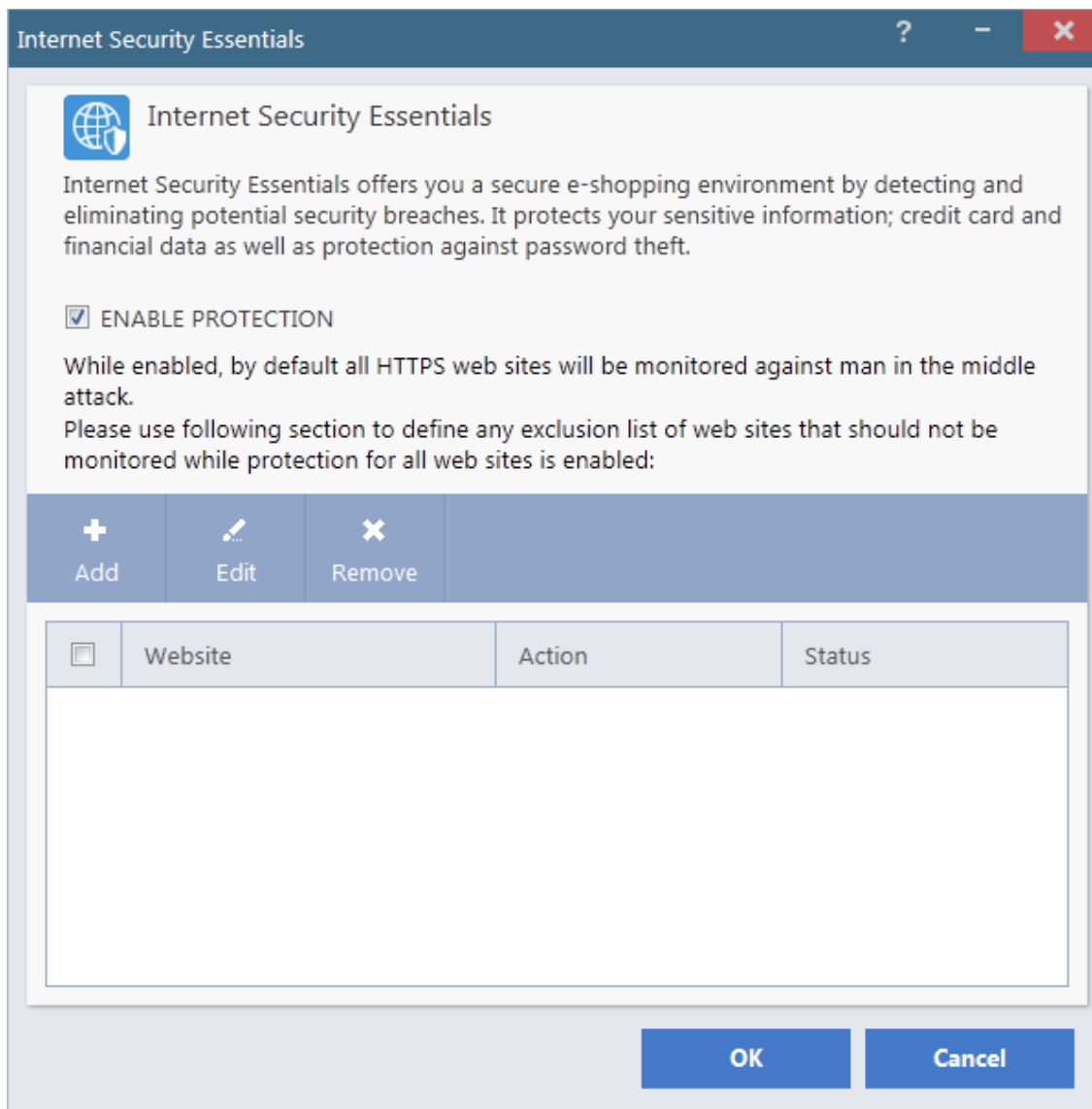
The alert means that the website you are visiting may be fraudulent as it is using a certificate signed by a root that is not in CISE's internal store of trusted root certificates.

- Protect me and block website access - Closes your connection to the website (recommended)
- I choose to continue - Allows the connection to proceed as normal. Only choose this option if you are sure the website can be trusted or is using, for example, a self-signed certificate that you have already been made aware of. Do not choose this option if this is one of your regular shopping or banking websites.

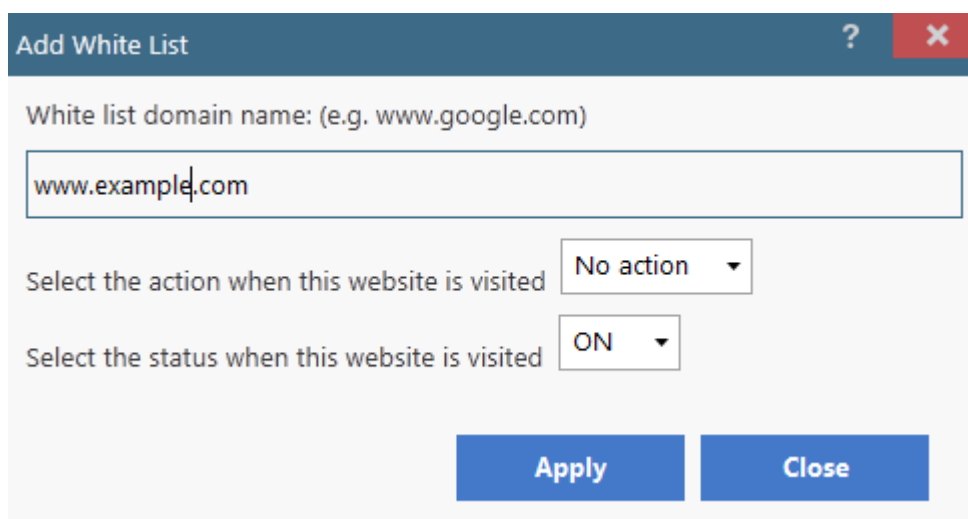
You can exclude websites from CISE checks by clicking the cog icon in the alert:



This will open the CISE white-list configuration screen:



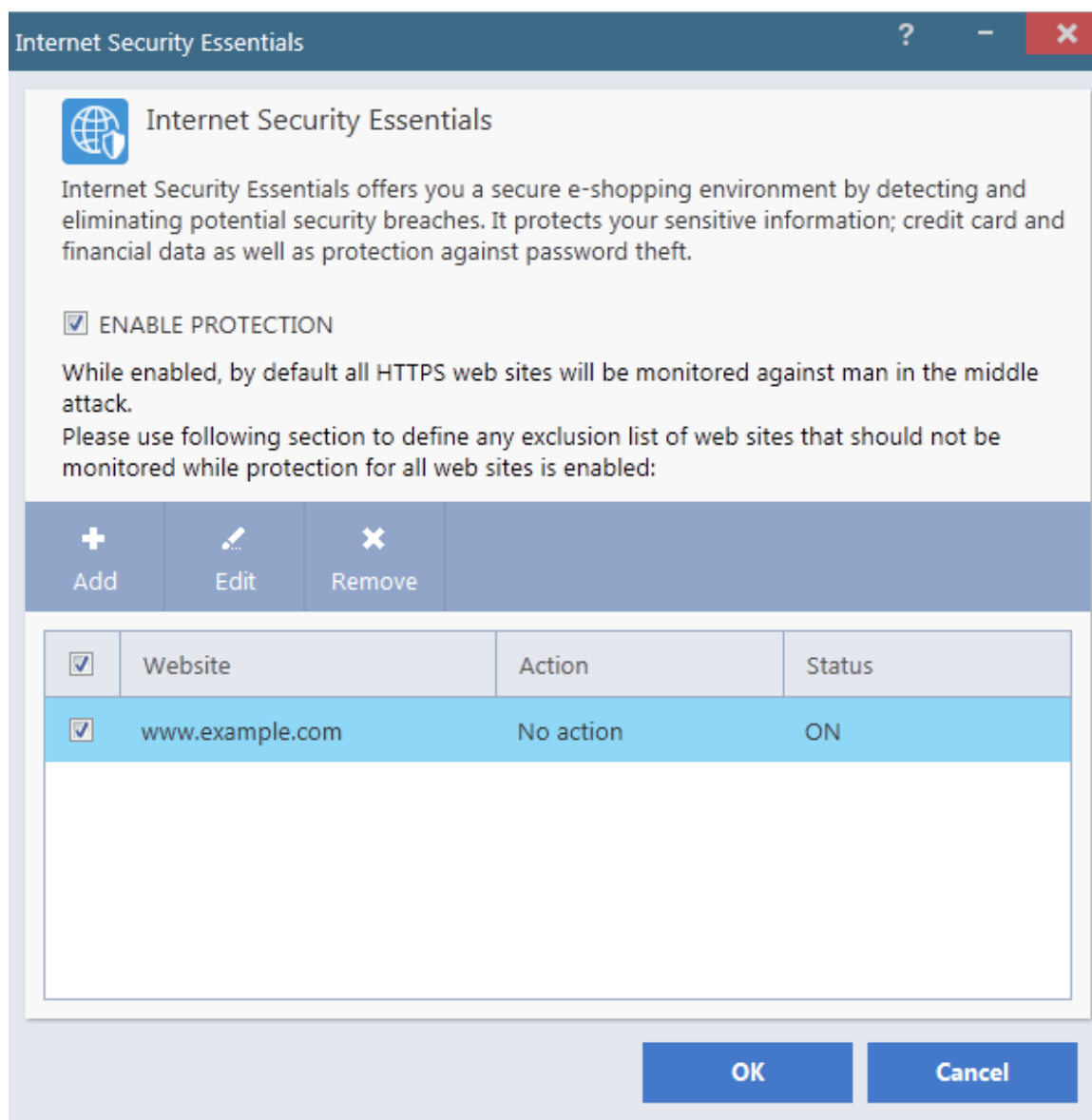
- Click the 'Add' button to open the white-list configuration dialog:



- Enter the URL of the web site you wish to exclude in the field provided.
- **Select action when this web site is visited** - 'No action' means CISE protection is switched off.
- **Select status when this website is visited** - allows you to enable or disable the website action.
  - **ON** - Will apply the 'No action' action i.e. CISE protection is disabled for this site
  - **OFF** - Will not apply the 'No action' action - CISE protections will be enabled for this site.

To exclude a site, make sure the drop-down boxes are set to 'No action' and 'ON'.

- Click 'Apply' to add the site to the white-list:



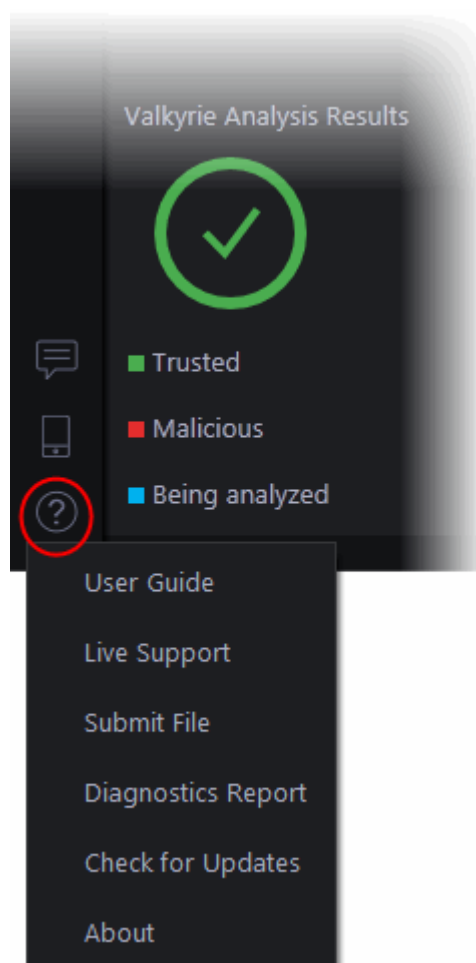
- Click the 'Edit' button if you wish to modify CISE protection for a site
- Click 'Remove' to delete a site from the white-list. Removing a site will automatically re-enable CISE protection.

[Click Here](#) to find out more about Comodo Security Essentials.



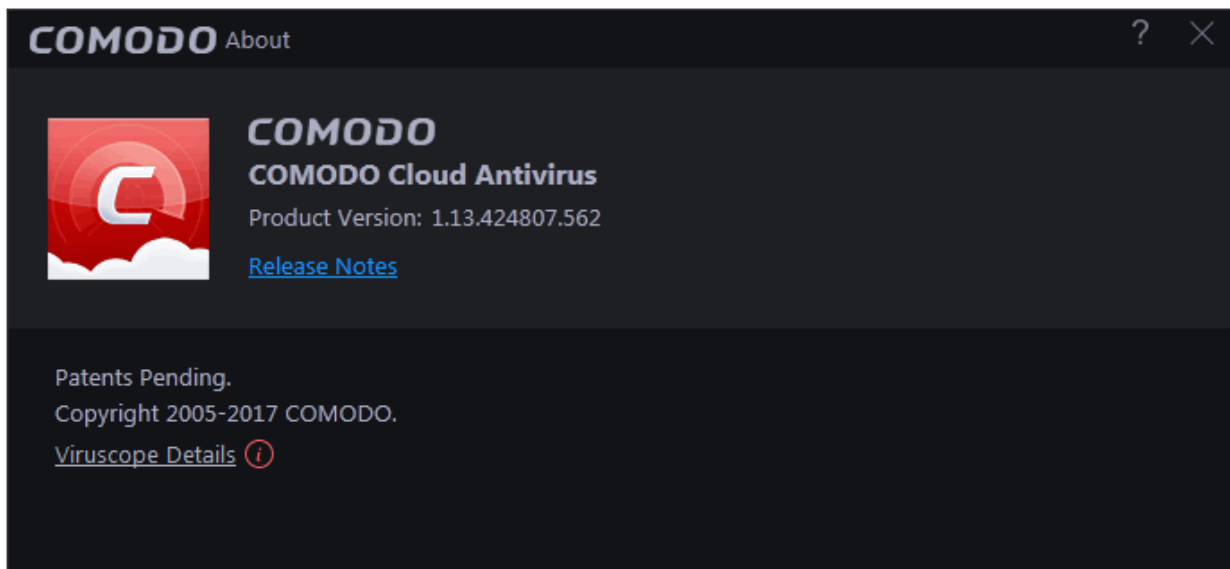
## 10. Comodo Support and About Information

The 'Help' icon from the side menu icon bar lets you view the Comodo Cloud Antivirus online help guide; start a chat support session with a technician at Comodo, submit suspicious files for analysis, check the application for upcoming updates, collect system information to report for further sending it to our technicians, and view the current product version, copyright information, and viruscope details.

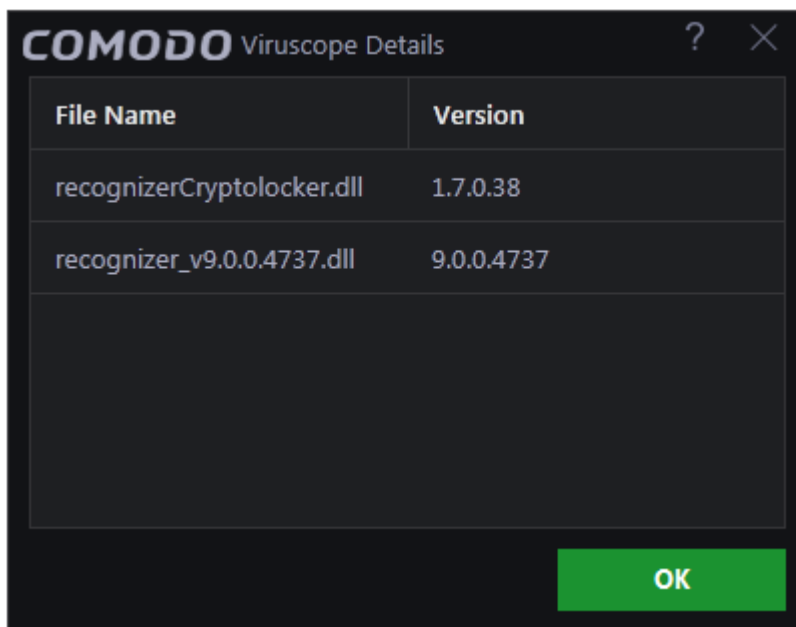


- **User Guide** - Opens the CCAV online help guide at <https://help.comodo.com>
- **Live Support** - Choose this option to chat with our technician for technical help for CCAV. A chat session will start in your browser window and you will be connected to a Microsoft certified support technician at Comodo. The expert support is available 24/7. Refer to the section **Getting Live Support** for more details.
- **Submit File** - Allows you to manually submit a suspicious file to Valkyrie for analysis. Valkyrie analysis involves automated and manual testing in order to discover whether or not the file is malicious. The results will be sent back to your computer once the analysis is complete. The results will be added to the global white-list and black-list to help fellow CCAV users who encounter the same file. Refer to the section **Viewing Valkyrie Analysis Results** for more details.
- **Diagnostics Report** - Generates a full report about your system, including loaded modules, services, Windows errors, Auto codes, IDE and more.

- **Check for Updates** - Peremptory antivirus database update as regularly as possible.
  - If updates are available, click 'Apply' to start the installation
  - Click 'Restart System Now' in order to your updates take affect
  - Click 'I will restart late' to postpone for later on
- **About** - Displays the product version, details of active Viruscope Recognizers, release notes for upcoming updates and copyright information.



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



## Appendix 1 - How to Tutorials

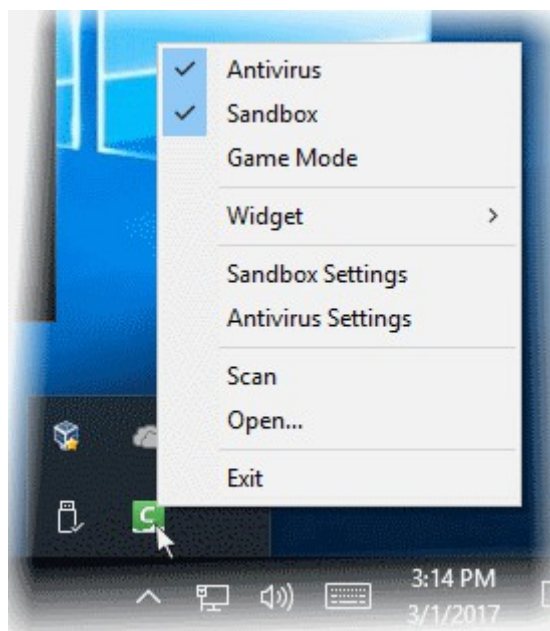
The following 'How To...' tutorials contain help with common tasks in Comodo Cloud Antivirus:

### How to..

- **Enable / Disable AV, Sandbox and Game mode** - How to enable or disable various CCAV components
- **Run an Antivirus scan on selected items** - How to start a manual scan on selected folders/files to check for viruses and other malware.
- **Block Incoming / Outgoing Internet connection to sandboxed applications** - How to control connections to applications in the container
- **Add exclusions by allowing Internet connection to sandboxed applications** - How to configure exceptions for contained applications to allow internet connection.
- **Enable/ Disable realtime scan** - How to scan your computer manually or automatically
- **Run a Virus scan on your computer** - How to run various types of virus scan
- **Run a Certificate scan on your computer** - how to scan your computer
- **Running an Application or Browser in the sandbox** - How to run your browser, inside the container to make internet surfing much more secure
- **Configure antivirus exclusions** - How to skip applications while running a scan
- **View lucky you statistics** - How to view zero-day threats that were blocked by Comodo before any other antivirus company had recognized them as malicious.
- **Switch Off Automatic Antivirus and Software Updates** - How to stop automatic software and virus updates
- **Evaluate the behavior of unknown files in the sandbox** - How to assess the behavior of unknown files
- **Detect Potentially Unwanted Applications (PUA)** - How to detect files whose activities are questionable or unclear.
- **Manually add items to quarantine** - How to add files to isolated environment
- **Delete quarantined items** - How to remove quarantined files
- **Restore a quarantined item** - How to restore an isolated file back to its original location
- **Submit as False Positive** - How to send files that you feel have been mis-identified as malware to Comodo for re-evaluation.
- **Configure Proxy and Host Settings** - How to set up proxy and host settings for provisioning CCAV updates
- **Enable / Disable Sandbox indicator** - How to enable / disable the green border around sandboxed applications
- **Enable / Disable viruscope** - How to enable or disable Viruscope, the advanced behavior monitor for sandboxed processes.
- **Respond to CCAV alerts** - How to manage, understand and answer Cloud Antivirus alerts
- **View CCAV Logs** - How to view CCAV and manage CCAV logs
- **Get instant support** - How to get fast and accurate support for any Computer related issue you may be experiencing.

## Enable / Disable AV, Sandbox and Game mode

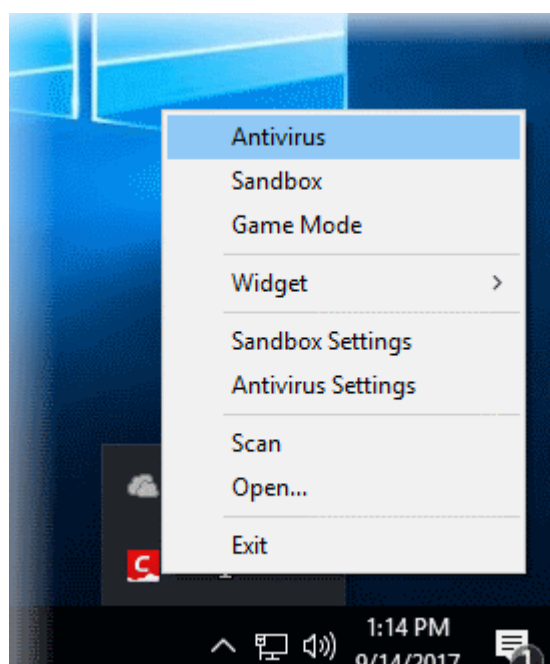
Right-click on the system tray icon to quickly enable or disable the **Antivirus**, **Sandbox** and **Game Mode**



### Antivirus

#### To enable/disable the Antivirus

1. Right-click on the CCAV tray icon
2. Click on the option 'Antivirus'



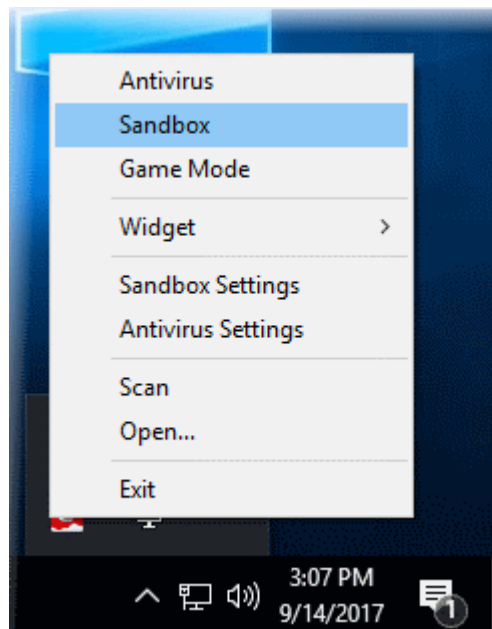
All antivirus protection will be disabled. Comodo recommends you re-enable the antivirus at the earliest opportunity to ensure you are protected from malware and attacks.

You can also view the status in **Antivirus Settings**.

## Sandbox

### To enable/disable the sandbox

- Right-click on the CCAV tray icon
  - Click on the option 'Sandbox'



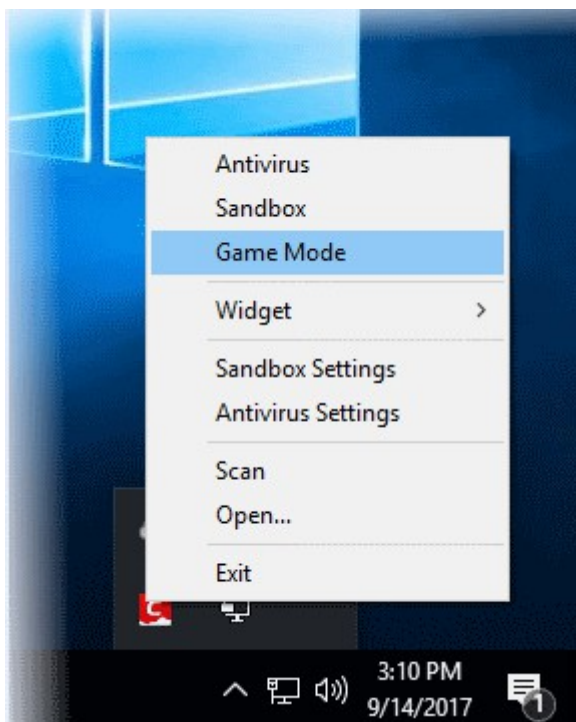
The Sandbox will be disabled if in enabled mode. By default the Sandbox option is enabled.

