COMODO
Creating Trust Online®

Comodo
Cloud Antivirus

Software Version 1.3

User Guide

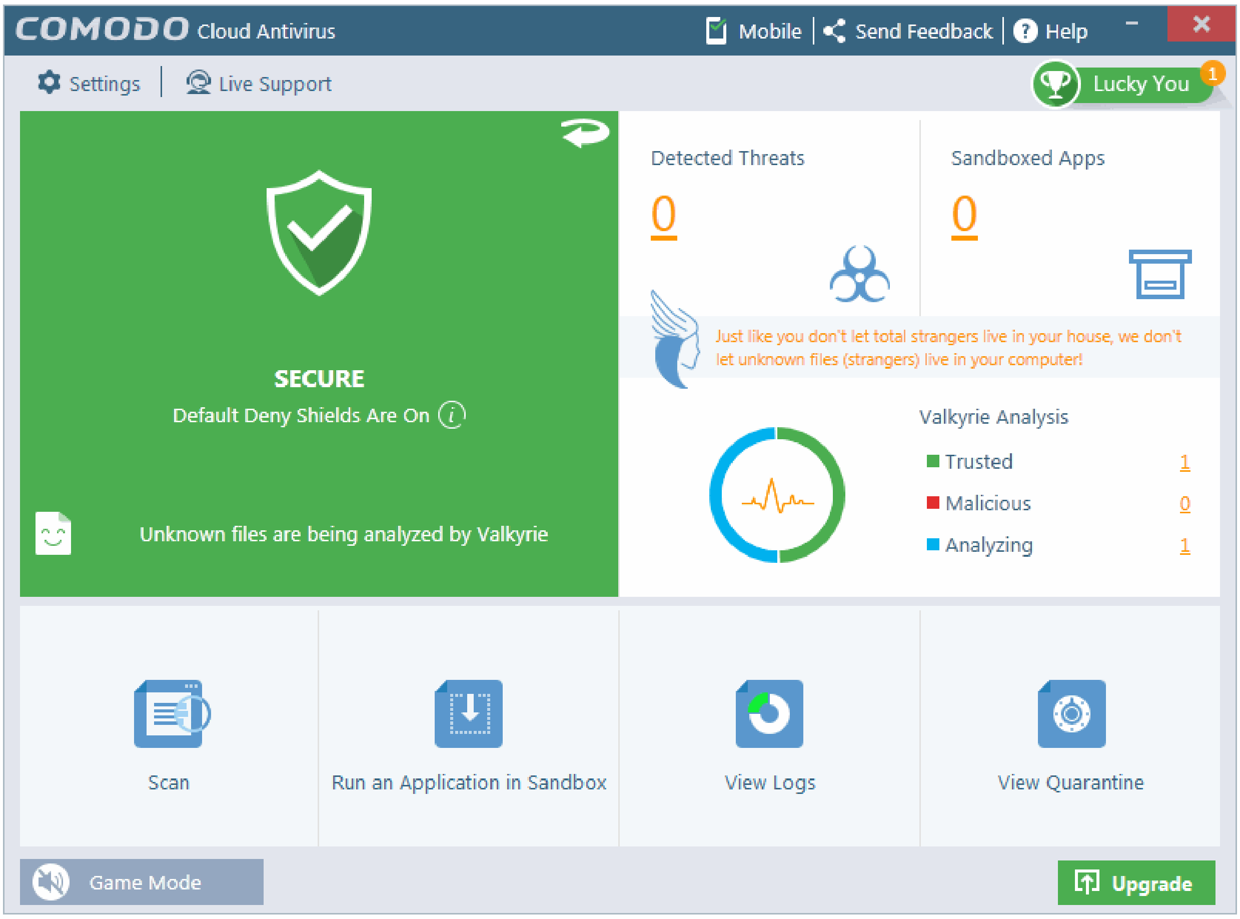
Guide Version 1.3.101416

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

Table of Contents

1. Introduction to Comodo Cloud Antivirus

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


COMODO Cloud Antivirus
Mobile
Send Feedback
Help
Settings
Live Support
Lucky You
1
SECURE
Default Deny Shields Are On
Unknown files are being analyzed by Valkyrie
Detected Threats
0
Sandboxed Apps
0
Just like you don't let total strangers live in your house, we don't let unknown files (strangers) live in your computer!
Valkyrie Analysis
Trusted 1
Malicious 0
Analyzing 1
Scan
Run an Application in Sandbox
View Logs
View Quarantine
Game Mode
Upgrade

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 Rating Scan
        - Run a Custom Scan
    - Processing Infected Files

1.1. System Requirements

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

Windows 10 Support (Both 32-bit and 64-bit versions) Windows 8 (Both 32-bit and 64-bit versions) Windows 7 (Both 32-bit and 64-bit versions) Windows Vista (Both 32-bit and 64-bit versions)	• 384 MB available RAM • 210 MB hard disk space for both 32-bit and 64-bit versions • CPU with SSE2 support • Internet Explorer Version 5.1 or above
Windows XP (32-bit)	• 256 MB available RAM • 210 MB hard disk space for both 32-bit and 64-bit versions • CPU with SSE2 support • Internet Explorer Version 5.1 or above

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

1.2. Installation

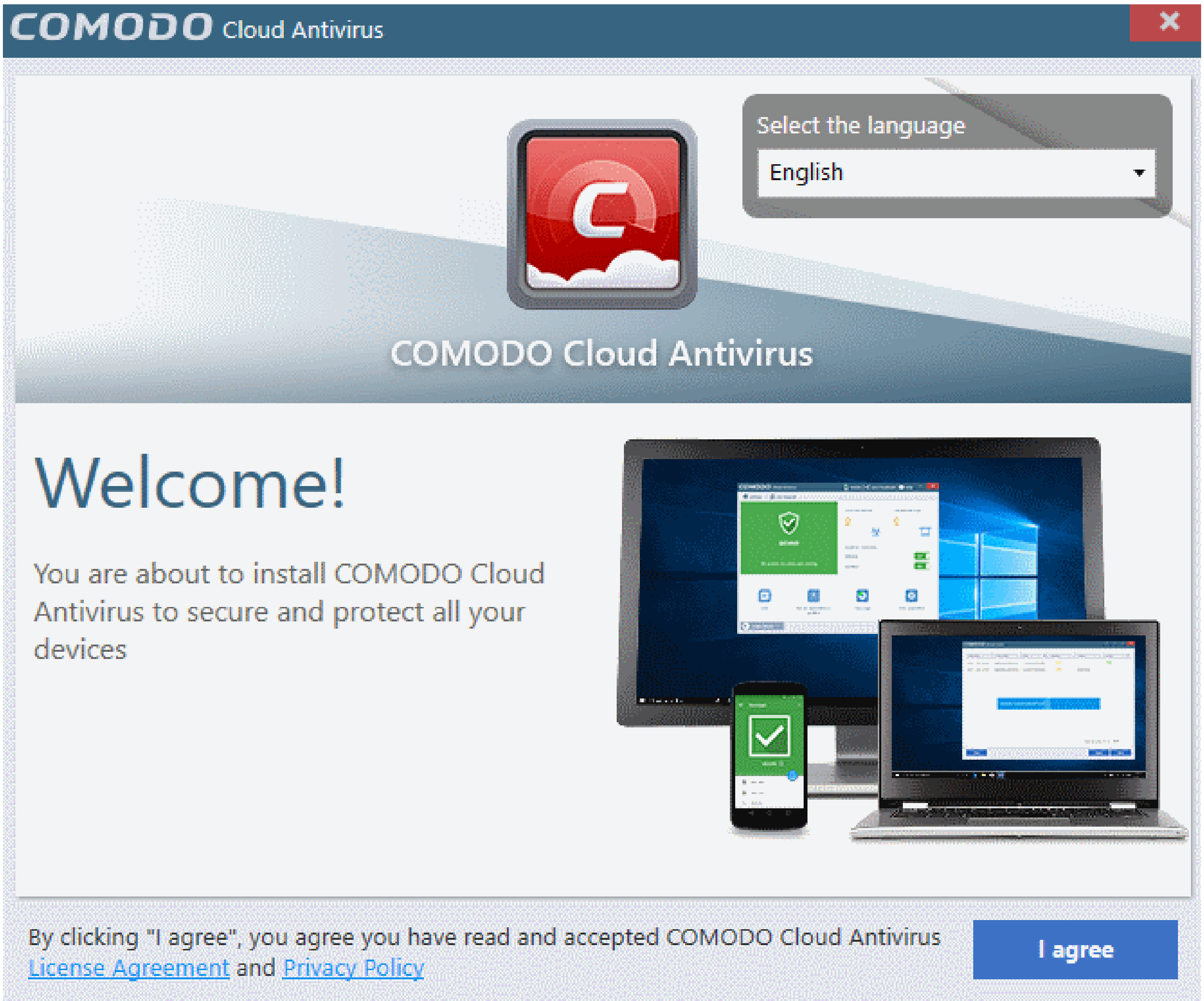
Note - Before beginning installation, please ensure you have uninstalled any other antivirus products and Comodo's CIS/CES that are on your computer. Failure to remove 3rd party AV products and CIS/CES could cause conflicts that mean CCAV will not function correctly. Users should consult their vendor's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

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

To install, download the Comodo Cloud Antivirus setup files to your local drive. (setup file can be downloaded from https://antivirus.comodo.com/cloud-antivirus.php)

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

The language selection dialog will be displayed.

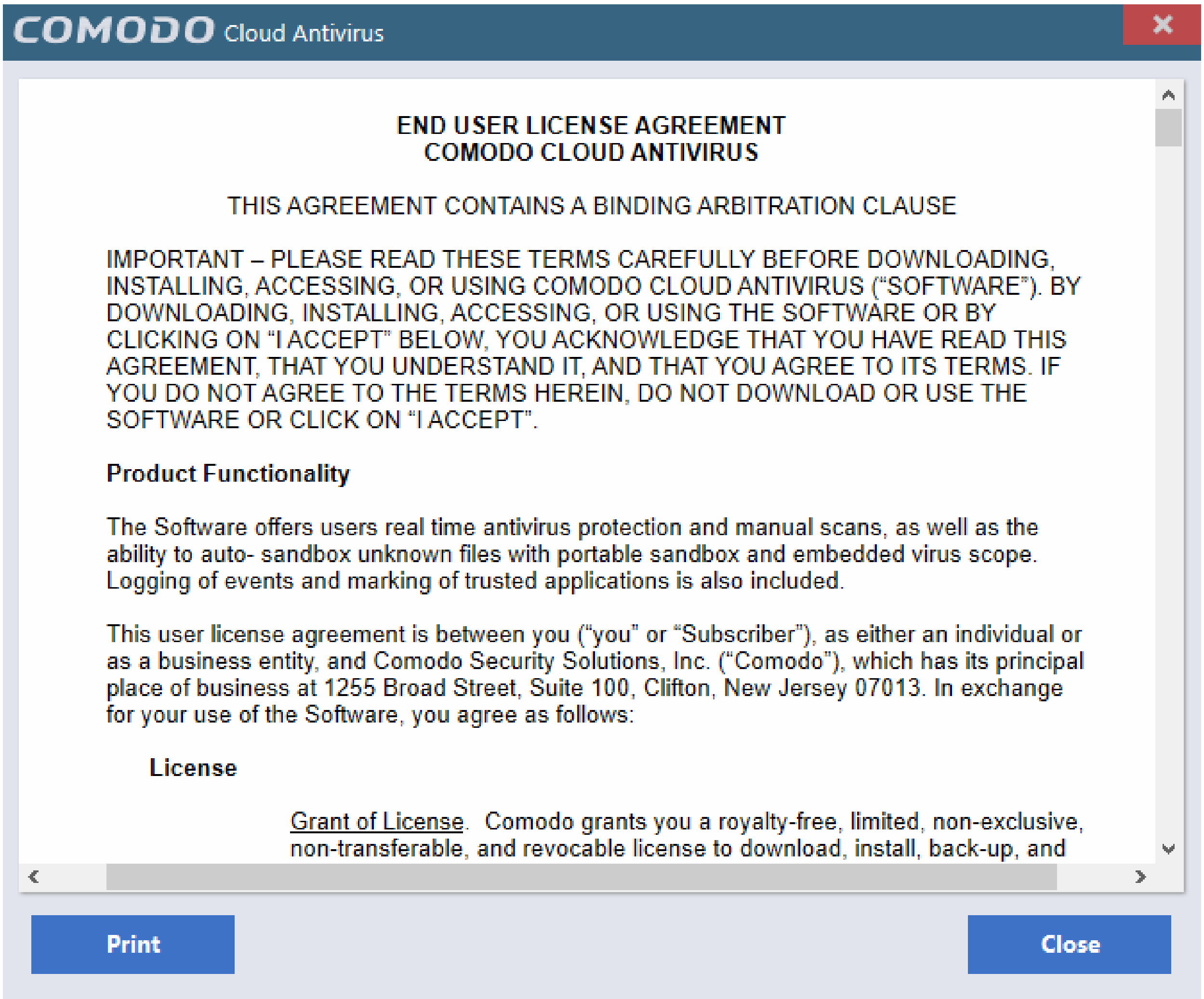


Welcome!

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

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

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



END USER LICENSE AGREEMENT
COMODO CLOUD ANTIVIRUS

THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE

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

Product Functionality

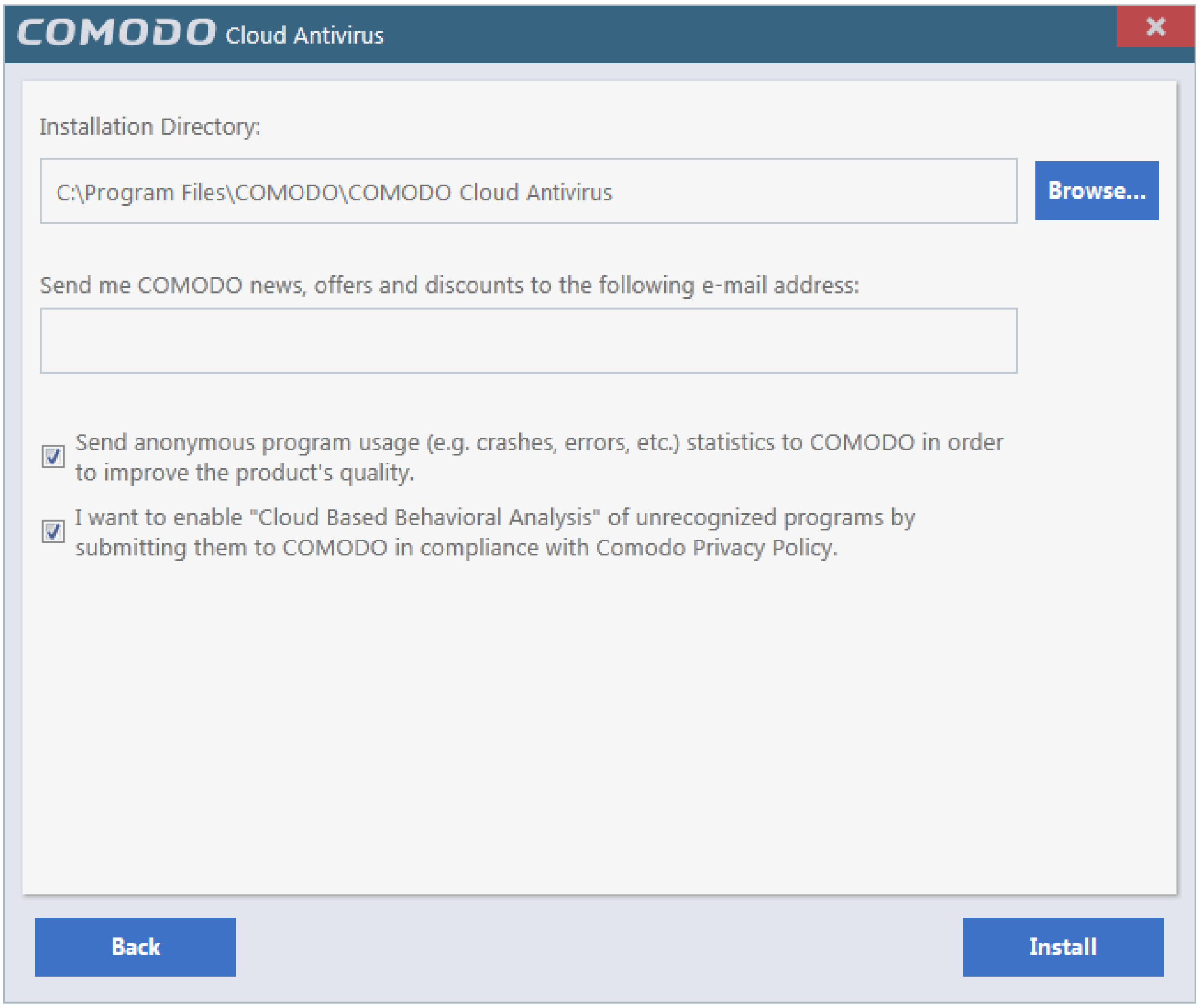
The Software offers users real time antivirus protection and manual scans, as well as the ability to auto- sandbox unknown files with portable sandbox and embedded virus scope. Logging of events and marking of trusted applications is also included.

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

License

Grant of License. Comodo grants you a royalty-free, limited, non-exclusive, non-transferable, and revocable license to download, install, back-up, and

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



Installation Directory:

C:\Program Files\COMODO\COMODO Cloud Antivirus

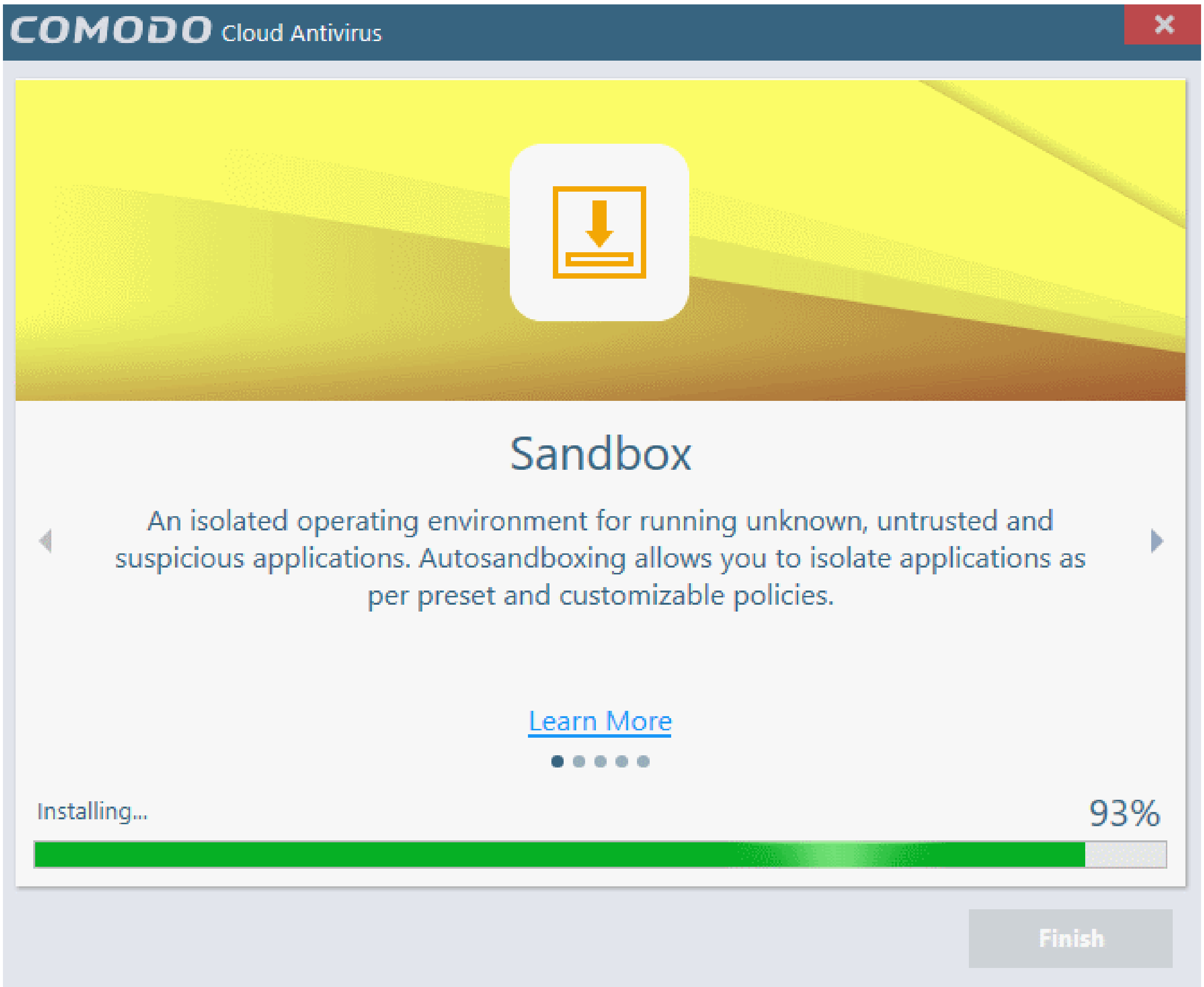
Send me COMODO news, offers and discounts to the following e-mail address:

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

☑ I want to enable "Cloud Based Behavioral Analysis" of unrecognized programs by submitting them to COMODO in compliance with Comodo Privacy Policy.

- 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. Any file that is identified as unrecognized is sent to the Comodo Instant Malware Analysis (CIMA) server for behavior analysis. Each file is executed in a virtual environment on Comodo servers and tested to determine whether it it behaves in a malicious manner. The results will be sent back to your computer in around 15 minutes. Comodo recommends users leave this setting enabled.
- Click the 'Install' button.

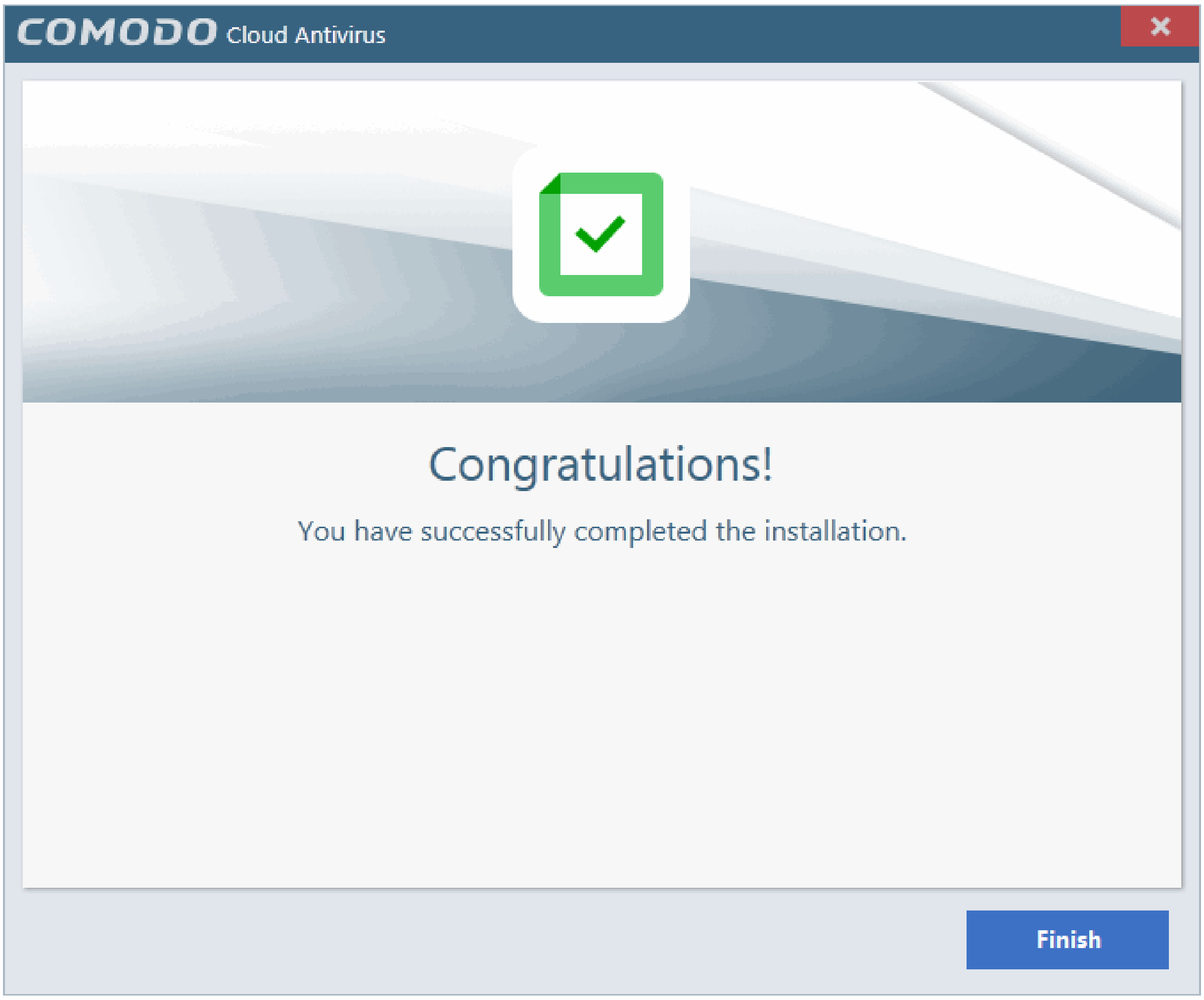
The installation progress will be displayed and on completion...



Sandbox

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

...the success message will be displayed.

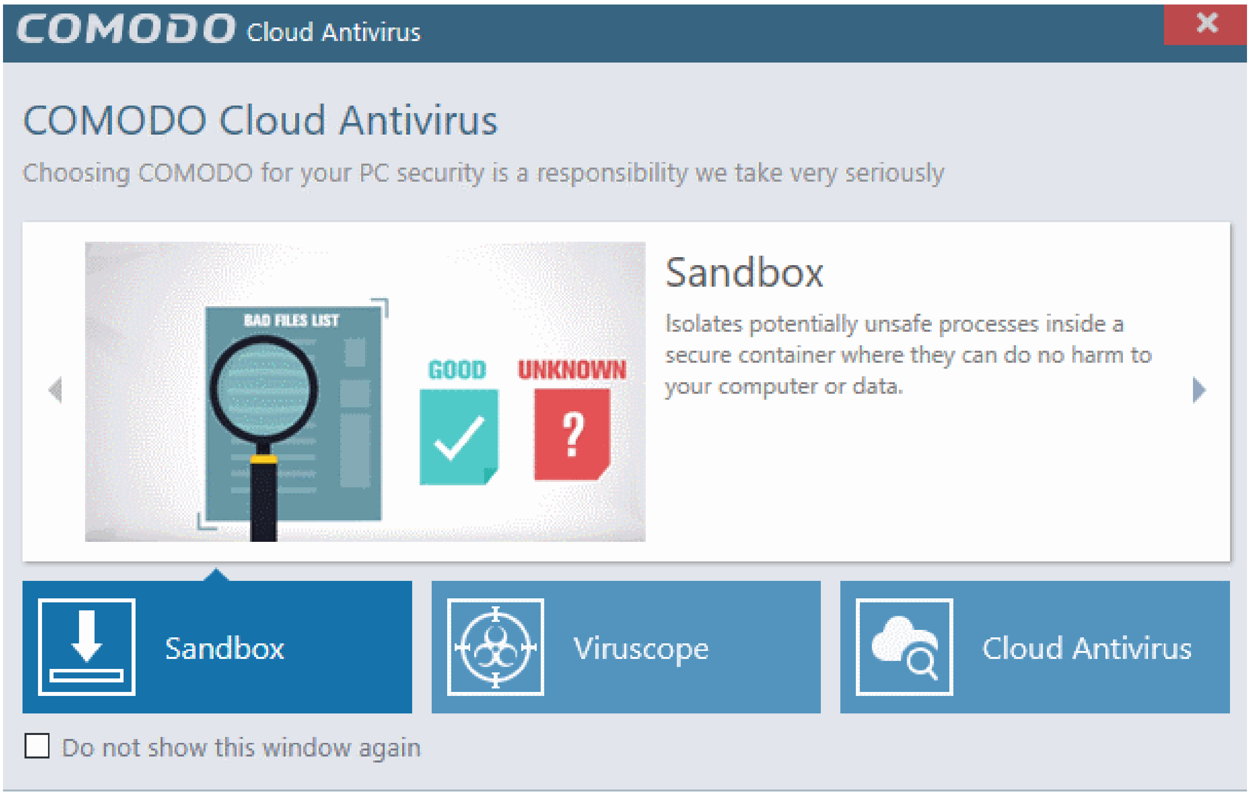


Congratulations!

You have successfully completed the installation.

- Click 'Close'

After successful installation, CCAV will launch the ratings scan automatically and a welcome screen will be displayed:



COMODO Cloud Antivirus

COMODO Cloud Antivirus

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

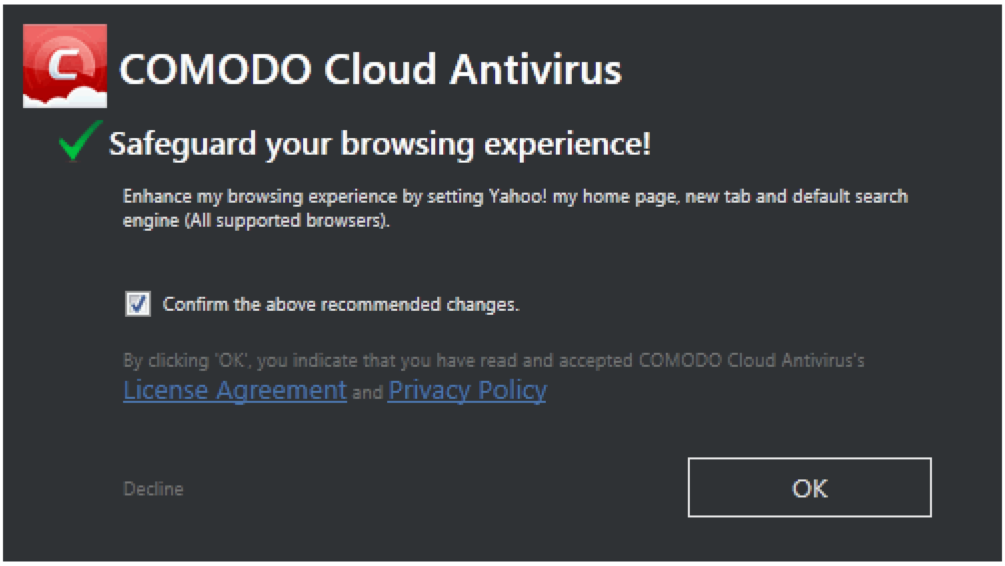
Sandbox

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

□ Do not show this window again

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

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



COMODO Cloud Antivirus

✓ Safeguard your browsing experience!

Enhance my browsing experience by setting Yahoo! my home page, new tab and default search engine (All supported browsers).

☑ Confirm the above recommended changes.

By clicking 'OK', you indicate that you have read and accepted COMODO Cloud Antivirus's License Agreement and Privacy Policy

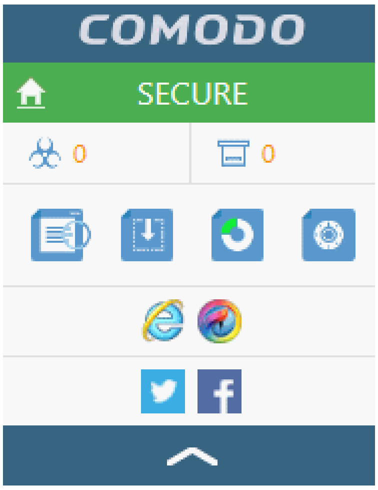
Currently supported browsers are Mozilla Firefox, Google Chrome, Internet Explorer, Comodo Dragon, Comodo IceDragon, Chromodo and Opera.

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 cancel the Yahoo enhancement and continue using your current search engine and home page.

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 sandbox
    - View logs
    - View Quarantine
- The fourth stripe consists of shortcuts to open the browsers installed on your computer inside Sandbox, for secure browsing sessions.
- 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 access the main interface.

There are 4 different ways to open Comodo Cloud Antivirus:

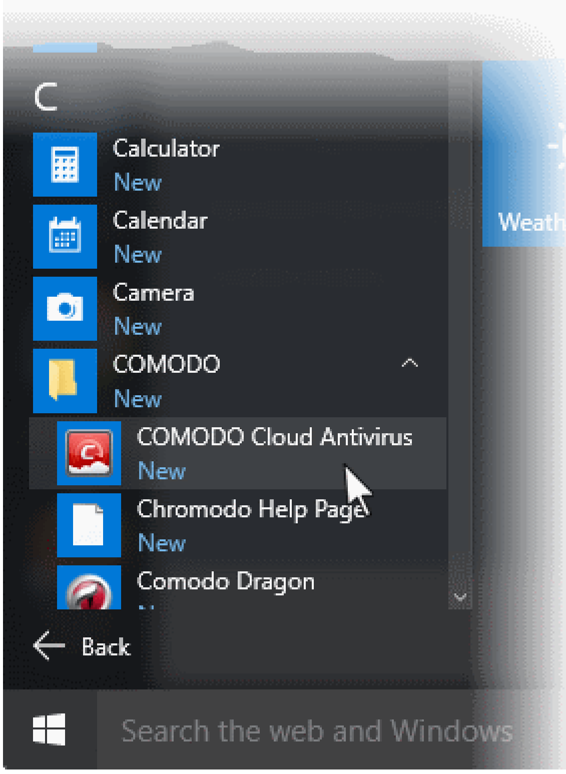
- **Windows Start Menu**
- **Windows Desktop**
- **Widget**
- **System Tray Icon**

Start Menu

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

- Click 'Start' or 'Windows' button and select 'All Programs'/'All Apps' > 'COMODO' > 'COMODO Cloud

Antivirus'

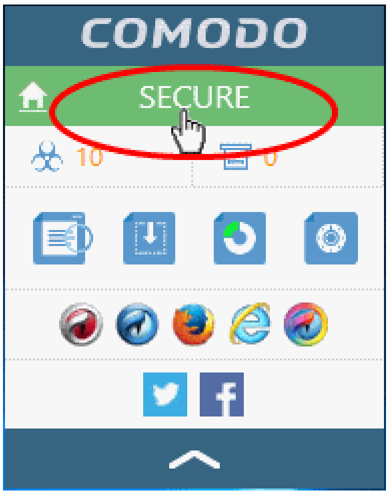


Windows Desktop

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

Widget

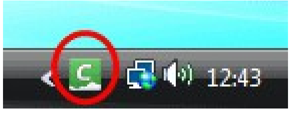
- Just click the information bar in the widget to start CCAV.



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 Twitter and Facebook and more. Refer to the section 'The Widget' for more details.

System Tray Icon

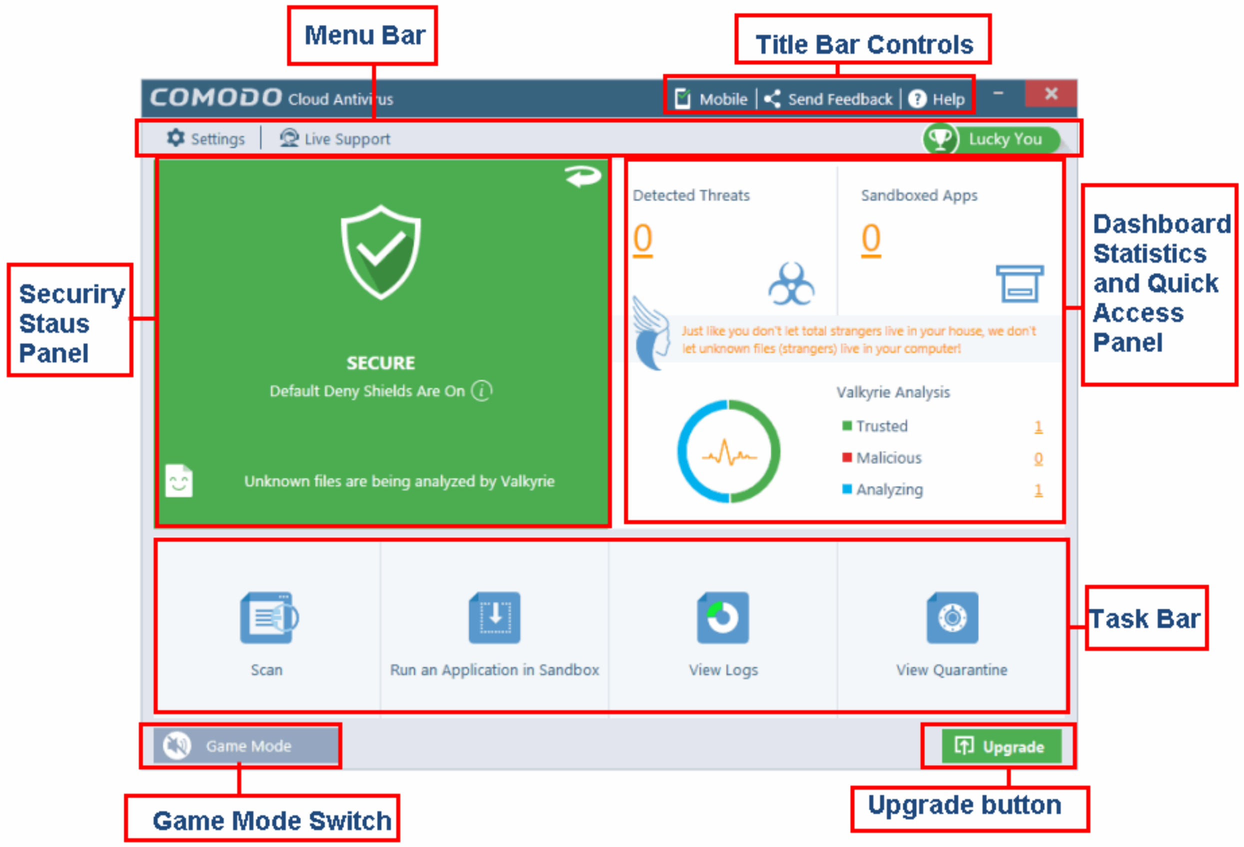
- Just double click the CCAV tray icon to start the main interface.



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

1.3.1. The Main Interface

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


Menu Bar
Title Bar Controls
COMODO Cloud Antivirus
Mobile | Send Feedback | Help
Settings | Live Support
Lucky You
Secruiry Staus Panel
SECURE
Default Deny Shields Are On
Unknown files are being analyzed by Valkyrie
Detected Threats
0
Sandboxed Apps
0
Just like you don't let total strangers live in your house, we don't let unknown files (strangers) live in your computer!
Valkyrie Analysis
Trusted 1
Malicious 0
Analyzing 1
Dashboard Statistics and Quick Access Panel
Scan
Run an Application in Sandbox
View Logs
View Quarantine
Task Bar
Game Mode
Upgrade
Game Mode Switch
Upgrade button

Menu Bar

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

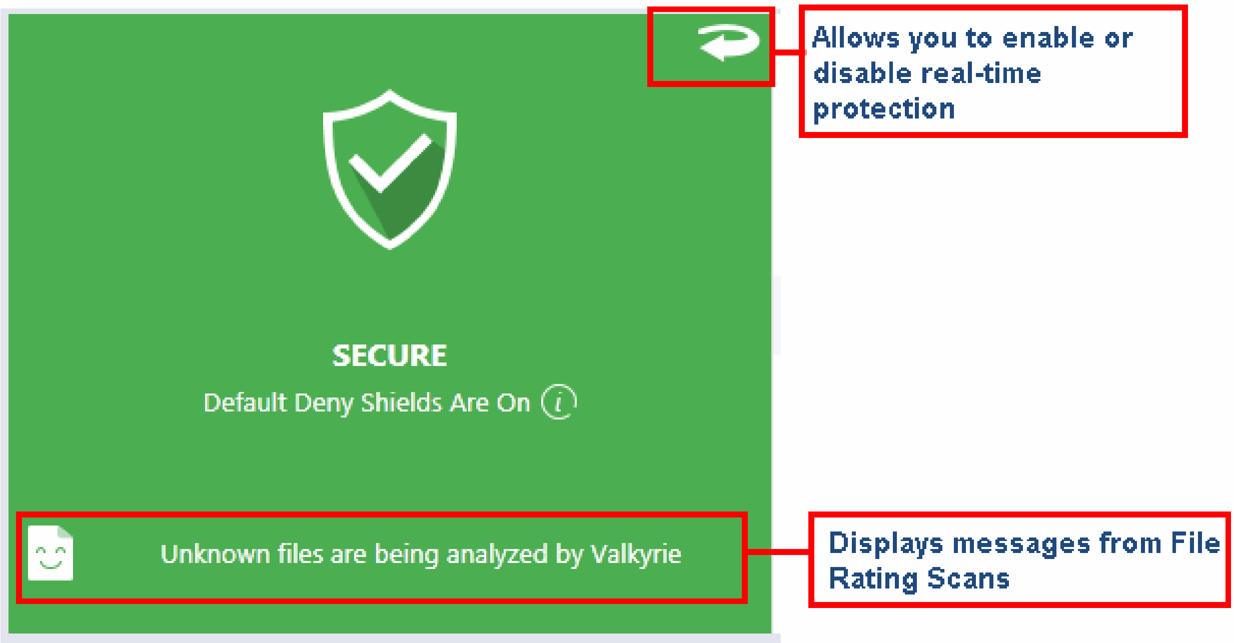
Tasks Bar

- Scan - Do a quick AV scan, full computer scan, file rating scan or configure a custom scan. Refer to the section 'Scan and Clean your Computer' for more details.

- Run an Application in Sandbox - Run a browser or any application inside the sandbox for full security. Refer to the section 'Run an Application in the Sandbox' for more details.
- View Logs - Allows you to view the logs of AV, sandbox and setting changes. Refer to the section 'View CCAV Logs' for more details.
- View Quarantine - Manage the quarantined items from this interface. Refer to the section 'View and Manage Quarantined Items' for more details.

Security Status Pane

The flip-able Security Status Pane indicates whether the protection systems are active, status of rating scan for submitting unknown files for analysis to Valkyrie and allows you to enable/disable Antivirus/Sandbox real-time protection status.


SECURE
Default Deny Shields Are On
Unknown files are being analyzed by Valkyrie

Allows you to enable or disable real-time protection

Displays messages from File Rating Scans

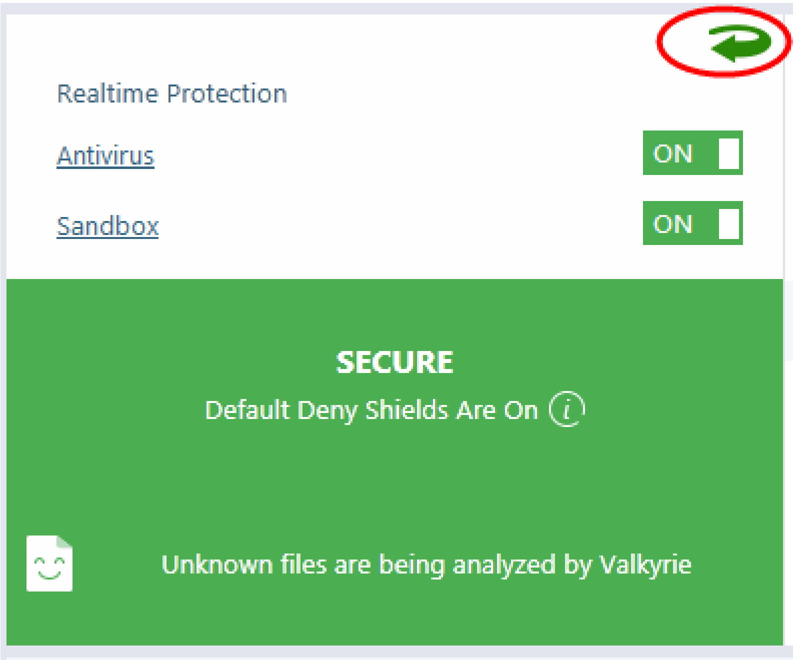
The text below the shield icon indicates the current security status. Refer to the sections 'Antivirus Configuration' and 'Sandbox Configuration' for more details.

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

The pane also displays status messages from Valkyrie. Clicking the message will take to respective interface for running the scan or to view the results.

To enable/disable real-time protection

- Click the curved arrow at the top right of the pane to flip it.

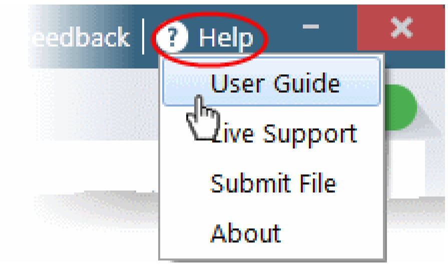

Realtime Protection
Antivirus ON
Sandbox ON
SECURE
Default Deny Shields Are On
Unknown files are being analyzed by Valkyrie

- Use the toggle switches to enable or disable real-time Antivirus and Sandbox protection.
- Click the Antivirus and Sandbox links to open the 'Settings' screen for configuring the respective module

Title Bar Controls

The title bar (top right) contains shortcuts for:

- **Comodo Mobile Security apps for Android phones and tablets**. - Click 'Mobile' to view and download Comodo mobile security apps such as 'Mobile Security', 'Anti-Theft', 'Back Up' and 'App Lock'. You can also get the apps from our website, https://m.comodo.com/ or from the 'Google Play' app store.
- **Send Feedback -** Allows you to provide your comments on the product. Clicking on the 'Send Feedback' link will open the default email client in your system for you to provide feedback about CCAV.
- **Submit Files and Get Help** - Click 'Help' for the following options:

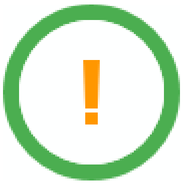


- **User Guide** - Opens the CCAV online help guide at https://help.comodo.com
- **Live Support** - Click this link to chat with our technician for technical help for CCAV. Refer to the section Getting Live Support for more details.
- **Submit** - Allows you to manually submit a suspicious file from your computer to Valkyrie for analysis. Valkyrie analysis involves automated and manual testing in order to discover whether or not the file is malicious. The results will be sent back to your computer once the analysis is complete. The results will also be added to the global whitelist and blacklist to help fellow CCAV users who encounter the same file. Refer to the section Viewing Valkyrie Analysis Results for more details.
- **About** - Displays the product version, details of active Viruscope Recognizers and copyright information.

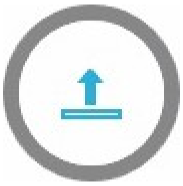
Dashboard Statistics and Quick Access Pane

The upper pane displays a snapshot summary of the number of threats detected by the antivirus, and the number of applications currently running in the sandbox. The lower pane displays the statistics from Valkyrie, based on results from Valkyrie Analysis of files submitted from Rating Scans.

- **Detected Threats** - Displays the number of threats detected by CCAV during real-time scanning as well as during manual scanning. Clicking on the number opens the 'Detected Threats' interface allowing you to 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 sandboxed environment. This includes applications auto-sandboxed and added manually to sandbox. Refer to the section '**Managing Sandboxed Applications**' for more details.
- **Valkyrie Analysis** - Displays a statistical summary the results of files submitted for Valkyrie Analysis from your computer.
    - The pie-chart shows the comparison of numbers of files with different verdicts with an indication of current Valkyrie detection status. Clicking the pie-chart will take to respective interface for running the scan or to view the results.

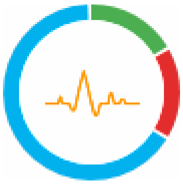


- Indicates that you need to run a File Rating scan to identify unknown files on your computer.

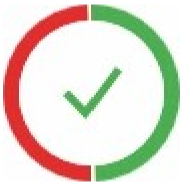


- Indicates that some unknown files are detected by rating scan but auto-submission is disabled. You can submit unknown files manually for Valkyrie Analysis.

- 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 some unknown files were submitted to Valkyrie and are currently under 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.

- Clicking the pie-chart will take you to respective interface for running the scan or to view the results.
- At the right of the pie chart, the numbers of files with different Valkyrie Analysis status are displayed.
    - Unknown - Number of files identified as unknown, but yet to be submitted for Valkyrie Analysis, as auto-submission is disabled.
    - Trusted - Number of files identified as trustworthy by Valkyrie Analysis
    - Malicious - Number of identified as malicious by Valkyrie Analysis
    - Analyzing - Number of files submitted to Valkyrie, but yet to be analyzed
- Clicking the numbers beside 'Unknown', 'Trusted', 'Malicious' and 'Pending' will open the respective results interface.

Game Mode

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

In game mode:

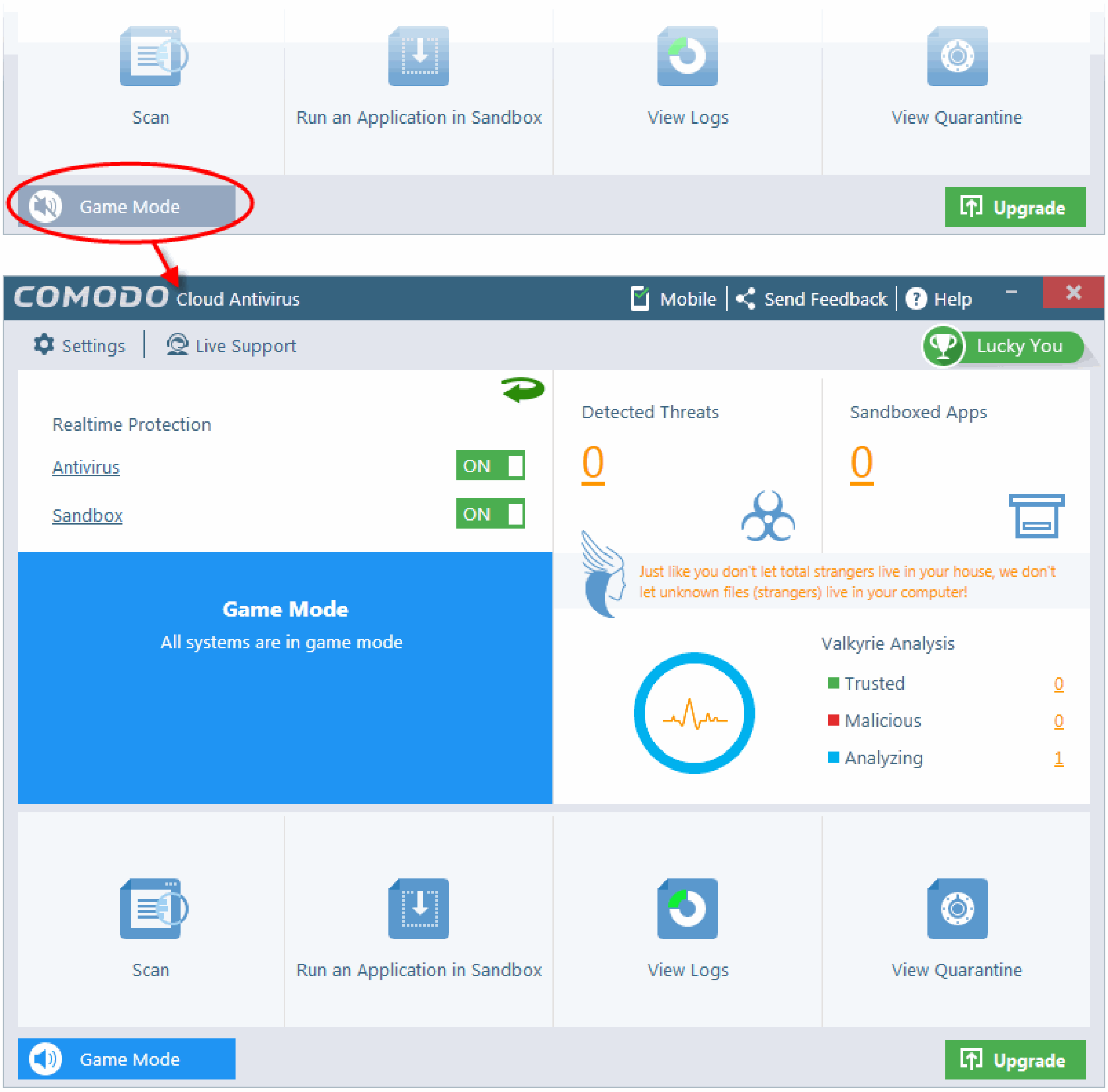
- AV, Viruscope and Sandbox alerts are suppressed.

- Automatic isolation of unknown applications and real-time virus detection are still functional.

To switch to Game mode

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

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



Realtime Protection

Antivirus ON

Sandbox ON

Game Mode

All systems are in game mode

Just like you don't let total strangers live in your house, we don't let unknown files (strangers) live in your computer!

Valkyrie Analysis

🟩 Trusted	0
🟥 Malicious	0
🟦 Analyzing	1

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

Upgrade

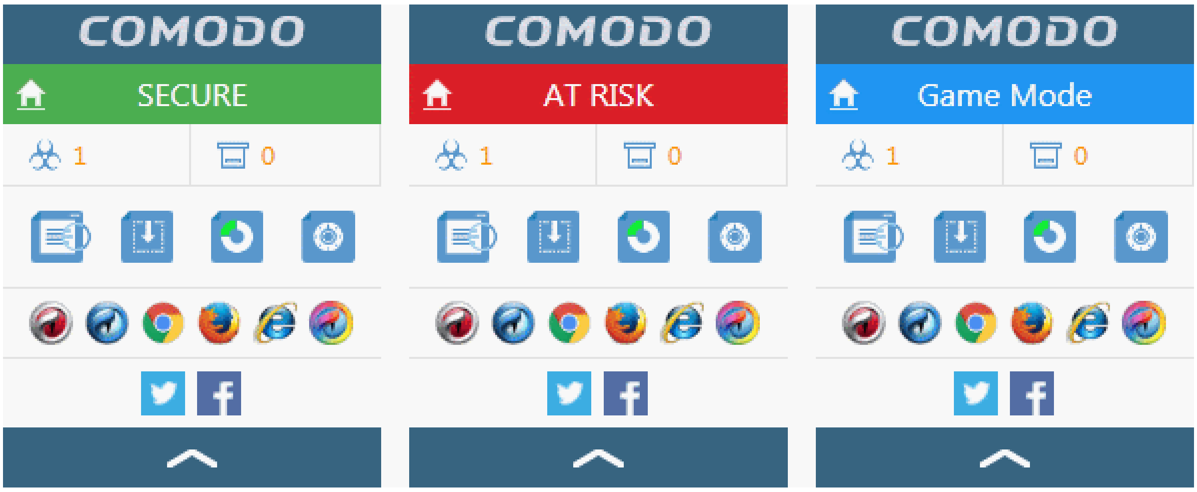
Clicking the 'Upgrade' button leads to the purchase page of 'Comodo Internet Security' (CIS), our full featured internet security solution. In addition to the features available in CCAV, CIS also includes a firewall, host intrusion prevention, online backup, 24/7 instant support and more.

- If you do not want the Upgrade button displayed, you can disable it from the 'User Interface' settings interface. Refer to the section **Customize User Interface** for more details.

1.3.2. The Widget

The CCAV Widget is a handy control that provides at-a-glance information about overall security status, AV scan detection status, sandbox status, and more. It contains shortcuts for executing common CCAV tasks, opening browsers in Sandbox and to popular social networking sites.

Right clicking on the Widget opens a context sensitive menu similar to the one displayed on right clicking the CCAV system tray icon. The context sensitive menu allows you to enable or disable CCAV components and configure various settings. Refer to section 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 main interface of the CCAV application.
- The second row tells you current AV and Sandbox statistics:
  - The first button ☣ 1 displays the number of threats detected by real-time and manual AV scans. Clicking the button opens the Detected Threats interface allowing you to take action on the threats. Refer to the section Managing Detected Threats for more details.
  - The second button ▭ 2 displays the number of applications currently running inside the sandbox. Clicking the button opens the Sandboxed Applications interface that displays a list of applications that are auto-sandboxed and manually added to sandbox. Refer to the section The Sandbox for more details.

  The statistics row will be displayed only if 'Show Statistics Pane' is enabled under the Widget options of CCAV system Tray icon or Widget right click menu. Refer to section The System Tray Icon for more details. (***Default = Enabled***)
- The third row contains shortcuts for the four common tasks you have in the task bar at the bottom of the home screen. Clicking the shortcut on the widget will run the task.

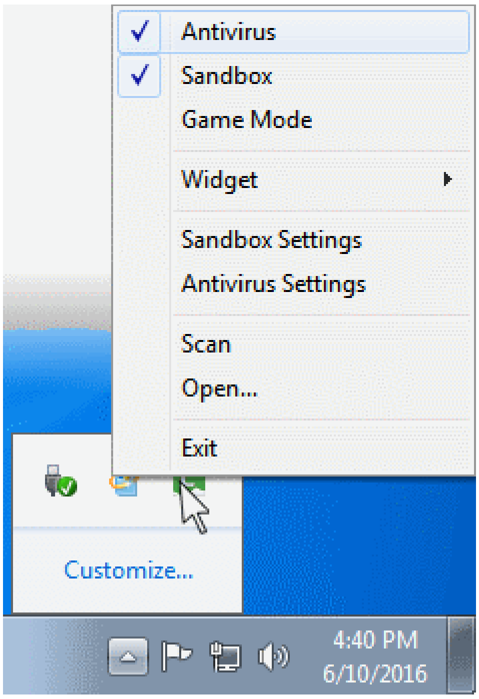
  The 'Common Tasks' row is displayed only if 'Show Common Tasks Pane' is enabled under 'Widget' options of the CCAV tray icon or the widget right-click menu. Refer to section The System Tray Icon for more details. (***Default = Enabled***)
- The fourth row contains shortcuts for browsers installed on your computer. Clicking on a browser icon will 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 'Browsers' row is displayed only if 'Show Browsers Pane' is enabled under the '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.

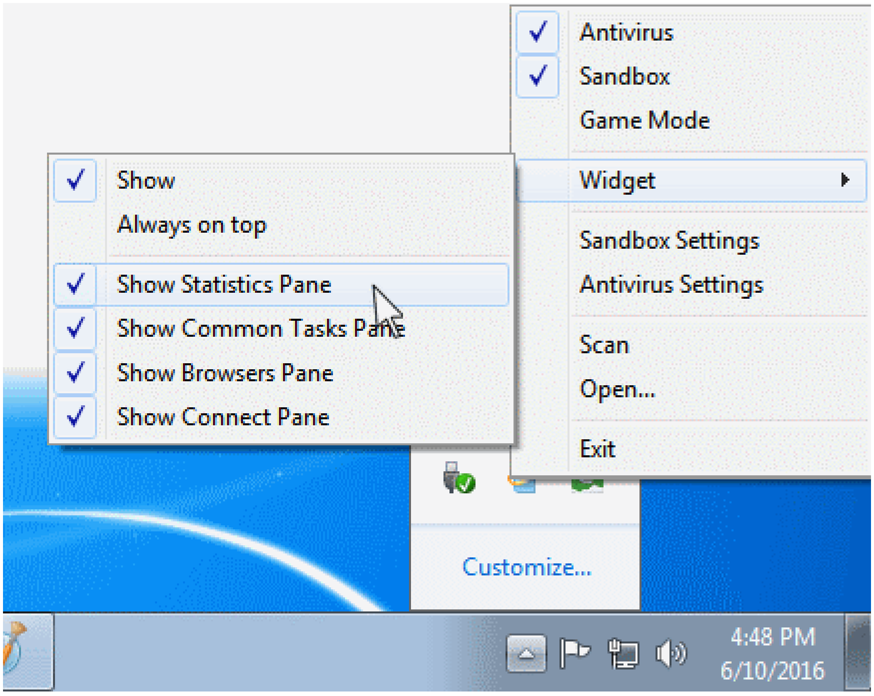
  This row is displayed only if 'Show Connect Pane' is enabled under the 'Widget' section of the CCAV tray right-click menu or the widget right-click menu. Refer to the section The System Tray Icon for more details. (***Default = Enabled***)
- The up arrow at the bottom allows you to collapse or expand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

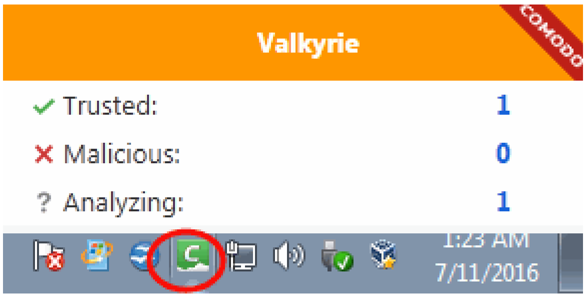


- **Antivirus** - Allows you to switch on/off AV protection settings. Tick mark indicates the protection is on.
- **Sandbox** - Allows you to switch the automatic sandbox on or off. Tick mark indicates the protection is on.
- **Game Mode** - Allows to switch on/off 'Game Mode'. Tick mark indicates 'Game Mode' is on. 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.

Comodo Cloud Antivirus will also display Valkyrie statistics if you hover your mouse over the tray icon:



Valkyrie

✓ Trusted: 1

✕ Malicious: 0

? Analyzing: 1

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

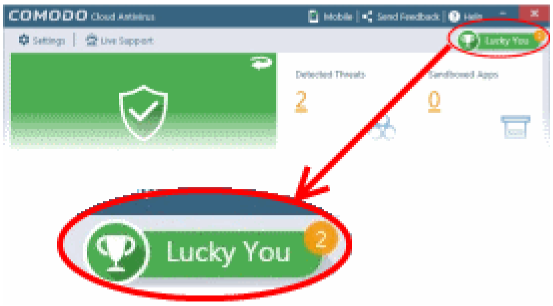
1.4. 'Lucky You' Statistics

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.

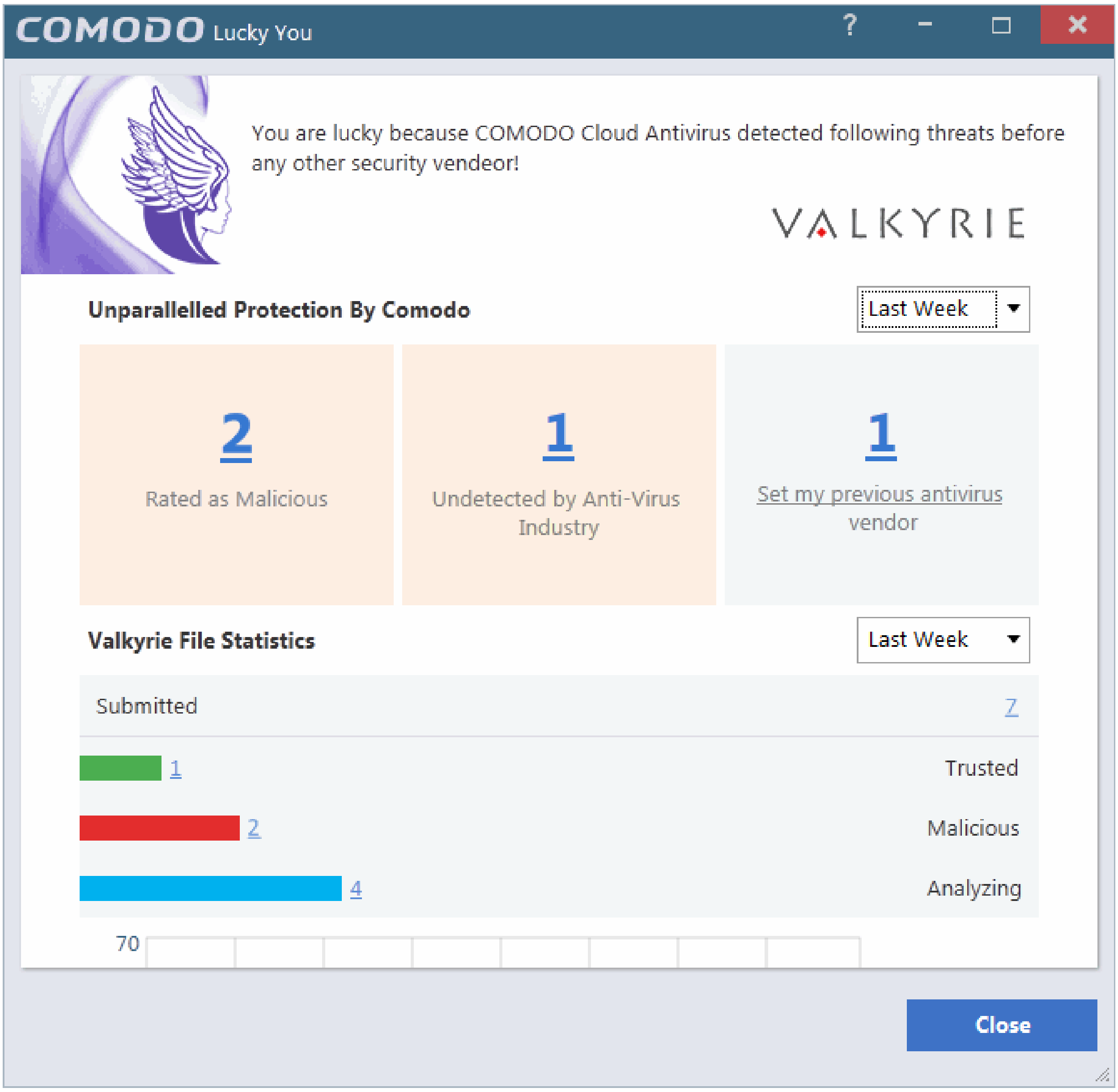
The 'Lucky' part is because traditional antivirus solutions would have allowed this malware to run on your computer. Fortunately, Comodo's Containment and Valkyrie technologies were on hand to protect you throughout. Containment kept the files locked away in a secure sandbox environment where they could do no harm while Valkyrie analysis identified the file as malware before anybody else.

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.

The number of 'Lucky You' threats that CCAV discovered is listed at the top right of the home screen:



- To view your 'Valkyrie Lucky You Statistics' details, click the 'Lucky You' button.



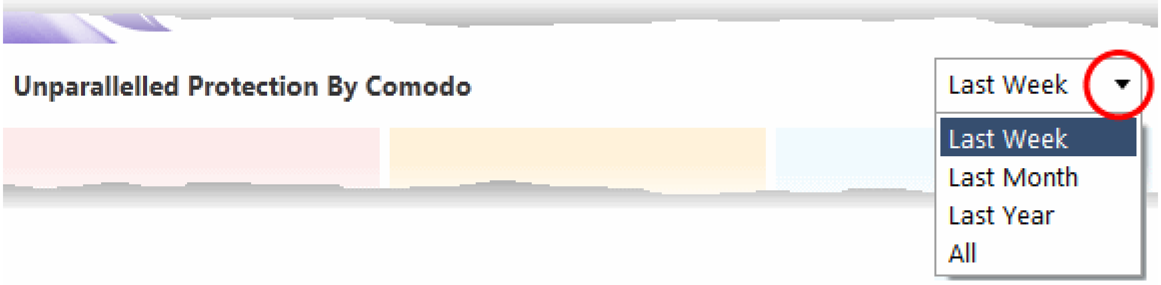
COMODO Lucky You
You are lucky because COMODO Cloud Antivirus detected following threats before any other security vendeor!
VALKYRIE
Unparallelled Protection By Comodo
Last Week
2
Rated as Malicious
1
Undetected by Anti-Virus Industry
1
Set my previous antivirus vendor
Valkyrie File Statistics
Last Week
Submitted
7
1
Trusted
2
Malicious
4
Analyzing
70
Close

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 been missed by other antivirus software vendors and statistics of files uploaded and their verdicts.

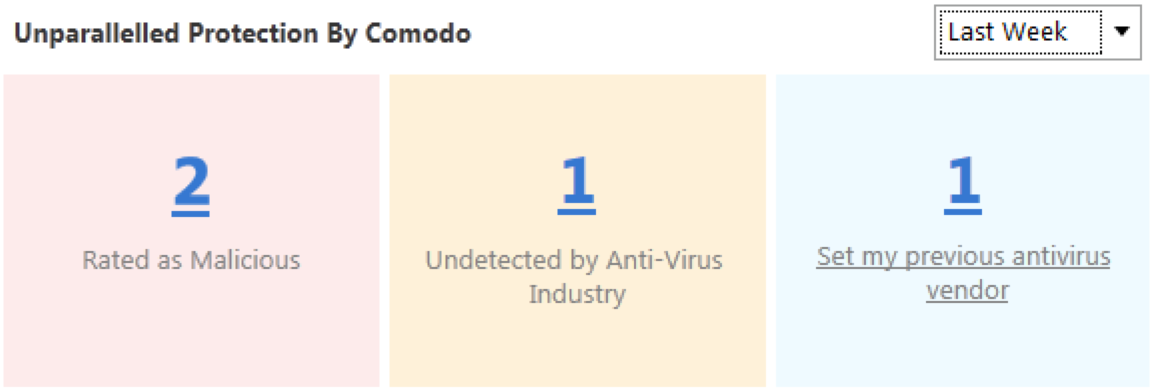
Protection by Comodo

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.



Unparallelled Protection By Comodo

Last Week

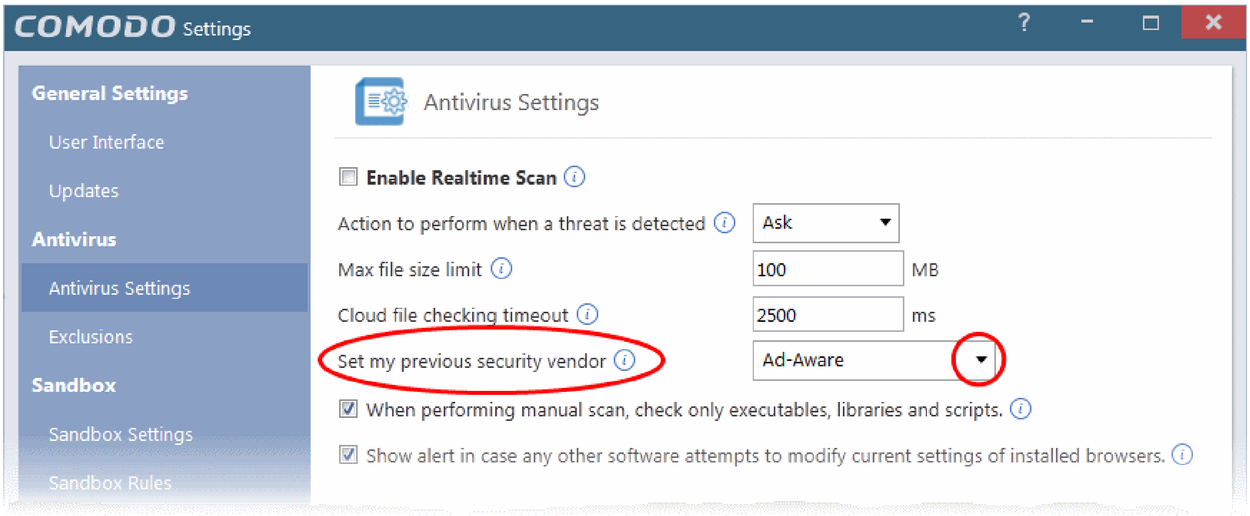
2 Rated as Malicious

1 Undetected by Anti-Virus Industry

1 Set my previous antivirus vendor

- **Rated as Malicious** - Displays the total number of items identified as malicious from your computer by Valkyrie, within the chosen period of time. Clicking the number displays 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. Clicking the number displays 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. Clicking the number displays 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 company' link to open the Antivirus Settings interface and choose the vendor from the 'Set my previous security vendor' drop-down.



COMODO Settings

Antivirus Settings

□ **Enable Realtime Scan**

Action to perform when a threat is detected: Ask

Max file size limit: 100 MB

Cloud file checking timeout: 2500 ms

Set my previous security vendor: Ad-Aware

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

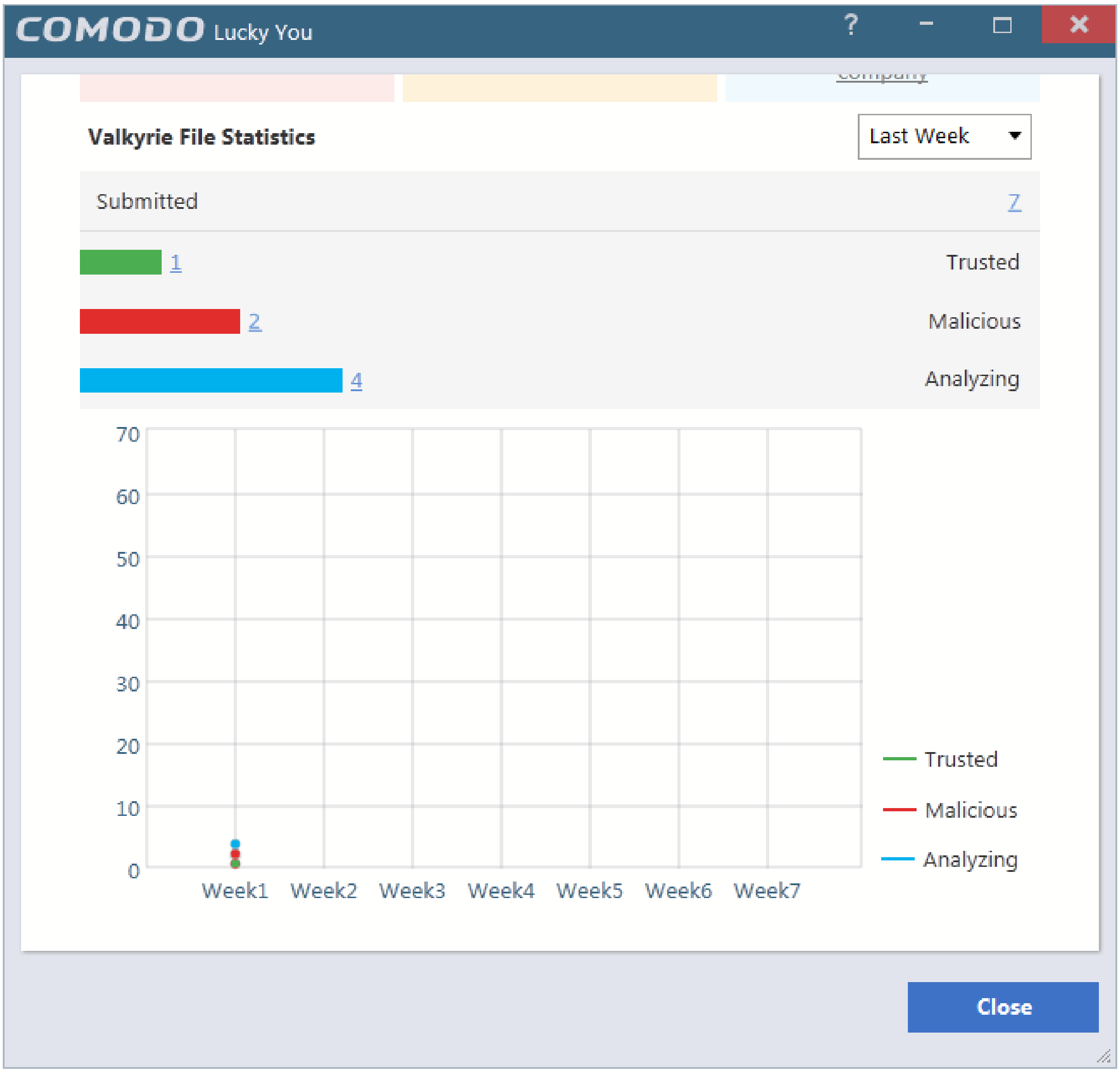
☑ Show alert in case any other software attempts to modify current settings of installed browsers.

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 at the left.

The statistics for the chosen period will be displayed as a bar chart.



COMODO Lucky You

Valkyrie File Statistics

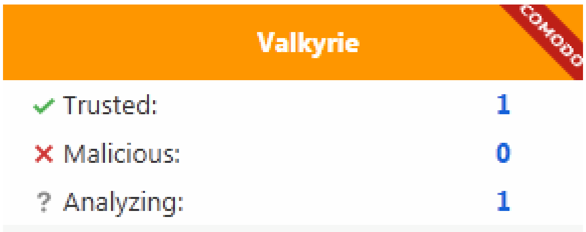
Last Week

Submitted	7
1	Trusted
2	Malicious
4	Analyzing

- Clicking on the numbers displays a list of files identified with respective verdicts.

The graph below the bar chart displays the comparison of statistics on weekly basis.

Note. You also view Valkyrie statistics at any time by placing your mouse cursor over the CCAV tray icon:



Valkyrie

✓ Trusted:	1
✕ Malicious:	0
? Analyzing:	1

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.

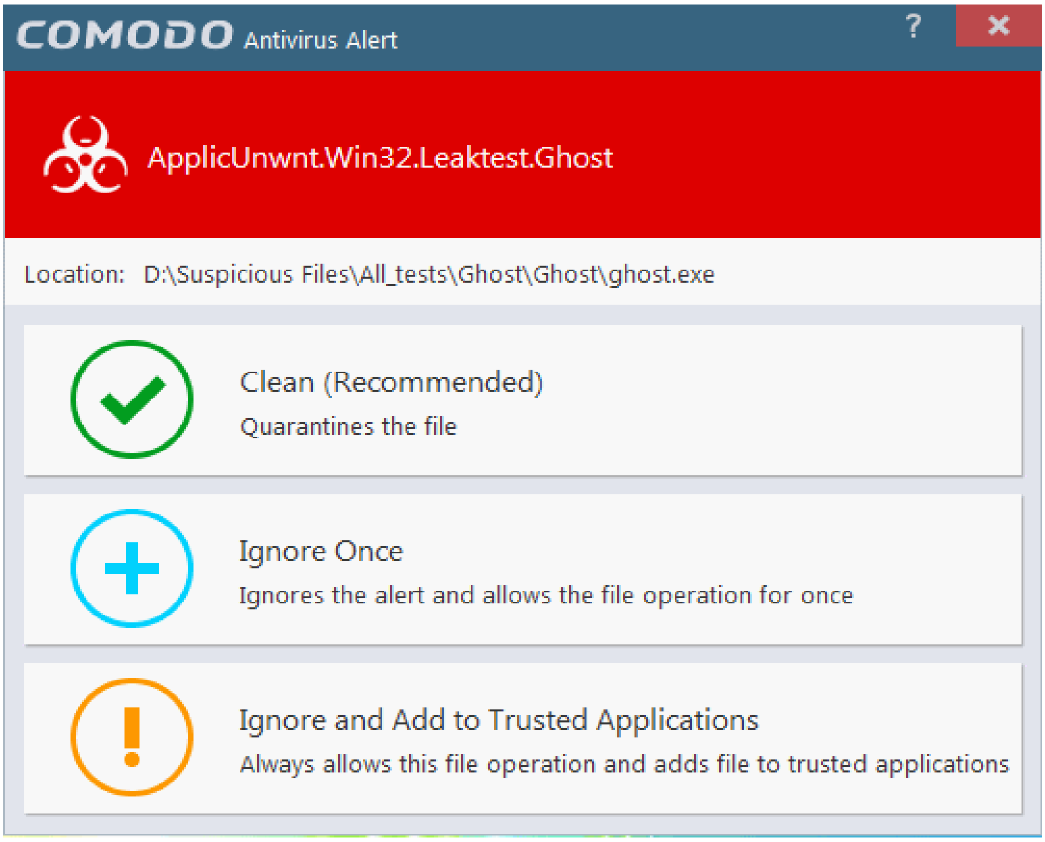
- Antivirus Alerts - Shown whenever virus or virus-like activity is detected. AV alerts will be displayed only when 'Enable Realtime Scan' is selected and the option 'Alert' for 'Action when threat is detected' is selected in Real-time Scanner Settings.
- Sandbox Alerts - Shown whenever an application 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 - Shown whenever the verdict on an 'Unknown' file submitted to Valkyrie for analysis is received from the FLS server.
- 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 Antivirus Settings.

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

Answering an Antivirus Alert

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

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



ApplicUnwnt.Win32.Leaktest.Ghost

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

Clean (Recommended)
Quarantines the file

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

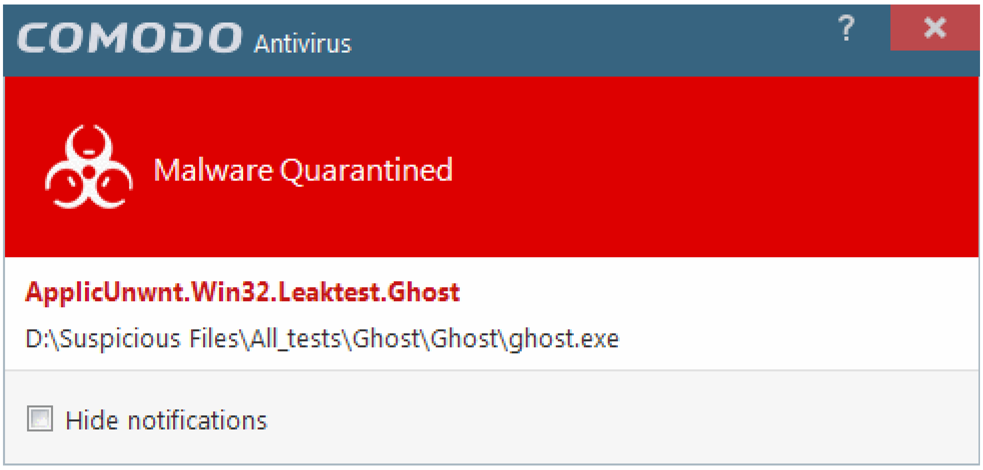
Ignore and Add to Trusted Applications
Always allows this file operation and adds file to trusted applications

The following response-options are available:

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

Antivirus Notification

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



Malware Quarantined

ApplicUnwnt.Win32.Leaktest.Ghost

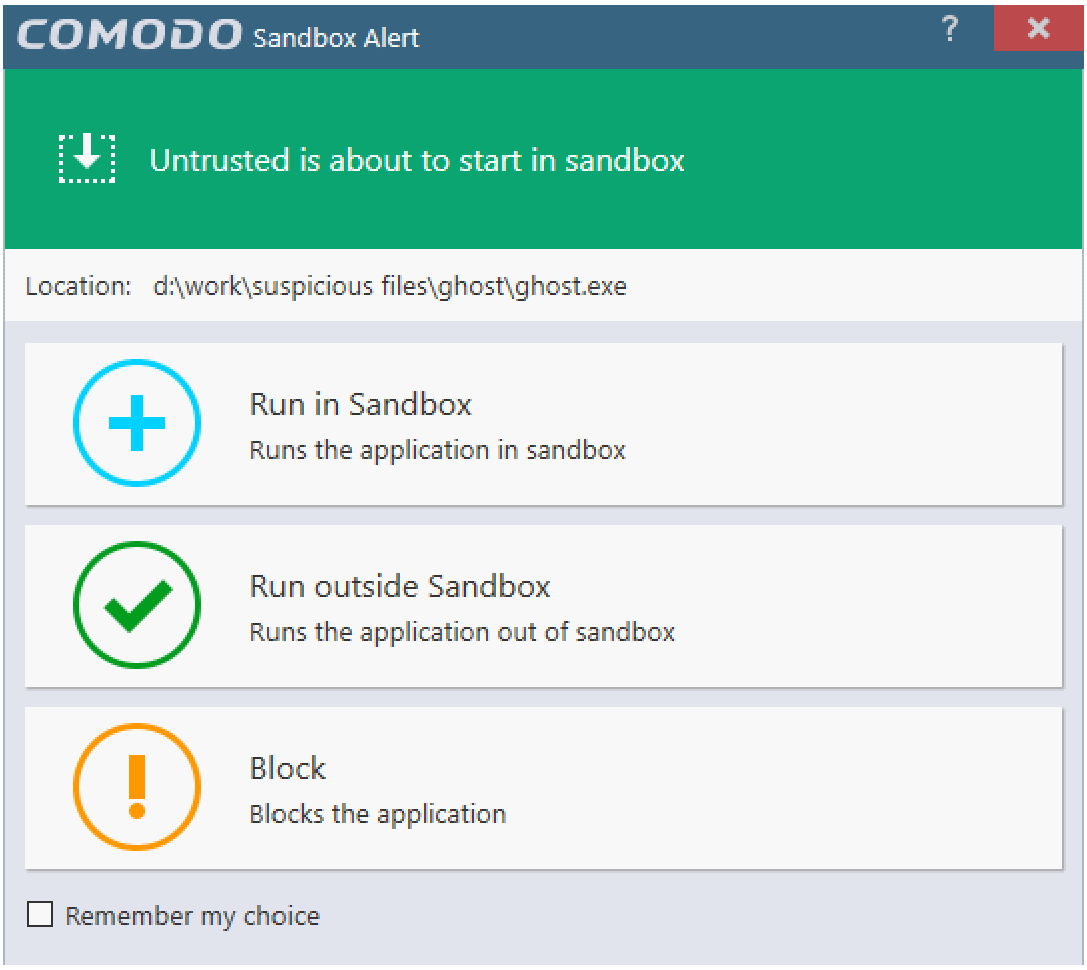
D:\Suspicious Files\All_tests\Ghost\Ghost\ghost.exe

□ Hide notifications

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

Answering a Sandbox Alert

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



COMODO Sandbox Alert

Untrusted is about to start in sandbox

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

Run in Sandbox
Runs the application in sandbox

Run outside Sandbox
Runs the application out of sandbox

Block
Blocks the application

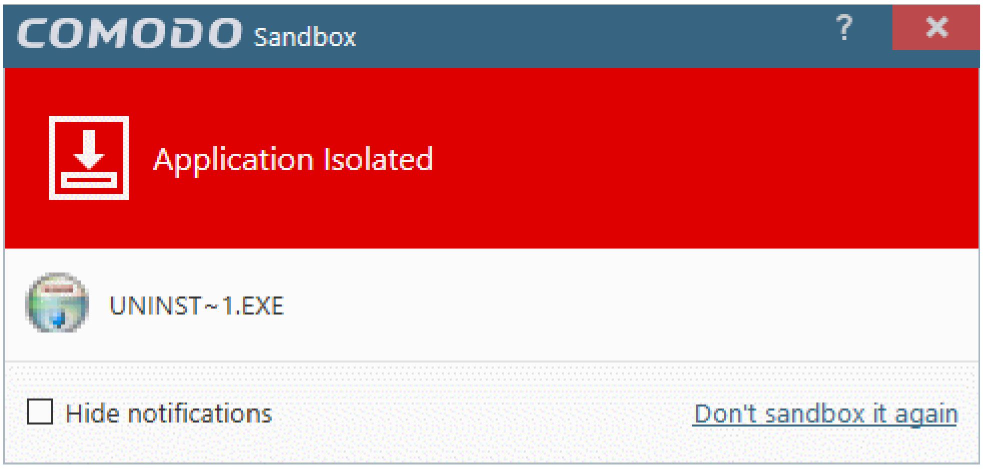
□ Remember my choice

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

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

Sandbox Notification

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



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

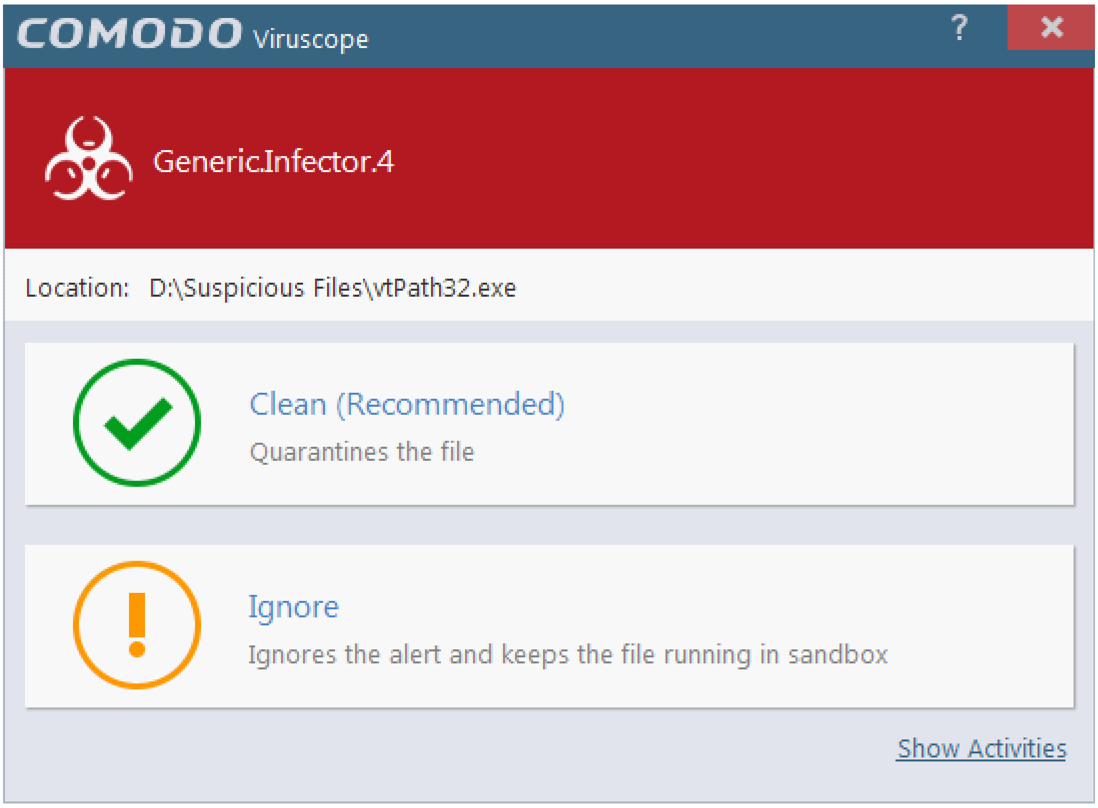
Please note that these 'Sandbox' notifications will be displayed only when you have chosen 'Sandbox all untrusted files' in the 'Sandbox Settings' interface *and* 'Show notifications' check box is enabled in 'General Settings' > 'Customize User Interface' screen.

Answering a Viruscope Alert

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

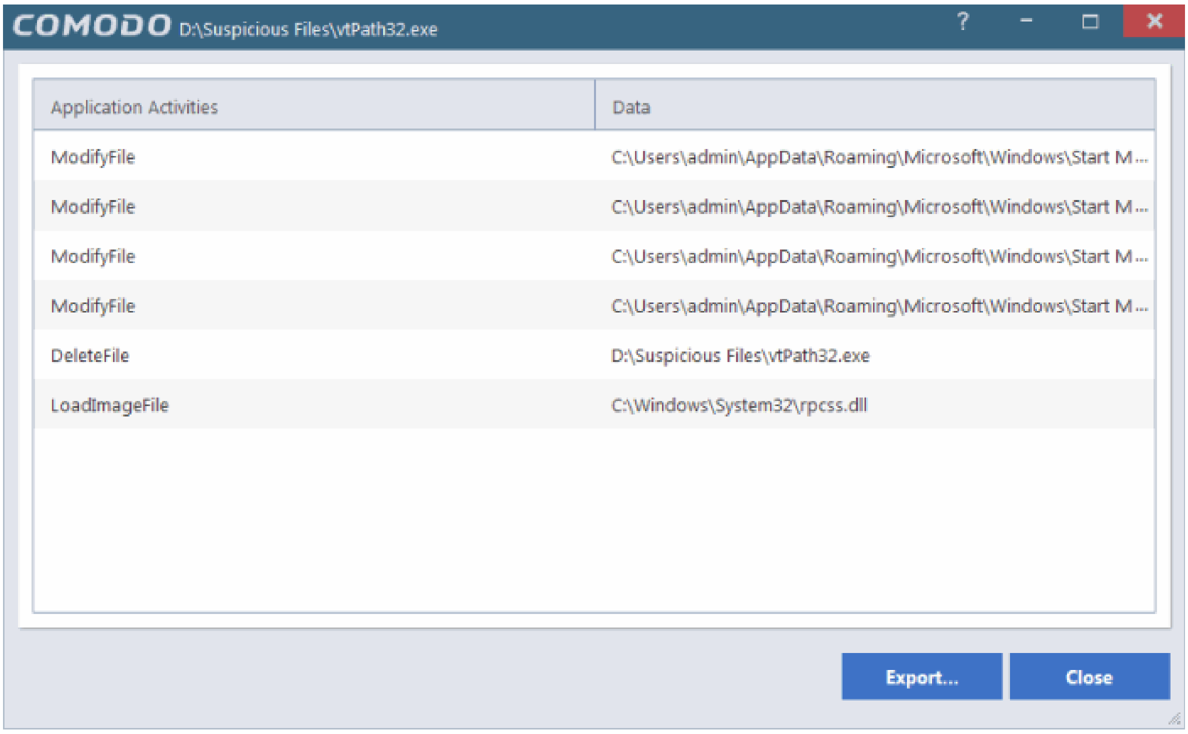
Please read the following advice before answering a Viruscope alert:

1. Carefully read the information displayed in the alert.



Location: D:\Suspicious Files\vtPath32.exe

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



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

Column Descriptions

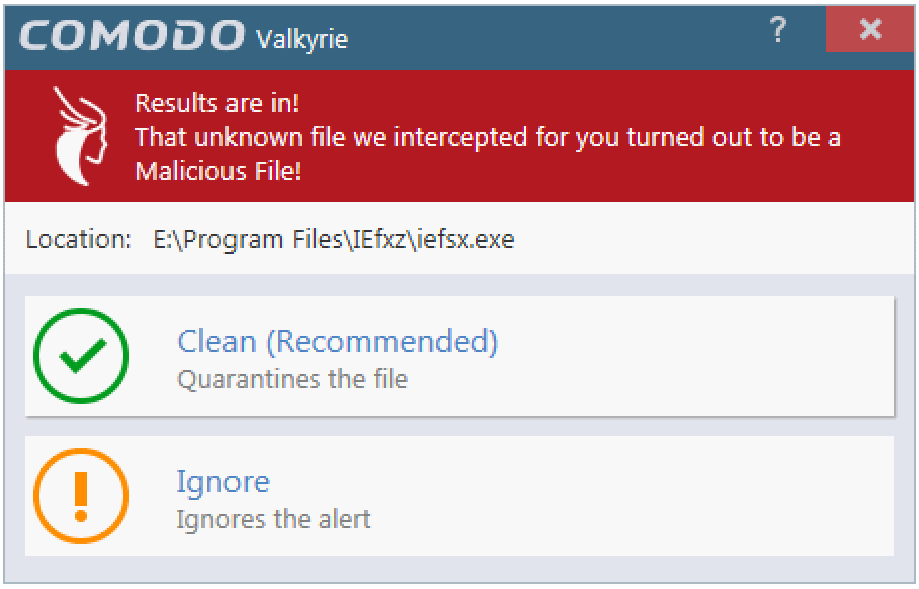
- Application Activities - Displays the activities of each of the processes run by the parent application.

- Data - Displays the file affected by the action.

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

Answering a Valkyrie Alert

CCAV displays Valkyrie alert when an 'Unknown' file automatically uploaded from a Rating Scan or a suspicious file manually uploaded for Valkyrie Analysis is found to be malicious and the verdict is returned to your computer.



Results are in!
That unknown file we intercepted for you turned out to be a Malicious File!

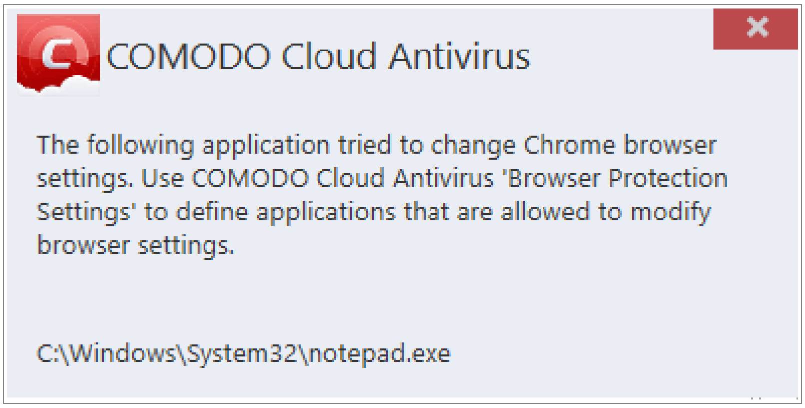
Location: E:\Program Files\IEfxz\iefsx.exe

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.

Browser Protection Alert

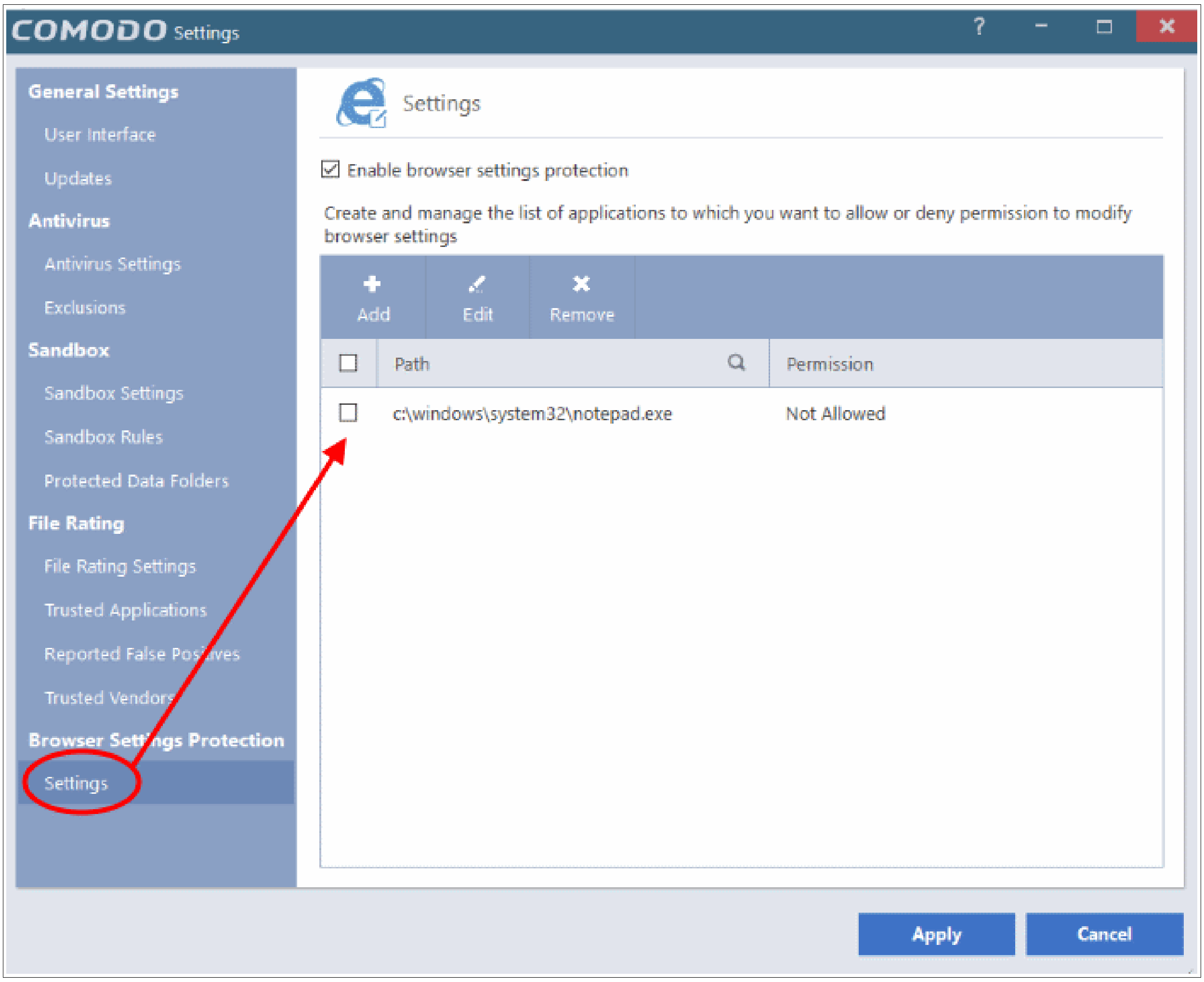
CCAV generates a Browser Protection Alert when an application tries to modify your browser settings for the first time. All such attempts by an application will be blocked but the alert message will be shown only for the first attempt for every application.



The following application tried to change Chrome browser settings. Use COMODO Cloud Antivirus 'Browser Protection Settings' to define applications that are allowed to modify browser settings.

C:\Windows\System32\notepad.exe

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.



COMODO Settings

Settings

☑ Enable browser settings protection

Create and manage the list of applications to which you want to allow or deny permission to modify browser settings

□	Path	Permission
□	c:\windows\system32\notepad.exe	Not Allowed

Note: Browser Protection Alerts will be displayed only if the option 'Enable browser protection settings' is enabled under Antivirus Settings.

2. Scan and Clean your Computer

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

To open the 'Scan' interface

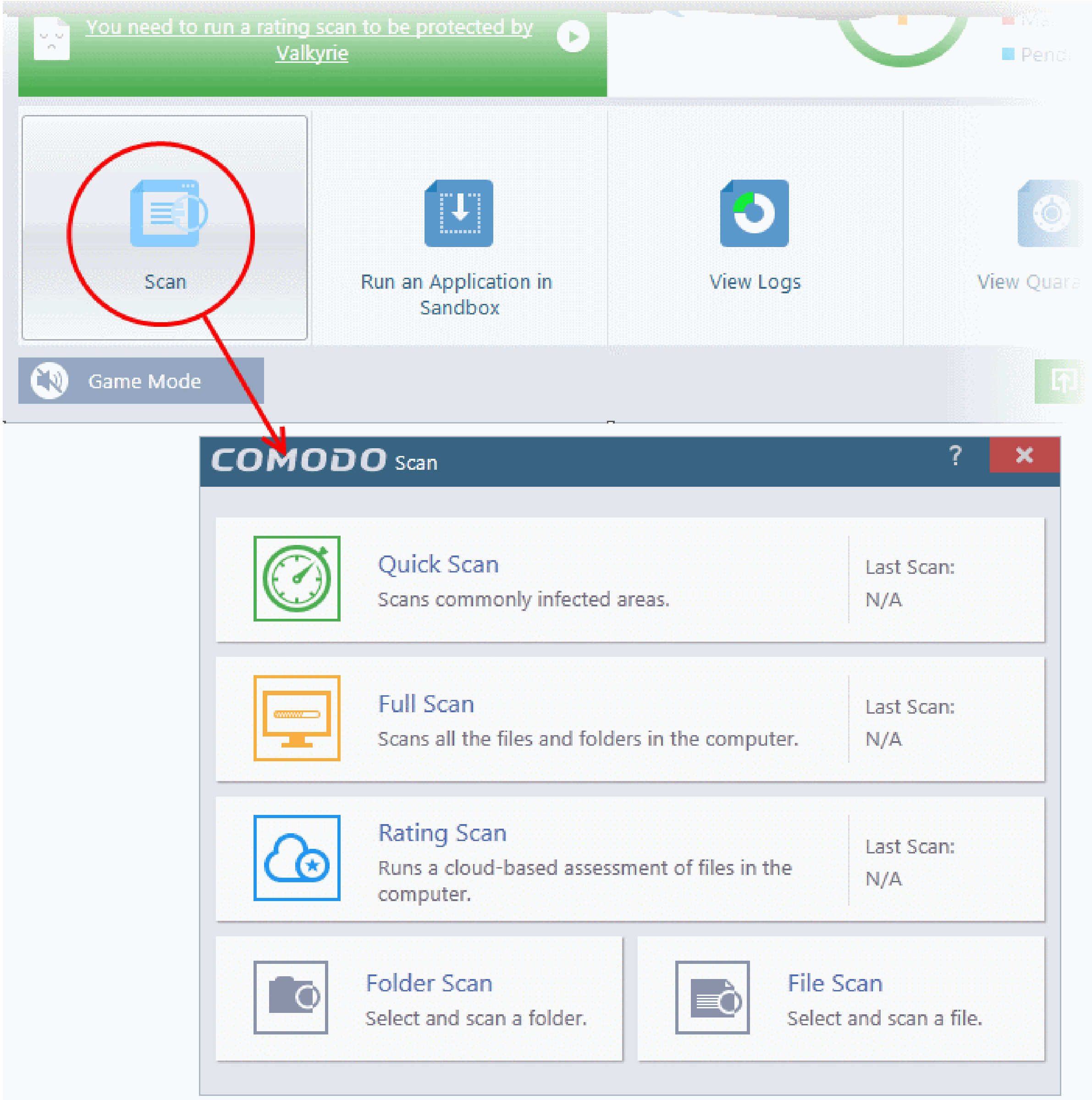
- Click 'Scan' from the 'Tasks Bar'.

OR

- Click the Scan shortcut button from the widget

OR

- Right-click on the CCAV system tray icon


You need to run a rating scan to be protected by Valkyrie
Scan
Run an Application in Sandbox
View Logs
View Quara
Game Mode
COMODO Scan
?
×

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

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

Rating Scan
Runs a cloud-based assessment of files in the computer.
Last Scan: N/A

Folder Scan
Select and scan a folder.

File Scan
Select and scan a file.

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

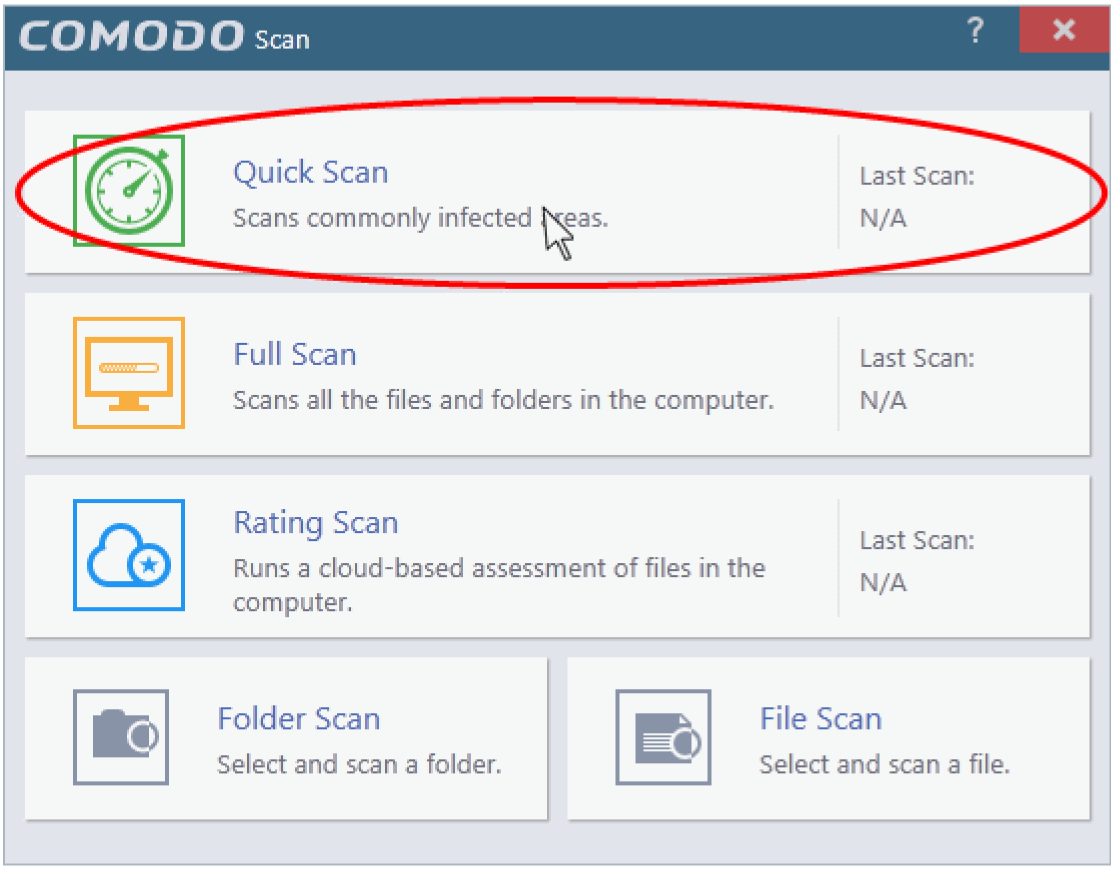
- Run a Quick Scan
- Run a Full Computer Scan
- Run a Rating Scan
- Run a Custom Scan
  - Scan a Folder
  - Scan a File
- Processing Infected Files
- Managing Detected Threats
- Viewing Valkyrie Analysis Results

2.1. Run a Quick Scan

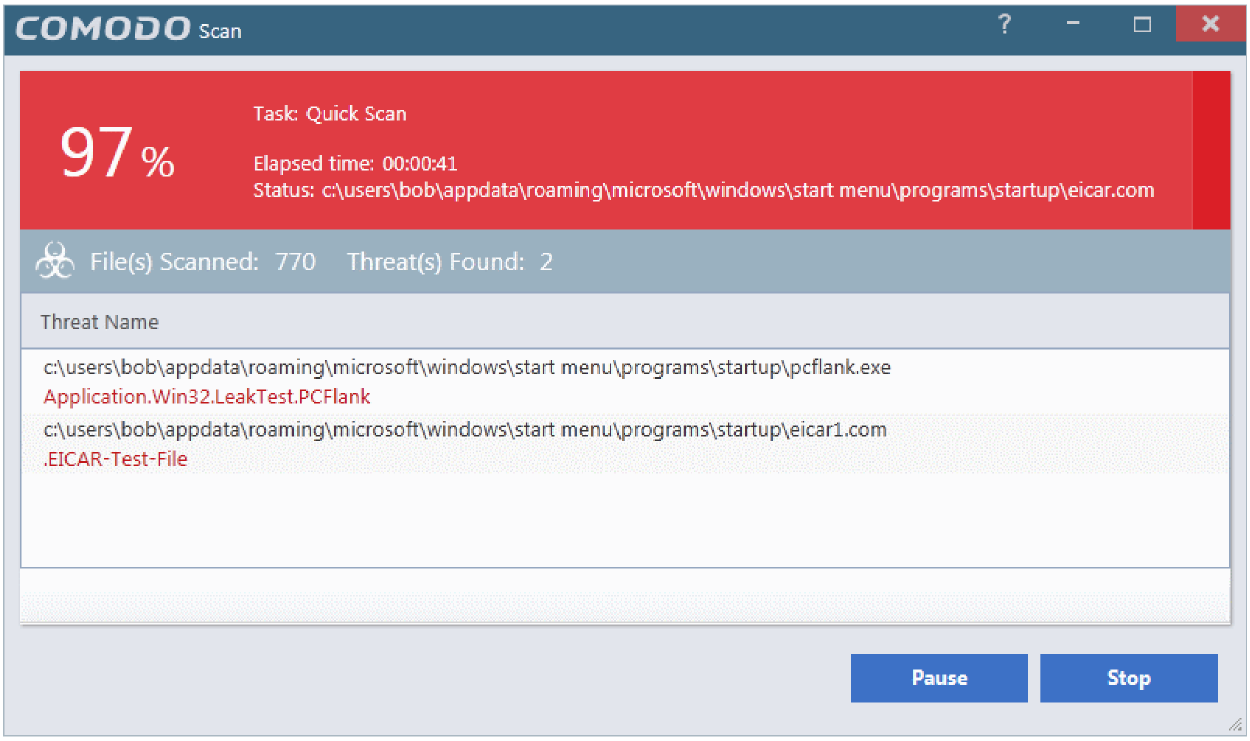
The 'Quick Scan' feature enables you to quickly scan those important areas of your computer which are highly prone to infection. Areas scanned include system memory, auto-run entries, hidden services, boot sectors and other significant areas like important registry keys and system files. These areas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

- Open the 'Scan' interface by clicking 'Scan' from the 'Task bar' or clicking on the scan button from the widget and click 'Quick Scan'.


COMODO Scan
?
Quick Scan
Scans commonly infected areas.
Last Scan:
N/A
Full Scan
Scans all the files and folders in the computer.
Last Scan:
N/A
Rating Scan
Runs a cloud-based assessment of files in the computer.
Last Scan:
N/A
Folder Scan
Select and scan a folder.
File Scan
Select and scan a file.

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



COMODO Scan

97 %

Task: Quick Scan

Elapsed time: 00:00:41

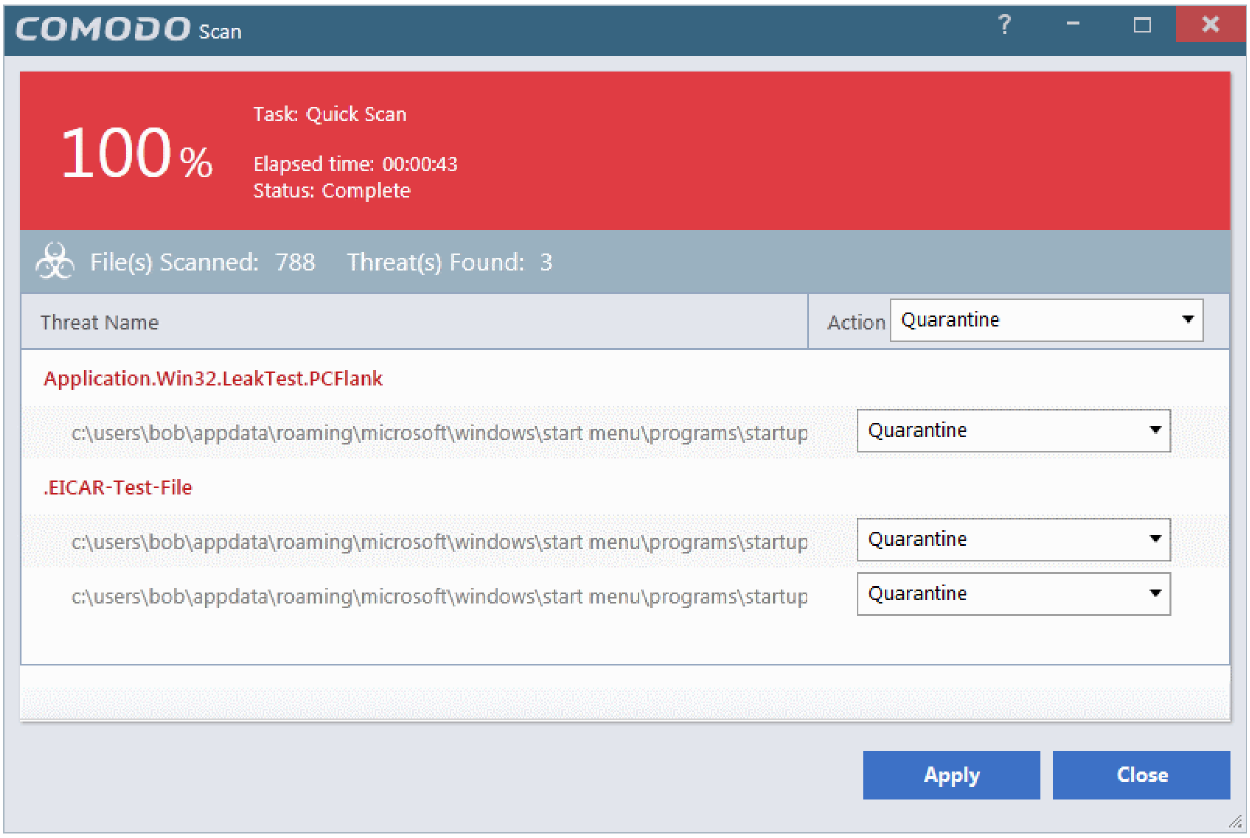
Status: c:\users\bob\appdata\roaming\microsoft\windows\start menu\programs\startup\eicar.com

File(s) Scanned: 770 Threat(s) Found: 2

Threat Name
c:\users\bob\appdata\roaming\microsoft\windows\start menu\programs\startup\pcflank.exe Application.Win32.LeakTest.PCFlank
c:\users\bob\appdata\roaming\microsoft\windows\start menu\programs\startup\eicar1.com .EICAR-Test-File

- 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.



COMODO Scan

100 %

Task: Quick Scan

Elapsed time: 00:00:43

Status: Complete

File(s) Scanned: 788 Threat(s) Found: 3

Threat Name	Action: Quarantine
Application.Win32.LeakTest.PCFlank	
c:\users\bob\appdata\roaming\microsoft\windows\start menu\programs\startup	Quarantine
.EICAR-Test-File	
c:\users\bob\appdata\roaming\microsoft\windows\start menu\programs\startup	Quarantine
c:\users\bob\appdata\roaming\microsoft\windows\start menu\programs\startup	Quarantine

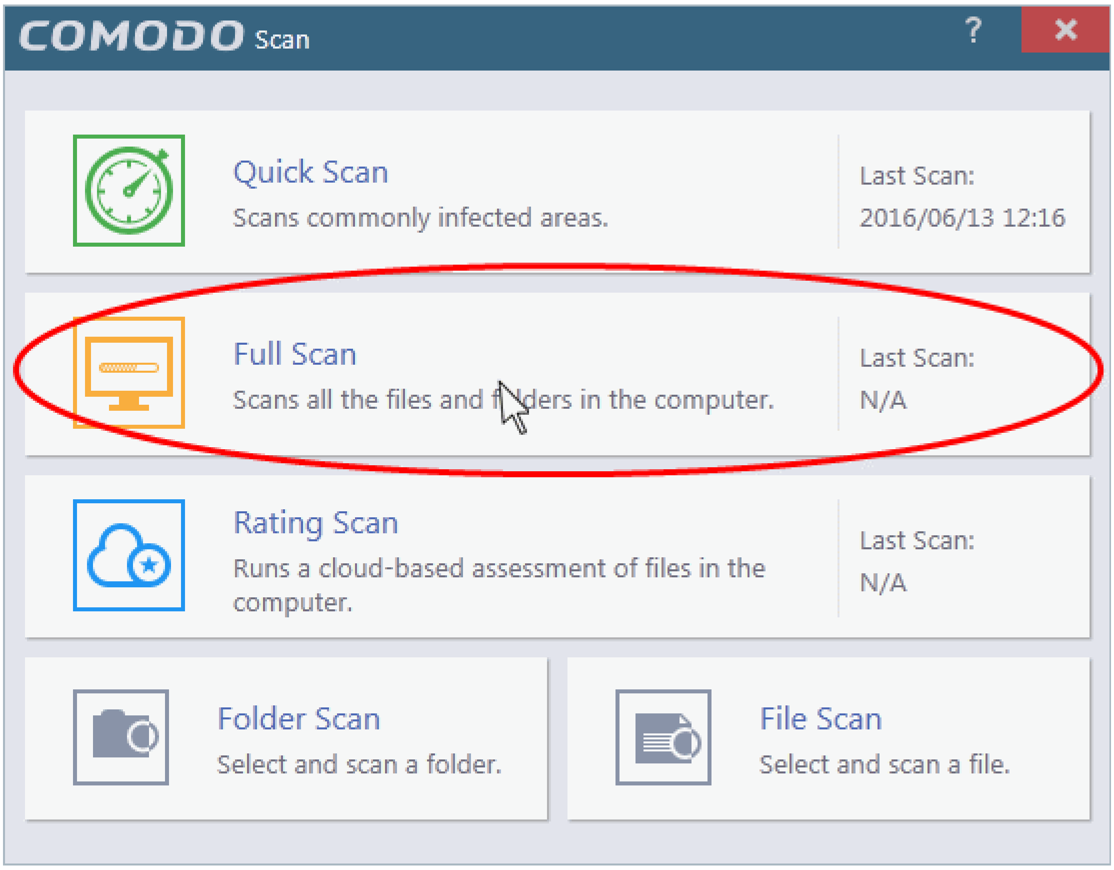
The results window shows the list of objects scanned and the number of threats (Viruses, Rootkits, Malware). Use the drop-down menu to choose whether to clean, move to quarantine or ignore the threat. Refer to Processing the infected files for more details.

2.2. Run a Full Computer Scan

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

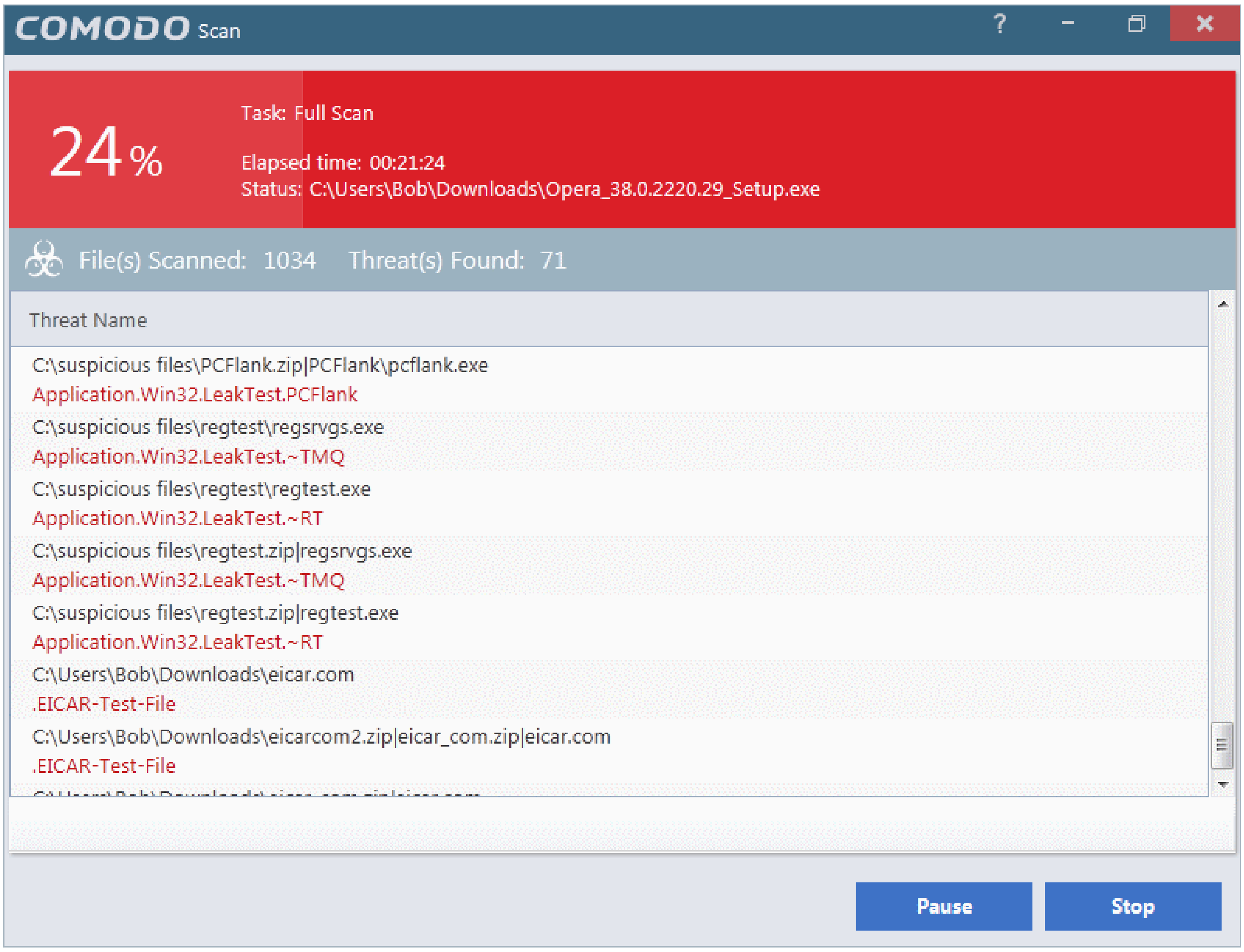
To run a Full Computer Scan

- 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:



COMODO Scan
?
×
Quick Scan
Scans commonly infected areas.
Last Scan:
2016/06/13 12:16
Full Scan
Scans all the files and folders in the computer.
Last Scan:
N/A
Rating Scan
Runs a cloud-based assessment of files in the computer.
Last Scan:
N/A
Folder Scan
Select and scan a folder.
File Scan
Select and scan a file.

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



24%

Task: Full Scan

Elapsed time: 00:21:24

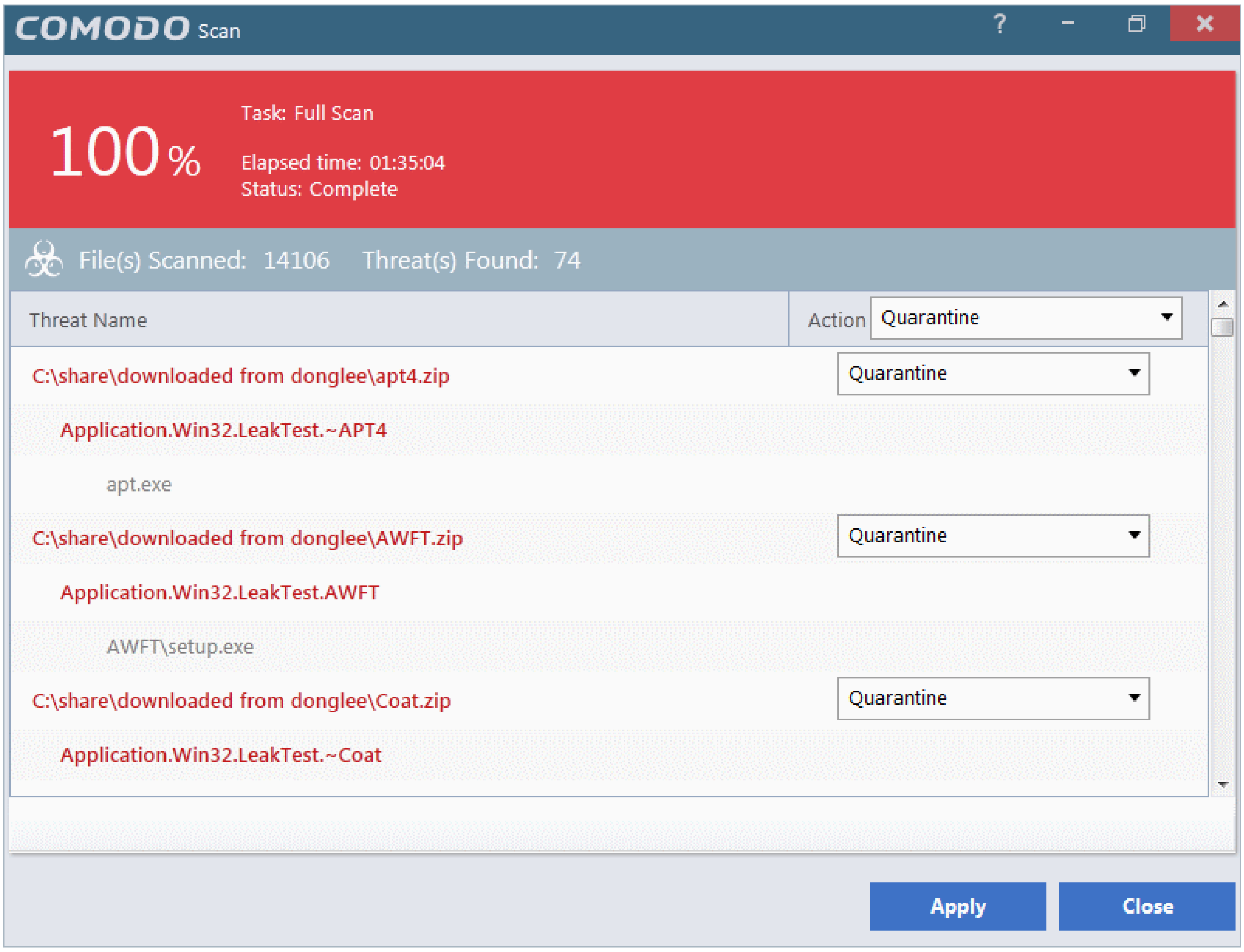
Status: C:\Users\Bob\Downloads\Opera_38.0.2220.29_Setup.exe

File(s) Scanned: 1034 Threat(s) Found: 71

Threat Name
C:\suspicious files\PCFlank.zip|PCFlank\pcflank.exe Application.Win32.LeakTest.PCFlank
C:\suspicious files\regtest\regsrvgs.exe Application.Win32.LeakTest.~TMQ
C:\suspicious files\regtest\regtest.exe Application.Win32.LeakTest.~RT
C:\suspicious files\regtest.zip|regsrvgs.exe Application.Win32.LeakTest.~TMQ
C:\suspicious files\regtest.zip|regtest.exe Application.Win32.LeakTest.~RT
C:\Users\Bob\Downloads\eicar.com .EICAR-Test-File
C:\Users\Bob\Downloads\eicarcom2.zip|eicar_com.zip|eicar.com .EICAR-Test-File

- 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.



COMODO Scan

100 %

Task: Full Scan

Elapsed time: 01:35:04

Status: Complete

File(s) Scanned: 14106 Threat(s) Found: 74

Threat Name	Action: Quarantine
C:\share\downloaded from donglee\apt4.zip	Quarantine
Application.Win32.LeakTest.~APT4	
apt.exe	
C:\share\downloaded from donglee\AWFT.zip	Quarantine
Application.Win32.LeakTest.AWFT	
AWFT\setup.exe	
C:\share\downloaded from donglee\Coat.zip	Quarantine
Application.Win32.LeakTest.~Coat	

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

2.3. Run a Rating Scan

The 'Rating Scan' feature runs a cloud-based assessment on files on your computer to assess how trustworthy they are.

Based on the trustworthiness, the files are rated as:

- **Trusted** - the file is safe
- **Unknown** - the trustworthiness of the file could not be assessed. If configured for auto-submission in the 'Sandbox Settings' interface, CCAV will automatically upload the unknown files to Valkyrie for analysis. Refer to the section Sandbox Settings for more details.