You can also view the status in [Sandbox Settings](#).

## Game Mode

### To enable/disable the game mode

- Right-click on the CCAV tray icon
  - Click on the option 'Game Mode'




Game Mode will be activated, suppressing all alerts. Protection will, of course, remain active. By default the game mode option is disabled.

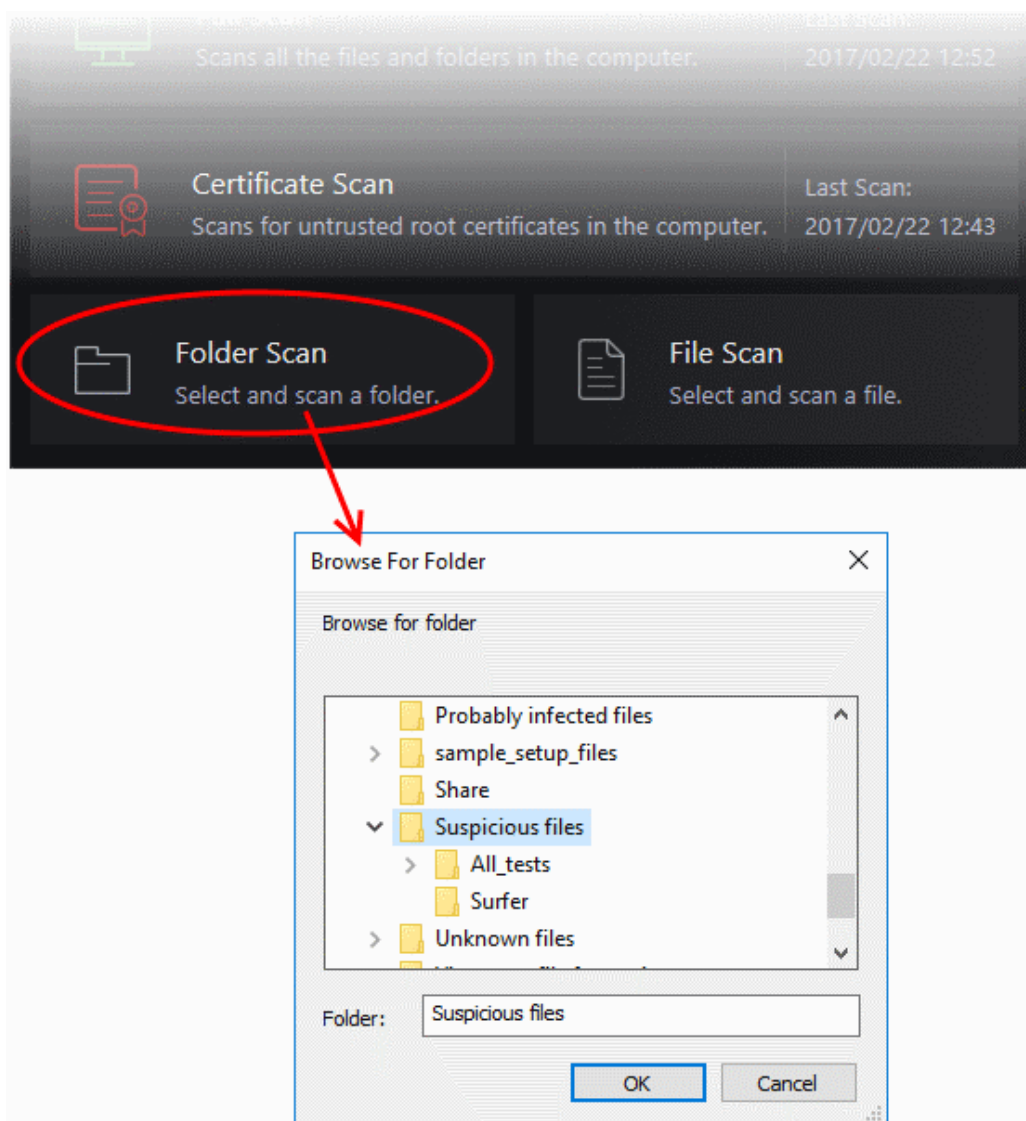
You can also view the status in **Game mode**.

## Run an Antivirus scan on selected items

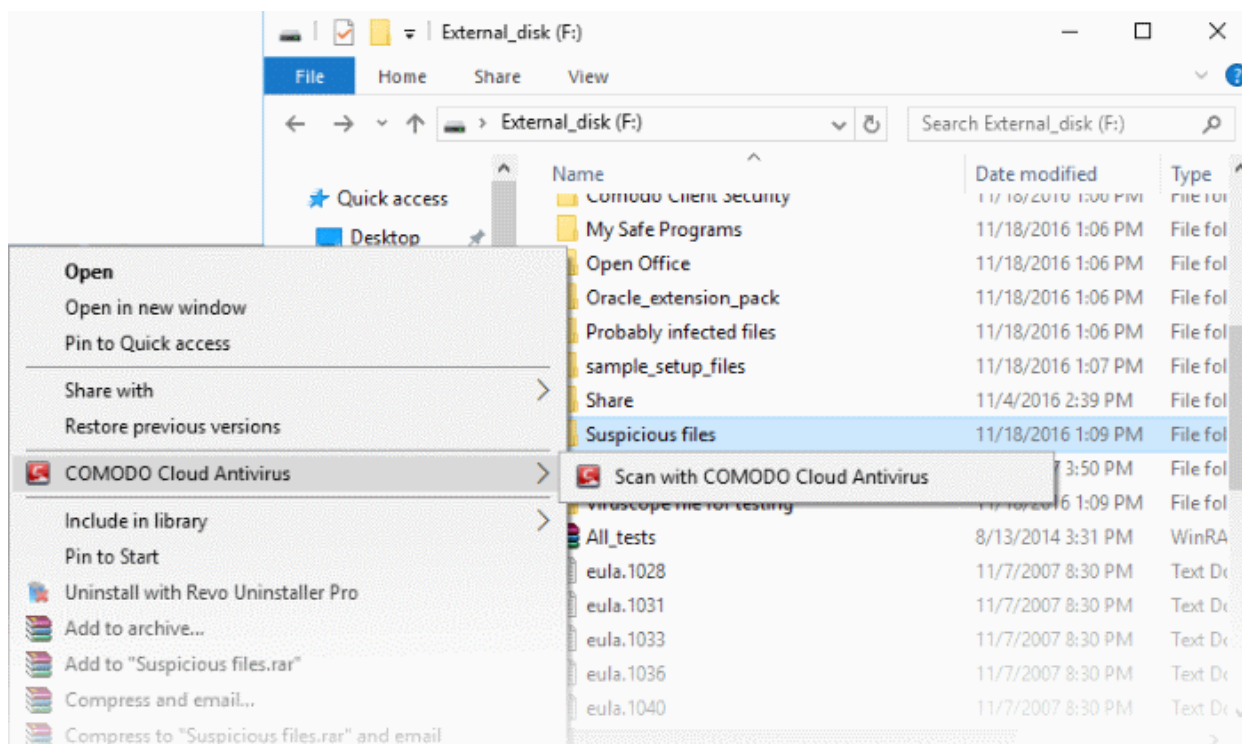
To run a virus scan on your system, launch an **On-Demand Scan** using the 'Scan' option. This executes an instant virus scan on the selected item on your computer. You can also use the right-click options to scan individual items.

### To run a scan on selected items

- Click 'Scan' from the 'Tasks Bar'.  
OR
- Click the Scan  shortcut button from the widget  
OR
- Right-click on 'Scan' from the CCAV system tray icon
- Click 'Folder Scan' if you want to scan a folder from the 'Scan' interface.  
OR
- Click 'File Scan' if you want to scan file from the 'Scan' interface.



- Alternatively, right-click on a 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.

Similarly you can individually scan files on your computer.

## Block Incoming / Outgoing Internet connection to sandboxed applications

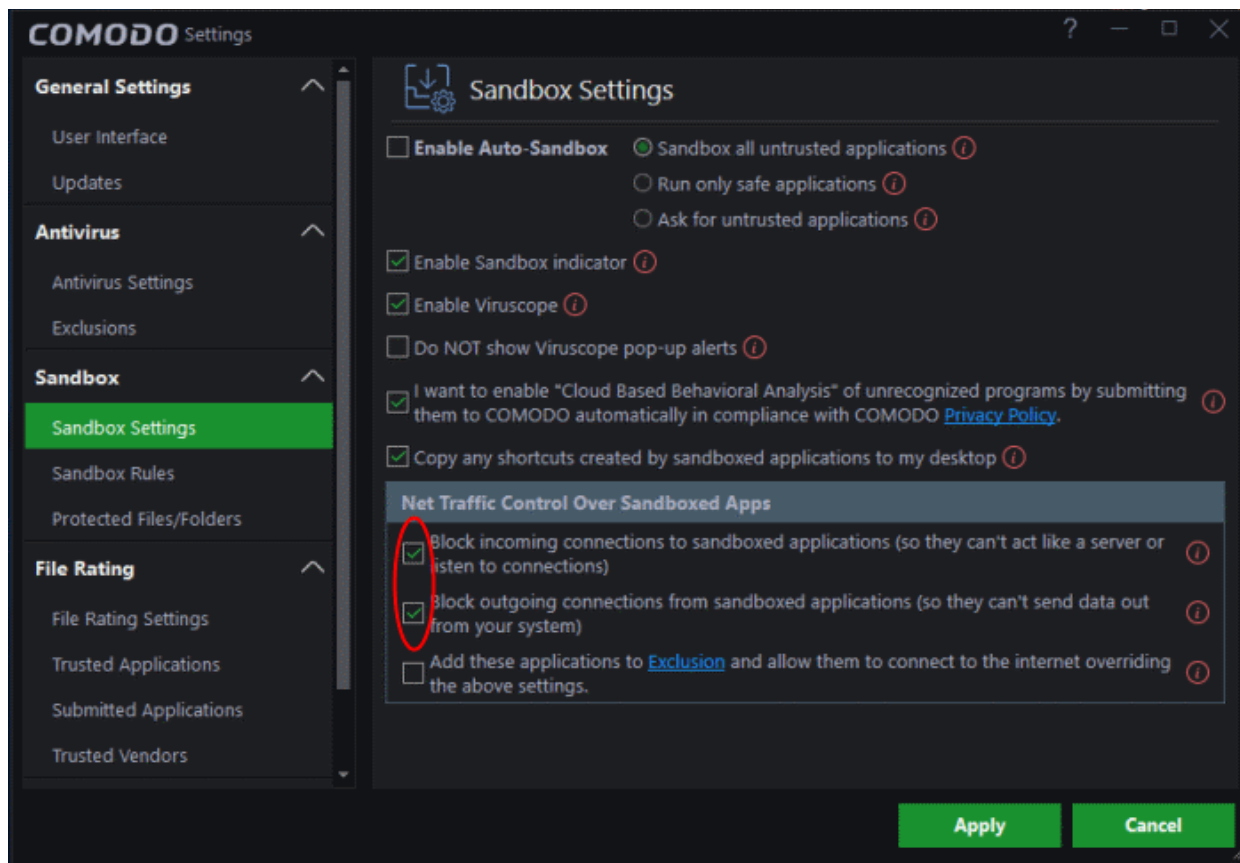
To open scan interface:

- Click 'Scan' from the 'Tasks Bar'.
- OR
- Click the 'Scan'  shortcut button from the widget
- OR
- Right-click on 'Scan' from the CCAV system tray icon

To control internet traffic:

- Click 'Sandbox Settings' on the scan interface
- Click 'Block incoming connections to sandboxed applications'
- OR
- Click 'Block outgoing connections from sandboxed applications'

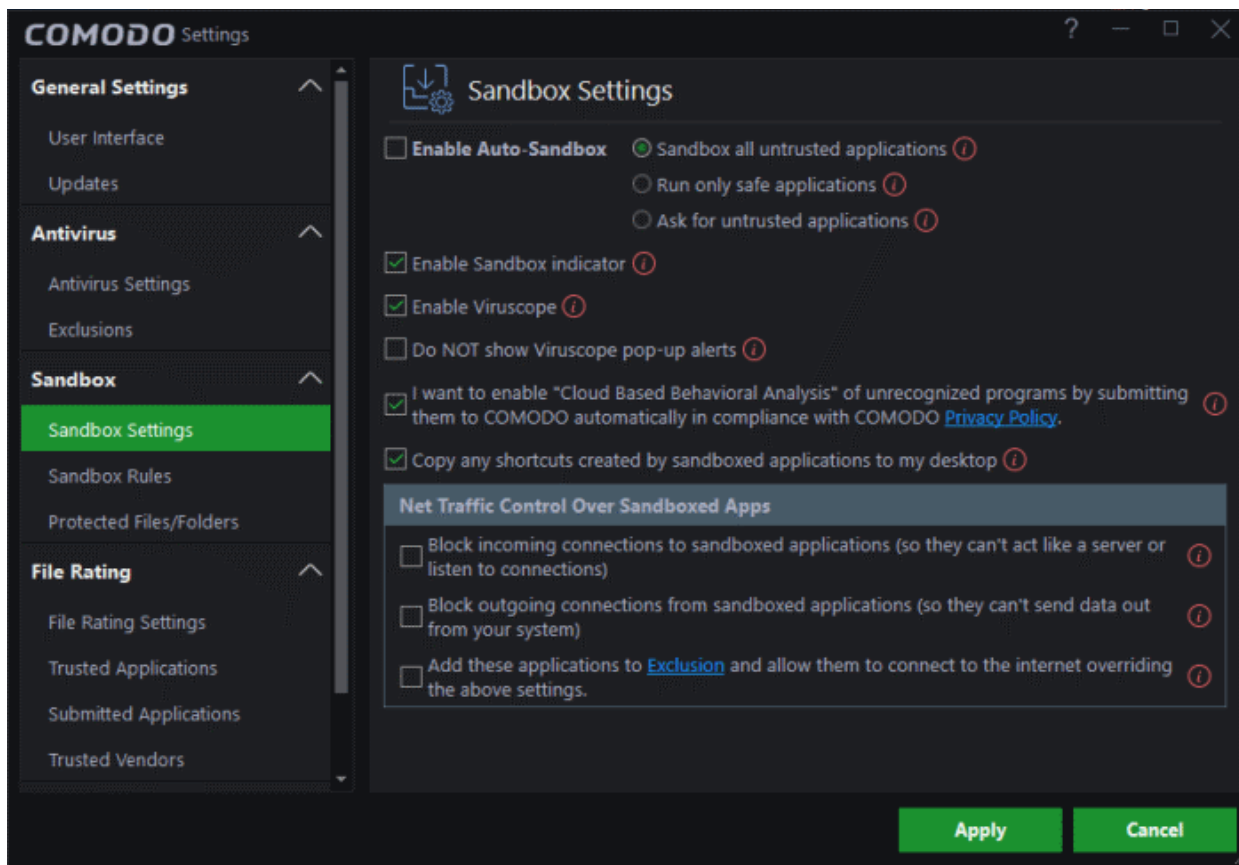




## Add exclusions by allowing Internet connection to sandboxed applications


To add exclusions to the above settings:

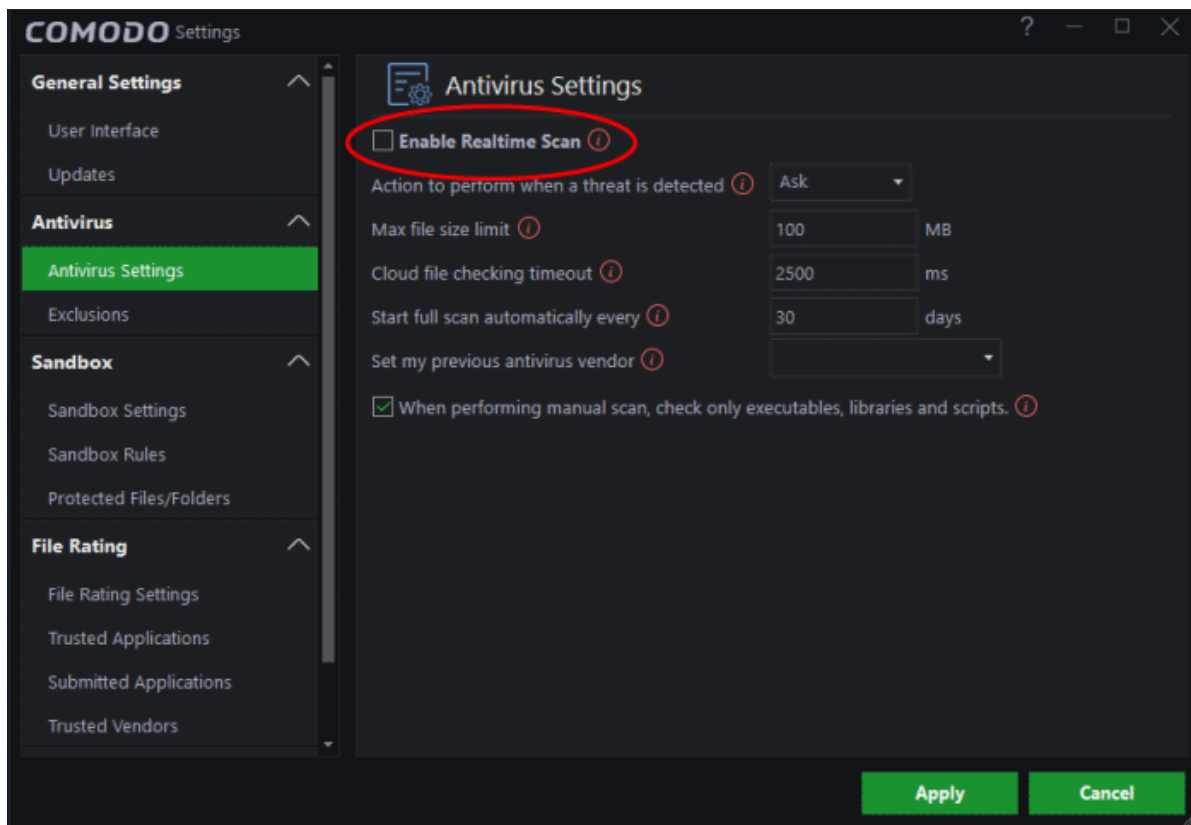
- Open the scan interface as mentioned earlier.
- Select the 'Add these applications to Exclusion ... override the above settings' option



## Enable/ Disable Realtime scan

To open scan interface:

- Click 'Scan' from the 'Tasks Bar'.  
OR
- Click the 'Scan'  shortcut button from the widget  
OR
- Right-click on 'Scan' from the CCAV system tray icon
- Click 'Antivirus Settings' in the scan interface
- Select the 'Enable Realtime Scan' option



## Run a virus scan on your computer

**CCAV offers multiple ways to run virus scans on your computer. To get started:**

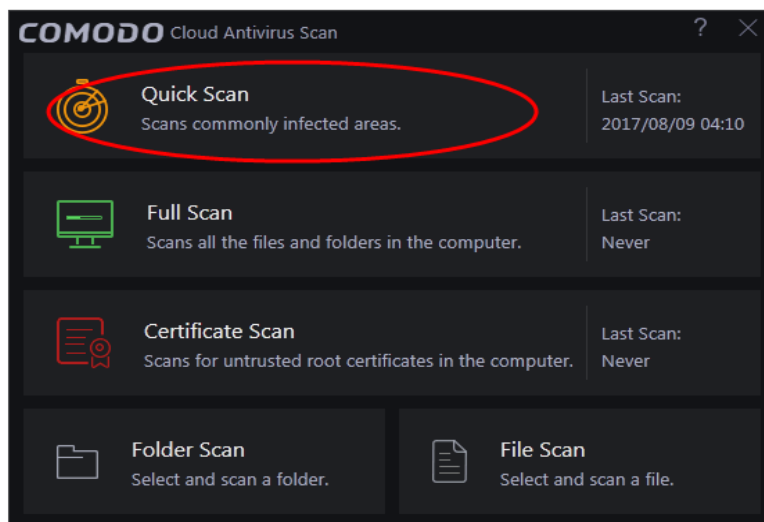
- Click 'Scan' on the CCAV home screen to open scan options

### Quick Scan

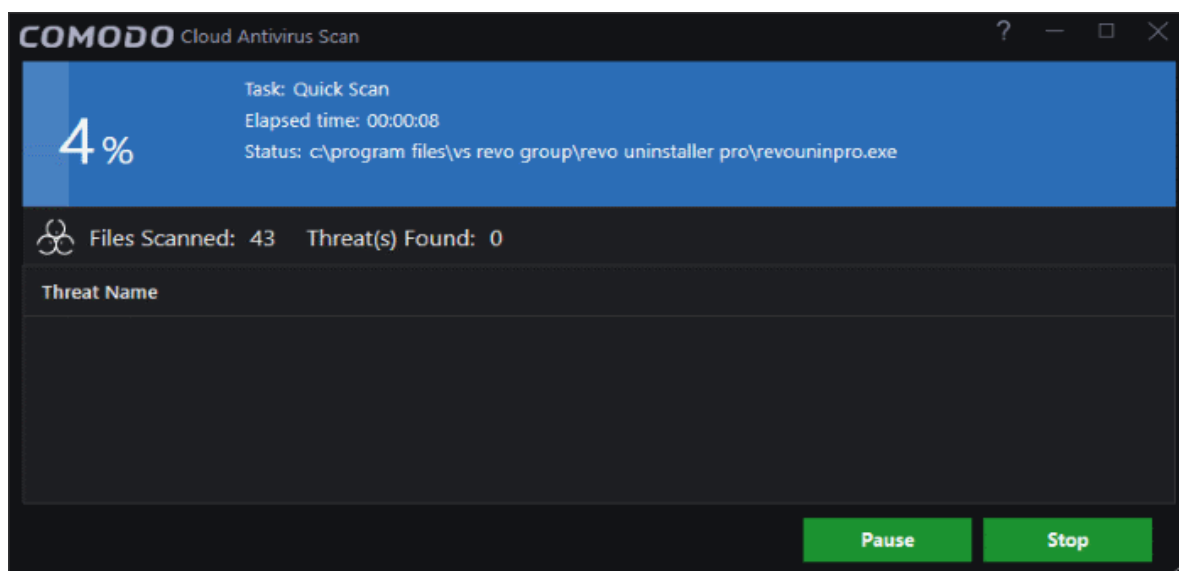
A quick scan covers the important areas of your computer that are frequently targeted for attack by malware.