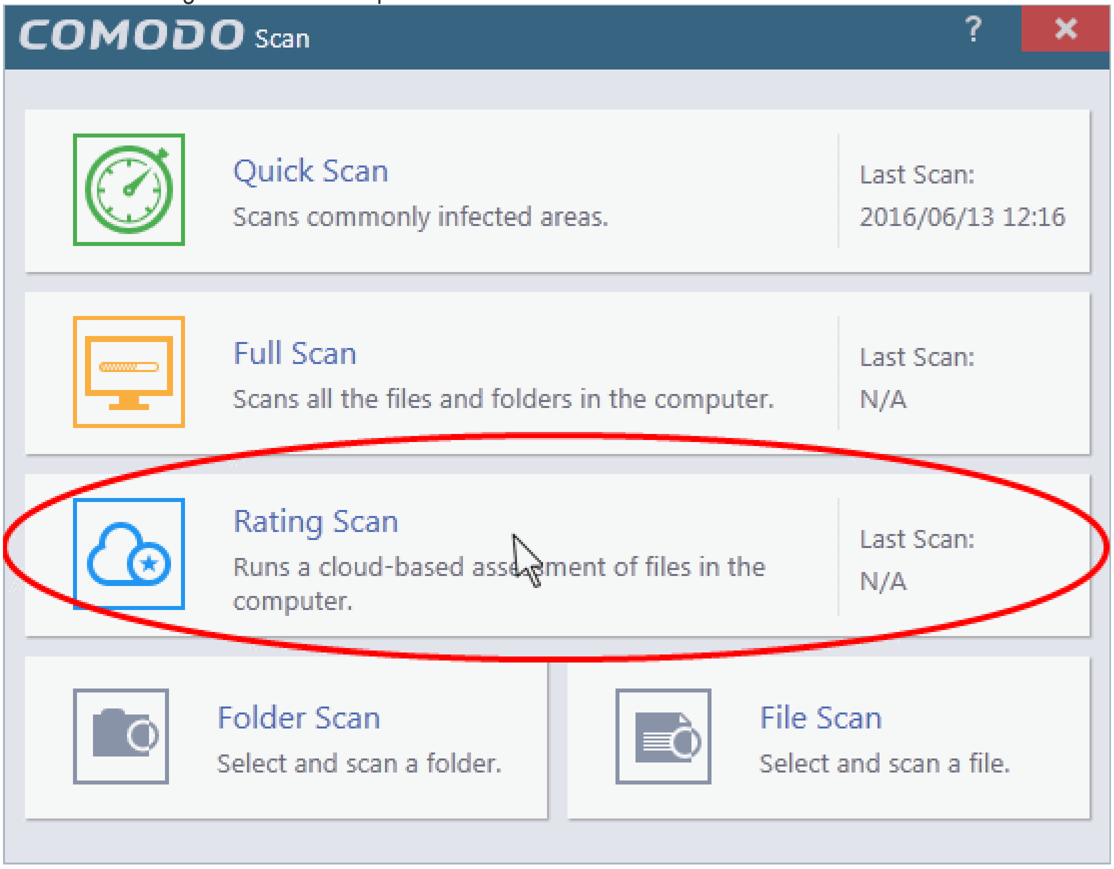
  If not enabled, you will be given an option to manually upload them for Valkyrie Analysis.

  The files will be analyzed with a range of static and behavioral checks at Comodo and the results will be sent back to your CCAV installation. You can view the results from the CCAV interface. Refer to the section Viewing Valkyrie Analysis Results for more details. Also, depending on the nature of each file, it will be added to the global blacklist or whitelist.
- **Malicious** - The file is unsafe and may contain malicious code. You will be presented with disinfection options for such files.

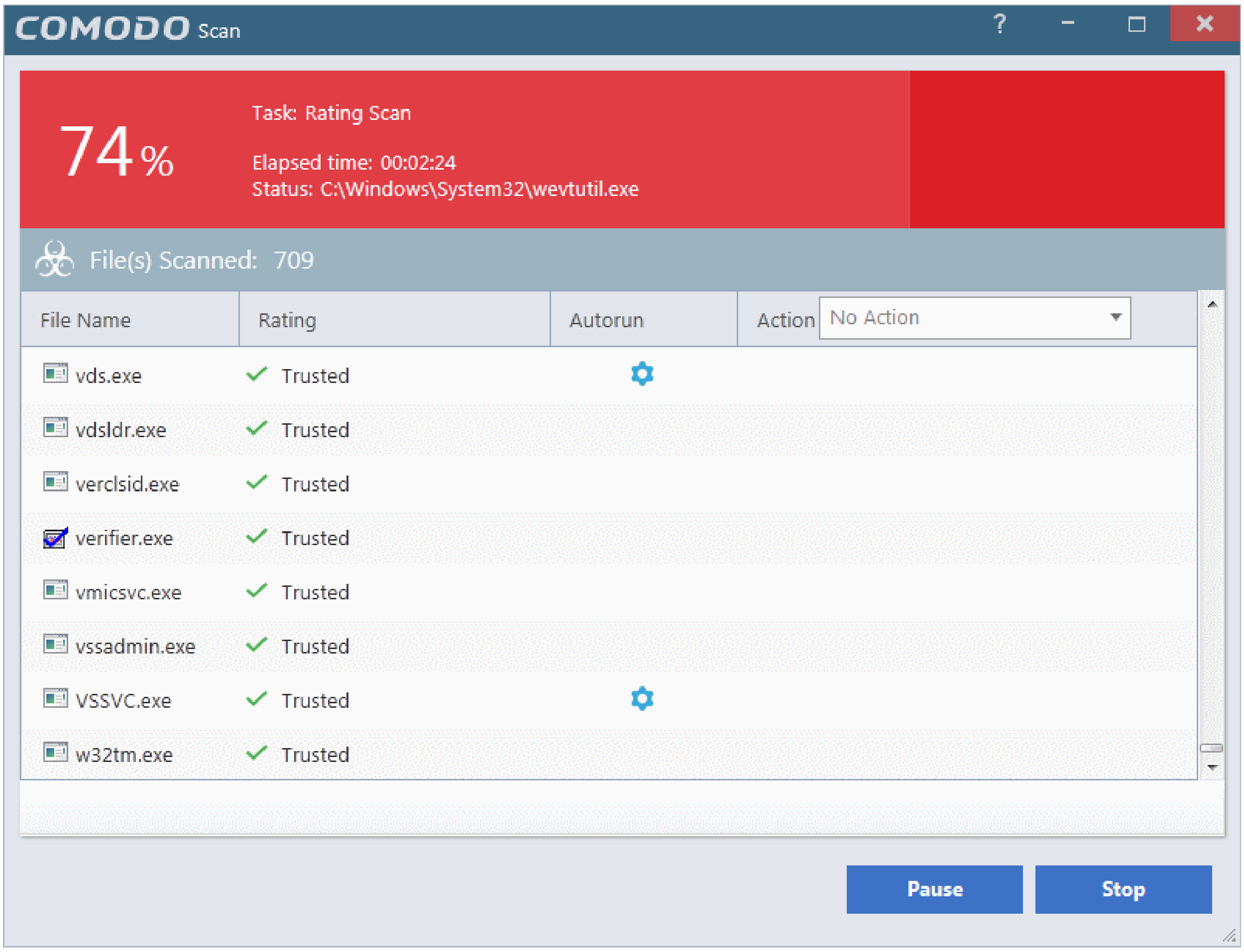
To run a Rating scan

- Open the 'Scan' interface by clicking 'Scan' on the CCAV home screen, or by clicking on the scan button on the widget

- Choose 'Rating Scan' from the options:


COMODO Scan
?
Quick Scan
Scans commonly infected areas.
Last Scan:
2016/06/13 12:16
Full Scan
Scans all the files and folders in the computer.
Last Scan:
N/A
Rating Scan
Runs a cloud-based assessment of files in the computer.
Last Scan:
N/A
Folder Scan
Select and scan a folder.
File Scan
Select and scan a file.

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



Task: Rating Scan

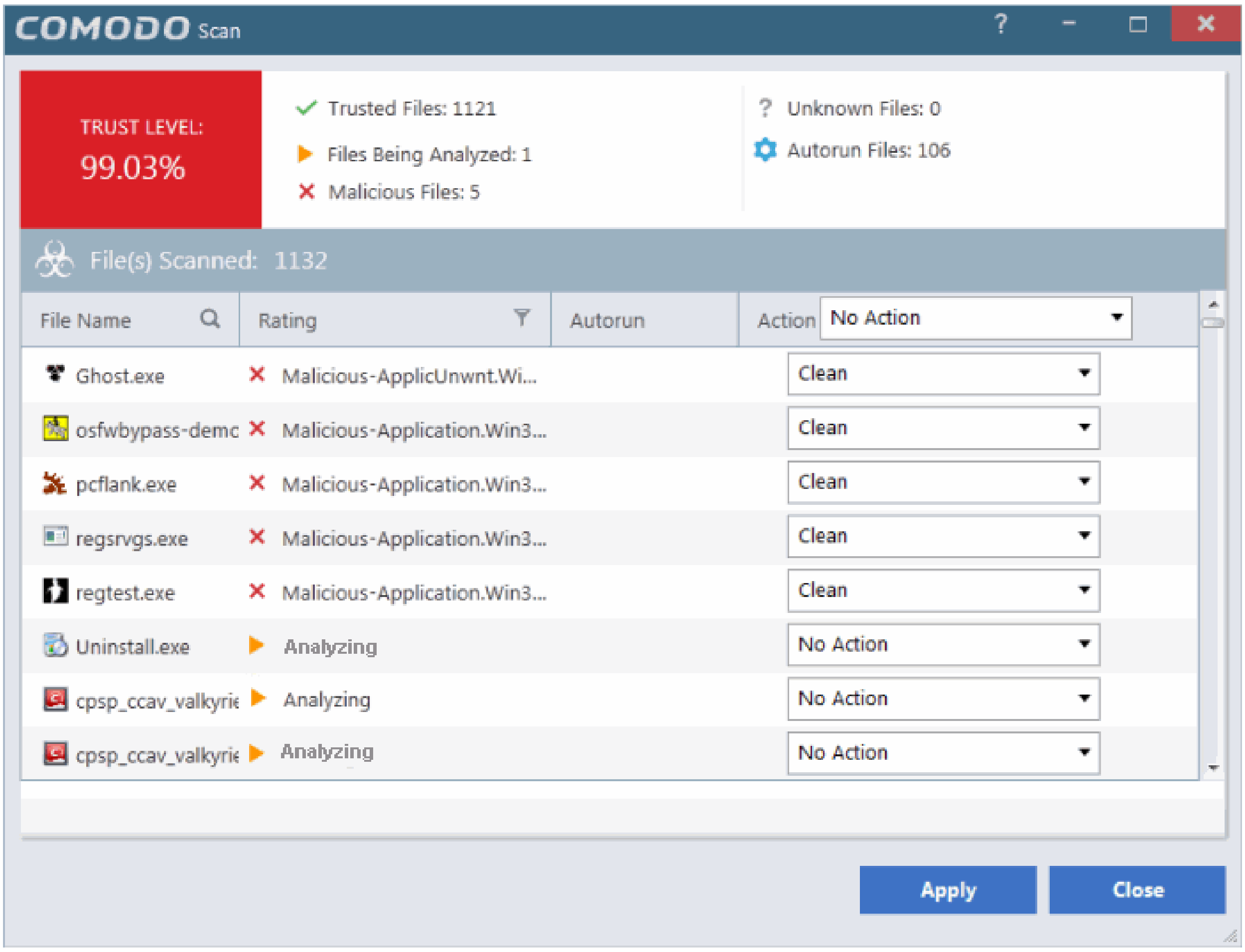
Elapsed time: 00:02:24
Status: C:\Windows\System32\wevtutil.exe

File(s) Scanned: 709

File Name	Rating	Autorun	Action: No Action
vds.exe	✓ Trusted	⚙	
vdsldr.exe	✓ Trusted		
verclsid.exe	✓ Trusted		
verifier.exe	✓ Trusted		
vmicsvc.exe	✓ Trusted		
vssadmin.exe	✓ Trusted		
VSSVC.exe	✓ Trusted	⚙	
w32tm.exe	✓ Trusted		

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

After the cloud scanners have finished their analysis, file ratings will be displayed as follows:



TRUST LEVEL: 99.03%

✓ Trusted Files: 1121

Files Being Analyzed: 1

✗ Malicious Files: 5

? Unknown Files: 0

Autorun Files: 106

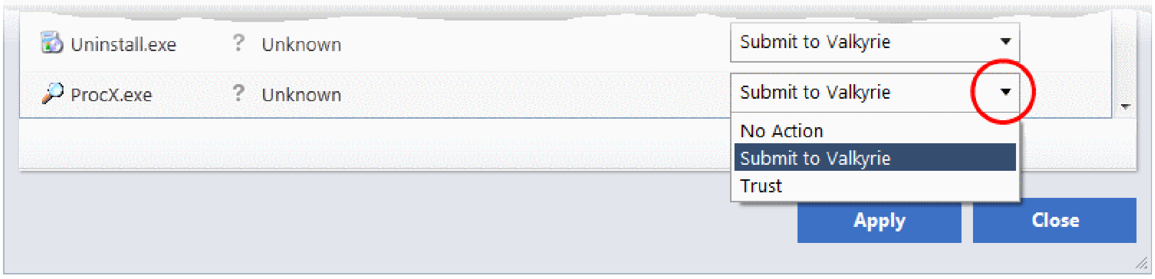
File(s) Scanned: 1132

File Name	Rating	Autorun	Action: No Action
Ghost.exe	✗ Malicious-ApplicUnwnt.Wi...		Clean
osfwbypass-demc	✗ Malicious-Application.Win3...		Clean
pcflank.exe	✗ Malicious-Application.Win3...		Clean
regsrvgs.exe	✗ Malicious-Application.Win3...		Clean
regtest.exe	✗ Malicious-Application.Win3...		Clean
Uninstall.exe	Analyzing		No Action
cpsp_ccav_valkyrie	Analyzing		No Action
cpsp_ccav_valkyrie	Analyzing		No Action

The results screen will display the trust level of files on your computer and a summary of number of files with different trust ratings.

- **File Name**: The file which was scanned
- **Rating**: The rating of the file as per the cloud based analysis. The possible ratings are:
    - **Trusted** - Indicates that the file is trustworthy, as per the cloud based file lookup service (FLS)
    - **Malicious** - Indicates that the file was found to be malicious by the FLS
    - **Unknown** - Indicates that the file is new and unknown to the File Lookup server. If auto-submission is enabled in CCAV, the file will be automatically uploaded for Valkyrie analysis. The file will be subjected to various automated and manual static and behavioral tests, and the results will be sent back to your computer. If auto-submission is not enabled, you can manually choose to upload the file from the drop-down options at the right.
    - **Analyzing** - Indicates that the file has been already submitted for Valkyrie analysis and it is under processing. The verdict will be available once analysis is complete.
- **Autorun**: Indicates whether the file is an auto-run file or not. Malicious auto-run files could be ruinous to your computer so we advise you clean or quarantine them immediately.
- **Action**: The drop-down provides options for actions that can be carried out of the file depending on its trust level.

  For files identified as '**Unknown**', the 'Action' drop-down displays the following options:



Uninstall.exe	? Unknown	Submit to Valkyrie
ProcX.exe	? Unknown	Submit to Valkyrie

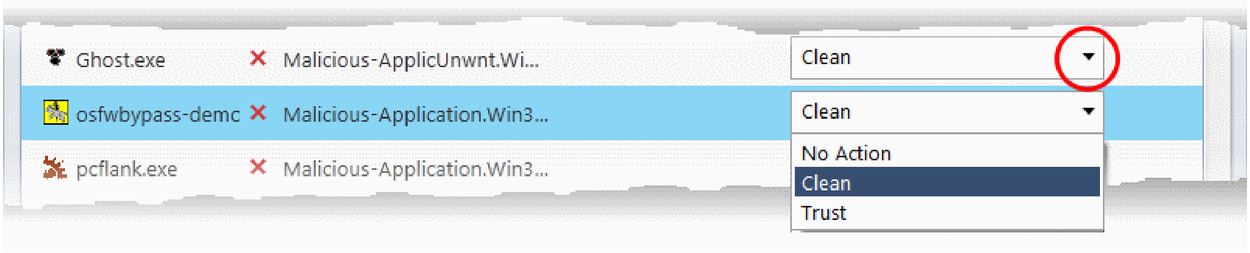
- **No Action** - If you wish to ignore the file, select 'No Action'. Use this option with caution. By choosing to neither 'Submit' nor 'Trust', this file will be detected by the next ratings scan that you run.
- **Submit to Valkyrie** - Selecting this option uploads the file to Valkyrie for analysis. This option is available only if auto-submission is not enabled from the 'Sandbox Settings' interface. Refer to the section Sandbox Settings for more details.
- **Trust** - Awards trusted status to the file. It will be given 'Trusted' rating from the next scan.

For the same action to be applied to all 'Unknown' files, make a selection from the drop-down menu at the top of the 'Action' column.

For files identified as '**Pending**', the 'Action' drop-down displays the following options:

- **No Action** - If you wish to ignore the file, select 'No Action'. Use this option with caution. By choosing not to 'Trust', this file will be detected by the next ratings scan that you run.
- **Trust** - Awards trusted status to the file. It will be given 'Trusted' rating from the next scan.

For files identified as '**Malicious**', the 'Action' drop-down displays the following options:



Ghost.exe	✕ Malicious-ApplicUnwnt.Wi...	Clean
osfwbypass-demc	✕ Malicious-Application.Win3...	Clean
pcflank.exe	✕ Malicious-Application.Win3...	

- **Clean** - If a disinfection routine is available for the selected infection(s), Comodo Antivirus will disinfect the application and retain the application file. If a disinfection routine is not available, Comodo Antivirus will move the files to Quarantine for later analysis. See Manage Quarantined Items for more info.
- **No Action** - If you wish to ignore the file, select 'No Action'. Use this option with caution. By choosing to neither 'Clean' nor 'Trust', this file will be detected by the next ratings scan that you run.
- **Trust** - The file assigned Trusted status in the File List and will be given 'Trusted' rating from the next scan.

For the same action to be applied to all 'Malicious' files, make a selection from the drop-down menu at the top of the 'Action' column.

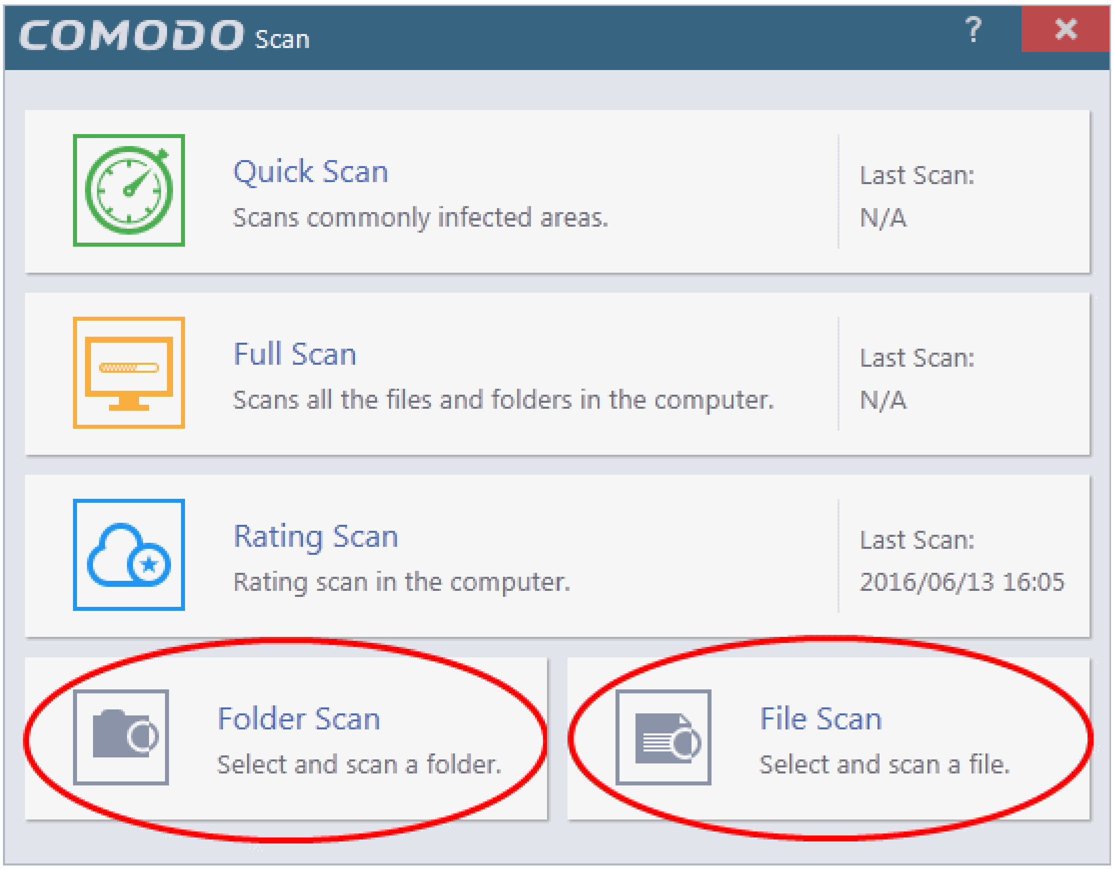
- Click 'Apply' to implement your choices for the items. The selected actions will be applied.

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 clicking on the scan button from the widget and click.'Folder Scan' or 'File Scan' from the 'Scan' interface.



The following sections explain more on:

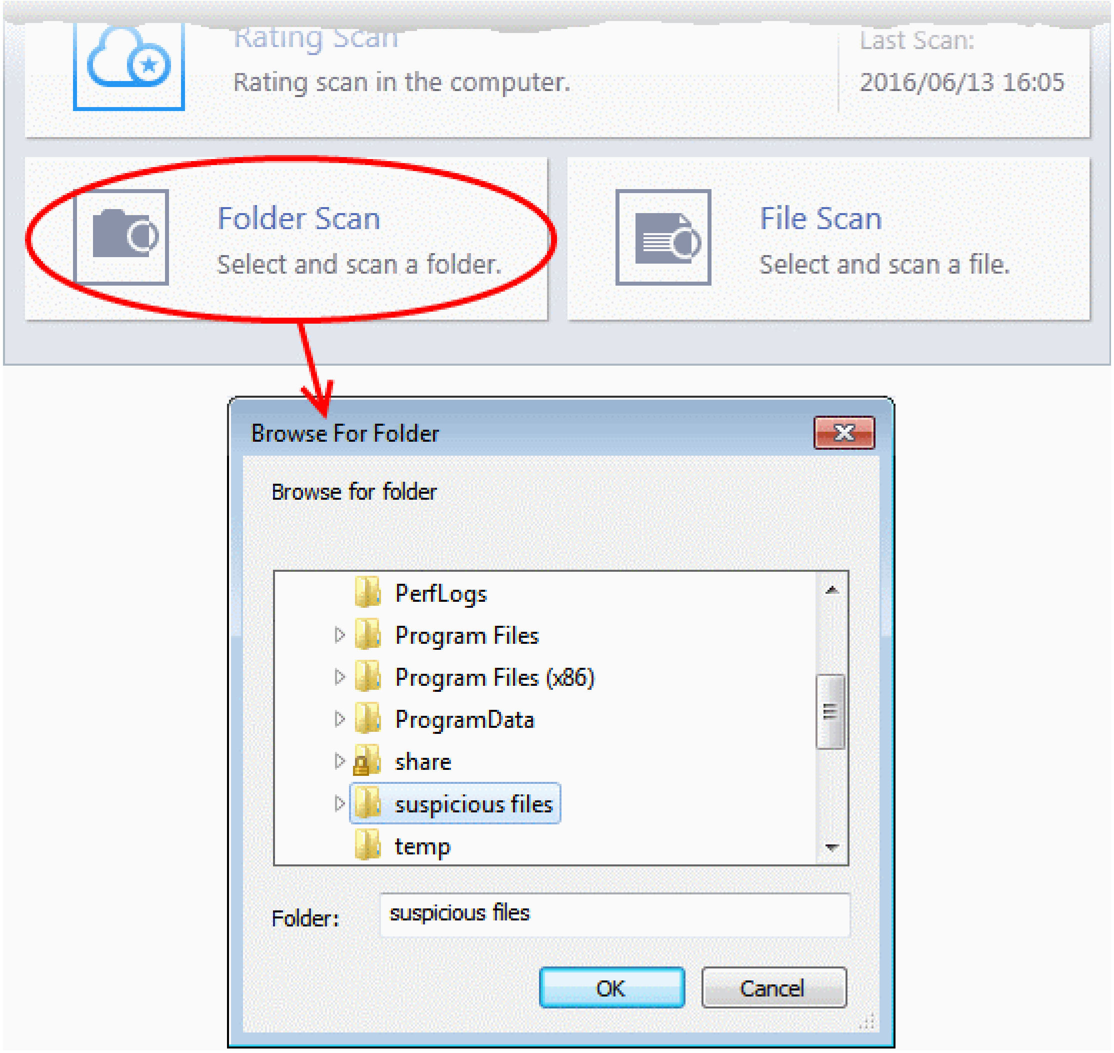
- Folder Scan - scan individual folders
- File Scan - scan an individual file

2.4.1. Scan a Folder

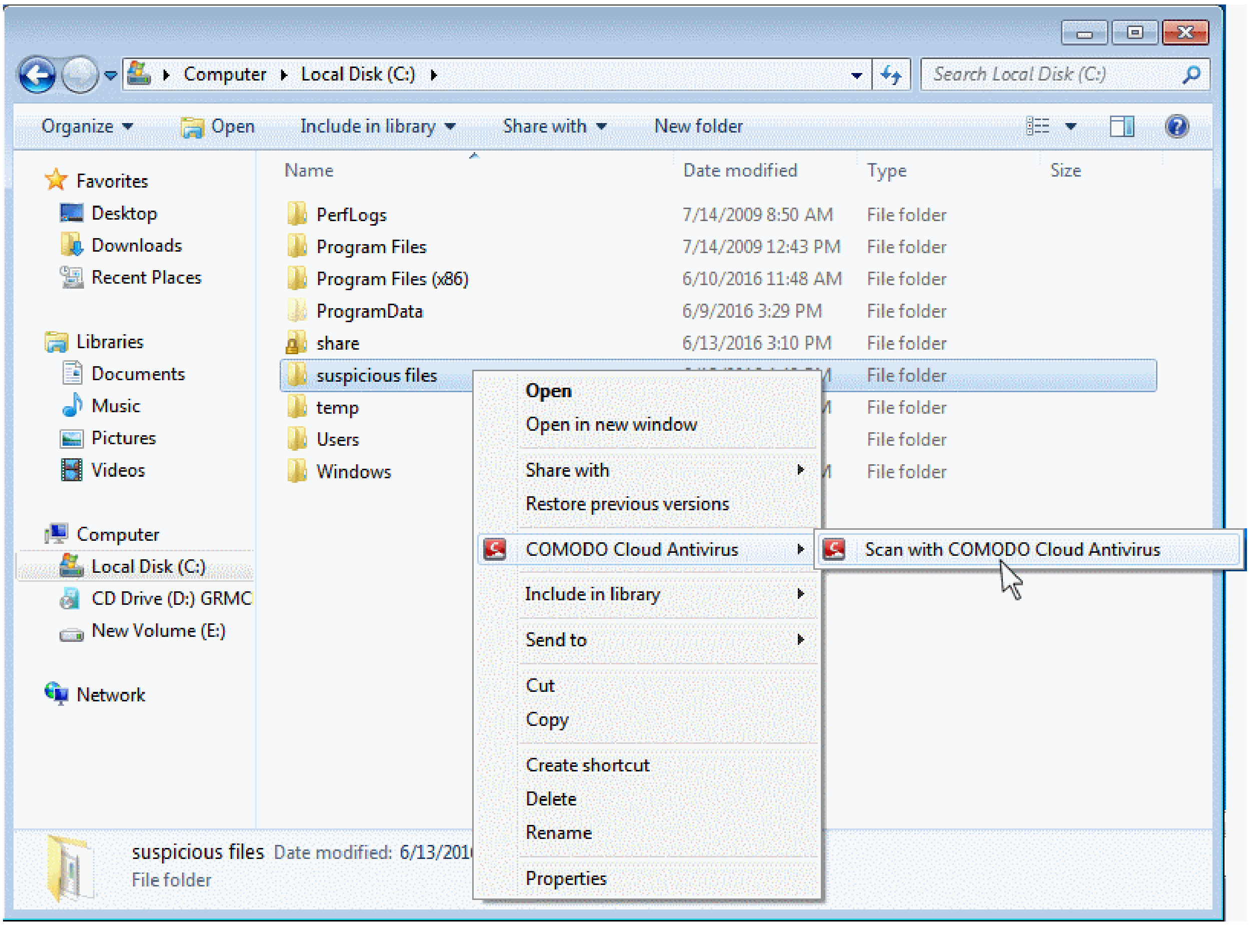
The 'Folder Scan' option allows you to scan a specific folder on your hard drive, CD/DVD or external device. For example you might have copied a folder from another computer in your network, an external device or downloaded from Internet and want to scan it for viruses and other threats before you open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

To scan a specific folder

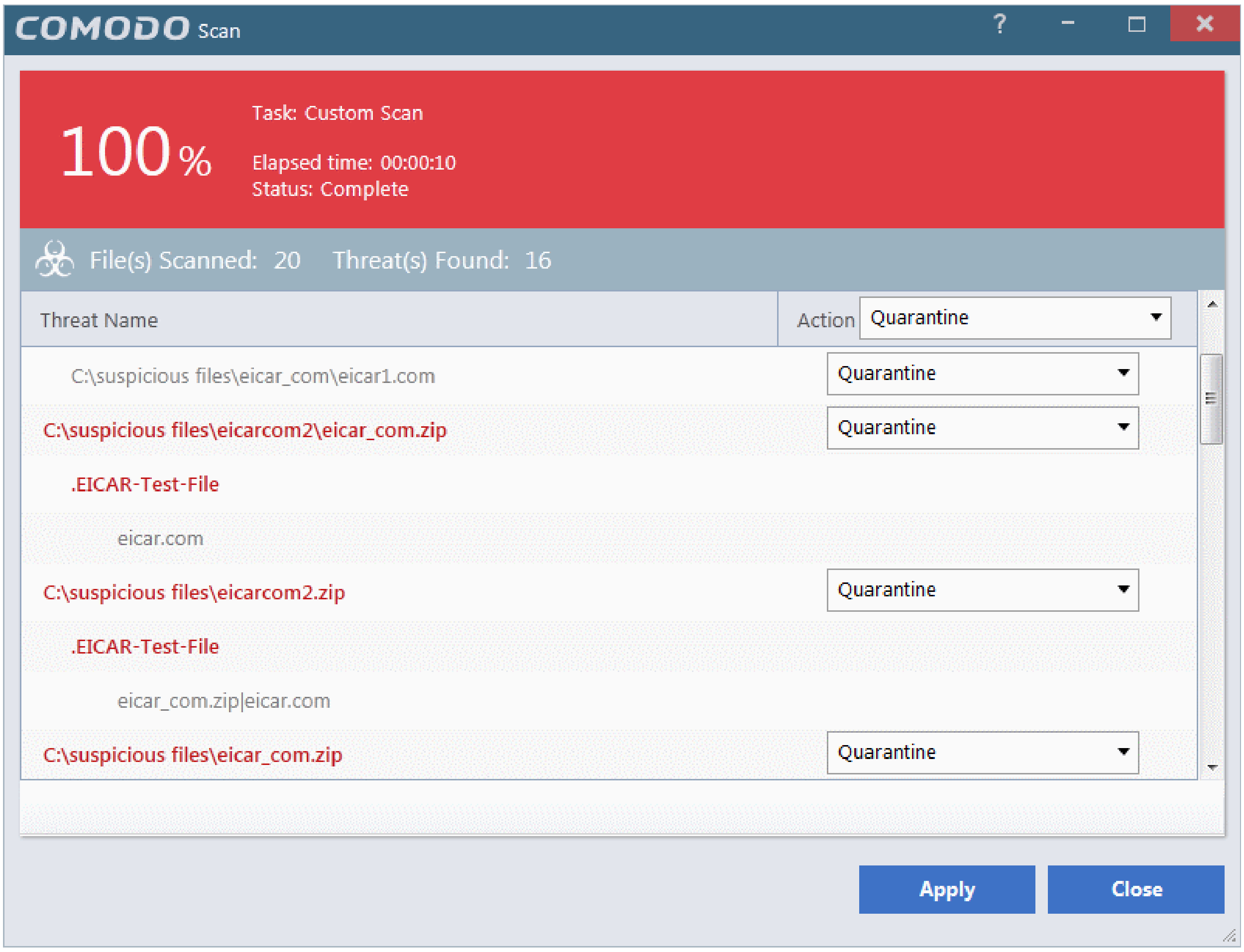
- Open the 'Scan' interface by clicking 'Scan' in the CCAV home screen or clicking on the scan button from the widget.
- Click 'Folder Scan' from the options.
- Navigate to the folder to be scanned in the 'Browse for Folder' window and click 'OK'.



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



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



Task: Custom Scan

Elapsed time: 00:00:10
Status: Complete

File(s) Scanned: 20 Threat(s) Found: 16

Threat Name	Action: Quarantine
C:\suspicious files\eicar_com\eicar1.com	Quarantine
C:\suspicious files\eicarcom2\eicar_com.zip	Quarantine
.EICAR-Test-File	
eicar.com	
C:\suspicious files\eicarcom2.zip	Quarantine
.EICAR-Test-File	
eicar_com.zip|eicar.com	
C:\suspicious files\eicar_com.zip	Quarantine

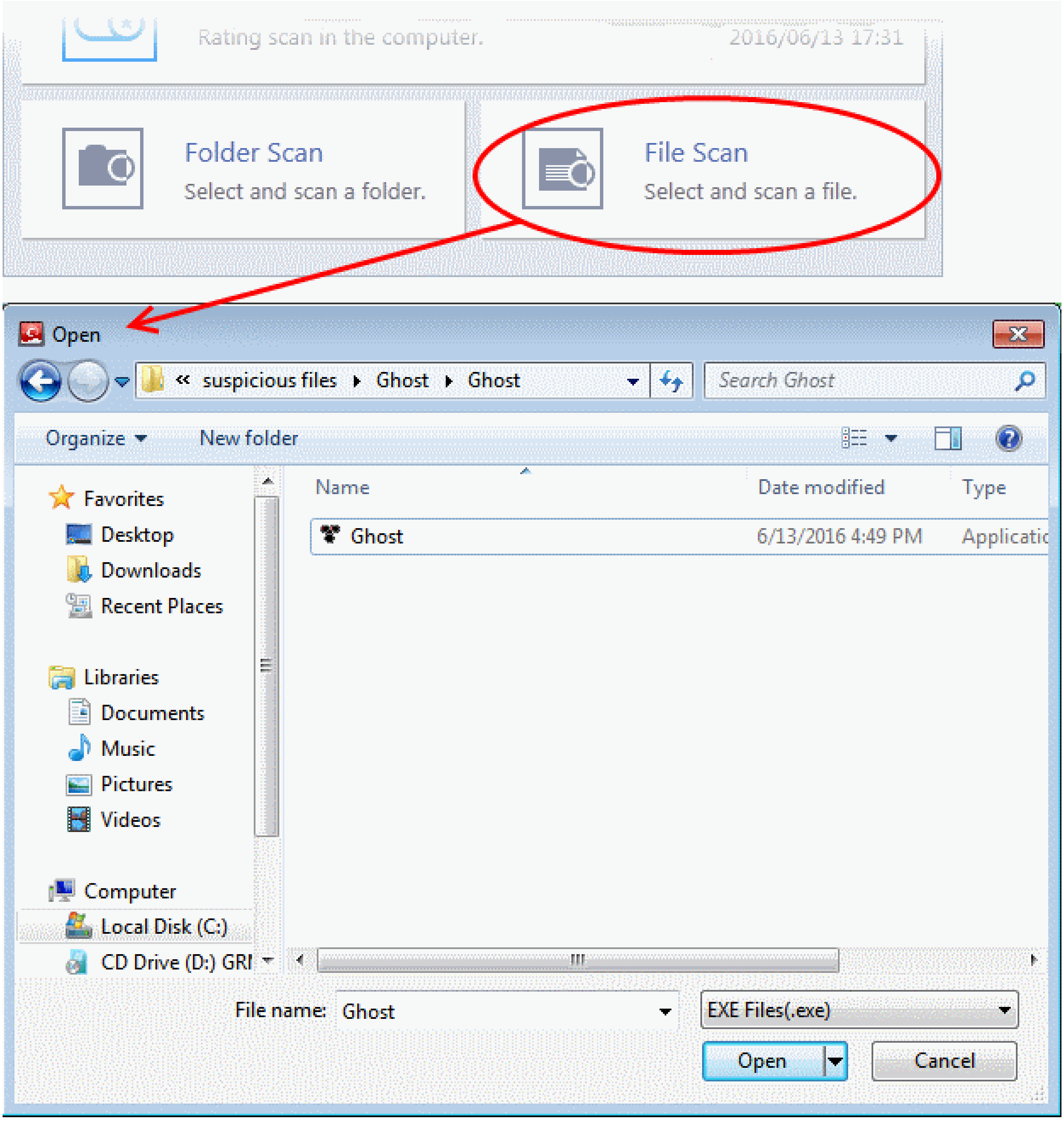
The scan results window displays the number of objects scanned and the number of threats detected (viruses, rootkits, malware and so on). You can choose to move the files to quarantine or ignore the threat based in your assessment. Refer to Processing the infected files for more details.

2.4.2. Scan a File

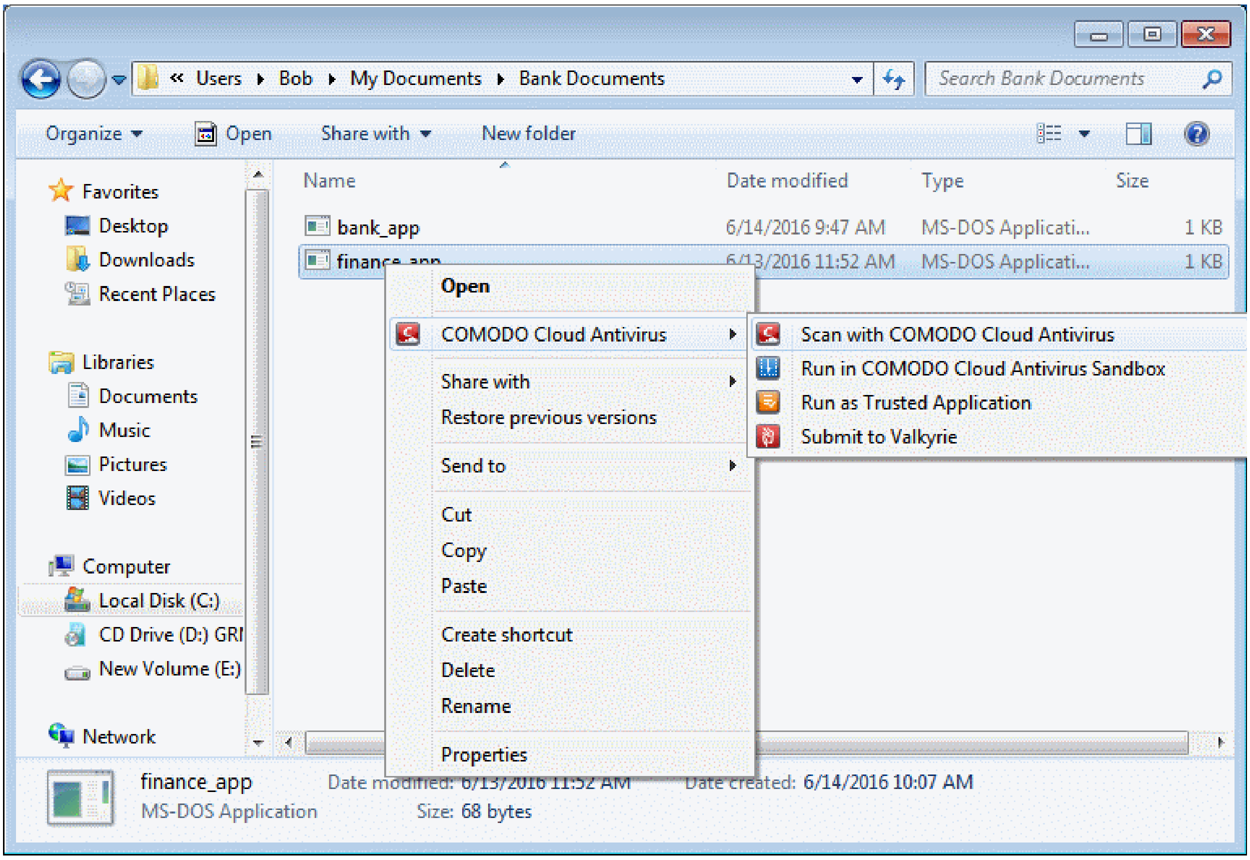
The 'File Scan' option allows you to scan a specific file on your hard drive, CD/DVD or external device. For example, you might have downloaded a file from the internet or dragged an email attachment onto your desktop and want to scan it for threats before you open it.

To scan a specific file

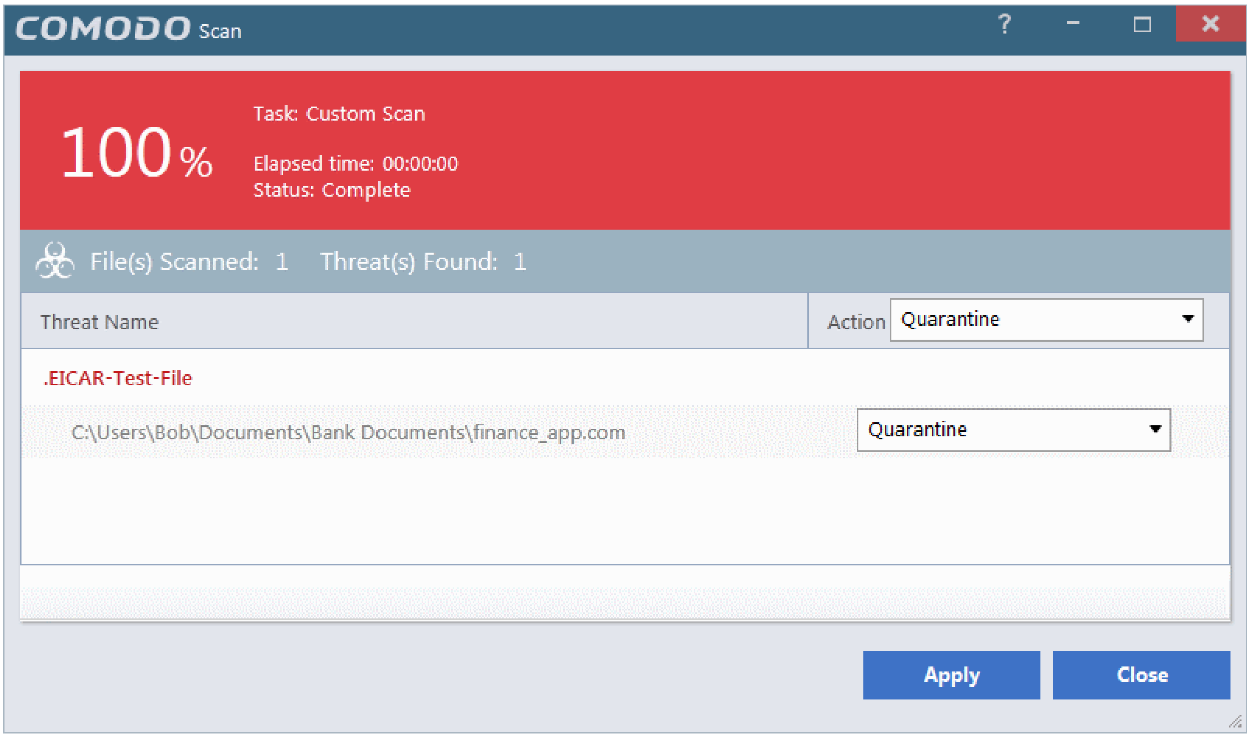
- Open the 'Scan' interface by clicking 'Scan' on the CCAV home screen, or by clicking the scan button on the widget.
- Choose 'File Scan', browse to the file you wish to scan and click 'Open':



- 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.



100 %

Task: Custom Scan

Elapsed time: 00:00:00

Status: Complete

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

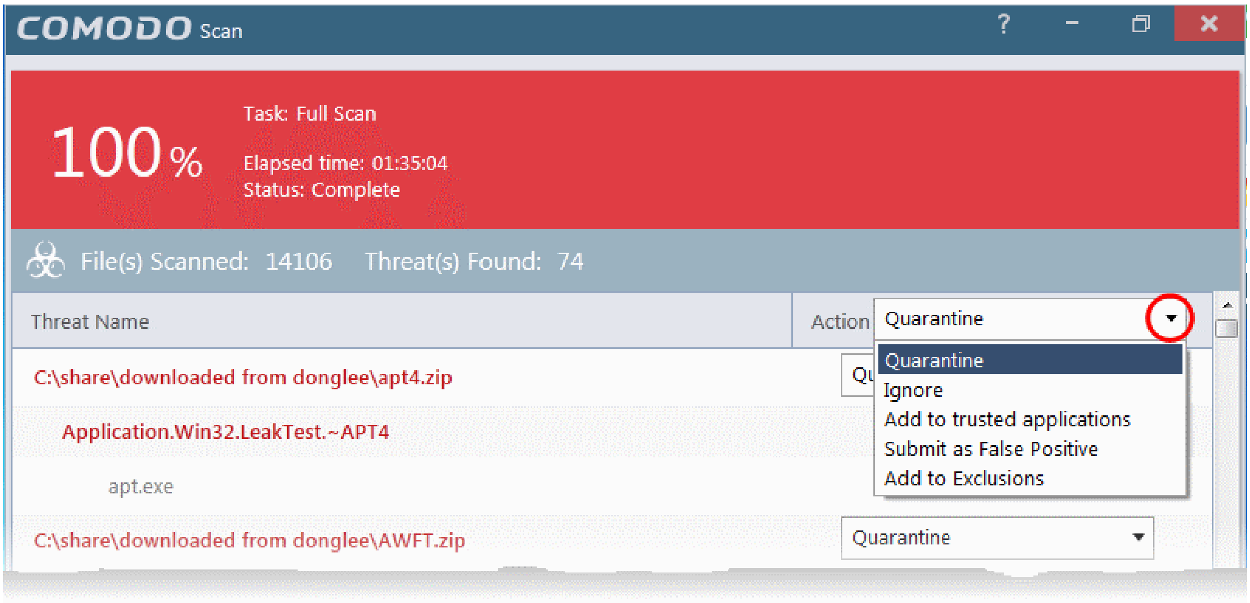
Threat Name	Action: Quarantine
.EICAR-Test-File	
C:\Users\Bob\Documents\Bank Documents\finance_app.com	Quarantine

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

2.5. 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.

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



COMODO Scan

100 %

Task: Full Scan

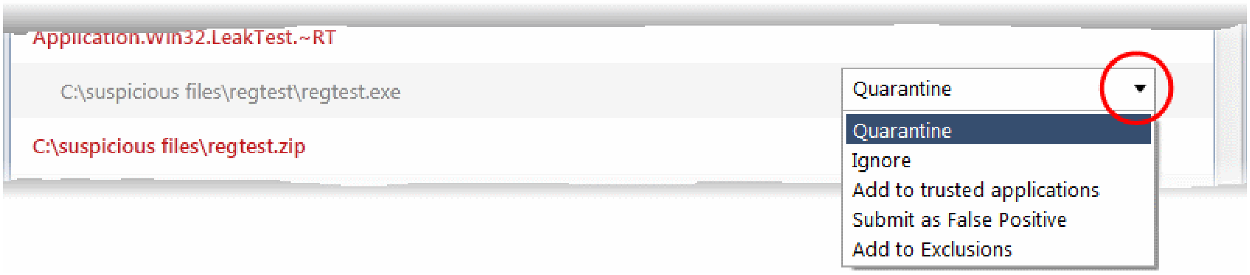
Elapsed time: 01:35:04

Status: Complete

File(s) Scanned: 14106 Threat(s) Found: 74

Threat Name	Action: Quarantine
C:\share\downloaded from donglee\apt4.zip	Qu
Application.Win32.LeakTest.~APT4	
apt.exe	
C:\share\downloaded from donglee\AWFT.zip	Quarantine

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



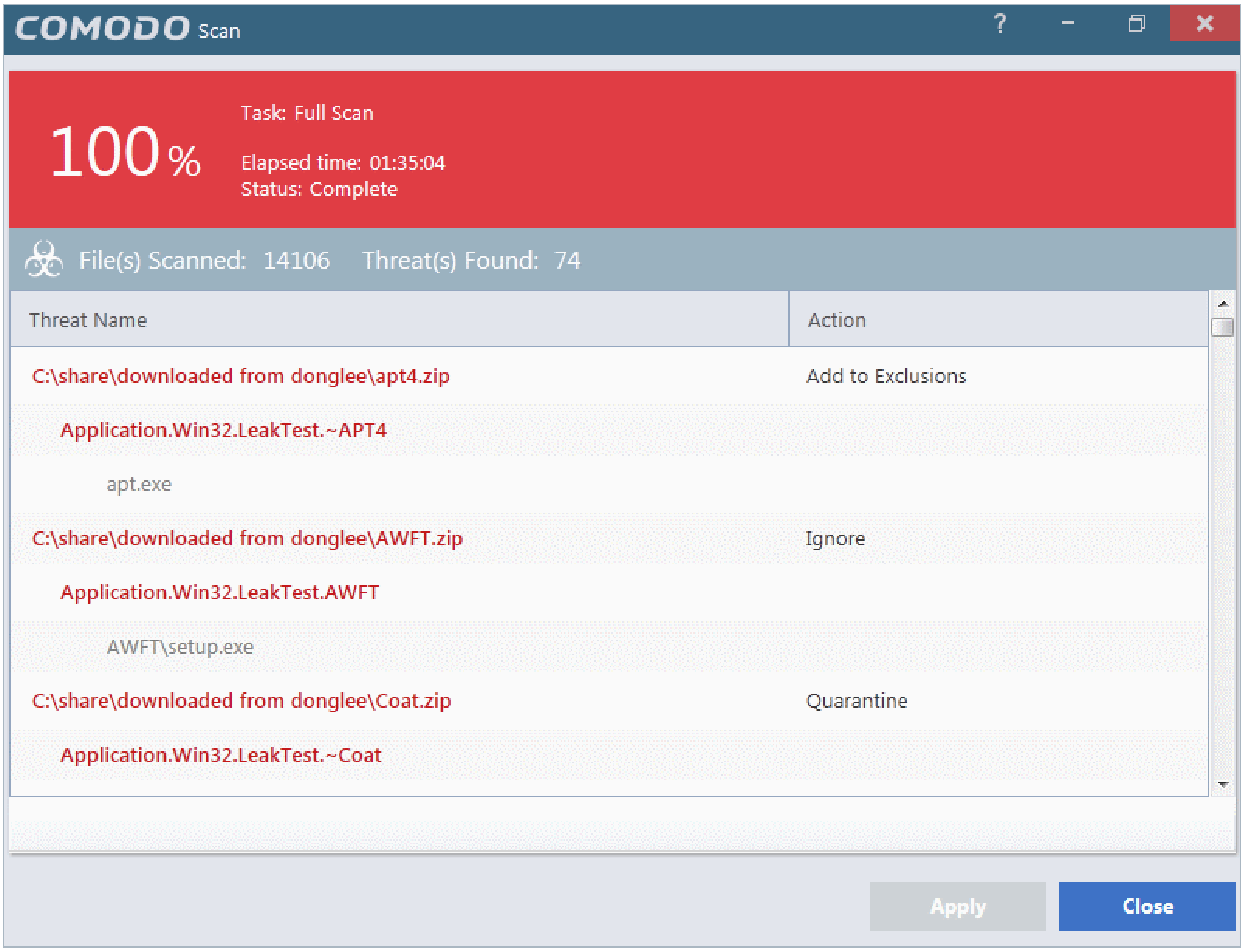
Application.Win32.LeakTest.~RT	
C:\suspicious files\regtest\regtest.exe	Quarantine
C:\suspicious files\regtest.zip	

The available actions are:

- **Quarantine -** The files will be moved to quarantine. For more details on quarantine feature, refer to the section 'View and Manage Quarantined Items'.
- **Ignore -** If you want to ignore the threat the threat this time only, select 'Ignore'. The file will be ignored only at that time and if the same application invokes again, the AV scanner will report it as a threat.
- **Add to trusted applications -** If you trust the file, select 'Add to trusted applications'. The file will be assigned 'Trusted' status in the 'Trusted Applications'. The alert will not generated if the same application invokes again.
- **Report as false positive -** If you are sure that the file is safe, select 'Report False Positive'. The Antivirus will send the file to Comodo for analysis. If the file is trustworthy, it is added to the Comodo safe list.
- **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.



100 %

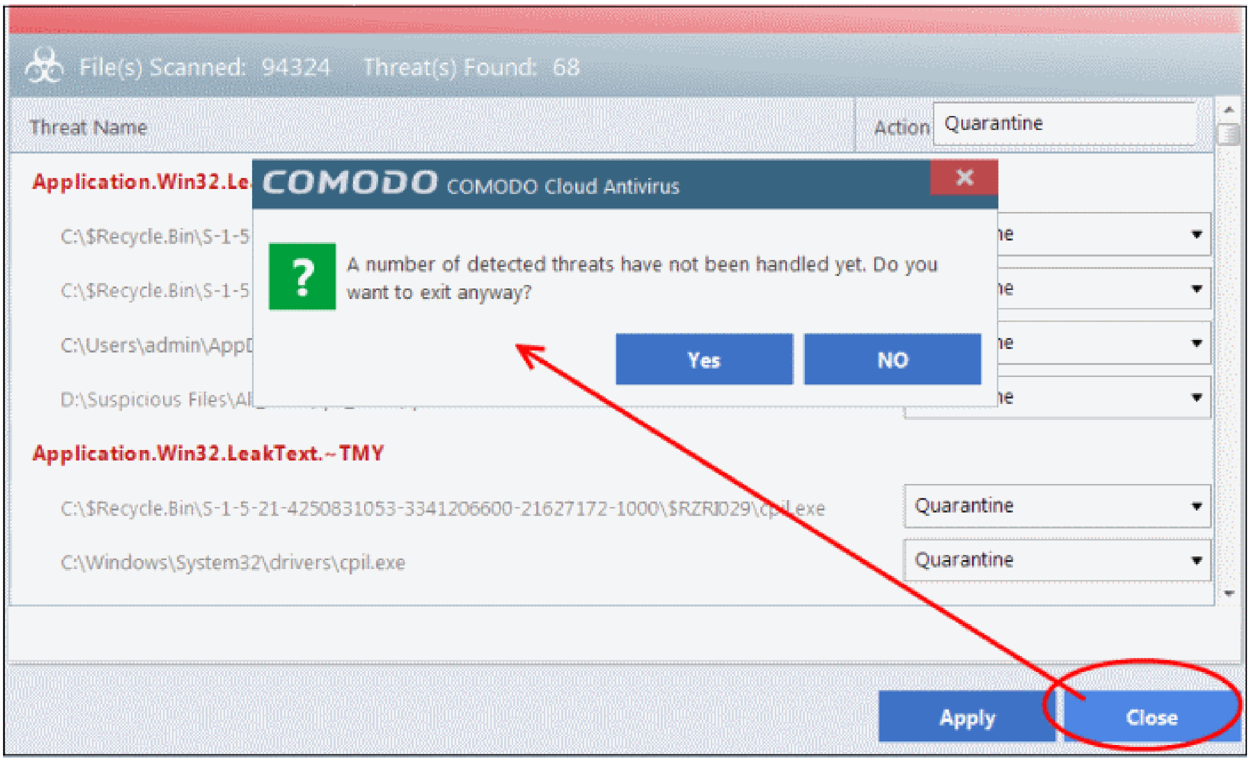
Task: Full Scan

Elapsed time: 01:35:04
Status: Complete

File(s) Scanned: 14106 Threat(s) Found: 74

Threat Name	Action
C:\share\downloaded from donglee\apt4.zip	Add to Exclusions
Application.Win32.LeakTest.~APT4	
apt.exe	
C:\share\downloaded from donglee\AWFT.zip	Ignore
Application.Win32.LeakTest.AWFT	
AWFT\setup.exe	
C:\share\downloaded from donglee\Coat.zip	Quarantine
Application.Win32.LeakTest.~Coat	

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



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

Threat Name	Action Quarantine
Application.Win32.Le	
C:\$Recycle.Bin\S-1-5	ne
C:\$Recycle.Bin\S-1-5	ne
C:\Users\admin\AppD	ne
D:\Suspicious Files\Al	ne
Application.Win32.LeakText.~TMY	
C:\$Recycle.Bin\S-1-5-21-4250831053-3341206600-21627172-1000\$RZRI029\cpil.exe	Quarantine
C:\Windows\System32\drivers\cpil.exe	Quarantine

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

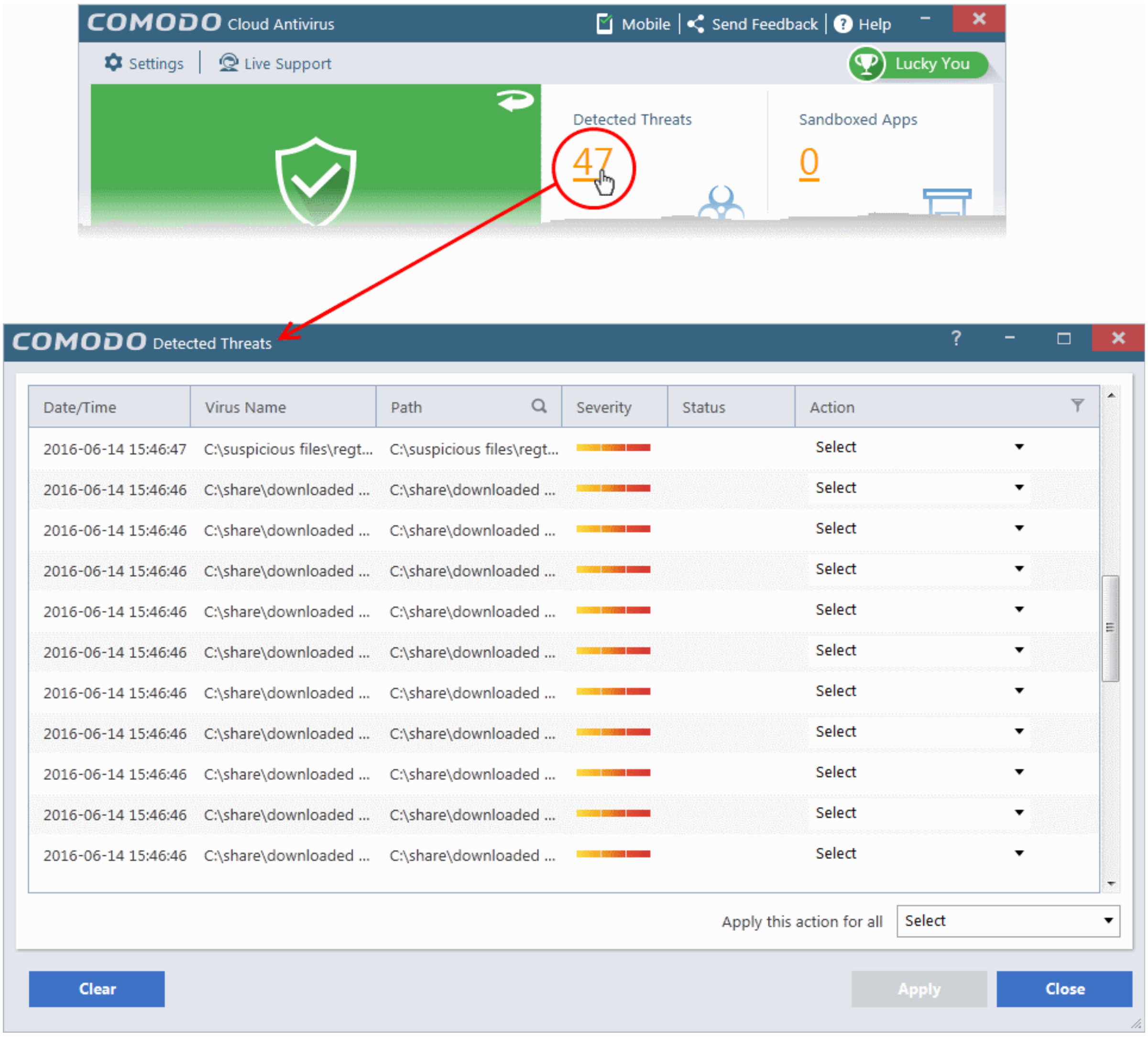
The 'Detected Threats' interface allows you to take action such as 'Quarantine', 'Trust' or 'Trust and Report False

Positive' later on. Refer to the section 'Managing Detected Threats' for more details.

2.6. Managing Detected Threats

The 'Detected Threats' interface displays items identified as malicious by real-time and manual scans, 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 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 home screen of CCAV.



Date/Time	Virus Name	Path	Severity	Status	Action
2016-06-14 15:46:47	C:\suspicious files\regt...	C:\suspicious files\regt...			Select
2016-06-14 15:46:46	C:\share\downloaded ...	C:\share\downloaded ...			Select
2016-06-14 15:46:46	C:\share\downloaded ...	C:\share\downloaded ...			Select
2016-06-14 15:46:46	C:\share\downloaded ...	C:\share\downloaded ...			Select
2016-06-14 15:46:46	C:\share\downloaded ...	C:\share\downloaded ...			Select
2016-06-14 15:46:46	C:\share\downloaded ...	C:\share\downloaded ...			Select
2016-06-14 15:46:46	C:\share\downloaded ...	C:\share\downloaded ...			Select
2016-06-14 15:46:46	C:\share\downloaded ...	C:\share\downloaded ...			Select
2016-06-14 15:46:46	C:\share\downloaded ...	C:\share\downloaded ...			Select
2016-06-14 15:46:46	C:\share\downloaded ...	C:\share\downloaded ...			Select
2016-06-14 15:46:46	C:\share\downloaded ...	C:\share\downloaded ...			Select

Apply this action for all: Select

Column Descriptions:

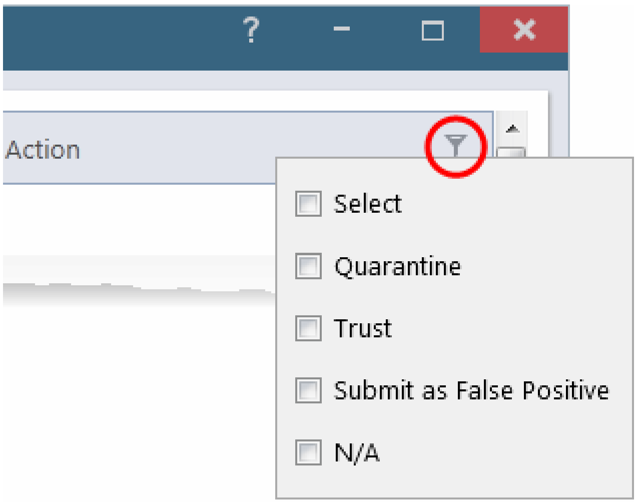
- **Date/Time** - The date and time at which the threat was detected
- **Virus Name** - The name of the malware contained in the application detected as threat
- **Path** - The location of the application in the system
- **Severity** - Indicates the risk level presented by the activity or request of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

  The available actions are:

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

  from the Quarantine interface. Refer to the section View and Manage Quarantined Items for more details.
- **Trust -** The item will be added to the Trusted Applications and will be excluded from the future scans. Choose this option only if the item is trustworthy.
- **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 global safelist.

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



  - To move 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 'Trust and Report 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 a online file verdict system that tests unknown files with a range of static and behavioral checks in order to identify those that are malicious. Because Valkyrie analyzes the entire run-time behavior of a file, it is more effective at detecting zero-day threats missed by the signature-based detection systems of classic antivirus products.

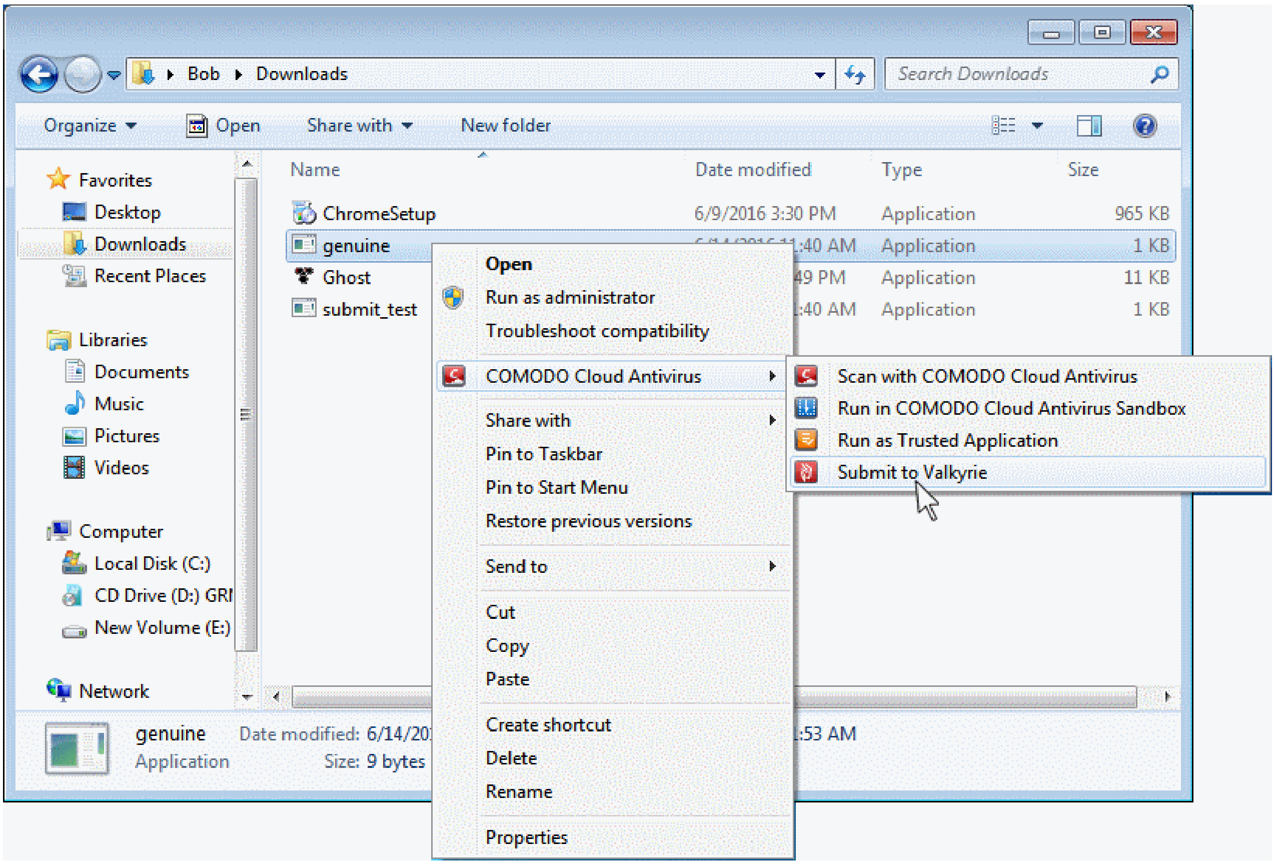
Comodo Cloud Antivirus allows you to upload unknown files identified from your computer to Valkyrie for analysis. Files submitted to our FLS server during a rating scan will be checked against our global whitelist and blackllists to identify trustworthy and malicious items. Files which could not be identified as trusted or malicious are classified as 'Unknown'. If auto-submission is enabled under Sandbox Settings, CCAV automatically uploads unknown files to Valkyrie for analysis. (Refer to Sandbox Settings for more details on this.)

If not enabled, the results screen of each File Rating scan allows you to manually upload unknown files. Refer to the section Running a Rating Scan for more details.

You can also manually upload files to Valkyrie by right-clicking on a file. For example, you can upload an executable file that you have recently downloaded from Internet to Valkyrie to ensure its trustworthiness.

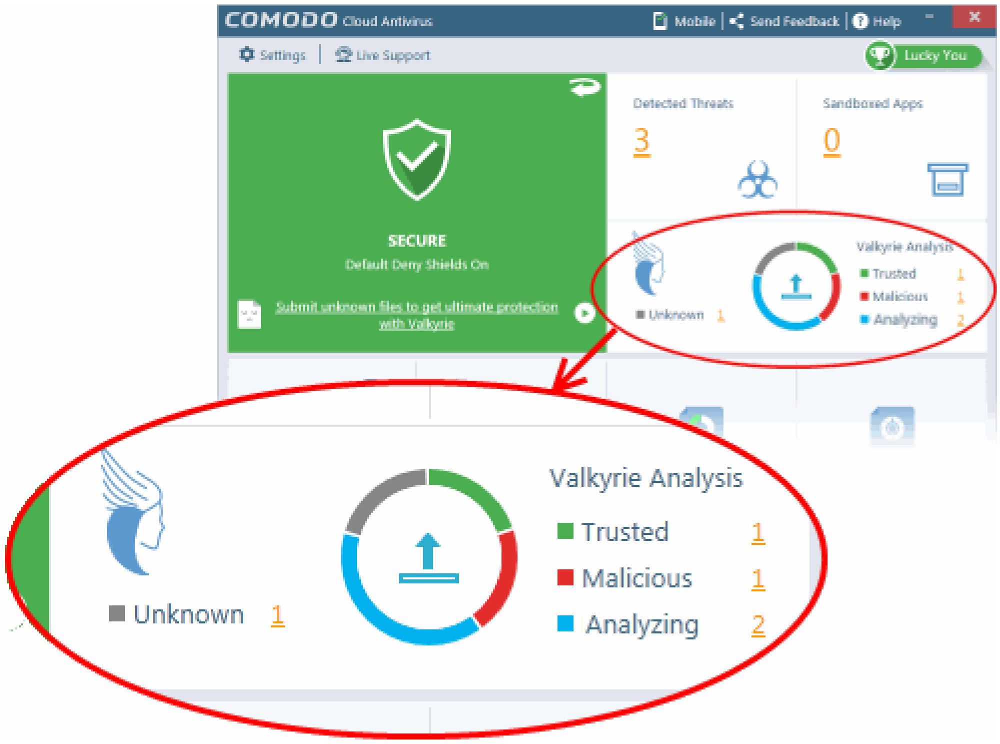
To manually submit a file

- Right click on the file to be uploaded from the Windows Explorer window and select 'Comodo Cloud Antivirus' > 'Submit to Valkyrie'



Files submitted both automatically and manually will undergo a series of automated and manual tests for their static and dynamic behavior at Comodo and the results will be sent back to your CCAV installation once the analysis is complete.

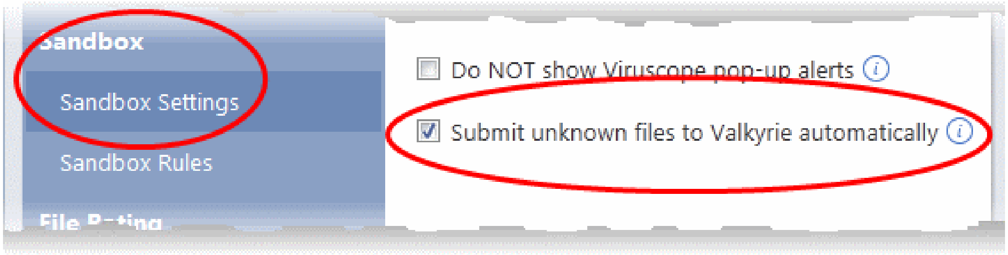
The 'Valkyrie Analysis' pane of the CCAV home screen displays the statistics and status messages from Valkyrie.



The pie-chart shows verdicts on unknown files on your computer. Clicking the pie-chart opens the respective interface for running a scan or viewing results.

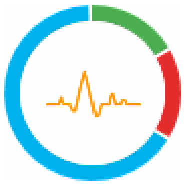
- Indicates that you need to run a File Rating scan to identify unknown files on your computer.

- Indicates that some unknown files are detected by rating scan but auto-submission is disabled. You can submit unknown files manually for Valkyrie Analysis. Clicking the up arrow starts the upload process.
  - Refer to the explanation above for details on manually submitting files.
  - To configure CCAV for automatic submission of unknown files, enable auto-submission from the Sandbox Settings interface. To do so:
    - Click the 'Settings' button ⚙ Settings at the top left of CCAV home screen to open the 'Settings' interface
    - Click 'Sandbox Settings' under 'Sandbox Settings' at the left of the 'Settings' interface
    - Ensure that the option 'Submit unknown files to Valkyrie automatically' is selected. (***Default = Enabled***)

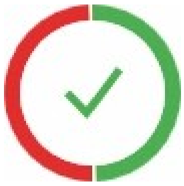


□ Do NOT show Viruscope pop-up alerts

☑ Submit unknown files to Valkyrie automatically

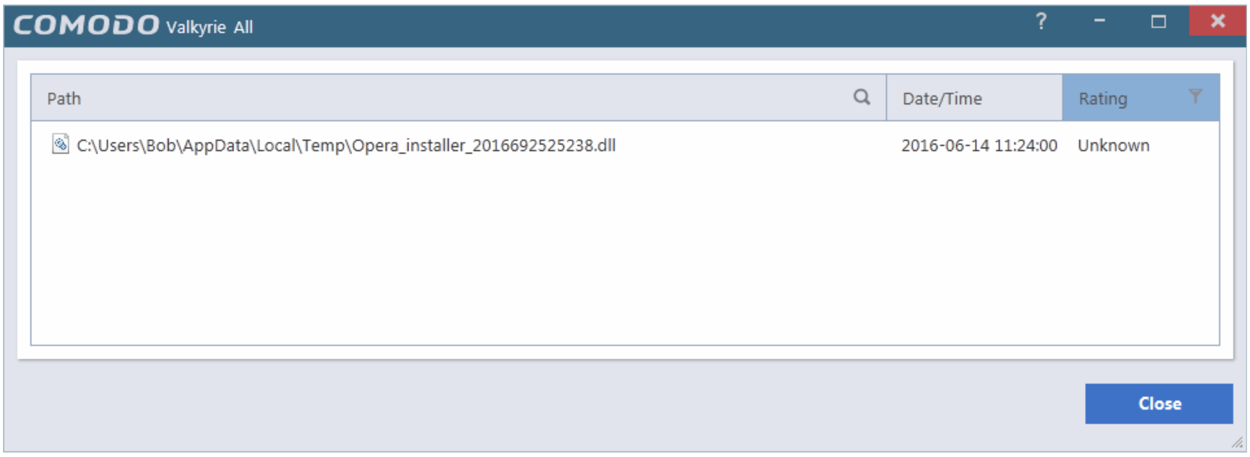


- Indicates that some unknown files were submitted to Valkyrie and are currently under analysis



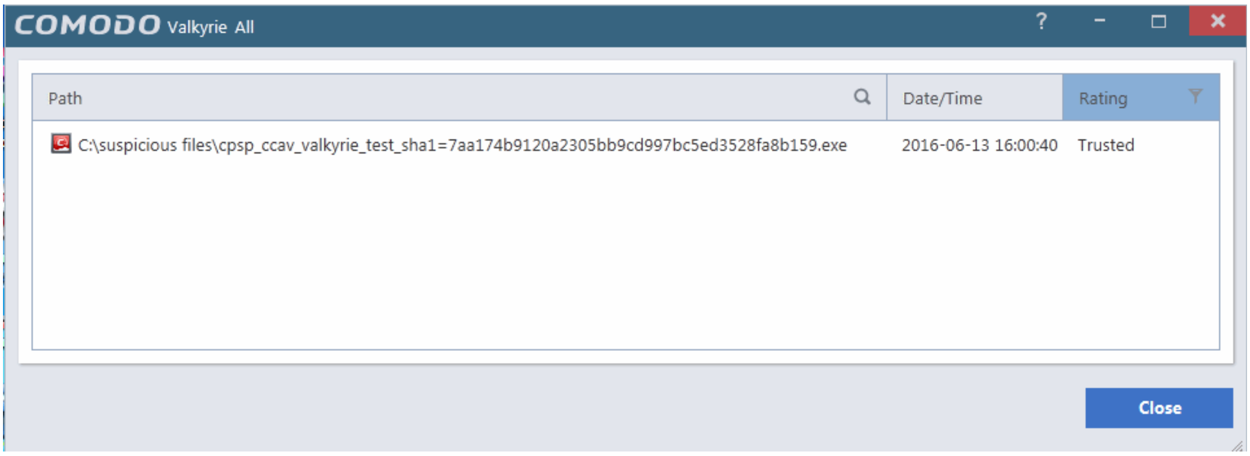
- Indicates that all unknown files have been submitted and analyzed by Valkyrie and there are no unknown or pending files left in your computer.

- **Unknown** - Displays the number of files identified as 'Unknown' from Rating scans. The statistics on Unknown files is displayed only if auto-submission is not enabled in CCAV under Sandbox Settings. Otherwise, all unknown files will be immediately uploaded to Valkyrie automatically at the end of each Rating scan.
    - Clicking the number will display the list of files identified as Unknown



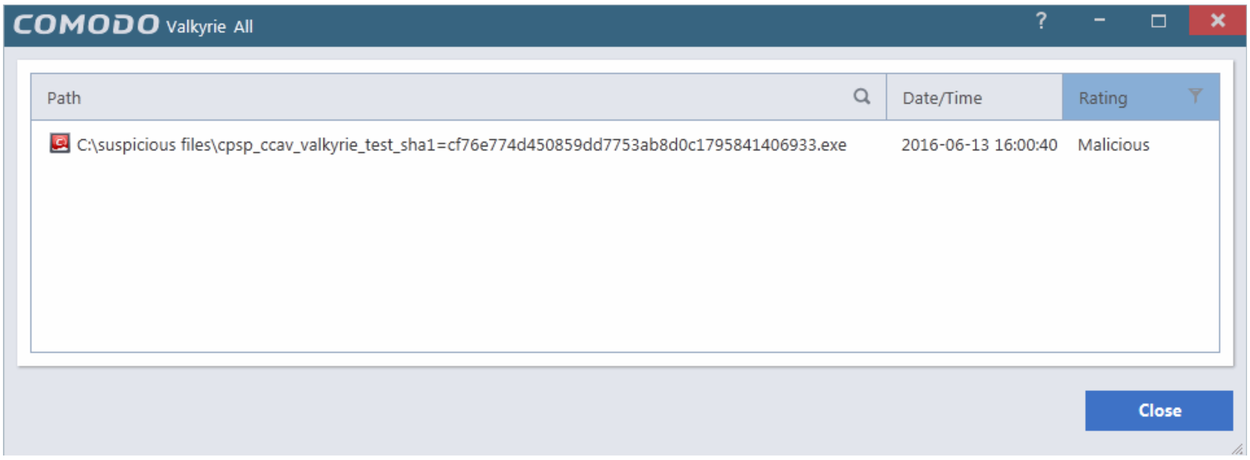
Path	Date/Time	Rating
C:\Users\Bob\AppData\Local\Temp\Opera_installer_2016692525238.dll	2016-06-14 11:24:00	Unknown

    - To upload the unknown files to Valkyrie, click the Up Arrow at the center of the pie-chart
- **Trusted** - Displays the number of files uploaded from your computer and identified as 'Trusted' by Valkyrie Analysis.
    - Clicking the number will display the list of files identified as 'Trusted'



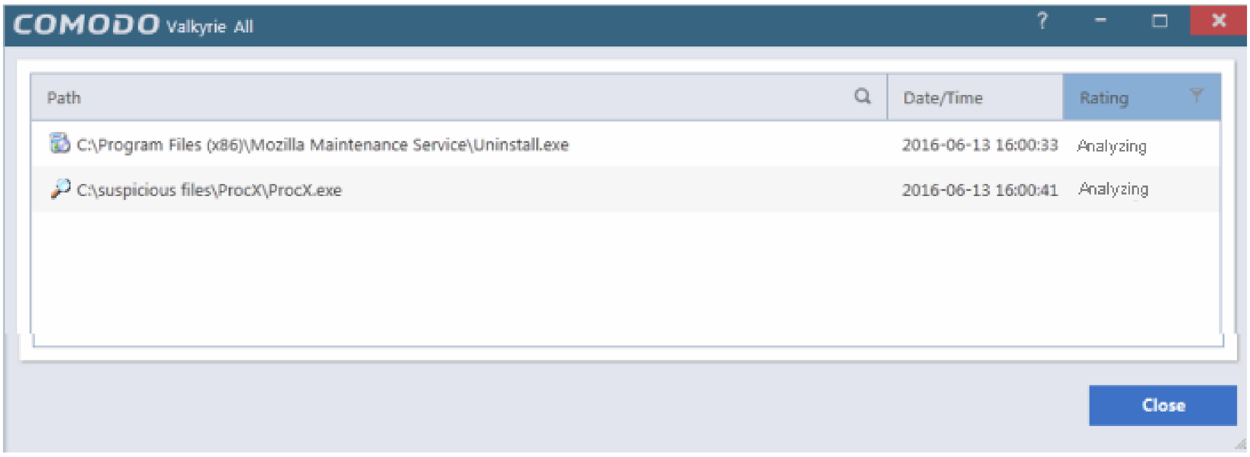
Path	Date/Time	Rating
C:\suspicious files\cpsp_ccav_valkyrie_test_sha1=7aa174b9120a2305bb9cd997bc5ed3528fa8b159.exe	2016-06-13 16:00:40	Trusted

- **Malicious** - Displays the number of files uploaded from your computer and identified as 'Malicious' by Valkyrie Analysis.
    - Clicking the number will display the list of files identified as 'Malicious'



Path	Date/Time	Rating
C:\suspicious files\cpsp_ccav_valkyrie_test_sha1=cf76e774d450859dd7753ab8d0c1795841406933.exe	2016-06-13 16:00:40	Malicious

- **Analyzing** - Displays the number of files uploaded from your computer and are under analysis process by Valkyrie. The verdicts on these files will be returned to your computer once the analysis is complete.
    - Clicking the number will display the list of pending files

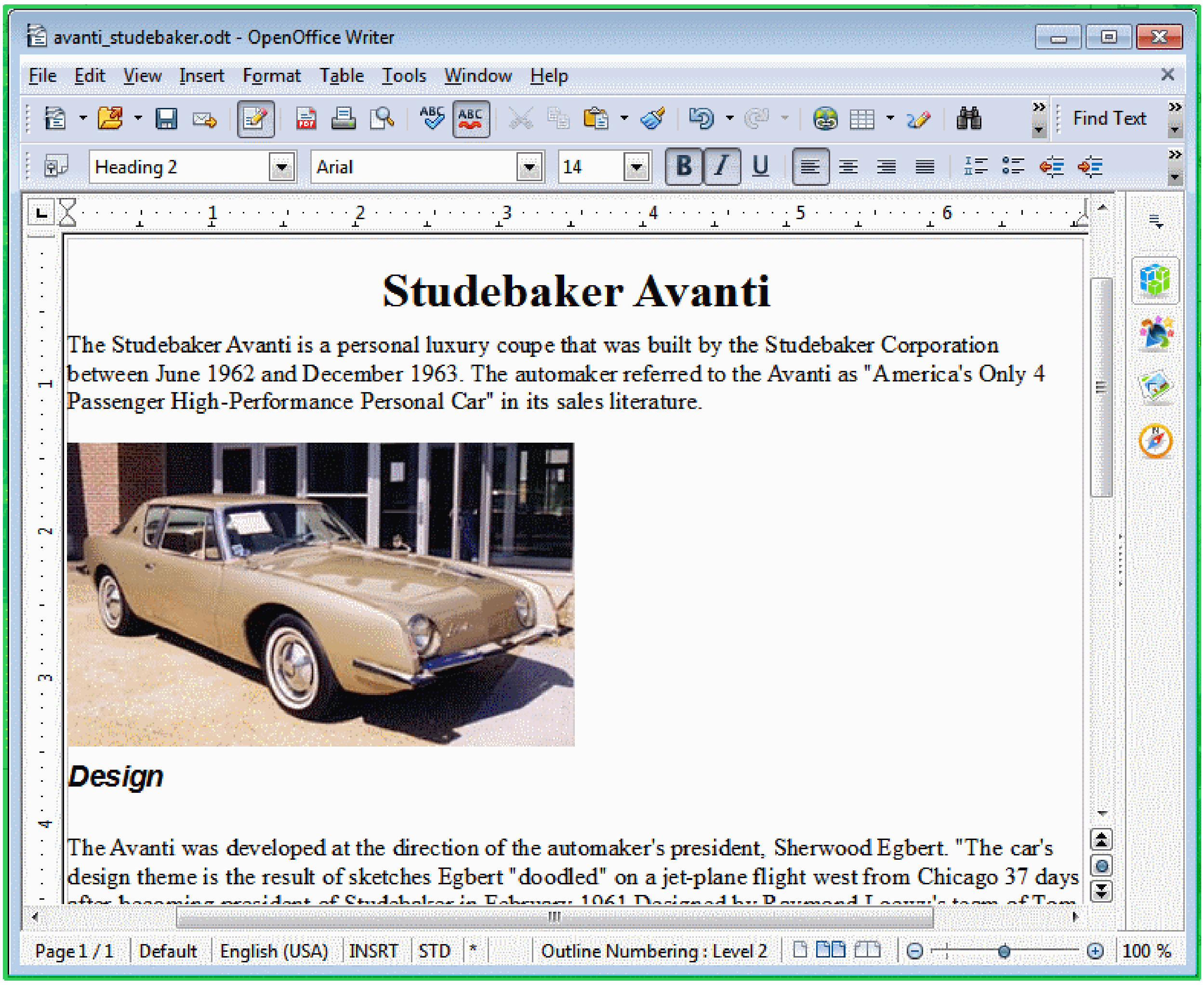


Path	Date/Time	Rating
C:\Program Files (x86)\Mozilla Maintenance Service\Uninstall.exe	2016-06-13 16:00:33	Analyzing
C:\suspicious files\ProcX\ProcX.exe	2016-06-13 16:00:41	Analyzing

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:


avanti_studebaker.odt - OpenOffice Writer
File Edit View Insert Format Table Tools Window Help
Find Text
Heading 2
Arial
14
B I U
Page 1 / 1 | Default | English (USA) | INSRT | STD | * | Outline Numbering : Level 2 | 100 %

Studebaker Avanti

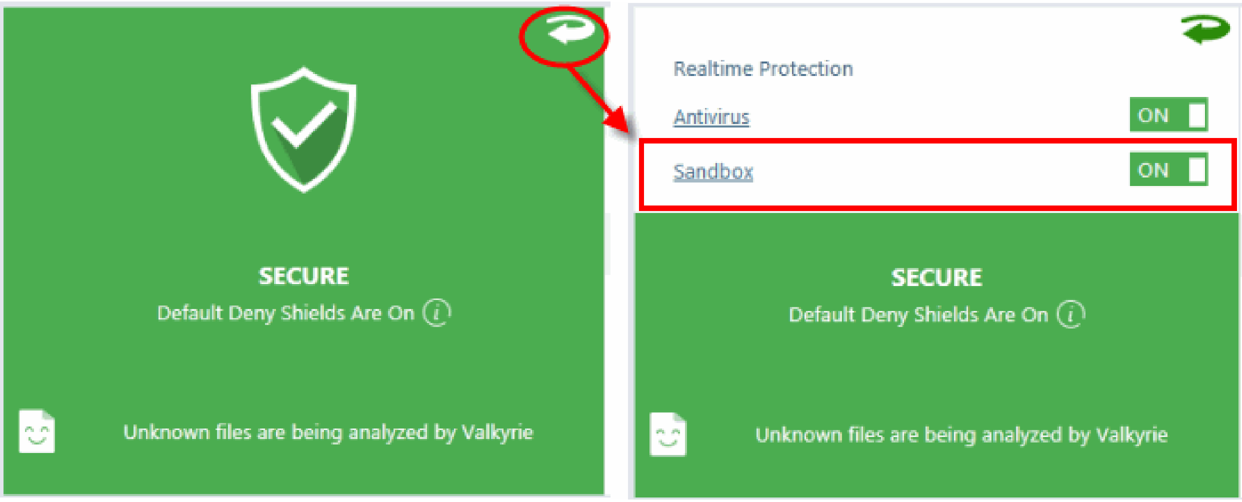
The Studebaker Avanti is a personal luxury coupe that was built by the Studebaker Corporation between June 1962 and December 1963. The automaker referred to the Avanti as "America's Only 4 Passenger High-Performance Personal Car" in its sales literature.

Design

The Avanti was developed at the direction of the automaker's president, Sherwood Egbert. "The car's design theme is the result of sketches Egbert "doodled" on a jet-plane flight west from Chicago 37 days after becoming president of Studebaker in February 1961. Designed by Raymond Loewy's team of Tom

All executables identified as 'Unknown', will automatically run inside the sandbox by default. You can disable or enable the auto-sandboxing feature from the home screen or from the right-click menu of the system tray icon or the widget.

- To enable/disable auto-sandbox from the home screen, click the curved arrow in the security staus pane and use the toggle switch beside 'Sandbox' under 'Realtime Protection'.


SECURE
Default Deny Shields Are On
Unknown files are being analyzed by Valkyrie

Realtime Protection

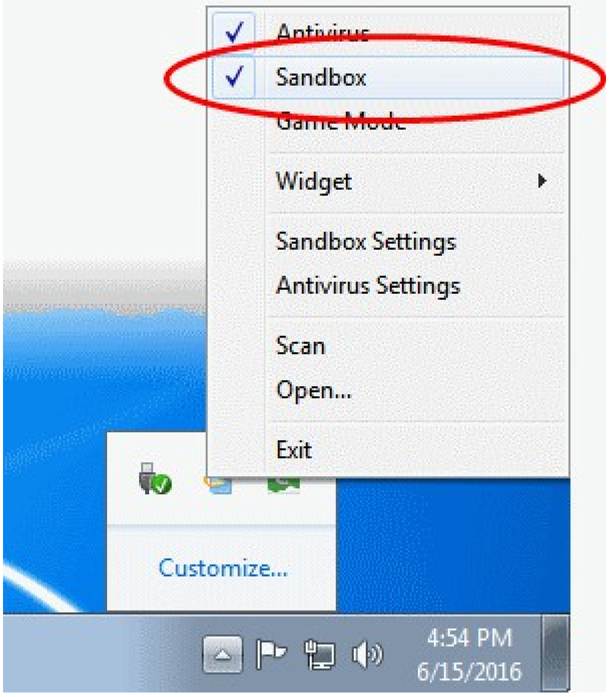
Antivirus: ON

Sandbox: ON

SECURE
Default Deny Shields Are On
Unknown files are being analyzed by Valkyrie

- Clicking the 'Sandbox' link opens the Sandbox Settings interface. Refer to the section Sandbox Settings for more details.

- Alternatively, right-click on the CCAV system tray icon or the widget and use the checkbox beside 'Sandbox' from the context sensitive menu to enable or disable it.



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 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.

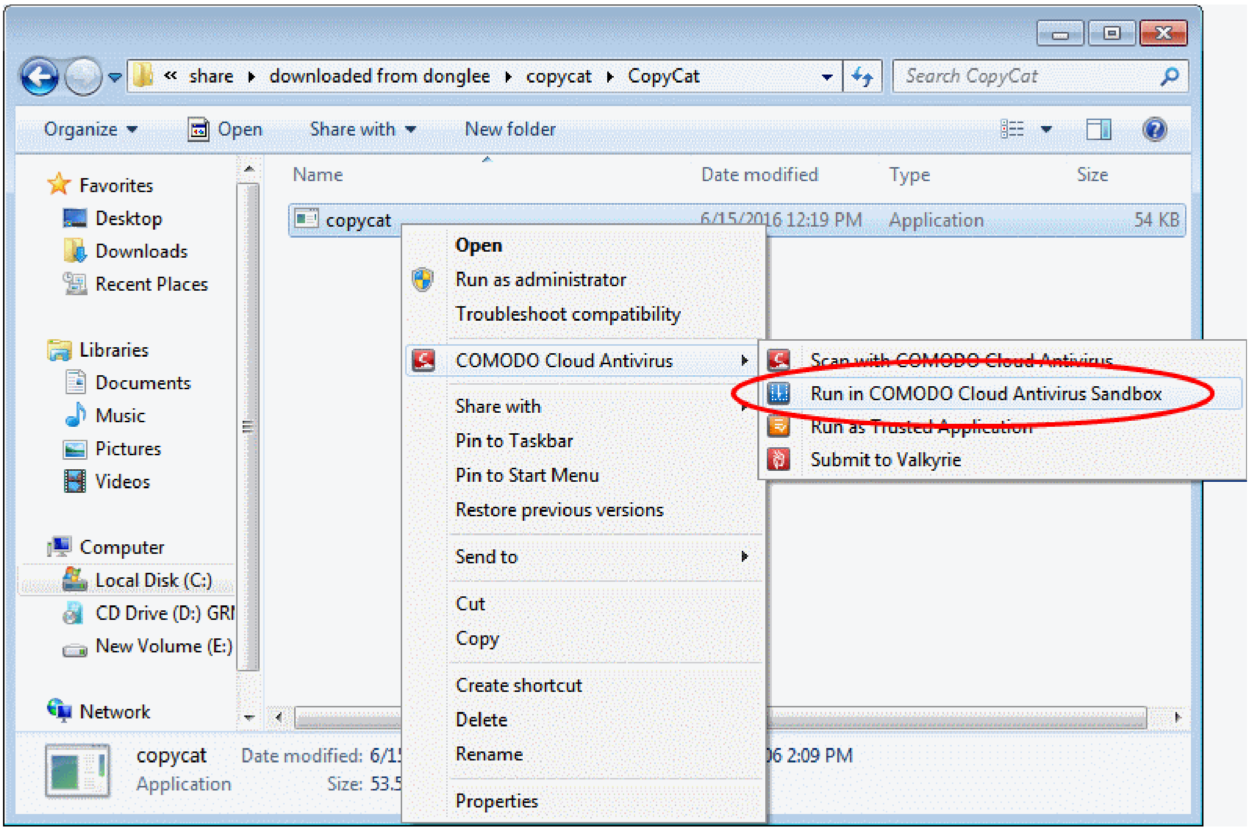
There are different ways in which you can run applications/browsers inside the sandbox. Following sections explain in detail on:

- 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 from the Windows explorer.

- Navigate to the item through Windows Explorer
- 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

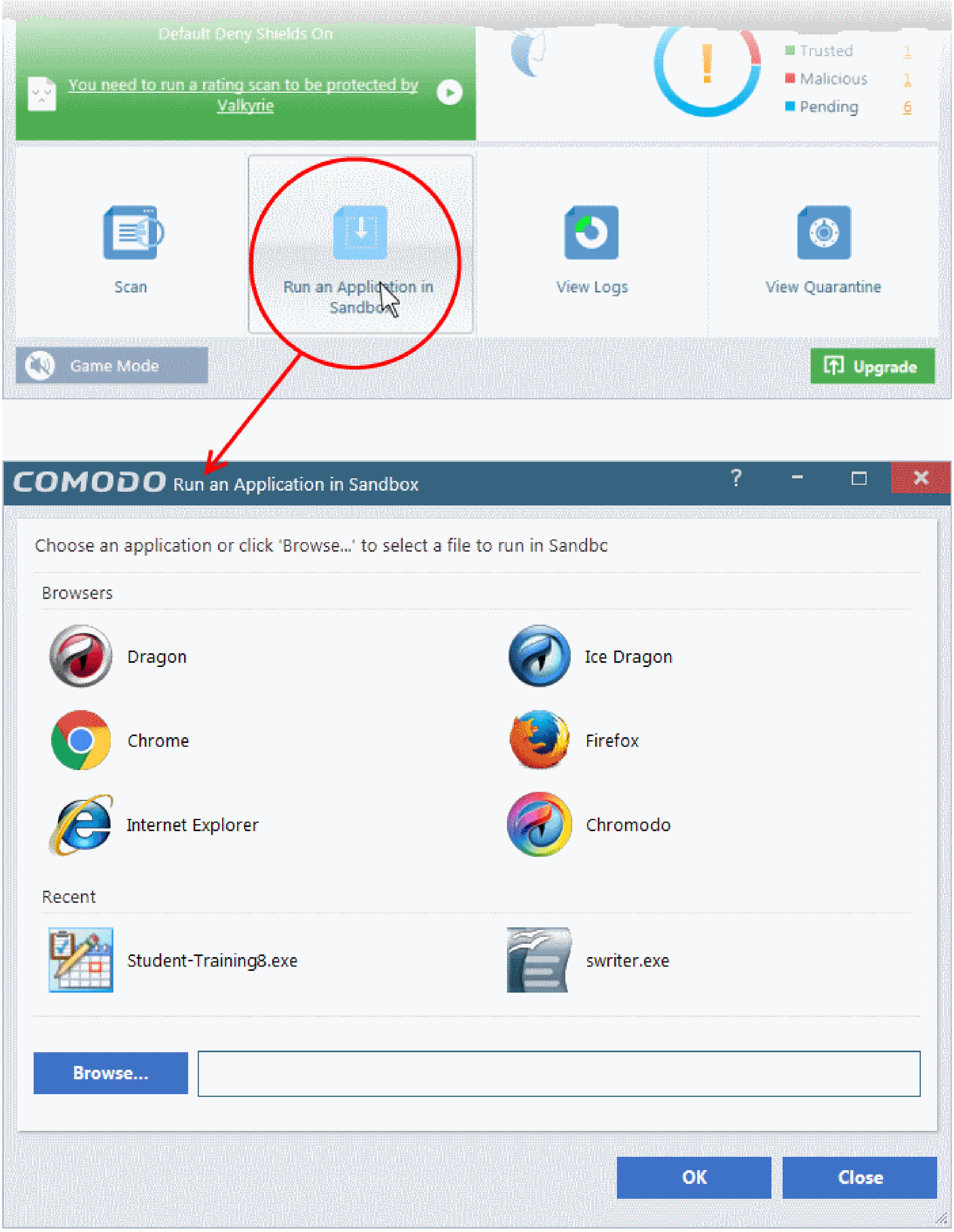
You can add applications and browsers to CCAV sandbox, allowing you to run those applications from CCAV home screen, inside the sandbox.

To add an application to the sandbox

- Click 'Run an Application in Sandbox' from CCAV home screen

OR

- Click the 'Sandbox' button from the CCAV Desktop widget



Choose an application or click 'Browse...' to select a file to run in Sandbc

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'

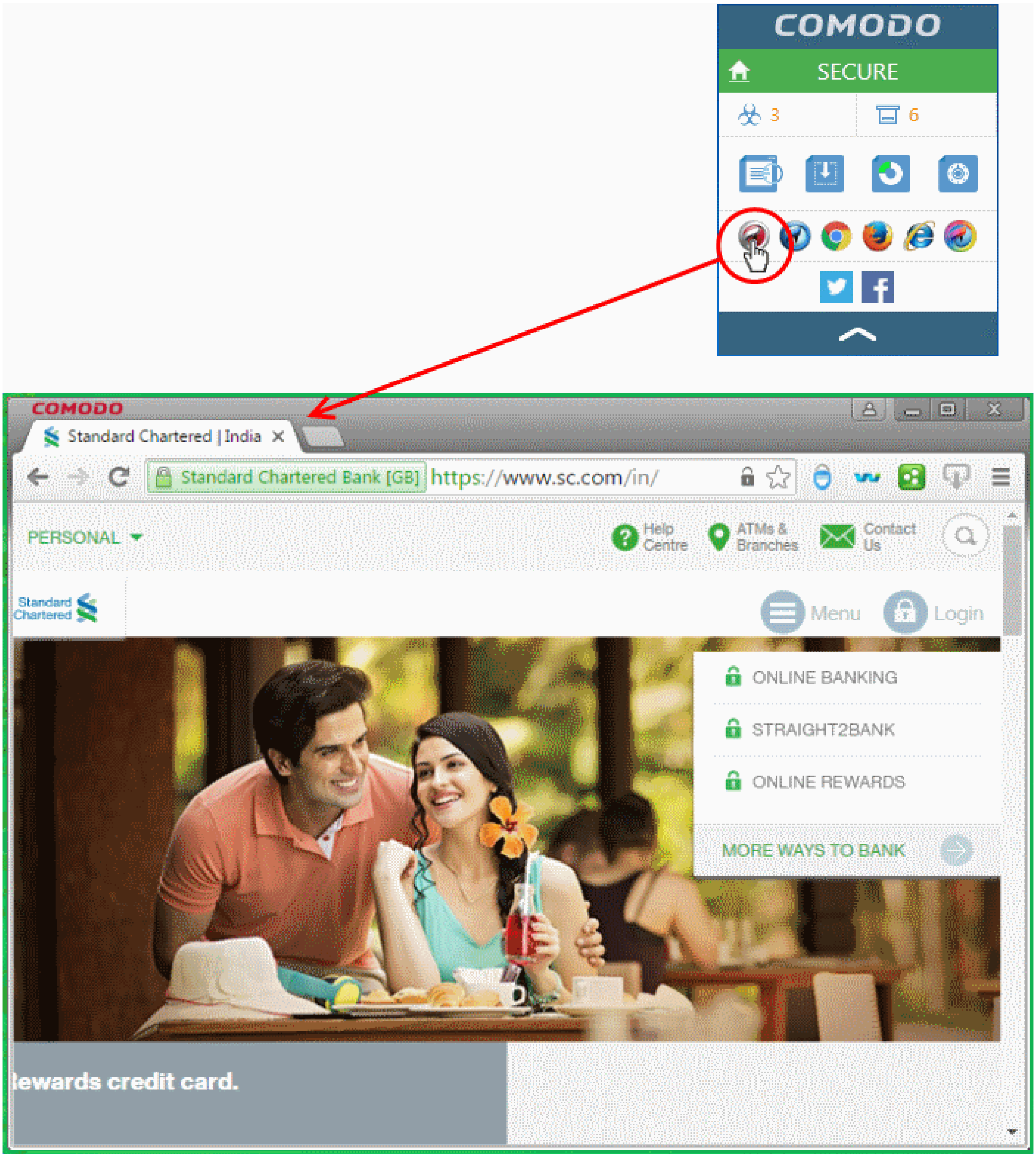
The application will start and run within the sandbox.

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 an Application in Sandbox' from the CCAV home screen and clicking on the application.

Run Browsers from Shortcuts in the Widget

The CCAV Desktop Widget displays shortcut icons of the browsers installed on your computer.

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



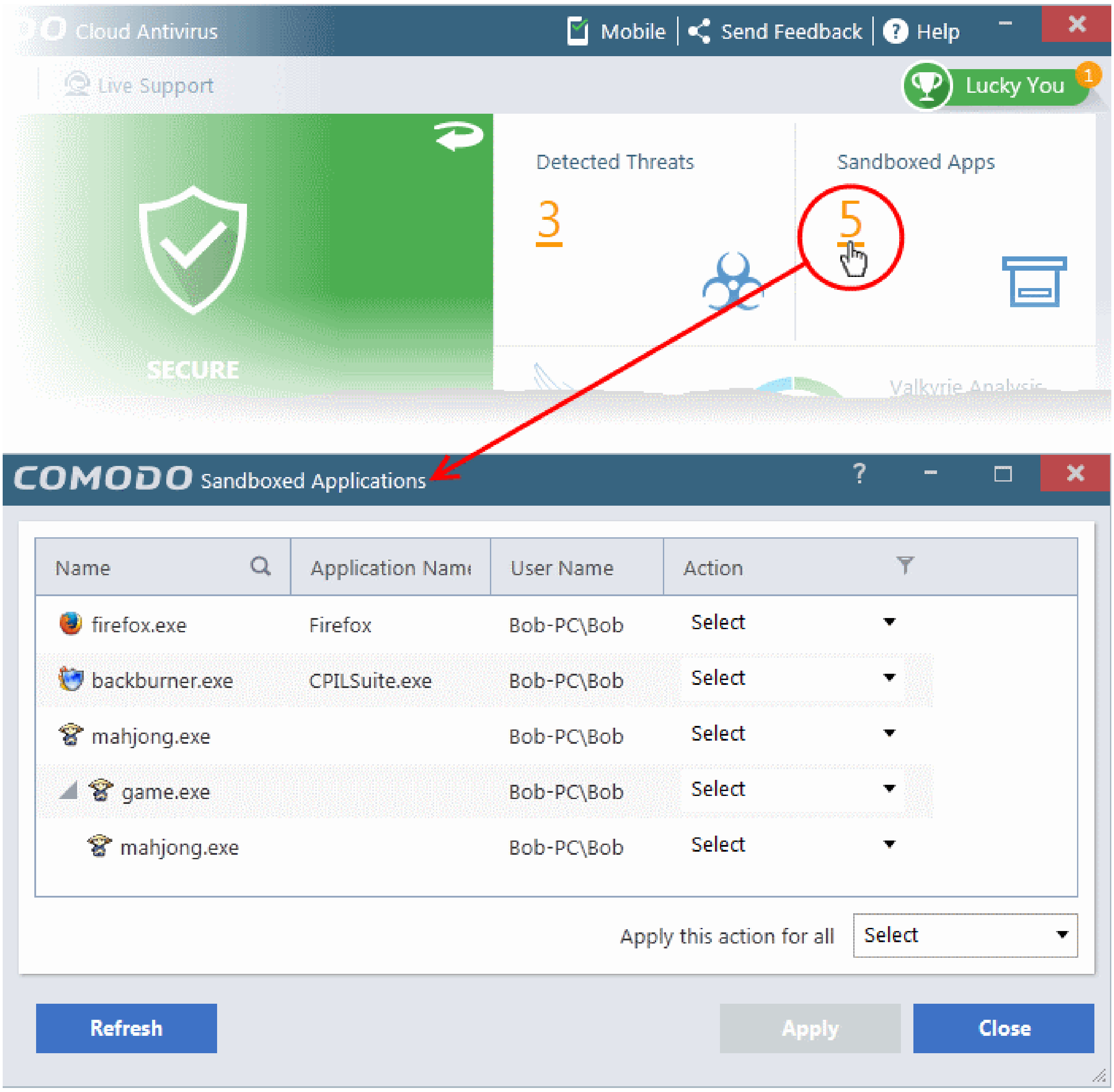
The browser will be started and executed inside the sandbox at 'Fully Virtualized' level. CCAV displays a green border around the browser window to indicate that it running inside the sandbox, if the setting 'Show highlight frame for virtualized programs' is enabled in Sandbox Settings.

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

3.2. Manage Sandboxed Items

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

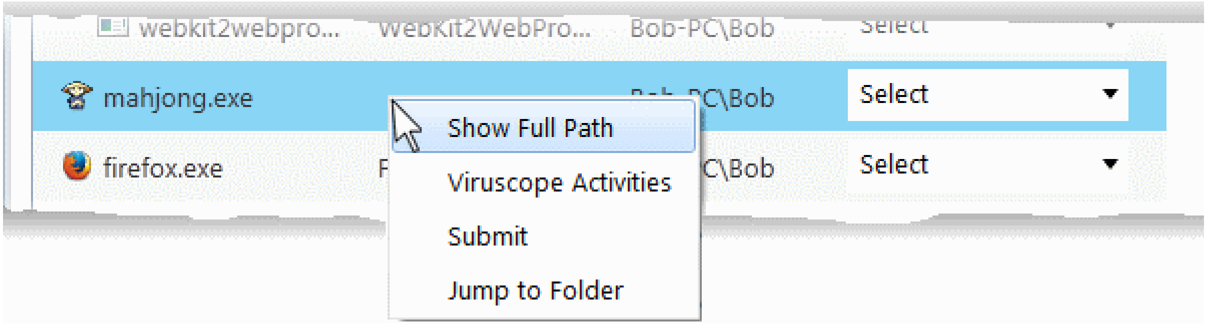
- To view and manage sandboxed applications, click the number in the 'Sandboxed Apps' section:



Name	Application Name	User Name	Action
firefox.exe	Firefox	Bob-PC\Bob	Select
backburner.exe	CPILSuite.exe	Bob-PC\Bob	Select
mahjong.exe		Bob-PC\Bob	Select
game.exe		Bob-PC\Bob	Select
mahjong.exe		Bob-PC\Bob	Select

Apply this action for all: Select

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

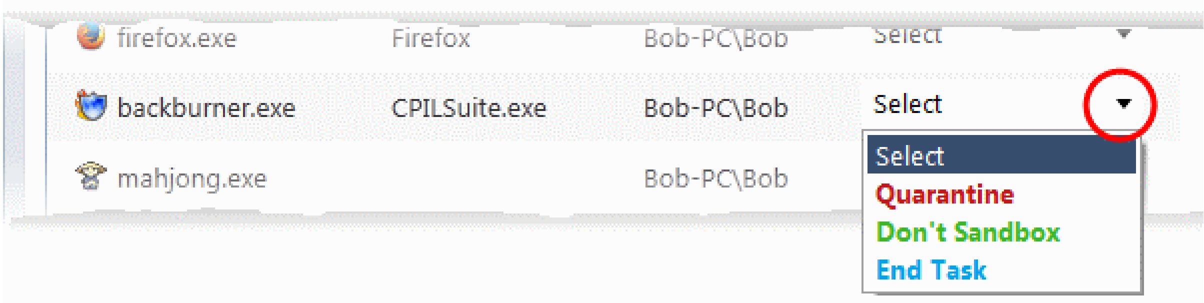


- **Show full Path** - Will display the exact storage location in which the executable resides

- **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:



firefox.exe	Firefox	Bob-PC\Bob	Select
backburner.exe	CPILSuite.exe	Bob-PC\Bob	Select
mahjong.exe		Bob-PC\Bob	

  - **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.

  Also see Sandbox Configuration and Sandbox Logs.

4. View CCAV Logs

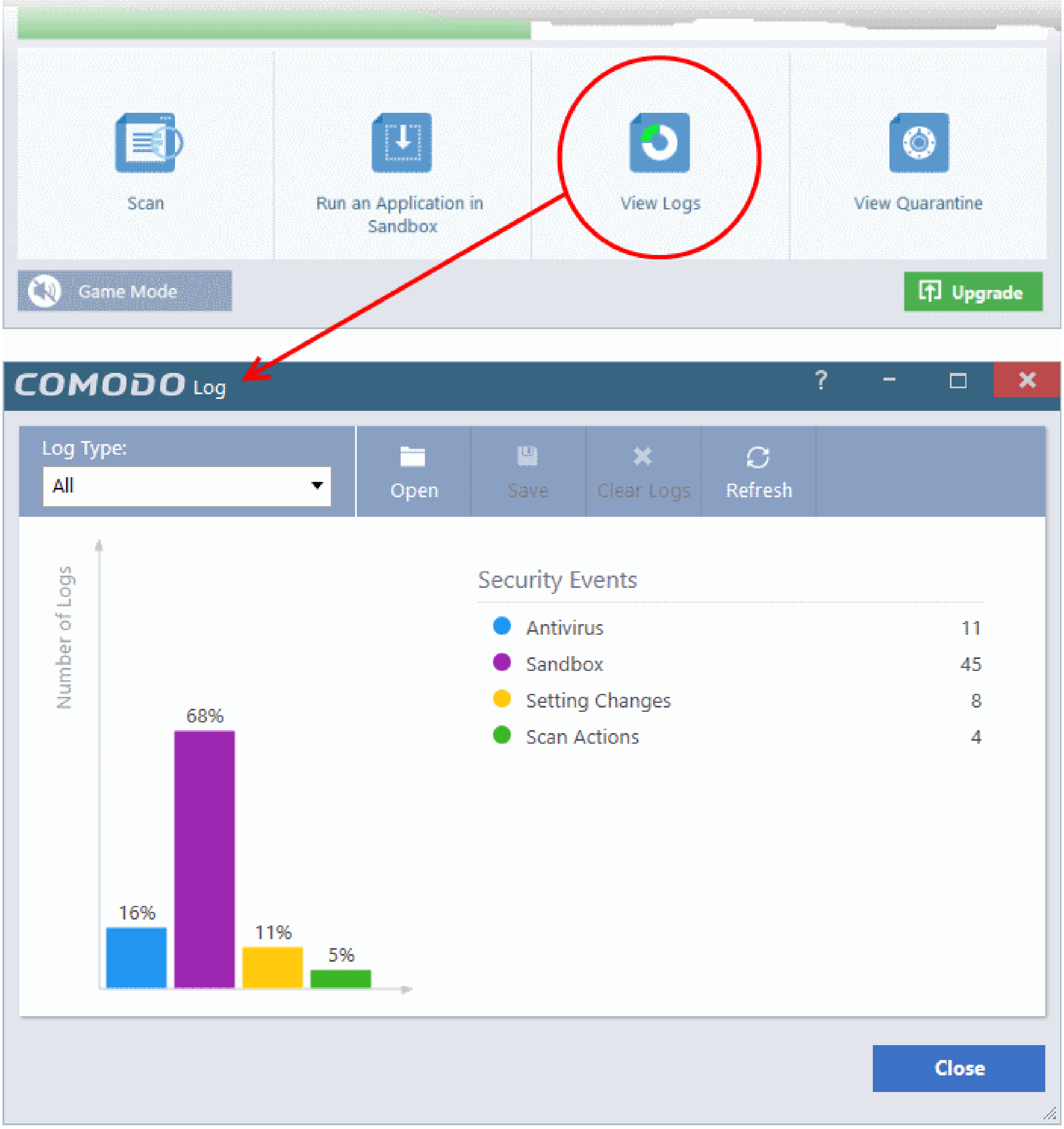
CCAV logs are records of all antivirus events, sandbox events, configuration changes and other user initiated actions. The 'Log' interface allows you to view and manage the logs.

To open the 'Log' interface

- Click 'View Logs' from the 'Tasks Bar' of the CCAV home screen

OR

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



Log Type: All

Security Events

●	Antivirus	11
●	Sandbox	45
●	Setting Changes	8
●	Scan Actions	4

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

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

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

The following sections contain more information about:

- Sandbox Logs
- Antivirus Logs

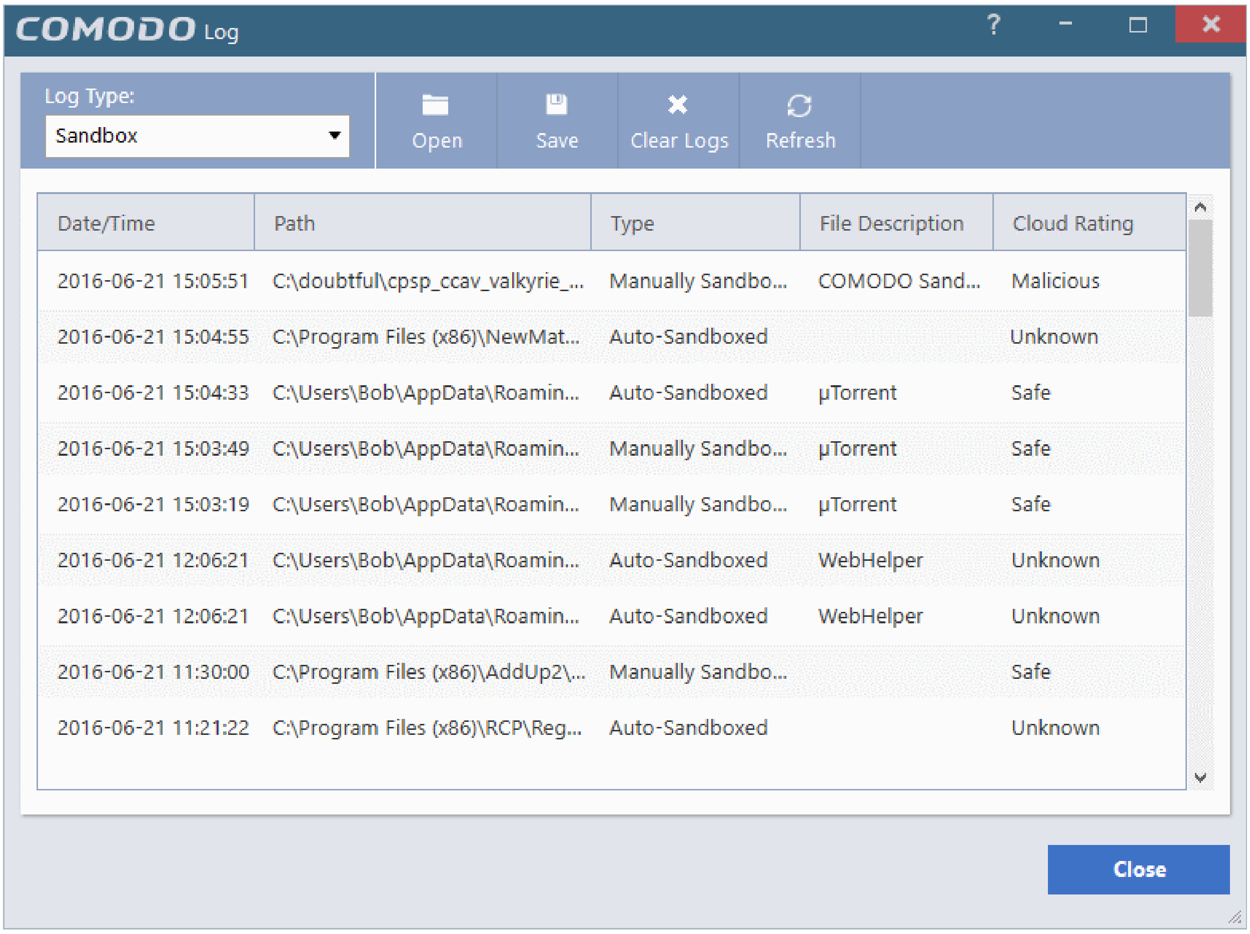
- Setting Changes Logs
- Scan Actions Logs

4.1. Sandbox Logs

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

To view Sandbox logs

- Open the 'Log' interface by clicking 'View Logs' from the home screen or clicking the 'View Logs' shortcut button from the widget
- Choose 'Sandbox' from the 'Log Type' drop down at the top left of the 'Log' interface



Log Type: Sandbox

Date/Time	Path	Type	File Description	Cloud Rating
2016-06-21 15:05:51	C:\doubtful\cpsp_ccav_valkyrie_...	Manually Sandbo...	COMODO Sand...	Malicious
2016-06-21 15:04:55	C:\Program Files (x86)\NewMat...	Auto-Sandboxed		Unknown
2016-06-21 15:04:33	C:\Users\Bob\AppData\Roamin...	Auto-Sandboxed	µTorrent	Safe
2016-06-21 15:03:49	C:\Users\Bob\AppData\Roamin...	Manually Sandbo...	µTorrent	Safe
2016-06-21 15:03:19	C:\Users\Bob\AppData\Roamin...	Manually Sandbo...	µTorrent	Safe
2016-06-21 12:06:21	C:\Users\Bob\AppData\Roamin...	Auto-Sandboxed	WebHelper	Unknown
2016-06-21 12:06:21	C:\Users\Bob\AppData\Roamin...	Auto-Sandboxed	WebHelper	Unknown
2016-06-21 11:30:00	C:\Program Files (x86)\AddUp2\...	Manually Sandbo...		Safe
2016-06-21 11:21:22	C:\Program Files (x86)\RCP\Reg...	Auto-Sandboxed		Unknown

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. **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

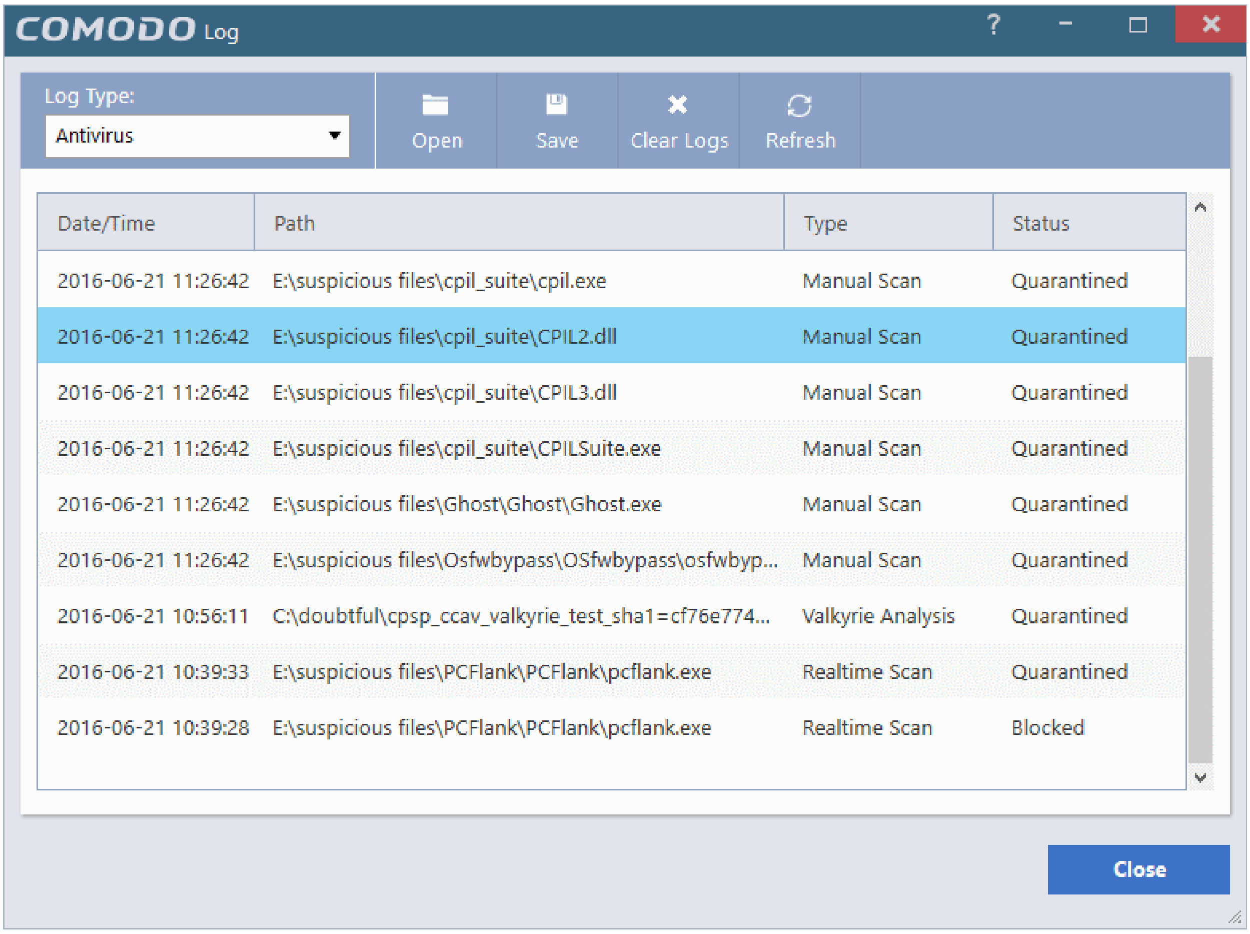
- To clear the 'Sandbox' logs, click the 'Clear logs' button.

4.2. Antivirus Logs

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

To view Antivirus logs

- Open the 'Log' interface by clicking 'View Logs' from the home screen or clicking the 'View Logs' shortcut button from the widget
- Choose 'Antivirus' from the 'Log Type' drop down at the top left of the 'Log' interface



Date/Time	Path	Type	Status
2016-06-21 11:26:42	E:\suspicious files\cpil_suite\cpil.exe	Manual Scan	Quarantined
2016-06-21 11:26:42	E:\suspicious files\cpil_suite\CPIL2.dll	Manual Scan	Quarantined
2016-06-21 11:26:42	E:\suspicious files\cpil_suite\CPIL3.dll	Manual Scan	Quarantined
2016-06-21 11:26:42	E:\suspicious files\cpil_suite\CPILSuite.exe	Manual Scan	Quarantined
2016-06-21 11:26:42	E:\suspicious files\Ghost\Ghost\Ghost.exe	Manual Scan	Quarantined
2016-06-21 11:26:42	E:\suspicious files\Osfwbypass\OSfwbypass\osfwbyp...	Manual Scan	Quarantined
2016-06-21 10:56:11	C:\doubtful\cpsp_ccav_valkyrie_test_sha1=cf76e774...	Valkyrie Analysis	Quarantined
2016-06-21 10:39:33	E:\suspicious files\PCFlank\PCFlank\pcflank.exe	Realtime Scan	Quarantined
2016-06-21 10:39:28	E:\suspicious files\PCFlank\PCFlank\pcflank.exe	Realtime Scan	Blocked

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' or 'Quarantined'

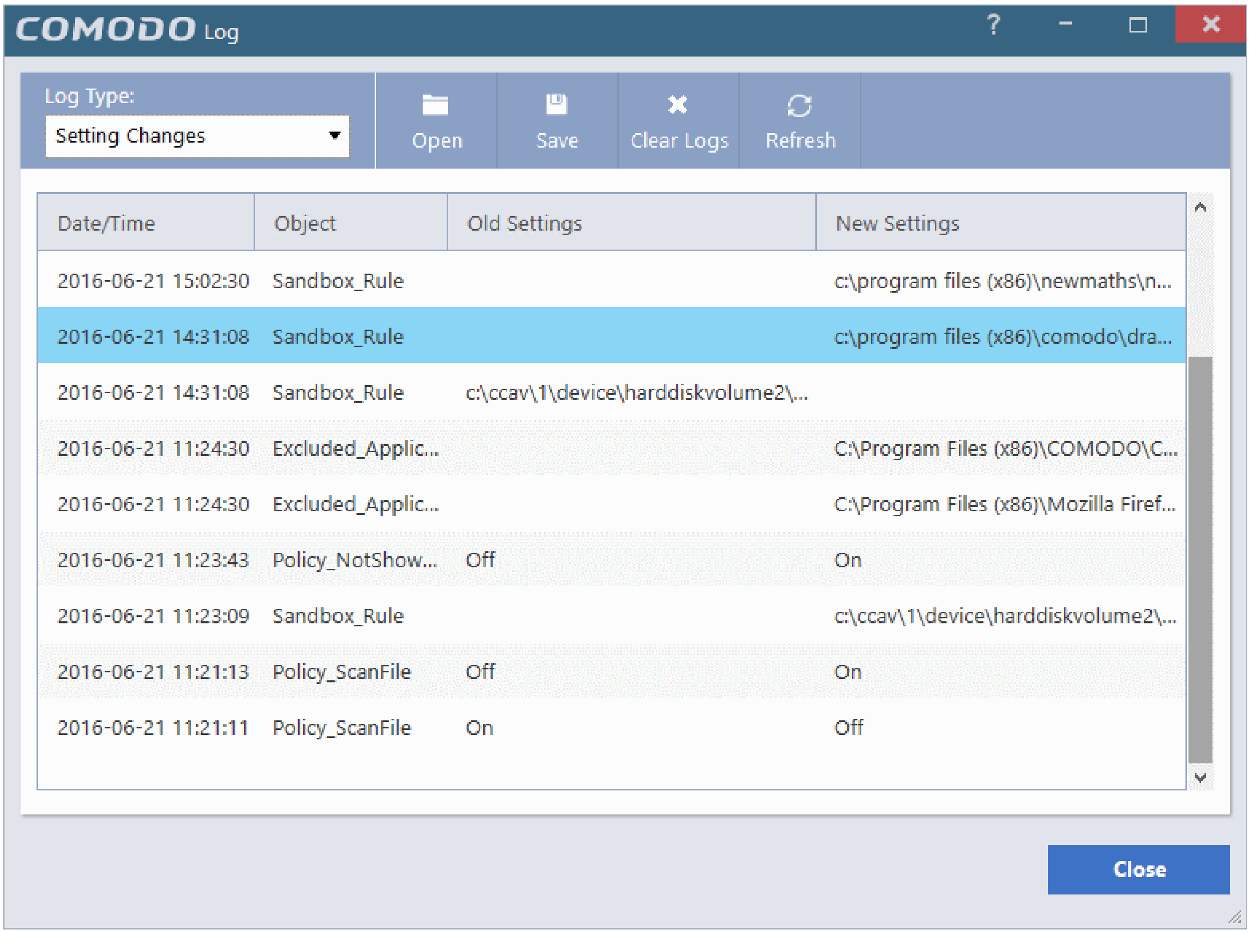
- To export the logs as a '.log' file, click the 'Save' button
- To open a stored log file, click the 'Open log file' button
- To update the list with the latest antivirus events, click the 'Refresh' button
- To clear the antivirus logs, click the 'Clear logs' button.

4.3. Setting Changes Logs

CCAV records all software configuration changes that you make, as the 'Setting Changes' logs.