#### To run a Quick Scan

- Click 'Scan' on the CCAV home screen then 'Quick Scan'
- OR
- Click the scan button on the widget then 'Quick Scan'

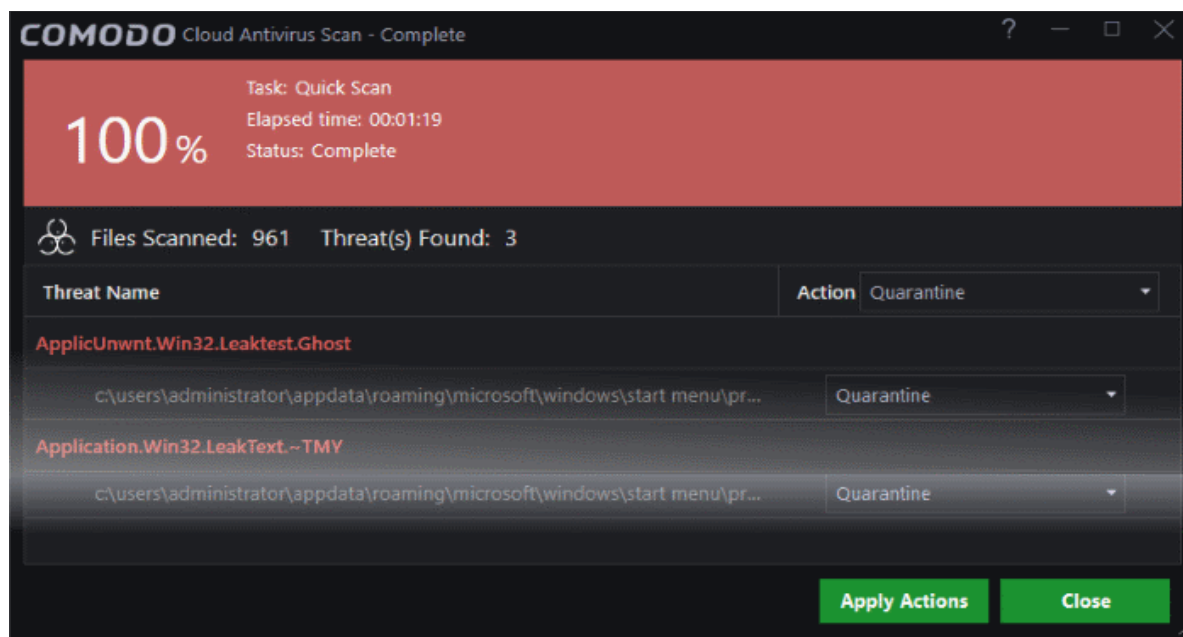


The scanner will start and the scan progress will be displayed:



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

The results window will be displayed when the scan is complete:



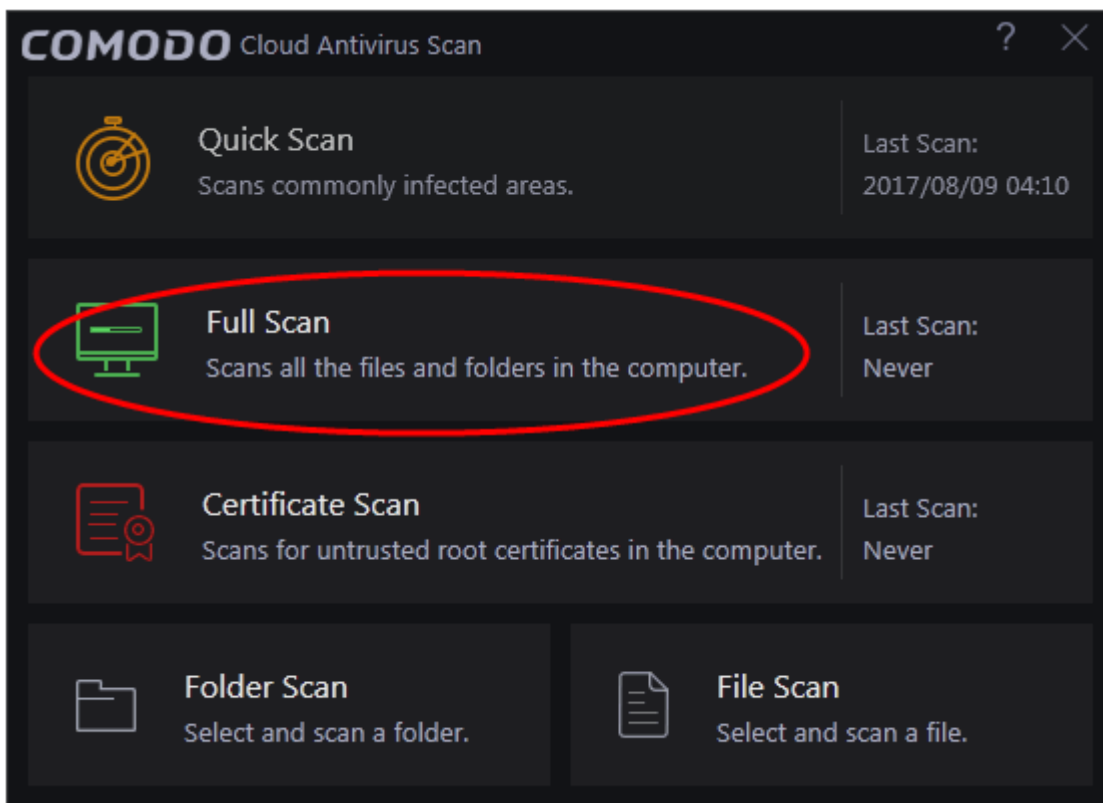
Use the drop-down menu to choose whether to clean, quarantine or ignore the threat. Refer to [Processing infected files](#) for more details.

## Full Scan

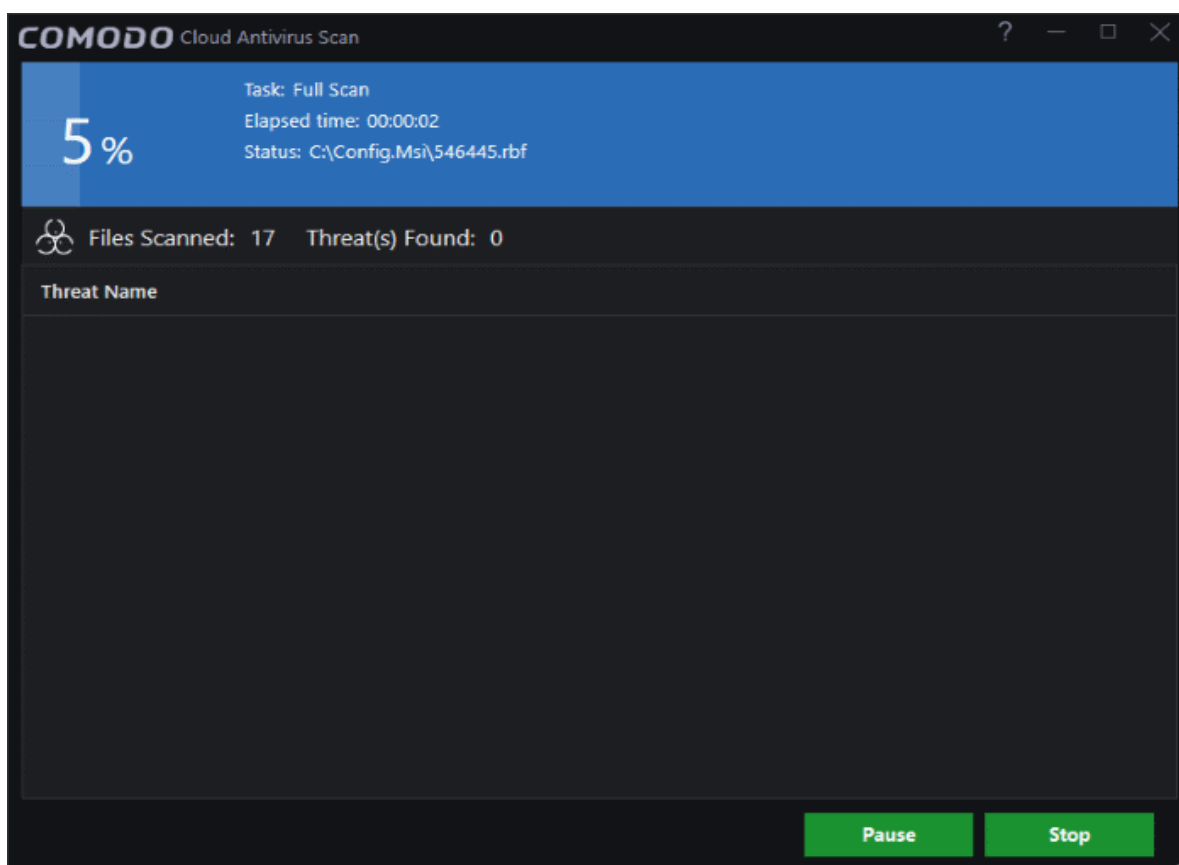
A 'Full System Scan' scans every local drive, folder and file on your system. External devices such as USB drives, storage drives and digital cameras will also be scanned.

### To run a Full Computer Scan

- Click 'Scan' on the CCAV home screen then 'Full Scan'
- OR
- Click the scan button on the widget then 'Full Scan'

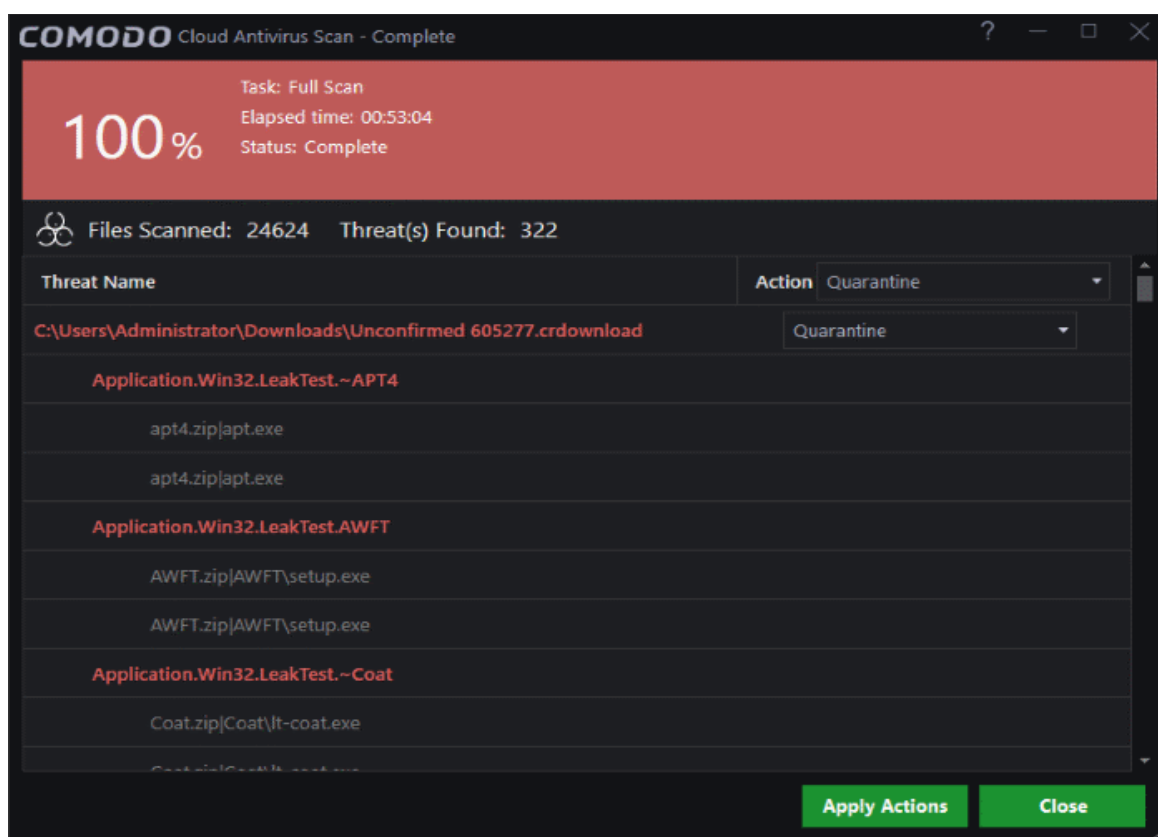


The scanner will start and the scan progress will be displayed:



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

The results window will be displayed when the scan is complete:



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 quarantine files or ignore the threat based in your assessment. Refer to [Processing the infected files](#) for more details.

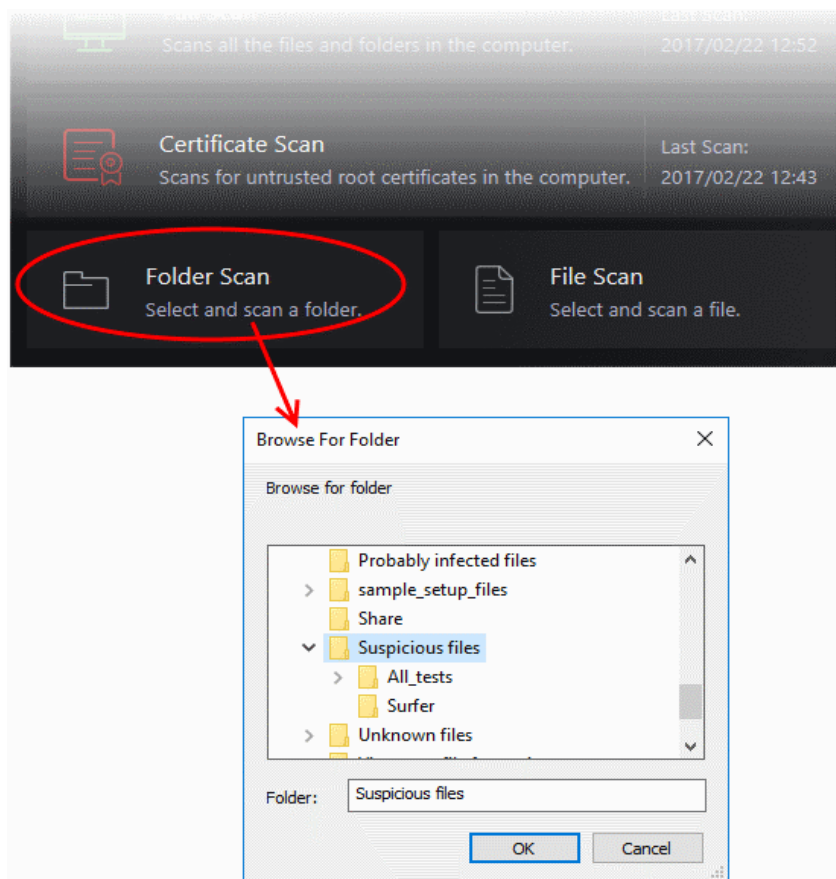
## Custom Scan

There are two types of custom scan:

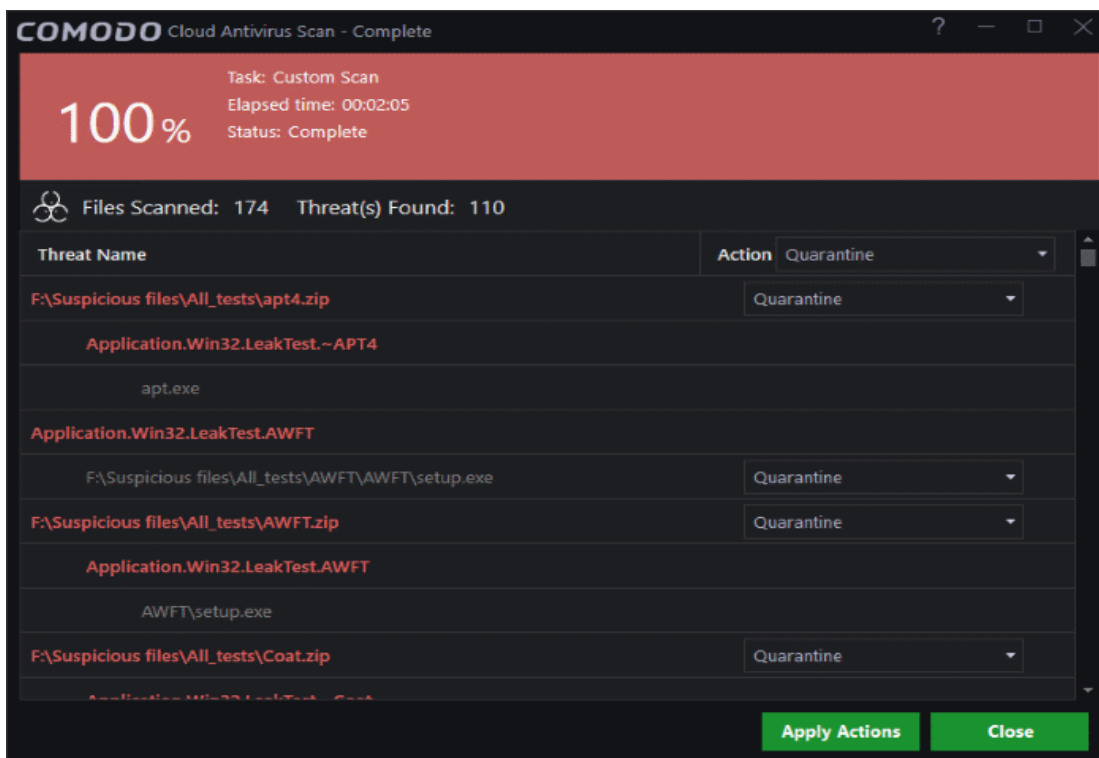
- **Folder Scan** - scan individual folders
- **File Scan** - scan an individual file

### To scan a folder:

- Click 'Scan' in the CCAV home screen OR click the scan button on the widget
- Click 'Folder Scan' from the options
- Browse to the folder you want to scan and click 'OK'



- Alternatively, right-click on a folder and select 'Scan with Comodo Cloud Antivirus' from the context-sensitive menu.
- The folder will be scanned instantly. The results will show any identified infections:



- 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 quarantine files or ignore the threat based in your assessment.

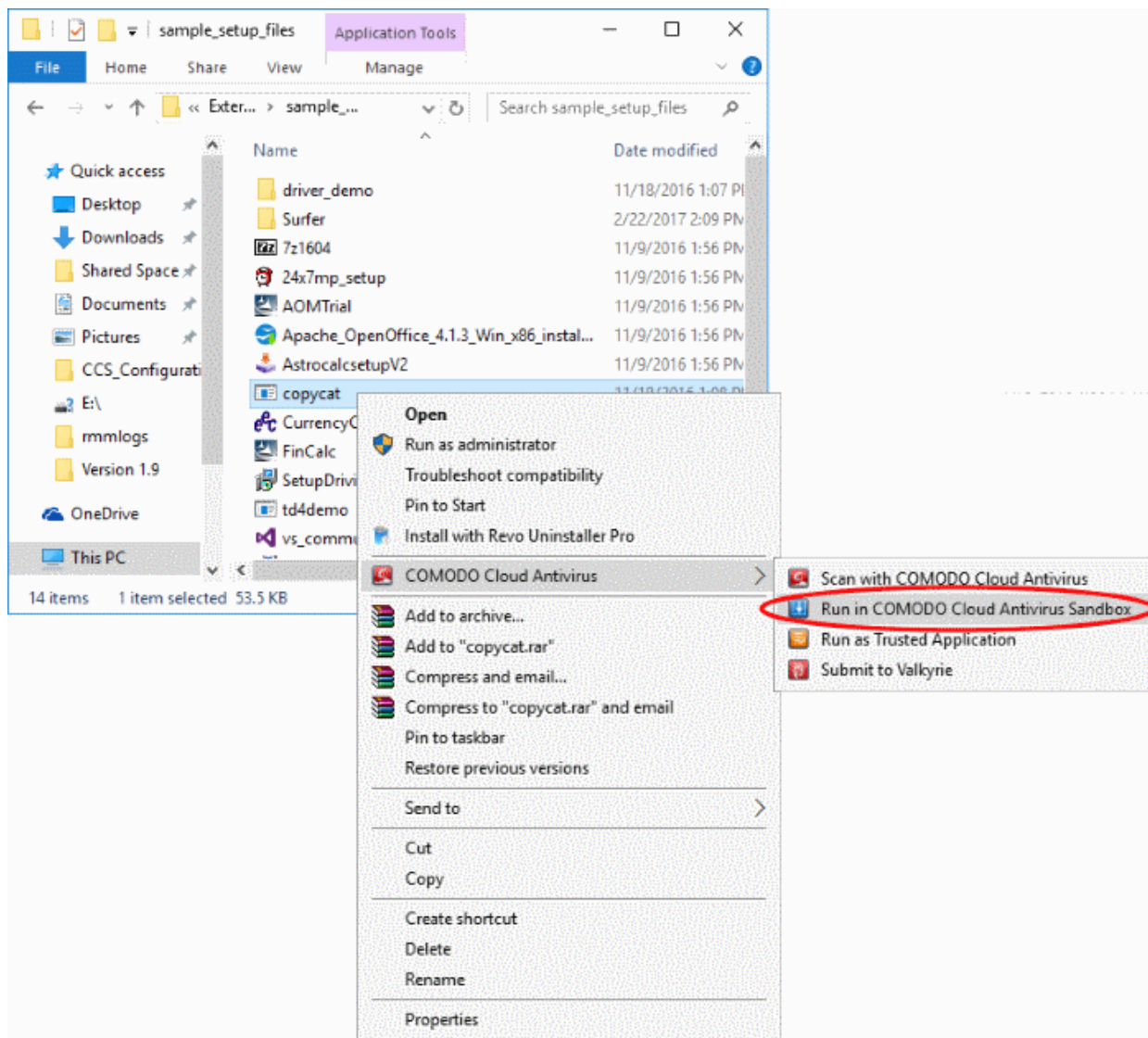
## Run an Application or Browser in the sandbox

You can run browsers or untested applications in the sandbox to prevent them from potentially infecting your PC. Both application types will run as normal in the sandbox, but will not be allowed to access other processes or user data. There are various methods you can use to manually run applications/browsers inside the sandbox:

- **Sandbox an application from the context sensitive menu**
- **Manually add an application to the sandbox**
- **Use the browser shortcuts on the Widget**

**To sandbox an application from context sensitive menu:**

- Locate the file you wish to run in the sandbox
- Right-click on the item and choose 'COMODO Cloud Antivirus' > 'Run in COMODO Cloud Antivirus Sandbox' from the context sensitive menu.