To view 'Setting Changes' logs

- Open the 'Log' interface by clicking 'View Logs' from the home screen or clicking the 'View Logs' shortcut button from the widget
- Choose 'Setting Changes' from the 'Log Type' drop down at the top left of the 'Log' interface



Date/Time	Object	Old Settings	New Settings
2016-06-21 15:02:30	Sandbox_Rule		c:\program files (x86)\newmaths\n...
2016-06-21 14:31:08	Sandbox_Rule		c:\program files (x86)\comodo\dra...
2016-06-21 14:31:08	Sandbox_Rule	c:\ccav\1\device\harddiskvolume2\...	
2016-06-21 11:24:30	Excluded_Applic...		C:\Program Files (x86)\COMODO\C...
2016-06-21 11:24:30	Excluded_Applic...		C:\Program Files (x86)\Mozilla Firef...
2016-06-21 11:23:43	Policy_NotShow...	Off	On
2016-06-21 11:23:09	Sandbox_Rule		c:\ccav\1\device\harddiskvolume2\...
2016-06-21 11:21:13	Policy_ScanFile	Off	On
2016-06-21 11:21:11	Policy_ScanFile	On	Off

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

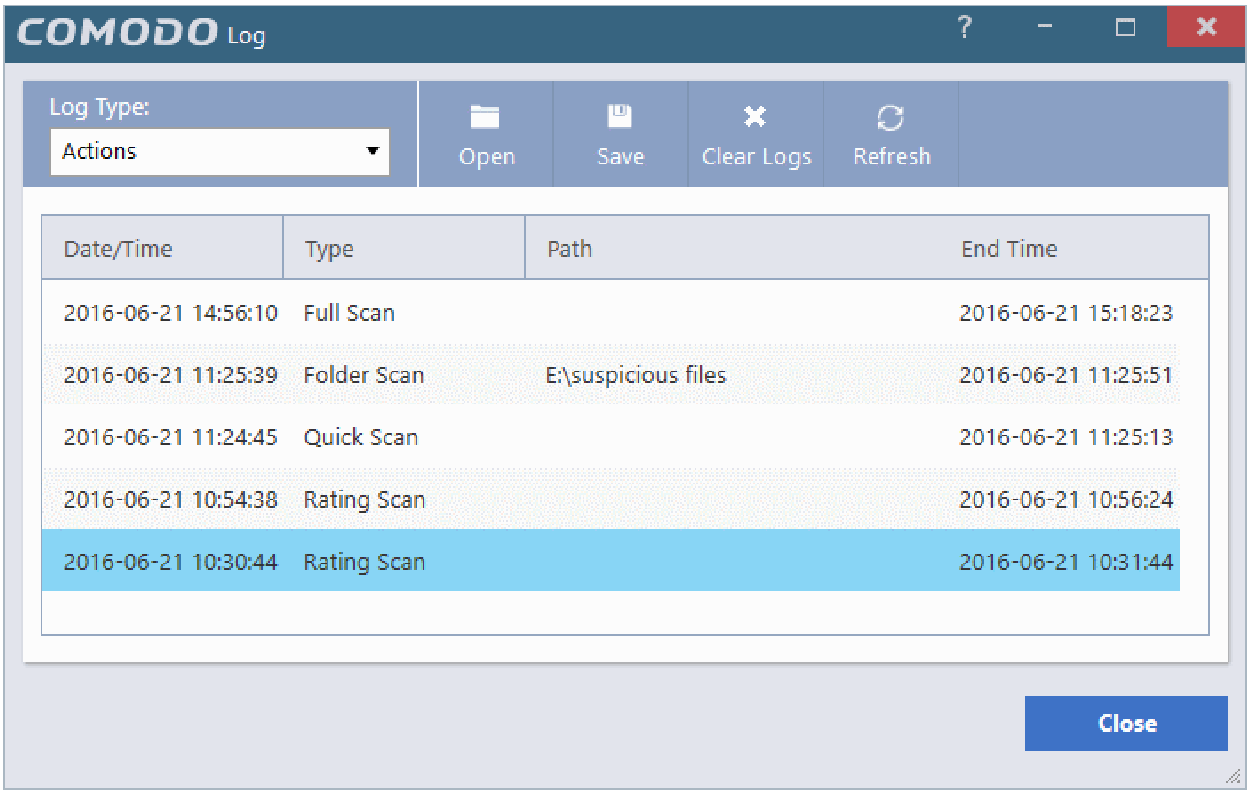
- To export the logs as a '.log' file, click the 'Save' button
- To open a stored log file, click the 'Open log file' button
- To update the list with the latest events, click the 'Refresh' button
- To clear the 'Setting Changes' logs, click the 'Clear logs' button.

4.4. Scan Actions Logs

CCAV keeps a record of all manually initiated virus scans. This includes manually started Full scans, Quick scans, Rating scans and custom scans and those started by right clicking on an item and choosing 'Scan with Comodo Cloud Antivirus'. Refer to the section Scan and Clean your Computer for more details.

To view 'Actions' logs

- Open the 'Log' interface by clicking 'View Logs' from the home screen or clicking the 'View Logs' shortcut button from the widget
- Choose 'Actions' from the 'Log Type' drop down at the top left of the 'Log' interface



Date/Time	Type	Path	End Time
2016-06-21 14:56:10	Full Scan		2016-06-21 15:18:23
2016-06-21 11:25:39	Folder Scan	E:\suspicious files	2016-06-21 11:25:51
2016-06-21 11:24:45	Quick Scan		2016-06-21 11:25:13
2016-06-21 10:54:38	Rating Scan		2016-06-21 10:56:24
2016-06-21 10:30:44	Rating Scan		2016-06-21 10:31:44

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

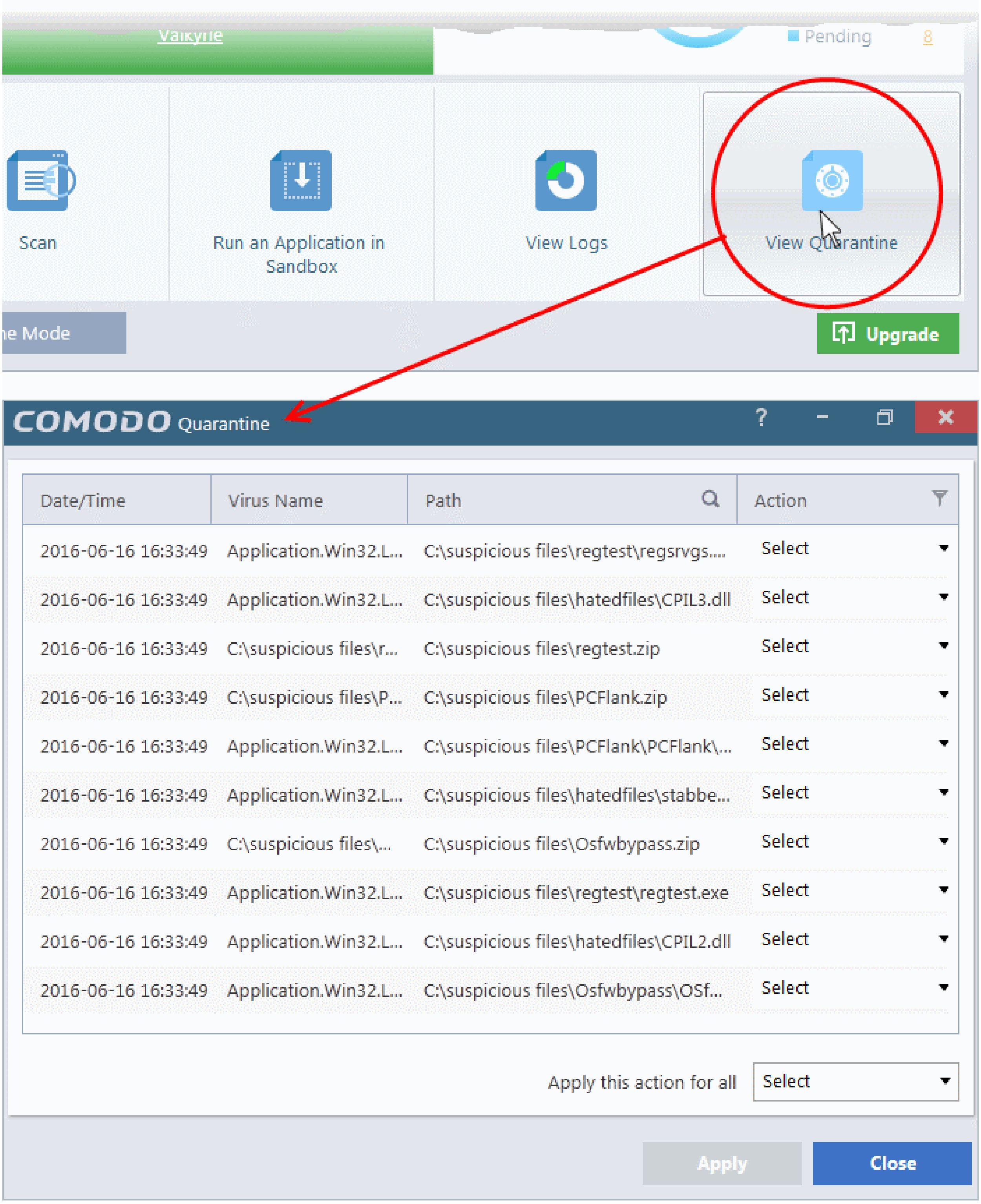
5. View and Manage Quarantined Items

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.

- To open the 'Quarantine' interface, click 'View Quarantine' from the home screen.

OR

- Click the 'Quarantine' icon from the CCAV desktop widget

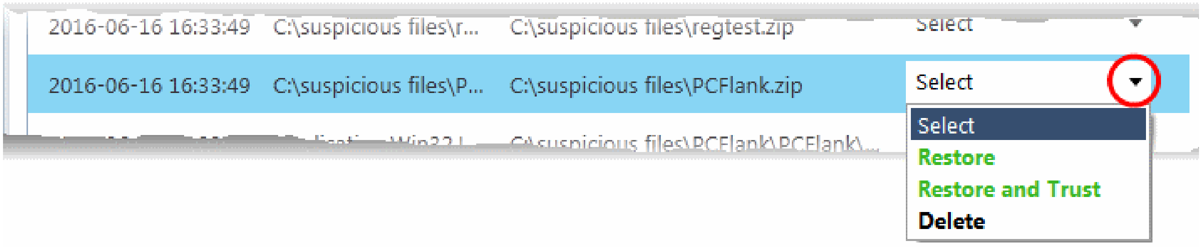


Date/Time	Virus Name	Path	Action
2016-06-16 16:33:49	Application.Win32.L...	C:\suspicious files\regtest\regsrvgs....	Select
2016-06-16 16:33:49	Application.Win32.L...	C:\suspicious files\hatedfiles\CPIL3.dll	Select
2016-06-16 16:33:49	C:\suspicious files\r...	C:\suspicious files\regtest.zip	Select
2016-06-16 16:33:49	C:\suspicious files\P...	C:\suspicious files\PCFlank.zip	Select
2016-06-16 16:33:49	Application.Win32.L...	C:\suspicious files\PCFlank\PCFlank\...	Select
2016-06-16 16:33:49	Application.Win32.L...	C:\suspicious files\hatedfiles\stabbe...	Select
2016-06-16 16:33:49	C:\suspicious files\...	C:\suspicious files\Osfwbypass.zip	Select
2016-06-16 16:33:49	Application.Win32.L...	C:\suspicious files\regtest\regtest.exe	Select
2016-06-16 16:33:49	Application.Win32.L...	C:\suspicious files\hatedfiles\CPIL2.dll	Select
2016-06-16 16:33:49	Application.Win32.L...	C:\suspicious files\Osfwbypass\OSf...	Select

Apply this action for all: Select

Column Descriptions

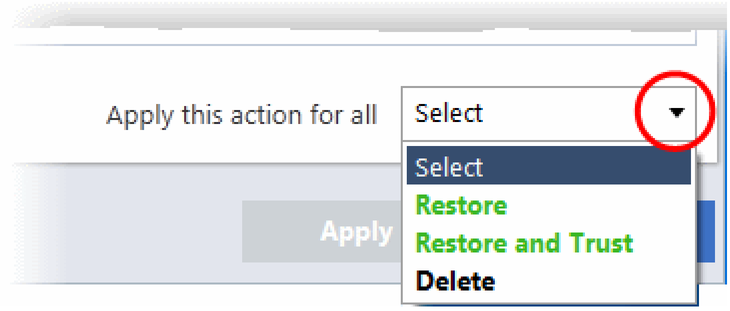
- **Date/Time** - The precise date and time at which the item was moved to quarantine
- **Virus Name** - The name of the malware that was quarantined
- **Path** - The location where the file was discovered
- **Action** - Displays a drop-down with options for handling the item.


2016-06-16 16:33:49 C:\suspicious files\r... C:\suspicious files\regtest.zip Select
2016-06-16 16:33:49 C:\suspicious files\P... C:\suspicious files\PCFlank.zip Select
C:\suspicious files\PCFlank\PCFlank\...
Select
Restore
Restore and Trust
Delete

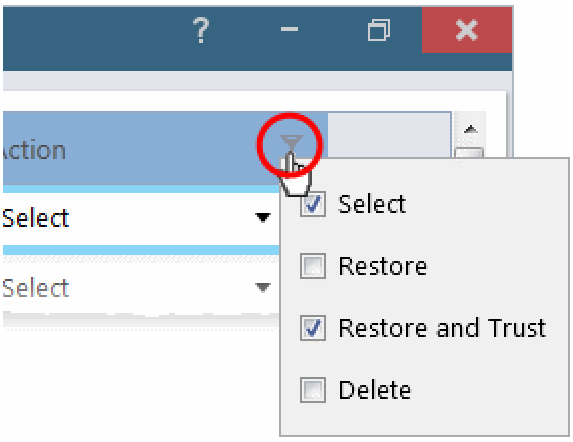
The available actions are:

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

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



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



The 'Quarantine' interface also allows you to:

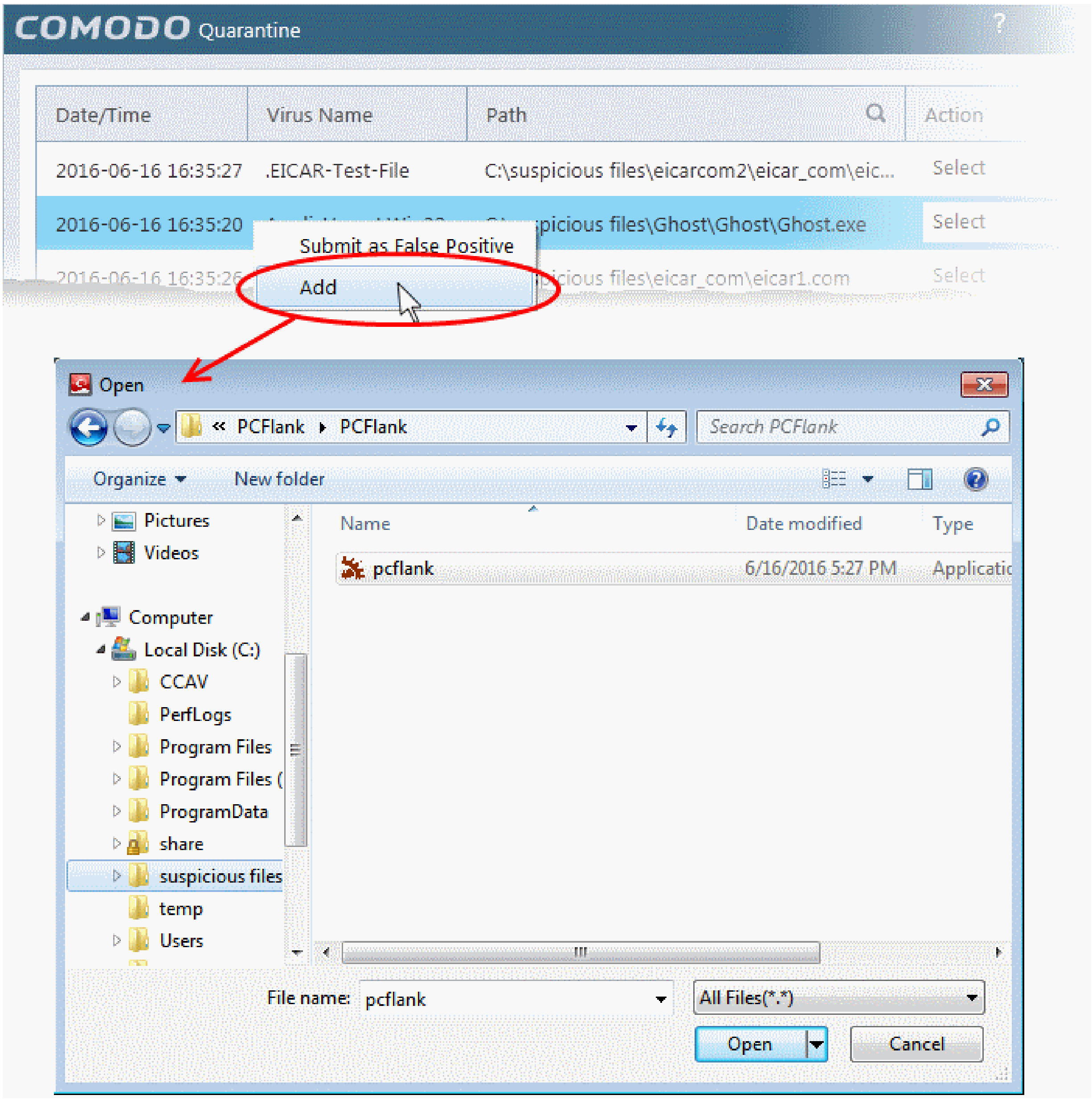
- Manually add items to quarantine
- Delete quarantined items
- Restore a quarantined item to its original location
- Submit false positives to Comodo for analysis

Manually add items to quarantine

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

To manually add a Quarantined Item

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



Date/Time	Virus Name	Path	Action
2016-06-16 16:35:27	.EICAR-Test-File	C:\suspicious files\eicarcom2\eicar_com\eic...	Select
2016-06-16 16:35:20		...picious files\Ghost\Ghost\Ghost.exe	Select
2016-06-16 16:35:26		...picious files\eicar_com\eicar1.com	Select

Name	Date modified	Type
pcflank	6/16/2016 5:27 PM	Applicatio

File name: pcflank

- Click 'Apply' to quarantine the file

To delete quarantined item(s)

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

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

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

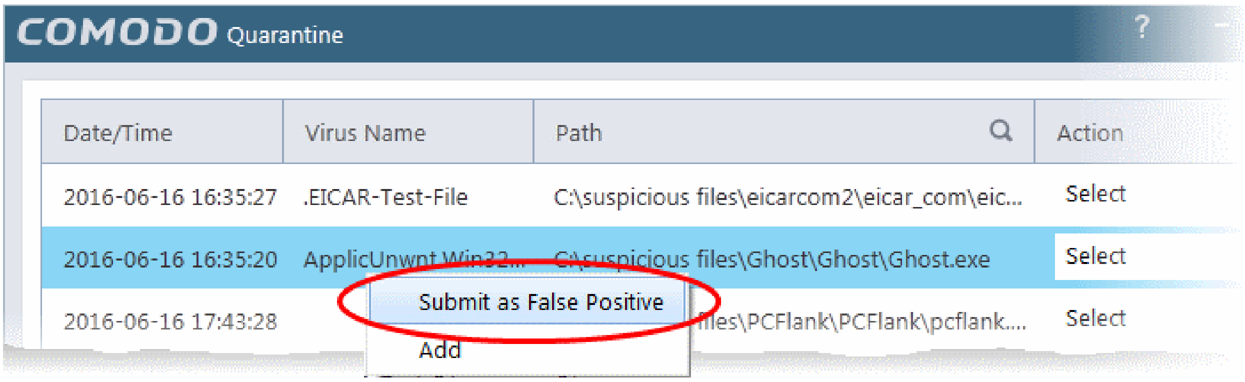
- To restore a single item, choose 'Restore' from the 'Action' drop-down in the item row.
- To restore a single item and exclude it from future scans, choose 'Restore and Trust' from the 'Action' drop-down in the item row.
- To restore all items, choose 'Restore' from the 'Apply this action to all' drop-down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

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

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

To submit a selected quarantined item to Comodo for analysis

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



Date/Time	Virus Name	Path	Action
2016-06-16 16:35:27	.EICAR-Test-File	C:\suspicious files\eicarcom2\eicar_com\eic...	Select
2016-06-16 16:35:20	ApplicUnwnt.Win32...	C:\suspicious files\Ghost\Ghost\Ghost.exe	Select
2016-06-16 17:43:28		files\PCFlank\PCFlank\pcflank....	Select

- Click 'Apply' for your changes to take effect

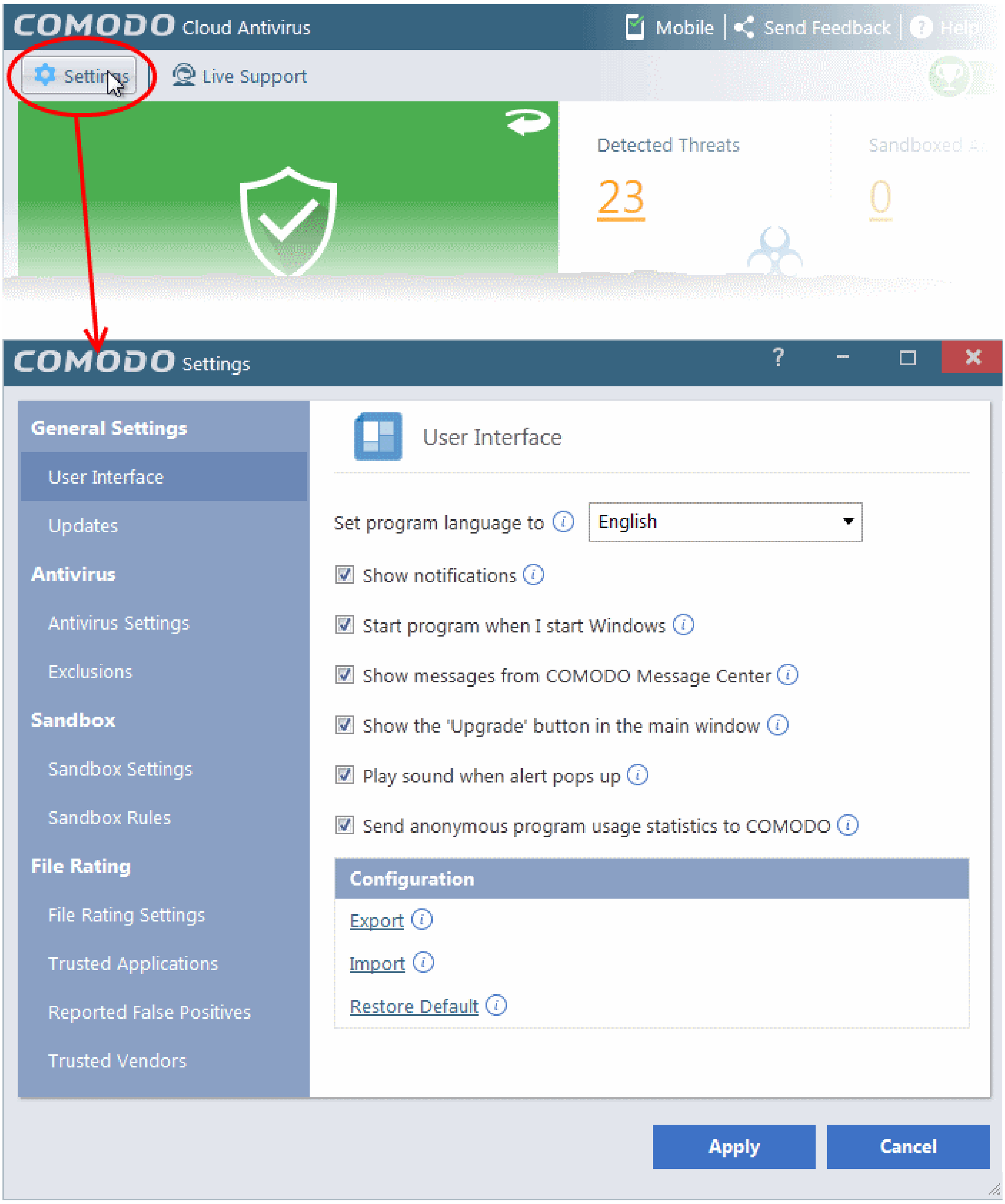
You can submit suspicious files to Comodo for deeper analysis. You can also submit files which you think are safe but have been identified as malware by CCAV (false positives). Comodo will analyze all submitted files. If they are found to be trustworthy, they will be added to the Comodo safe list (whitelisted).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

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

6. CCAV Settings

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

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



COMODO Settings

- General Settings
  - User Interface
  - Updates
- Antivirus
  - Antivirus Settings
  - Exclusions
- Sandbox
  - Sandbox Settings
  - Sandbox Rules
- File Rating
  - File Rating Settings
  - Trusted Applications
  - Reported False Positives
  - Trusted Vendors

User Interface

Set program language to: English

☑ Show notifications

☑ Start program when I start Windows

☑ Show messages from COMODO Message Center

☑ Show the 'Upgrade' button in the main window

☑ Play sound when alert pops up

☑ Send anonymous program usage statistics to COMODO

Configuration

Export

Import

Restore Default

Apply | Cancel

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

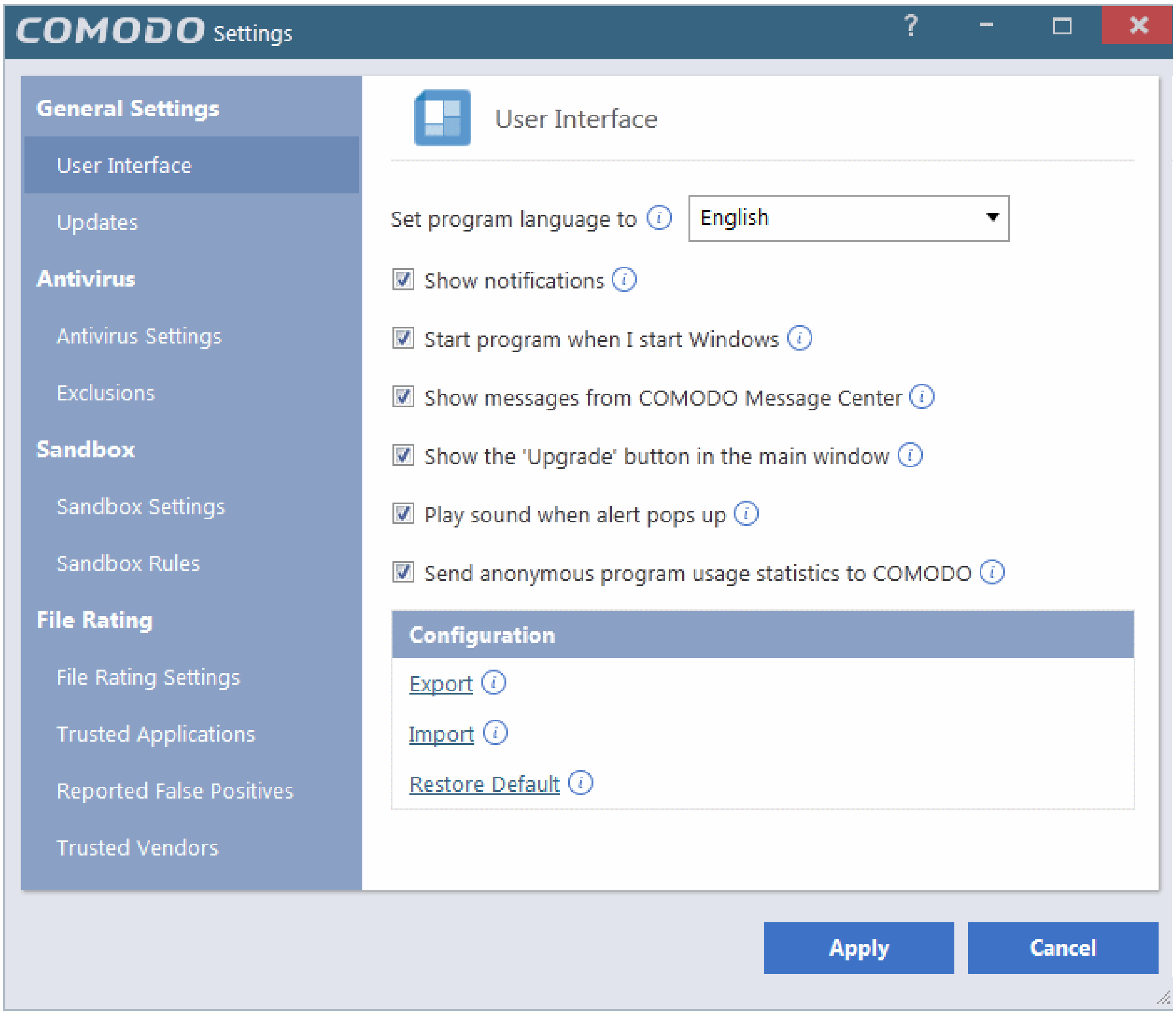
- General Settings - Allows you to configure the appearance and behavior of the application
  - Customize User Interface
  - Configure Program and Updates
- Antivirus - Allows you to configure the 'Antivirus' module
  - Antivirus Settings
  - Exclusions
- Sandbox - Allows you to configure the 'Sandbox'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

- Sandbox Rules

- File Rating - Allows you to view and manage Trusted applications list, files submitted to Comodo and Trusted Vendors list
    - File Rating Settings
    - Trusted Applications
    - Submitted Files
    - Trusted Vendors List

6.1. General Settings

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



Set program language to English

☑ Show notifications

☑ Start program when I start Windows

☑ Show messages from COMODO Message Center

☑ Show the 'Upgrade' button in the main window

☑ Play sound when alert pops up

☑ Send anonymous program usage statistics to COMODO

Configuration

Export

Import

Restore Default

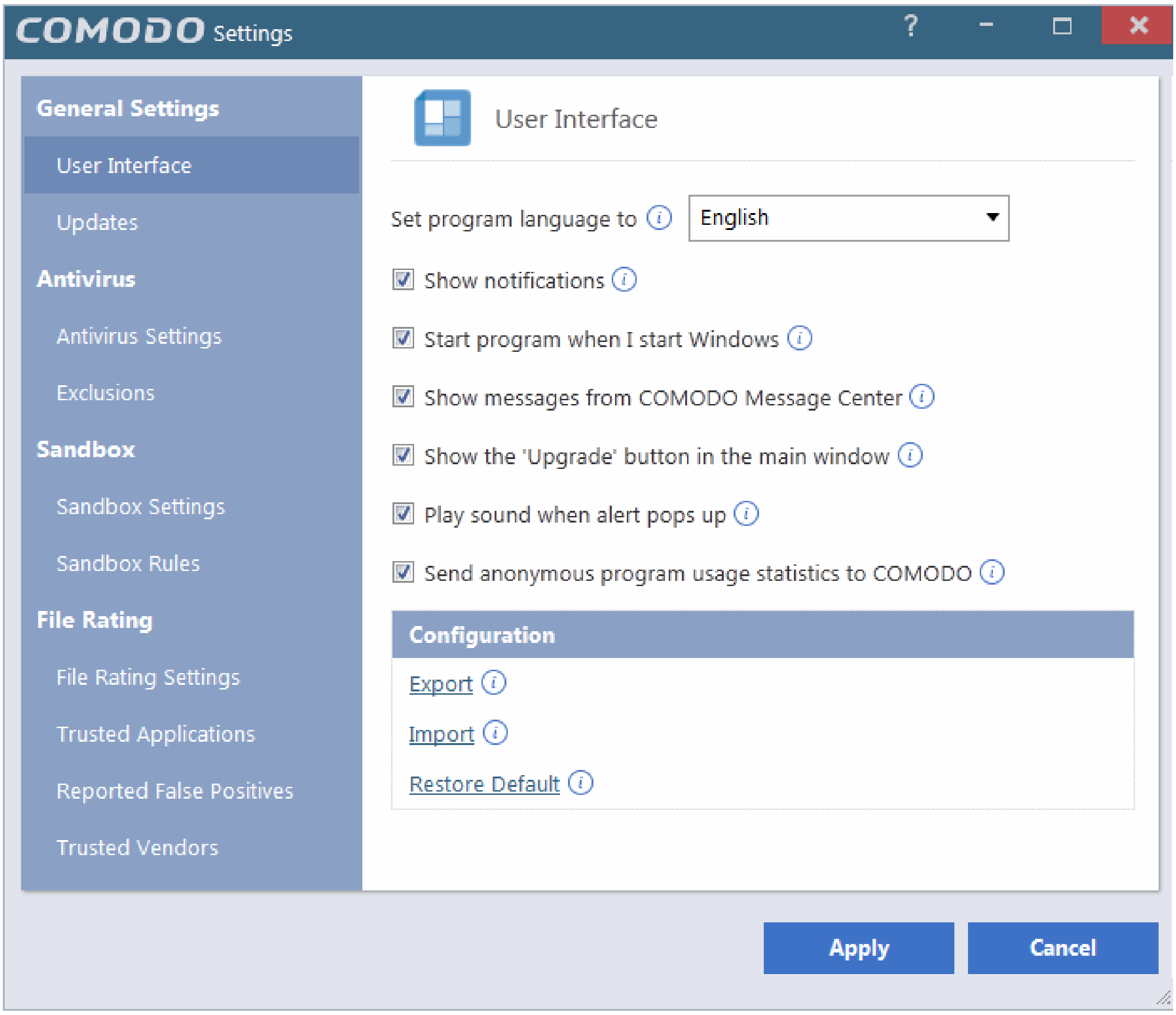
The category has the following sections:

- User Interface
- Updates

6.1.1. Customize User Interface

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

- To open 'User Interface' settings, click 'User Interface' under 'General Settings' on the left:



User Interface

Set program language to: English

☑ Show notifications

☑ Start program when I start Windows

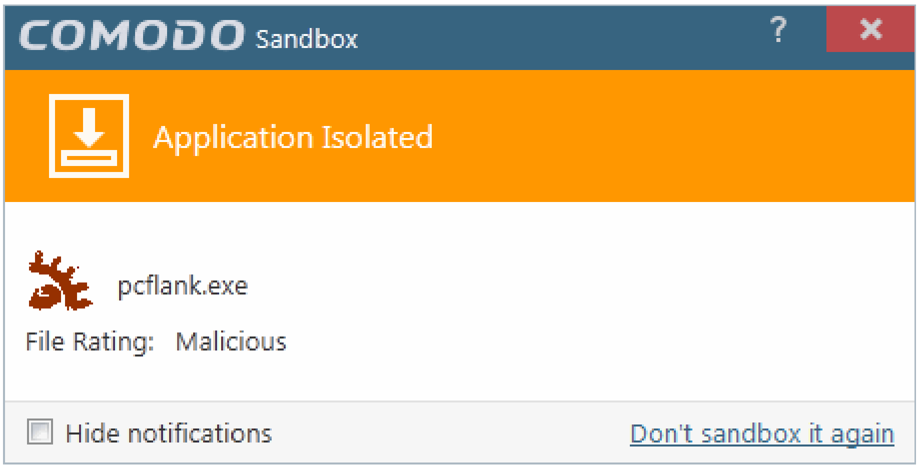
☑ Show messages from COMODO Message Center

☑ Show the 'Upgrade' button in the main window

☑ Play sound when alert pops up

☑ Send anonymous program usage statistics to COMODO

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



pcflank.exe

File Rating: Malicious

☐ Hide notifications

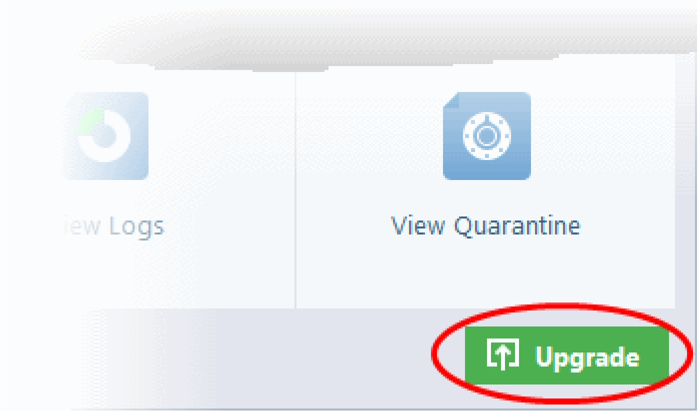
Antivirus notifications will also be displayed if you have selected 'Quarantine' or 'Block' in the 'Action when threat is detected' setting in the 'Antivirus' settings screen.

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

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

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

- **Show 'Upgrade' button' in the main window** - By default, a green 'Upgrade' button appears at the bottom right of the CCAV home screen. It allows you to upgrade your Antivirus installation to Comodo Internet Security - our full featured internet security solution. If you do not want the button to be displayed, de-select this option. ***(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 anonymized 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 and avoid having to configure everything over again.

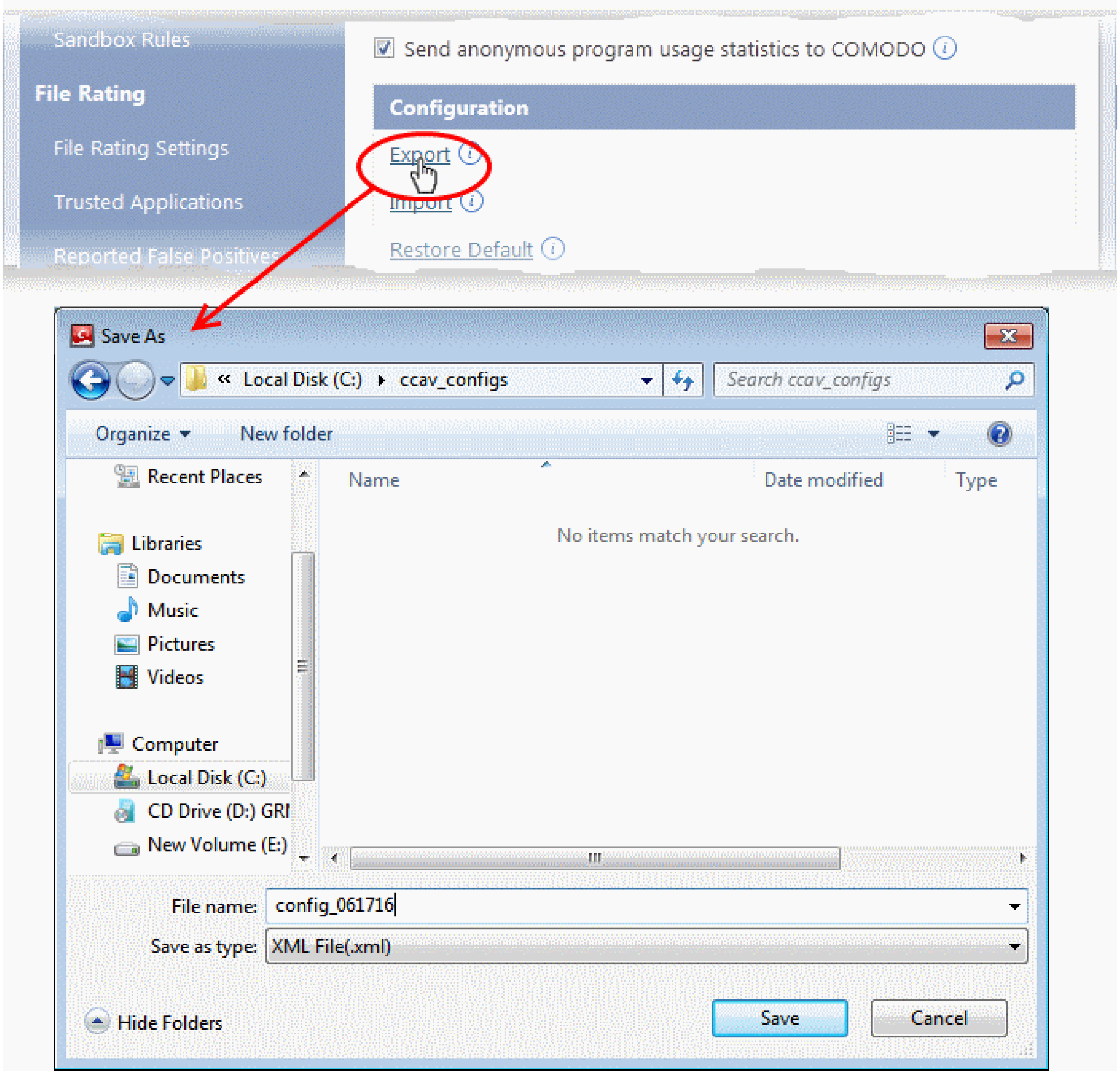
The following sections explain how to:

- 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:



☑ Send anonymous program usage statistics to COMODO

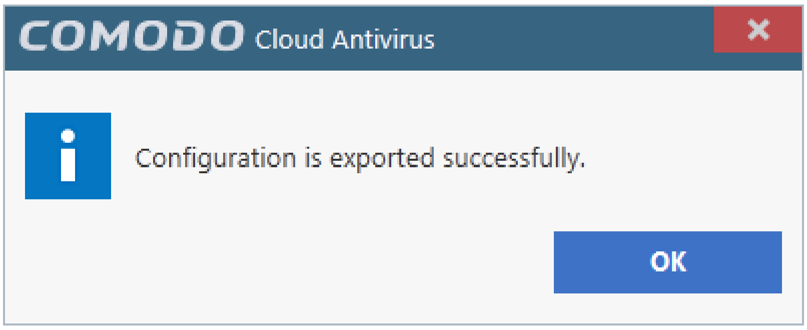
No items match your search.

File name: config_061716

Save as type: XML File(.xml)

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

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

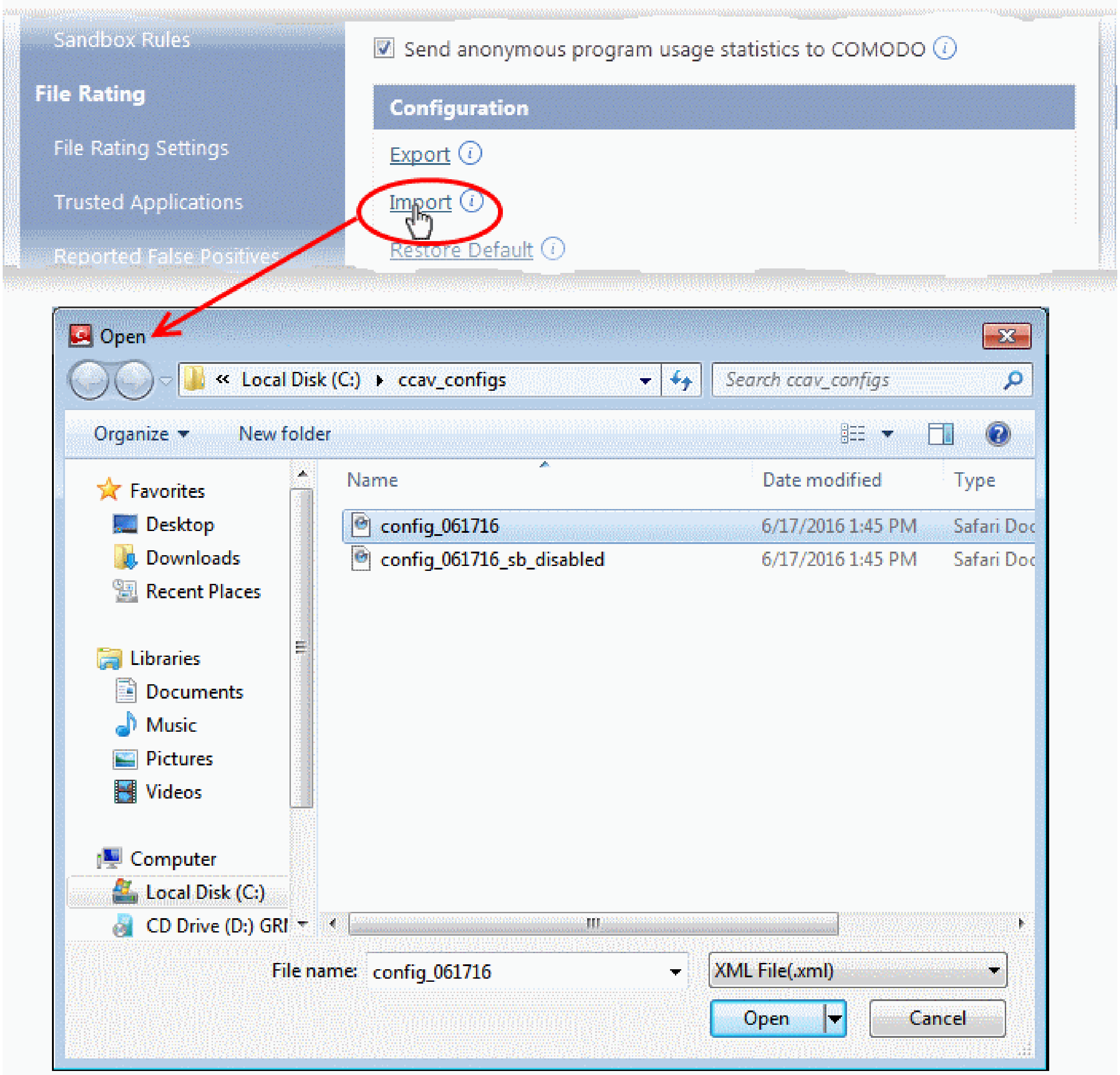


Configuration is exported successfully.

Import a saved configuration from a file

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

The 'Open' dialog will open:



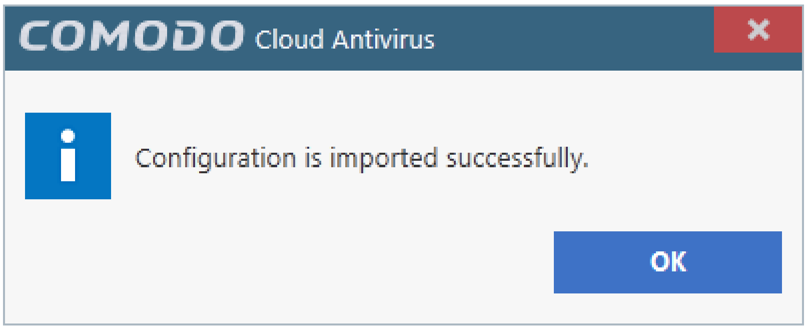
Name	Date modified	Type
config_061716	6/17/2016 1:45 PM	Safari Doc
config_061716_sb_disabled	6/17/2016 1:45 PM	Safari Doc

File name: config_061716

XML File(.xml)

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

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

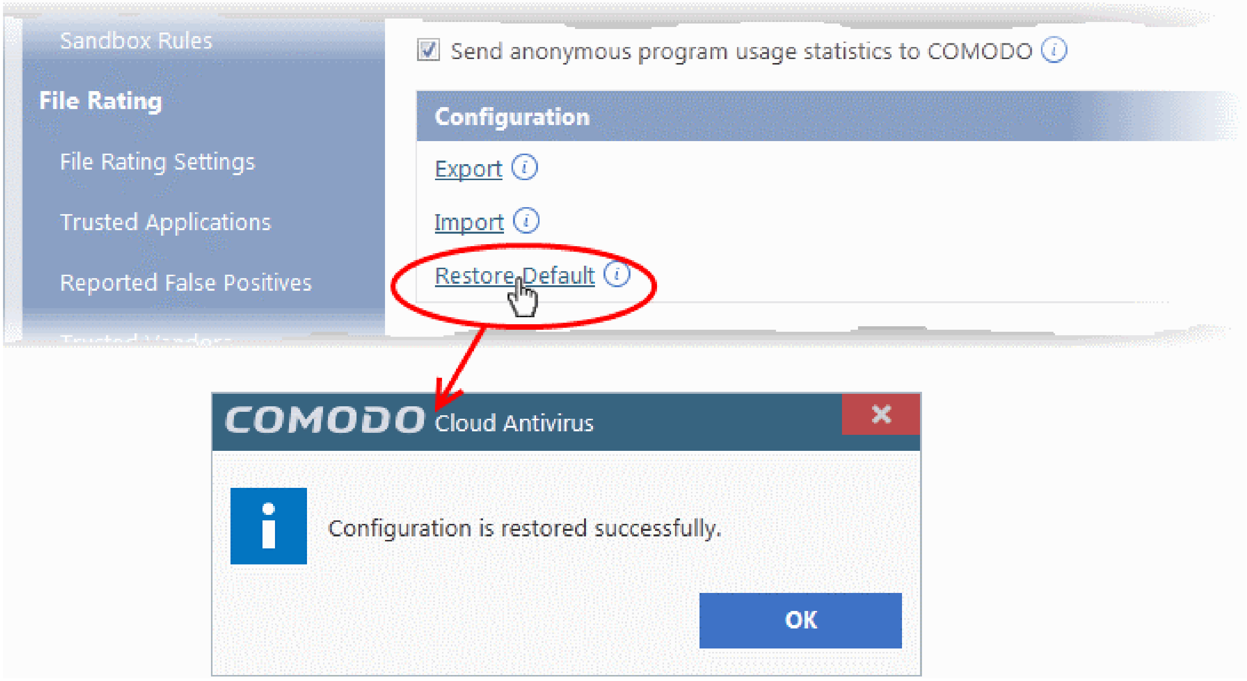


Configuration is imported successfully.

Restore your CCAV installation to Factory Default settings

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

A confirmation dialog will appear indicating successful restoration:

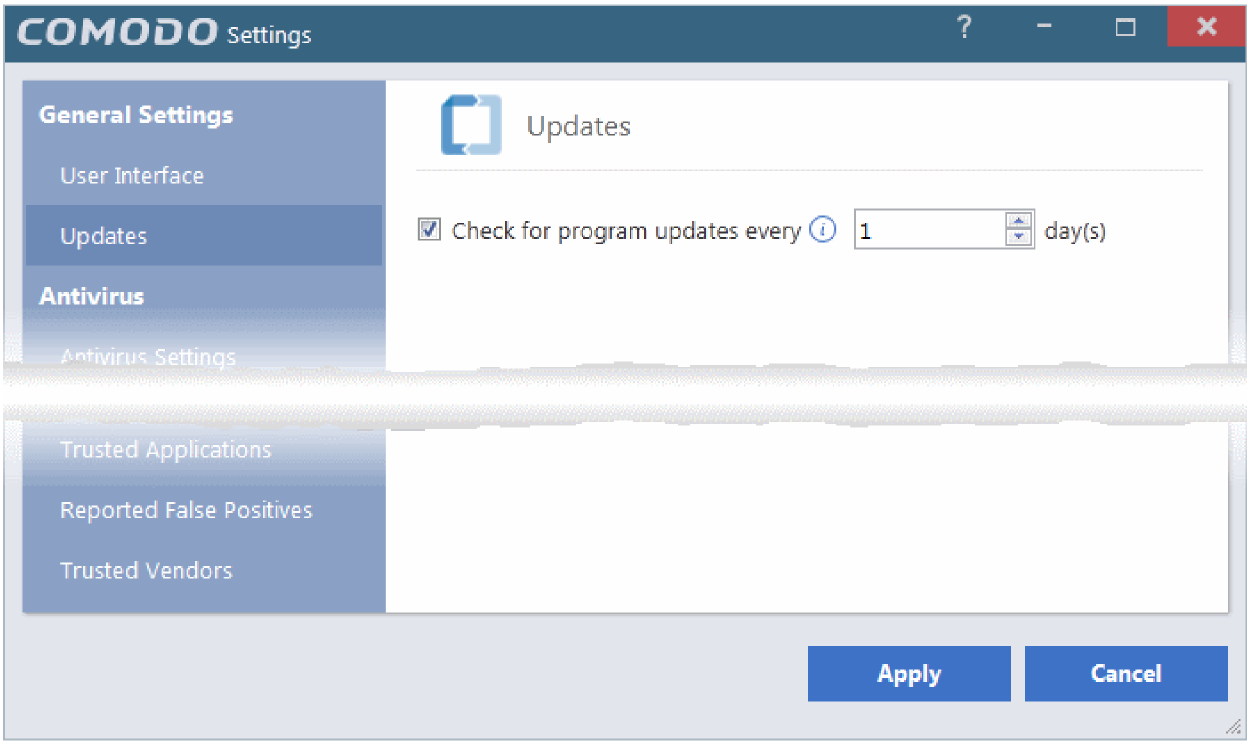


Configuration is restored successfully.

6.1.2. Configure Program Updates

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

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

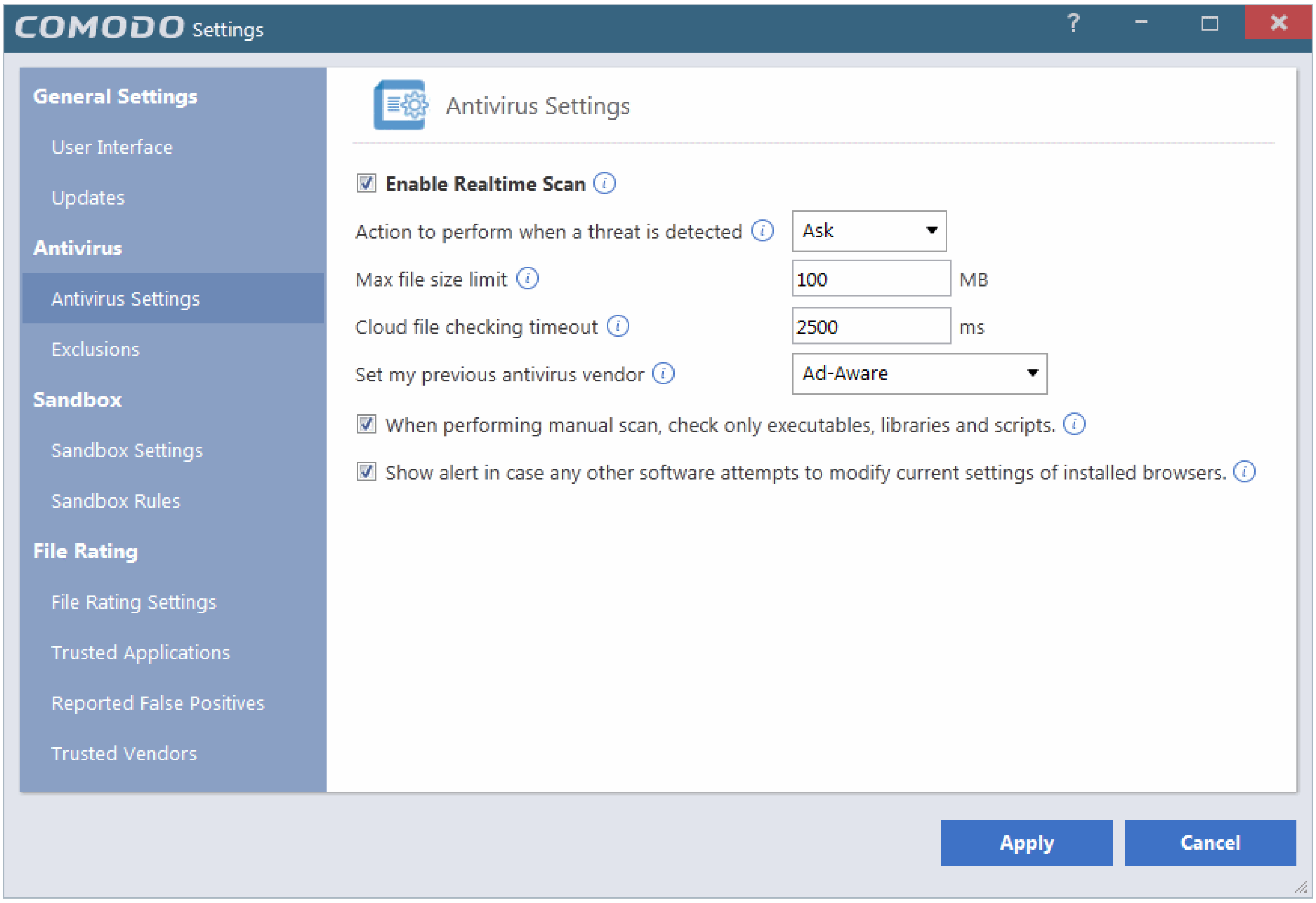


☑ Check for program updates every 1 day(s)

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

6.2. Antivirus Settings

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



☑ Enable Realtime Scan

Action to perform when a threat is detected: Ask

Max file size limit: 100 MB

Cloud file checking timeout: 2500 ms

Set my previous antivirus vendor: Ad-Aware

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

☑ Show alert in case any other software attempts to modify current settings of installed browsers.

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

- Antivirus Settings
- Exclusions

6.2.1. Antivirus Settings

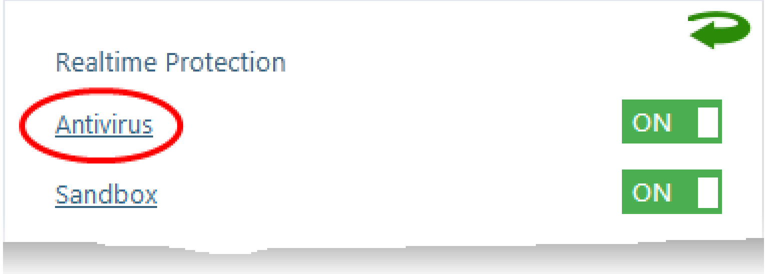
CCAV's real-time scanner constantly monitors all files and processes on your computer for potential threats. If you launch a program or file which creates destructive anomalies, then the scanner blocks it and alerts you immediately. The Antivirus settings interface allows you to enable/disable the real-time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

To open the 'Antivirus Settings' area

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

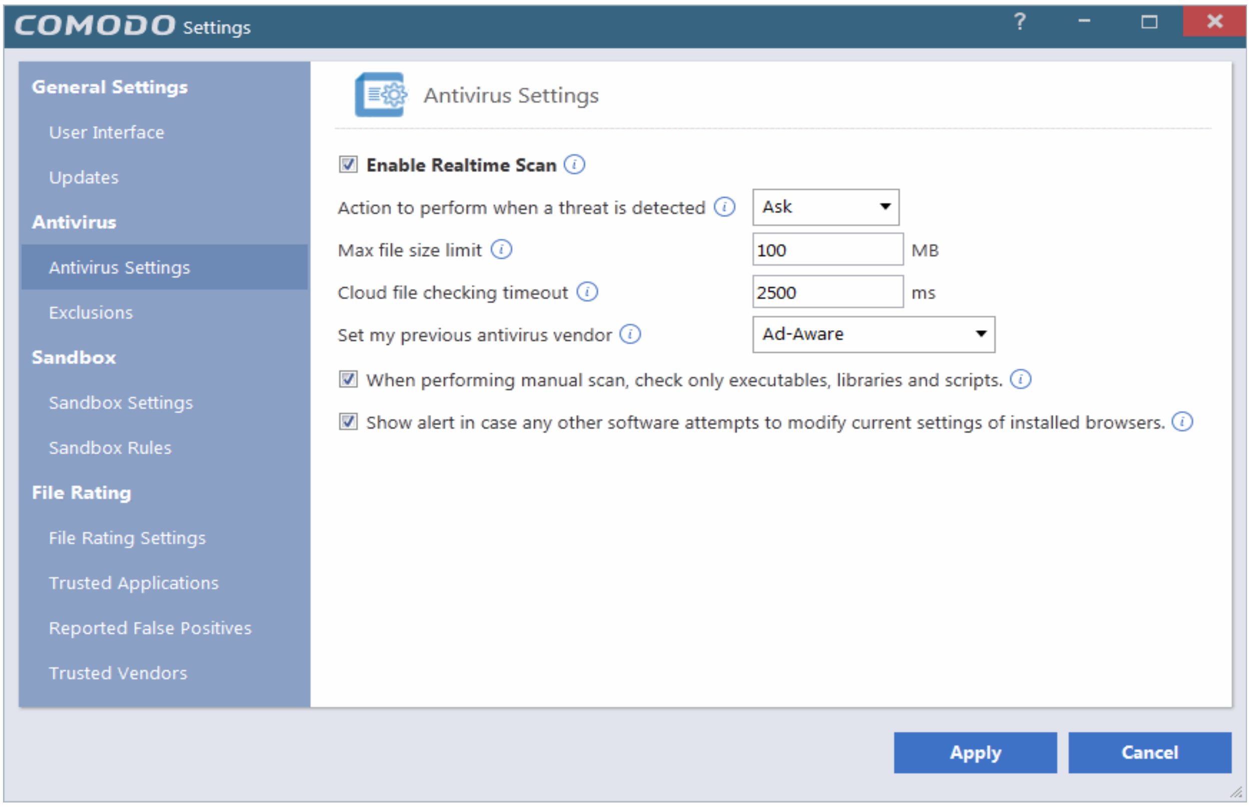
OR

- Flip the security status pane in the home screen by clicking the curved arrow and click the 'Antivirus' link under 'Realtime Protection'



OR

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



Antivirus Settings

☑ Enable Realtime Scan

Action to perform when a threat is detected: Ask

Max file size limit: 100 MB

Cloud file checking timeout: 2500 ms

Set my previous antivirus vendor: Ad-Aware

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

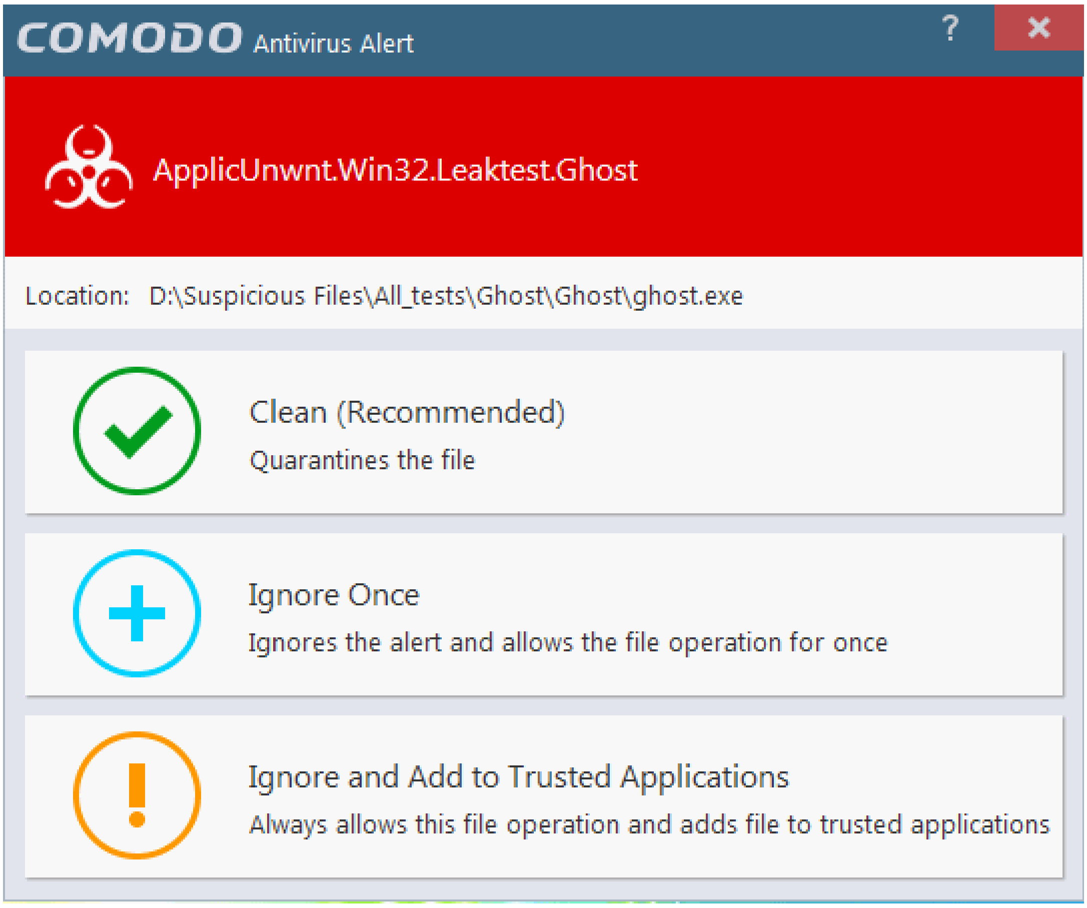
☑ Show alert in case any other software attempts to modify current settings of installed browsers.

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

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

The real-time scanner also scans system memory on start. If you launch a program or file which creates destructive anomalies, then the scanner blocks it and alerts you immediately. Should you wish, 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 when a threat is detected** - Allows you to configure how CCAV should react when malware is detected by the real-time protection engine (***Default = Alert***). The available options are:
  - **Alert** - An alert will be displayed whenever a malware is identified. An example of Antivirus Alert is shown below:



COMODO Antivirus Alert

ApplicUnwnt.Win32.Leaktest.Ghost

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

Clean (Recommended)
Quarantines the file

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

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

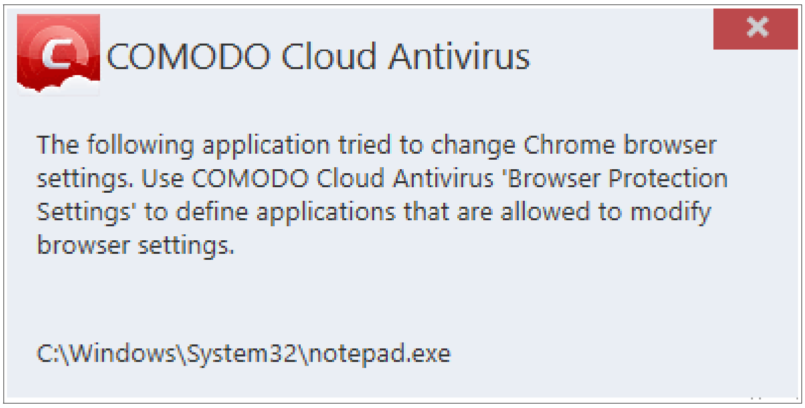
You can choose to clean, ignore or add the file to trusted files list. If you need more details about this options, refer to Antivirus Alerts in Understanding CCAV Alerts. Choosing not show antivirus alerts in favor of automatically quarantining or blocking will minimize disturbances but at some loss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

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

- **Max file size limit** - Allows you to set the maximum size of a file that CCAV should scan. Files larger than the size specified here will not be not scanned. (***Default = 100 MB***)
- **Cloud file checking timeout** - Allows you to 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***)
- **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 derails on on-demand/manual scans, refer to the section Scan and Clean your Computer. (***Default = Enabled***)
- **Enable Browser Settings Protection-** If enabled, CCAV blocks all attempts made by any software that tries to change your browser settings (e.g. default search engine, home page, privacy setting etc) and shows an alert message for the first time for every software. Such applications that are blocked are added to the 'Browser Protection Settings' area automatically. Users can change(add, edit or remove the application) the

rule later.(*Default = Enabled*).