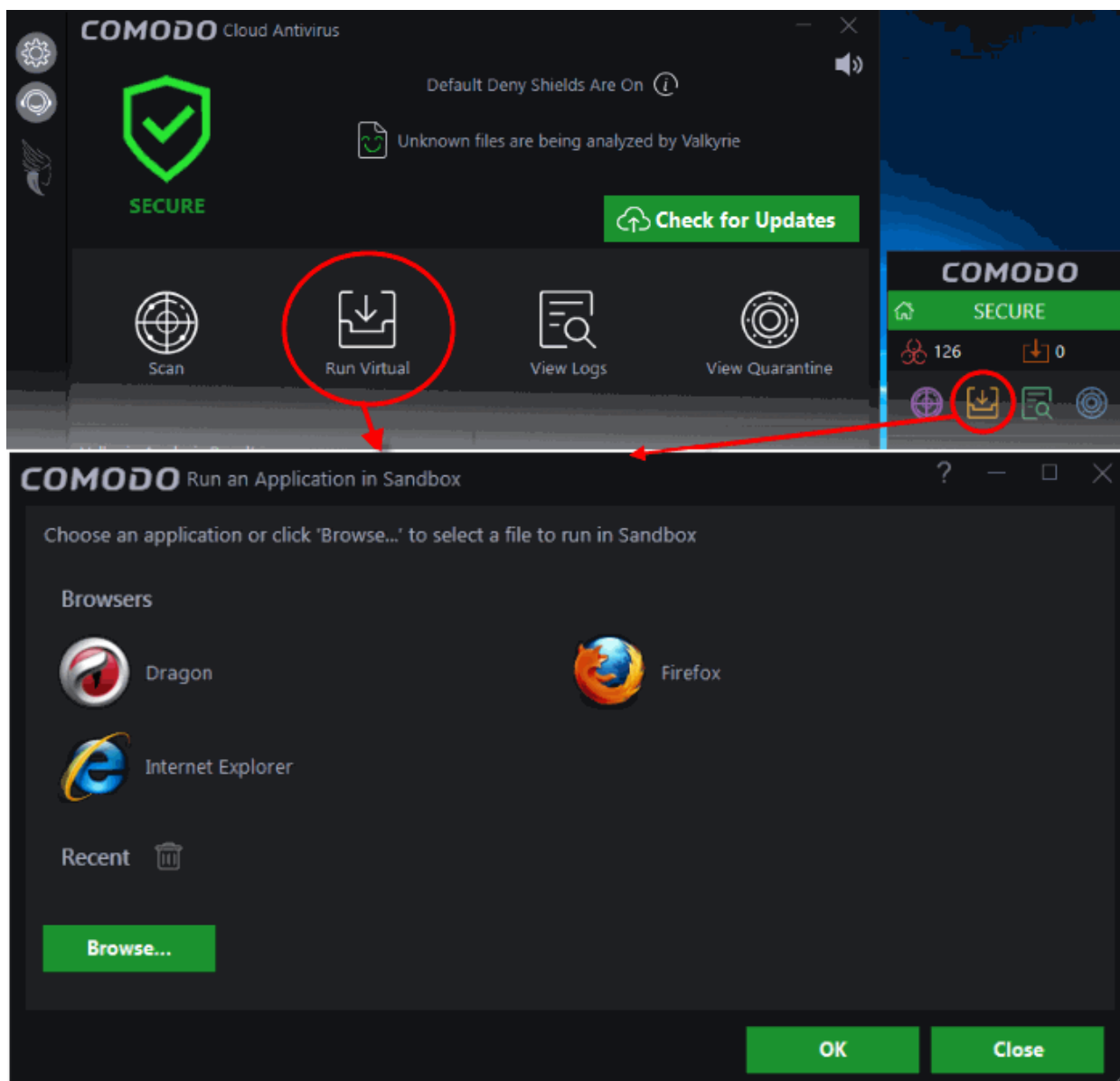


**To add an application to the sandbox:**

- Click 'Run Virtual' button  on the CCAV main interface

OR

- Click the 'Run Virtual' button  on the CCAV desktop widget



The 'Run an Application in Sandbox' interface will open:

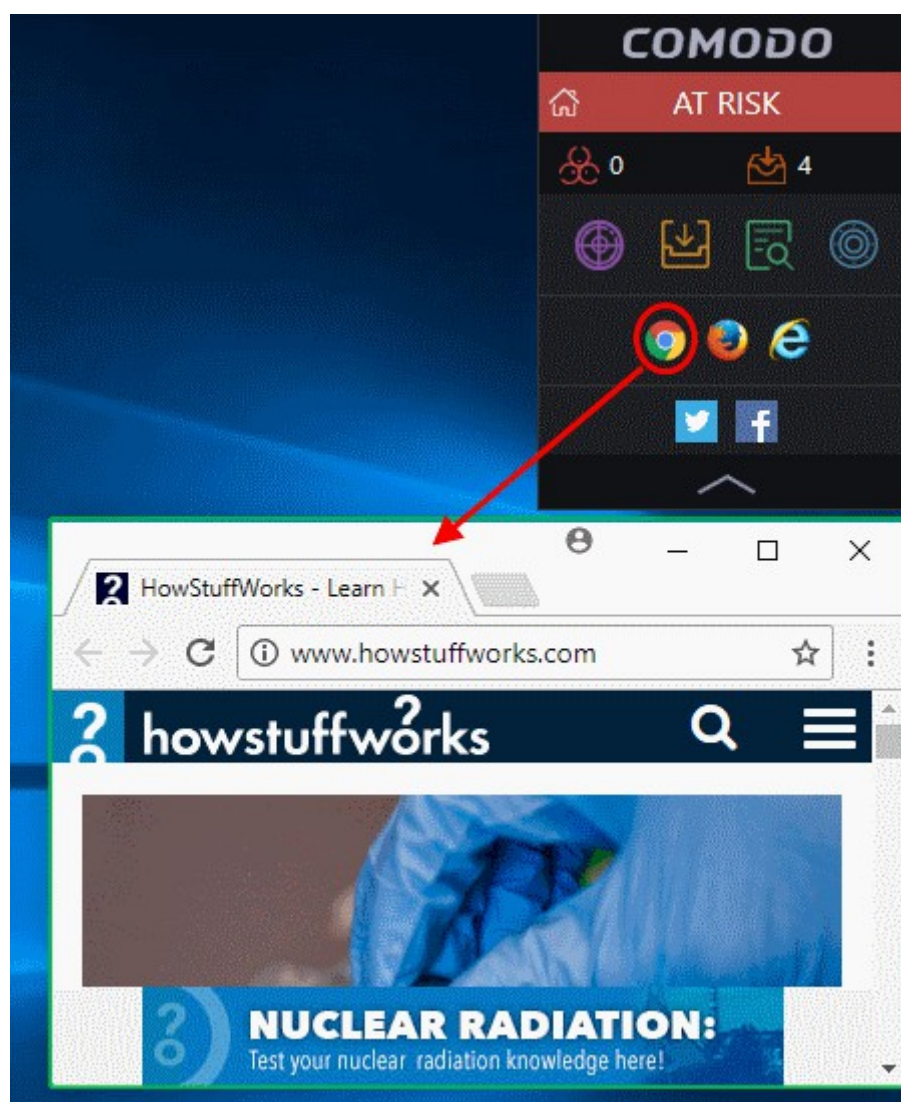
- The interface contains shortcuts to all browsers installed on your computer. Simply click any browser and it will be launched within the sandbox environment

You can run other applications in the sandbox too:

- Click 'Browse' and navigate to the location of the executable you wish to sandbox and click 'Open'
- Click 'OK'

The application will start and run within the sandbox.

You can also launch browsers in the sandbox by clicking the links in the widget:



The browser will be started and executed inside the sandbox at 'Fully Virtualized' level. If 'Show highlight frame for virtualized programs' is enabled in **Sandbox Settings** then CCAV displays a green border around the sandboxed browser.

## Run a Certificate Scan on your computer

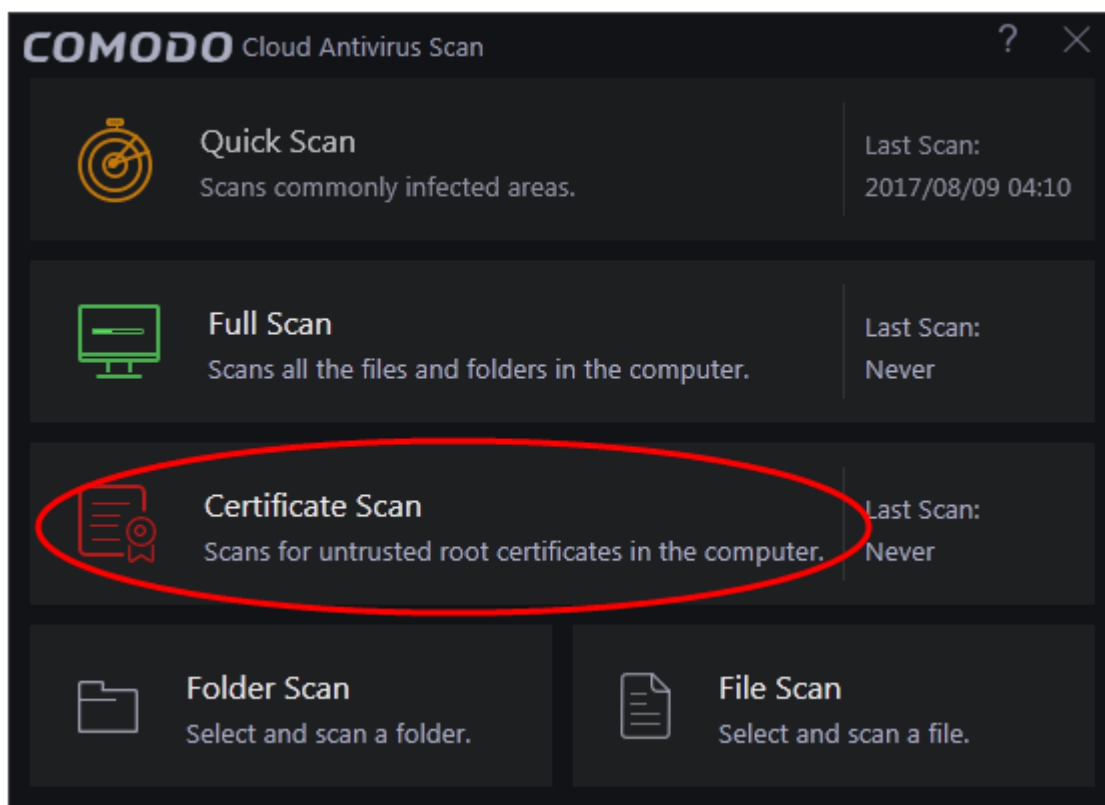
- The 'Certificate Scan' feature examines all root SSL certificates installed on your computer and identifies any untrusted roots.
- Root certificates are used by browsers to validate the websites that you connect to. They are also used by operating systems to check the legitimacy of software that you download.
- For example, when you connect to a secure website, Mozilla Firefox and Google Chrome use these root certificates to check the SSL certificate on the website. If the website certificate is not signed by a trusted root then those browsers will warn you and recommend you do not continue. Similarly, Microsoft Windows uses these root certificates to check that any software you download is legitimate. If the software is not signed by a trusted root then Windows will warn you that you are taking a risk by installing it.
- All root certificates are embedded in what is known as the 'certificate store' in your Windows OS. If a malicious actor managed to get a root in your local certificate store then it could mean your browser and/or

operating system would trust a fraudulent website or a piece of malware.

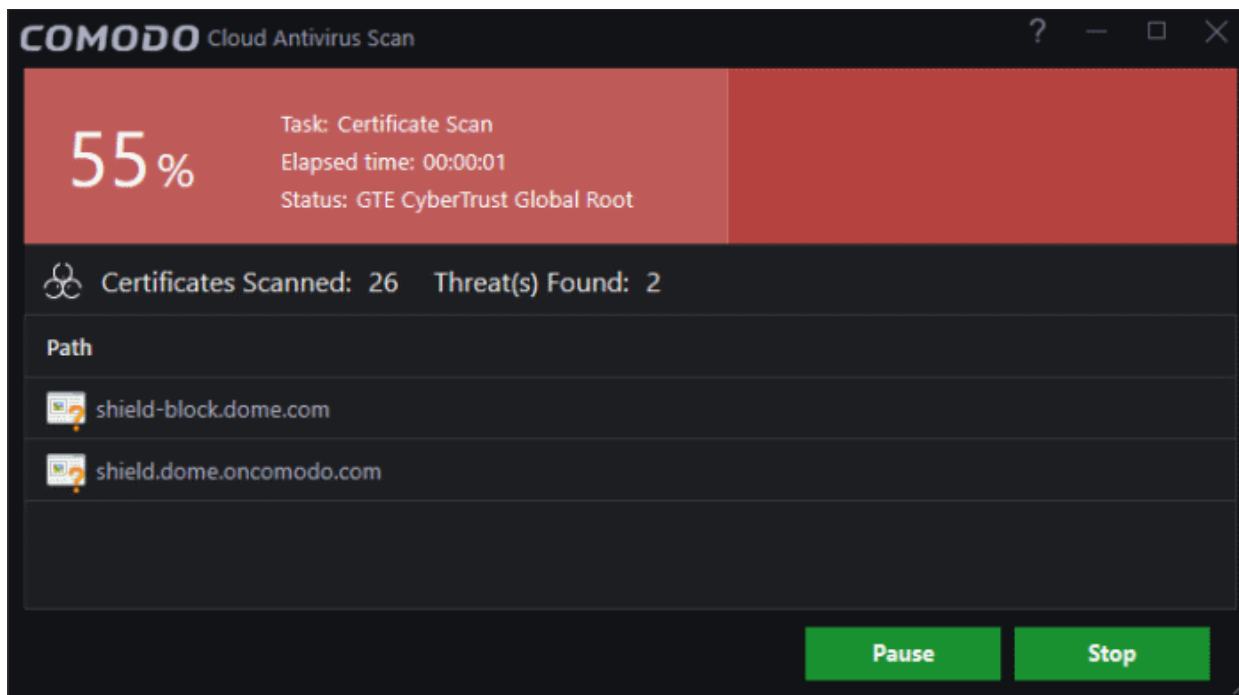
- A certificate scan will find all root certificates that are not part of the major root programs run by browsers and operating systems.

## To run a Certificate scan

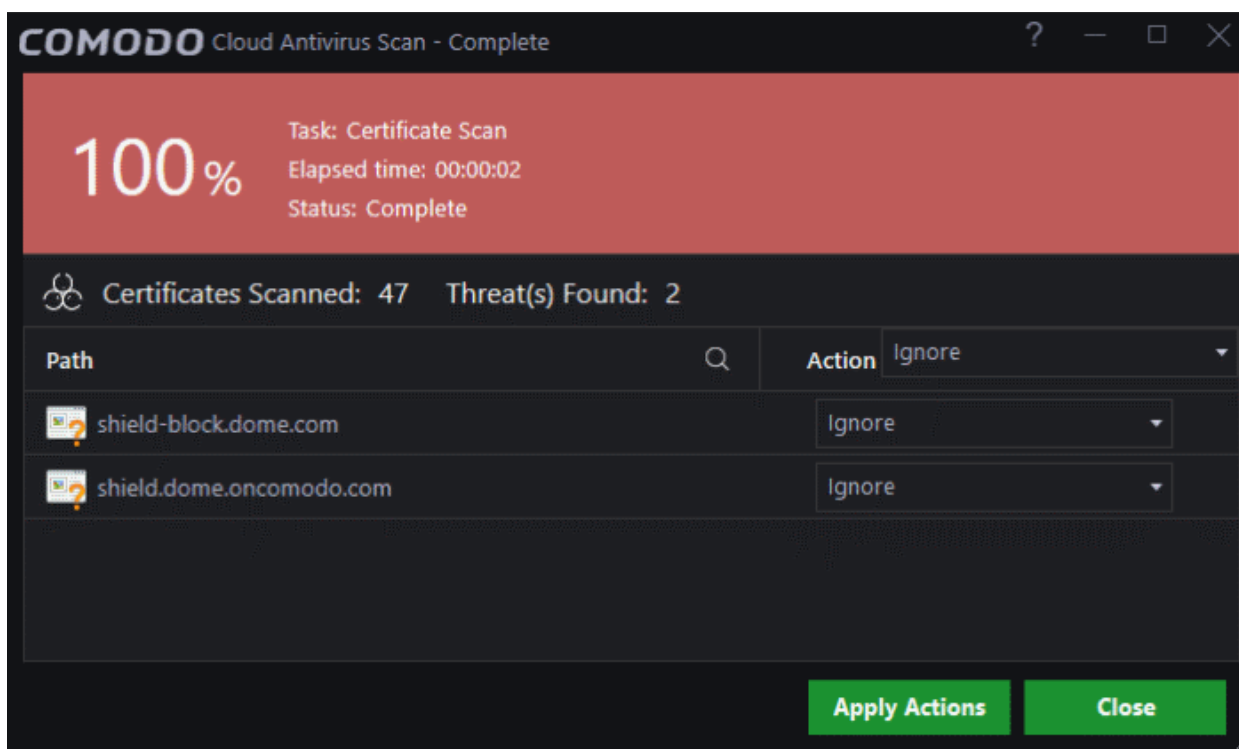
- Click 'Scan' on the CCAV home screen OR click the scan button on the widget
- Click 'Certificate Scan' in the scan options page



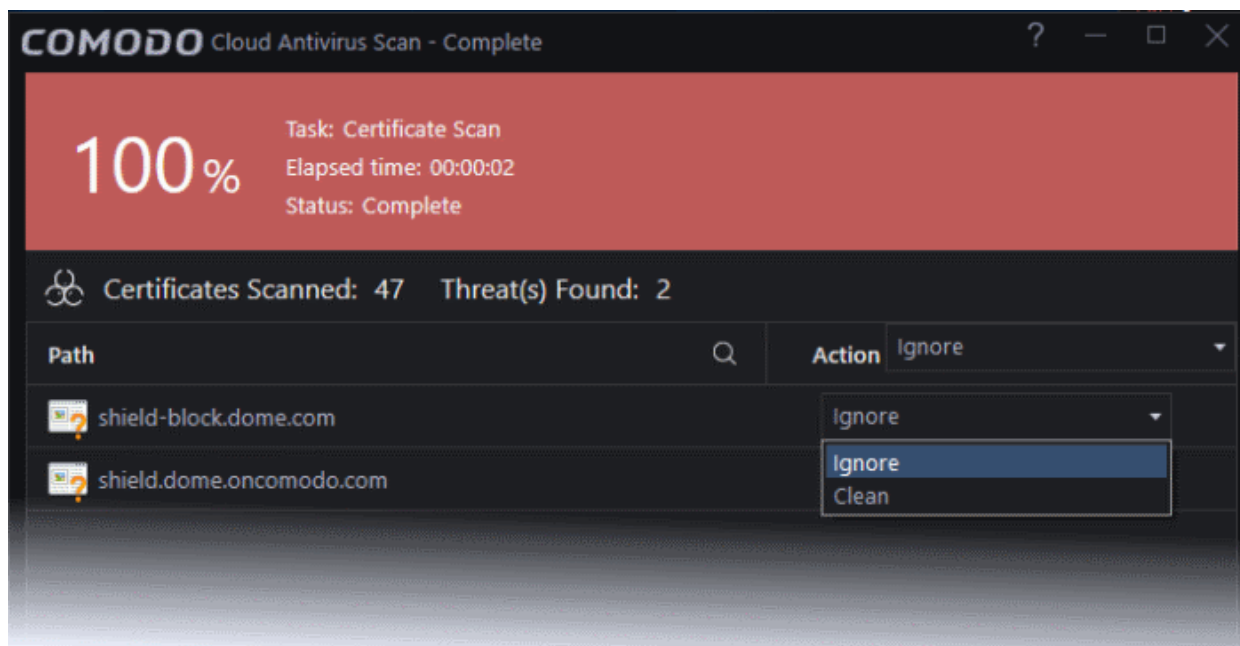
The scan will check roots installed on your PC against the list of trusted store of roots:



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



- The results show the total number of root certificates found on your system, and lists all untrusted certificates.
- You can take the following actions against untrusted certificates:
  - **Ignore** - Will take no action on the certificate. The certificate will be flagged as untrusted by subsequent scans.
  - **Clean** - Delete the certificate.



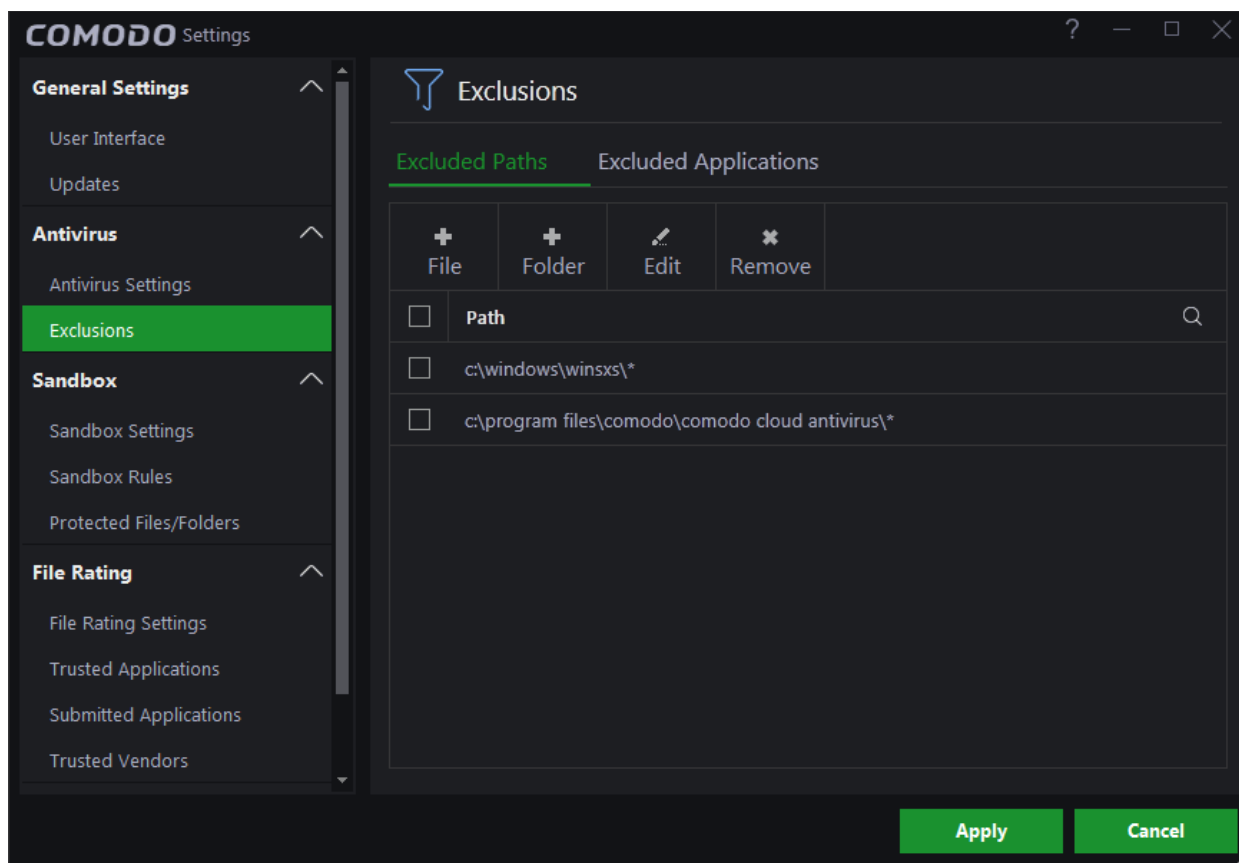
- Click 'Apply Actions' to implement your choices.

## Configure Antivirus Exclusions

- The exclusion section allows you to create a list of files and folders that should be skipped during antivirus scans.
- The section displays all currently excluded items. This includes manually excluded items and items which you chose to ignore at the **Scan Results** window or an **Antivirus Alert**.

### To open the 'Exclusions' interface

- Click the 'Settings' icon on the on the CCAV home screen
- Select 'Antivirus' then 'Exclusions'

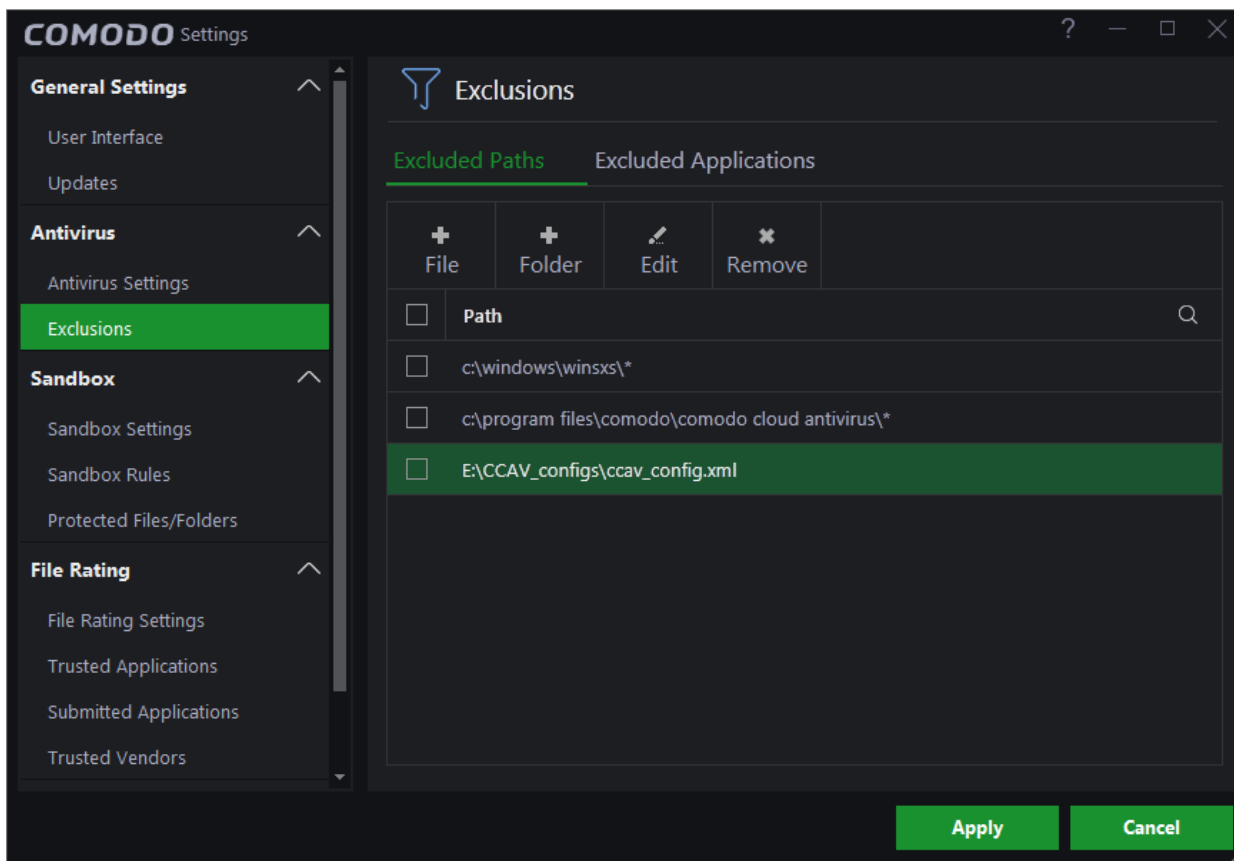


The panel has two tabs:

- **Excluded Paths** - Exclude files or folders from real-time, on-demand and scheduled antivirus scans.
- **Excluded Applications** - Exclude applications from real-time antivirus scans.