An example is shown below:

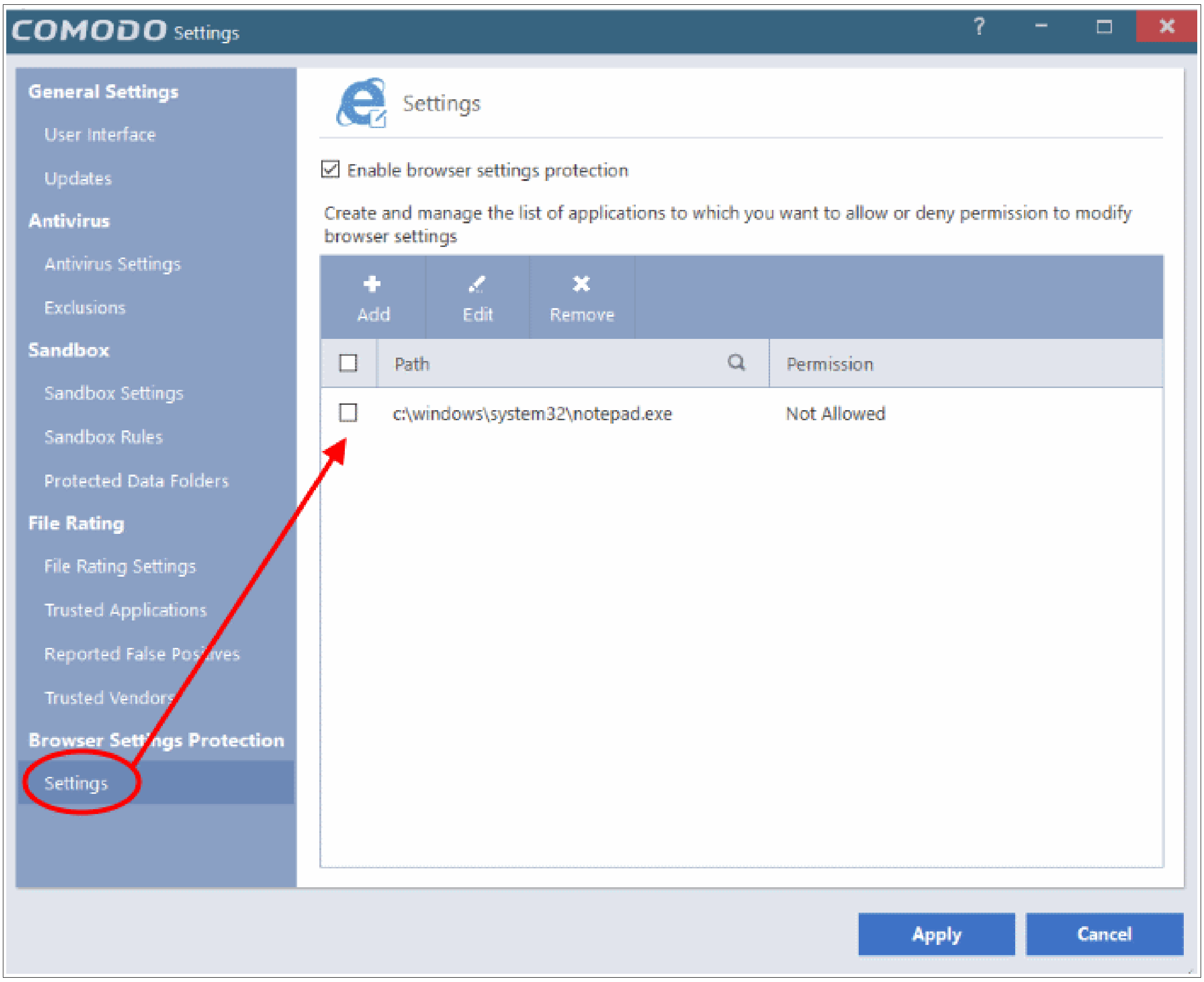


COMODO Cloud Antivirus

The following application tried to change Chrome browser settings. Use COMODO Cloud Antivirus 'Browser Protection Settings' to define applications that are allowed to modify browser settings.

C:\Windows\System32\notepad.exe

- CCAV shows an alert specifying the name of the application that modified the browser setting. Once the alert is displayed, the application information will be added to the Broser protection setting.



Settings

☑ Enable browser settings protection

Create and manage the list of applications to which you want to allow or deny permission to modify browser settings

□	Path	Permission
□	c:\windows\system32\notepad.exe	Not Allowed

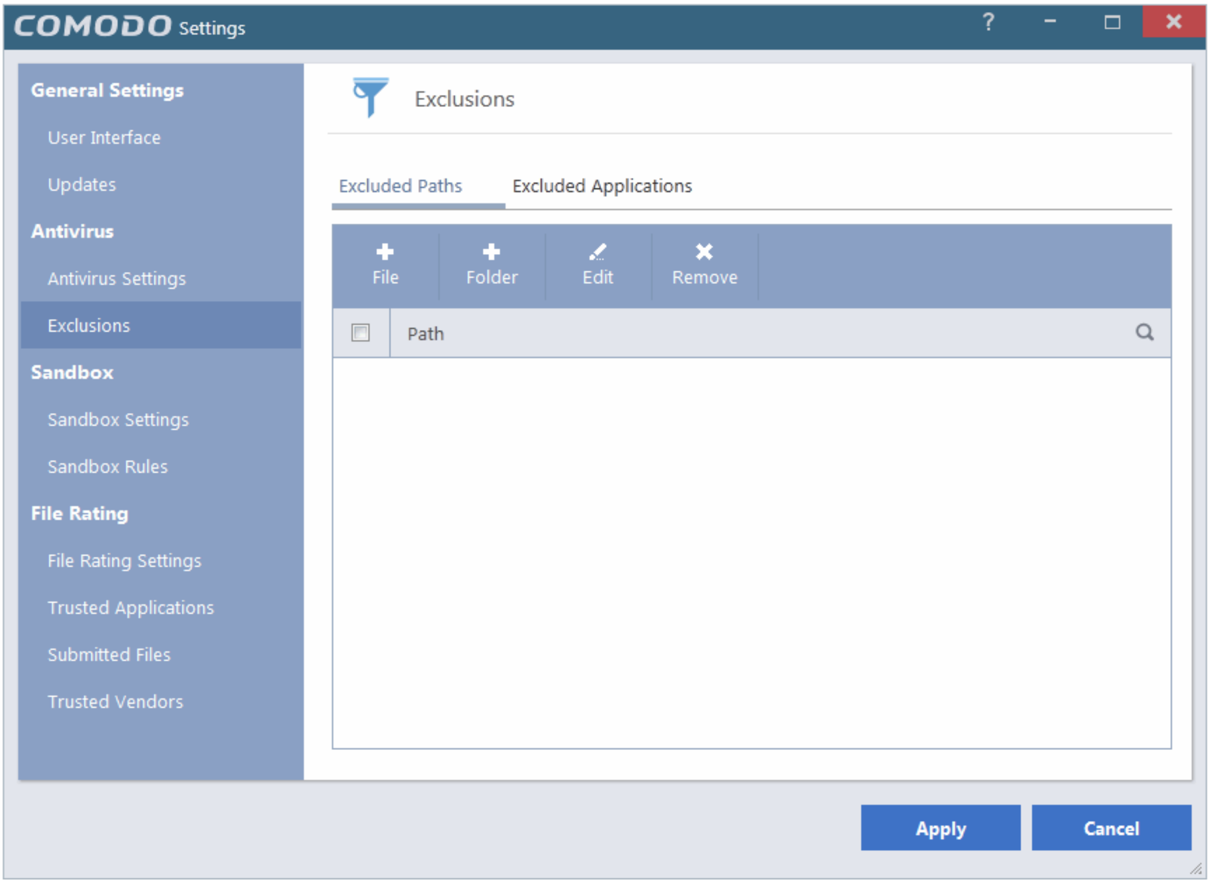
6.2.2. Exclusions

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

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

To open the Exclusions panel

- Open the 'Settings' interface by clicking 'Settings' from the top left of the CCAV interface
- Select 'Exclusions' under 'Antivirus' on the left hand menu



The 'Exclusions' panel has two tabs:

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

Excluding Drives/Folders/Files from all types of scans

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

To add file to excluded paths

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

You can choose to add a:

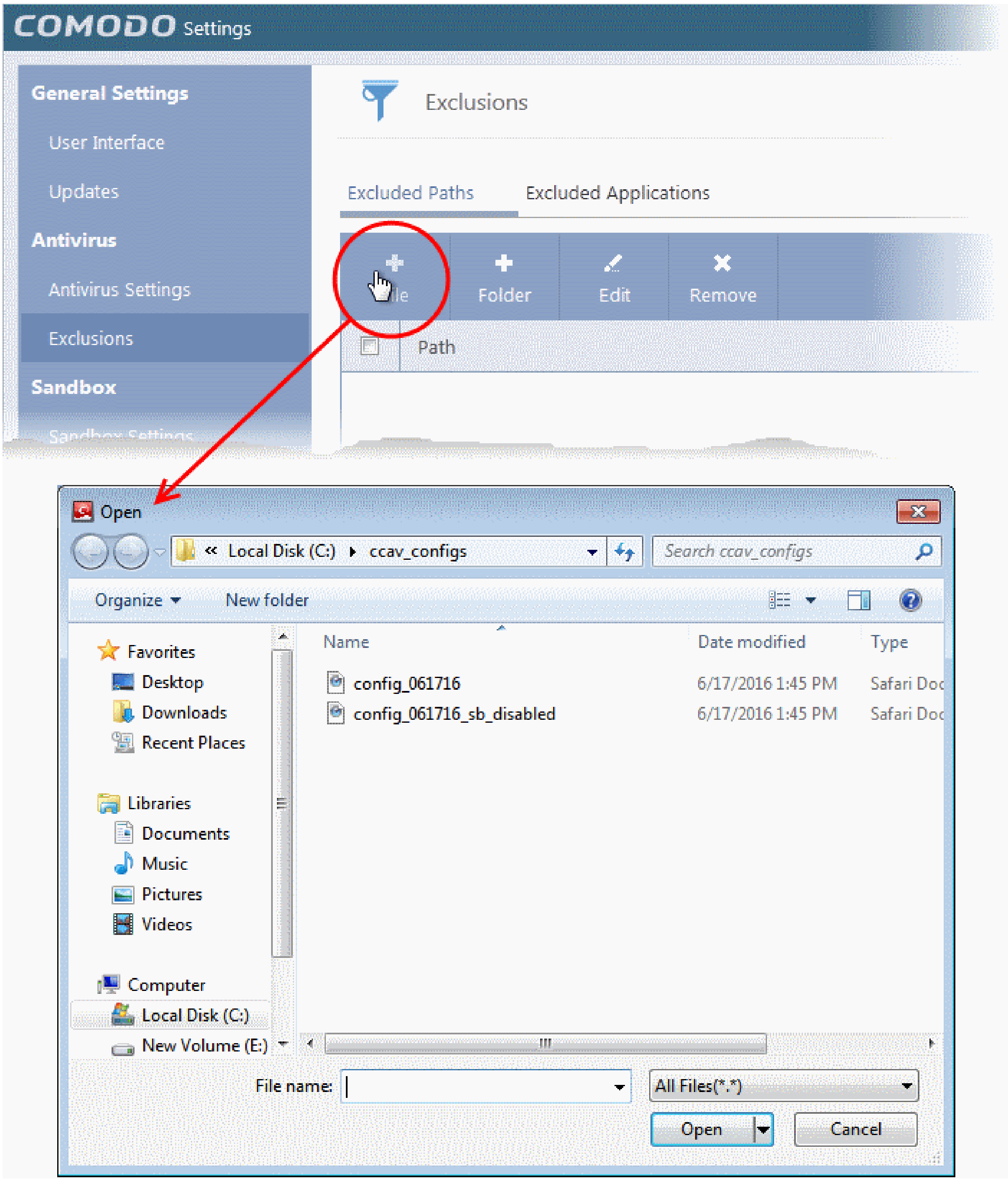
- An individual File

  OR
- Drive partition/Folder

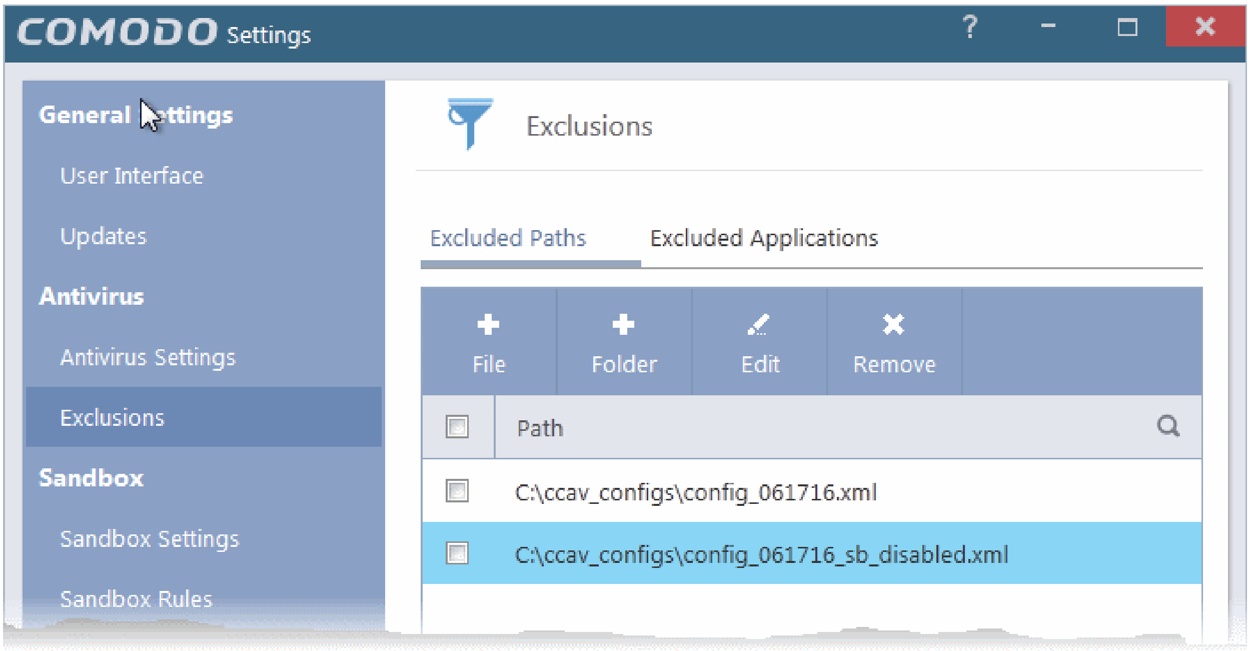
Adding an individual File

You can specify individual files as excluded path.

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



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



□	Path
□	C:\ccav_configs\config_061716.xml
□	C:\ccav_configs\config_061716_sb_disabled.xml

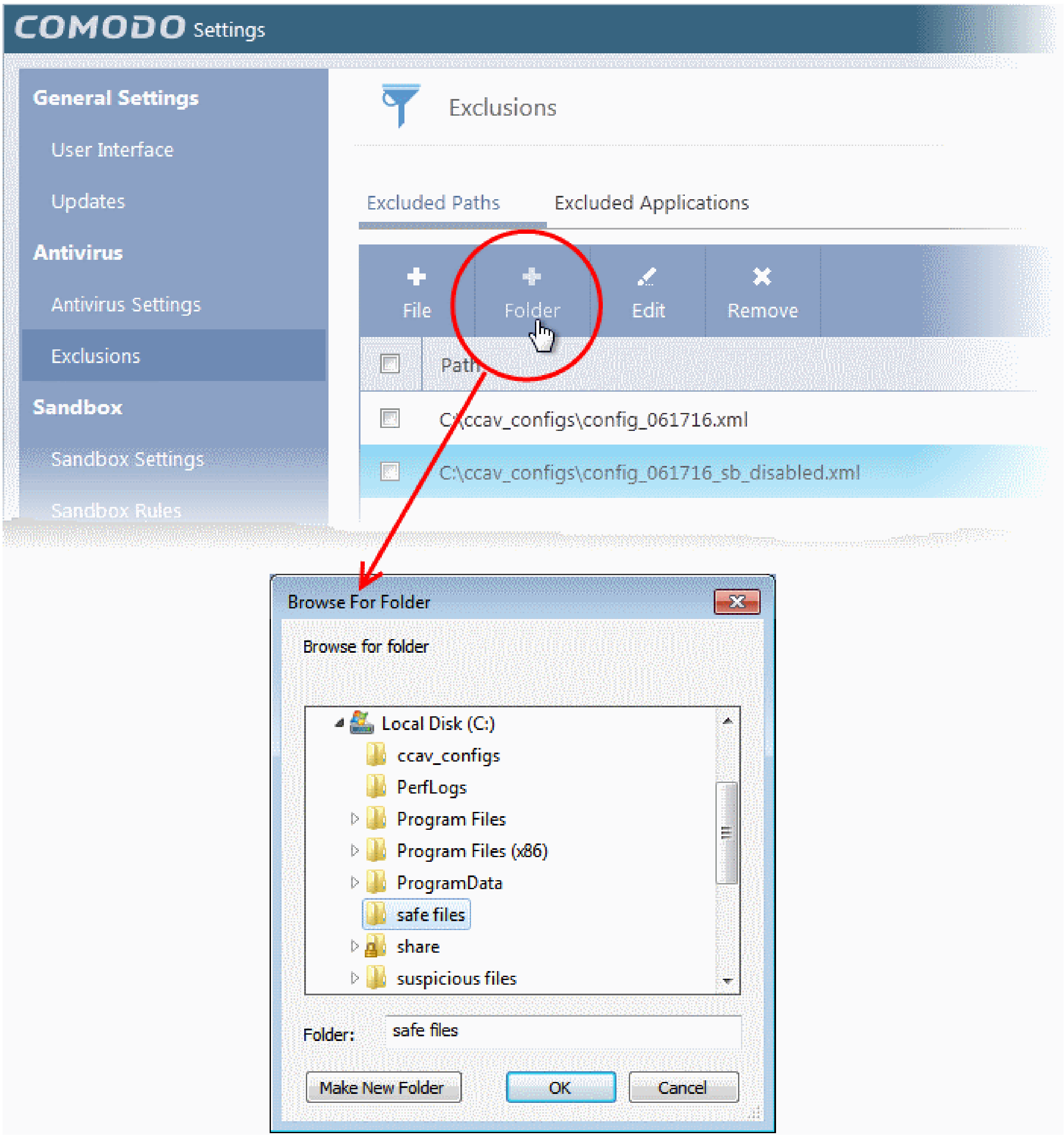
The file will be added to Excluded Paths.

- 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 future antivirus scans.

Adding a Drive Partition/Folder

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

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



□ C:\ccav_configs\config_061716.xml

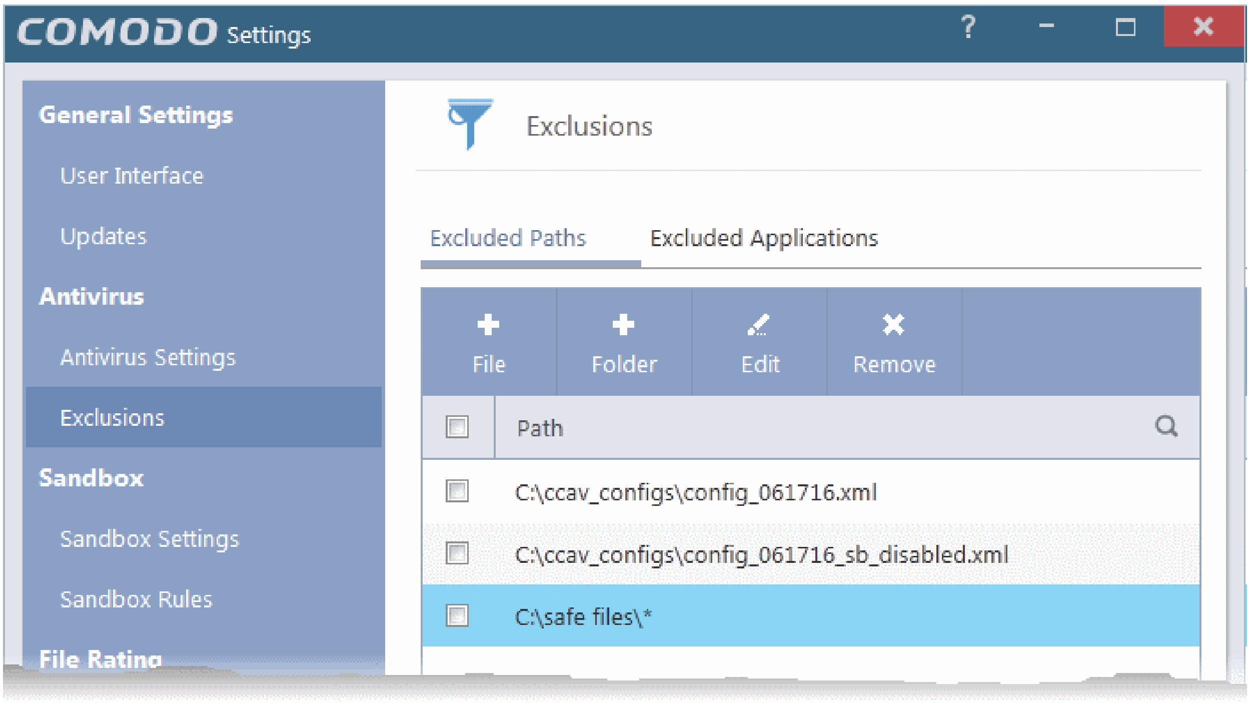
□ C:\ccav_configs\config_061716_sb_disabled.xml

Folder: safe files

The 'Browse for folder' dialog will appear.

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

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

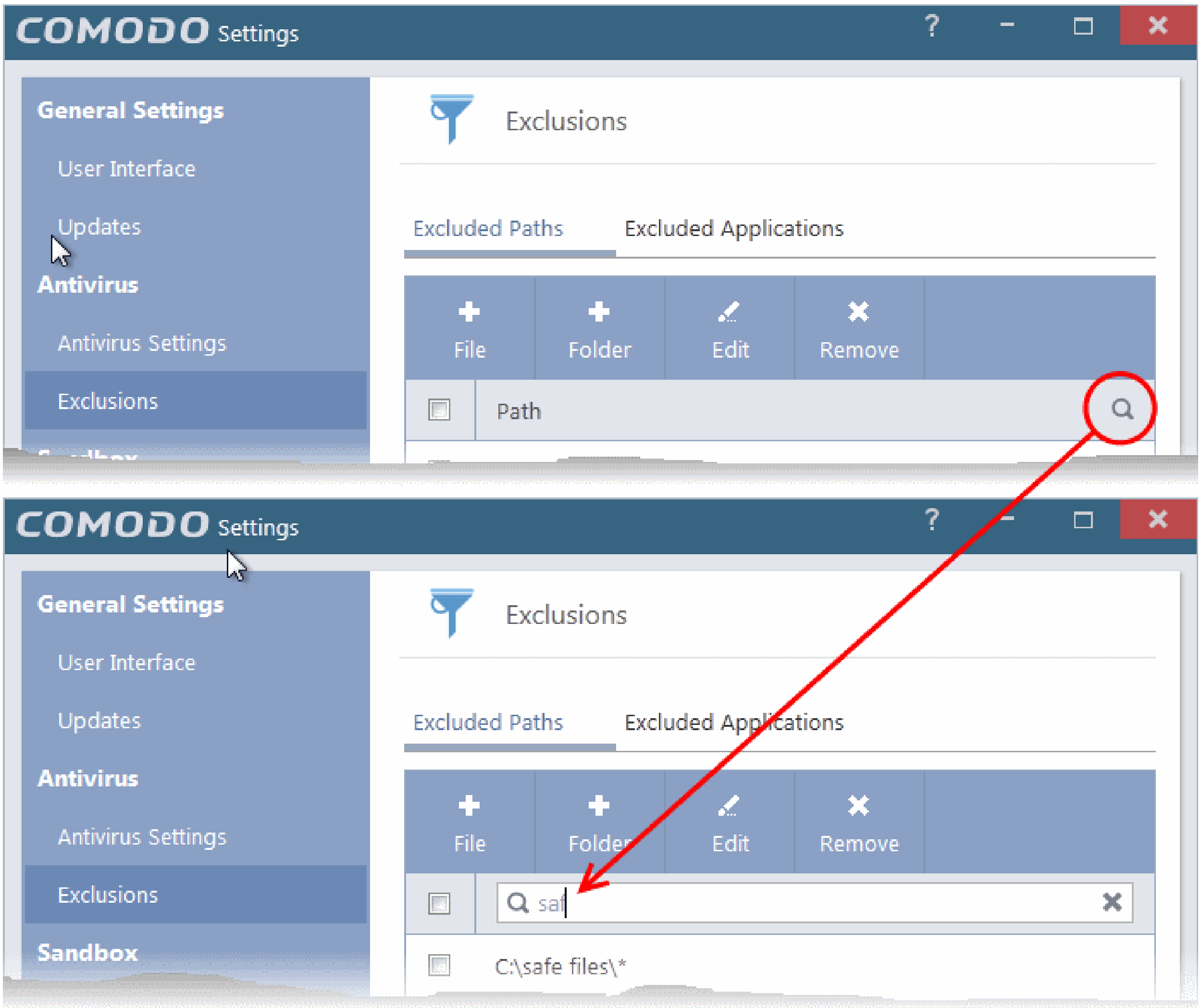


□	Path
□	C:\ccav_configs\config_061716.xml
□	C:\ccav_configs\config_061716_sb_disabled.xml
□	C:\safe files*

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

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.

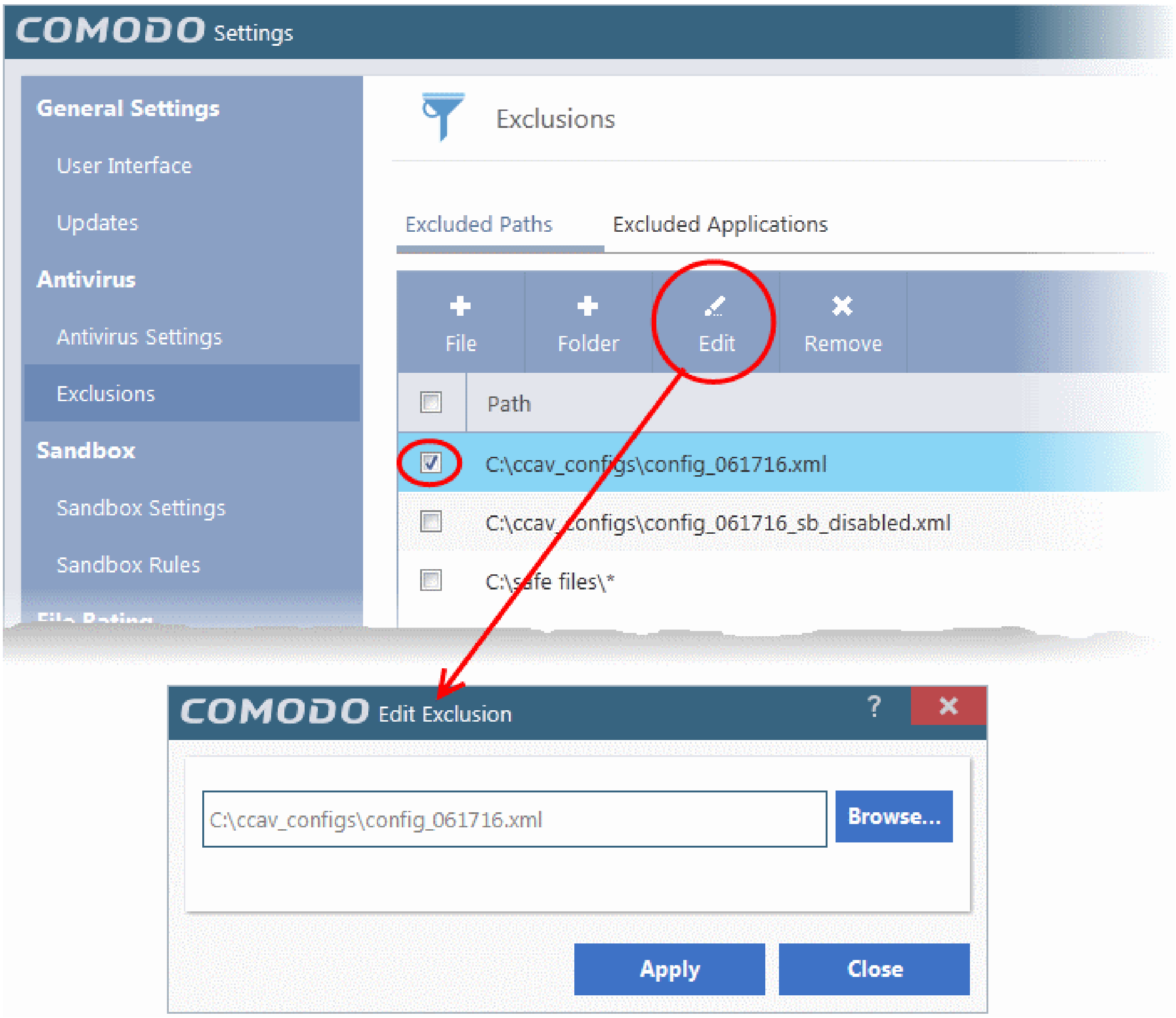


- Enter the path, folder name or file name to be searched in full or part in the search field.
- The search results will be displayed.
- Click the icon 'X' in the search field to close the search option.

To edit the path of an added item

- Double click on the item

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



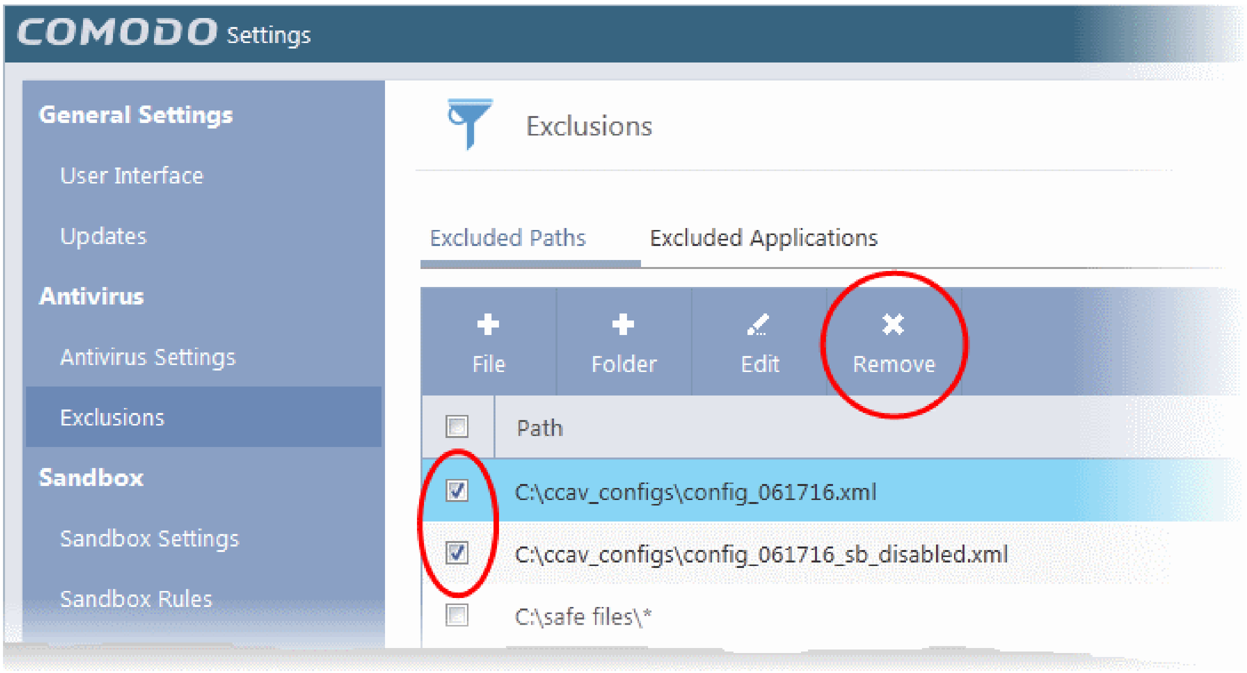
☐	Path
☑	C:\ccav_configs\config_061716.xml
☐	C:\ccav_configs\config_061716_sb_disabled.xml
☐	C:\safe files*

C:\ccav_configs\config_061716.xml

- Next, click the 'Browse...' button and navigate to the file to which you want to modify.
- Make the required changes for the file path in the 'Modify' dialog and click 'Apply'.

To remove item(s) from Excluded Paths

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

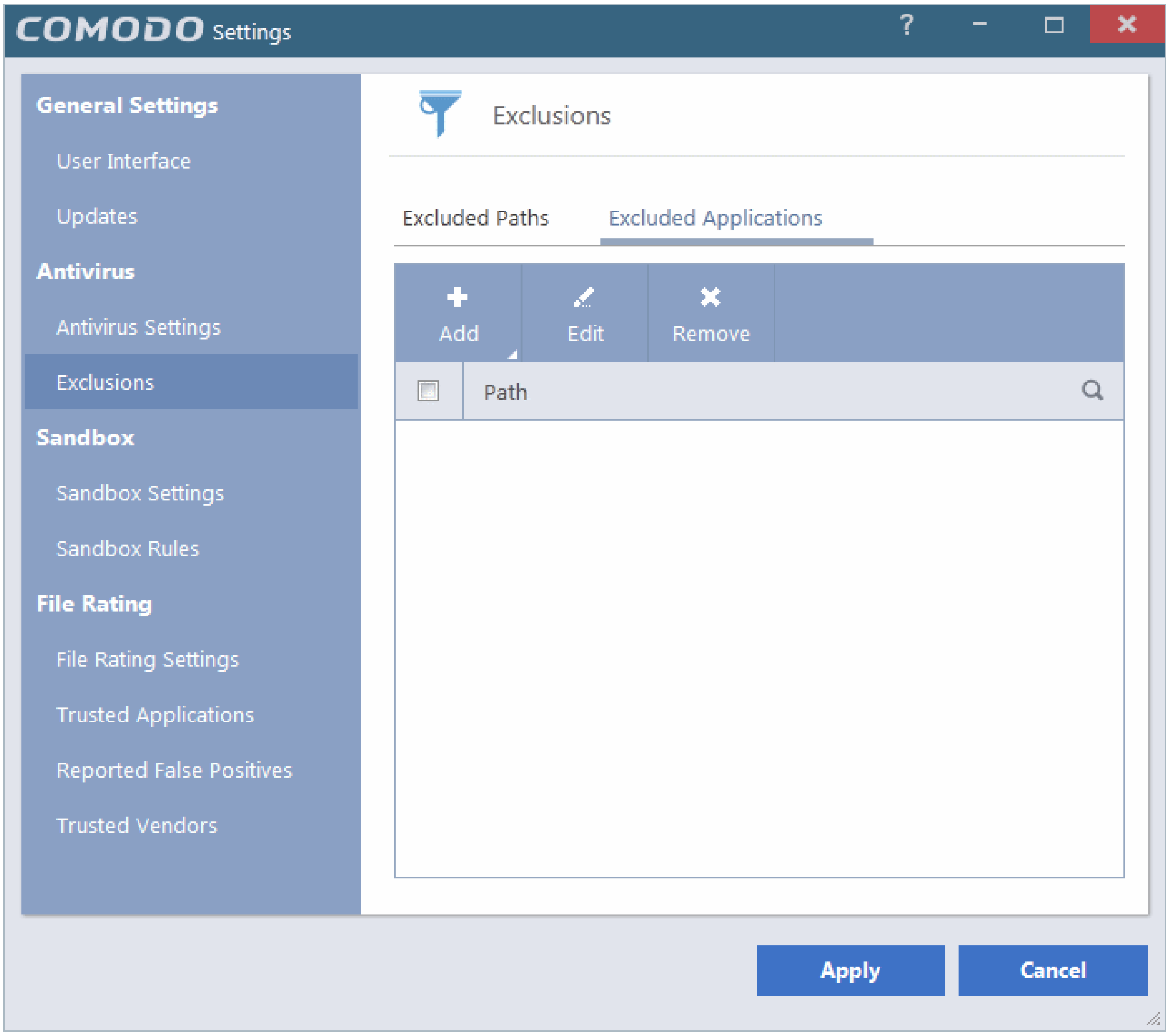


	Path
☑	C:\ccav_configs\config_061716.xml
☑	C:\ccav_configs\config_061716_sb_disabled.xml
□	C:\safe files*

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

Excluding Programs/Applications from Real-time Scans

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

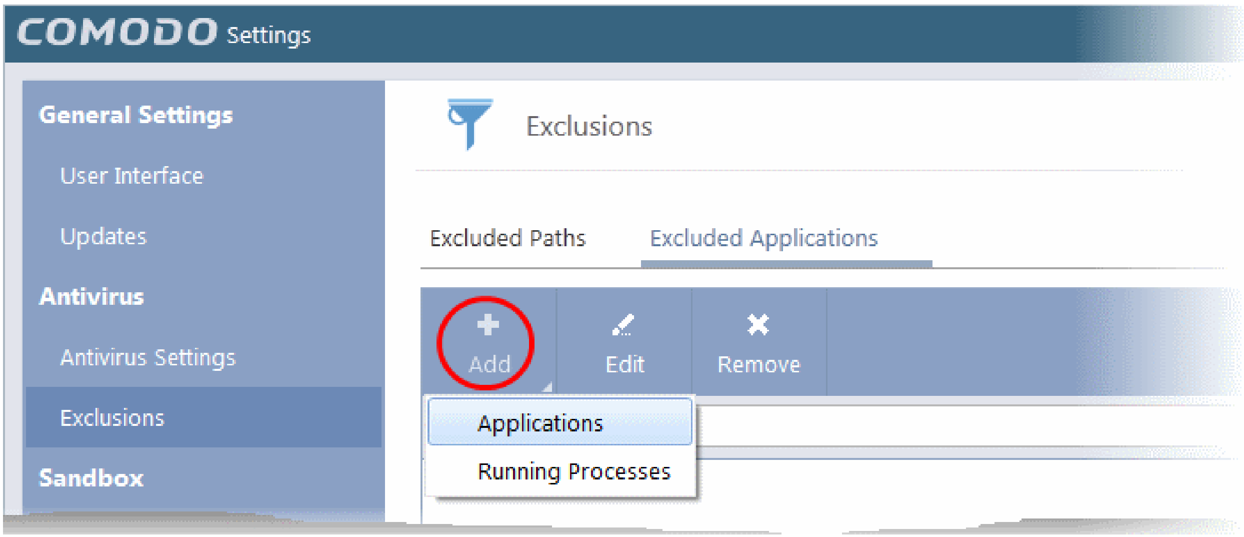


Manually adding applications to the 'Exclusions' list

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.

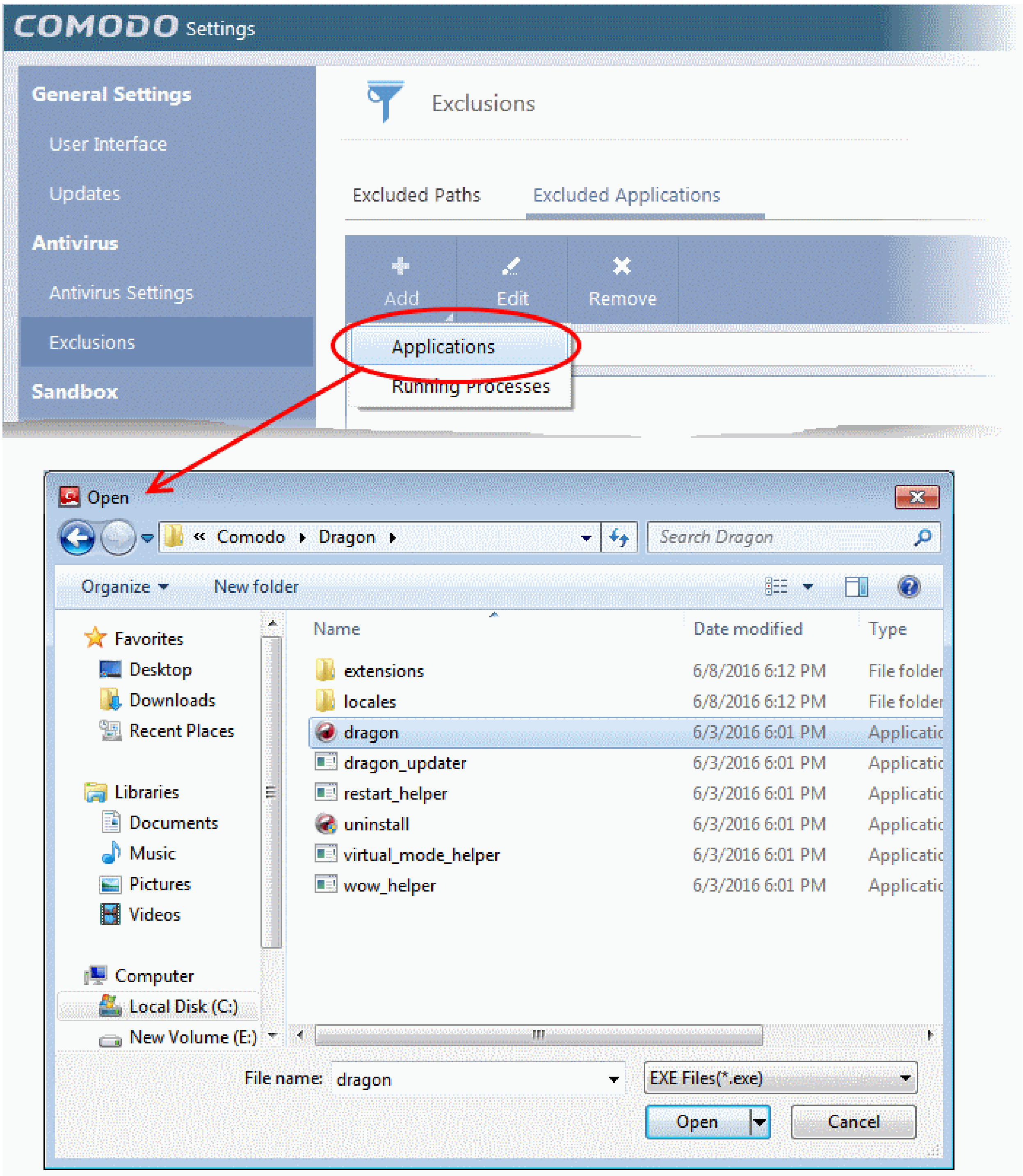


You can choose to add an application by:

- **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 choose the target application from the list of processes that are currently running on your PC.

Browsing to the Application

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

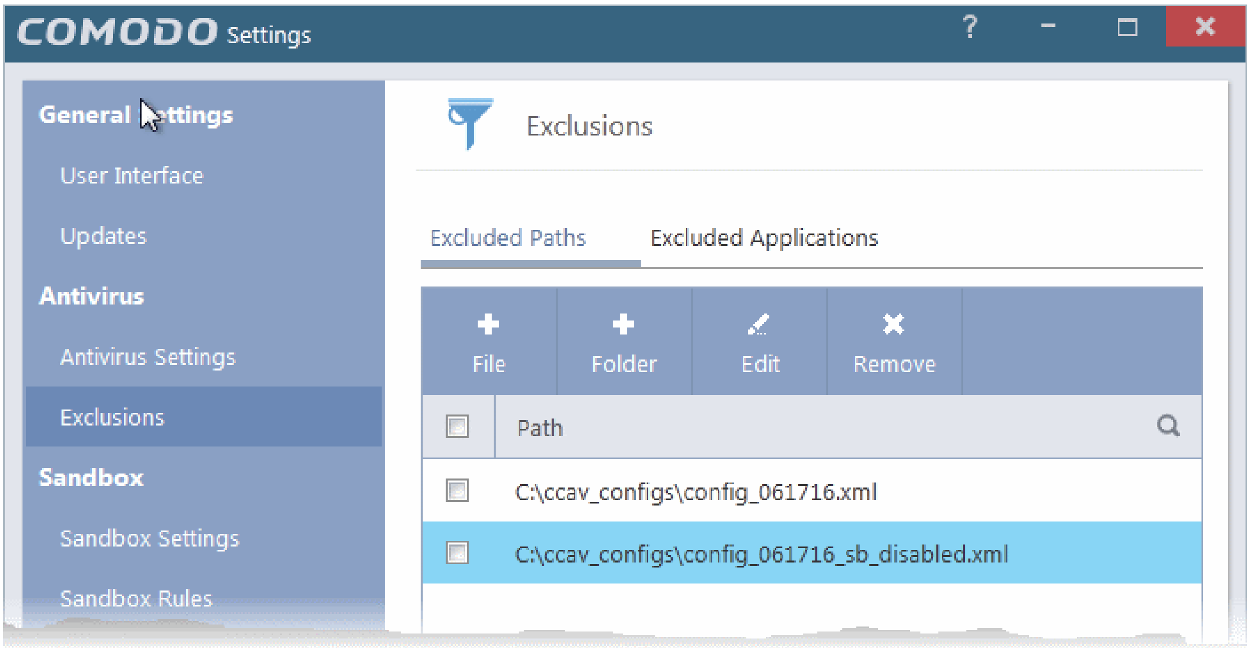


Name	Date modified	Type
extensions	6/8/2016 6:12 PM	File folder
locales	6/8/2016 6:12 PM	File folder
dragon	6/3/2016 6:01 PM	Applicatic
dragon_updater	6/3/2016 6:01 PM	Applicatic
restart_helper	6/3/2016 6:01 PM	Applicatic
uninstall	6/3/2016 6:01 PM	Applicatic
virtual_mode_helper	6/3/2016 6:01 PM	Applicatic
wow_helper	6/3/2016 6:01 PM	Applicatic

File name: dragon

EXE Files(*.exe)

The file will be added to 'Excluded Applications'.

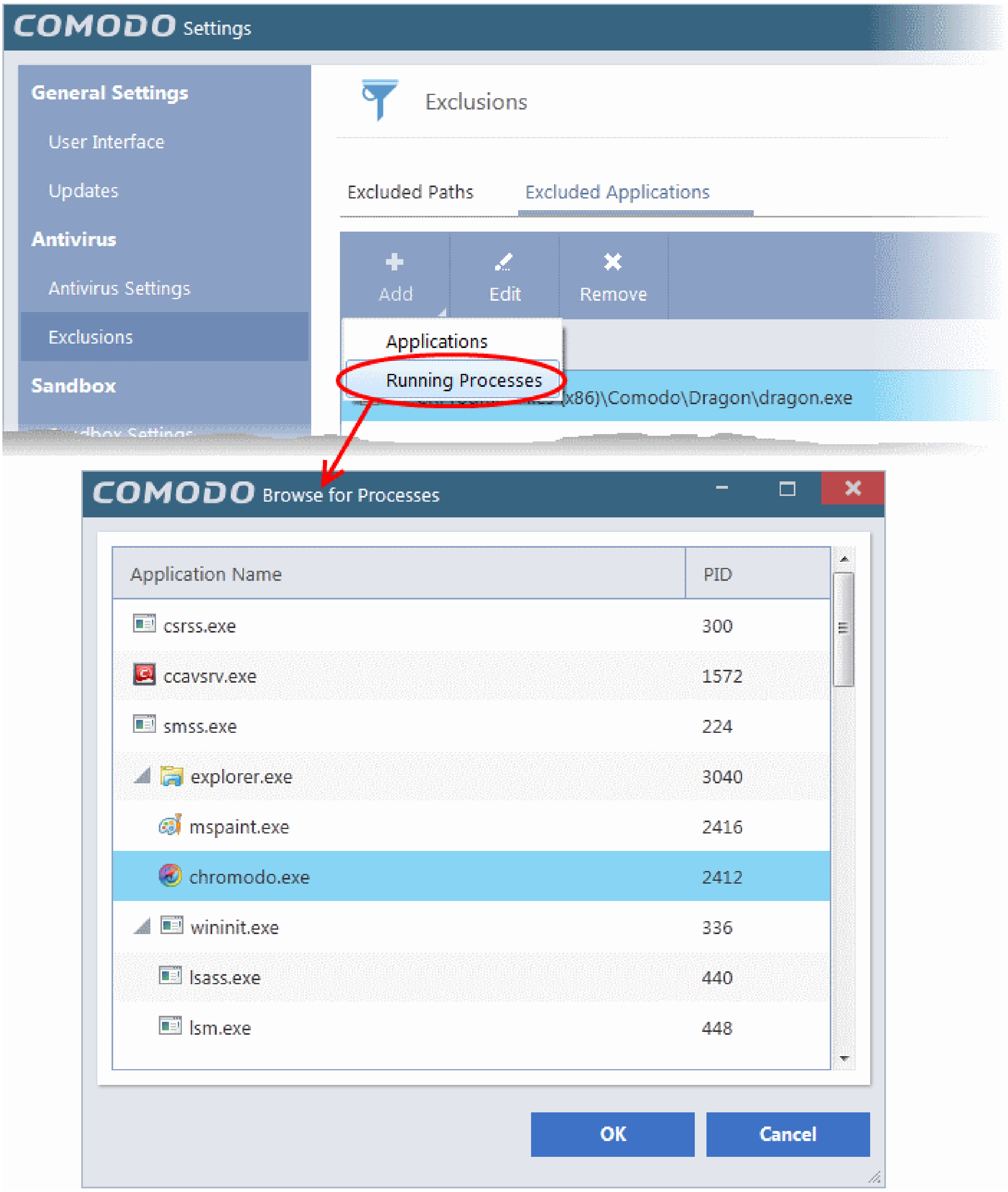


□	Path
□	C:\ccav_configs\config_061716.xml
□	C:\ccav_configs\config_061716_sb_disabled.xml

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

Adding application from running processes

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

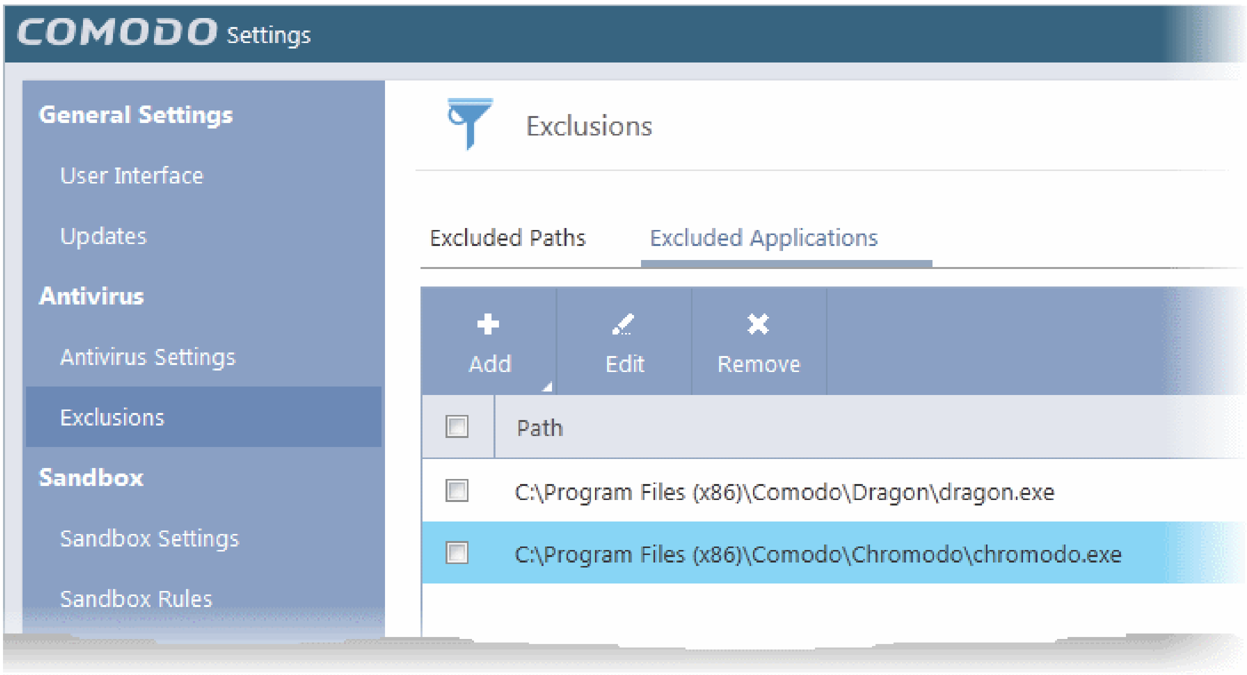


Application Name	PID
csrss.exe	300
ccavsrv.exe	1572
smss.exe	224
explorer.exe	3040
mspaint.exe	2416
chromodo.exe	2412
wininit.exe	336
lsass.exe	440
lsm.exe	448

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

- Select the process you wish to add to excluded applications and click 'OK'.

The application will be added to Excluded Applications.

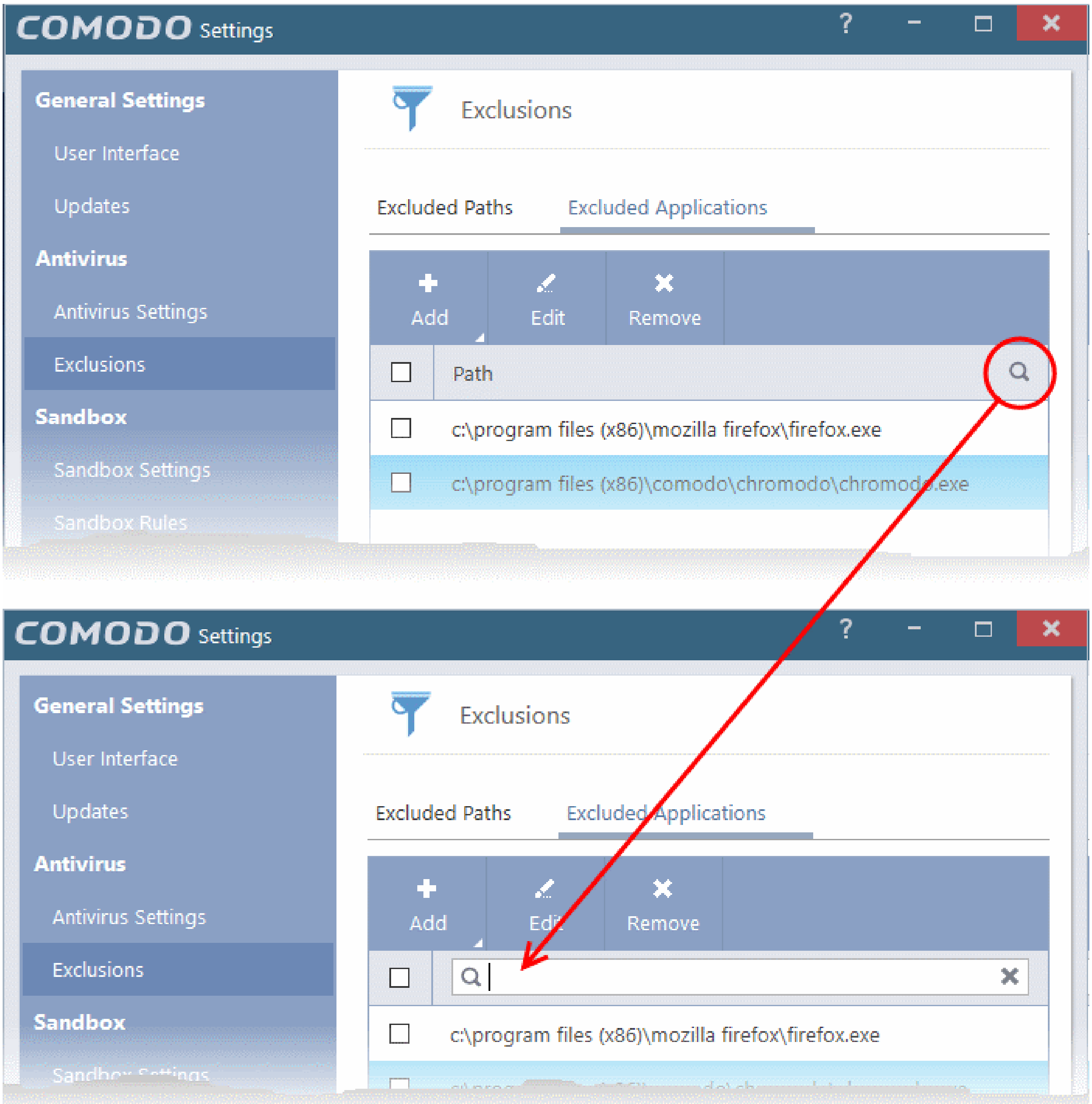


□	Path
□	C:\Program Files (x86)\Comodo\Dragon\dragon.exe
□	C:\Program Files (x86)\Comodo\Chromodo\chromodo.exe

- Repeat the process to add more items.
- Click 'Apply' for saving your settings. The items 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 the top right.



c:\program files (x86)\mozilla firefox\firefox.exe

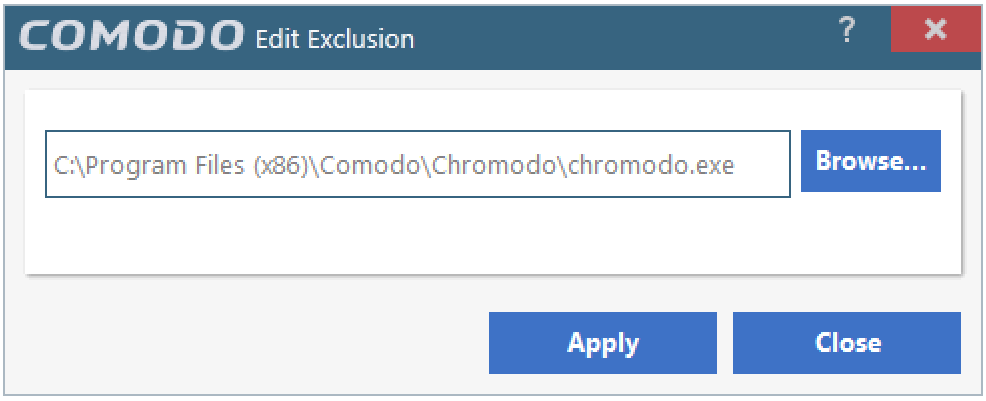
c:\program files (x86)\comodo\chromodo\chromodo.exe

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

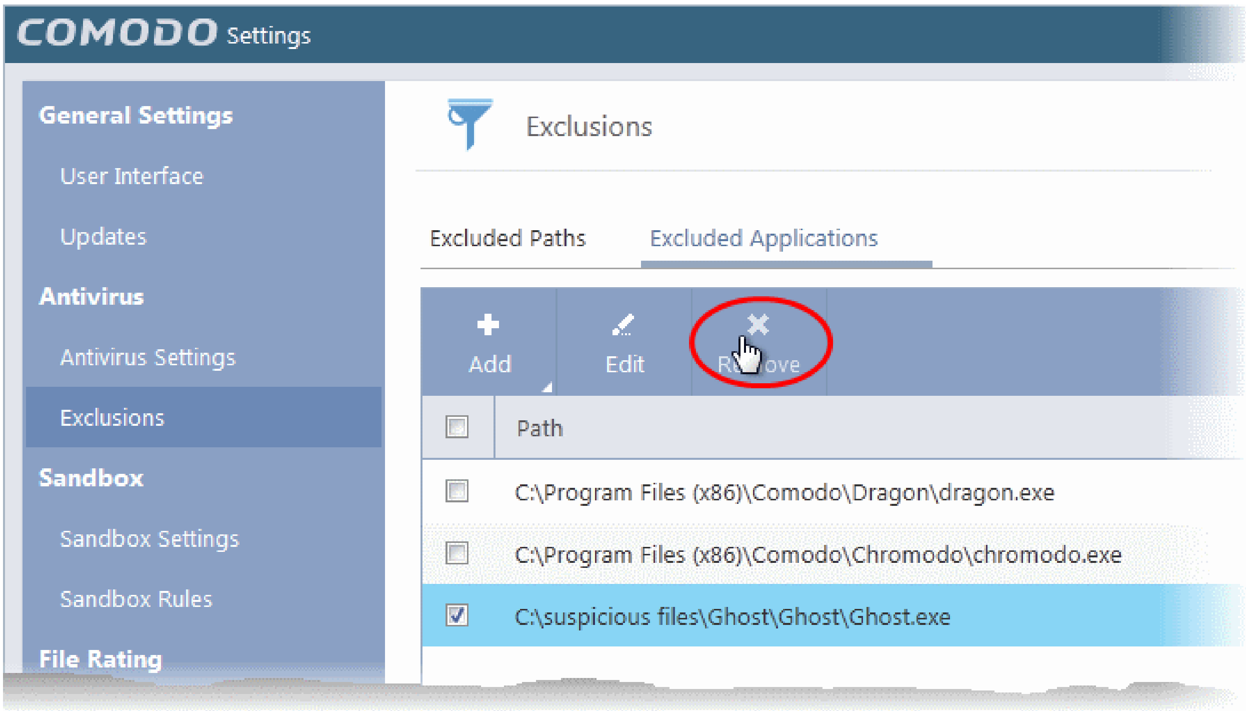


C:\Program Files (x86)\Comodo\Chromodo\chromodo.exe

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

To remove item(s) from the Excluded Applications

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

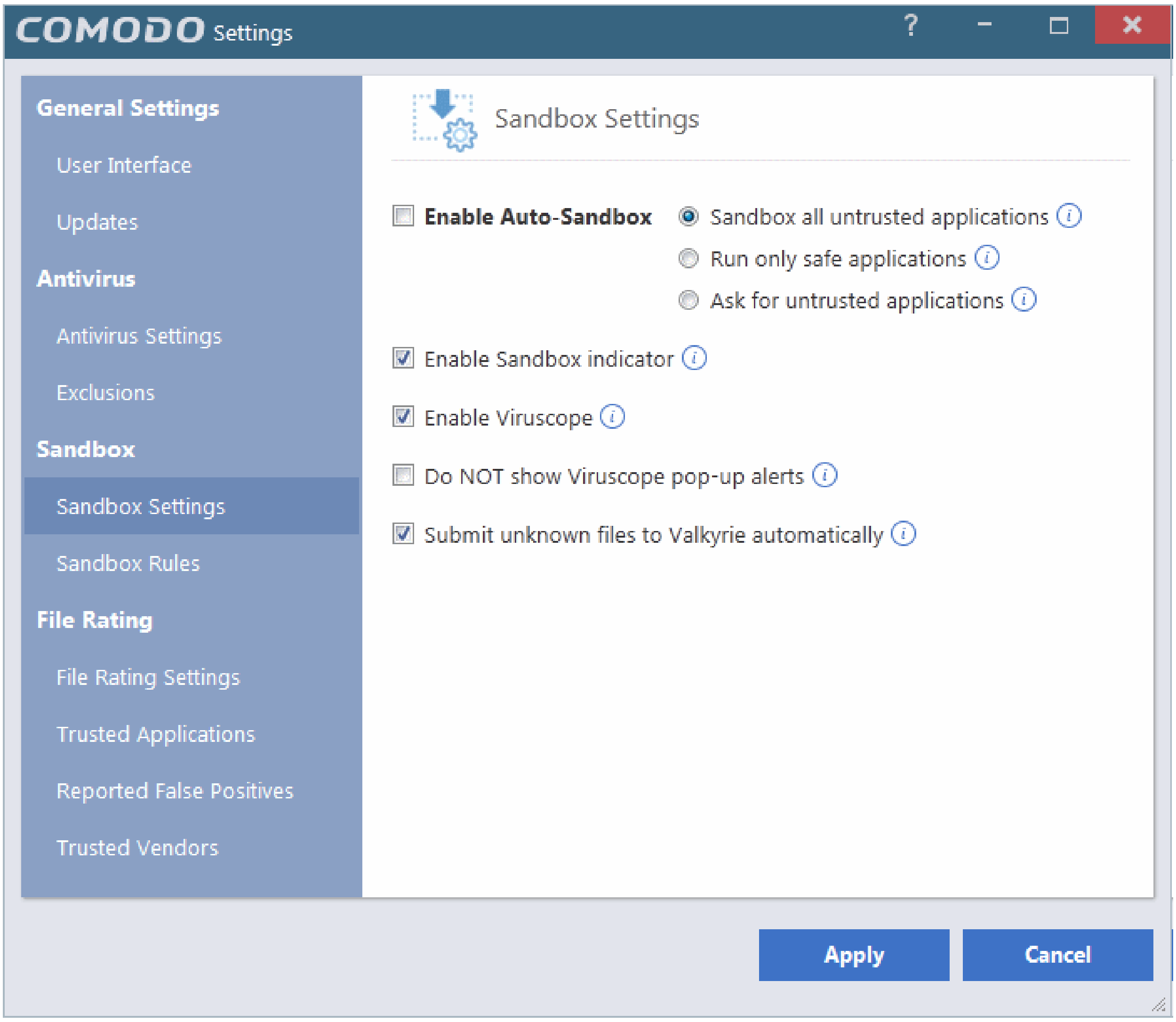


☐	Path
☐	C:\Program Files (x86)\Comodo\Dragon\dragon.exe
☐	C:\Program Files (x86)\Comodo\Chromodo\chromodo.exe
☑	C:\suspicious files\Ghost\Ghost\Ghost.exe

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

6.3. Sandbox Settings

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



Sandbox Settings

□ **Enable Auto-Sandbox** ● Sandbox all untrusted applications ○ Run only safe applications ○ Ask for untrusted applications

☑ Enable Sandbox indicator

☑ Enable Viruscope

□ Do NOT show Viruscope pop-up alerts

☑ Submit unknown files to Valkyrie automatically

Refer to the following sections for more details:

- Sandbox Settings
- Sandbox Rules

6.3.1. Sandbox Settings

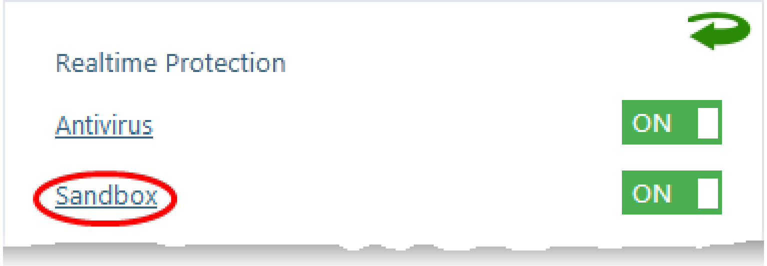
The sandbox settings area allows you to configure your overall sandbox policy.