Exclude file/folders from virus scans

- Click 'Settings' on the CCAV home screen
- Click 'Antivirus' > 'Exclusions' in the left-hand menu
- Click the 'Excluded Paths' tab
- Click '+ File' to exclude a file, or click '+Folder' to exclude a folder
- Browse to the file or folder you wish to exclude
- Click 'Open'
- The file/folder will be added to the excluded paths list:

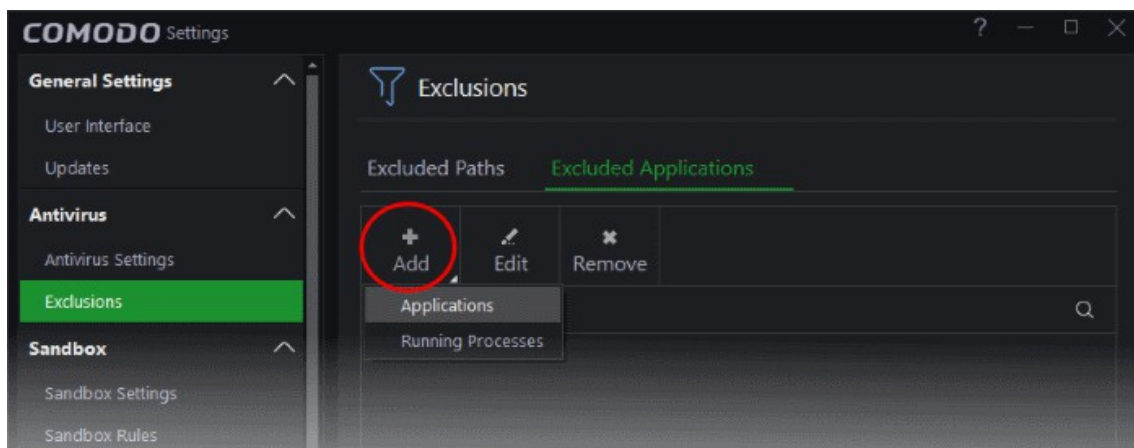


- Repeat the process to add more files/folders
- Click 'Apply' for your settings to take effect. Items added to 'Excluded Paths' will be omitted from all types of virus scan in future.
- Use the 'Edit' and 'Remove' buttons to modify/delete items as required.

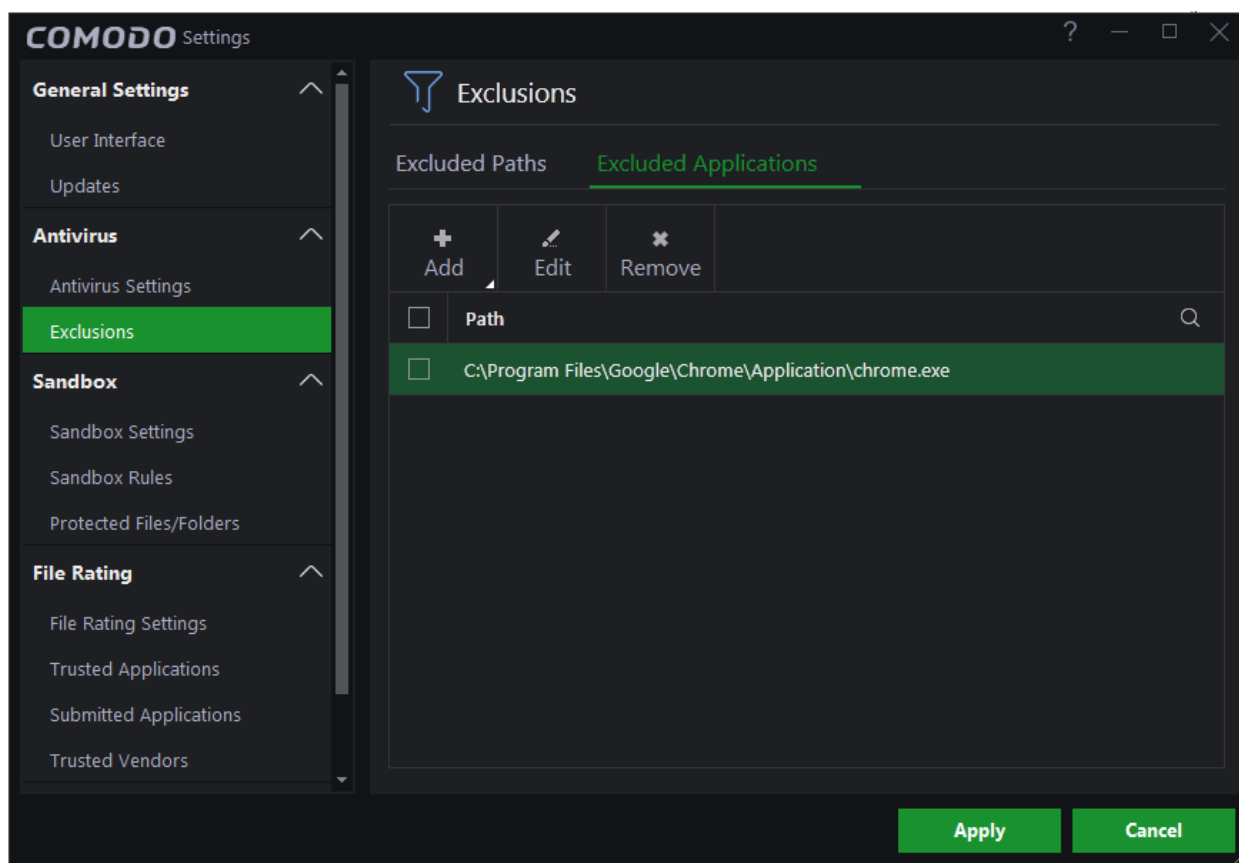
## Exclude Programs/Applications from Real-time Scans

- Click 'Settings' on the CCAV home screen
- Click 'Antivirus' > 'Exclusions' in the left-hand menu
- Click the 'Excluded Applications' tab
- Click the 'Add' button:
  - Select 'Applications' to browse your hard drive for a specific application you want to excludeOR
  - Select 'Running Processes' to exclude an application that is currently running on your computer





- Select the application you wish to exclude
- Click 'Open'
- The application will be added to the excluded paths list:



- Repeat the process to add more applications
- Click 'Apply' for your settings to take effect. Applications added to 'Excluded Applications' will be omitted from all types of virus scan in future
- Use the 'Edit' and 'Remove' buttons to modify/delete items as required

## View lucky you statistics

- The 'Lucky You' interface shows statistics on brand new malware that was found on your system. These are files that were identified as malicious by Comodo before any other antivirus company detected them as such.
- Each file in this interface started life as an 'Unknown' file. This means it was neither definitely safe nor definitely malware. In this circumstance, Comodo Cloud Antivirus locks the file in an secure environment called the container where it can do no harm. Meanwhile, our Valkyrie system rigorously tests the file in the cloud to evaluate its behavior.
- If the Valkyrie tests show the file is malicious, it is immediately quarantined/deleted and the file is added to the 'Lucky You' statistics. You are 'Lucky' because traditional AV solutions would have allowed these 'Unknown' files to run freely on your computer.
- You can also set your previous antivirus vendor so you can see how many threats were caught by CCAV that would previously have been missed.

To view your 'Valkyrie Lucky You Statistics':

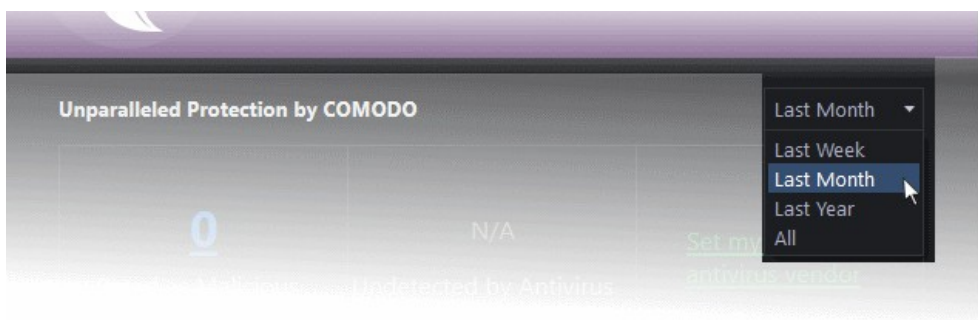
- Click the 'Lucky You' icon at the top-left of the CCAV interface:



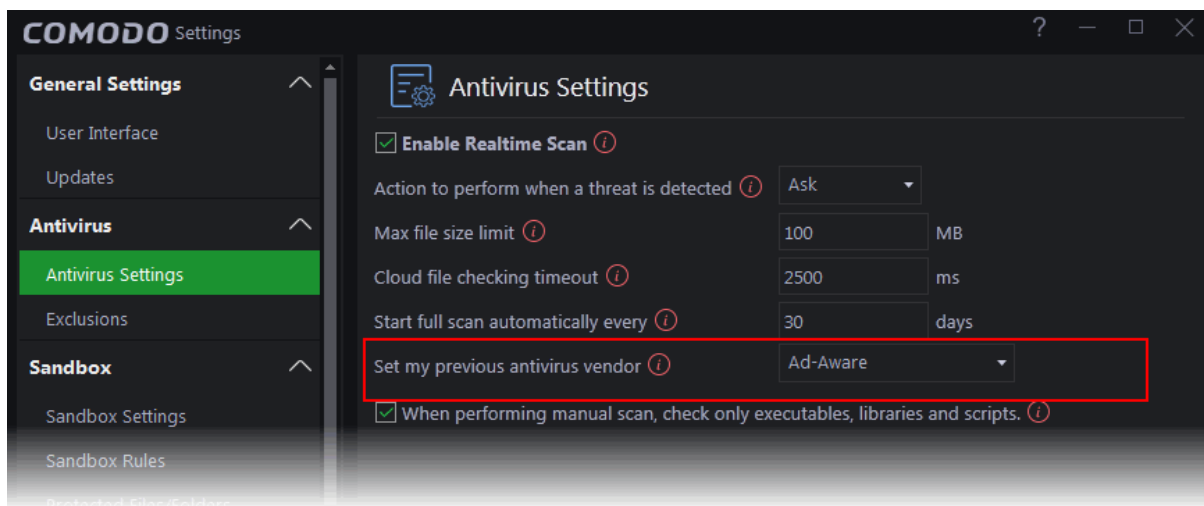
- The 'Lucky You' page shows the number of brand new threats identified on your system by Comodo's Valkyrie system.
- The 'Undetected by' stats show how many of these threats would have been missed by other antivirus software vendors.
- Click the numbers themselves to view a list of the actual files discovered:



- You can change the time-period shown using the drop-down on the right:




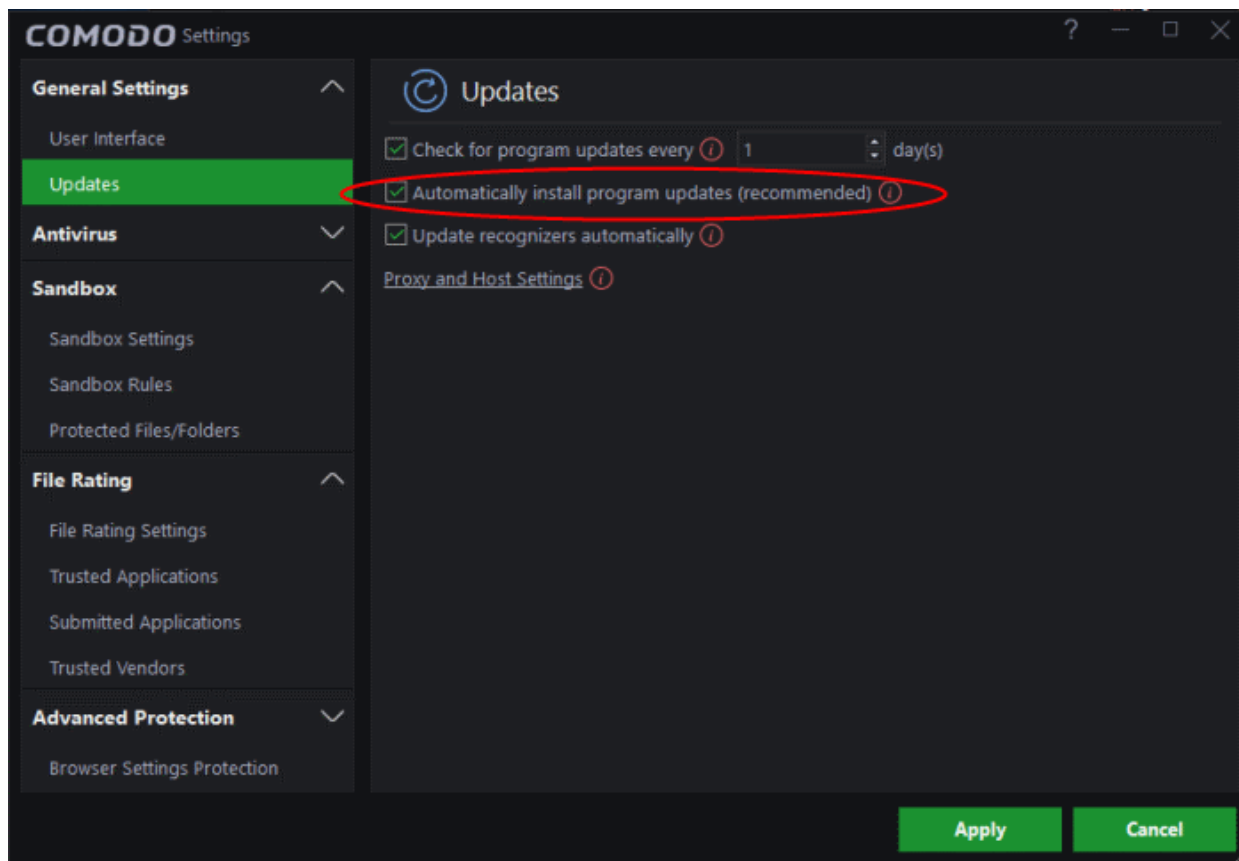
- You can choose your previous antivirus vendor as follows:
  - Click 'Settings' on the CCAV home screen
  - Click 'Antivirus' > 'Antivirus Settings'
  - Choose your previous vendor from the 'Set my previous security vendor' drop-down.



## Switch Off Automatic Antivirus and Software Updates

To switch off Automatic antivirus and software updates:


- Click the 'Settings' icon  on the home screen
- OR
- Right-click on the system tray icon and select 'Antivirus settings'
- Click 'Updates' option in the left-hand menu:

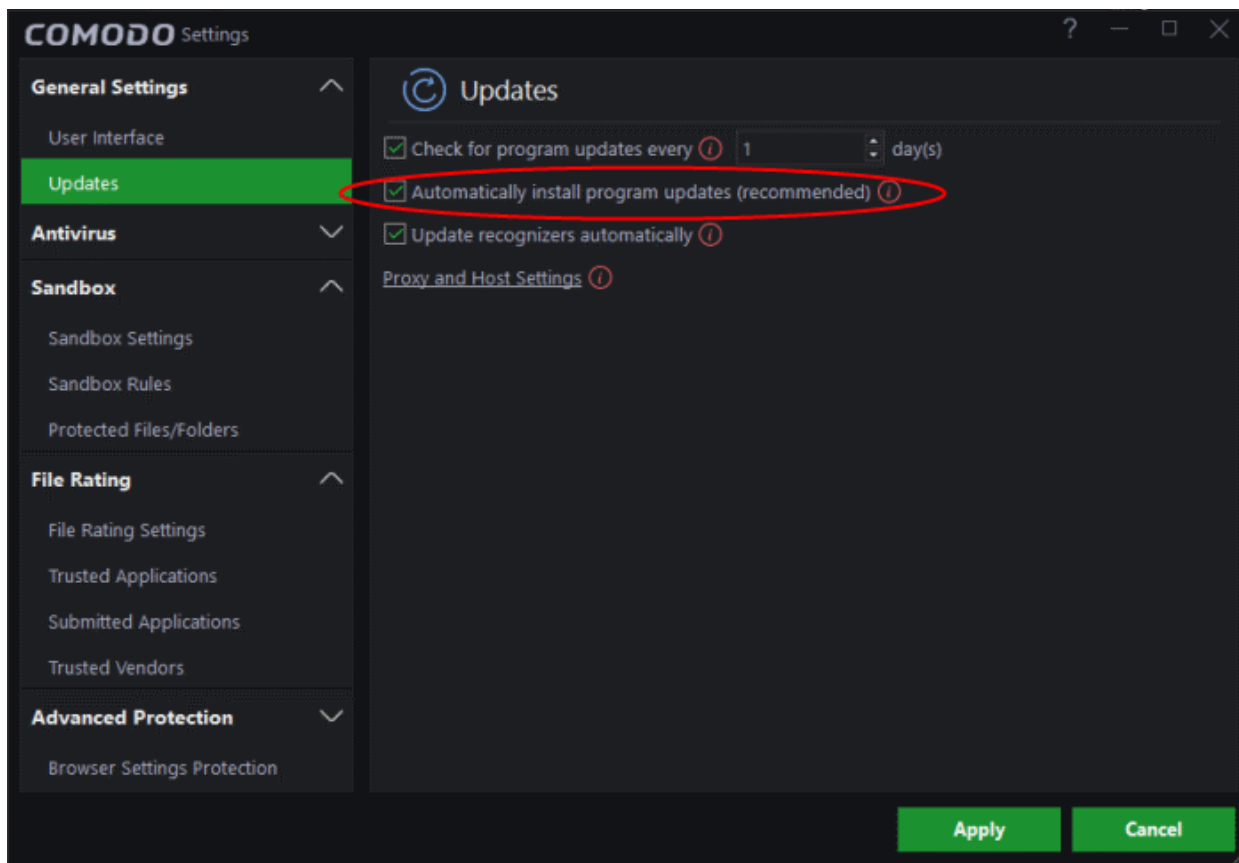


- Deselect “Automatically install program updates (recommended)” to disable updates
- Please note this option is enabled by default as we recommend auto-updates are left enabled.

## Switch Off Automatic Antivirus and Software Updates

To switch off Automatic antivirus and software updates:

- Click the 'Settings' icon  on the home screen
- OR
- Right-click on the system tray icon and select 'Antivirus settings'
- Click 'Updates' option in the left-hand menu:




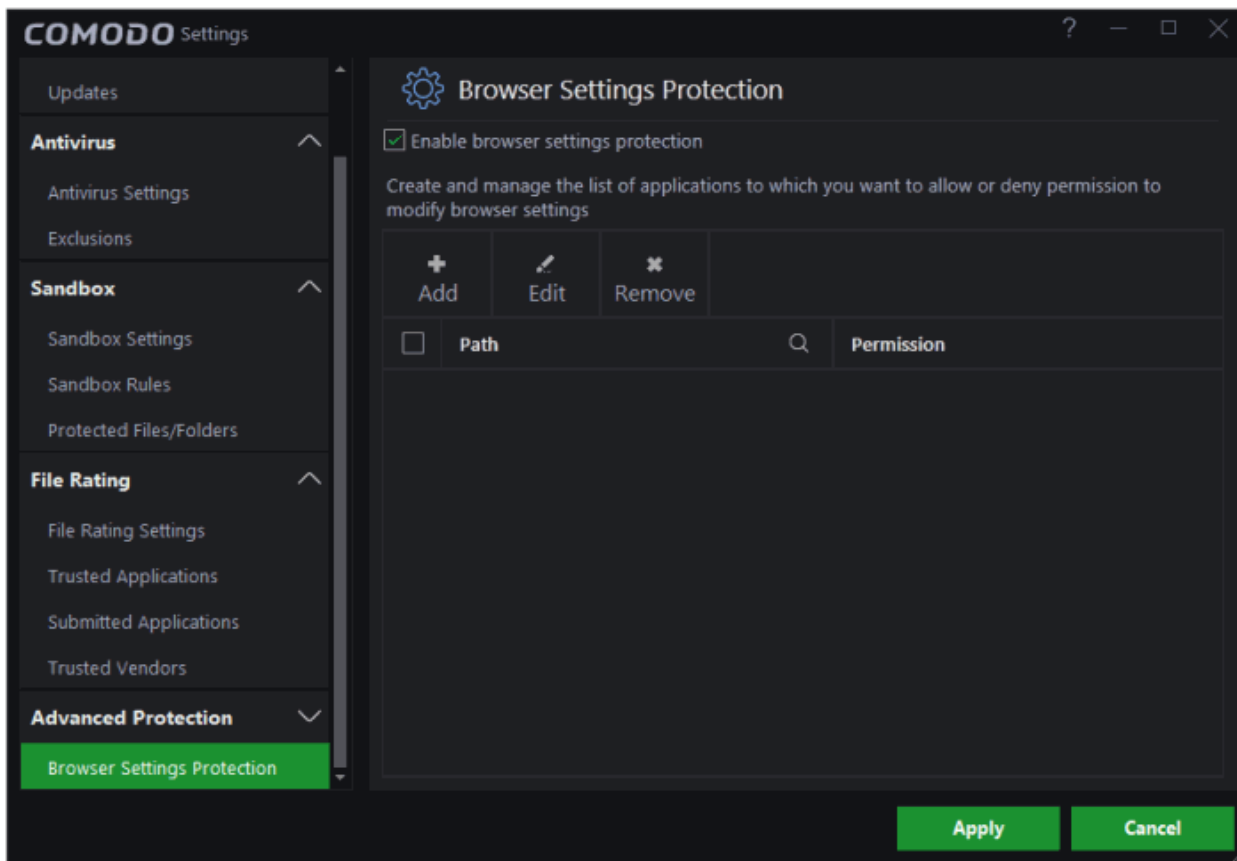
- Deselect “Automatically install program updates (recommended)” to disable updates
- Please note this option is enabled by default as we recommend auto-updates are left enabled.

## Enable/ Disable browser settings protection

By protecting your 'Browser settings' you can avoid third party applications from making changes to your browser settings.

### To Enable / Disable the 'Browser Settings Protection' interface

- Click the 'Settings' icon  at the top left of the CCAV home screen to open the 'Settings' interface
- Choose 'Browser Settings Protection' under 'Advanced Protection' on the left menu

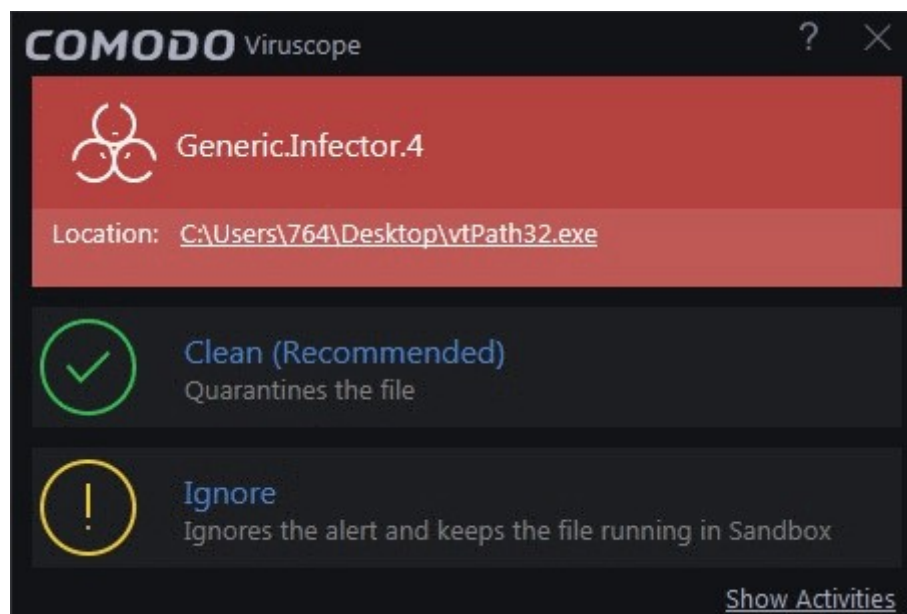


- **Enable browser settings protection** - Switch browser protection on or off.
  - If deselected, any protection that you have created will be disregarded.
  - If the protection is switched on, the blocked apps will be automatically added to the list.