To open sandbox settings

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

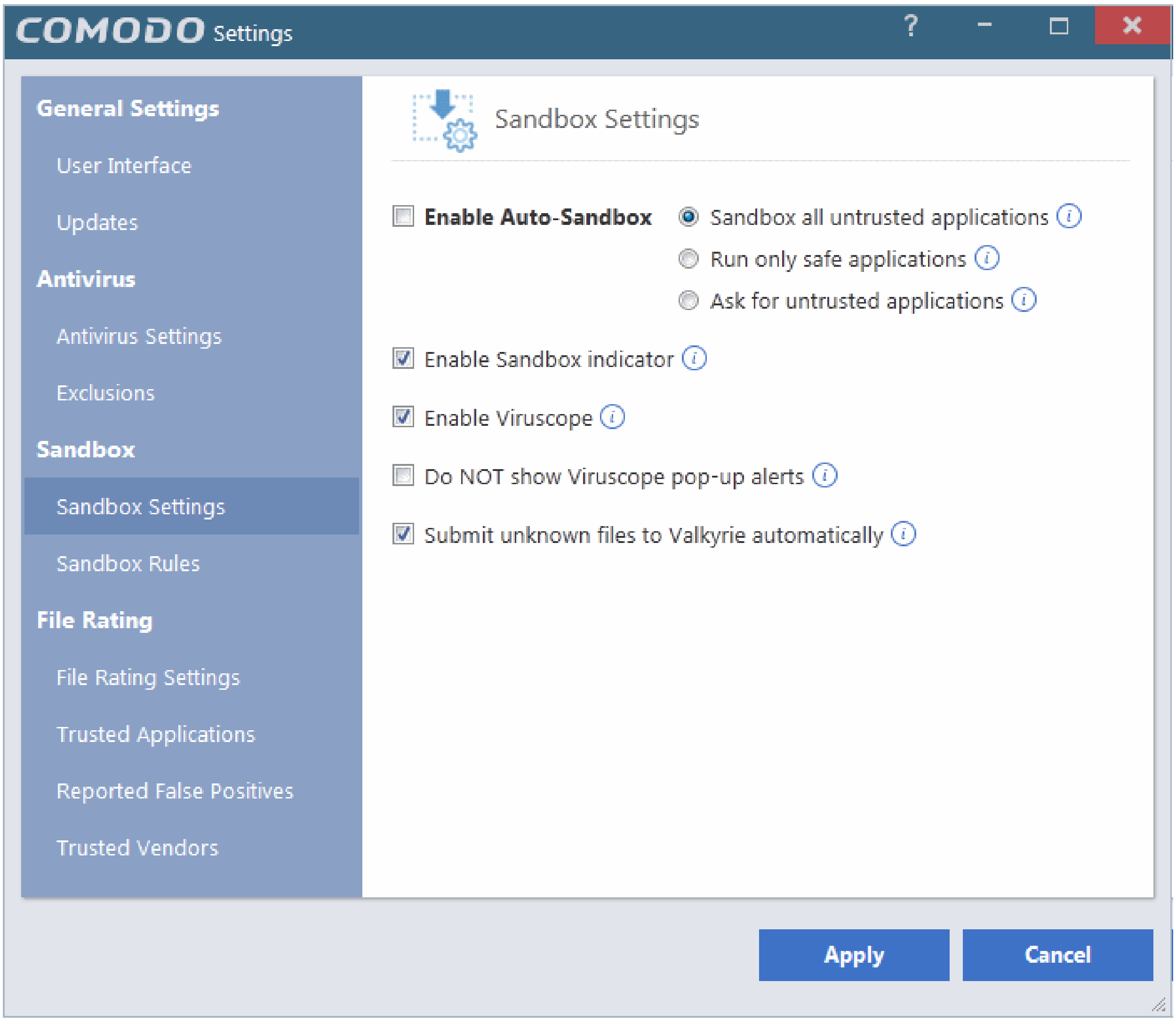
OR

- Flip the security status pane in the home screen by clicking the curved arrow and click the 'Sandbox' link under 'Realtime Protection'



OR

- Right-click on the CCAV system tray icon or the widget and choose 'Sandbox Settings' from the options.



Sandbox Settings

□ **Enable Auto-Sandbox** ● Sandbox all untrusted applications ○ Run only safe applications ○ Ask for untrusted applications

☑ Enable Sandbox indicator

☑ Enable Viruscope

□ Do NOT show Viruscope pop-up alerts

☑ Submit unknown files to Valkyrie automatically

- **Enable Auto-Sandbox -** Switch automatic sandboxing on or off. If you disable the sandbox, then any sandbox rules that you have created will be disregarded. If you enable the sandbox, you have the following options:
  - Sandbox all untrusted files - CCAV will automatically run 'unknown' files and applications in the sandbox. A file can have one of three trust statuses - Trusted, Untrusted or Unknown. 'Trusted' files are those that are either on the Comodo white-list of known-good applications, or have been trusted by the user. Trusted files and are allowed to run outside the sandbox. 'Untrusted' files are usually viruses and other forms of malware and will be quarantined by the antivirus scanner. 'Unknown' files are those which are neither 'Trusted' nor 'Untrusted'. As their precise intentions are not yet known, we run these applications in the sandbox. If they later transpire to be malicious, they will not have been able to cause damage to your computer or data because they were sandboxed.
  - Run only safe applications - Only applications from Trusted Vendors or those in your list of Trusted Applications will be allowed to run on your computer. All other applications will be blocked.
  - 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. (***Default = Disabled***)
- **Submit unknown files to Valkyrie automatically -** By default, files identified as 'Unknown' by a File Rating scan are automatically uploaded to Valkyrie for further 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 also be added to the global whitelist and blacklist to help fellow CCAV users who encounter the same file. Refer to the section **Viewing Valkyrie Analysis Results** for more details.

  If you do not want CCAV to automatically upload Unknown files, disable this option (***Default = Enabled***)

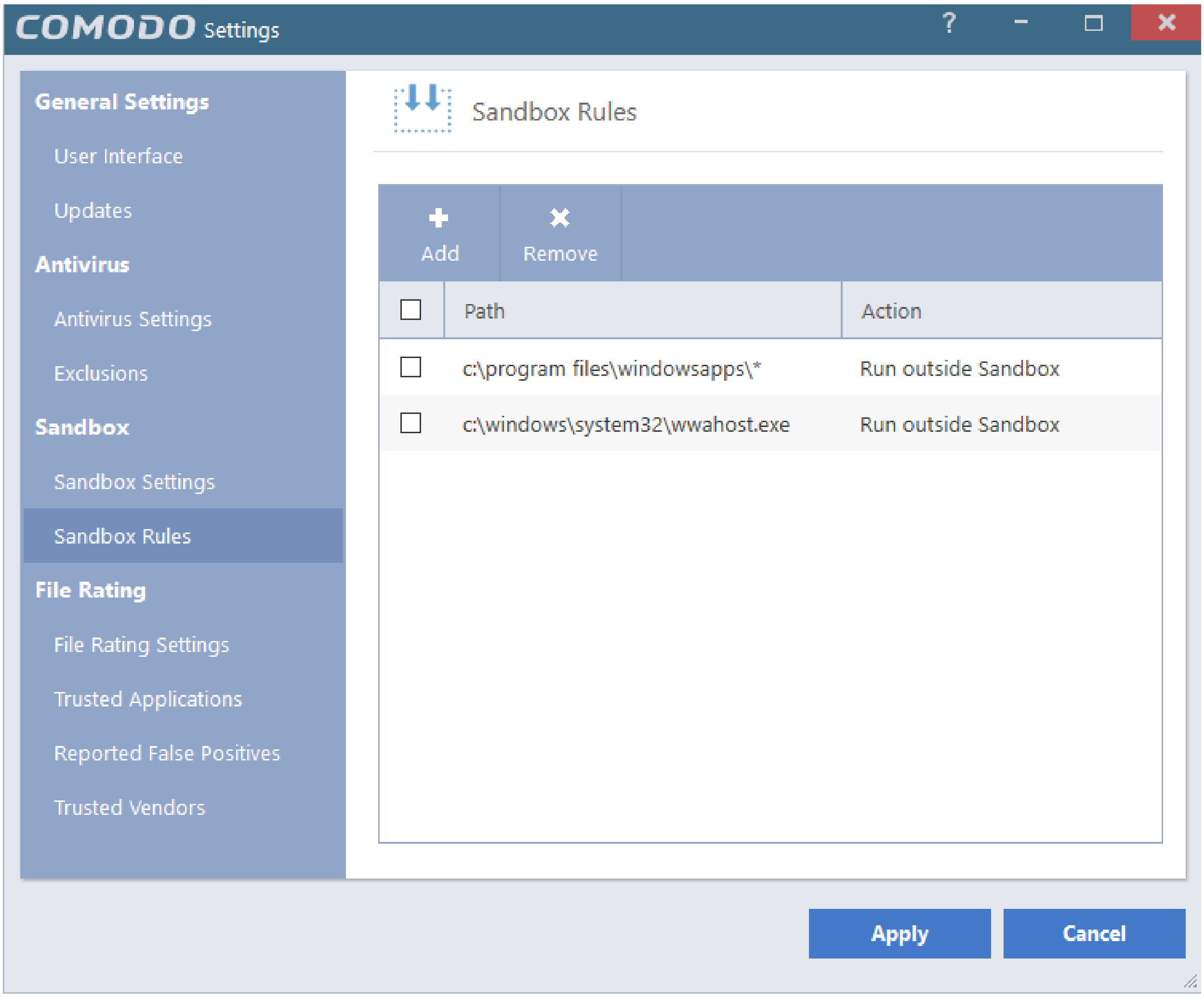
- Click 'Apply' for your settings to take effect.

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

- Open the 'Settings' interface by clicking 'Settings' at the top left of the home screen then select 'Sandbox Rules' under 'Sandbox'



□	Path	Action
□	c:\program files\windowsapps\*	Run outside Sandbox
□	c:\windows\system32\wwahost.exe	Run outside Sandbox

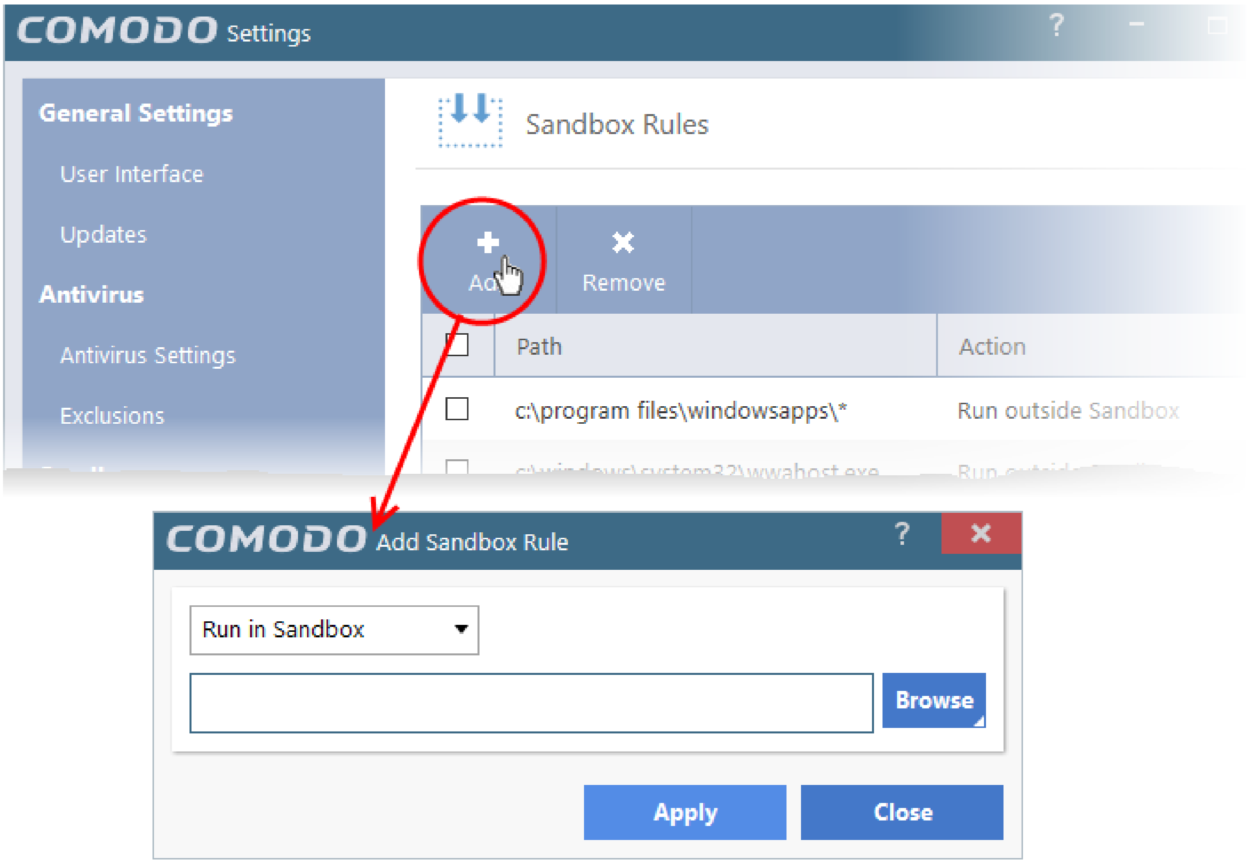
The interface displays a list of existing rules along with the application path and the sandbox action associated with it.

Adding a new rule

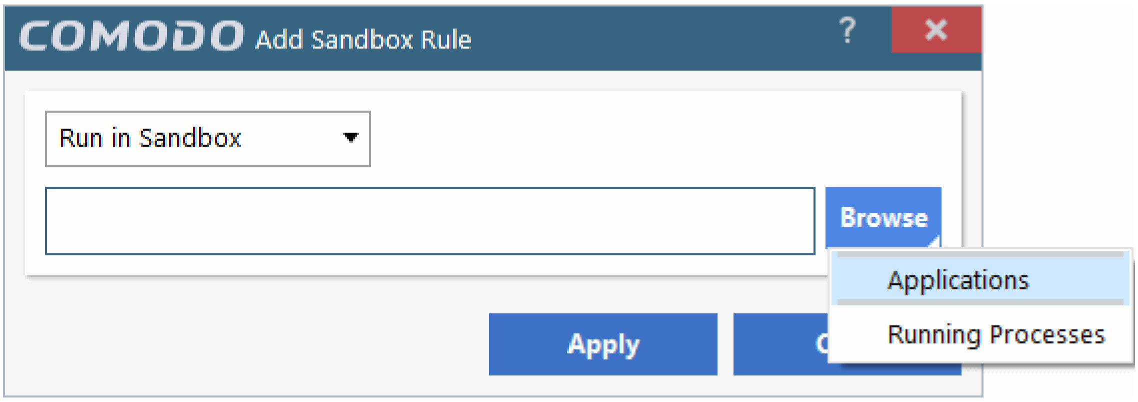
You can add new sandbox rules by specifying applications and sandbox actions to be respectively applied to them.

To add a sandbox rule

- Click 'Add' from 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, click the 'Browse...' button to specify the application to which the rule should be applied.



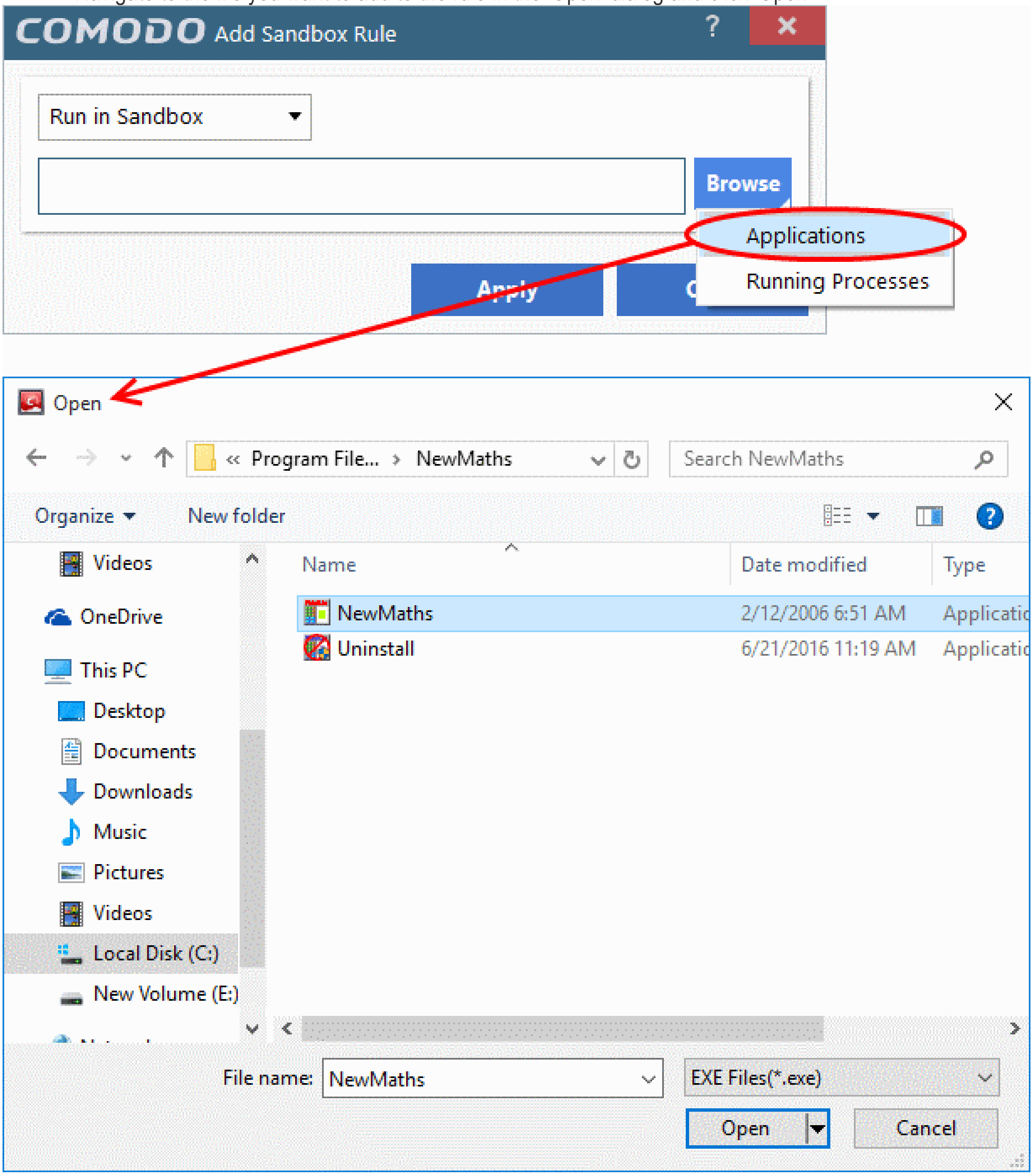
You can choose to add an application by:

- 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 choose the target application from the list

of processes that are currently running on your PC.

Browsing to the Application

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

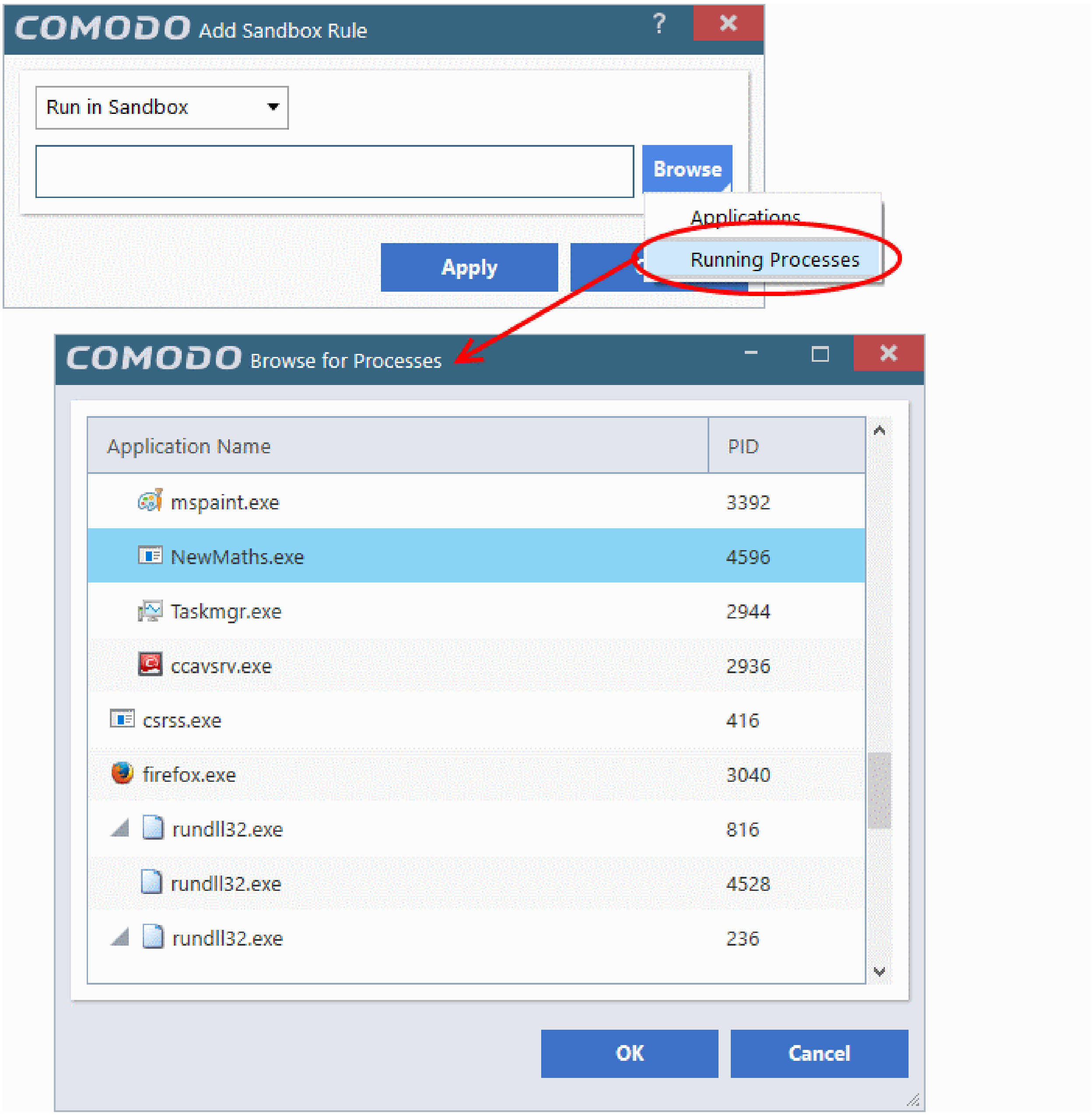


The file will be added to the rule.

- Click 'Apply' from the Add Sandbox Rule.
- Repeat the process to add more rules.
- Click 'Apply' from the 'Settings' dialog for your rules to take effect.

Adding Application from Running Processes

- Choose 'Running processes' from the 'Browse' drop-down



Application Name	PID
mspaint.exe	3392
NewMaths.exe	4596
Taskmgr.exe	2944
ccavsrv.exe	2936
csrss.exe	416
firefox.exe	3040
rundll32.exe	816
rundll32.exe	4528
rundll32.exe	236

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

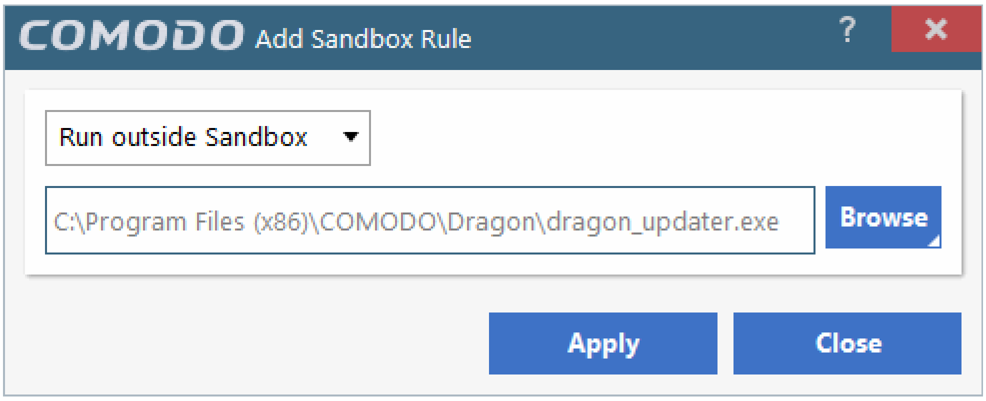
- Select the process you wish to add to the rule and click 'OK'.

The application will be added to rule.

- Click 'Apply' from the Add Sandbox Rule.
- 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.



C:\Program Files (x86)\COMODO\Dragon\dragon_updater.exe

The edit dialog is similar to 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 rules will be disregarded anyway.

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

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

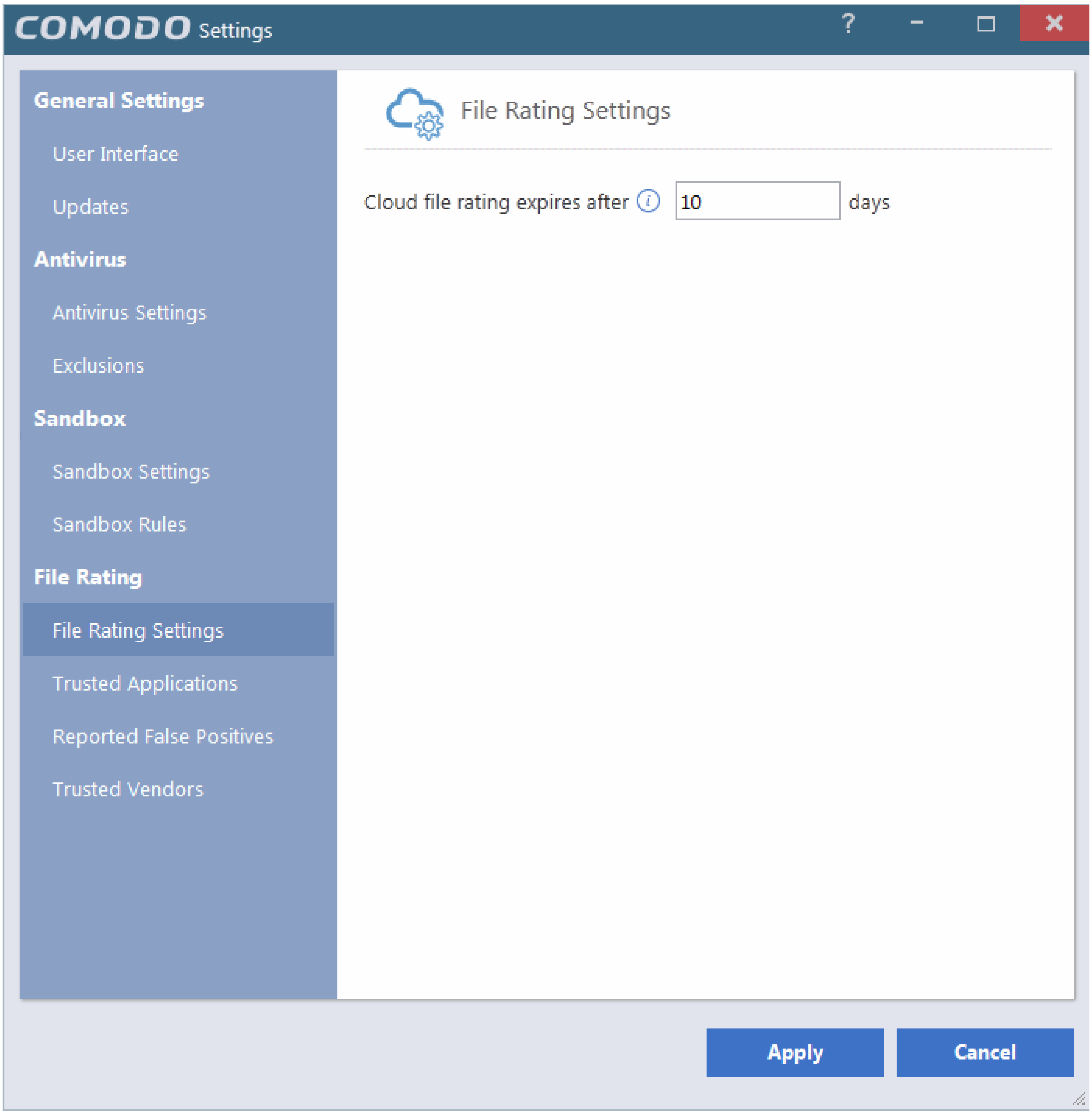
6.4. File Rating Settings

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

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

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

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



Cloud file rating expires after 10 days

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

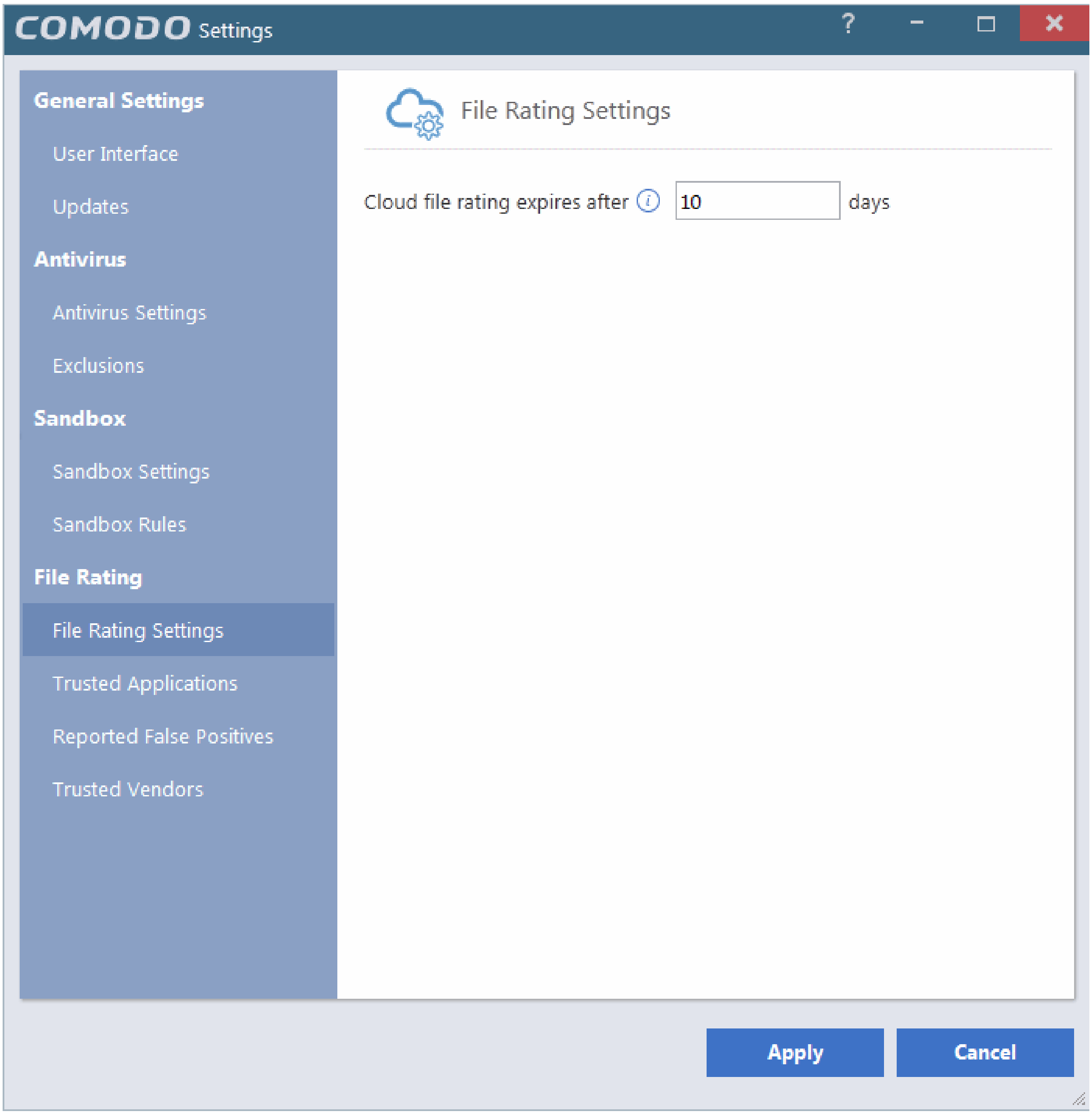
- File Rating Settings - Configure settings that govern the overall behavior of file rating.
- Trusted Applications - Add and manage applications to local Trusted Applications list.
- Submitted Files - View any files already submitted to Comodo for analysis.
- Trusted Vendors - View the list of trusted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

6.4.1. File Rating Settings

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

To open the 'File Rating Settings' interface

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



Cloud file rating expires after 10 days

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

6.4.2. Trusted Applications

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

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

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

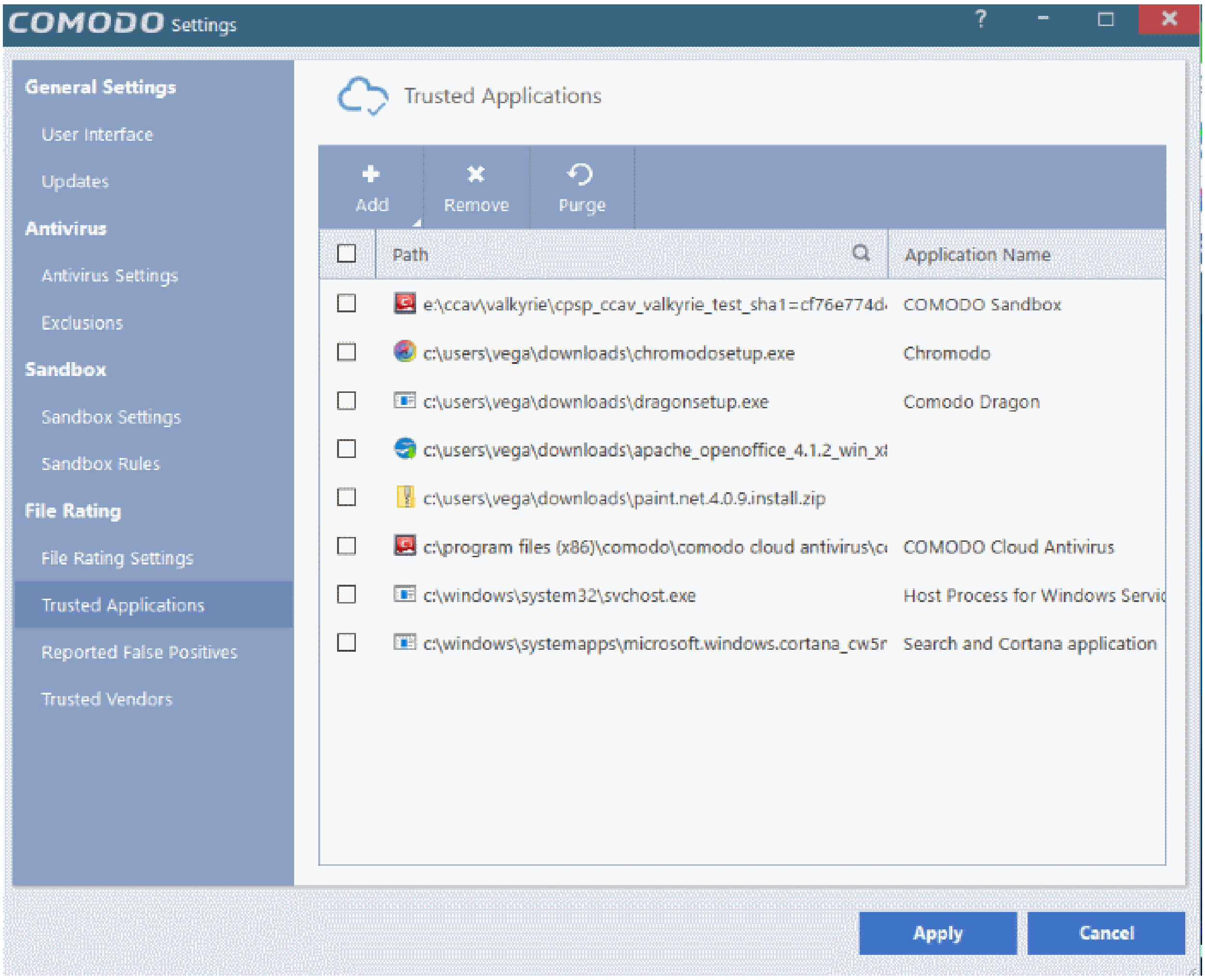
By granting 'Trusted' status to executables you can reduce the amount of alerts that Sandbox generates whilst maintaining a high level of security. This is particularly useful for developers that are creating new applications that, by their nature, are as yet unknown to the Comodo safe list.

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

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

To open the 'Trusted Applications' interface

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



☐	Path	Application Name
☐	e:\ccav\valkyrie\cpsp_ccav_valkyrie_test_sha1=cf76e774d	COMODO Sandbox
☐	c:\users\vega\downloads\chromodosetup.exe	Chromodo
☐	c:\users\vega\downloads\dragonsetup.exe	Comodo Dragon
☐	c:\users\vega\downloads\apache_openoffice_4.1.2_win_x	
☐	c:\users\vega\downloads\paint.net.4.0.9.install.zip	
☐	c:\program files (x86)\comodo\comodo cloud antivirus\c	COMODO Cloud Antivirus
☐	c:\windows\system32\svchost.exe	Host Process for Windows Servic
☐	c:\windows\systemapps\microsoft.windows.cortana_cw5r	Search and Cortana application

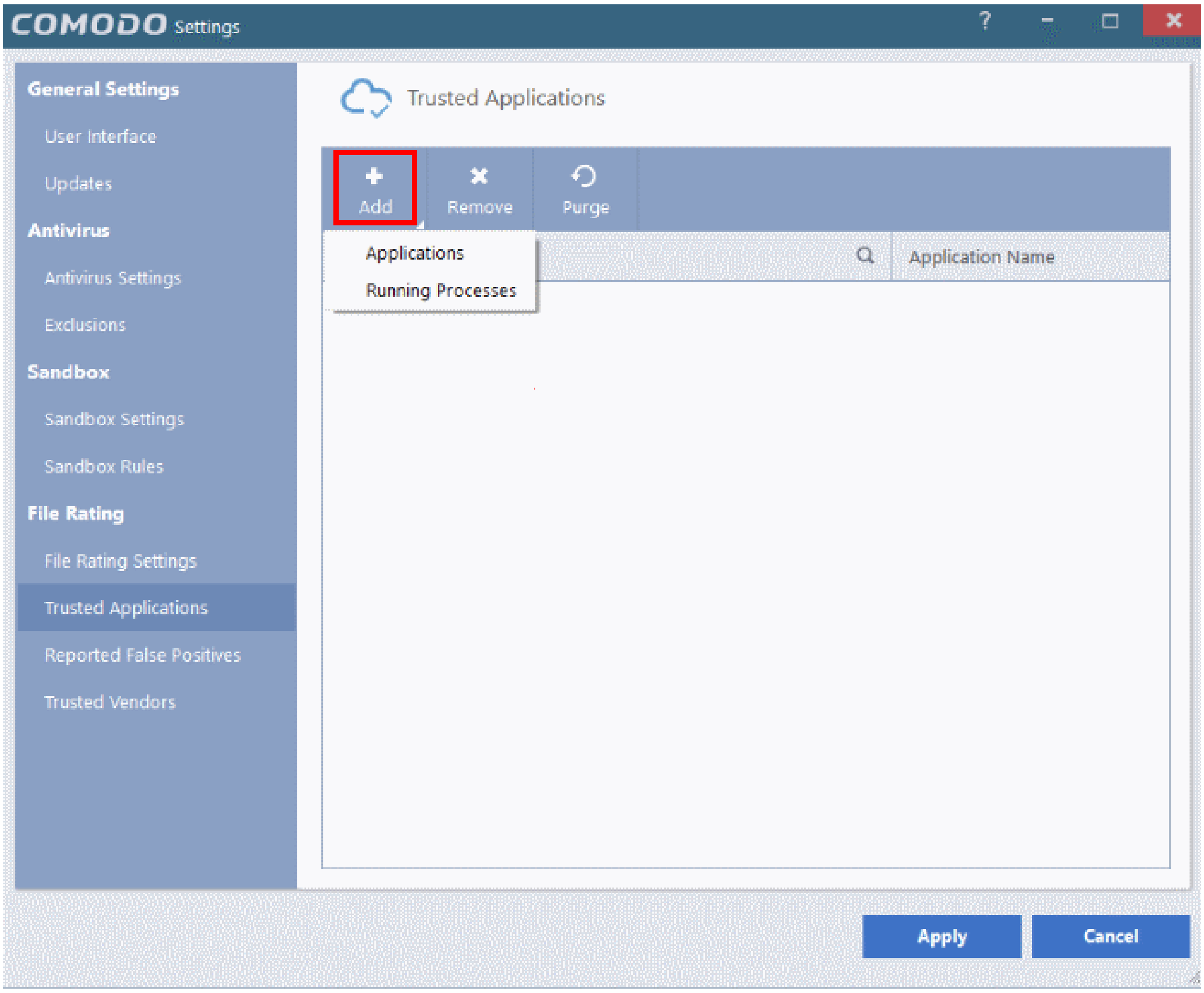
The interface displays a list of files added as 'Trusted Applications' with the following details:

- **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

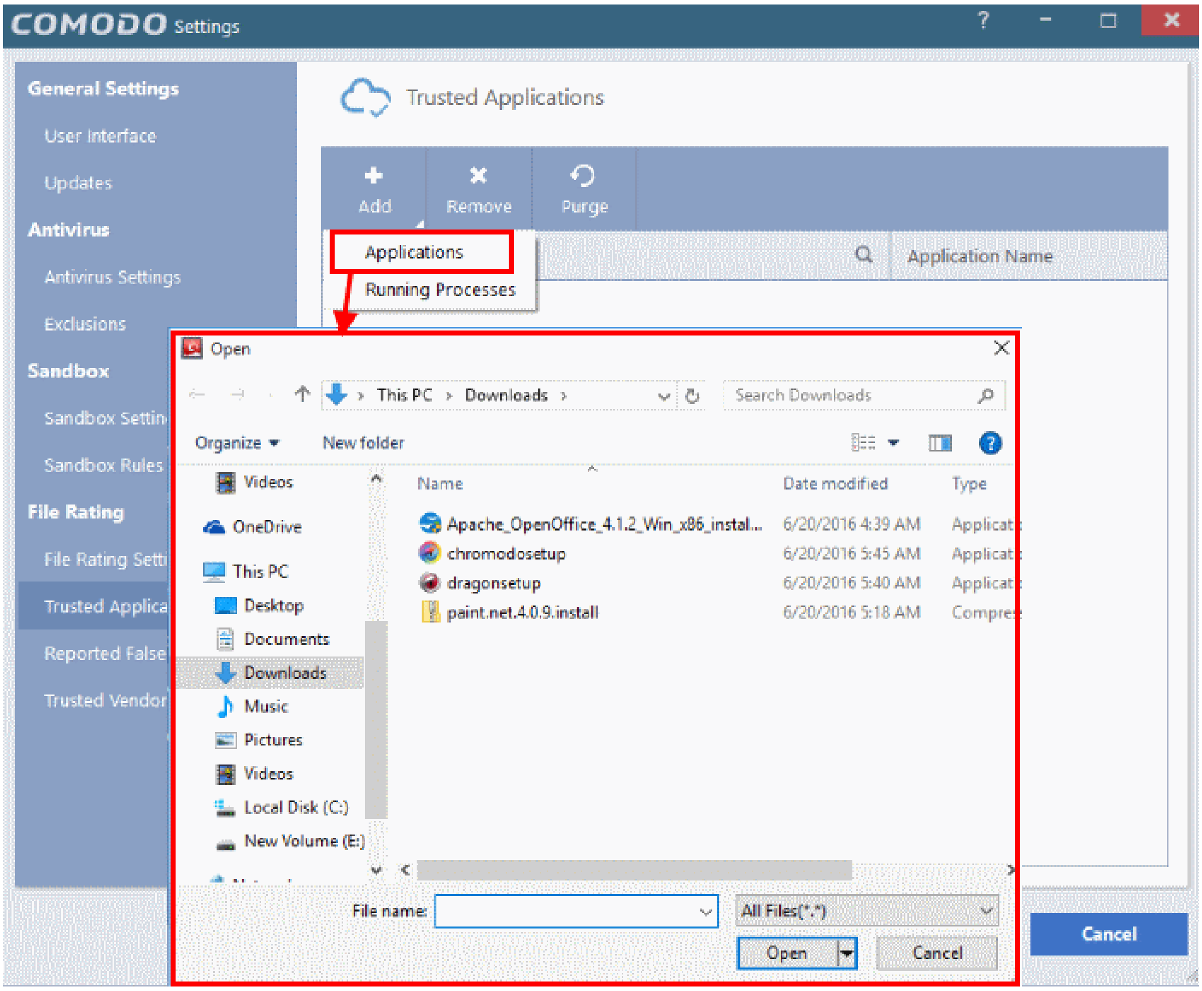


You can add an application by :

- 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'.



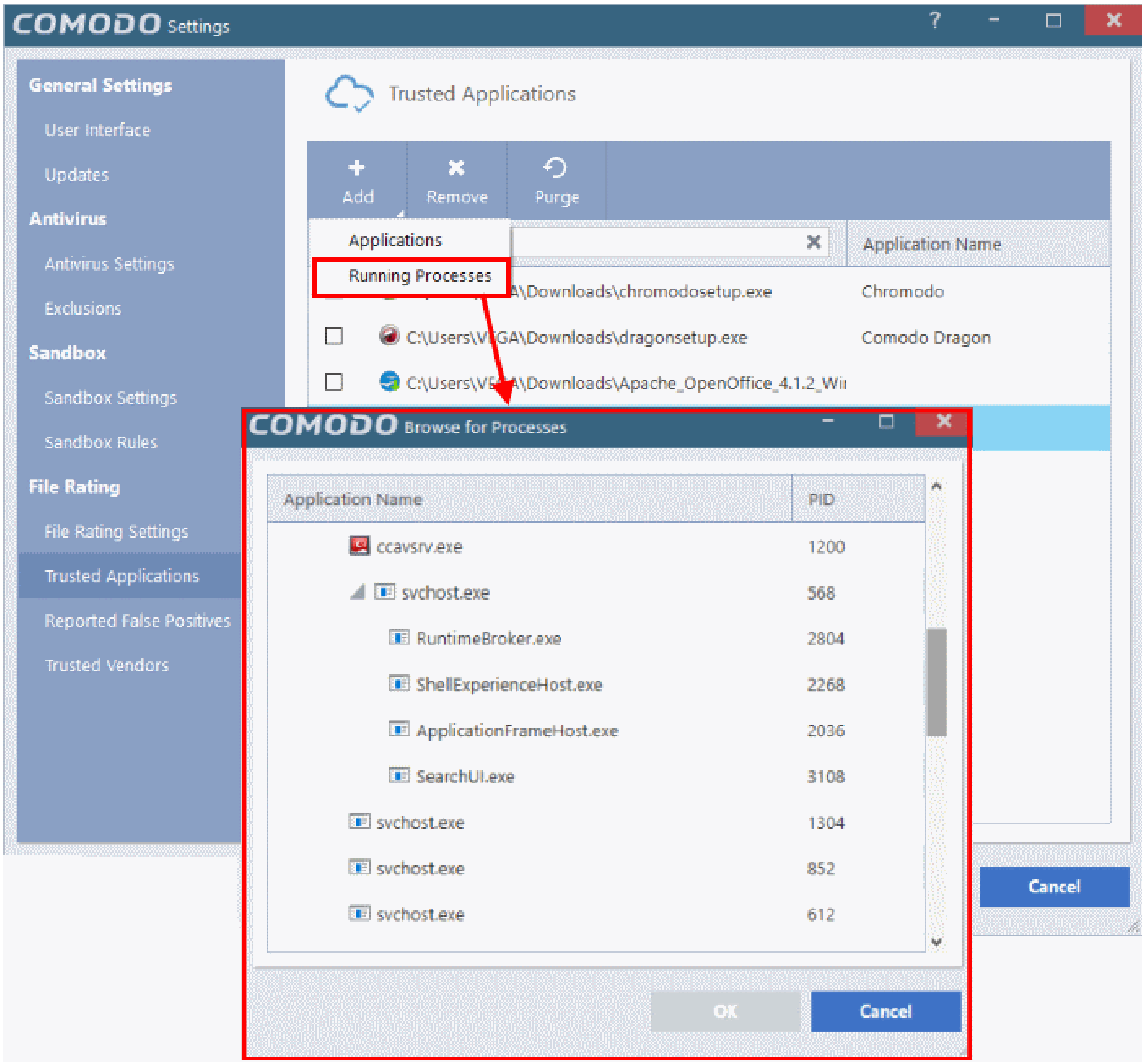
Name	Date modified	Type
Apache_OpenOffice_4.1.2_Win_x86_instal...	6/20/2016 4:39 AM	Applicat
chromodosetup	6/20/2016 5:45 AM	Applicat
dragonsetup	6/20/2016 5:40 AM	Applicat
paint.net.4.0.9.install	6/20/2016 5:18 AM	Compre

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

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

To add applications from Running processes

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

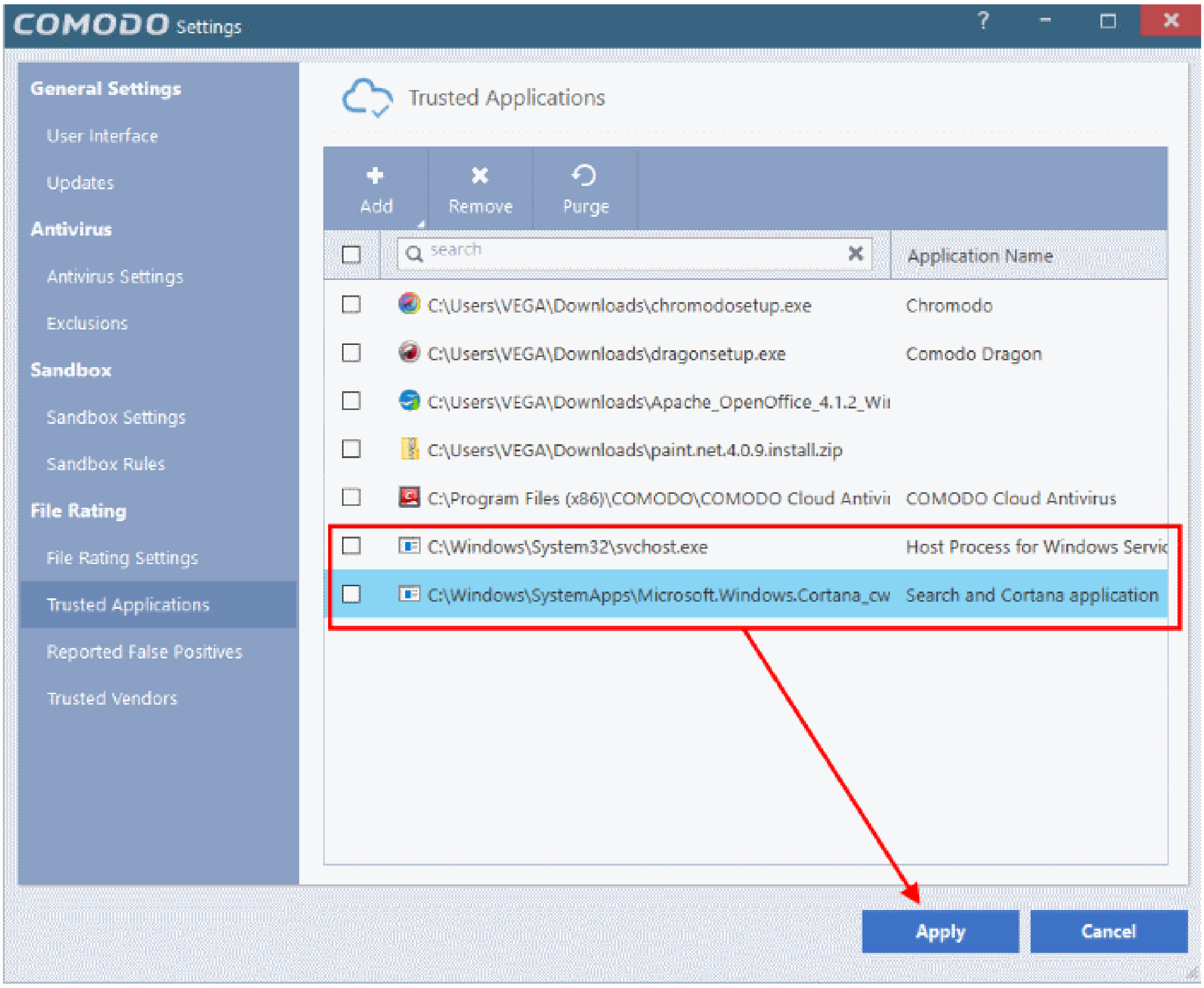


	Application Name
☐ …A\Downloads\chromodosetup.exe	Chromodo
☐ C:\Users\V…GA\Downloads\dragonsetup.exe	Comodo Dragon
☐ C:\Users\V…A\Downloads\Apache_OpenOffice_4.1.2_Wi	

Application Name	PID
ccavsrv.exe	1200
svchost.exe	568
RuntimeBroker.exe	2804
ShellExperienceHost.exe	2268
ApplicationFrameHost.exe	2036
SearchUI.exe	3108
svchost.exe	1304
svchost.exe	852
svchost.exe	612

- Select the process you wish to add to trusted applications and click 'OK'.

The selected applications will be added to the 'Trusted Applications' list.



□		Application Name
□	C:\Users\VEGA\Downloads\chromodosetup.exe	Chromodo
□	C:\Users\VEGA\Downloads\dragonsetup.exe	Comodo Dragon
□	C:\Users\VEGA\Downloads\Apache_OpenOffice_4.1.2_Wi	
□	C:\Users\VEGA\Downloads\paint.net.4.0.9.install.zip	
□	C:\Program Files (x86)\COMODO\COMODO Cloud Antivi	COMODO Cloud Antivirus
□	C:\Windows\System32\svchost.exe	Host Process for Windows Servic
□	C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw	Search and Cortana application

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

To remove item(s) from the Trusted Applications list

- Select the 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.

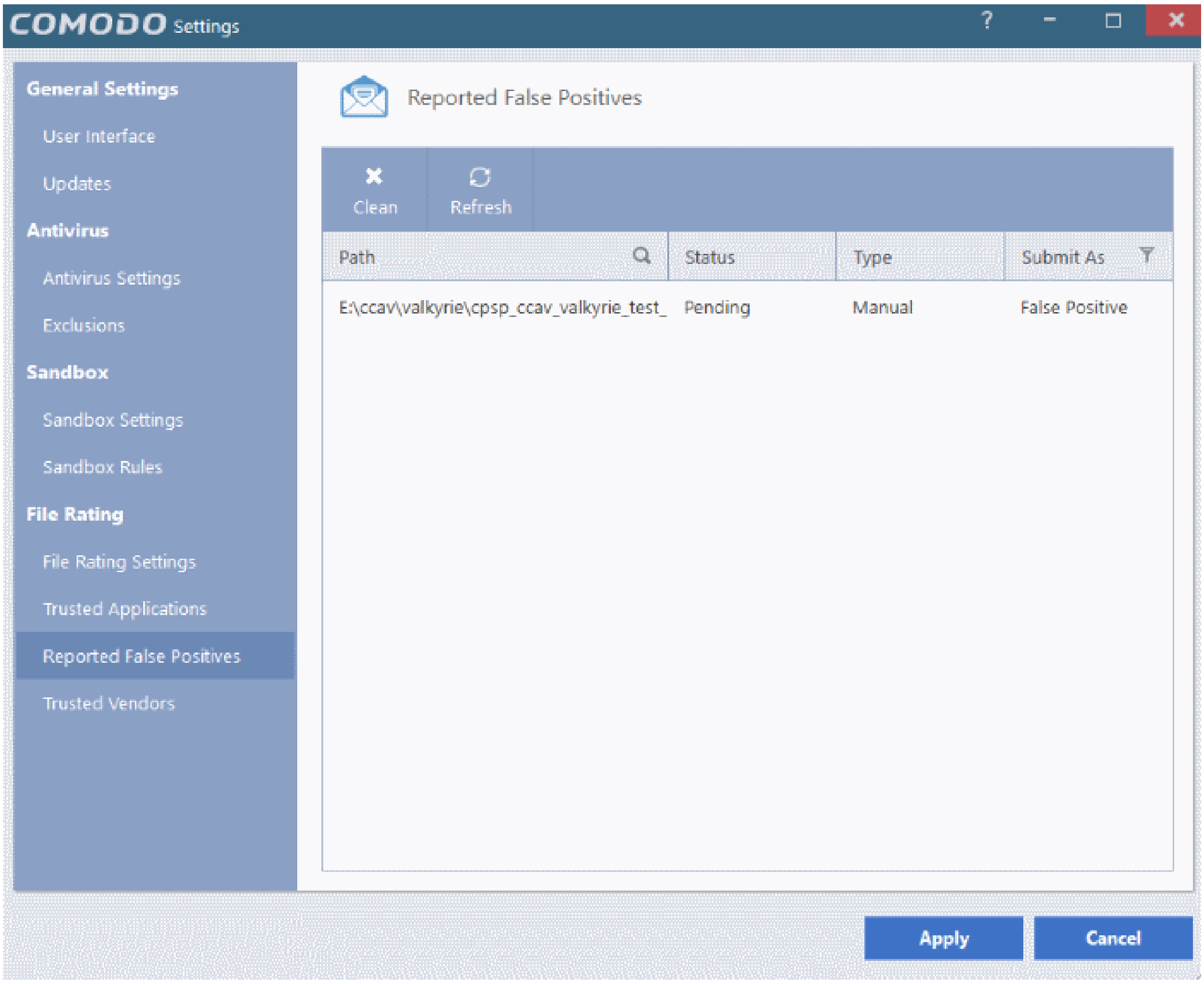
6.4.3. Reported False Positives

Files identified as 'unknown' or 'malicious' are queued for submission 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 'Reported False Positives' area allows you to view files you have submitted for analysis to Comodo.

To open the 'Reported False Positives' interface

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



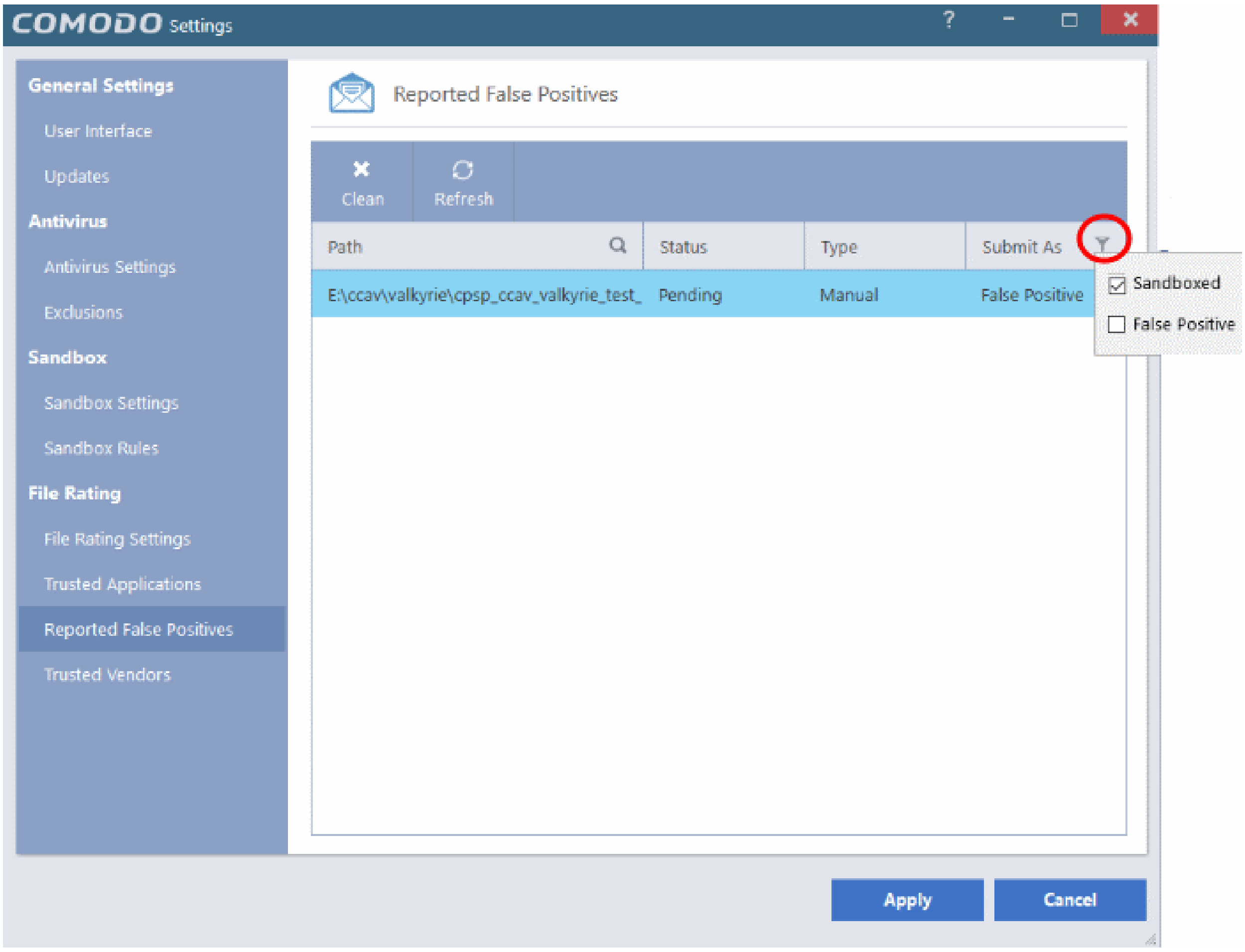
Path	Status	Type	Submit As
E:\ccav\valkyrie\cpsp_ccav_valkyrie_test_	Pending	Manual	False Positive

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

- **Path** - The installation path of the application/executable file
- **Status** - The precise status of the file submitted.
- **Type** - The type of submission of file.
- **Submitted As** - Indicates whether the file was submitted as an auto-sandboxed file or as a false positive from an antivirus scan.

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

You can filter the results to show only Sandboxed or False Positives by clicking the funnel icon beside the 'Submit As' column header.