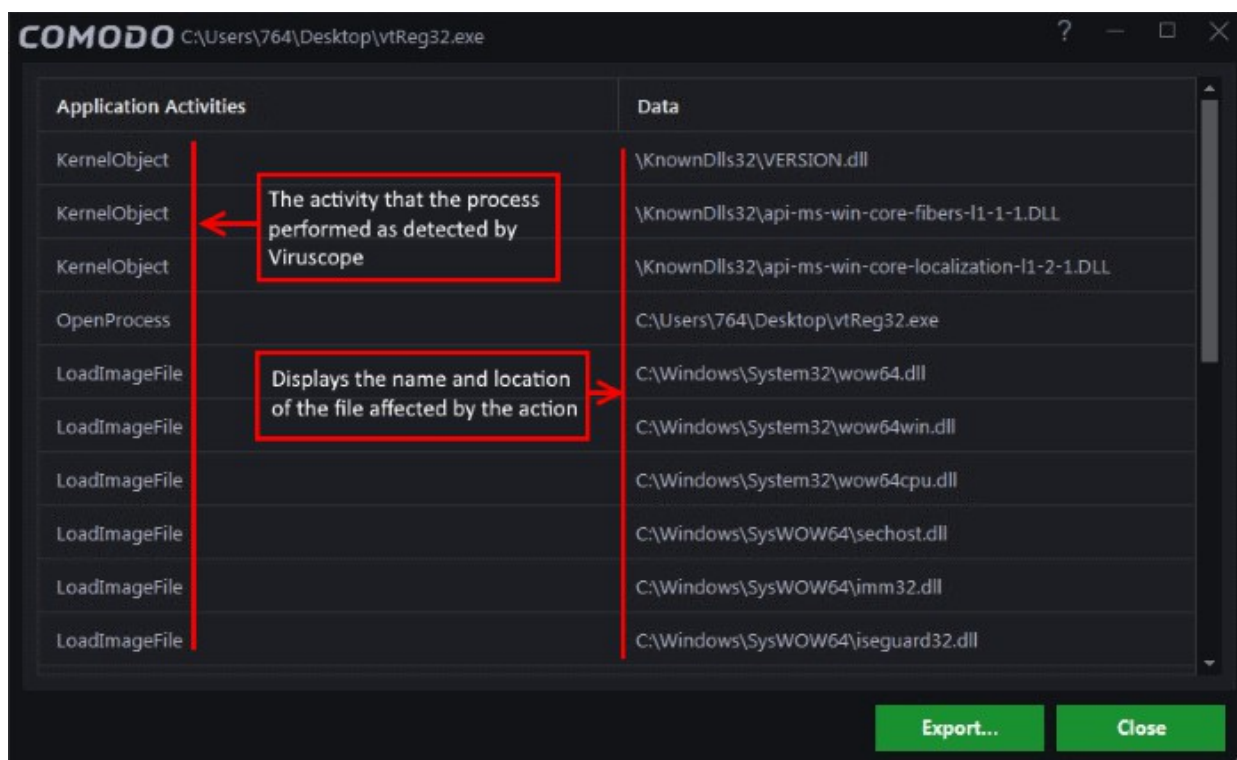
## Evaluate the behavior of unknown files in the sandbox

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

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



- If you are not sure about the parent application shown 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'.
- Click 'Show Activities' at the bottom right of the alert to view a detailed breakdown of its actions:



Viruscope identifies zero-day malware by using a sophisticated set of behavior 'Recognizers', each of which can detect actions typical of a malicious application.

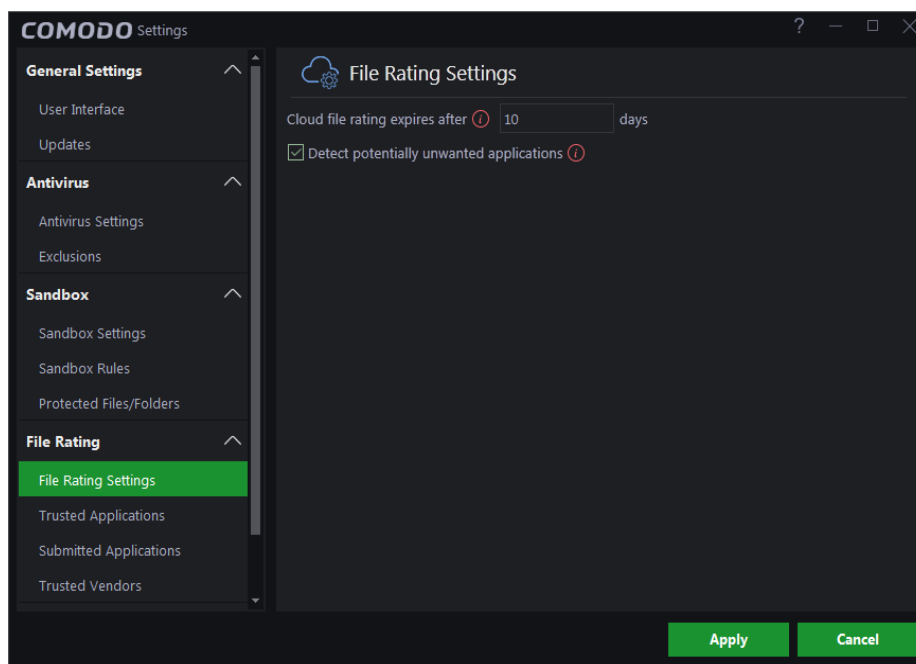
## Detect Potentially Unwanted Applications (PUA)

- A PUA is software that, while not explicitly malicious, may contain functionality that has not been made clear


to the user.

- An example would be a browser toolbar which ostensibly provides weather updates, but also tracks the user's online activity.
- Unlike malware, PUAs are usually installed with the users permission and often have their own EULA. Other example PUA's include adware, grayware and spyware.

You will receive an alert when a potentially unwanted application is detected by CCAV. This option is enabled by default in 'File Rating' settings. Unlike malware, many PUA's are 'legitimate' pieces of software with their own EULA agreements. However, the 'true' functionality of the software might not have been made clear to the end-user at the time of installation. For example, a browser toolbar may also contain code that tracks a user's activity on the Internet. By default PUA detection is enabled for improved protection.



To view settings for PUA detection:

- Click the 'Settings' icon  at the top left of the CCAV home screen to open the 'Settings' interface
- Click File Rating > 'File Rating Settings' to open the file rating interface
- Deselect the 'Detect potentially unwanted applications' option if you do not want PUAs to be identified

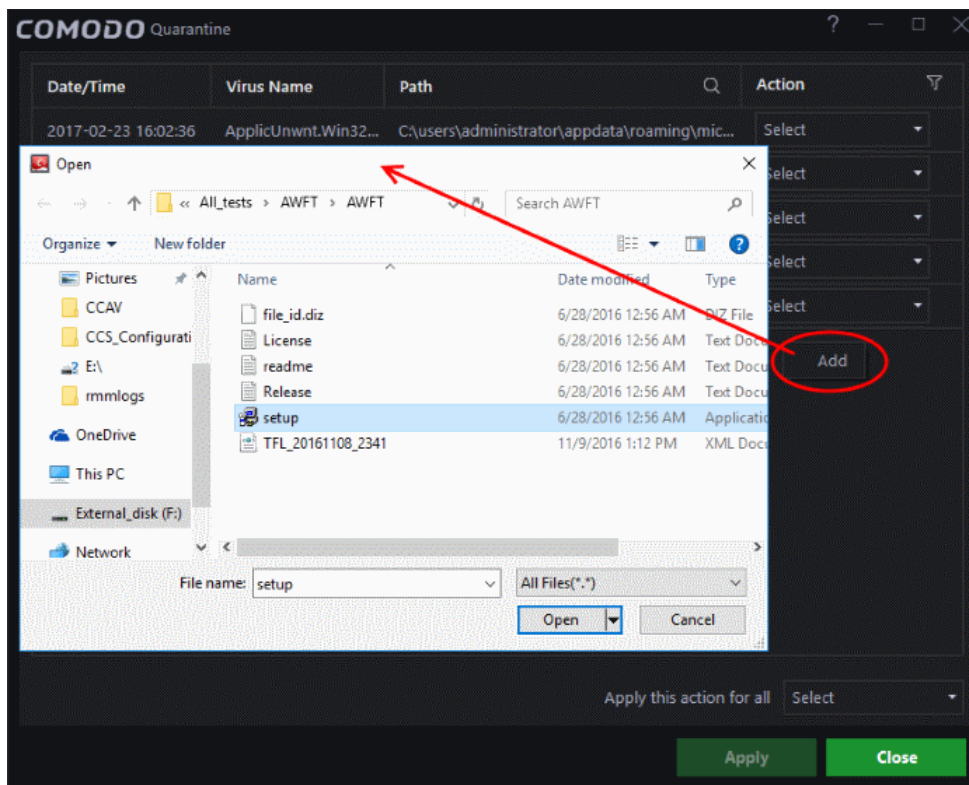
## Manually add items to quarantine

You can manually quarantine the files or folders that you feel are suspicious in nature.

To do this:

- Click anywhere on the quarantined interface and choose 'Add'

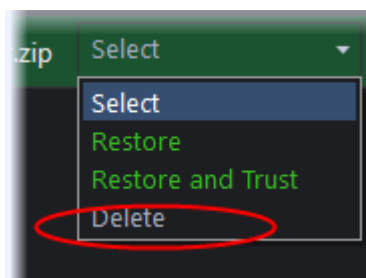




- Select the file you wish to quarantine and click 'Open'
- Click 'Apply' to quarantine the chosen file

## Delete quarantined items

- To delete a single file / folder, choose 'Delete' from the drop-down beside

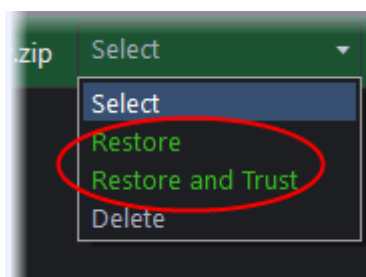


- To delete all the quarantined items at the same time, select 'Delete' from the bottom left menu
- Click 'Apply' to save your changes.

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

## Restore a quarantined item

- To restore a single file / folder, choose 'Restore' from the 'Action' drop-down menu 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 at once and exclude from future scans, click 'Restore and Trust' from the 'Action drop-down in the item row.

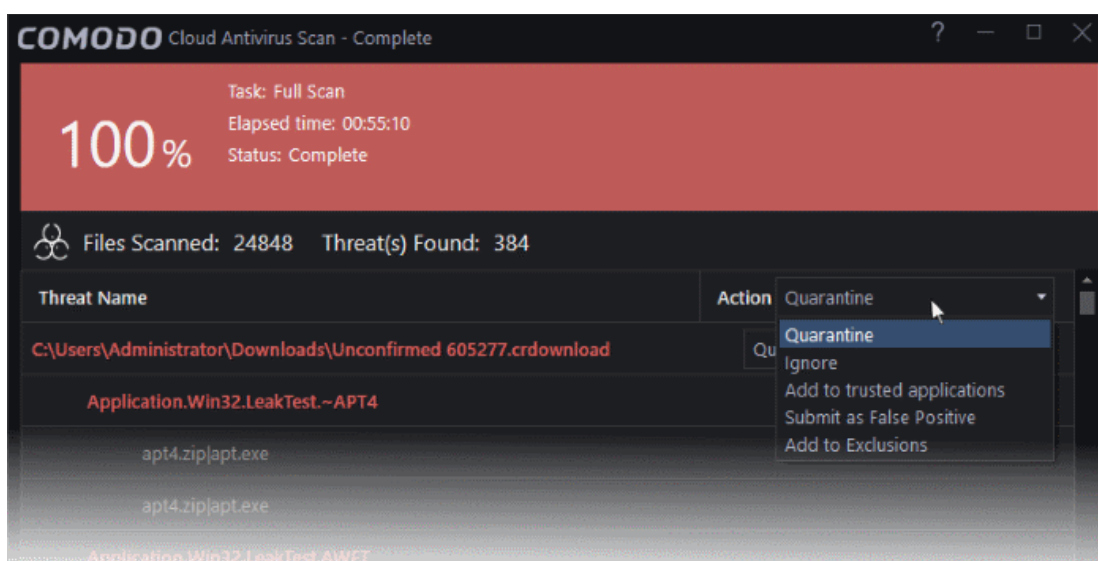


- To restore a single item and exclude it from the future scans, choose 'Restore' and Trust' from the 'Apply this action to all' drop down menu in the item row.
- Click 'Apply' to save your changes

Any restored files will be moved back to their original locations

## Submit as False Positive

'Submit as False Positive' is an option present in the CCAV scan results. If you feel that a file identified as malware is safe, you can choose the Submit to False Positive option provided by CCAV. The file will be sent to Comodo for analysis. If the file is trustworthy it will be added to the Comodo safe list.



- To submit as False Positive follow the below procedure:
- 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 the file as a false positive.
- Choose 'Submit as False Positive' option from the 'Action' drop-down at top right, to move the file as safe list.

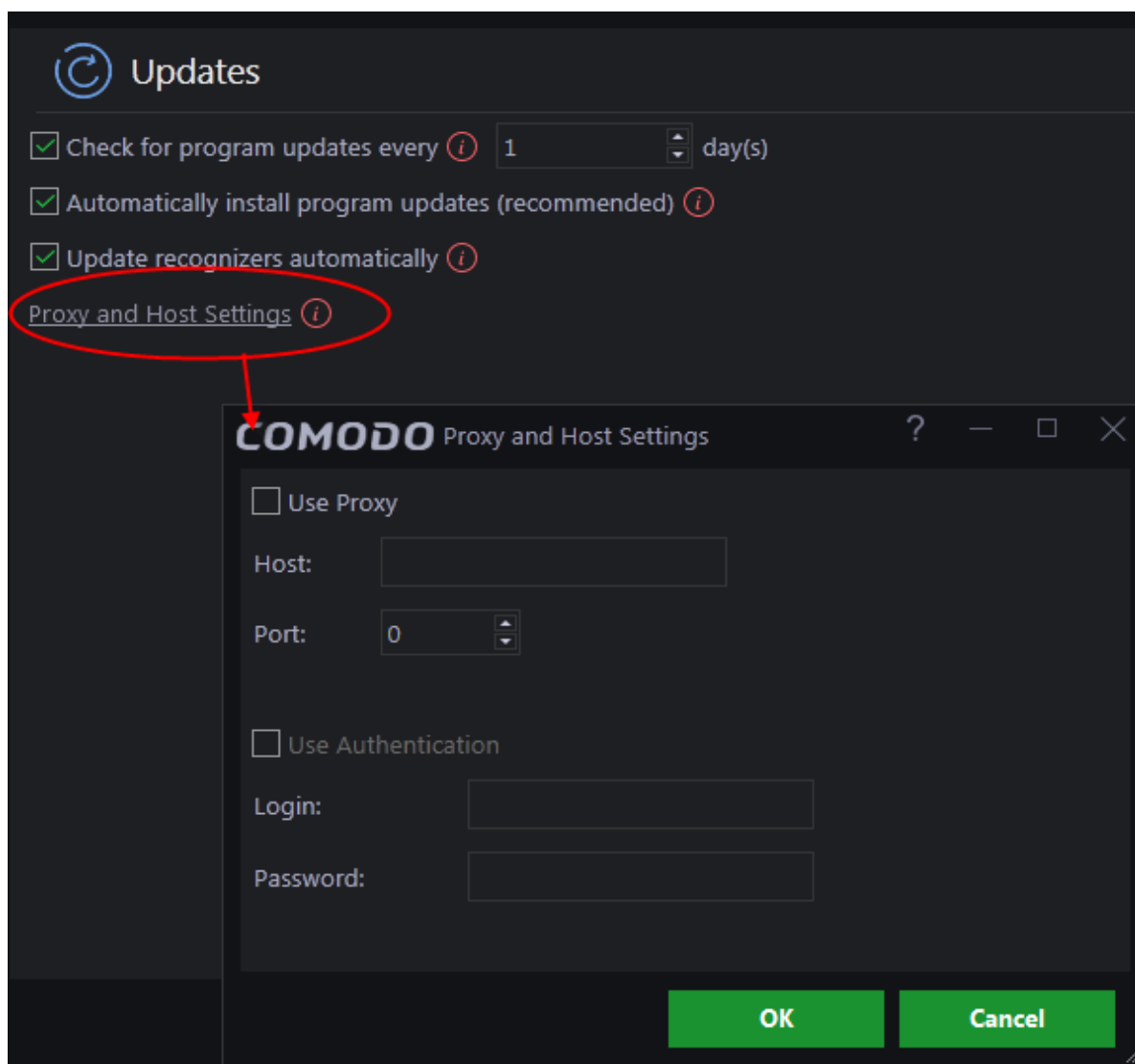
## Configure Proxy and Host Settings

- Advanced users and system administrators may wish to first download updates to an intermediary server and have individual CCAV installation establishments gather their updates from that server.
- This helps to conserve bandwidth and accelerate the update process when a large number of endpoints are involved. By default, CCAV downloads updates from Comodo proxy servers.

You can choose the host from where updates are downloaded through the 'Proxy and Host Settings' interface

## To configure updates via proxy server

- Click 'Proxy and Host Settings' link. The 'Proxy and Host Settings' interface will open:



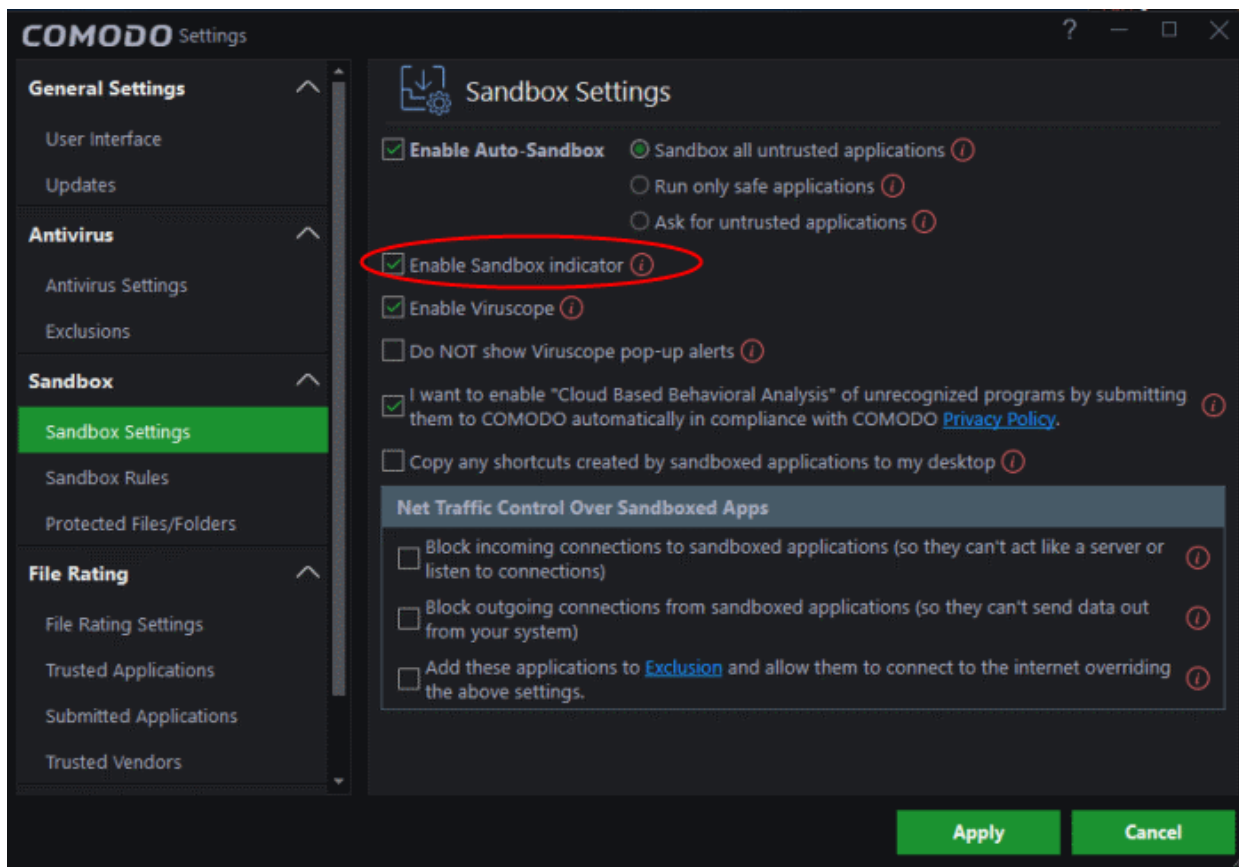
- Enable the 'Use Proxy' check-box.
- Enter the host name and port numbers. If the proxy server requires access credentials, select the 'Use Authentication' check-box and enter the login / password accordingly.
- Click 'OK' to save your settings
- Click 'Apply' for your changes to take effect.

## Enable/ Disable Sandbox indicator

By default, CCAV will display a green border around an application in the event that it is running in the sandbox. You can enable/disable this border as follows:

- Click the 'Settings' icon on the home screen then 'Sandbox' > 'Sandbox Settings'
- OR

- Click the 'Sandbox' link under 'Realtime Protection' on the home screen  
OR
- Right-click on the CCAV tray icon and choose 'Sandbox Settings' from the options.



The sandbox settings interface will open:

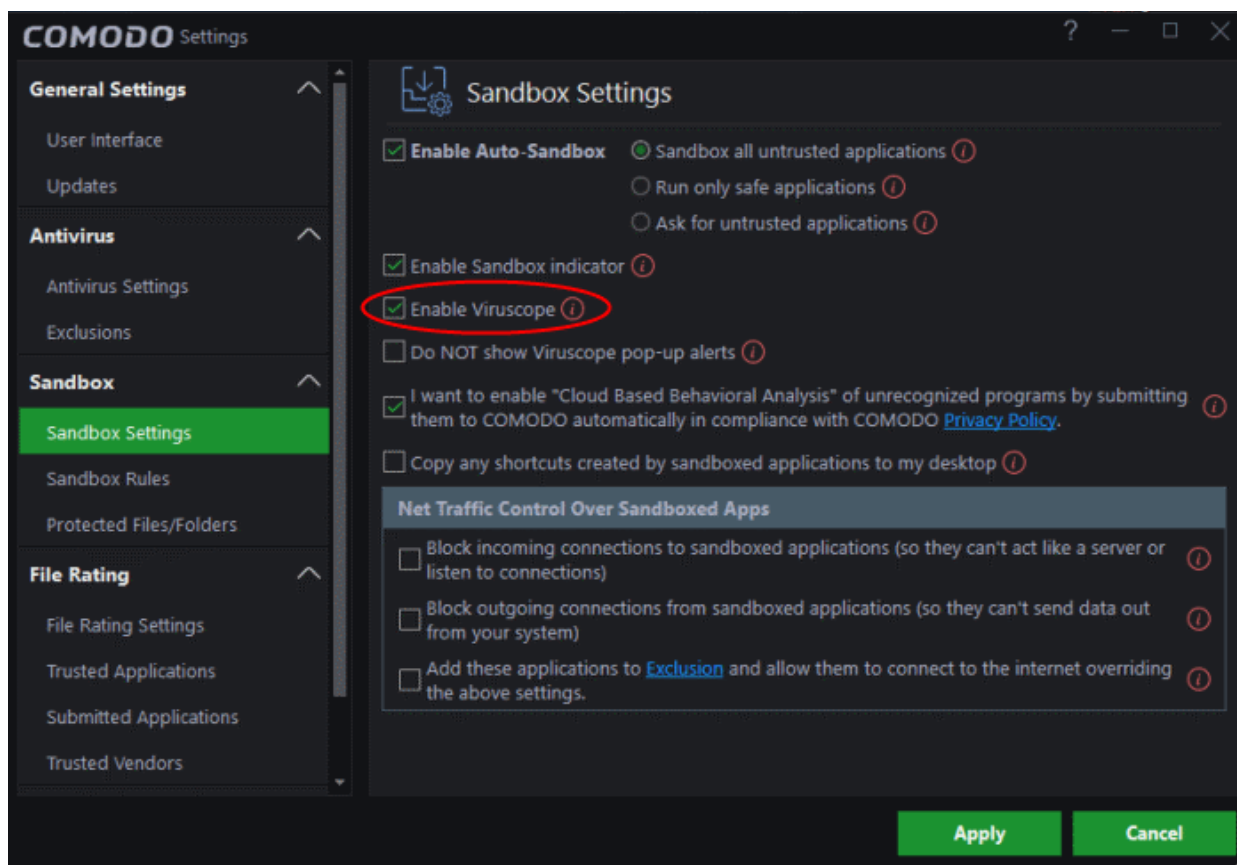
- Deselect 'Enable Sandbox indicator' to remove the green border. You can re-enable the border at any time by returning to this section.

## Enable / Disable viruscope

Viruscope monitors the activities of sandboxed processes and alerts you if they take actions that could potentially threaten your privacy. Viruscope is enabled by default to ensure your computer enjoys the highest levels of protection.

### To enable / disable viruscope

- Click the 'Settings' icon on the home screen then 'Sandbox' > 'Sandbox Settings'  
OR
- Click the 'Sandbox' link under 'Realtime Protection' on the home screen
- Enable or disable the 'Enable Viruscope' option as required:



## Respond to alerts

Comodo Cloud Antivirus alerts provide warnings about security threats. You should understand how to respond to these alerts to ensure the safety of your computer.

There are different categories of alerts:

- **Antivirus alerts**
- **Sandbox alerts**
- **Viruscope alerts**
- **Valkyrie alerts**
- **Browser Protection alerts**
- **Crash Reporting alerts**
- **PUA Detection alerts**

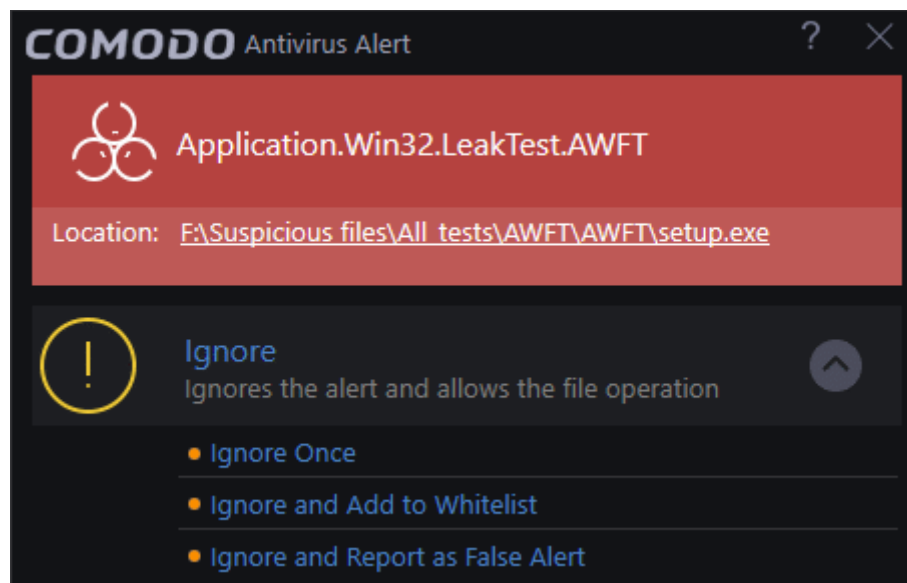
### Antivirus alerts:

The AV alert will be shown when your computer encounters malware. The alert message contains the name of the virus detected and the location of the file or application infected.

**Note:** Realtime scanning must be enabled to activate this type of alert (highly recommended)

When you receive an AV alert, the following 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.
- **Ignore** - Allows the process to run and does not attempt to clean the file or move it to quarantine. Click 'Ignore', only if you are sure the file is safe. Clicking 'Ignore' will open three further options:



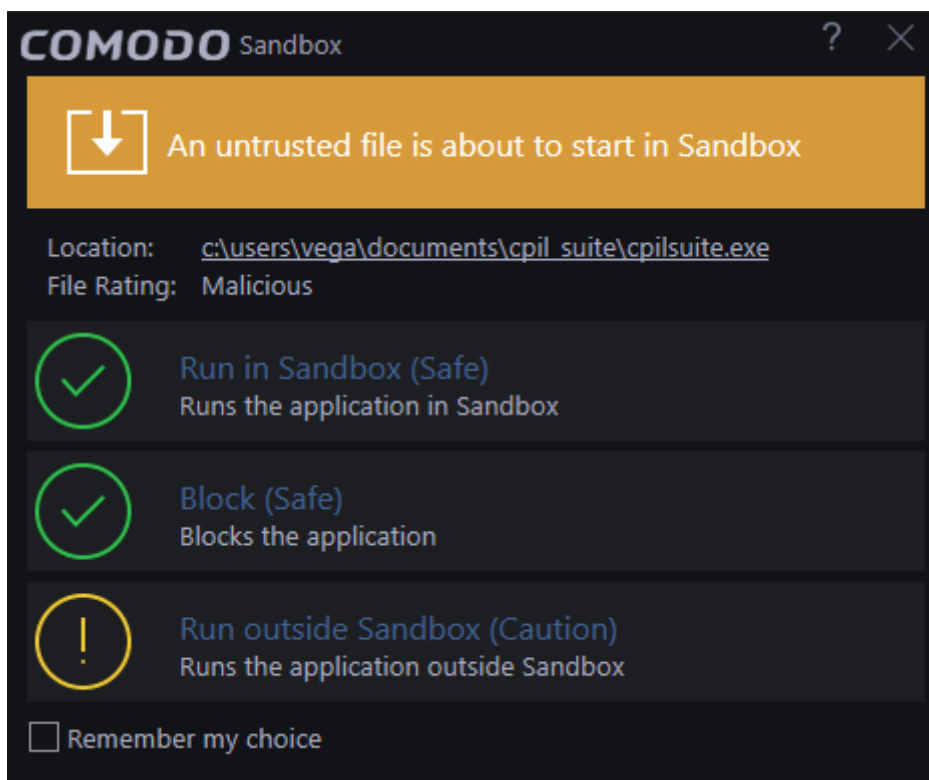
- **Ignore Once** - The file is allowed to run temporarily. Another alert will shown by the real-time scanner the next time the file runs. It will also be flagged the next time you run an antivirus scan.
- **Ignore and Add to Whitelist** - The file is allowed to run and is added to **Trusted Applications**. The file will no longer be flagged as malicious by the antivirus.
- **Ignore and Report as False Alert** - Allows the process to run and the file will be **submitted as false positive** and added to the **trusted applications list**.

## Sandbox alerts:

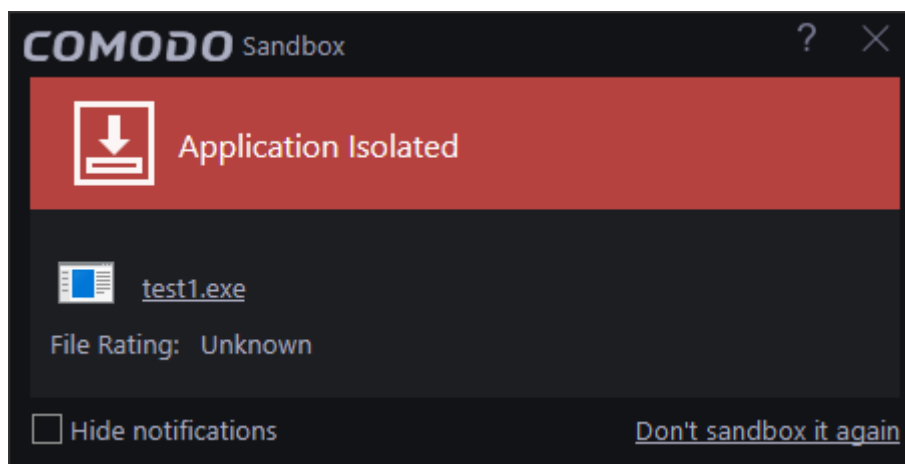
Sandbox alerts are shown when an untrusted application is opened. The alert presents you with the following options:

- **Run in Sandbox - Recommended.** Runs the application in a secure, isolated environment. The application will not be able to modify other processes and will be completely blocked from making changes to your computer while in the sandbox.
- **Block** - Stops the application from running
- **Run outside Sandbox** - Allows the application to run as normal on your computer. Unless you are sure the application is safe, Comodo recommends you run unknown applications in the sandbox. The application will function as normal in the sandbox, but is prevented from causing damage to your computer.

**Note:** 'Enable Auto-Sandbox' must be switched on for you to receive this type of alert.



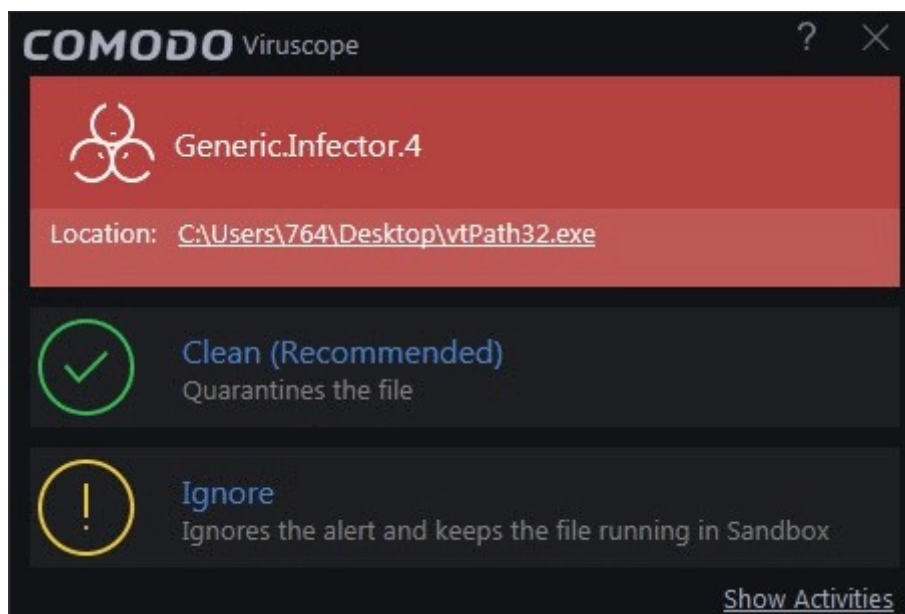
**Note:** If your sandbox setting is 'Sandbox all untrusted files' then you will receive the "Application Isolated" alert for all untrusted files. You can choose to make it a trusted file by clicking "Don't sandbox it again".



## Viruscope alerts:

This alert is shown when applications in sandbox run unauthorized events and when non-sandboxed programs like installers / updaters take suspicious actions. You need to be watchful of alerts when you have not made changes to your computer.

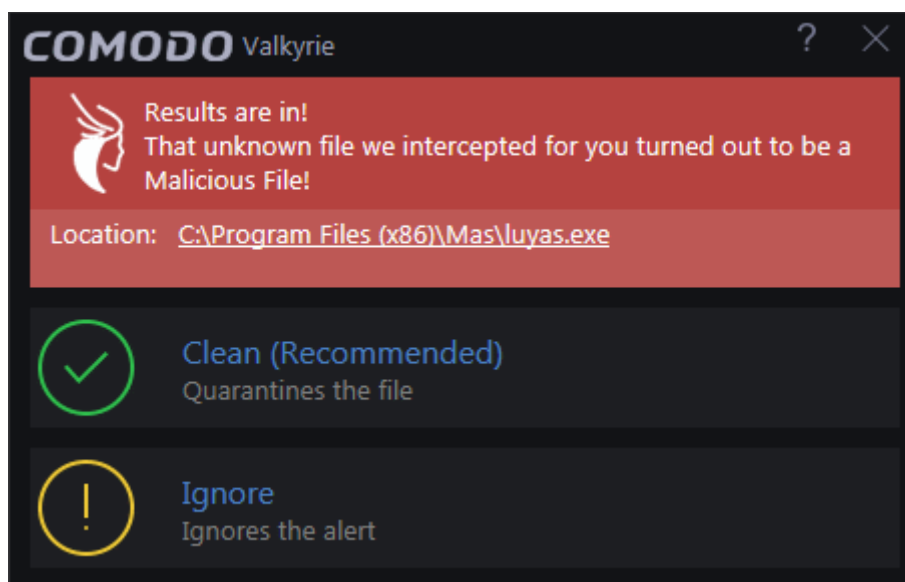
**Note:** You need to enable Viruscope in the sandbox settings to enable this alert.



- Clean - Click 'Clean', If you are not sure of the authenticity of the parent application indicated in the 'Location' field to quarantine it
- Ignore - Click 'Ignore', if it is an application you trust, to allow the process to run
- Show Activities - Click this link at the bottom right, to view the list of activities exhibited by the process through the 'process activities List'

## Valkyrie Alerts

This alert is shown whenever CCAV receives a verdict of an 'Unknown' file that was submitted to Valkyrie. A notification will also be displayed if an unknown file is discovered but 'Submit unknown files automatically' is disabled in **Sandbox Settings**.

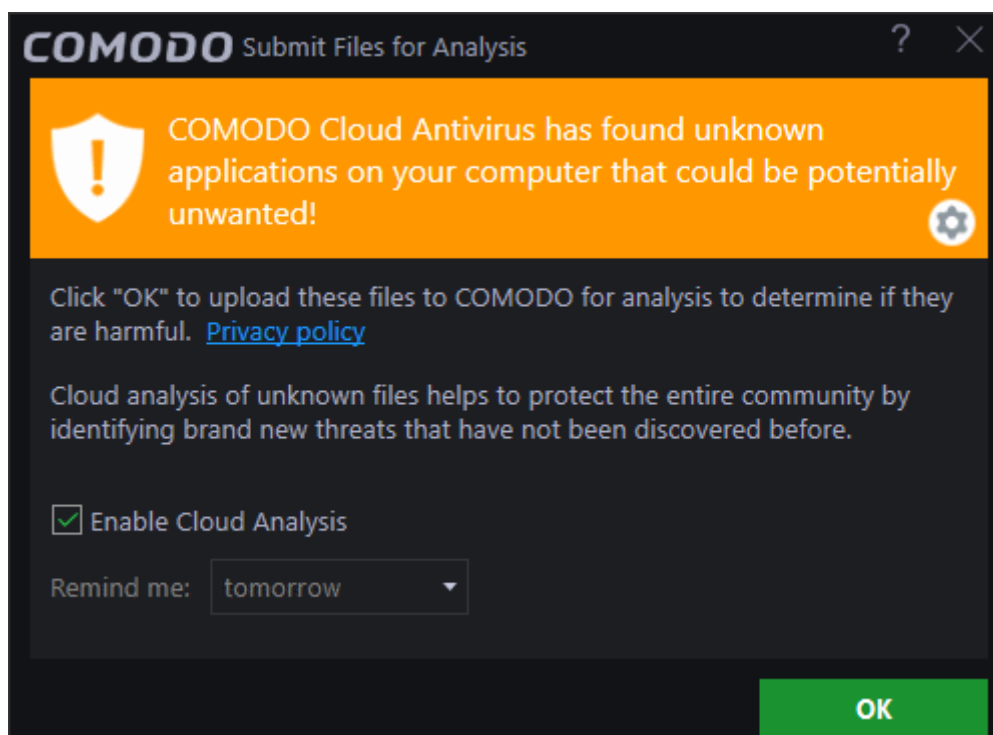


The following response-options are available:

- Clean - Moves the file to 'Quarantine'.
- Ignore - Allows the file and does not attempt to clean the file or move it to quarantine. The file will be identified as Malicious in the future scans.



The below notification will be displayed when an unknown file is detected but you have chosen to disable 'I want to enable 'Cloud Based Behavioral Analysis' of unrecognized programs ...' in Sandbox settings



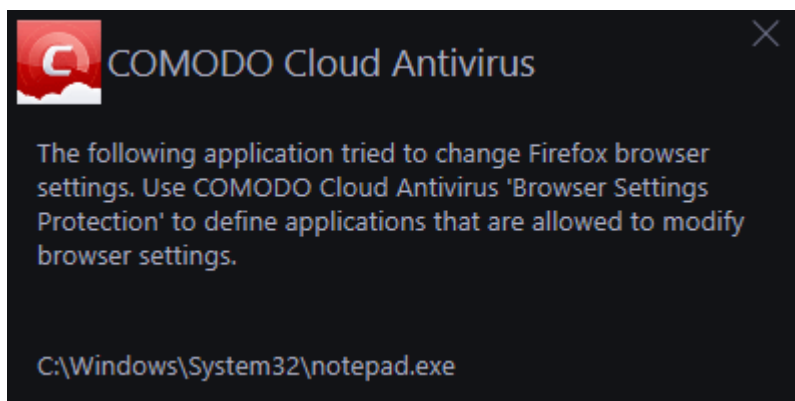
If you click 'OK' with this selected then these notifications will no longer be shown and unknown files will be automatically uploaded to Valkyrie in future. Clicking 'OK' also enables the 'I want to enable "Cloud Based Behavioral Analysis" of unrecognized programs...' option.

To select an option, deselect 'Enable Cloud Analysis' check box, select the option and click 'OK'.

- If you select the last option, 'Don't ask again', the notification will not be displayed anymore.
- If this option is selected then in order to submit unknown files automatically to Valkyrie, you have to enable the option in the '**Sandbox Settings**' interface.

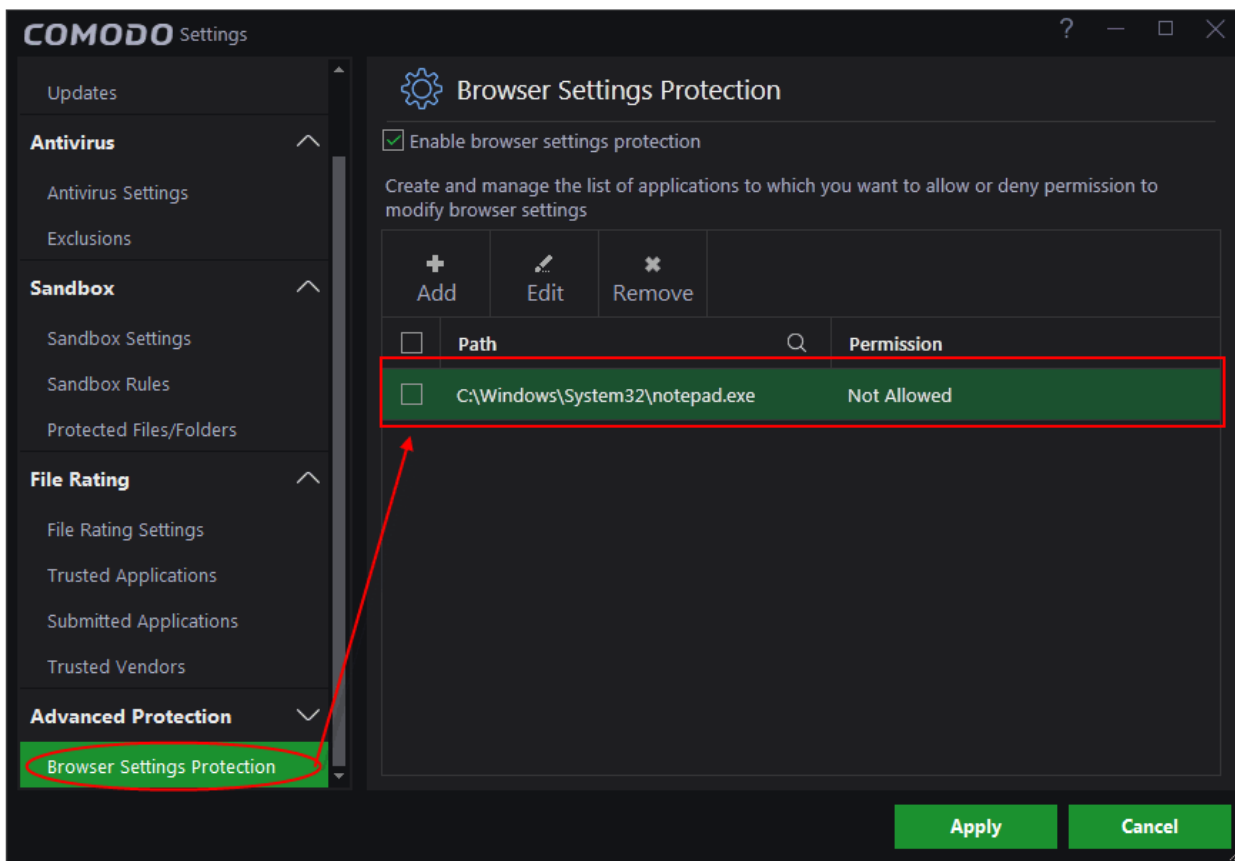
## Browser Protection alerts

This alert is shown when an application attempts to change your browser settings for the first time (e.g. default search engine, home page, privacy setting etc).



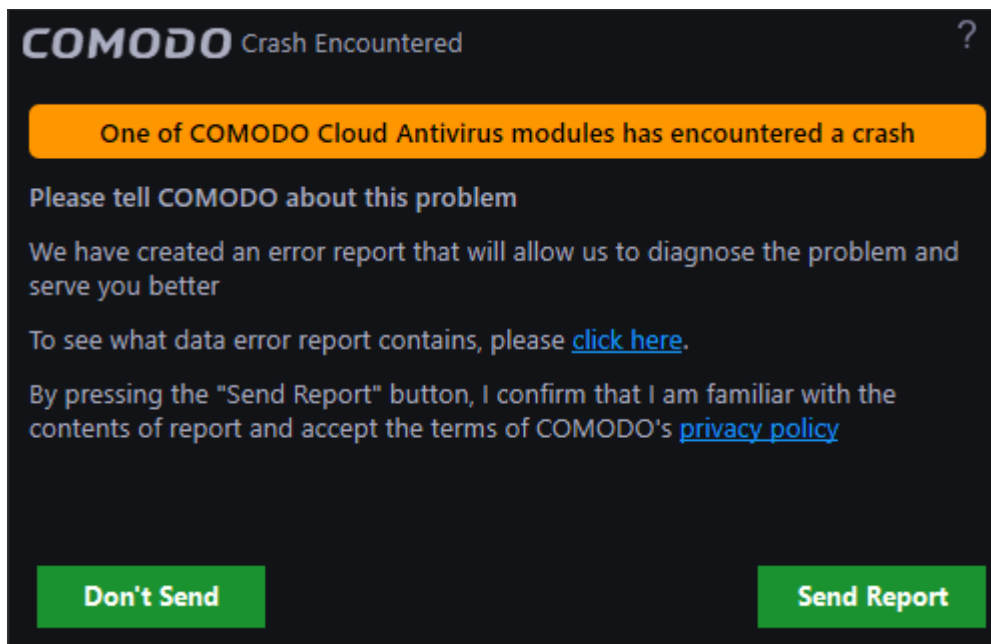
Blocked applications will automatically be added to the 'Browser Settings Protection' area of CCAV. You can subsequently change access permissions for each application from this interface. You can also use this interface to manually add applications that you want to restrict.