Path	Status	Type	Submit As
E:\ccav\valkyrie\cpsp_ccav_valkyrie_test_	Pending	Manual	False Positive

☑ Sandboxed
□ False Positive

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

6.4.4. Trusted Vendors

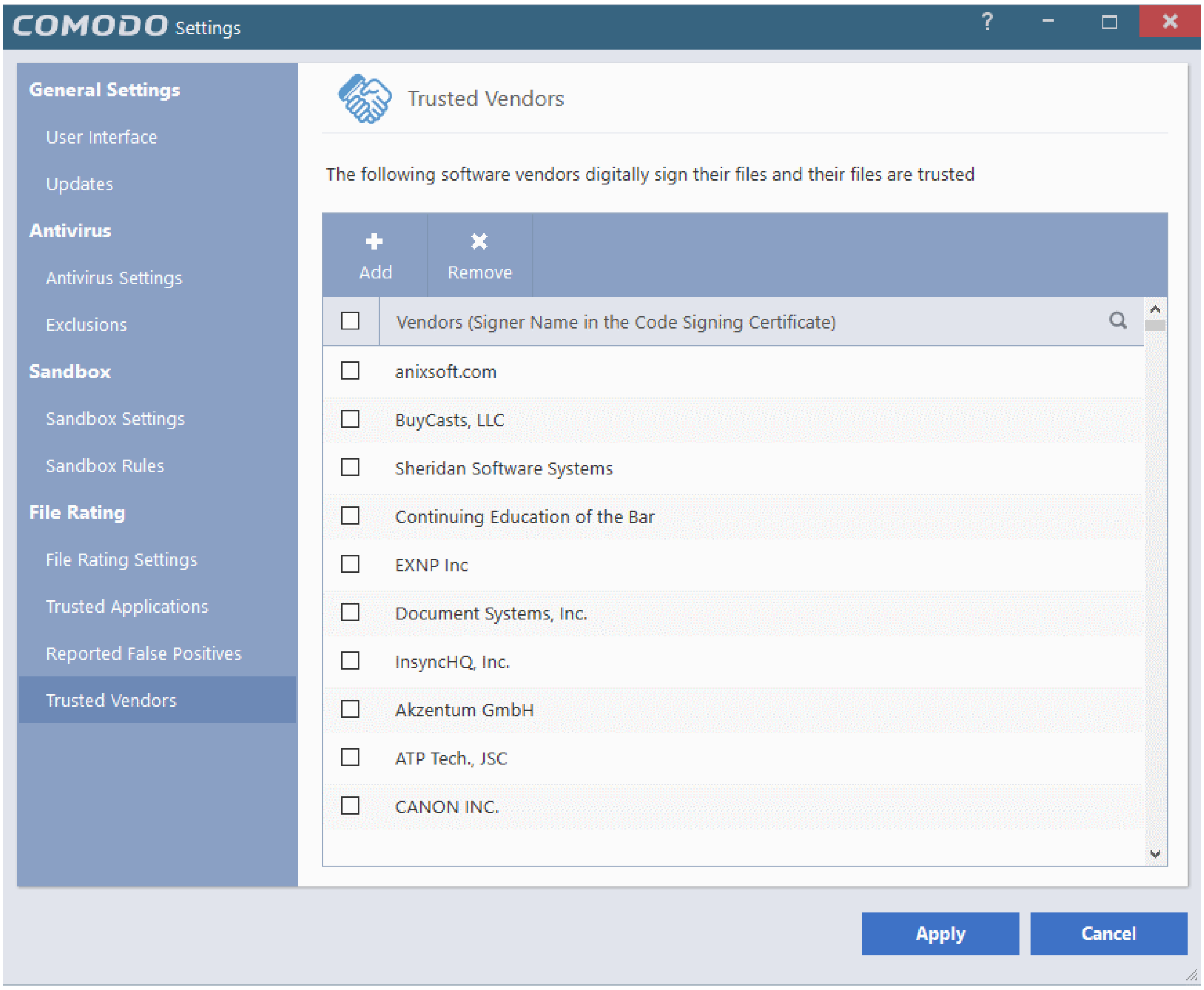
In Comodo Cloud Antivirus, there are three basic methods in which an application can be treated as safe. Either it has to be part of the Comodo 'Safe List' (of known-safe software), or the application is signed by one of the vendors in the 'Trusted Software Vendor List', or the file is added to the list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

Software publishers may be interested to know that they can have their signatures added, free of charge, to the 'master' Trusted Software Vendor List that ships with CCAV. Details about this can be found at the foot of this page.

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

To open the 'Trusted Vendors' interface

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



Trusted Vendors

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

□	Vendors (Signer Name in the Code Signing Certificate)
□	anixsoft.com
□	BuyCasts, LLC
□	Sheridan Software Systems
□	Continuing Education of the Bar
□	EXNP Inc
□	Document Systems, Inc.
□	InsyncHQ, Inc.
□	Akzentum GmbH
□	ATP Tech., JSC
□	CANON INC.

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

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

Background

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

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

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

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

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

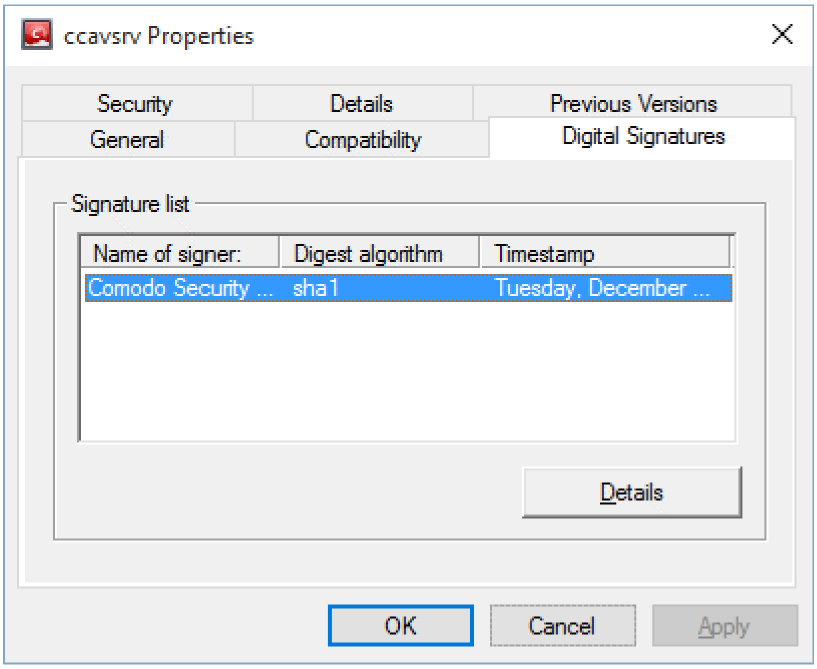
However, companies can't just 'sign' their own software and expect it to be trusted. This is why each code signing certificate is counter-signed by an organization called a 'Trusted Certificate Authority'. 'Comodo CA Limited' and 'Verisign' are two examples of a Trusted CA's and are authorized to counter-sign 3rd party software. This counter-signature is critical to the trust process and a Trusted CA only counter-signs a vendor's certificate after it has conducted detailed checks that the vendor is a legitimate company.

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

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

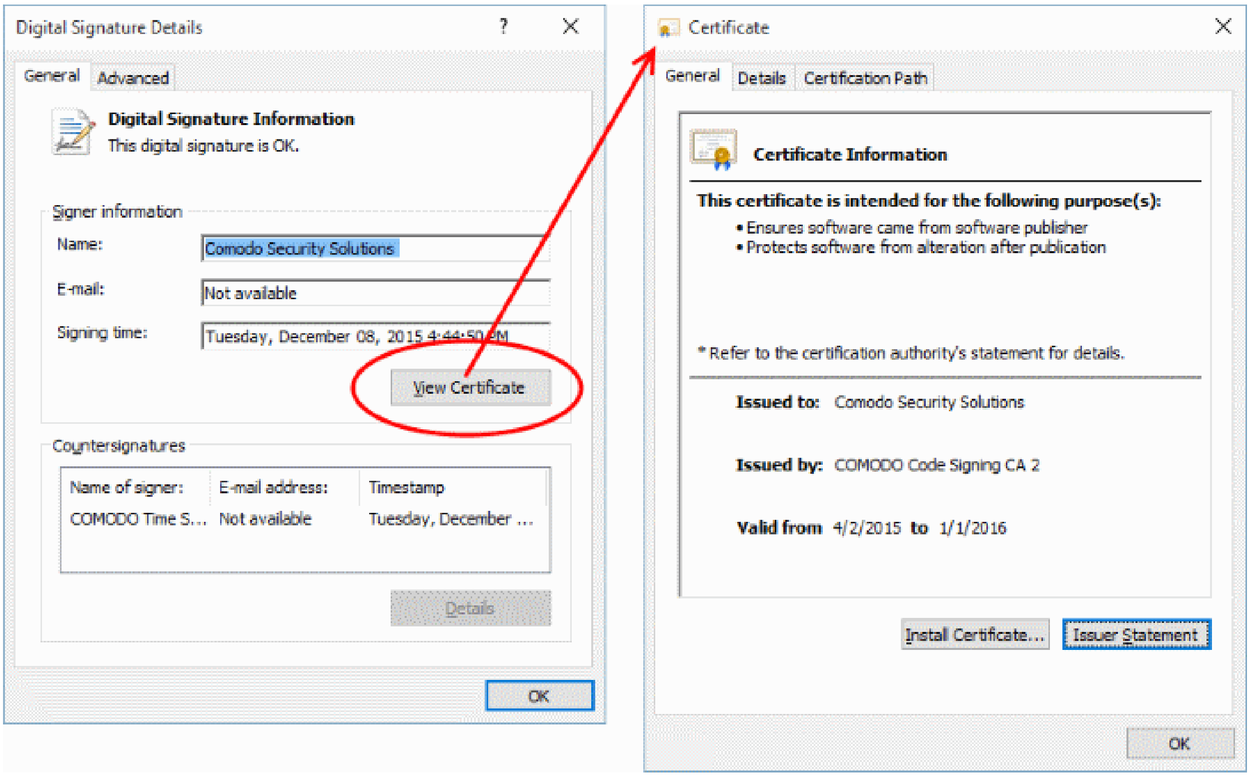
- Browse to the (default) installation directory of CCAV.
- Right click on the file 'ccavsrv.exe'.
- Select 'Properties' from the menu.
- Click the tab 'Digital Signatures (if there is no such tab then the software has not been signed).

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



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

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



Digital Signature Information
This digital signature is OK.

Signer information
Name: Comodo Security Solutions
E-mail: Not available
Signing time: Tuesday, December 08, 2015 4:44:50 PM

Countersignatures

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

Certificate Information

This certificate is intended for the following purpose(s):
- Ensures software came from software publisher
- Protects software from alteration after publication

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

Issued to: Comodo Security Solutions

Issued by: COMODO Code Signing CA 2

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

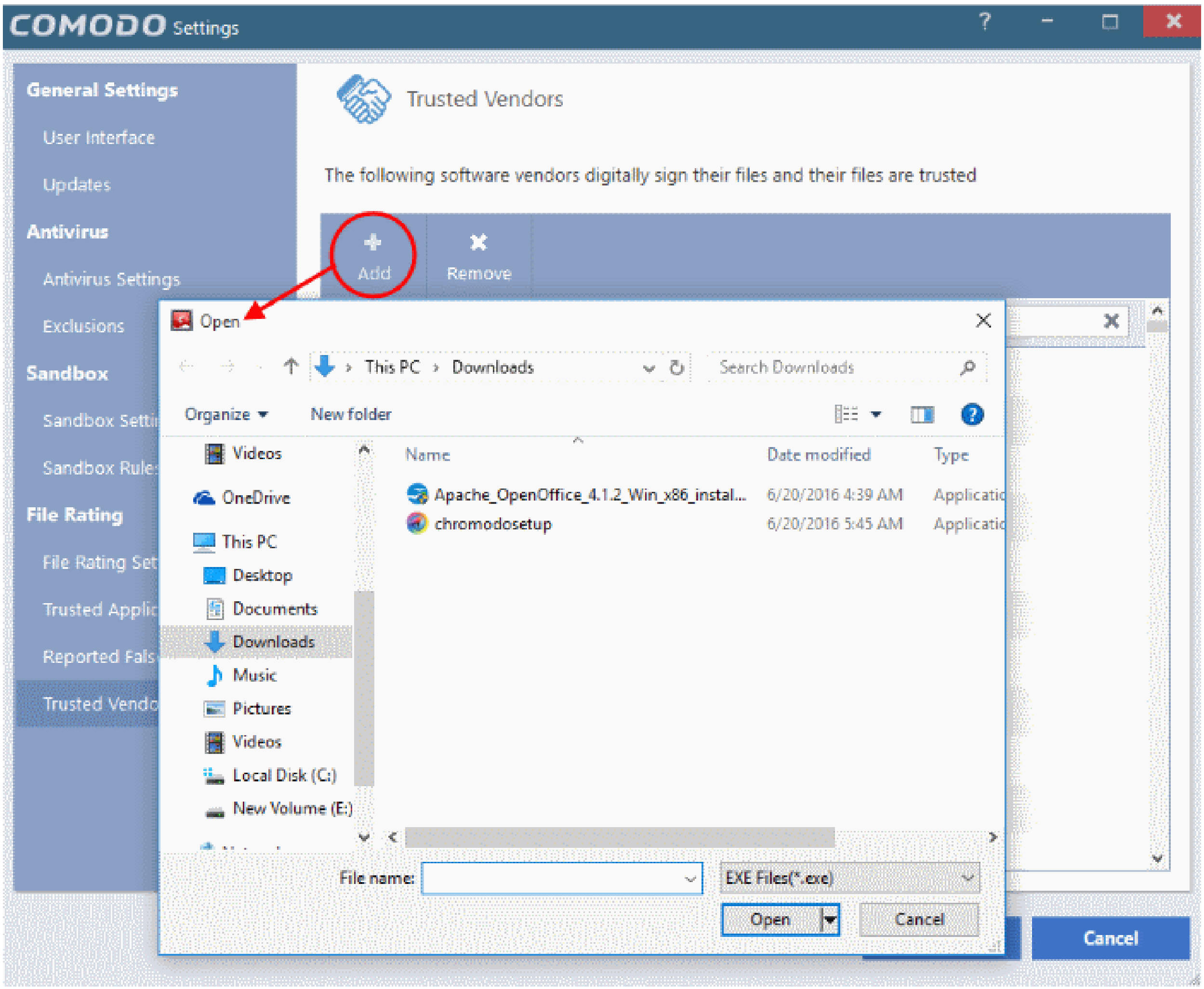
It should be noted that the example above is a special case in that Comodo, as creator of 'ccavsrv.exe', is both the signer of the software and, as a trusted CA, it is also the counter-signer (see the 'Countersignatures' box). In the vast majority of cases, the signer or the certificate (the vendor)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

Adding and Defining a User-Trusted Vendor

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

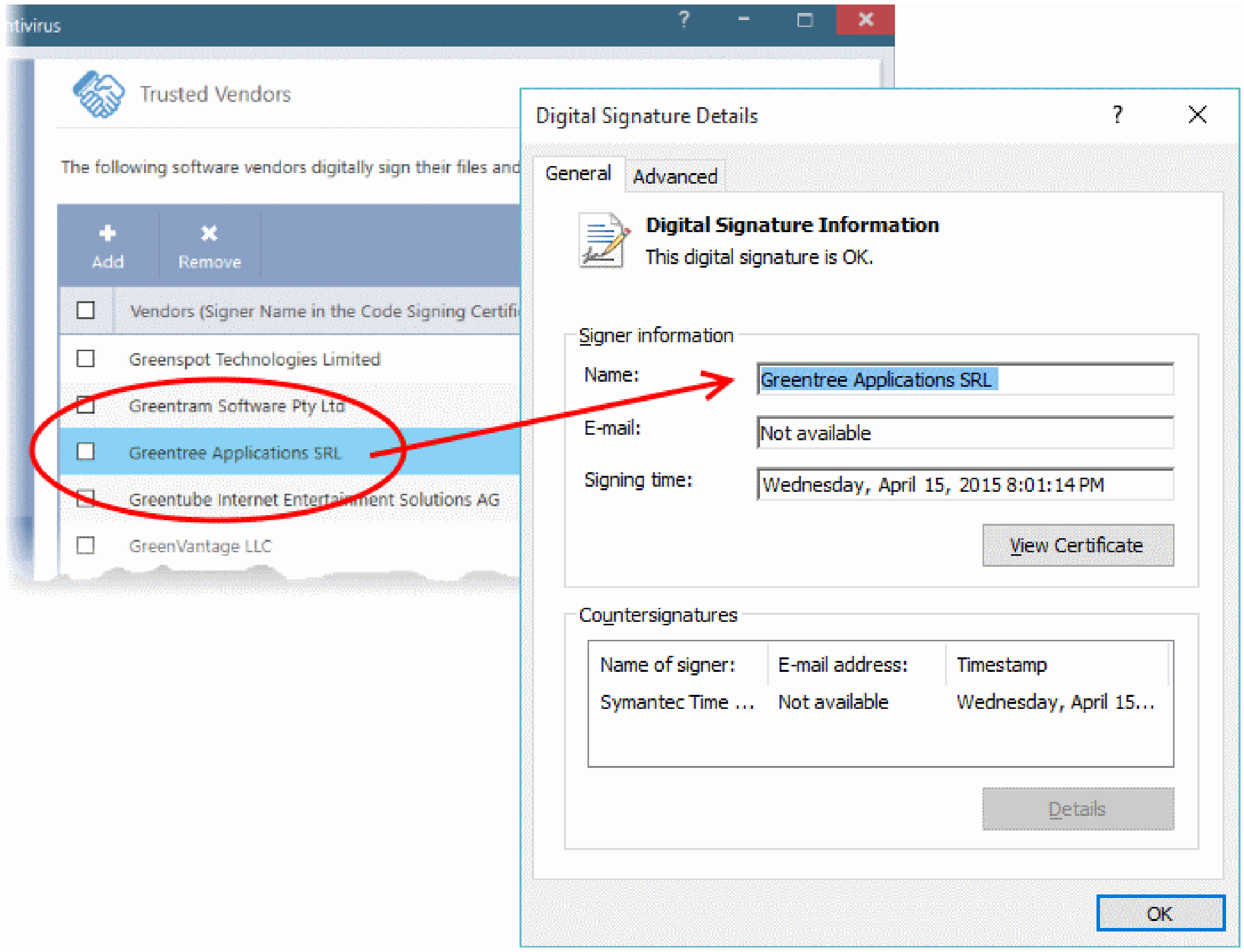
To add a trusted vendor

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



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

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



The following software vendors digitally sign their files and

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

Digital Signature Information
This digital signature is OK.

Signer information

Name: Greentree Applications SRL

E-mail: Not available

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

Countersignatures

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

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

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

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

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

The Trusted Vendor Program for Software Developers

Software vendors can have their software added to the default 'Trusted Vendor List' that is shipped with Comodo Cloud Antivirus. This service is free of cost and is also open to vendors that have used code signing certificates from any Certificate Authority. Upon adding the software to the Trusted Vendor list, CCAV automatically trusts the software and does not generate any warnings or alerts on installation or use of the software.

The vendors have to apply for inclusion in the Trusted Vendors list through the sign-up form at http://internetsecurity.comodo.com/trustedvendor/signup.php and make sure that the software can be downloaded by our technicians. Our technicians check whether:

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

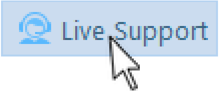
before adding it to the default Trusted Vendor list of the next release of CCAV.

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

7. 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.

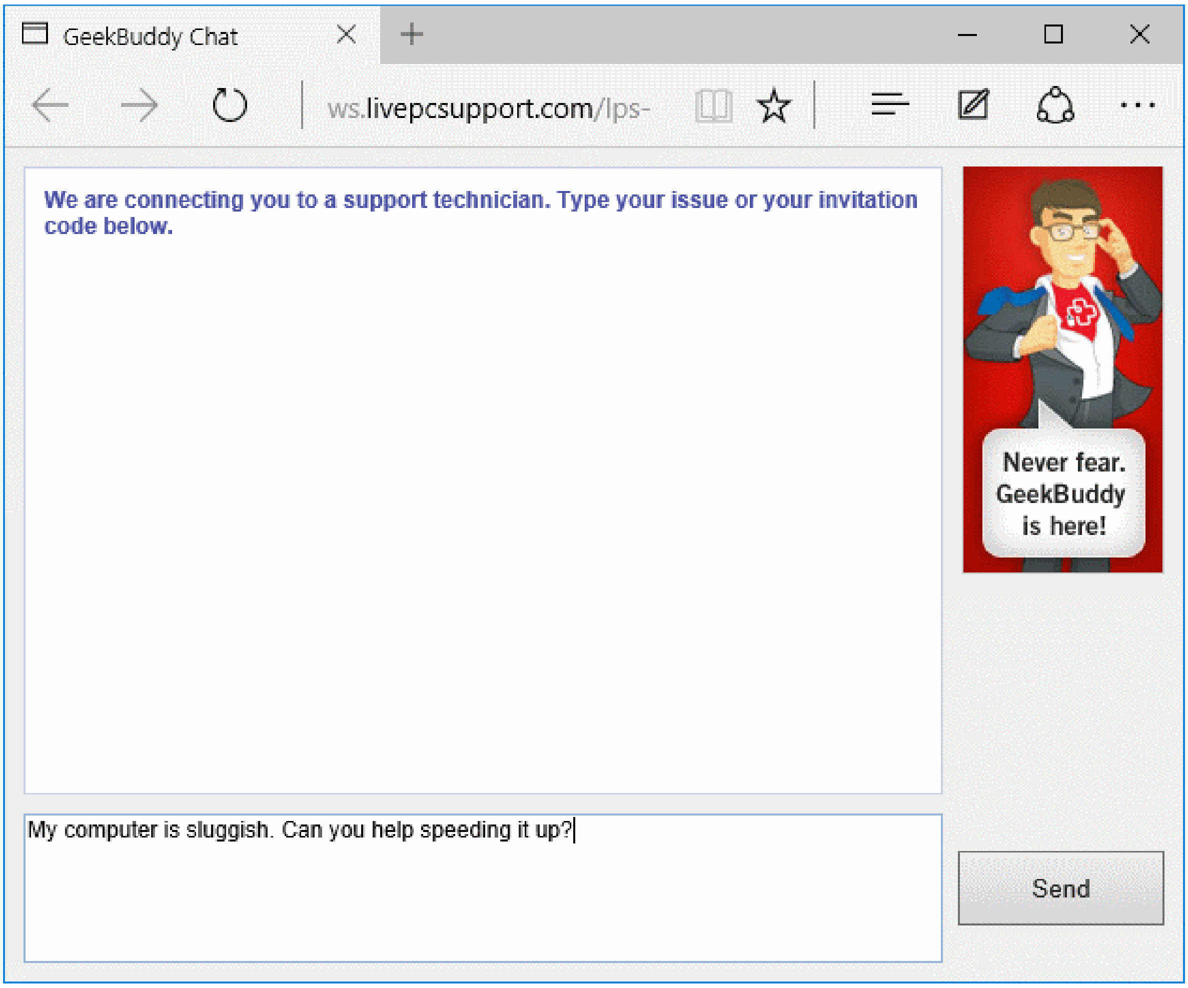
To get an instant support

- Click the 'Live Support' button  from the menu bar

OR

- Click Help at the top right and choose 'Live Support' from the options

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



We are connecting you to a support technician. Type your issue or your invitation code below.

My computer is sluggish. Can you help speeding it up?

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.

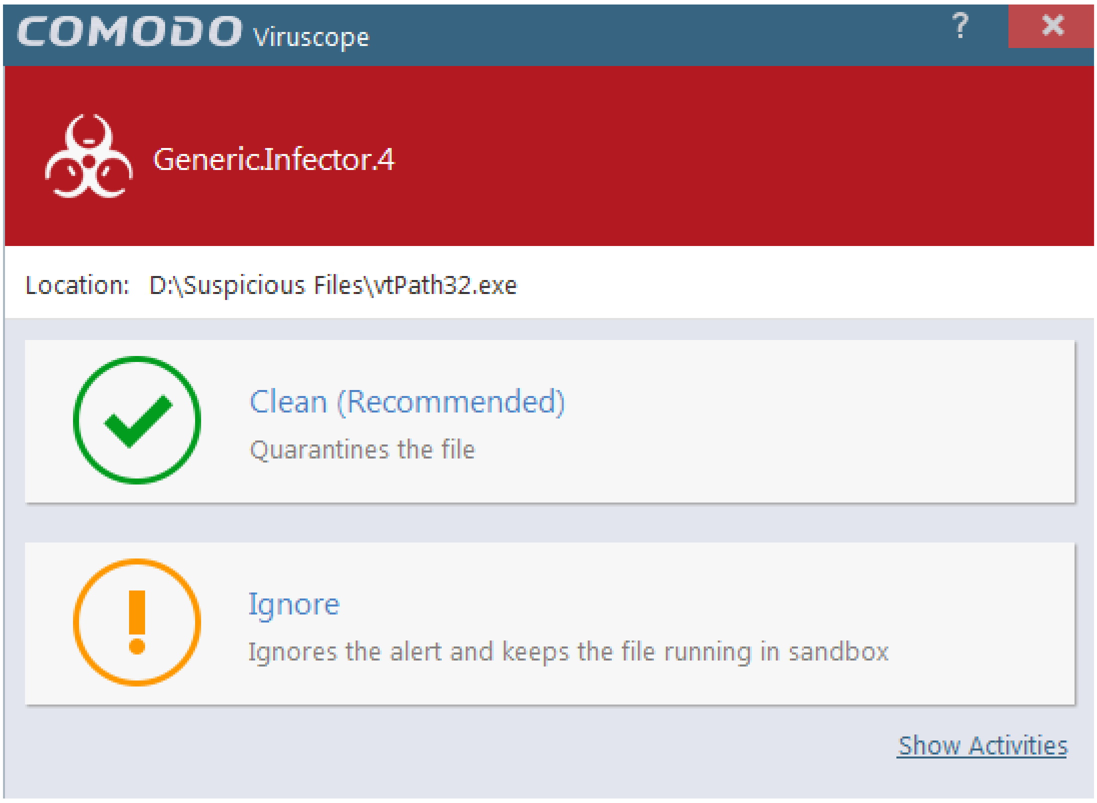
8. Viruscope - Feature Spotlight

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

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

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

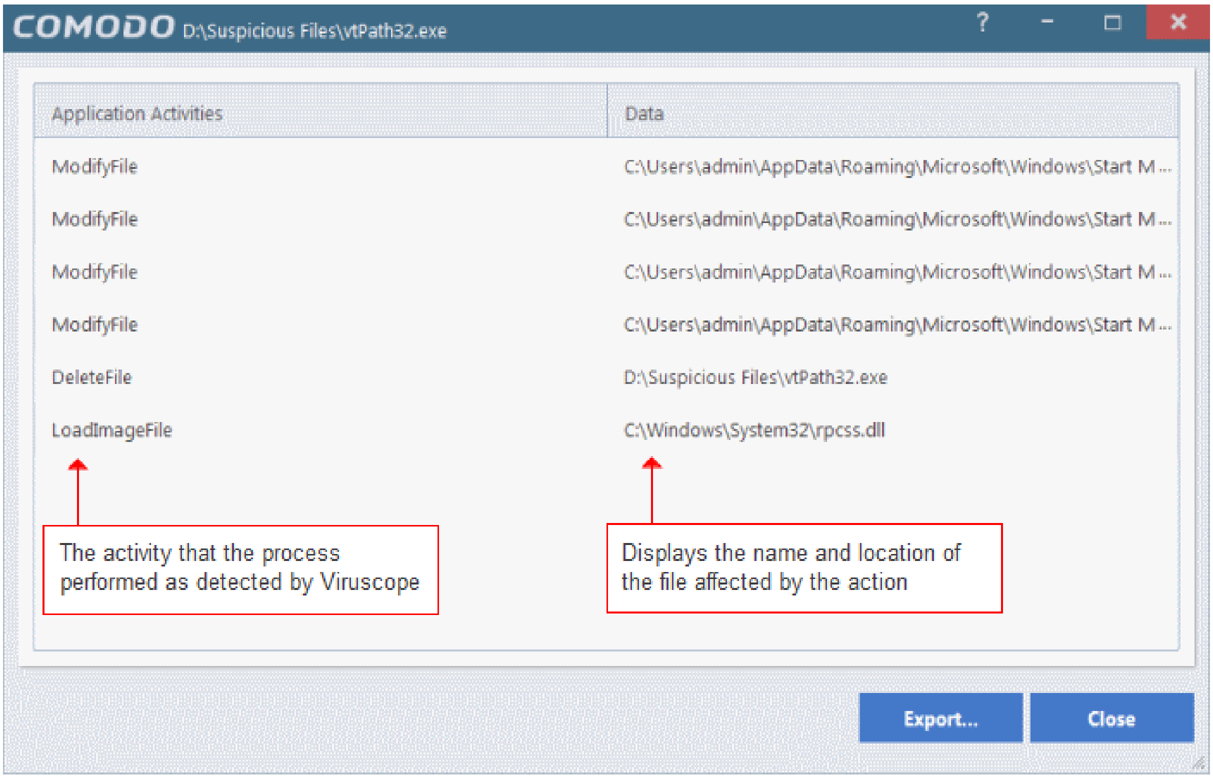
You will see an alert if Viruscope discovers a sandboxed process or an installer/updater is behaving in a suspicious manner:



Generic.Infector.4

Location: D:\Suspicious Files\vtPath32.exe

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



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

The activity that the process performed as detected by Viruscope

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

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

What are behavior recognizers?

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

File activities:

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

Registry activities:

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

Process activities:

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

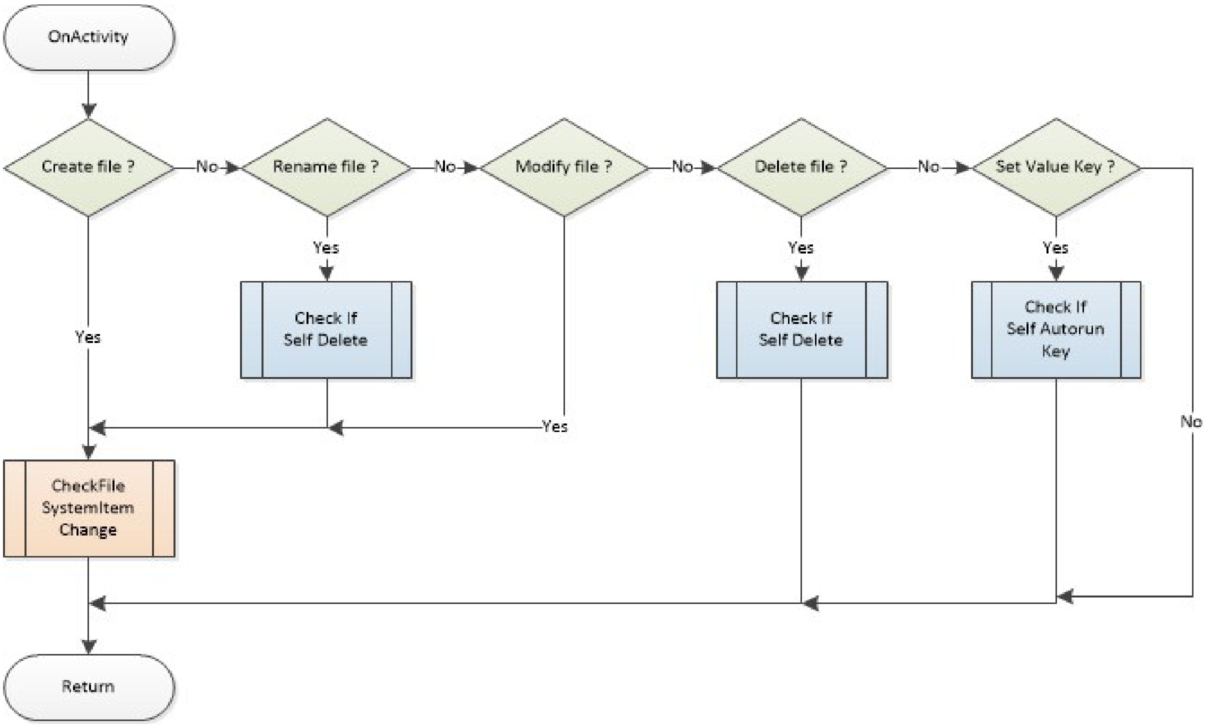
Technically, the core Viruscope technology contains the following items:

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

It will use these items to execute the following tasks:

- After queing the activities of each process, the worker thread will sequentially send each one to the behavior recognizers for analysis.
- A recognizer may traverse the entire process tree and activity list created by Viruscope.
- A recognizer may build its own process tree (the default recognizer uses this technique) and/or queue of activities (the default recognizer doesn't use a cache of activities)

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



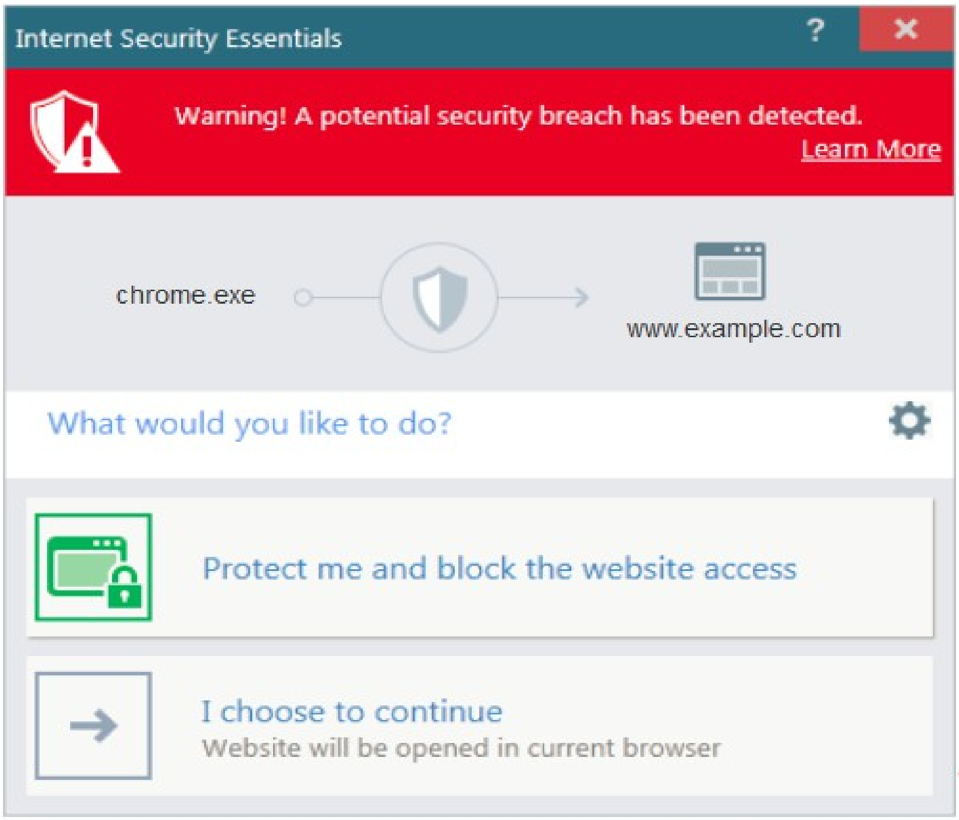
Viruscope is another key layer of security in the CCAV arsenal, taking our protection beyond that found in any other antivirus product. Our real-time virus monitor protects you against known threats, while auto-sandboxing protects you against unknown threats. With Viruscope on top, you also get proactive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

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 malcious certificate. You will have the option to discontinue the connection (recommended) or to continue.



Internet Security Essentials

Warning! A potential security breach has been detected.

What would you like to do?

Protect me and block the website access

I choose to continue

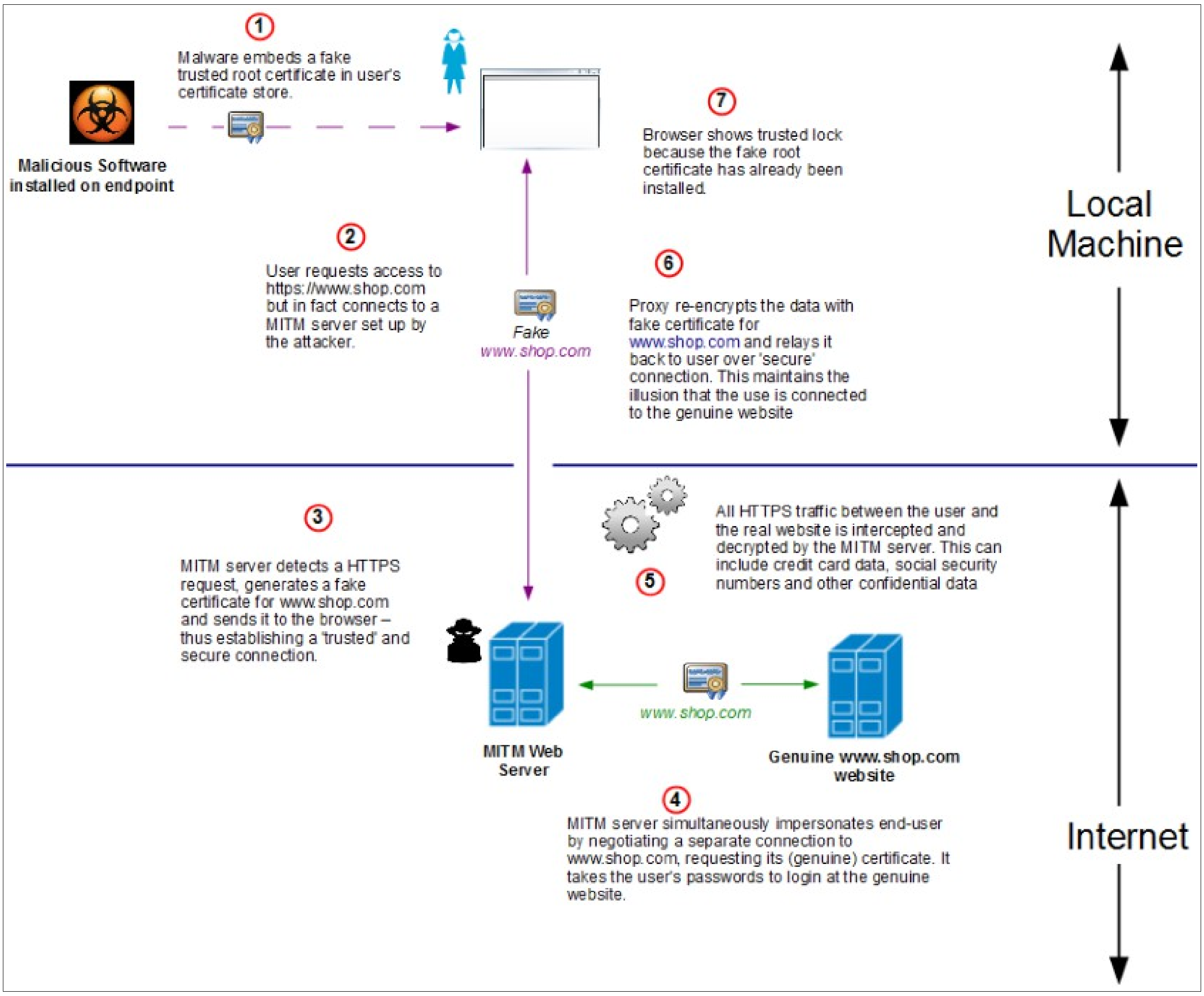
Website will be opened in current browser

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?

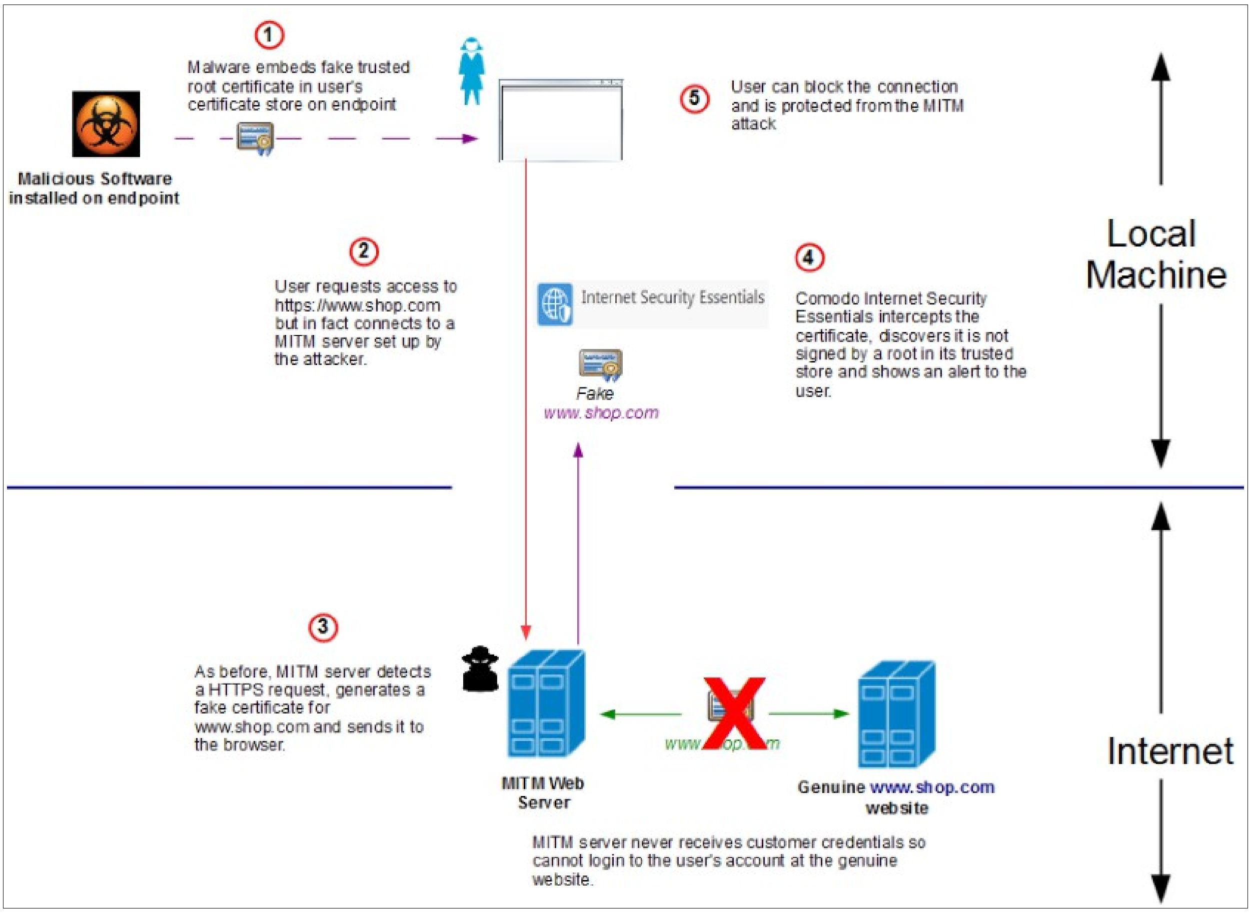
Man-in-the-middle attacks occur when an attacker forces a client to connect to a server other than the one that the client intended to connect.

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:


1
Malware embeds a fake trusted root certificate in user's certificate store.
Malicious Software installed on endpoint
7
Browser shows trusted lock because the fake root certificate has already been installed.
Local Machine
2
User requests access to https://www.shop.com but in fact connects to a MITM server set up by the attacker.
Fake www.shop.com
6
Proxy re-encrypts the data with fake certificate for www.shop.com and relays it back to user over 'secure' connection. This maintains the illusion that the use is connected to the genuine website
3
MITM server detects a HTTPS request, generates a fake certificate for www.shop.com and sends it to the browser – thus establishing a 'trusted' and secure connection.
5
All HTTPS traffic between the user and the real website is intercepted and decrypted by the MITM server. This can include credit card data, social security numbers and other confidential data
MITM Web Server
www.shop.com
Genuine www.shop.com website
4
MITM server simultaneously impersonates end-user by negotiating a separate connection to www.shop.com, requesting its (genuine) certificate. It takes the user's passwords to login at the genuine website.
Internet

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 follwing diagram shows hows CISE will thwart a man-in-the-middle attack:


1
Malware embeds fake trusted root certificate in user's certificate store on endpoint
Malicious Software installed on endpoint
5
User can block the connection and is protected from the MITM attack
2
User requests access to https://www.shop.com but in fact connects to a MITM server set up by the attacker.
Internet Security Essentials
Fake www.shop.com
4
Comodo Internet Security Essentials intercepts the certificate, discovers it is not signed by a root in its trusted store and shows an alert to the user.
Local Machine
Internet
3
As before, MITM server detects a HTTPS request, generates a fake certificate for www.shop.com and sends it to the browser.
MITM Web Server
www.shop.com
Genuine www.shop.com website
MITM server never receives customer credentials so cannot login to the user's account at the genuine website.

What is the install location of Comodo Internet Security Essentials?

By default, Comodo Intenet Security Essentials is installed at:

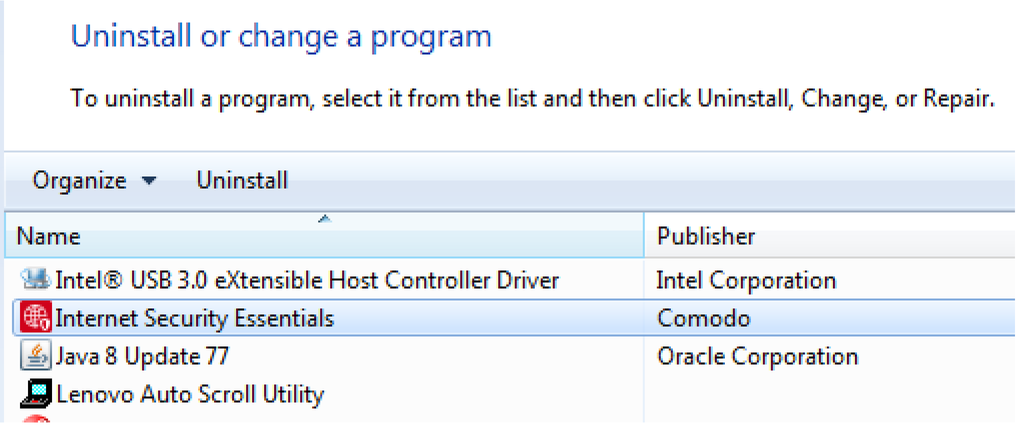
C:\Program Files (x86)\Comodo\Internet Security Essentials

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'



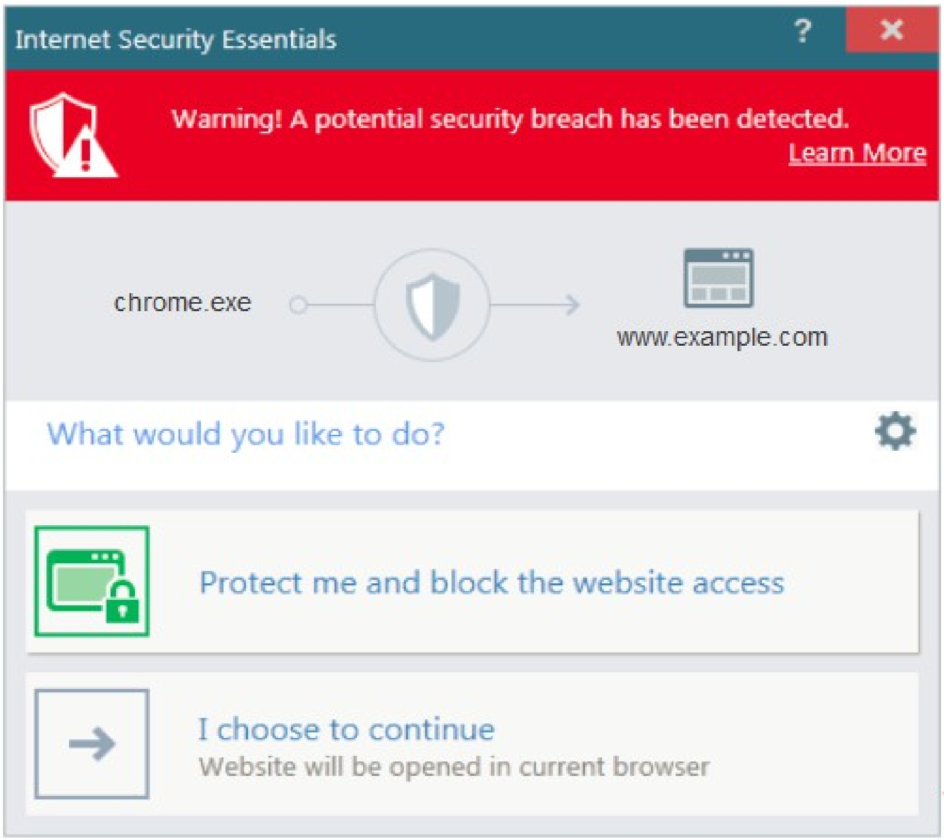
Uninstall or change a program

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

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	

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:



Internet Security Essentials

Warning! A potential security breach has been detected.

Learn More
chrome.exe
www.example.com

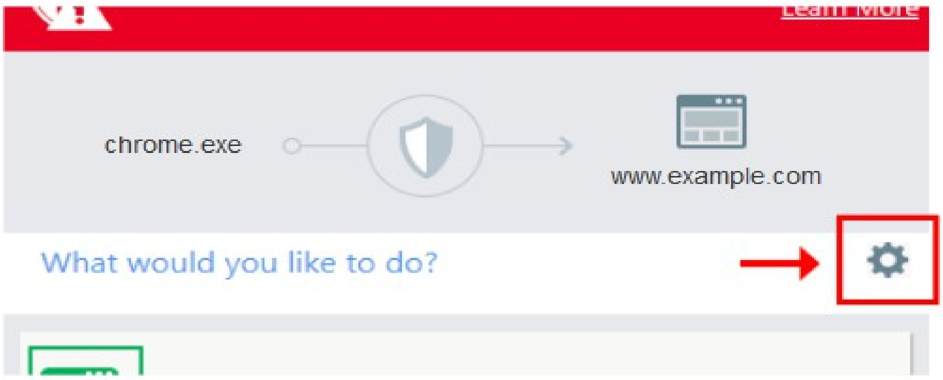
What would you like to do?

Protect me and block the website access
I choose to continue
Website will be opened in current browser

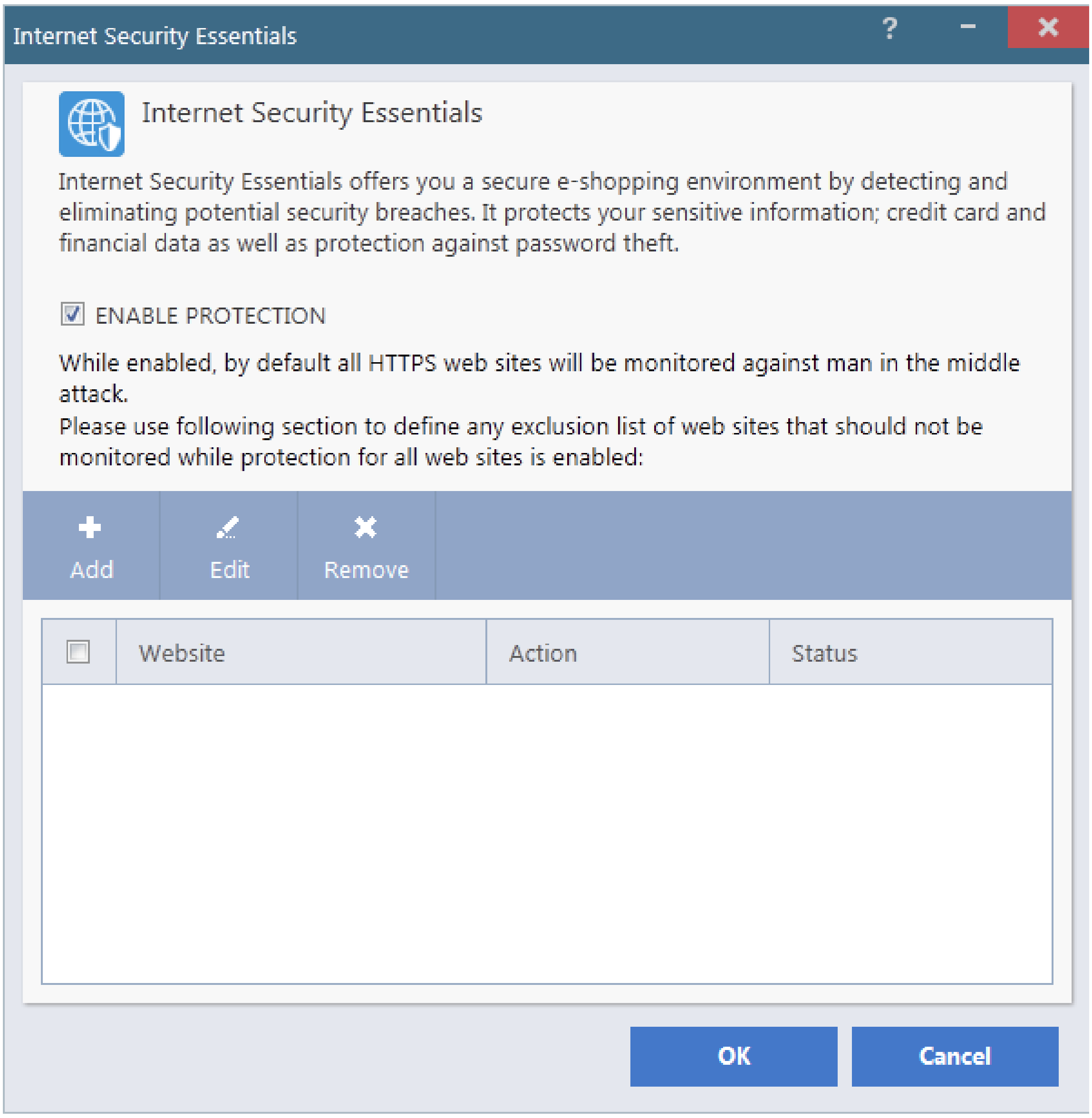
The alert means that the website you are visiting may be fraudulent as it is using a certificate signed by a root that is not in CISE's internal store of trusted root certificates.

- 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:



Internet Security Essentials

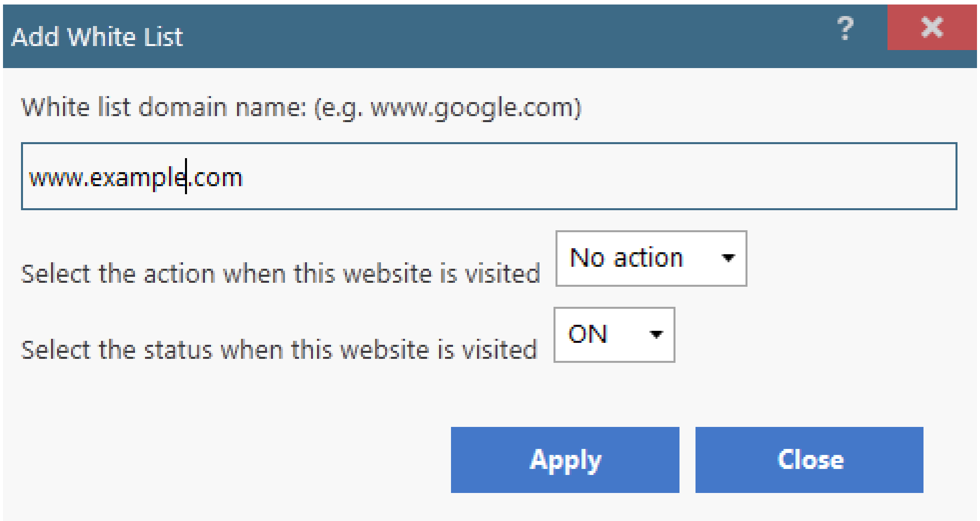
Internet Security Essentials offers you a secure e-shopping environment by detecting and eliminating potential security breaches. It protects your sensitive information; credit card and financial data as well as protection against password theft.

☑ ENABLE PROTECTION

While enabled, by default all HTTPS web sites will be monitored against man in the middle attack.
Please use following section to define any exclusion list of web sites that should not be monitored while protection for all web sites is enabled:

□	Website	Action	Status

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



Add White List

White list domain name: (e.g. www.google.com)

www.example.com

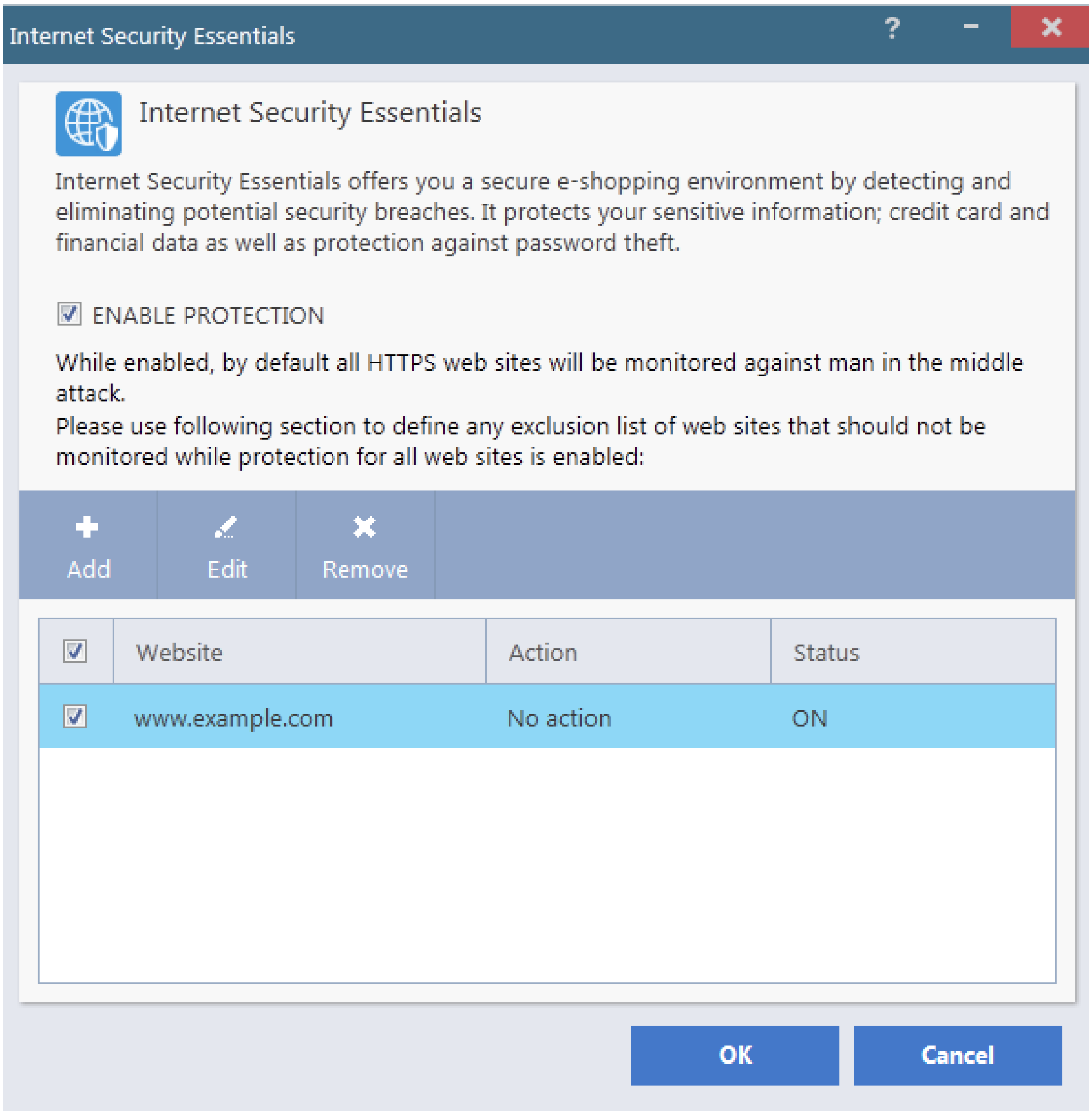
Select the action when this website is visited: No action

Select the status when this website is visited: ON

- 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:



Internet Security Essentials

Internet Security Essentials

Internet Security Essentials offers you a secure e-shopping environment by detecting and eliminating potential security breaches. It protects your sensitive information; credit card and financial data as well as protection against password theft.

☑ ENABLE PROTECTION

While enabled, by default all HTTPS web sites will be monitored against man in the middle attack.
Please use following section to define any exclusion list of web sites that should not be monitored while protection for all web sites is enabled:

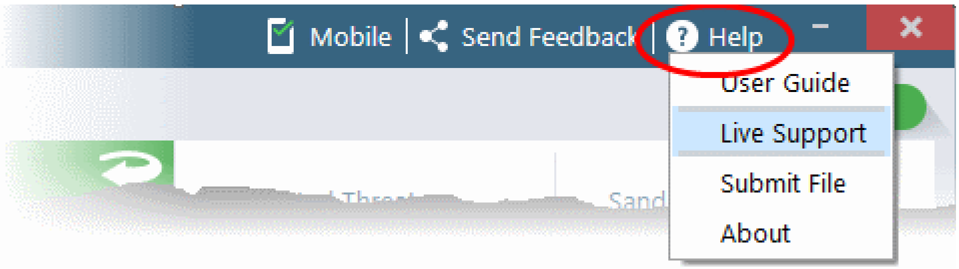
☑	Website	Action	Status
☑	www.example.com	No action	ON

- 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.

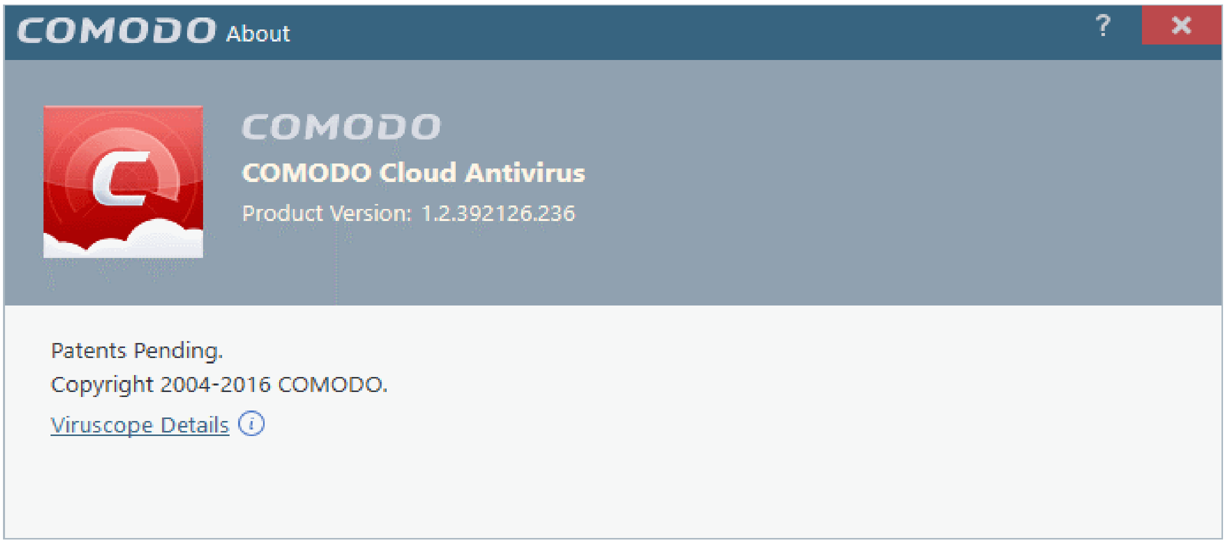
Click Here to find out more about Comodo Security Essentials.

10. Comodo Support and About Information

You can view the online help guide for Comodo Cloud Antivirus, start a chat support session with a technician at Comodo, submit a suspicious file for analysis and view the About dialog by clicking the 'Help' link at the top right.



- **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 also be added to the global whitelist and blacklist to help fellow CCAV users who encounter the same file. Refer to the section Viewing Valkyrie Analysis Results for more details.
- **About -** Displays the product version, details of active Viruscope Recognizers and copyright information.



COMODO

COMODO Cloud Antivirus

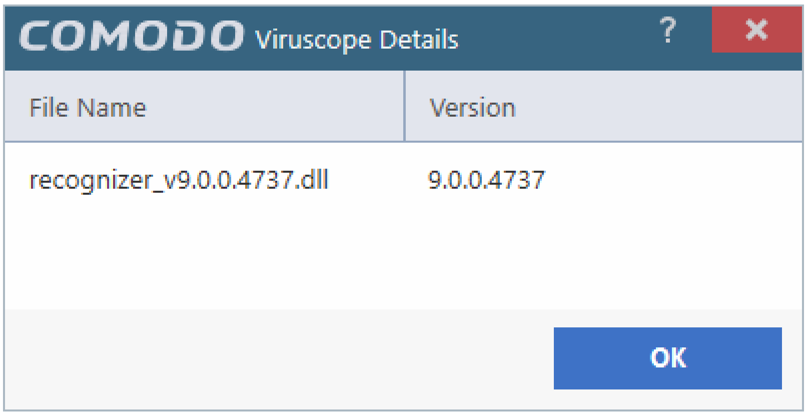
Product Version: 1.2.392126.236

Patents Pending.

Copyright 2004-2016 COMODO.

Viruscope Details

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



File Name	Version
recognizer_v9.0.0.4737.dll	9.0.0.4737

About Comodo

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

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

Comodo Security Solutions, Inc.

1255 Broad Street
Clifton, NJ, 07013
United States
Email: EnterpriseSolutions@Comodo.com

Comodo CA Limited

3rd Floor, 26 Office Village, Exchange Quay, Trafford Road, Salford, Greater Manchester M5 3EQ,
United Kingdom.
Tel : +44 (0) 161 874 7070
Fax : +44 (0) 161 877 1767

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