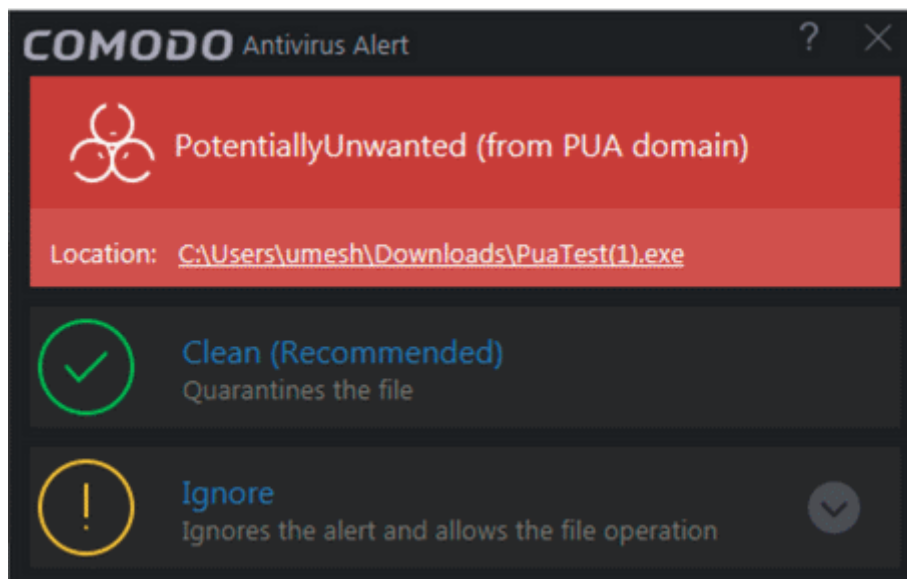
## Crash reporting alerts

This alert is shown whenever the antivirus module encounters a crash. You can help Comodo rectify the issue by sending the error report to Comodo for analysis.



## PUA detection alerts

These alerts are shown if you attempt to download a piece of software from a domain that is known to serve potentially unwanted software (PUA). Example PUA's include adware and browser toolbars.



## View CCAV Logs

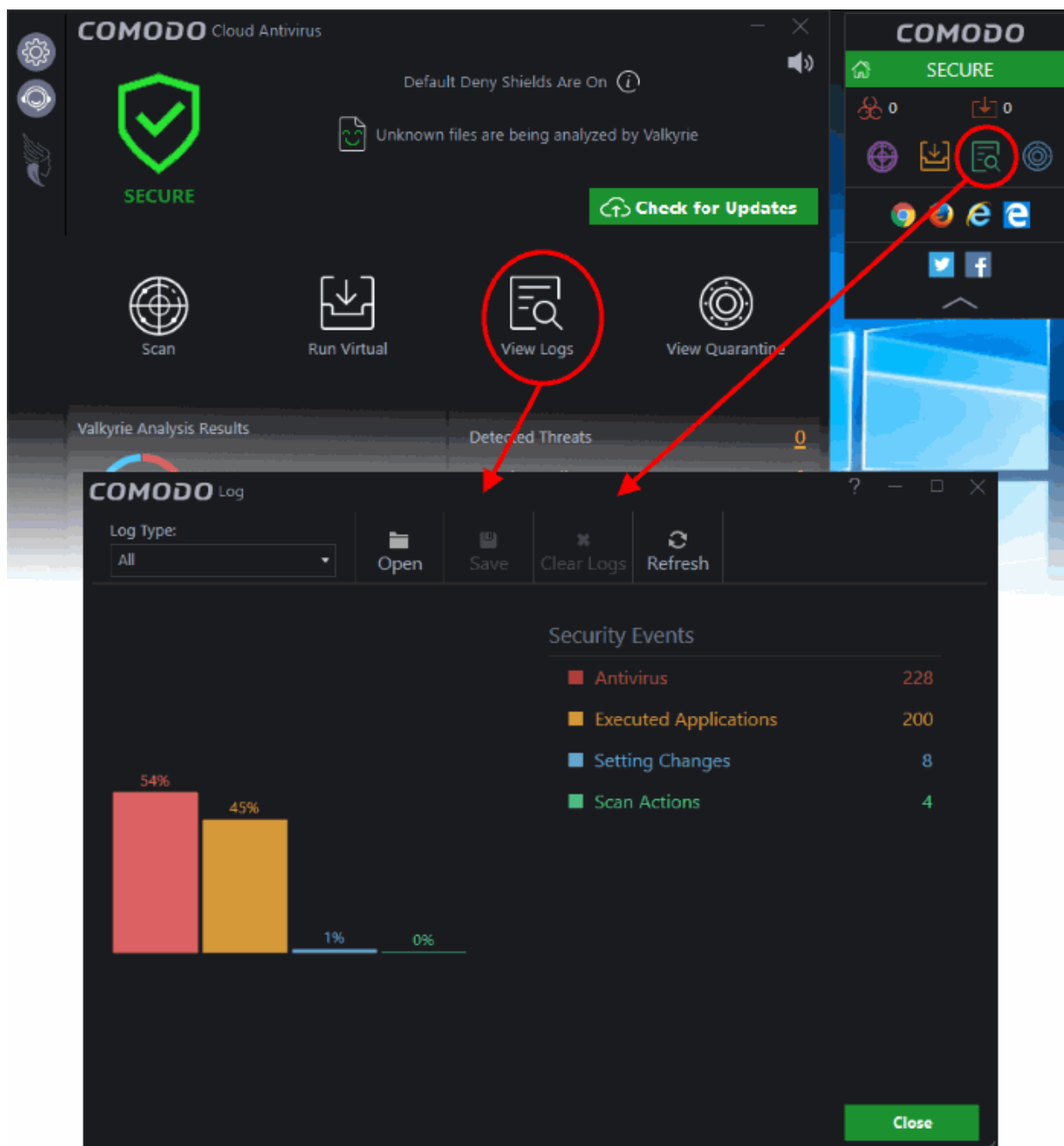
CCAV logs are a record of all antivirus events, sandbox events, configuration changes and other user initiated actions. The 'Log' interface you to view and manage logs.

### To view the main 'Log' interface

- Click 'View Logs' on the of the CCAV home screen

OR

- Click the 'View Logs' shortcut button  on the widget



A summary of all available logs will be shown. You can choose the type of logs you wish to see from the drop down menu at top left.

- 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'.

The various individual log interfaces are:

- **Antivirus Logs**

- **Executed Applications Logs (Sandbox Logs)**
- **Setting Changes Logs**
- **Scan Actions Logs**

In all log interfaces, you will be able to perform the below activities:

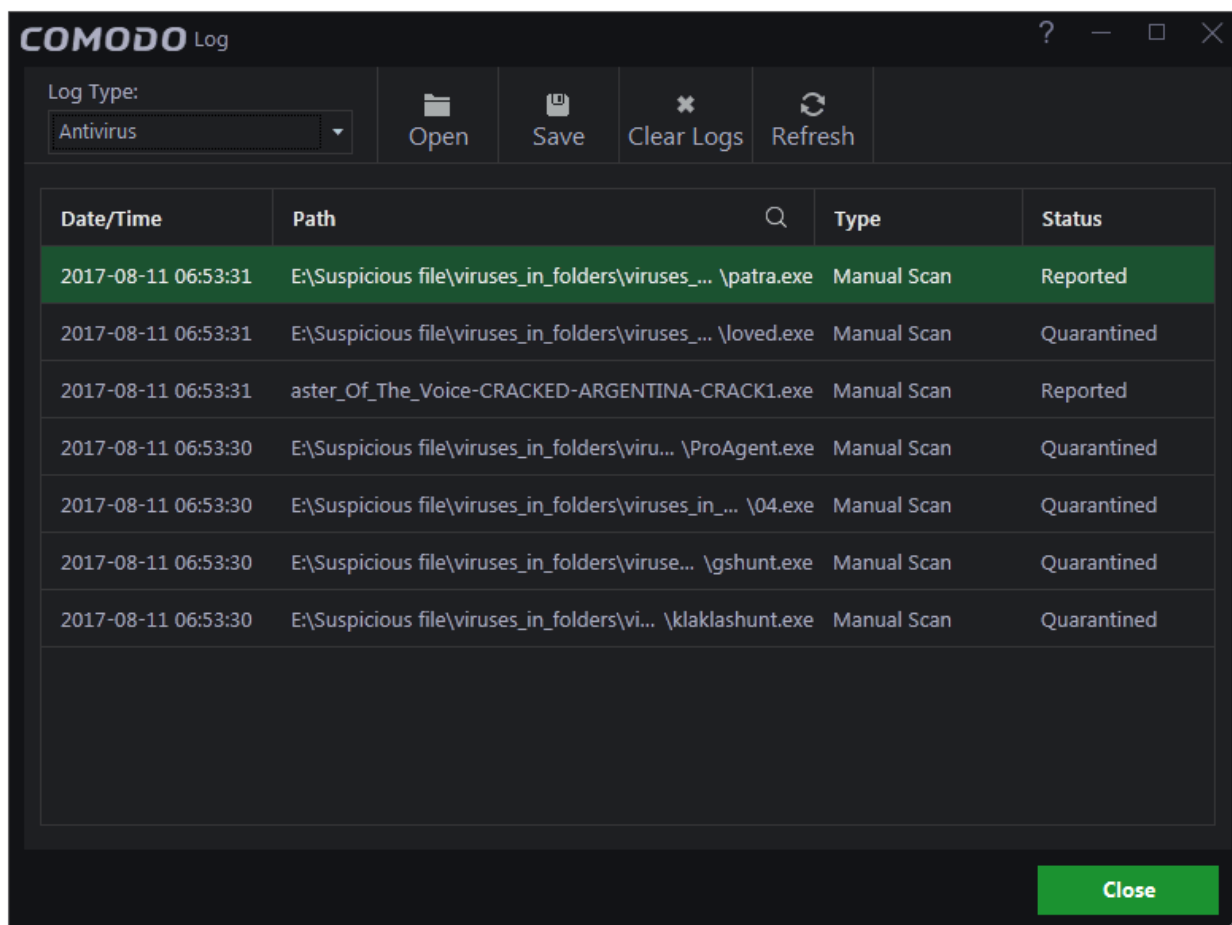
- To export the logs as a '.log' file, click the 'Save' button
- To open a stored log file, click the 'Open' log file button
- To update the list with the latest events, click the 'Refresh' button
- To clear the 'Executed Application' logs, click the 'Clear Logs' button.

## Antivirus Logs

CCAV has a record of all files and folders that are declared malware by the virus scanner through real-time scans, manual scans and Valkyrie analysis.

### To view Antivirus logs

- Click 'View Logs' on the CCAV home screen OR click the 'View Logs' button on the widget
- Select 'Antivirus' from the 'Log Type' drop-down at the top left

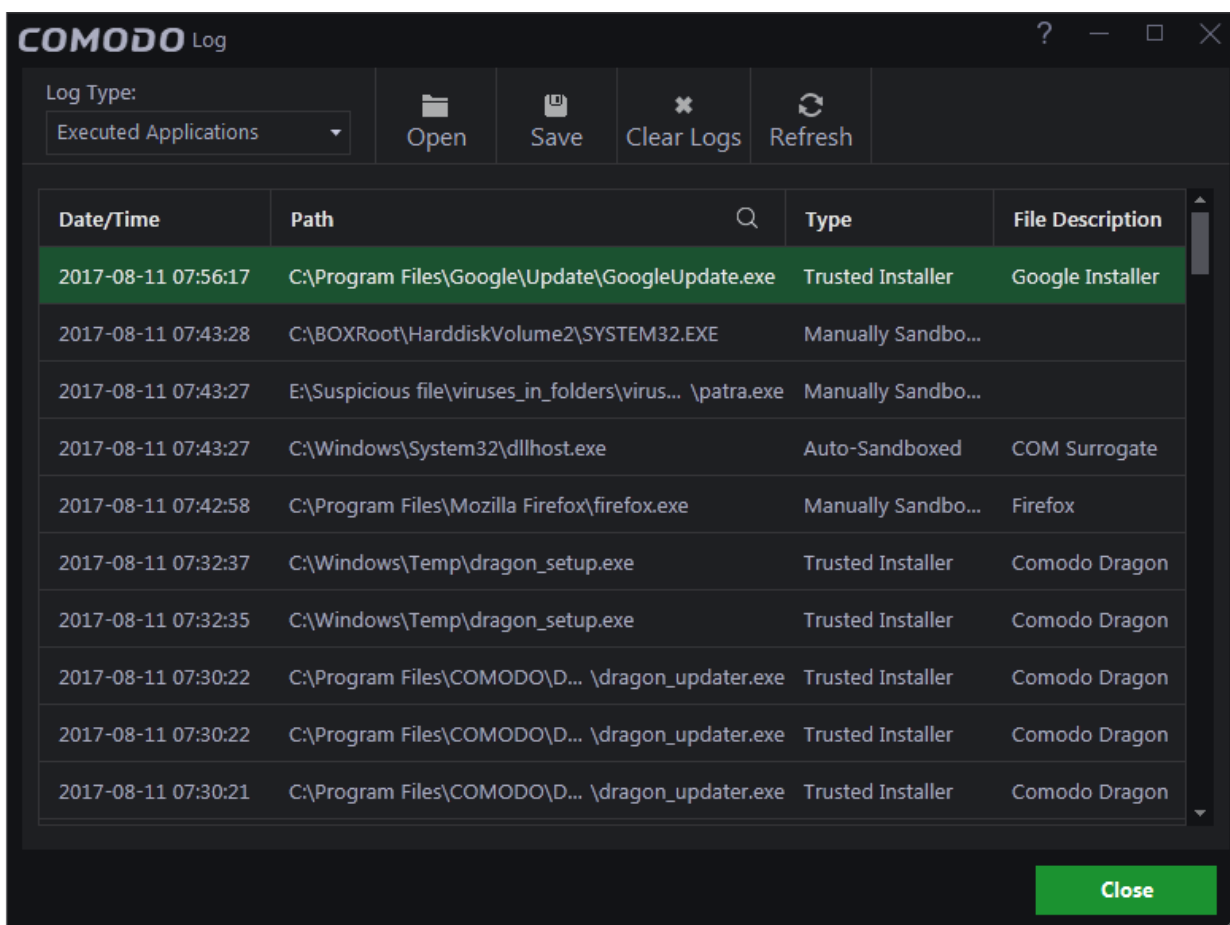


## Executed Application Logs (Sandbox Logs)

CCAV 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.

## To view Executed Applications Logs (Sandbox logs)

- Click 'View Logs' on the home screen OR click the 'View Logs' button on the widget
- Choose 'Executed Applications' from the 'Log Type' drop-down at top left:

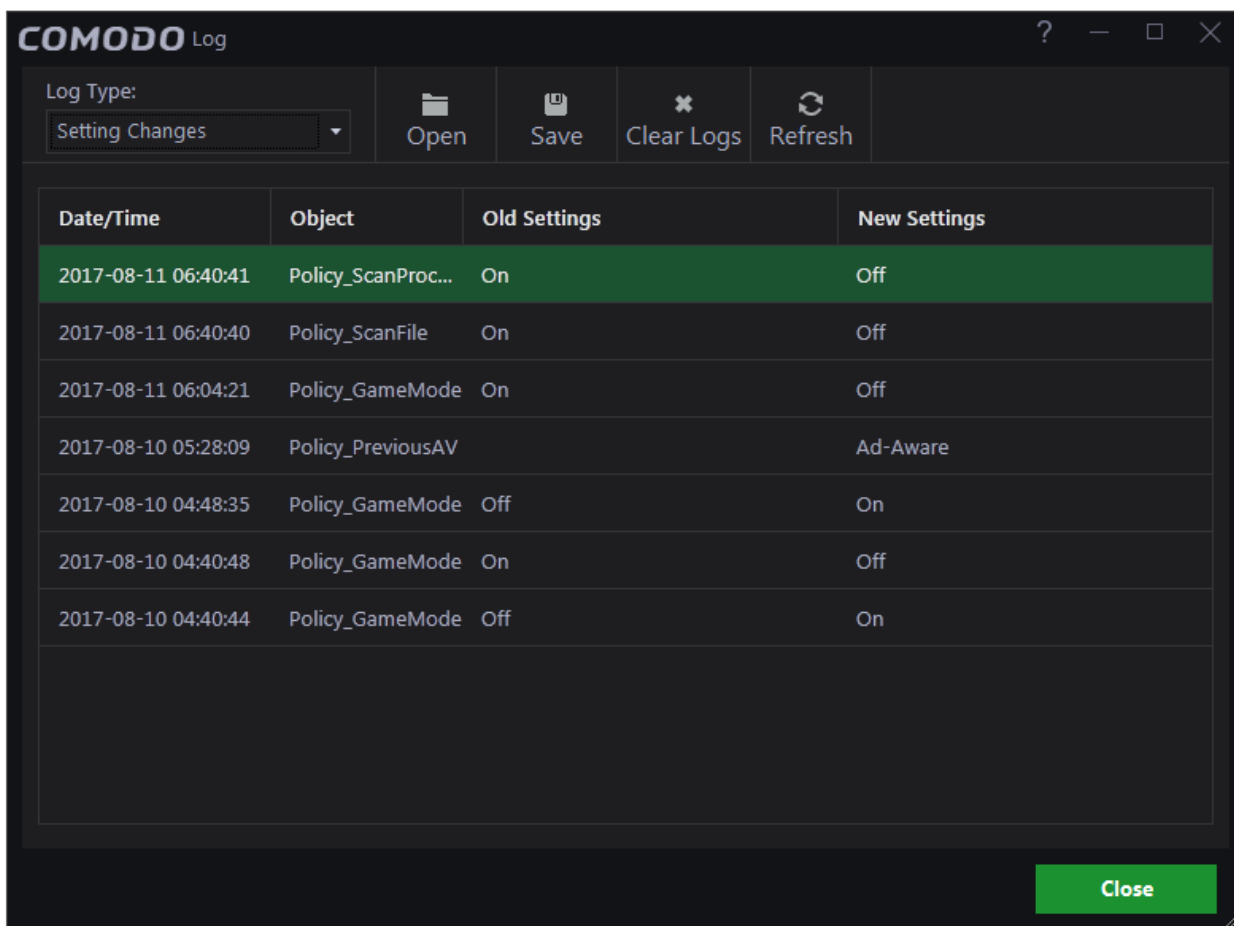


## Setting Change logs

Setting changes logs are a record of all software configuration changes that you make.

### To view 'Setting Changes' logs:

- Click 'View Logs' on the home screen OR click the 'View Logs' button on the widget
- Choose 'Setting Changes' from the 'Log Type' drop-down at the top left of the 'Log' interface



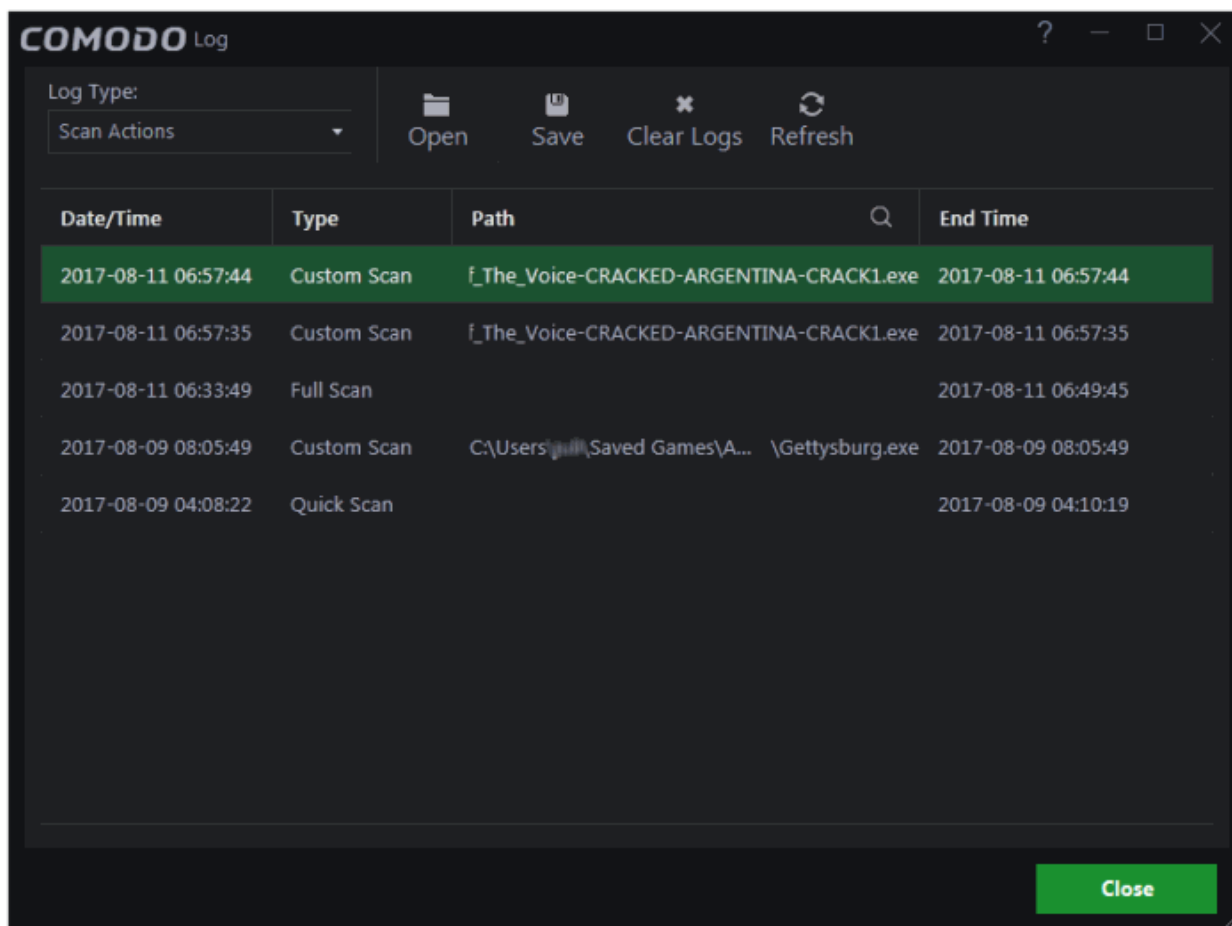
## Scan Action Logs

CCAV keeps a record of all manually initiated virus scans. This includes manual full scans, quick scans, certificate scans and custom scans. Refer to [Scan and Clean your Computer](#) to read more about running a scan.

To view 'Actions' logs

- Click 'View Logs' on the home screen OR click the 'View Logs' button on the widget
- Choose 'Scan Actions' from the 'Log Type' drop-down at the top left of the 'Log' interface

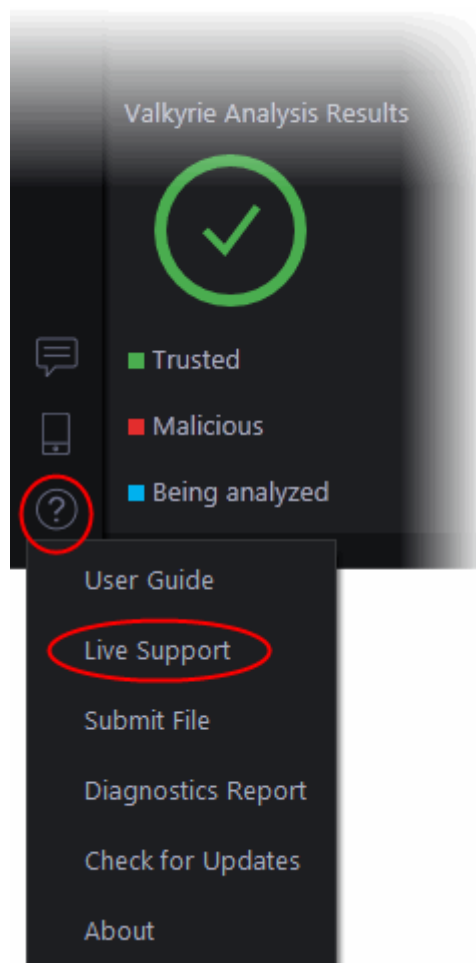




## Get instant support

To get instant support from Comodo for Comodo Cloud Antivirus application:

- Click the help icon on the bottom left of the CCAV home screen
- Click the 'Live Support' option from the drop down menu displayed



## About Comodo

The Comodo organization is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Building on its unique position as the world's largest certificate authority, Comodo authenticates, validates and secures networks and infrastructures from individuals to mid-sized companies to the world's largest enterprises. Comodo provides complete end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats, both known and unknown. With global headquarters in Clifton, New Jersey, and branch offices in Silicon Valley, Comodo has international offices in China, India, the Philippines, Romania, Turkey, Ukraine and the United Kingdom. For more information, visit [comodo.com](http://comodo.com).

### **Comodo Security Solutions, Inc.**

1255 Broad Street

Clifton, NJ, 07013

United States

Email: [EnterpriseSolutions@Comodo.com](mailto: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